BAOU
Education for All

Dr. Babasaheb Ambedkar
Open University
(Established by Government of Gujarat)

Hacking Techniques

MSCCS-401

Master of Science
Cyber Security

2022

Hacking Techniques

Dr. Babasaheb Ambedkar Open University

System Analysis and Design

Expert Committee

Prof. (Dr.) Nilesh K. Modi Professor and Director, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad	(Chairman)
Prof. (Dr.) Ajay Parikh Professor and Head, Department of Computer Science Gujarat Vidyapith, Ahmedabad	(Member)
Prof. (Dr.) Satyen Parikh Dean, School of Computer Science and Application Ganpat University, Kherva, Mahesana	(Member)
M. T. Savaliya Associate Professor and Head Computer Engineering Department Vishwakarma Engineering College, Ahmedabad	(Member)
Mr. Nilesh Bokhani Assistant Professor, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad	(Member)
Dr. Himanshu Patel Assistant Professor, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad	(Member Secretary)

Course Writers

Bijay Kumar Paikaray	Centurion University of Technology and Management, Bhubaneswar

Content Editors

Prof. (Dr.) Nilesh K. Modi	Professor and Director, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad
Mr. Nilesh N. Bokhani	Assistant Professor School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad

Acknowledgement: The cont ent i n this book is modifications based on the work created and shared by the Odisha State Open University (OSOU) for the subject Hacking Techniques used according to terms described in Creative Commons Attribution-ShareAlike 4.0International (CC BY-SA 4.0)

ISBN -

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr. Babasaheb Ambedkar Open University

MSCCS-401

Hacking Techniques

BLOCK-1: INTRODUCTION TO HACKING

BLOCK-2: HACKING TECHNIQUES

BLOCK-3: HACKING WEB APPLICATIONS AND WIRELESS NETWORKS

Block

1 INTRODUCTION TO HACKING

UNIT-1 Overview of Hacking

Unit Structure

1.0 Introduction

In a cyber-security world, the person who is able to discover weakness in a system and manages to exploit it to accomplish his goal referred as a Hacker, and the process is referred as Hacking.

Now a day, people started thinking that hacking is only hijacking Facebook accounts or defacing websites. Yes, it is also part of hacking field but it doesn't mean that it is the main part of hacking.

So what is exactly hacking, what should we do to become a hacker? You need not worry; you will learn it from this unit. The main thing you need to become a hacker is to have self-interest. You should always ready to learn something and learn to create something new.

The term "white hat hacker" in Internet slang refers to an ethical computer hacker, or a computer security expert, who specializes in penetration and in other testing methodologies to ensure the security of an organization's information systems. Hacking is a term coined by IBM meant to imply a broader category than just penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively.

1.1 Learning Objective

After learning this unit you should be able to

- Know about hacking and hacker.
- Know about who is a hacker and how to attack?
- Identify different types of hackers.
- Learn more about different types of cybercrimes.
- Revisit the concepts of security threats and its types.
- Identify the programming languages that are useful to hackers.
- Learn more about the concept of Ethical Hacking.
- Explain the Phases of Ethical Hacking
- Differentiate between Hackers and Crackers
- Know the advantages and disadvantages of Ethical Hacking.

1.2 What is Hacking?

” Hacking is art of exploring the hidden things that are being hidden from general usage and finding loop holes in the security and use them to benefit the others”

In another way we can tell Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.

Example of Hacking: Using password cracking algorithm to gain access to a system.

Computers have become mandatory to run a successful business. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. The term “Hacking” means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

1.3 What is a Hacker?

Everyone here thinks that hacking is just stealing of data and information illegally but this perception is absolutely wrong.

“Hacking is unauthorized use of computer and network resources. (The term “hacker” originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.)”

Hacking is not always unauthorized. Hacking also includes exploring the Things that are being hidden from the general usage. So exploring things
i.e being Hidden from general User is also hacking.

1.3.1 Who is a Hacker?

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

1.3.2 Who is attacking you?

When talking about attackers and hacking it often happens that we ask people working at customer’s sites “who is scaring you?” Most of the time the answer we hear is not “Well, you know that we are scared by script kids, playing with those couple of un-patched machines we have,” nor is it “We really scared about industrial spies.” Rather, 98% of the time the answer is “We don’t know.”

These answers possibly mean that the company, feeling as a potential target, has not developed a proper IT Security Risk Analysis, while trying to figure out who may want to attack its IT infrastructure and gain access to its information.

This mistake probably happens because every time people hear “hackers profiling,” the word “profiling” automatically makes them think about something that has already happened, rather than something that may happen.

The hacking world has changed dramatically in the last thirty years, and the somehow “romantic” figure of the hacker of the ‘80s is far from today’s.

1.3.3 Types of Hackers

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Symbol	Description
	Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration testing and vulnerability assessments.
	Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

	Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
	Script kiddies: A non-skilled person who gains access to computer systems using already made tools.
Knowledge Is Free. We Are Anonymous. We Are Legion. We Do Not Forgive. We Do Not Forget. Expect Us.	**Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
	Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

1.4 What is a Cybercrime?

Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using mobile phones via SMS and online chatting applications.

1.4.1 Type of Cybercrime

- The following list presents the common types of cybercrimes:
- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, and account details, etc. on social media, websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.
- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering:** This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

1.5 What is a Security Threat?

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack. In these tutorial series, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

1.5.1 What are Physical Threats?

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

The following list classifies the physical threats into three (3) main categories;

- **Internal**: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External**: These threats include Lightning, floods, earthquakes, etc.
- **Human**: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

To protect computer systems from the above mentioned physical threats, an organization must have physical security control measures.

The following list shows some of the possible measures that can be taken:

- **Internal**: Fire threats could be prevented by the use of automatic fire detectors and extinguishers that do not use water to put out a fire. The unstable power supply can be prevented by the use of voltage controllers. An air conditioner can be used to control the humidity in the computer room.
- **External**: Lightning protection systems can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of Lightning causing damage. Housing computer systems in high lands are one of the possible ways of protecting systems against floods.
- **Humans**: Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms.

1.5.2 What are Non-physical threats?

A non-physical threat is a potential cause of an incident that may result in;

- Loss or corruption of system data
- Disrupt business operations that rely on computer systems
- Loss of sensitive information
- Illegal monitoring of activities on computer systems
- Cyber Security Breaches
- Others

The non-physical threats are also known as logical threats. The following list is the common types of non-physical threats;

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

To protect computer systems from the above-mentioned threats, an organization must have logical security measures in place. The following list shows some of the possible measures that can be taken to protect cyber security threats

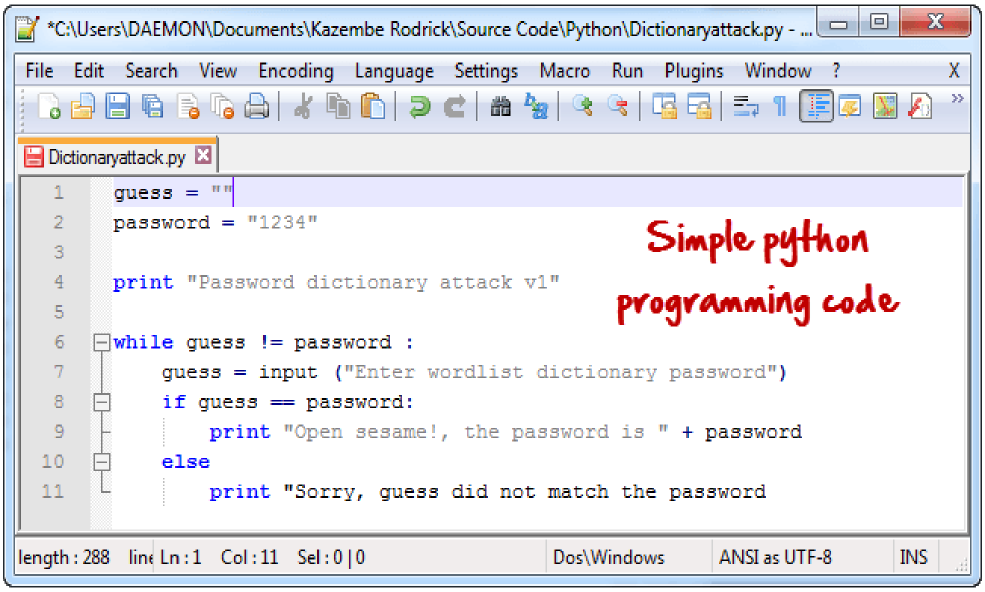
To protect against viruses, Trojans, worms, etc. an organization can use anti-virus software. In additional to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user’s computer.

Unauthorized access to computer system resources can be prevented by the use of authentication methods. The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc.

Intrusion-detection/prevention systems can be used to protect against denial of service attacks. There are other measures too that can be put in place to avoid denial of service attacks.

1.6 What is a Programming Language?

A programming language is a language that is used to develop computer programs. The programs developed can range from operating systems; data based applications through to networking solutions.


*C:\Users\DAEMON\Documents\Kazembe Rodrick\Source Code\Python\Dictionaryattack.py - ...
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Dictionaryattack.py
Simple python programming code
length : 288 line Ln : 1 Col : 11 Sel : 0 | 0 Dos\Windows ANSI as UTF-8 INS

```
guess = ""
password = "1234"

print "Password dictionary attack v1"

while guess != password :
    guess = input ("Enter wordlist dictionary password")
    if guess == password:
        print "Open sesame!, the password is " + password
    else
        print "Sorry, guess did not match the password
```

1.6.1 Why should you learn how to program?

- Hackers are the problem solver and tool builders, learning how to program will help you implement solutions to problems. It also differentiates you from script kiddies.

- Writing programs as a hacker will help you to automate many tasks which would usually take lots of time to complete.

- Writing programs can also help you identify and exploit programming errors in applications that you will be targeting.

- You don't have to reinvent the wheel all the time, and there are a number of open source programs that are readily usable. You can customize the already existing applications and add your methods to suit your needs.

1.6.2 What Languages should we learn?

The answer to this question depends on your target computer systems and platforms. Some programming languages are used to develop for only specific platforms. As an example, Visual Basic Classic (3, 4, 5, and 6.0) is used to write applications that run on Windows operating system. It would, therefore, be illogical for you to learn how to program in Visual Basic 6.0 when your target is hacking Linux based systems.

1.6.3 Programming languages that are useful to hackers

Sr no.	Computer languages	Description	Platform	Purpose
1	**HTML**	Language used to write web pages.	*Cross platform	**Web hacking** Login forms and other data entry methods on the web use HTML forms to get data. Been able to write and interpret HTML, makes it easy for you to identify and exploit weaknesses in the code.
2	**JavaScript**	Client side scripting language	*Cross platform	**Web Hacking** JavaScript code is executed on the client browse. You can use it to read saved cookies and perform cross site scripting etc.
3	**PHP**	Server side scripting language	*Cross platform	**Web Hacking** PHP is one of the most used web programming languages. It is used to process HTML forms and performs other custom tasks. You could write a custom application in PHP that modifies settings on a web server and makes the server vulnerable to attacks.

4	**SQL**	Language used to communicate with database	*Cross platform	**Web Hacking** Using SQL injection, to by-pass web application login algorithms that are weak, delete data from the database, etc.
5	**Python** **Ruby** **Bash** **Perl**	High level programming languages	*Cross platform	**Building tools & scripts** They come in handy when you need to develop automation tools and scripts. The knowledge gained can also be used in understand and customization the already available tools.
6	**C & C++**	High level programming	*Cross platform	**Writing exploits, shell codes, etc.** They come in handy when you need to write your own shell codes, exploits, root kits or understanding and expanding on existing ones.
7	**Java** **CSharp** **Visual Basic** **VBScript**	Other languages	Java &CSharp are *cross platform. Visual Basic is specific to Windows	**Other uses** The usefulness of these languages depends on your scenario.

* Cross platform means programs developed using the particular language can be deployed on different operating systems such as Windows, Linux based, MAC etc.

1.6.4 Other skills

In addition to programming skills, a good hacker should also have the following skills:

- Know how to use the internet and search engines effectively to gather information.
- Get a Linux-based operating system and know the basics commands that every Linux user should know.
- Practice makes perfect, a good hacker should be hard working and positively contribute to the hacker community. He/she can contribute by developing open source programs, answering questions in hacking forums, etc.

1.7 What is Ethical Hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.
- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

1.7.1 Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization’s image and save an organization a lot of money.
- Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

1.7.2 Legality of Ethical Hacking

Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking. The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual’s skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

1.7.3 The Concept of Ethical Hacking

The following are the basic concepts of ethical hacking:

1. Phase of Pen testing

Pen Test, like forensics, is almost as much an art as it is a science – you can only be taught so far, technical techniques and tools are all very well, but you really need a mind that can think sideways and approach a task from as many angles as possible.

2. Foot printing

Tools and tricks to get the information about the computer, IP and mac address, related user and system.

3. Scanning

Before starting the pen testing, pen tester must have some information about network and system. So pen tester scans the entire network with some tool like Nmap, Zenmap, ping and hping etc.

4. Enumeration

During the enumeration phase, possible entry points into the tested systems are identified. The information collected during the reconnaissance phase is put to use.

5. System Hacking

System hacking is login to system without credentials not only by pass the credentials but also you can work in system as root user by privilege escalation.

6. Trojans

It is a generally non-self-replicating type of malware program containing malicious code. A Trojan often acts as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. While Trojans and backdoors are not easily detectable by themselves, computers may appear to run slower due to heavy processor or network usage.

7. Viruses and Worms

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

8. Sniffing Traffic

It is a program that monitors and analyzes network traffic, detecting and finding problems. Various technique and tool is used for sniffing like kali linux MITM attack, tshark, urlsnarf etc.

9. Social engineering

In this technique, ethical hacker creates the phishing page of website to obtain credential of users.

10. Denial of service

A DoS attack generally consists of efforts to temporarily interrupt or suspend or down the services of a host connected to the Internet.

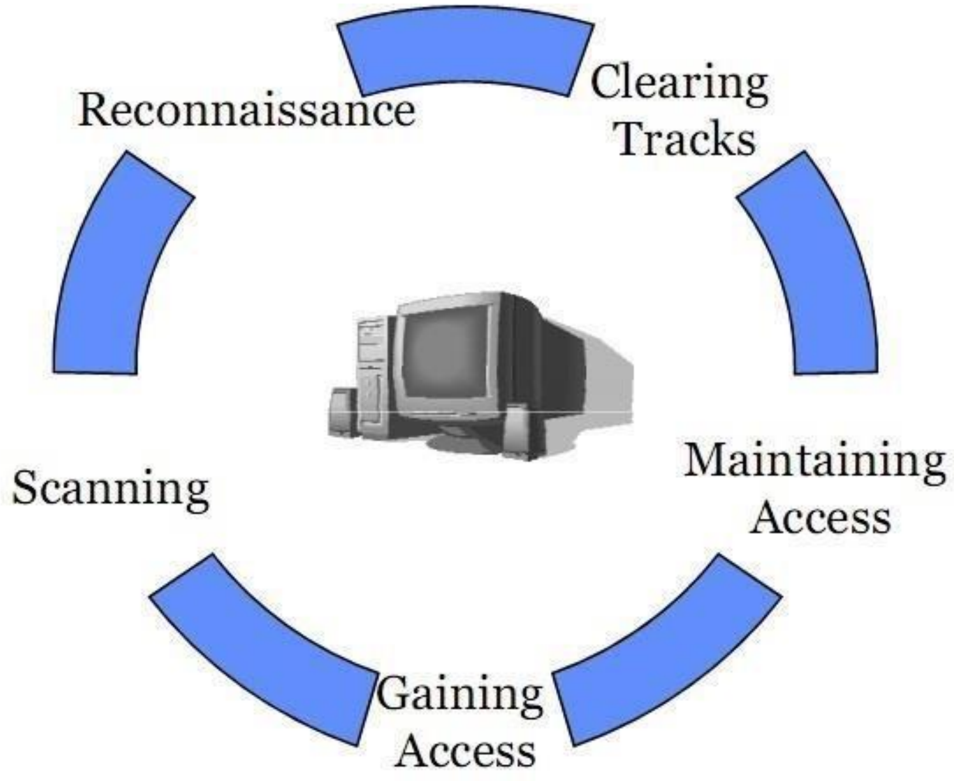
1.7.4 Potential Security Threats to Your Computer Systems

A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure. Knowing how to identify computer security threats is the first step in protecting computer systems. The threats could be intentional, accidental or caused by natural disasters.

1.8 Phases involved in hacking

The five phases of Hacking are as follow:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks



1.8.1 The Five Phases of Hacking

Reconnaissance: - This is the primary phase where the Hacker tries to collect as much information as possible about the target. It includes identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc.

Scanning: - It involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase can include diallers, port scanners, network mappers, sweepers, and vulnerability scanners. Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts.

Gaining Access:- After scanning, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline. Examples include stack based buffer overflows, denial of service (DoS), and session hijacking.

Maintaining Access: - Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

Covering Tracks: - Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include steganography, the use of tunnelling protocols, and altering log files.

1.8.2 Role of Ethical Hacker

As serious security professionals, we almost give “similar security talk” to other business teams in other organization regarding anti-virus definitions, VPNs, encryption, mobile security, social media security, hacking, and so on. But when these security measures are not taken seriously, they fall apart.

This is when vulnerabilities set in and malicious elements seize the opportunity to penetrate the system.

Now comes the “certified ethical hacker”, whose primary job is to attack his own organization’s system to weed out vulnerabilities before “real hackers” do. The adrenaline rush of being an ethical hacker is unparalleled. Though an ethical hacker's role is similar to that of a “penetration tester”, it involves broader duties. "The term ethical hacking is said to have been coined by IBM” (White hat (computer security).

1.8.3 Common Hacking Methodologies

The most common methods used by intruders to gain control of home computers are briefly described below.

1. Trojan horse programs

Trojan horse programs are a common way for intruders to trick you (sometimes referred to as "social engineering") into installing "back door" programs. These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus.

2. Back door and remote administration programs

On Windows computers, three tools commonly used by intruders to gain remote access to your computer are BackOrifice, Netbus, and SubSeven. These back door or remote administration programs, once installed, allow other people to access and control your computer.

3. Denial of service

Another form of attack is called a denial-of-service (DoS) attack. This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. It is important to note that in addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

4. Being an intermediary for another attack

Intruders will frequently use compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service (DDoS) tools are used. The intruders install an "agent" (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions. Then, when a number of agents are running on different computers, a single "handler" can instruct all of them to launch a denial-of-service attack on another system. Thus, the end target of the attack is not your own computer, but someone else’s - your computer is just a convenient tool in a larger attack.

5. Unprotected Windows shares

Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet. The greater immediate risk to the Internet community is the potentially large number of computers attached to the Internet with unprotected Windows networking shares combined with distributed attack tools. Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate.

There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

6. Mobile code (Java/JavaScript/ActiveX)

There have been reports of problems with "mobile code" (e.g. Java, JavaScript, and ActiveX). These are programming languages that let web developers write code that is executed by your web browser. Although the code is generally useful, it can be used by intruders to gather information (such as which web sites you visit) or to run malicious code on your computer. It is possible to disable Java, JavaScript, and ActiveX in your web browser.

7. Cross-site scripting

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.
You can potentially expose your web browser to malicious scripts by following links in web pages, email messages, or newsgroup postings without knowing what they link to using interactive forms on an untrustworthy site
viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags.

8. Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access. Relative to DSL and traditional dial-up users, cable modem users have a higher risk of exposure to packet sniffers since entire neighbourhoods of cable modem users are effectively part of the same LAN. A packet sniffer installed on any cable modem user's computer in a neighbourhood may be able to capture data transmitted by any other cable modem in the same neighbourhood.

1.9 What is a Profile?

According to Rogers (2000d), “hackers are not a homogeneous group” In addition, “there is no generic profile of a hacker.”Voiskounsky et al. (2000) claimed that hackers derive from the heterogeneity of the population of the hacker community in Russia. Many researchers tried to categorize hackers into several subgroups depending on diverse characteristics (see Rogers, 2000b).

Landreth (1985) defined the hacker community as novice, students, tourists, crasher, and thief based on the activities hackers were involved in. The novice is thought to be the least experienced and the person who makes petty mischief. The student group is considered those who easily get bored and are unchallenged at school and who try to explore others' computer systems at home.

Hollinger (1988) claimed that people involved in hacking activities should fit into three categories: pirates, browsers, and crackers. The pirates have a low level of hacking techniques. They are limited to pirate computer software. The browsers have middle level of technical ability and are able to access to individuals' personal files. They usually 9 don't destroy files. The crackers have the best hacking techniques and are considered the most serious abusers.

Goodell (1996) maintained that hackers can be divided into three groups: hackers, crackers, and phreakers. Hackers are involved in hacking to obtain knowledge and satisfy intellectual curiosity. Crackers usually commit destruction, vandalism, and defacement on web pages. Phreakers are mainly interested in manipulating and attacking the telephone system.

Chandler (1996) categorized hackers into four different generations. The first generation of hackers was smart and techno-oriented students, programmers, and computer scientists from MIT. They were interested in hacking for academic and professional curiosities. The second generation of hackers was more likely to be technological radicals. They made "blue boxes" that allowed a person to get long distance telephone service without charge.

Chantler (1996) categorized hacker groups into three sub-groups: elite, neophytes, and losers (lamers) based on hackers' attributes such as hackers' activities, their prowess at hacking, their knowledge, motivation, and how long they had been hacking. The elite group has a high level of hacking techniques and desires to achieve self-discovery and enjoys the excitement and challenge. The neophytes have moderate level of hacking skill and still learn more knowledge about hacking. The losers (lamers) don't have intellectual 10 knowledge and mainly use hacking skill for a desire for profit, revenge, theft, and espionage.

Power (1998) indicated that hackers can be categorized into sport intruders, competitive intelligence, and foreign intelligence. The sport intruders break into computer servers, deface web pages, and damage files. The competitive intelligence tries to avoid illegal hacking and unethical activities and mainly fall into the realm of competitive espionage (Rogers, 2000b). The foreign intelligence is involved in hacking activities for the purpose of a nation's security or economic interests.

Parker (1998) subdivided hackers into seven profiles of cybercriminals: pranksters, hackersters, malicious hackers, personal problem solvers, career criminals, extreme advocates, and malcontents, addicts, and irrational and incompetent people. Pranksters are referred to people who perpetrate tricks on others. They seldom inflict harm on others.

Adamiski (1999) noted that hacker community has a loose hierarchy, and this is composed of the elite, ordinary, and darksiders. The elite have a high level technique so that they can make software and attack tools. The ordinary hacker group is similar to crackers. They are involved in breaking into computer systems and attacking telephone 11 company computer switches. The darksiders are engaging in financial gain through hacking.

Rogers (2000b) classified the hacking community in seven distinct categories: newbie/tool kit (NT), cyber-punks (CP), internals (IT), coders (CD), old guard hackers (OG), professional criminals (PC), and cyber-terrorists (CT) depending upon level of technical ability. The NT has limited computer skills and use tool kits2 to conduct attack. The CP category is made up of hackers who usually have better computer skills. They can make basic levels of their own software; they also intentionally engage in defacing web pages or send "Spam" mails.

1.10 The Hacking Mindset

The idea that looking for magic shortcuts, and "hacks" might be related to the belief that one is special or doesn't need to put in long hours of demanding work in order to achieve something.

I'd like to expand on this idea a bit and explain why we think the "hacking" mentality (in language learning or even "life" itself) may actually be a sign of a fixed mindset. If you have a fixed mindset, you don't like being told that things require hard work and sustained effort. After all, you're special. You should be able to achieve success without effort, because you inherently deserve it.

1.10.1 The Hacker Mindset

The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music. Actually, you can find it at the highest levels of any science or art. Software hackers recognize these kindred spirits elsewhere and may call them hackers too and some claim that the hacker nature is really independent of the particular medium the hacker works in.

1.11 The Basic Difference between Hackers and Crackers

Hacker: A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge; freely share what they have discovered, and never intentionally damage data.

Cracker: A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data; deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.

1.12 Skills Required Becoming an Ethical Hacker

Skills allow you to achieve your desired goals within the available time and resources. As a hacker, you will need to develop skills that will help you get the job done. These skills include learning how to program, use the internet, good at solving problems, and taking advantage of existing security tools.

1.13 Ethical Hacking- Advantages and Disadvantages

Advantages of Ethical Hacking

Most of the benefits of ethical hacking are obvious, but many are overlooked. The benefits range from simply preventing malicious hacking to preventing national security breaches. The benefits include:

- Fighting against terrorism and national security breaches
- Having a computer system that prevents malicious hackers from gaining access
- Having adequate preventative measures in place to prevent security breaches

Disadvantages of Ethical Hacking

As with all types of activities which have a darker side, there will be dishonest people presenting drawbacks. The possible drawbacks of ethical hacking include:

- The ethical hacker using the knowledge they gain to do malicious hacking activities
- Allowing the company's financial and banking details to be seen
- The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system
- Massive security breach

1.14 Let us Sum up

Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks. Cybercrime is committing a crime with the aid of computers and information technology infrastructure. Ethical Hacking is about improving the security of computer systems and/or computer networks. A threat is any activity that can lead to data loss/corruption through to disruption of normal business operations. There are physical and non-physical threats Physical threats cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters. Non-physical threats target the software and data on the computer systems. Finally we have learnt that Programming skills and Networking skills are essential to becoming an effective hacker. Hacking tools are programs that simplify the process of identifying and exploiting weaknesses in computer systems.

1.15 Self Assessment Questions

1. What is hacking?

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

2. Explain difference between hackers and crackers.

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

3. What is cybercrime?

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

4. What is security threat?

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

5. What is ethical hacking?

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

1.16 Model Questions

1. Explain about deference types of hacker.
2. What is the legality in ethical hacking?
3. Explain about the concept of ethical hacking.
4. Write about the role of ethical hacking.
5. Write about Basic Difference between Hackers and Crackers.
6. Write about Advantages and Disadvantages Ethical Hacking.

1.17 References & Further Readings

1. http://www.guru99.com/learn-everything-about-ethical-hacking-tools-and-skills.html
2. http://cdn.ttgtmedia.com/searchNetworking/downloads/hacking_for_dummies.pdf
3. http://picateshackz.com/2015/04/understand-hacker-mindset-to-become-real-hacker.html#G2EfK2R3iPelK6Hx.99
4. The hacker mentality: exploring the relationship between psychological variables and hacking activities by hyung-jin woo (under the direction of joseph r. Dominick).

UNIT-2 Footprinting & Reconnaissance

Unit Structure

2.0 Introduction

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

Footprinting where we collect public information and building a map of the server or domain objective, without interacting direct with it.Footprinting where there is active target identification through and techniques such as port scanning, and different identifications of services, operating systems and server banners. Footprinting is one of the most important techniques security auditing, since allows them gather information about the target we are analyzing.

2.1 Learning Objective

After learning this unit you should be able to

- Know about what is Footprinting.
- Learn about footprinting terminologies
- Know about the different type of footprinting.
- Study about tricks and techniques of footprinting.
- Identify the footprinting threats.
- Understand the process of Information Gathering.
- List the advantages and some weaknesses of information gathering.
- Learn about the basic concepts Hacker Methodology.
- Know the Ethical Tools used for the reconnaissance phase.

2.2 What is Footprinting?

Footprinting is basically the first step of the hacking which is used by Hackers and penetration testers for gathering information about a server where a website is hosted, A hacker does footprinting in-order to find weakness and security holes of the server through which it can be rooted (Hacked) and same is the Job of penetration tester but often hackers do this for bad purpose but a penetration tester is hired to do this in order to increase security. The purpose of footprinting to learn as much as you can about a system of the server, it's remote access capabilities, its ports and services which are running behind it, Registrar queries, DNS queries, and the aspects of its security. All kinds of Hacking Must start with footprinting if you are targeting a specific server and system. This is the start of a successful attack on a system, and you can get much information depending upon your skills.

2.3 Footprinting Terminologies

Footprinting is the process of using various tools and technologies to understand and learn the best way to attack a target. Attackers find out as much as possible without actually giving themselves away. They find public information or appear as normal users. The attacker/hacker does a ‘whois’ lookup to find as much information as possible about the network along with the domain name. They might stroll through your DNS tables using nslookup, dig, or other utilities to do domain transfers to find the names of machines. The hacker/attacker browses other public information looking for the public web site and anonymous FTP sites. Specifically, hackers/attackers look for domain names, network blocks, particular IP addresses, networking protocols in use, internal domain names, IDSs (Intrusion Detection Systems), telephone numbers, ACLs (Access Control Lists), etc. Footprinting is necessary to identify the above listed items. Hackers use this information to attack. Security personnel can use it to strengthen their security stance.

2.3.1 Uses of Footprinting

Footprinting is a necessary evil. What does that mean? Successful hackers are building their information database about your company’s security weaknesses. Wouldn’t be nice to know these weaknesses in advance to take proper action? Yes, it would be nice. Therefore, security personnel need to add footprinting to their already long task list. One has to remember that an organization’s security is a process, not a technology. A good security system provides multiple layers of security. The system would be defined as “a collection of things or elements which, working together, produce a result not achievable by the things alone.”

It allows a hacker to gain information about the target system. This information can be used to carry out further attacks on the system. That is the reason by which it may be named a Pre-Attack, since all the information is reviewed in order to get a complete and successful resolution of the attack.

2.3.2Crawling

Crawling is the process of surfing the internet to get the required information about the target. The sites surfed can include the target’s website, blogs and social networks. The information obtained by this method will be helpful in other methods too.

2.4 Types of Footprinting and their Explanation

Below are types of footprinting and their sub-branches:-

2.4.1 Open Source Footprinting

It is a type of safest footprinting as it is in legal limits and you can do it without any fear that if you are doing any kind an illegal task. It includes finding basic information which is majorly present for public use too, Like finding out the phone numbers, Emails Addresses, performing who is request for the domain name, searching through DNS tables, and scanning certain ip addresses through automated tools (I,ll post them later with detailed info, of usage), and searching out some common means of finding information about the server system and owner.

Many of the companies post a large amount of information about them self at the their own website without realizing the fact that it can be useful for a hacker too, also sometimes in HTML and coding comments are present which themselves give hackers a lot of information about coding. As comments are present their to tell a coder about the function of some specific code.

2.4.2 Network Enumeration

Network enumerating is a computing activity in which user names and info on groups, shares and services of networked computers are retrieved. It should not be confused with Network mapping which only retrieves information about which servers are connected to a specific network and what operating system is run on them. It includes identifying the domain name and also searching for the registrar information since companies domains are listed with registrar information. The hacker simply needs to know which registrar the company is listed with. There are five types of queries listed under.

Registrar Queries:

Registrar Queries or WHOIS (pronounced as the phrase who is) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.

Organizational Queries:

This is searching a specific registrar to obtain all instances of the target's name. The results show many different domains associated with the company as it may use a large number of domains with its dedicated server or system you can say.

Domain Query:

A domain query is based off of results found in an organizational query. Using a domain query, you could find the company's address; domain name, administrator and his/her phone number, and the system's domain servers as while registering a domain this is included in registration forum. The administrative contact could be very useful to a hacker as it provides a purpose of how to do social engineering. So this is where social engineering comes into play. Many administrators now post false phone numbers to protect themselves from this so that they may not be fooled so easily.

POC Query:

This query finds the many IP addresses a machine may have which are majorly public and are associated with machine.

DNS Interrogation:

After gathering the information needed using the above techniques, a hacker would begin to query the DNS using tools. A common problem with system administrators is allowing untrusted, or worse, unknown users, to perform a DNS Zone Transfer. Many freeware tools can be found on the internet and can be used to perform DNS interrogation. Tools such as nslookup, for PC, and AGnet Tools, for Mac, also in Linux flavor many open source applications are present for this purpose.

2.5 Similar Common Tricks And Techniques Regarding Footprinting

2.5.1 OS Identification

This involves sending illegal ICMP (Internet Control Message Protocol) or (TCPTransmission Control Protocol) packets to a machine for identifying Operating system used on server or machine in simple words.

2.5.2 Ping Sweep

Try Pinging Different IP addresses found by you during Footprinting:-

Try Pinging Different IP addresses found by you so that you may figure out that which IP is alive in-order to scan for open ports later.

2.5.3 Performing TCP Scans

Scan ports on machines to see which services are offered by system. TCP scanscan be performed by scanning a single port on a range of IPs (Many IPs But checking one port on them), or by scanning a range of ports on a single IP (Many Ports but on a single IP). Both techniques will produce helpful information for hacker and you.

2.5.4 Performing UDP Scans

Send garbage UDP packets to a desired port. Well normally don't perform

UDP scans a whole lot because most machines show and reply with an ICMP 'port unreachable' message. Meaning that no service is available, most of the advanced machines and servers show this behavior.

2.6 Footprinting Threats

Attackers gathers valuable system-level information such as account details, OS and other software versions, server names, and db schema details from footprinting techniques.

Threats include:

- Business loss
- Corporate espionage
- Privacy loss
- Social engineering
- System and network attacks
- Information leakage

2.7 Information Gathering

2.7.1 What is Information Gathering?

Information gathering helps the individual and the organization to undertake complicated tasks that would otherwise be extremely hard to accomplish if not out rightly impossible without the benefit of gathered information. As defined in the dictionary, information gathering is the act of collecting information from various sources through various means.

In the literal sense, information gathering is a basic human skill necessary for undertaking basic human activities such as eating, sleeping, working etc. For in order to eat, one must know if the food is edible or not; and in order to sleep, one must know if the sleeping place is comfortable or not.

As applied in the fields of business and other specialized organizations (scientific, military, academic) however, information gathering is an advanced skill which requires the training and education of personnel in the procedures and methods of gathering information from sources that are of higher level than ordinary sources. In the case of interviewing personalities for example, a researcher usually gets to interview authorities and proper officials, and thus, he must know the proper ways to address distinguished personalities of the community and the society in general.

In general practice, information gathering is the collection of data for dealing with the individual's or the organization's current situation. More data means more and better ways of dealing with the current situation. More data broadens the minds of those who will use the data to solve current organizational problems. New ideas come more easily if there are lots of facts to be used as bases.

There are two main types of sources in the field of information gathering, namely:

- **Existing sources** – existing sources are those sources of information that can be found in the printed, in video, in audio and other materials that are available to the public or upon request to proper bureaucracy.

- **Natural sources** – natural sources are first hand sources such as those who have tried products, services and methods, and expressing their experience and opinions to the researcher.

2.7.2 Who undertakes information gathering and why

Information gathering is an assignment of the research specialist within the organization's intelligence department. They are the personnel properly trained and equipped to carry out the research tasks in the most efficient manner. The proper handling of data requires methods and procedures unique to the field of information gathering. Research personnel do this task unequivocally thru skills like data sifting, intelligent questioning, and other research skills. Other company personnel can also do their own information gathering on the personal level to improve their job performances and as a self-help tool. Researchers undertake information gathering in order to:

- Broaden the scope of knowledge of the organization
- For the development of particular skills
- To reduce the apprehension caused by the unknown
- For a higher level of understanding of special subjects

- And obviously, for solving problems

Additionally, on the non-professional aspect of the research undertaking, information can also give inspiration and entertainment.

2.7.3 How to Undertake Information Gathering

In order to implement a good information gathering design, a step-by-step approach is advisable for any researcher to follow:

- **Analyzing the problem** – The researcher needs to identify the purpose and the process of the research he is doing. For whom is he doing it and why? These questions and more needs to be answered right at the start of the research.

- **Identifying the sections of the information gathering** – Before going through with the process of information gathering, a sectioning of the general outline of the task can be helpful. Sections such as those classifying the recipients of the data, the detailing of the specific questions that needs to be answered, and also the setting of the knowledge levels of the team members involved facilitates an easier to follow research program.

- **After the outline of the research task-** The researcher may then set the actual plan of activities needed to carry out the information gathering tasks. Questions such as: Where to go to for the research? What materials need to be invested in? What skills are needed to be implemented? And the details of the research materials like the availability, languages, location and accessibility needs some suasion.

- **The gathering methods and tools** – The tools that are involved in information gathering such as data storage devices and publications have their own set of required skills that the researcher must readily possess or is capable of having. Languages contained in publications could pose a problem and data storage devices could have proprietary names. And names, as we all know in the computer industry means lots of adjustments.

- **Begin the gathering** – During the gathering of the data, the researcher encounters various amounts of information that may or may not be relevant to the present subject of the research. He must sift through all of these carefully.

- **Review and record the data obtained** – a recording that includes everything from the start to the end of the gathering process must be set in writing to provide all the information that the organization needs.

2.7.4 Advantages and Some Weaknesses of Information Gathering

Information gathering, per se, delivers a great deal of advantage to the organization undertaking it. Due to its enlightening nature for example, the researcher and his organization catches a better glimpse of other people's situations. They are able to empathize with other people if they knew better. Better alternatives in problem solving are also in the offing upon learning of mistakes already committed by other parties.

On the down side, with the proliferation of massive amounts of data in the Internet, any researcher who took up gathering of information in the Internet can suffer from information overload. There's just no absolute lead with information gathering in the Internet and pursued leads might lead to the doldrums in information gathering.

2.7.5 Best ways of information gathering

An organization reduces the stress on itself if it has an efficient means of information gathering. And for that efficiency to take place, some key points in the practice of information gathering needs to be stressed:

- A Staff needs to be organized and distributed to take on specific assignments.
- They also must be trained in the different approaches to inquiring.
- Everyone involved must be constantly updated in the ongoing research project
- With interviews, the information gathering staff should have good questioning skills
- Creativity, inventiveness and adaptability are key qualities that bring progress to the gathering of information.

2.7.6 Team reporter facilitates information gathering

Team reporter is a web based email application that updates everyone on the team especially remote working teams about project status and the progress the team is making on it. Each member of the remote working team submits a report on his expertise via email that Team reporter automatically sends to each member. Members can gather information about the whole project and the team with Team reporter. All these Team reporter undertakes by means of the following procedures:

- Creating questions that the team members will answer.
- Tailoring the questions to be asked to fit project needs
- Scheduling the sending out of email queries.
- Team members replying with their status reports.
- Upon receiving individual team member reports, scheduling of overall status updates to every team member.
- Adopting preset business scenarios.
- Prompting team members who forget their reports.
- Arranging an archive of team status reports

Team reporter has the following advantages:

- Ready in 5 minutes
- Free start-up
- Accessible even to novice users and managers
- No IT software or hardware requirements
- Only email login required for Team members

2.8 Finding information in a Company's URL

There are three ways to get a great URL. The first is with magical inspiration: that perfect and available name comes to you in the shower. The second is with a ton of money, by buying an existing domain. The third (if inspiration and money are lacking) is with the process outlined below, which may yield a workable name. These days, you start with the URL and then check that some variation of the company name is available (for registration purposes). That part is relatively easy.

2.8.1 Relax (But Avoid Really Horrible Ones)

URLs matter a lot less than it would seem when you are starting out. One can think of plenty of terrible names that did great and vice versa. We are now moving away from destination sites. Search engines and browser capabilities, such as Firefox's awesome bar, will help people find you.

If you are relying on a great name to build traffic doesn't. Unless you have a lot of money to buy an existing domain and that is probably not a good use of your cash there are cheaper ways to build traffic.

So then, "okay" is good enough. Don't obsess over the URL. Save your obsessing for usability design. But avoid the real stinkers, the names that make people laugh at you and then ignore you. We live in a global world, too, so do check that your great URL does not mean "Your mother is a mangy dog" in Chinese, French, or whatever.

2.8.2 Process for Getting a Great URL

Here is the three-step process:

1. Go for a run (or whatever exercise you enjoy doing).
2. Have a double espresso.
3. Do something totally relaxing, like petting your cat, to clear your mind and let inspiration set in.

Did that do the trick? No? Try the longer process:

1. Choose some "themes" that relate to your biz.
2. Brainstorm with some pals to come up with a really long list of words that vaguely relate to those themes.
3. Use bulk registration to test a lot of them. Make a shorter list of what is available with .com.
4. Check that shorter list against:
   - a trademark search on uspto.gov,
   - some people who will give you an honest response,
   - a few major languages for the "mangy dog" test.
5. If that cut leaves you short, go back to some of the names you like and try them out with .net. In some cases .net is okay, particularly if the .com name is owned by someone small and non-competitive whom you can buy out later.

6. Still coming up short? Try country extensions. For example, if you want rabbit.com, try rabbit (Italy). This is risky. It sounds clever and occasionally works, but mostly confuses people.

7. Once you get a viable list of three that check out, buy all three and then test, test, test. And test with as broad a community as you can get. Use Twitter, your blog, whatever connects you to your network quickly. And go outside your network.

8. If all three fall short of this last hurdle, start from the top: go for a run, double espresso, etc. Allow time for this. The best ideas come at the oddest times and usually when you are thinking of something else.
9. When you find your chosen one:
   - Register the trademark at uspto.gov.
   - Protect major country extensions, .net, .info, and other extensions that a squatter or competitor may try to take if they see you get traction.

- Create a logo that works.
- Ensure the company name is available. In the worst case, CoolSite.com could be run by Boring Company LLC doing business as (DBA) CoolSite.com.

10. Go, End, go!

2.9 The Hacker Methodology

Many newbie hackers seem to be confused regarding the process or methodology to employ a successful hack. Most want to simply go straight to the exploit without doing the due diligence to make certain that the hack will work and you won't get caught.

Here, I want to lay out for you the proper methodology, with example tools and techniques for a hack, from start to finish.

Step 1: Performing Reconnaissance

Good reconnaissance is critical to great hacking. In general, a good hacker wills recon for about 2 to 3 times longer than he/she would performing the actual hack. It's not unusual to spend weeks or months gathering information before even beginning to attempt an exploit.

Most exploits are dependent on operating systems, applications, ports, and services, so you need to gather this information before you start hacking. If you don't, you will likely fail, get caught, or both. I can't emphasize this enough. Newbie hackers are always so anxious to get to the exploit that they often ignore this phase of the attack.

Recon can be broken into at least two categories, passive and active.

Passive Reconnaissance

Passive reconnaissance can be defined as gathering information about the target without actually "touching" the target, or in a way that looks like normal traffic.

It is use Netcraft to gather info about websites, such as the web server, operating system, last reboot, and other technologies. All of this information is critical before starting the hack.

In addition, passive reconnaissance can include DNS and SNMP mining, dumpster diving, social engineering, using social media such as Facebook and LinkedIn, and of course, Google hacking, among other techniques.

Active Reconnaissance

Active reconnaissance is information gathered about the target by actually sending packets to the target and evaluating the response. The results of active recon are much more specific and reliable, but also much riskier. Anytime we send a packet to a site, our IP address is left behind.

Nmap, Hping, Netdiscover, P0f, and Xprobe2 are among the many tools we can use to gather info on remote targets that can be useful in revealing open ports, running services, and operating systems.

Active recon can also include enumeration of the network. Techniques such as banner grabbing and the use of vulnerability assessment tools such as Nessus, Nikto, and Retina are also often a part of this phase.

Step 2: Gaining Access (Exploitation)

Exploitation can take many, many forms, and the successful hacker will use their imagination to come up with multiple attack vectors. Metasploit is an excellent tool for exploitation, but don't fall in love with it. As soon as Metasploit develops new exploits, the AV software manufacturers immediately begin developing a new signature for it.

Once you have done thorough recon and know all the ports, services and apps, try looking into the vulnerability databases such as SecurityFocus, TechNet, and others for known vulnerabilities and exploits.

Be creative and think about all of the protocols that the system or network uses and how they might be abused. Always consider the possibility of a man-in-the middle attack and never overlook the good social engineering attack.

Step 3: Privilege Escalation

Very often, we can get access to the system or network, but only with the privileges of an ordinary user. This happens often when we use a client-side attack, where we are attacking an ordinary user's vulnerable applications, such as the web browser, Adobe Flash, Adobe Reader, etc.

Ultimately, we want root or sysadmin privileges that will give us unfettered access to the entire network. This is where we need to escalate privileges. Furthermore, if we have a legitimate account on a website or LAN, we may be able to escalate its privileges to gain root or sysadmin.

In some cases, if we have been able to compromise one system with user privileges on the network, we can pivot from that single system to compromise another system with system privileges.

If you can get the Metasploit Meterpreter on the system, the meterpreter has a command "getsystem" that iterates through 15 known privilege escalation methods to gain system admin privileges.

Once again, do not downplay or ignore the possibility of using social engineering techniques to gain system admin privileges by, in many cases, asking for the password under the proper context.

Step 4: Leaving Behind a Backdoor or Listener

Once we have successfully exploited the system and then escalated our privileges to sysadmin or root, it will be necessary to leave behind a listener or rootkit. This listener, ideally, will persist beyond when the system is rebooted and will be there when we want to come back to the system and continue to use/exploit/extract.

This listener can take many forms, such as Netcat, a command shell, VNC, Meterpreter, etc.

Step 5: Extracting Data

Ultimately, the primary reason for exploiting/hacking a machine is to gain access and extract or exfiltrate data. This can be credit card data, personally identifiable information (PII), intellectual property, or other valuable information.

To do so, we need a way to remove the data in a way that is not readily noticeable by the sysadmin, and ideally, encrypted. Recub and Cryptcat are two tools that can remove data stealthily.

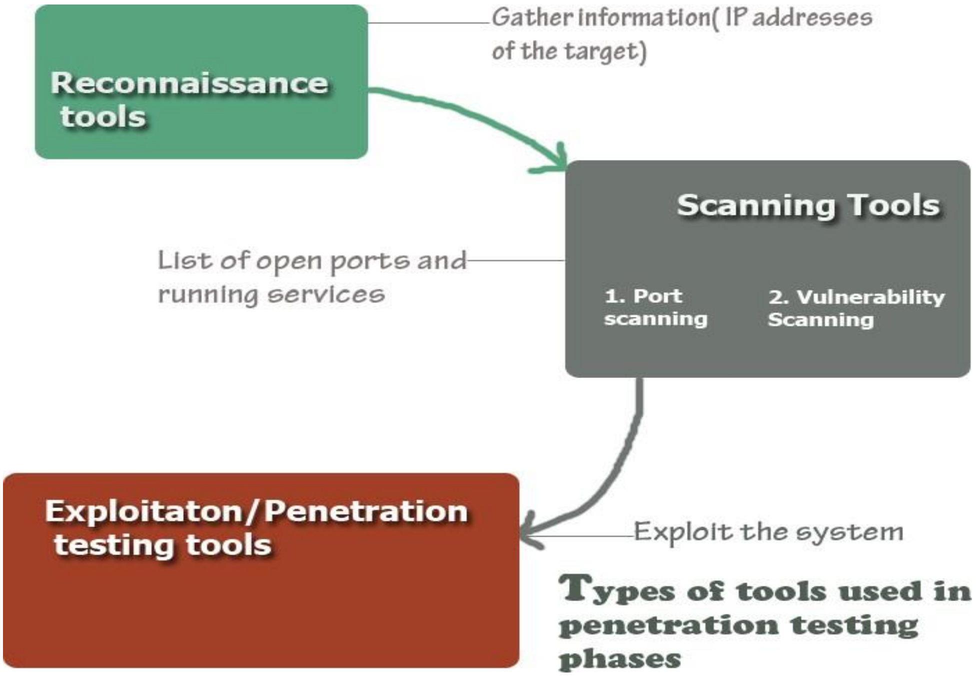
Metasploit'sMeterpreter also has an upload and downloads command for uploading malicious software and downloading critical and valuable data.

Step 6: Covering Your Tracks

To make certain that our exploits don't lead back to us, we need to cover our tracks. This can take many forms such clearing log files, removing any software we uploaded, removing our command history, etc. Metasploit'sMeterpreter has a killav script to disable antivirus software, as well as a cleared command that removes the event logs on Windows systems.

2.10 Tools Used For The Reconnaissance Phase

In footprinting or reconnaissance phase, a penetration tester collects as much information as possible about the target machine. The primary purpose of this phase is to gather intelligence so as you can conduct an effective penetration test. At the end of his phase, you are expected to have a list of IP of your target machine that you can scan later on.


Reconnaissance tools
Gather information(IP addresses of the target)
Scanning Tools
List of open ports and running services
1. Port scanning
2. Vulnerability Scanning
Exploitaton/Penetration testing tools
Exploit the system
Types of tools used in penetration testing phases

2.10.1 Reconnaissance /Footprinting Tools

Reconnaissance can be either active or passive. In active reconnaissance you send traffic to the target machine while a passive reconnaissance uses Internet to gather information. When you use active reconnaissance, you need to remember that the target machine may notice that you are planning a penetration test. In the case of passive test, target machine has no clue about who is gather intelligence and planning an attack. The following are the tools you can use:

1. **Google:** use advanced Google search to gather information about the target's website, webservers and vulnerable information. Sometimes, jobs posted in the companies' websites reveal valuable information about the type of information technologies used in the target company.

2. **The harvester:** you can use it to catalogue email address and subdomains. It works with all the major search engines including Bing and Google. This is a build in tool of Kali Linux.

3. **WHOIS:** to get information about domains, IP address, DNS you can run whois command from your Linux machine. Just type whois followed by the domain name:

Whois yourdomain.com

Alternatively, you can visit whois.net and type the domain name of your target.

4. **Netcraft:** they have a free online tool to gather information about webservers including both the client and server side technologies. Visit http://toolbar.netcraft.com/site_report/ and type the domain name.

5. **Nslookup:** you can use it to query DNS server in order to extract valuable information about the host machine. You can use this tool both in Linux and Windows. From your windows machine, open the command prompt and the type ‘nslookup’ followed by the domain name.

6. **Dig:** another useful DNS lookup tool used in Linux machine. Type dig followed by the domain name.

7. **MetaGoofil**: it’s a Meta data collection tool. Meta data means data about data. For instance, when you create word document in Microsoft word, some additional information are added to this word file such as file size, date of creation, the user name of the creator etc.-all these additional information is called meta data. MetaGoogle scours the Internet for metadata of your target. You can use it with both Linux (built in Kali Linux) and Windows.

8. **Threatagent drone:** it is a web based tool. You need to sign up at https://www.threatagent.com/ and type the domain name that you want to reconnaissance. Once the drone extracts all the information about your target, it will create a complete report about the target, which will include the IP address range, email address, point of contacts etc.

9. **Social engineering**: it is perhaps the easiest way to gather information about an organization. You can find lots of free information about social engineering in the Internet. Depending on the types of information you need about your target organization, you need to choose the appropriate technique. But remember that this technique needs time to master and you need to plan it very carefully, otherwise your activity can easily trigger an alert.

After gathering solid information about the target, the next step is to start scanning the target system.

Scanning Tools

A pen tester scans the target machine in order to find the weakness in the systems. The two major activities of the scanning phase are port scanning and vulnerability scanning.

Port scanning helps to identify a list of opened ports in the target and based on the list of ports you can determine what types of services are running in the system.

The second step in scanning is to run a vulnerability scan to identify specific weakness in the software and services running in the servers.
At the end of port scan you will have the following information:

- Number and type of opened ports
- Type of services running in the servers
- Vulnerabilities of the services and software

10. Nmap: If you have doubt about which tool to use for scanning, use Nmap. This tool creates a complete list of opened ports in your target. You can use is both in Windows and Linux environment. The graphical interface for Windows is called Zenmap, which you can run without learning any command. But, for greater control and granularity for the output, you need to learn the commands.

11. Nessus: Once you find the list of open ports, the next step is start looking for vulnerability in the servers. One of the efficient tools to vulnerability scan is Nessus. Remember that Nessus is not a free tool.

12. Nexpose: if you are looking for a free vulnerability scanner, you can use nexpose community edition from rapid7.

Penetration testing/exploitation

This is the most important phase of a penetration test, which is also known as exploitation because a pen tester makes real attempts to gain access to the target system at this phase.

13. MEDUSA: you can use it to gain to the authentication services in the target machine. Medusa can authenticates with a number of popular services such as FTP, HTTP, IMAP, MS SQL, MySQL, PCAnywhere, POP3, RLOGIN, SMTPM, Telnet, SSH, VNC etc. before using Medusa you need to have several information in your hand such as username, target IP address, a password file(a dictionary file containing a list of popular and widely used passwords).

14. Hydra: this is another useful tool like Medusa used to break authentication system.

15. Metasploit: it can be considered one of the finest open source exploit in the world. The best thing about Metasploit is that it is free. If you are planning to become an open tester and what to learn exploitation, you can start using metasploit without any hesitation. On the other hand, an exploitation tool like Metasploit is a real exploit. When an exploitation tool discovers any vulnerability, it exploits it immediately, which may cause severe damage to the system or can cause network disruption. So, take extra care when playing with any such tools.

2.11 Let us Sum Up

According to Christine Orshesky, there is an increasing need for corporations to protect themselves from computer viruses and other things that bump around the on-line community. Denial of Service attacks and widespread virus infections have raised the issue of 'due care'. No longer is it reasonable to rely solely on the installation of antivirus products to protect the on-line environment. A holistic approach that provides the corporation with an integrated and layered security posture is necessary to achieve protection – including policy, procedures, awareness, and technology. There are many devices available to the hacker to footprint any company's network. Use these tools to find the weaknesses before they do. Therefore, you can prepare an organized approach to your layered security. Never try to use the above mentioned tools in a network or system without authorization from the proper authority. The intention of the post is to help the IT professional who also wants to learn and develop a career in penetration testing.

2.12 Self Assessment Questions

1. What is footprinting in hacking?

……………………………………………………………………………………
……………………………………………………………………………………
……………………………………………………………………………………
……………………………………………………………………………………
……………………………………………………………………………………

2. What are the footprinting threats?

……………………………………………………………………………………
……………………………………………………………………………………

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

3. Explain about Open Source Footprinting.

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

4. Write about sort note Information Gathering.

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

5. How to undertake information gathering?

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………..……………………………………………………

2.13 Model Questions

4. Explain about Advantages and Disadvantages of information gathering.
5. Explain about TCP Scans.
6. Explain different Types of footprinting.
7. Write about Tools used for the reconnaissance phase.
8. What are the Hacker Methodology explain it.

2.14 References & Further Readings

1. http://www.teamreporterapp.com/information-gathering/
2. https://null-byte.wonderhowto.com/how-to/hack-like-pro-hacker-methodology-0155167/
3. https://hackertarget.com/brute-forcing-passwords-with-ncrack-hydra-and-medusa/
4. http://resources.infosecinstitute.com/penetration-testing-intelligence-gathering/#gref

UNIT-3 System Hacking

Unit Structure

3.0 Introduction

Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator’s original purpose. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator’s original purpose is most common among teenagers and young adults. System Hacking actually involves gaining access and changing the integrity of the system. In this unit, you’ll learn the basics of gaining access to a system, how authentication works, and how & when to use that to your advantage.

3.1 Learning Objective

After learning this unit you should be able to

- Know about System hacking.
- Know about different type of System hacking.
- Learn different types of tools used by hackers.
- Study about hacking process.
- Differentiate between hacking and cracking.
- Differentiate Legal Hacking and illegal hacking.
- Know about various methods for password cracking.
- Learn about keystroke logger.

3.2 What is System Hacking

System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks. This unit explains the main methods of system hacking password cracking; privilege escalation, spyware installation, and keylogging and the countermeasures IT security professionals can take to fight these attacks. Security expert Lisa Bock also covers Steganography, spyware on a cell phone, and tactics for hiding tools.

3.3 Types of System Hacking

There are of four types of password attack

1. Passive online attack
2. Active online attack
3. Offline attack
4. Non-technical attack

1. Passive Online Attack

In passive online attacks an attacker don’t contact with authorizing party for stealing password, in other words he attempts password hacking but without communicating with victim or victim account. Types of passive online attacks include wire sniffing, Man in the middle attack and reply attack.

2. Active Online Attack

This type of attack can be directly termed as password guessing. An attacker tries number of passwords one by one against victim to crack his/her password.

3. Offline Attack

Offline password attacks are performed from a location other than the actual computer where the password reside or were used. Offline attacks requires physical access to the computer which stores password file, the attacker copies the password file and then tries to break passwords in his own system. Offline attacks include, dictionary attacks, hybrid attacks, brute force attack, pre-computed hash attacks, syllable attacks, rule based attacks and rainbow attacks.

4. Non Technical Attack

This type of attacks does not require any technical knowledge hence termed as non-technical attacks. This kind of attacks may include, social engineering, shoulder surfing, keyboard sniffing and dumpster diving.

3.4 What is Rootkits?

A rootkit is a type of malicious software that is activated each times your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals, network connections, and the keyboard.

Root kit helps hackers to maintain hidden access to the system using virus , Trojan horse, spyware etc.

3.5 Steganography

The art and science of hiding information by embedding messages within other, seemingly harmless messages is called Steganography. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, Steganography is used to supplement encryption. An encrypted file may still hide information using Steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

3.6 Hacker Tools

There now are more than 100,000 known viruses with more appearing virtually daily. The myriad of hackers and their nefarious deeds can affect any computer owner whether an occasional home user, e-mailer, student, blogger, or a network administrator on site or on the internet. No matter your level of computer use, you must protect your computer, business, or even your identity. The best way to know how to protect your computer is to understand the hacker's tools and recognize their damage.

3.6.1 Hacking Tools

1. Lophtcrack

LophtCrack is a recovery and password auditing tool originally created by Mudge. It tries to crack Windows passwords from obtained hashes from stand-alone Windows workstation, primary domain controllers, networked servers or Active Directory. It can sometimes sniff hashes off the wire. These tools also have several methods of generating password guesses.

Is Lophtcrack Free?

No, 3 versions of LophtCrack: Professional, Administrator and Consultant are available for purchase.

Does LophtCrack Work on all Operating Systems?

No, it only works for Microsoft Windows.

What are the Typical Uses for L0phtCrack?

L0phtCrack is used to recover lost Microsoft Windows passwords or to test someone's password strength. It uses brute force, rainbow tables, and hybrid and dictionary attacks. Even if this one of the tools of choice, crackers' use old versions because of its high availability and low price.

Download from: http://1337x.org/torrent/42867/0/ (use torrent client to download)

2. LCP

Main purpose of LCP program is user account passwords auditing and recovery in

Windows NT/2000/XP/2003. Accounts information import, Passwords recovery, Brute force session distribution, Hashes computing.

A good free alternative to Lophtcrack.

LCP was briefly mentioned in our well read Rainbow Tables and Rainbow Crack article.

Download from:http://www.lcpsoft.com/english/download.htm

3. Hacking windows administrator password of xp/vista/7

This hack will show you how to reset Windows administrator password (for Win 2000, XP, Vista and Win 7) at times when you forget it or when you want to gain access to a computer for which you do not know the password.

Most of us have experienced a situation where in we need to gain access to a computer which is password protected or at times we may forget the administrator password without which it becomes impossible to login to the computer. So here is an excellent hack using which you can reset the password or make the password empty (remove the password) so that you can gain administrator access to the computer. You can do this with a small tool called Offline NT Password & Registry Editor. This utility works offline, that means you need to shut down your computer and boot off your using a floppy disk, CD or USB device (such as pen drive). The tool has the following features.

You do not need to know the old password to set a new one

You will detect and offer to unlock locked or disabled out user accounts!

There is also a registry editor and other registry utilities that works under Linux/Unix, and can be used for other things than password editing.

How it works?

Most Windows operating systems stores the login passwords and other encrypted passwords in a file called same (Security Accounts Manager). This file can be usually found in \windows\system32\config. This file is a part of Windows registry and remains inaccessible as long as the OS is active. Hence it is necessary that you need to boot off your computer and access this same file via boot. This tool intelligently gains access to this file and will reset/remove the password associated with administrator or any other account.

Offline NT Password &Reg Editor Download

It is recommended that you download the CD version of the tool since floppy drive is outdated and doesn't exist in today's computer. Once you download you'll get a bootable image which you need to burn it onto your CD. Now boot your computer from this CD and follow the screen instructions to reset the password.

Another simple way to reset non-administrator account passwords

Here is another simple way through which you can reset the password of any non-administrator accounts. The only requirement for this is that you need to have administrator privileges. Here is a step-by-step instruction to accomplish this task.

1. Open the command prompt (Start->Run->type cmd->Enter)

2. Now type net user and hit Enter

3. Now the system will show you a list of user accounts on the computer. Say for example you need to reset the password of the account by name eldho, and then do as follows

4. Type net user eldho * and hit Enter. Now the system will ask you to enter the new password for the account. That's it. Now you've successfully reset the password for John without knowing his old password.

4. Key-Logger

Keyloggers capture and store all the keystokes which we typed in the system; modern keyloggers can capture system events&activities, screen shotes and clipboard.

Some of them can act as spy too, all the datas will be sending to your mail id.

Download from: http://1337x.org/torrent/47798/0/ (use torrent client to download)

5. USB Keylogger

It capture all the keystrokes by using a USB drive which contain the usbkeylogger software

Download from:http://www.keyghost.com/USB-Keylogger.htm (paided s/w :( )

6. Keyloggerfor Mobile

A Keylogger is program or file that has been executed to record all of the keystrokes a computer. This can be utilized for monitoring all the activities that takes place on a computer and the details will be stored in the software.

Keylogger for S60v3 is used to monitor the keystroke that occurs on your Symbian device when the application is running. The software is written is python language and it requiring its runtime environment for proper working.

7. Spyware

It will capture all the events,activities, website visited, keystroke, and screenshots, from a remote machine to our machine through mail

Download from: http://1337x.org/torrent/47798/0/(use torrent client to download)

8. Openpuff (Stenography Tool)

OpenPuff is a advanced watermarking and Steganography, or data hiding, program capable of storing up to 256MB of encrypted data using an invisible copyright mark in pictures, video, audio, and flash files. OpenPuff supports many carrier formats: images (BMP, JPG, PCX, PNG, TGA), audio support (AIFF, MP3, NEXT/SUN, WAV), video support (3GP, MP4, MPG, VOB) and flash-Adobe support (FLV, SWF, PDF).

Download from: http://embeddedsw.net/zip/OpenPuffv340.zip

3.6.2 Viruses, Exploits, Worms, and More

The term computer "virus" originated to describe machine code command inserted into a computer's memory that, on execution, copies itself into other programs and files on the computer. Depending on the hacker's intent, the design of a virus can merely be an inconvenience or have very serious consequences up to a potential catastrophe.

Generally, a virus is a piece of software, a series of data, or a command sequence that exploits a bug, glitch, or vulnerability. Each example is appropriately termed an "exploit." An exploit causes unintended or unanticipated behavior to occur in a computer's operating system or applications while propagating itself within the computer.

An exploit and operates through a network security vulnerability or "hole" without previous access to the vulnerable system is a "remote" exploit. An exploit that needs prior access to a system is termed a "local" exploit. These are usually intended to increase the hacker's access privileges beyond those granted by a system administrator.

Worms are simply viruses that send copies over network connections. A bomb resides silently in a computer's memory until set off by a date or action. A Trojan horse is a malicious program that cannot reproduce itself, but is distributed by CD or e-mail.

3.7 Avoid Computer Holes/Vulnerabilities

Install only trusted software and delete unknown emails. If you have any doubt about a piece of software's function, do not install it. If you receive e-mails from random people's names, resist your curiosity and do not open it, just delete it.

Under no conditions download or open attachments from anyone that you do not know and even then be cautious. Banks and most companies that create online personal accounts will not send you attachments. If they do, it is probably best to go to the company site and request the download or at least see if it is legitimate. Avoid adult web sites, a hacker's paradise.

Whether in your e-mail or online, do not click on ads. If the ad is of interest, find the site. Be careful with what you physically put into your computer. This is especially true for shared R/W CDs, USB hard disks, or flash drives. This is an easy path for a virus to follow from computer to computer.

3.7.1 Protection: Install Anti-Virus Software

Anti-virus software searches for evidence of the presence of viral programs, worm, bombs, and Trojan horses by checking for the characteristic appearances or behaviours that is typical of these programs. When found the program logs its discovery, its type, often its name or an identifier, and it potential for damage. The anti-virus software then eliminates or isolates/quarantines the infected files. For the individual, commercial software is relatively inexpensive; however, there are free anti-virus programs available.

Since new viruses appear almost daily with new code it is imperative that you update you antivirus program often to keep up with these threats; therefore, make sure to set your program to update automatically. To avoid the annoyance of computer slowdown schedule full scale scans late at night.

The same is true for your Windows Operating System. Very often, your OS is where hackers discover the holes to exploit. Of course, in an ever-continuing battle, this software is continuously updated with security patches.

Finally, secure your wireless network with a router that has a built in firewall. Almost all wireless routers are set to no security when first installed. Log into the router and at least set it to basic security with a strong password to replace the factory setting that any hacker knows. A firewall or router that is not configured properly or non-existent allows hackers to scan passwords, e-mails, or files that cross your network connection.

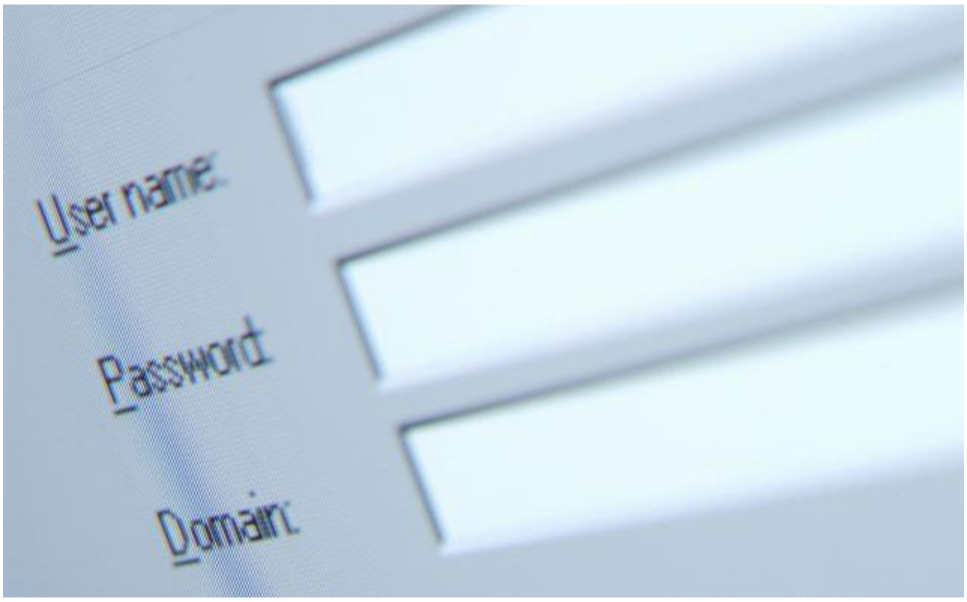
3.8 System Hacking Scenario

Password hacking is one of the easiest and most common ways hackers obtain unauthorized computer or network access. Although strong passwords that are difficult to crack (or guess) are easy to create and maintain, users often fail to take advantage of this. Therefore, passwords are one of the weakest links in the information-security chain. Passwords rely on secrecy for their security. After a password is compromised, its original owner isn’t the only person who can access the system with it. As you'll learn, hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This unit demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exit in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems.

3.8.1 Is Computer Hacking a Crime?

The term "hacking" is often used as if it's synonymous with illegal computer access. Hacking isn't necessarily a criminal activity, however. A computer hacker can simply be someone who knows how to circumvent the limitations of a device or a piece of software. Ethical hackers often break into computer systems with permission to find vulnerabilities and improve security. Hacking is a crime when the perpetrators access systems without the owner's permission.

3.8.2 Hacking Process



The term "hacking" is a very broad one. Hacking a device or system can refer to altering or improving it, without any suggestion of illicit access. An example of such a "hack" might be turning off the Wi-Fi adapter on your laptop to save the battery. More commonly, hacking, means circumventing the security measures of a computer or networked computer system. It can be done legally and ethically; non-maliciously but illegally; or illegally and with intent to do harm, in which case the term "cracking" may apply.

3.8.3 Laws and Regulations

The laws relating to computer hacking vary from region to region. Broadly speaking, it's typically illegal to access a private computer system unless you have the express permission of the individual or organization the system belongs to. Penalties are usually more severe if malicious damage is involved. Hacking into government systems, even without any malicious intent, often carries a particularly high penalty, as this can have national security implications.

3.8.4 Hacking Versus Cracking

The hacker community is strongly opposed to what they see as the widespread misuse of the term "hacking" to designate malicious intrusions and deliberate damage of computer systems. Many self-described hackers regard this kind of behaviour as unacceptable and prefer the term "cracking" to describe it, with the perpetrators being described as "crackers." Ethical hacking is sometimes referred to as "white hat hacking" to distinguish it from cracking, which is also termed "black hat hacking." "Gray hat hacking" describes activity that's somewhere between the two, existing in a legal and ethical gray area.

3.8.5 Illegal Hacking

Illegal hacking involves computer-related activity that breaks the law. Motivations include simple curiosity, where a person has no intention of damaging a system or causing problems, and is solely interested in obtaining information. If done without permission, this kind of hacking is still illegal. Some incursions are motivated by prankishness and involve annoying but ultimately fairly benign conduct. More serious acts of cracking or black hat hacking include vandalizing websites, deleting information, stealing private information such as lists of client names and details, or placing malware on computer systems.

3.8.6 Legal Hacking

Legal hacking is very narrowly defined, so it's up to hackers to familiarize themselves with local and national laws regarding hacking, and to work within them. Generally speaking, hacking may be legal if you are working on your own computer system or if you have explicit and detailed written permission for anything you do to someone else's system.

3.8.7 Uses of Legal Hacking

Legal hacking is often used by organizations who want to ensure the safety of their computer systems. To this end, hackers may volunteer or be recruited to attempt to break into a system or device as if they were criminals, in order to pinpoint security flaws. Some companies issue public challenges to hackers to break into their systems, offering a reward; more typically, security consultants are contracted to attempt a hack.

3.9 Remote Password Guessing

As an organization's IT security practices mature, it gets better at protecting its network perimeter systems: the patches get applied more regularly, the firewall rules become more restrictive, the OS gets locked-down more rigorously. Even at such companies, authentication systems often lag behind. If the employees, partners, customers, vendors need to remotely access an application with logon screen that requires a password, two things will often hold true:

1. The application will assist the user in remembering the password.

This may involve emailing the password to the user's email address. If you're an attacker, you will try gaining access to that inbox to retrieve the password.

The application may also present the user with a "secret question" picked by him or her in advance. Unfortunately, such questions often have easy-to-guess answers. Favourite colour: Blue. Favourite month: March. It doesn't take many tries to go through likely answers to such questions. Even if it doesn't work for a particular user, it may work over a large population of targeted users. In many cases, answering such questions may not trigger the account lock-out mechanism.

Finally, the application may provide a different response to a valid username than to an invalid username. For instance, if the username and password are both incorrect, it might say "Access denied." But if the username is correct, it might say "Password incorrect."

Make sure your users recognize the importance of protecting access to their email boxes. Help them by protecting the email servers. Also, consider implementing complexity requirements for answers to secret questions or give users a few secret questions to chose from, but omit common questions such as those about colour. Finally, don't provide too much information in response to a failure to logon successfully.

2. The user will select an easy to remember and easy-to-guess password.

There are too many passwords to remember. Of course, users will try to select those that are easy for them to remember. Much has been said about encouraging users to select hard-to-guess passwords, so I won't repeat the discussion here. Once concern to keep in mind is that if your selection requirements are too strict, or if the users need to change the password too often, they will still find a way to beat the system. They may write the passwords down or use the same password across multiple systems/sites/organizations.

Also, the use of default passwords plagues many environments. If possible, require that your users change the pre-assigned password after first logging on to the system, and make sure the default passwords you assign are difficult to guess.

Automatically locking an account after several failed logon attempts will address many of these concerns, but sometimes it's not a feasible option. We may be concerned about denying service to our customers or executives. Or we may not have the staff to deal with unlock-my-account requests. A nice compromise is often a mechanism that locks the account for a few minutes, then automatically unlocks it. This can slow down the attacker's guessing tactics, yet allow the legitimate user to login after a brief waiting period. Implementing CAPCHA to discern between human and non-human users of your site can be effective as well to discourage automated password guessing.

3.9.1 Include Remote Password Guessing in Your Assessment

If your security assessment procedures do not already include remote password guessing, consider adding this task. The steps that come to mind include:

Identify publicly-accessible services/applications that request username/password credentials and attempt by passing them via manual guessing. Keep an eye out for account lock-out mechanisms.

Query Google and examine your public website to identify possible usernames. (The Backtrack CD has some nice tools for that.)

Compile a list of possible passwords the users might use, accounting for your organization's location, name, and industry-specific terminology. Add common names and words like "password" to the list. I find that having a short, but intelligently-crafted list is more effective than using a 100KB dictionary file (the long file often takes too long to cycle through remotely).

After trying the manual route, make use of an automated password guessing tool to see whether it can guess logon credentials using the short password list you put together. Hydra is an excellent tool for this task. It's free, fast, and effective, even though it's poorly documented. (Anyone feels like writing a comprehensive guide to using Hydra, or pointing us to one that already exists?) Hydra is included on the above-mentioned Backtrack CD, and supports most of the protocols you're likely to encounter in the field.

3.10 Eavesdropping

Eavesdropping is as an electronic attack where digital communications are intercepted by an individual whom they are not intended.

This is done in two main ways: Directly listening to digital or analog voice communication or the interception or sniffing of data relating to any form of communication.

Eavesdropping is the act of intercepting communications between two points.

In the digital world, eavesdropping takes the form of sniffing for data in what is called network eavesdropping. A specialized program is used to sniff and record packets of data communications from a network and then subsequently listened to or read using cryptographic tools for analysis and decryption.

For example, Voice over IP (VoIP) calls made using IP-based communication can be picked up and recorded using protocol analyzers and then converted to audio files using other specialized software.

Data sniffing is easily done on a local network that uses a HUB since all communications are sent to all the ports (non-recipients just drop the data) and a sniffer will simply accept all of the incoming data.

This goes the same for wireless networking where data is broadcast so even non-recipients can receive the data if they have the proper tools.

Actual eavesdropping, that is the simple act of listening to other people talk without them knowing it, can be done using current technology such as hidden microphones and recorders.

Hacking into devices such as IP phones is also done in order to eavesdrop on the owner of the phone by remotely activating the speaker phone function.

Devices with microphones including laptops and cellphones also can be hacked to remotely activate their microphones and discretely senddata to the attacker.

3.11 Various methods of password cracking

Most people understand that good password security is the first and most effective strategy for protecting sensitive systems and data, yet systems are regularly compromised via breached user accounts.

It is fairly common knowledge that one should use strong passwords that are not easily "guessed" - such as by employing passwords that are 12 to 16 characters in length that use both upper and lower case letters, and which include non-alphanumeric characters.

But sophisticated hackers are not always simply attempting to "guess" passwords based on information lifted from social networks and the like, but instead are using various methods to undermine what most would think to be a secure password choice.

PC Pro's Davey Winder posted a nice little write-up on the top ten methods hackers use to crack passwords

Winder's top ten and a brief excerpt of the technique are as follows:

1. Dictionary attack

This uses a simple file containing words that can, surprise, be found in a dictionary. In other words, if you will excuse the pun, this attack uses exactly the kind of words that many people use as their password.

2. Brute force attack

This method is similar to the dictionary attack but with the added bonus, for the hacker, of being able to detect non-dictionary words by working through all possible alpha-numeric combinations from aaa1 to zzz10.

3. Rainbow table attack

A rainbow table is a list of pre-computed hashes - the numerical value of an encrypted password, used by most systems today - and that’s the hashes of all possible password combinations for any given hashing algorithm mind. The time it takes to crack a password using a rainbow table is reduced to the time it takes to look it up in the list.

4. Phishing

There's an easy way to hack: ask the user for his or her password. A phishing email leads the unsuspecting reader to a faked online banking, payment or other site in order to login and put right some terrible problem with their security.

5. Social engineering

A favorite of the social engineer is to telephone an office posing as an IT security tech guy and simply ask for the network access password. You’d be amazed how often this works.

6. Malware

A key logger or screen scraper can be installed by malware which records everything you type or takes screen shots during a login process, and then forwards a copy of this file to hacker central.

7. Offline cracking

Often the target in question has been compromised via an hack on a third party, which then provides access to the system servers and those all-important user password hash files. The password cracker can then take as long as they need to try and crack the code without alerting the target system or individual user.

8. Shoulder surfing

The service personnel 'uniform' provides a kind of free pass to wander around unhindered, and make note of passwords being entered by genuine members of staff. It also provides an excellent opportunity to eyeball all those post-it notes stuck to the front of LCD screens with logins scribbled upon them.

9. Spidering

Savvy hackers have realized that many corporate passwords are made up of words that are connected to the business itself. Studying corporate literature, website sales material and even the websites of competitors and listed customers can provide the ammunition to build a custom word list to use in a brute force attack.

10. Guess

The password crackers best friend, of course, is the predictability of the user. Unless a truly random password has been created using software dedicated to the task, a user generated 'random' password is unlikely to be anything of the sort.

3.12 Keystroke Logger

No doubt everyone wants to know who and how is using their PC. Especially when it comes to situations when the owner is away from PC and cannot physically control its usage. Here is when using keystroke logger can be a perfect solution for you as it will keep you informed of everything what was typed on your PC.

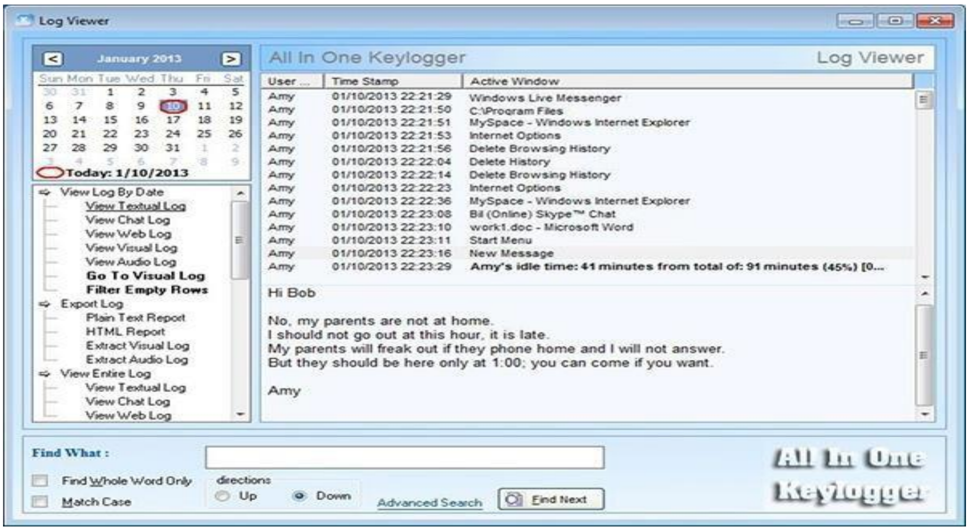
Keystroke logger Software allows tracking everything what was typed on your PC. With keystroke recorder you can easily get access to all keystrokes, messages typed in Instant messengers, texts of emails which were typed, passwords, texts typed in different documents and so on. In other words keystroke logger tracks any keyboard activity including system keys and controls on multimedia keyboards.

Keystroke loggers are often used as a spyware tool by cybercriminals to steal personally identifiable information (PII), login credentials and sensitive enterprise data. Keystroke logger recorders may also be used by employers to observe employees' computer activities, parents to supervise their children's internet usage, users to track possible unauthorized activity on their devices or law enforcement agencies to analyze incidents involving computer use. These uses are considered ethical or appropriate in varying degrees.

3.12.1 Types of Keystroke Logger

A hardware-based Keystroke logger is a small device that serves as a connector between the computer keyboard and the computer. The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adaptor, making it relatively easy for someone who wants to monitor a user's behavior to hide such a device.

Most workstation keyboards also plug into the back of the computer, keeping the connections out of the user's line of sight. A hardware Keystroke logger may also come in the form of a module that is installed inside the keyboard itself. When the user types on the keyboard, the Keystroke logger collects each keystroke and saves it as text in its own miniature hard drive, which may have a memory capacity of up to several gigabytes. The person who installed the Keystroke logger must later return and physically remove the device in order to access the information that has been gathered. There are also wireless Keystroke logger sniffers that can intercept and decrypt data packets being transferred between a wireless keyboard and its receiver.



User ...	Time Stamp	Active Window
Amy	01/10/2013 22:21:29	Windows Live Messenger
Amy	01/10/2013 22:21:50	C:\Program Files
Amy	01/10/2013 22:21:51	MySpace - Windows Internet Explorer
Amy	01/10/2013 22:21:53	Internet Options
Amy	01/10/2013 22:21:56	Delete Browsing History
Amy	01/10/2013 22:22:04	Delete History
Amy	01/10/2013 22:22:14	Delete Browsing History
Amy	01/10/2013 22:22:23	Internet Options
Amy	01/10/2013 22:22:36	MySpace - Windows Internet Explorer
Amy	01/10/2013 22:23:08	Bil (Online) Skype™ Chat
Amy	01/10/2013 22:23:10	work1.doc - Microsoft Word
Amy	01/10/2013 22:23:11	Start Menu
Amy	01/10/2013 22:23:16	New Message
Amy	01/10/2013 22:23:29	**Amy's idle time: 41 minutes from total of: 91 minutes (45%) [0...**

Hi Bob

No, my parents are not at home.
I should not go out at this hour, it is late.
My parents will freak out if they phone home and I will not answer.
But they should be here only at 1:00; you can come if you want.

Amy

Screenshot of data captured from Keystroke logger software

A key logging software program Bottom of Form does not require physical access to the user's computer for installation. It can be downloaded on purpose by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly and executed as part of a rootkit or remote administration Trojan (RAT). The rootkit can launch and operate stealthily in order to evade manual detection or antivirus scans.

A common Keystroke logger program typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file that does all the recording and an executable file that installs the DLL file and triggers it to work. The Keystroke logger program records each keystroke the user types and uploads the information over the internet periodically to whoever installed the program. There are many other ways that key logging software can be designed to monitor keystrokes, including hooking keyboard APIs to another application, malicious script injection or memory injection.

Some key logging programs may include functionality for recording user data besides keystrokes, such as capturing anything that has been copied to the clipboard and taking screenshots of the user's screen or a single application.

3.12.2 Detection, Prevention and Removal

As there are various types of Keystroke logger that use different techniques, no single detection or removal method is considered the most effective.

Antikeylogger software is designed specifically to scan for software-based Keystroke loggers, by comparing the files on a computer against a Keystroke logger signature base or a checklist of common Keystroke logger attributes. Using an antikeylogger can be more effective than using an antivirus or antispyware program, as the latter may identify a Keystroke logger as a legitimate program instead of spyware.

3.13 Let us Sum-up

Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Those individuals who engage in computer hacking activities are typically referred to as “hackers.”

Computer programmers as a subculture of the general engineering and scientific community have their own set of heroes with aspects based on the values that programmers respect. These heroic figures, called hackers, are not at all like the popular press version of the computer hacker. Legendary hackers are both real and fictional, but tend to share certain common features: extraordinary programming skill, cleverness in the face of difficulty, an ability to suspend all other activities while producing a solution to a problem, an appreciation for a clever solution to a seemingly insignificant problem, weakness in some other aspect to balance their skill as a hacker, and adherence to some form of the Hacker Ethic.

3.14 Self Assessment Questions

1. What is System Hacking?

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

2. Types of System Hacking

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

3. What Is Rootkits?

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

4. What is Steganography?

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

5. Why need uses of legal hacking?

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

…………………………………………………………………………………
…………………………..……………………………………………………

3.15 Model Questions

1. What is Eavesdropping and explain its?
2. Explain about different type of hacker tools.
3. Write the different between hacker tools and hacking tools.
4. Write the sort notes about legal hacking and illegal hacking.
5. Write the various methods of password cracking.

3.16 References & Further Readings

1. http://itstillworks.com/computer-hacking-crime-1387.html
2. https://isc.sans.edu/forums/diary/Remote+Password+Guessing+Concerns+Observations+Recommendations/3212/
3. http://kyrion.in/blog/2017/06/22/computer-hacking-crime/
4. https://www.gohacking.com/hack-windows-administrator-password/

UNIT-4 Sniffer

Unit Structure

4.0 Introduction

Some of the more “legitimate” uses for a sniffer fall towards the roles of the network administrators. They can be used to probe the network for bandwidth usage, helping pinpoint which individual machines may be running malware or simply have wrong network settings. Sniffers are often used as a practical defense against finding intrusion attempts by detecting inappropriate traffic. If you’re ever going to be in a role where you need to ensure your network is protected, you would do well to learn how to use a sniffer. I recommend Wireshark (formerly known as Ethereal), it’s free (as in beer) and well supported with great documentation. Other alternatives are NAI Sniffer (commercial), TCPDump (*nix), WinDump (Win32), Cain & Abel, Dsniff, and Ettercap (the last three are more specialized for password extraction but can still be used to test your applications or network protocols).

Sniffers can also be used to bypass security. Many application protocols pass credentials in plain text or use weak encryption that is easy for a sniffer to decode. Common examples of insecure protocols are FTP, Telnet, POP3, SMTP, and HTTP Basic Authentication. Instead, secured/encrypted protocols should be used, SFTP, SSH, HTTPS (SSL).

4.1 Learning Objective

After learning this unit you should be able to

- Know about what a sniffer is and what is sniffing.
- Classify different types of sniffers and its use.
- Identify different types of hackers.
- Study about how sniffer attacks takes place.
- Know about ARP and how ARP works and its use.
- Study about ARP spooling and spooling attack.
- Know aboutDNS, DNS work and DNS spooling.
- Understand DNS Spoofing Techniques and poisoning.
- Know about the MAC, MAC spooling and MAC spooling attack.
- Know the Countermeasure of sniffing attacks.

4.2 What is a Sniffer

A sniffer, which can also be referred to as a network analyzer, is a piece of software that analyzes network traffic, decodes it, and gives it back packet information so that a network administrator can use it to help diagnose problems on the network. But because these tools can be so powerful, they can also help give leverage to those of the black hat world by allowing them to pull plain text information off the network as well (usernames, passwords, unencrypted emails, instant message chat, etc.).

4.3 What is Sniffing

Sniffing is one of the most effective techniques in attacking a wireless network whether it is mapping the network to gain information, to grab information, or to capture encrypted data. Sniffers usually act as network probes or snoops; examine network traffic but not intercepting or altering it.

A sniffer sometimes referred to as a network monitor or network analyzer, can be used by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the sniffer an administrator can identify erroneous packets and use the data pinpoint bottlenecks and help maintain efficient network data transmission.

Sniffer simply captured all data packets pass through a given network interface.

By placing a sniffer on a network in promiscuous mode a malicious intruder can capture and analyze all of the network traffic. Within a given network, user name and password information is generally transmitted in clear text which means that information is generally transmitted in clear text which means that the information would be viewable by analyzing the packets being transmitted.

A sniffer can only capture packet information within a given subnet so it is not possible for a malicious attacker to place a packet sniffer on their home ISP network and capture network traffic from inside your corporate network.

However if one machine on the internal networks becomes compromised through a Trojan or other security breach, the introducer could run sniffer from that machine and use the captured user name and password information to compromise other machine on the network.

4.3.1 Types of Sniffing

Sniffing is of two types:
1. Active Sniffing
2. Passive sniffing

The terms active and passive sniffing has also been used to describe wireless network sniffing. They have analogous meaning. Passive wireless sniffing involves sending no packets, and monitoring the packets send by other. Active sniffing involves sending out multiple networks to identify APs.

4.3.1.1 Active Sniffing

When sniffing is performed on a switched network, it is known as active sniffing.

Active sniffing relies on injecting packets into the network that cause traffic. Active sniffing is required to bypass the segmentation that switches provided. Switch maintain their own Arp cache special type of memory known as content addressable Memory (CAM),keeping track of which host is connected to which port.

Sniffers are operated at the Data Link Layer of OSI model. This means that they do not have to play by the same rules as application and services that resides further up stack. Sniffer can grab whatever they see on the wire and record it for later review. They allow the user to see all the data contained in packet, even information that should remain hidden.

4.3.1.2 Passive Sniffing

Hubs see all the traffic in that particular collision domain. Sniffing performed on a hub is known as passive sniffing.

Passive sniffing is performed when the use is on a hub. Because the user is on a hub, all traffic is sent to all ports. All the Attacker must do is to start the sniffer and just wait for someone on the same collision domain to start sending or receiving data. Collision domain is a logical area of the same collision domain to start sending or receiving data. Collision domain is a logical area of the network in which one or more data packets can collide with each other.

Compatibility of Passive Sniffing

Passive sniffing worked well during the days that hubs were used. The problem is that there are few of these devices left.Nowdays most of the network are working on switches where active sniffing is useful.

4.4 Understanding Packet Sniffers

Network traffic is one of most resource laden stream which contains everything we talk about on internet. If you can get data from it, you can know what is my password or even Google's Password, in technical words it's called as Network Sniffing and software which are used to sniff data are called as Packet Sniffers. SO if you place a sniffer on a router (router is a hardware which sends data to right destination) you can see all the data and record it. Imagine the power of it now!!!

4.4.1 What is A Packet Sniffer?

A packet sniffer is a program which runs silently and monitors data on a network stream. It's called as passive as it does not send any information to you but just collects and stores it somewhere. If you run such a sniffer on your system, it can tell you your own IP address and IP addresses of other sites which you visit.

4.4.2 How Packet Sniffers Work?

Sniffers are basically small programs with one goal, interception of data. They can watch all unencrypted data that travels from your computer or when on router it can see all the data travelling through network. Now the question is how they are allowed to read data. It's possible because of the architecture itself. Which means, if you send some data I will read it but I will accept it only when the data is addressed to me.But now think, we have 4-5 computers in a network? You send a message to Computer A which is not having any sniffer. But Computer B is having one. If you send some information to computer A, the message is send to everybody with IP address of Computer A, so all the computers except A should reject it, but I have one sniffer on Computer B. So though computer itself rejects it but the sniffer accepts the data.

Thus if you are sending unencrypted data on a network, there is a high chance of your data being stolen.

4.4.3 What Are The Types Of Packet Sniffers?

- **Commercial Sniffers** which are used by network administrator to control the type and see the bottle neck data.
- **Underground Sniffers** which are used to steal data, so as to gain access of data stored which can be used for bad.

4.4.4 What are the uses of packet sniffers?

Packet Sniffers was never made to hack or stole information. They had a different goal, to make things secure. But then everything has a dark side. Here are few uses:-

- Network Analysis to find the traffic and its problem around the network.
- Detect Attackers if some resource is used high and traffic is coming from same ip again and again.
- Searching unencrypted text like password.
- To convert data into human readable format, mostly used in war to get hold of enemies.

Sniffers are very hard to detect due to its passiveness but there is always a way.

4.5 Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

4.5.1 How ARP Works

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

Since protocol details differ for each type of local area network, there are separate ARP Requests for Comments (RFC) for Ethernet, ATM, Fiber Distributed-Data Interface, HIPPI, and other protocols.

4.5.2 What Is ARP Spoofing?

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

4.5.3 ARP Spoofing Attacks

The effects of ARP spoofing attacks can have serious implications for enterprises. In their most basic application, ARP spoofing attacks are used to steal sensitive information. Beyond this, ARP spoofing attacks are often used to facilitate other attacks such as:

- **Denial-of-service attacks:** DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.

- **Session hijacking:** Session hijacking attacks can use ARP spoofing to steal session IDs, granting attacker's access to private systems and data.

- **Man-in-the-middle attacks:** MITM attacks can rely on ARP spoofing to intercept and modify traffic between victims.

4.5.4 ARP Spoofing Detection, Prevention and Protection

The following methods are recommended measures for detecting, preventing and protecting against ARP spoofing attacks:

- Packet filtering: Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in ARP spoofing prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).

- Avoid trust relationships: Organizations should develop protocols that rely on trust relationships as little as possible. Trust relationships rely only on IP addresses for authentication, making it significantly easier for attackers to run ARP spoofing attacks when they are in place.

- Use ARP spoofing detection software: There are many programs available that help organizations detect ARP spoofing attacks. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.

- Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster ARP spoofing attack prevention by encrypting data prior to transmission and authenticating data when it is received.

4.6 ARP Poisoning

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.

The attack itself consists of an attacker sending a false ARP reply message to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address (and vice-versa, so his or her target's MAC is now associated with the attacker's IP address). Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to its real destination. Because ARP Poisoning attacks occur on such a low level, users targeted by ARP Poisoning rarely realize that their traffic is being inspected or modified. Besides Man-in-the-Middle Attacks, ARP Poisoning can be used to cause a denial-of-service condition over a LAN by simply intercepting or dropping and not forwarding the target's packets.

4.6.1 ARP Poisoning (MITM) Attack

A Man-In-The-Middle (MITM) attack is achieved when an attacker poisons the ARP cache of two devices with the (48-bit) MAC address of their Ethernet NIC (Network Interface Card). Once the ARP cache has been successfully poisoned, each of the victim devices sends all their packets to the attacker when communicating to the other device. This puts the attacker in the middle of the communications path between the two victim devices; hence the name Man-In-The-Middle (MITM) attacks. It allows an attacker to easily monitor all communication between victim devices.

4.7 Domain Name System (DNS)

The domain name system (DNS) is the way that internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website. For example, if someone types TechTarget.com into a web browser, a server behind the scenes will map that name to the IP address 206.19.49.149.

Web browsing and most other internet activity rely on DNS to quickly provide the information necessary to connect users to remote hosts. DNS mapping is distributed throughout the internet in a hierarchy of authority. Access providers and enterprises, as well as governments, universities and other organizations, typically have their own assigned ranges of IP addresses and an assigned domain name; they also typically run DNS servers to manage the mapping of those names to those addresses. Most URLs are built around the domain name of the web server that takes client requests.

4.7.1 How does DNS work?

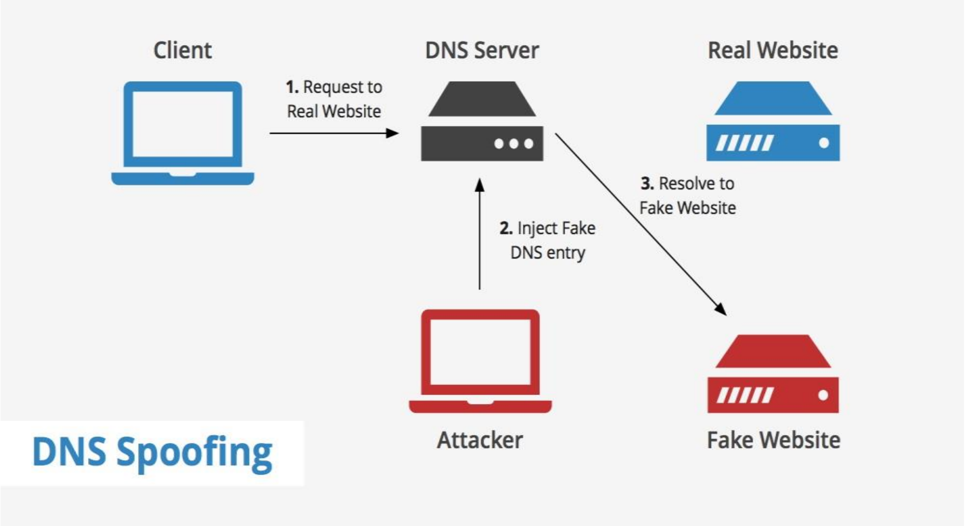
DNS servers answer questions from both inside and outside their own domains. When a server receives a request from outside the domain for information about a name or address inside the domain, it provides the authoritative answer. When a server receives a request from inside its own domain for information about a name or address outside that domain, it passes the request out to another server usually one managed by its internet service provider. If that server does not know the answer or the authoritative source for the answer, it will reach out to the DNS servers for the top-level domain e.g., for all of .com or .edu. Then, it will pass the request down to the authoritative server for the specific domain e.g., techtarget.com or stkate.edu; the answer flows back along the same path.

4.7.2 How does DNS increase web performance?

To promote efficiency, servers can cache the answers they receive for a set amount of time. This allows them to respond more quickly the next time a request for the same lookup comes in. For example, if everyone in an office needs to access the same training video on a particular website on the same day, the local DNS server will ordinarily only has to resolve the name once, and then it can serve all the other requests out of its cache. The length of time the record is held the time to live is configurable; longer values decrease the load on servers, shorter values ensure the most accurate responses.

4.7.3 What Is DNS Spoofing?

DNS spoofing occurs when a particular DNS server's records of "spoofed" or altered maliciously to redirect traffic to the attacker. This redirection of traffic allows the attacker to spread malware, steal data, etc. For example, if a DNS record is spoofed, then the attacker can manage to redirect all the traffic that relied on the correct DNS record to visit a fake website that the attacker has created to resemble the real site or a different site completely.



4.7.4 How Does Normal DNS Communication Work?

A DNS server is used for the purpose of resolving a domain name (such as keycdn.com) into the associated IP address that it maps to. Once the DNS server finds the appropriate IP address, data transfer can begin between the client and website's server. The visualization below shows a how this process takes place at a high level.

Once the DNS server finds the domain-to-IP translation, it will cache it so that upon subsequent requests for that domain, the DNS lookup will happen much faster. However, this is where DNS spoofing can become a real problem since a false DNS lookup can be injected into the DNS server's cache thus altering the visitors' destination.

4.7.5 How Does DNS Spoofing Work?

DNS spoofing is an overarching term and can be carried out using various methods such as:

- DNS cache poisoning
- Compromising a DNS server
- Implementing a Man in the Middle Attack

However, an attacker's end goal is usually the same no matter which method they use. Either they want to steal information, re-route you to a website that benefits them, or spread malware. The most discussed method to perform DNS spoofing is using cache poisoning which we'll explain next.

4.7.6 How to Prevent DNS Spoofing

As a website visitor, there's not much you can do to prevent DNS spoofing. Rather, this falls more in the hands of the actual DNS provider that is handling a website's DNS lookups as well as the website owner. Therefore, a few tips for site owners and DNS providers include:

Implement DNS spoofing detection mechanisms – it's important to implement DNS spoofing detection software. Products such as XArp help product against ARP cache poisoning by inspecting the data that comes through before transmitting it.

Use encrypted data transfer protocols – Using end-to-end encryption via SSL/TLS will help decrease the chance that a website / its visitors are compromised by DNS spoofing. This type of encryption allows the users to verify whether the server's digital certificate is valid and belongs to the website's expected owner.

Use DNSSEC – DNSSEC, or Domain Name System Security Extensions, uses digitally signed DNS records to help determine data authenticity. DNSSEC is still a work in progress as far as deployment goes, however implement in the Internet root was level in 2010. An example of a DNS service that fully supports DNSSEC is Google's Public DNS.

4.7.7 Understand DNS Spoofing Techniques

DNS Spoofing (or DNS Poisoning) this is a technique that tricks a DNS server into believing it has received authentic information when in reality it hasn't. Once the DNS server has been poisoned, the information is generally

Cache

d for a while, spreading the effect of the attack to the users of the server. When a user requests a certain website URL, the address is looked up on a DNS server to find the corresponding IP address. If the DNS server has been compromised, the user is redirected to a website other than the one that was requested, such as a fake website.

To perform a DNS attack, the attacker exploits a flaw in the DNS server software that can make it accept incorrect information. If the server doesn't correctly validate DNS responses to ensure that they come from an authoritative source, the server ends up caching the incorrect entries locally and serving them to users that make subsequent requests. This technique can be used to replace arbitrary content for a set of victims with content of an attacker's choosing. For example, an attacker poisons the IP addresses DNS entries for a target website on a given DNS server, replacing them with the IP address of a server the hacker controls. The hacker then creates fake entries for files on this server with names matching those on the target server. These files may contain malicious content, such as a worm or a virus. A user whose computer has referenced the poisoned DNS server is tricked into thinking the content comes from the target server and unknowingly downloads malicious content.

The types of DNS spoofing techniques are as follows:
Intranet Spoofing Acting as a device on the same internal network
Internet Spoofing Acting as a device on the Internet
Proxy Server DNS Poisoning Modifying the DNS entries on a proxy server so the user is redirected to a different host system
DNS Cache Poisoning Modifying the DNS entries on any system so the user is redirected to a different host.

4.8 DNS Cache Poisoning

Since DNS servers cache the DNS translation for faster, more efficient browsing, attackers can take advantage of this to perform DNS spoofing. If an attacker is able to inject a forged DNS entry into the DNS server, all users will now be using that forged DNS entry until the cache expires. Once the cache expires, the DNS entry will return to normal as the DNS server will go through the complete DNS lookup process again. However, if the DNS server's software still hasn't been updated, then the attacker can replicate this error and continue funnelling visitors to their website.

DNS cache poisoning can also sometimes be quite difficult to spot. If the malicious website is very similar to the website it is trying to impersonate, some users may not even notice the difference. Additionally, if the attacker is using DNS cache poisoning to compromise one company's DNS records in order to have access to their emails for example, then this may also be difficult to detect.

4.9 What is MAC Flooding?

The MAC Flooding is an attacking method intended to compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table. This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch. This table allows the switches to direct the data out of the ports where the recipient is located. As we've already seen, the hubs broadcast the data to the entire network allowing the data to reach all hosts on the network but switches send the data to the specific machine(s) which the data is intended to be sent. This goal is achieved by the use of MAC tables the aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So, considerable number of incoming frames will be flooded at all ports.

MAC Address Table is full and it is unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like broadcasting. Let's see, what are the benefits of the attackers with the MAC Flooding attacks.

4.9.1 What is MAC Flooding Attack?

In computer network jargon, MAC flooding is a technique employed in order to compromise the security of the network switches.

Switches maintain a list (called a CAM Table) that maps individual MAC addresses on the network to the physical ports on the switch.

This enables it to only send data out of the physical port where the recipient computer is located, instead of indiscriminately broadcasting the data out of all ports like a hub.

The advantage of this method is that data is only routed to the network segment containing the computer that the data is specifically destined for.

In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table.

The result of this attack causes the switch to enter a state called "fail open mode", in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation.

A malicious user could then use a packet sniffer (such as Wire shark) running in promiscuous mode to capture sensitive data from other computers (such as unencrypted passwords, e-mail and instant messaging conversations), which would not be accessible were the switch operating normally.

Some more advanced switches, such as those from Nortel, Cisco or Allied Telesis gives you an opportunity to set up protection against this attack with limiting and/or hardwiring some MAC addresses to a dedicated port.

You can also set the policy that if a port gets too many MAC addresses, the default is to shut the port down, and generate a log message.

4.9.2 How to prevent the MAC Flooding Attack?

We can prevent the MAC Flooding attack with various methods. The following are some of these methods.

1) Port Security
2) Authentication with AAA server
3) Security measures to prevent ARP Spoofing or IP Spoofing
4) Implement IEEE 802.1X suites

Port Security

The port security is often used as a counter measure for MAC Flooding attack. The switches are configured to limit the number of MAC addresses that can be learned on ports connected to the end stations. Also a small table of ‘secure’ MAC addresses is maintained with the traditional MAC address table. This table also acts as a subset of the MAC address table. Cisco switches are available with in-built port security system.

Authentication with AAA server

In this method, the discovered MAC addresses are authenticated against an authentication, authorization and accounting server (AAA Server) and these addresses are subsequently filtered

Security measures to prevent ARP spoofing or IP Spoofing.

Security measures to prevent ARP Spoofing or IP Spoofing in some cases may also perform additional MAC address filtering on uncast packets.

Implement IEEE 802.1X suites

Implementing IEEE 802.1X suites will allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address.

These are the methods often used to prevent the MAC Flooding attack.

4.10 Countermeasure

In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

There are several stages involved in combating denial of service attacks. The first is recognizing that you are undergoing an attack. The second is determining what kind of attack is being executed. For example is it a single source attack or are there multiple sources being used? The final stage involves counteracting the attack. Different methods are utilized to combat different types of attacks and knowledge of how the attack is being performed can help in choosing the best solution. Different techniques can also be used depending on whether or not the network has mobile components in it. We will illustrate some techniques that have been suggested to determine the type of attack and some of the countermeasures that can be instigated in response.

4.11 Let us Sum-up

“Sniffer for the detection of lost Mobile phones” paves a way by means of which the lost mobile phones can be recovered. But the process of detection is yet to be developed through the software. There are certain boundary conditions or criteria that have to be qualified for the identification of the lost mobile like the power of the mobile should be good enough, the mobile phone should not be in the shadow region etc., but however this method can be improved by using modern technologies and devices.

In common industry usage, a sniffer (with lower case "s") is a program that monitors and analyzes network traffic, detecting bottlenecks and problems.

Using this information, a network manager can keep traffic flowing efficiently. Sniffer (with a capital "S") is a trademark owned by Network General. The generic term may have originated from Sniffer, which is said to be the first packet capture and decode software that was offered for the purpose of network analysis and troubleshooting.

4.12 Self Assessment Questions

1. What is a Sniffer?

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

2. Discuss about different types of Sniffing.

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

3. What is ARP Spoofing?

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

4. What is ARP poisoning?

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

5. Explain how does DNS work?

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………
……………………………..……………………………………………………

4.13 Model Questions

1. Write the sort note about packet sniffer?
2. What is ARP and how its work?
3. Discuss about the ARP Spoofing detection, prevention and protection.
4. What is MAC Flooding?
5. What is MAC flooding attack?
6. What is the different between sniffer and sniffing?

4.14 References & Further Readings

1. http://www.colasoft.com/resources/sniffer.php
2. https://en.wikipedia.org/wiki/Packet_analyzer
3. https://www.keycdn.com/support/dns-spoofing/
4. http://www.infosecisland.com/blogview/3684-How-to-Detect-a-Mac-Flooding-Attack.html

Answer of Self Assessment Questions (Unit-1)

1. What is hacking?

Hacking is unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system. In another way we can tell Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access**.** Example of Hacking: Using password cracking algorithm to gain access to a system

2. Explain difference between hackers and crackers.

A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge; freely share what they have discovered, and never intentionally damage data.

A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data; deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.

3. What is cybercrime?

Cybercrime, also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone. The Department of Justice divides cybercrime into three categories: crimes in which the computing device is the target, for example, to gain network access; crimes in which the computer is used as a weapon, for example, to launch a denial of service (DoS) attack; and crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally-obtained data.

4. What is security threat?

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack. In these tutorial series, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

5. What is ethical hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.
- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

Answer of Self Assessment Questions (Unit-2)

1. What is footprinting in hacking?

Footprinting is the first and most convenient way that hackers use to gather information about computer systems and the companies they belong to. The purpose of footprinting is to learn as much as you can about a system, its remote access capabilities, its ports and. services, and the aspects of its security.

Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

2. What are the footprinting threats?

Footprinting threats is the attackers gathers valuable system-level information such as account details, OS and other software versions, server names, and db schema details from footprinting techniques.

Threats include:

- Business loss
- Corporate espionage
- Privacy loss
- Social engineering
- System and network attacks
- Information leakage

3. Explain about Open Source Footprinting.

Open Source Footprinting is the easiest and safest way to go about finding information about a company. Information that is available to the public, such as phone numbers, addresses, etc.

Performing who is requests, searching through DNS tables, and scanning certain IP addresses for open ports, are other forms of open source footprinting. Most of this information is fairly easy to get, and getting it is legal, legal is always good.

4. Write about sort note Information Gathering.

Preparation is crucial to any social engineering engagement. Information gathering is the most time-consuming and laborious phase of the attack cycle but is often a major determinant of the success or failure of the engagement. The professional social engineer must be aware of: information-gathering tools freely available online, the many accessible locations online that house valuable pieces of data, the software which can be used to aid in finding and collating the data, and the value or use of seemly insignificant data which can be collected online, over the phone, or in-person.

5. How to undertake information gathering?

Information gathering is an assignment of the research specialist within the organization’s intelligence department. They are the personnel properly trained and equipped to carry out the research tasks in the most efficient manner. The proper handling of data requires methods and procedures unique to the field of information gathering. Research personnel do this task unequivocally thru skills like data sifting, intelligent questioning, and other research skills. Other company personnel can also do their own information gathering on the personal level to improve their job performances and as a self-help tool. Researchers undertake information gathering in order to:

- Broaden the scope of knowledge of the organization
- For the development of particular skills
- To reduce the apprehension caused by the unknown
- For a higher level of understanding of special subjects
- And obviously, for solving problems

Additionally, on the non-professional aspect of the research undertaking, information can also give inspiration and entertainment.

Answer of Self Assessment Questions (Unit-3)

1. What is System Hacking

System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks. This unit explains the main methods of system hacking—password cracking; privilege escalation, spyware installation, and key logging—and the countermeasures IT security professionals can take to fight these attacks. Security expert Lisa Bock also covers Steganography, spyware on a cell phone, and tactics for hiding files and tools.

2. Types of System Hacking

There are of four types of password attack

1. Passive online attack
2. Active online attack
3. Offline attack
4. Non technical attack

Passive Online Attack

In passive online attacks an attacker don't contact with authorizing party for stealing password, in other words he attempts password hacking but without communicating with victim or victim account. Types of passive online attacks include wire sniffing, Man in the middle attack and reply attack.

Active Online Attack

This type of attack can be directly termed as password guessing. An attacker tries number of passwords one by one against victim to crack his/her password.

Offline Attack

Offline password attacks are performed from a location other than the actual computer where the password reside or were used. Offline attacks requires physical access to the computer which stores password file, the attacker copies the password file and then tries to break passwords in his own system. Offline attacks include, dictionary attacks, hybrid attacks, brute force attack, pre-computed hash attacks, syllable attacks, rule based attacks and rainbow attacks.

Non Technical Attack

This type of attacks does not require any technical knowledge hence termed as non-technical attacks. This kind of attacks may include, social engineering, shoulder surfing, keyboard sniffing and dumpster diving.

3. What Is Rootkits?

A rootkit is a type of malicious software that is activated each times your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals, network connections, and the keyboard.

Root kit helps hackers to maintain hidden access to the system using virus , Trojan horse, spyware ect.

4. What is Steganography?

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

Steganography techniques can be applied to images, a video file or an audio file. Typically, however, Steganography is written in characters including hash marking, but its usage within images is also common. At any rate, Steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

5. Why need uses of legal hacking?

Legal hacking is often used by organizations who want to ensure the safety of their computer systems. To this end, hackers may volunteer or be recruited to attempt to break into a system or device as if they were criminals, in order to pinpoint security flaws. Some companies issue public challenges to hackers to break into their systems, offering a reward; more typically, security consultants are contracted to attempt a hack.

Answer of Self Assessment Questions (Unit-4)

1. **What Is Sniffer?**

   A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks, where they sniff packets, they're often called packet sniffers.

2. **Discuss about different types of Sniffing.**

   Sniffing can be either Active or passive in nature.

   Passive Sniffing

   In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

   Active Sniffing

   In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port.

3. **What is ARP Spoofing?**

   ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker’s MAC address with the IP address of a legitimate computer or server on the network. Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

4. **What is ARP poisoning?**
   Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user.

5. **Explain how does DNS work?**
   The Domain Name System (DNS) is a central part of the Internet, providing a way to match names (a website that you are looking for) to numbers (the address for the website). Anything connected to the Internet - laptops, tablets, mobile phones, and websites - has an Internet Protocol (IP) address made up of numbers. Your favorite website might have an IP address like 64.202.189.170, but this is obviously not easy to remember. However a domain name such as bestdomainnameever.com is something people can recognize and remember. DNS syncs up domain names with IP addresses enabling humans to use memorable domain names while computers on the Internet can use IP addresses.

Block

2

HACKING TECHNIQUES

Unit – 1
Trojans, Backdoors, Viruses and Worms

Learning Objectives :

After learning this unit you should be able to

- Know about Trojan and its types.
- Know about how to reverse connect Trojans work.
- Know about different type of Overt and Covert.
- Study about Wrapping and its use.
- Know about What Are the Countermeasure Techniques in Preventing Trojans.
- Study about Trojan-Evading techniques.
- Know about Backdoor and its installation.
- How to Protecting against Trojans and Backdoors.
- Understand Virus Detection Methods.
- Know How a Virus Spreads and Infects the System.

Structure

1.1 Introduction

Trojans and backdoors are two ways a hacker can gain access to a target system. They come in many different varieties, but they all have one thing in common: They must be installed by another program, or the user must be tricked into installing the Trojan or backdoor on their system. Trojans and backdoors are potentially harmful tools in the ethical hacker’s toolkit and should be used judiciously to test the security of a system or network.

Viruses and worms can be just as destructive to systems and networks as Trojans and backdoors. In fact, many viruses carry Trojan executables and can infect a system then create a backdoor for hackers. This chapter will discuss the similarities and differences among Trojans, backdoors, viruses, and worms. All of these types of malicious code or malware are important to ethical hackers because they are commonly used by hackers to attack compromised systems.

1.2 About Trojans

You may know the story of old Greek. Greeks attacked to one of the Troy's cities. After an unsuccessful attack, Greeks made a great plan to win. They made a big horse from wood and left it in front of the Troy's gate. The troy's civilians thought that it was a gift and brought that horse which is called Trojan into the city. In late night, Greek militaries came out of the horse and destroyed the whole city.

The applications works like this story and it is one of the most popular applications which are used for attacking computers. A new game, new free software or an electronic postal card can be a Trojan and it can harm your data or makes a backdoor and your system. Therefore we should be careful about what ever software, an unknown person offers to us.

1.3 List the Different Types of Trojans

Trojans can be created and used to perform different attacks. Some of the most common types of Trojans are:

- **Remote Access Trojans (RATs)** used to gain remote access to a system
- **Data-Sending Trojans** used to find data on a system and deliver data to a hacker
- **Destructive Trojans** used to delete or corrupt files on a system
- **Denial of Service Trojans** used to launch a denial or service attack
- **Proxy Trojans** used to tunnel traffic or launch hacking attacks via other system
- **FTP Trojans** used to create an FTP server in order to copy files onto a system
- **Security software disabler Trojans** used to stop antivirus software

1.4 How Do Reverse-Connecting Trojans Work?

Reverse-connecting Trojans let an attacker access a machine on the internal network from the outside. The hacker can install a simple Trojan program on a system on the internal network, such as the reverse WWW shell server. On a regular basis (usually every 60 seconds), the internal server tries to access the external master system to pick up commands. If the attacker has typed something into the master system, this command is retrieved and executed on the internal system. Reverse WWW shell uses standard HTTP. It's dangerous because it's difficult to detect—it looks like a client is browsing the Web from the internal network.

1.5 What Are the Indications of a Trojan Attack?

Unusual system behavior is usually an indication of a Trojan attack. Actions such as programs starting and running without the user's initiation; CD-ROM drawers opening or closing; wallpaper, background, or screen saver settings changing by themselves; the screen display flipping upside down; and a browser program opening strange or unexpected websites are all indications of a Trojan attack. Any action that is suspicious or not initiated by the user can be an indication of a Trojan attack.

1.6 What Is Meant by Overt and Covert Channels?

An overt channel is the normal and a legitimate way that programs communicate within a computer system or network. A covert channel uses programs or communications paths in ways that were not intended.

rojans can use covert channels to communicate. Some client Trojans use covert channels to send instructions to the server component on the compromised system. This sometimes makes Trojan communication difficult to decipher and understand.

Covert channels rely on a technique called tunneling, which lets one protocol be carried over another protocol. Internet Control Message Protocol (ICMP) tunneling is a method of using ICMP echo-request and echo-reply to carry any payload an attacker may wish to use, in an attempt to stealthily access or control a compromised system.

1.7 What is Meant by “Wrapping”?

Wrappers are software packages that can be used to deliver a Trojan. The wrapper binds a legitimate file to the Trojan file. Both the legitimate software and the Trojan are combined into a single executable file and installed when the program is run.

Generally, games or other animated installations are used as wrappers because they entertain the user while the Trojan in being installed. This way, the user doesn’t notice the slower processing that occurs while the Trojan is being installed on the system—the user only sees the legitimate application being installed.

1.8 Trojan Construction Kit and Trojan Makers

Several Trojan-generator tools enable hackers to create their own Trojans. Such toolkits help hackers construct Trojans that can be customized. These tools can be dangerous and can backfire if not executed properly. New Trojans created by hackers usually have the added benefit of passing undetected through virus-scanning and Trojan-scanning tools because they don’t match any know signatures.

Some of the Trojan kits available in the wild are Senna Spy Generator, the Trojan Horse Construction Kit v2.0, Progenic Mail Trojan Construction Kit, and Pandora’s Box.

1.9 What are the Countermeasure Techniques in Preventing Trojans?

Most commercial antivirus program has anti-Trojan capabilities as well as spyware detection and removal functionality. These tools can automatically scan hard drives on startup to detect backdoor and Trojan programs before they can cause damage. Once a system is infected, it’s more difficult to clean, but you can do so with commercially available tools.

It’s important to use commercial applications to clean a system instead of freeware tools, because many freeware removal tools can further infect the system. In addition, port-monitoring tools can identify ports that have been opened or files that have changed.

1.10 Understand Trojan-Evading Techniques

The key to preventing Trojans and backdoors from being installed on a system is to educate users not to install applications downloaded from the Internet or open e-mail attachments from parties they don't know. Many systems administrators don't give users the system permissions necessary to install programs on their system for that very reason.

1.11 Backdoors

As you can guess, a backdoor is an unusual way which an attacker can use it to get into the system. Normal users use login boxes and password protected ways to use the system. Even system administrator may add some security features to this system to make it more protect, but the attacker can easily use installed backdoor to get into system without any password or authenticating.

Most of attackers like to protect their backdoor on victim system. They do not like that some another attacker use the same vulnerability to get into victim system and change their configurations. That is why an expert attacker after getting access protects vulnerability which is used for getting access to the system. Although the system could be in a company and somebody else use that for working, but attacker is the owner of system and can install any application or use stored infractions which is exists on that system.

Sometimes attacker makes a very secure backdoor even much safer than normal way to get into system. A normal user may use only one password for using the system but a backdoor may needs many authentications or SSH layer to let attacker use the system. Usually it is harder to get into the victim system from installed backdoor in compare with normal logging in.

1.11.1 Backdoor Installation Methods

At the most of times, after getting the control of victim system by an attacker, he installs a backdoor on victim system to keep his access in future. It is as easy as running a command on victim machine. But there are also some easier ways to install a backdoor. Most popular way is using Trojans. With sending a greeting card or a free game a backdoor can install on victim system and let attacker to control system.

Another way to install a backdoor is using ActiveX. Whenever a user visit a website, embedded ActiveX could run on system. Most of websites show a message about running ActiveX for voice chat, downloading applications or verifying the user. But the truth is they can easily install anything on user machine with only running ActiveX for once. There are several kinds of applications which are used to improve the abilities of websites, such as Java applets but Java applets have a limited access to the system but with ActiveX you can have a full control of machine which is running given ActiveX.

Microsoft made a security policy for protecting the system against this trick. Developers of ActiveX should sign their published ActiveX and the signature should be valid. If any user wants to run an ActiveX without a valid signature, the browser shows the alert about the security problems which may happen after running ActiveX. Unfortunately most of the users do not care to this alert and run any ActiveX which is embedded to browsing web page. It could be very dangerous to run any ActiveX without a valid signature from any unknown source.

1.12 Undetectable Control

Attackers use different mechanisms to make their backdoors undetectable and untraceable. If system administrator sees an abnormal behavior in system, he can understand that it may because of some virus or backdoor, therefore he will find the backdoor and attacker cannot access to the system anymore. If he can trace the destination of packets he also can find the attacker. That is why, expert attackers tries to hide their communication and backdoor tasks. There are several ways to do hiding which we shortly describe some of them.

1.12.1 Cryptography

In many situations attackers use cryptography to encrypt transferred data between victim system and attacker. They use different methods of encryption to make commands and transfer data between victim machine and attacker’s system transparent for system administrator during monitoring the network traffics and behaviors.

In most cases, there is no need to use a very powerful encryption technique, because attacker only use encryption algorithm for hiding the data during transmission. If attacker uses a very powerful technique like RSA, it may cause to increase the CPU usage of victim machine and makes transfer time longer.

In these cases, attackers usually use AES symmetric encryption methods. Serpent is one of popular methods which are used by backdoors. Although Serpent is very strong, still it can be broken with XSL attack but it is much stronger than other AES methods and attackers use that because they believe XSL could be an expensive attack for breaking an effective algorithm like Serpent.

SSH or VPN is another methods which attackers use for encrypting the traffic. Delivering packets using VPN or SSH is undetectable by firewalls and administrators and attacker can use standard services which are already installed on the network for encrypting the backdoor control packets.

1.12.2 Root Kits

Although backdoors can be very dangerous but because they run like a normal application, they can be easily findable. Taking a look in system task list, services or registry may show the backdoor. Expert attacker use more powerful backdoors called Root kits. Root kits work as a part of operating system and do not let the users to see real tasks or services. Operating system will be under full control of attacker and he can hide everything he wants in system. Root kits have two main groups with different architectures, Classic Root kits and Kernel Root Kits.

1.12.2.1 Classic Root Kits

Classic Root kits focused on UNIX based operating systems, like Linux and SunOS. Usually, in these Root kits attackers replace /bin/login file with another version which lets attacker to use his own user name and password to get into system. In this situation, if system administrator changes the root password or limit the access of root user to log into system remotely, attacker can logging in with his saved password. It can also use for saving the passwords of other users in attacker's database.

Sometimes, Classic Root kits hide more things. For example they change ifconfig command to hide network card flags from administrator eyes. If they do not change the classic ifconfig file, during sniffing of attacker, administrator can see the PROMISC flag and he can understand that a sniffer program is running.

Other UNIX commands which usually changes by classic root kits for hiding are: du, find, ls, netstat and ps.

1.12.2.2 Kernel Root Kits

Kernel root kits replace themselves with the kernel of operating system. In this case you cannot trust anything in your system. Whenever an application wants to run on system, operating system reports the results which attacker wants. With Kernel root kits, all processes, tasks, network configurations, port numbers, content of files and any other things that you can believe can show themselves in another way and attacker can force operating system to lie about whatever the user or administrator wants to know.

With Kernel Root kits detection and tracing the backdoors is very hard and they can even stop antivirus or system monitors. It is the most powerful way of using backdoors.

1.12.3 Using Different Protocols and Port Numbers

Attacker may use a random port number instead of standard ports for running a service and victim machine. Unexpected running of SSH service on port 22 which is always monitored by administrator may cause to trace the attack by system administrator. That is why most of attackers use another port numbers to make it harder to detect the running service of the attacker.

Some of the backdoors works more professionally. They change port numbers or using protocol during attack. For example a good backdoor can change the connection protocol from TCP to UDP and even ICMP. If system administrator blocks a port or protocol on gateway, backdoor can switch to another protocol or port number and let attacker to reconnect into the system.

1.12.4 Reverse Control

Most of firewalls or administrators block some connections to outside. They may just let local user to browse websites and not more. Even it can be harder with a NAT system and giving private IP addresses, it is impossible for attacker to connect to a system which is exists on a private LAN.

Backdoors can use another strategy in these situations. Attacker runs his own server on a specific IP address and in given time backdoor tries to connect to the server inside the firewall and ask from attacker's server for commands which should be run on victim machine. Backdoor can also use standard HTTP protocol to connect to attacker server and the server will give the command in HTTP format. It looks like a web browsing for firewall or administrator. This strategy can also work from behind of huge firewall system and it really hard to detect.

The only way which may case to detect these connections is to monitoring the number of requests which sends from a system to a special IP address. Sometimes attackers use chaining many servers on different IP addresses to connect randomly by victim system. This method is even harder to protect.

1.12.5 Backdoor Timing

There are many services which are used for updating the systems during idle time. Cron command on UNIX machines or Schedule tasks on windows machines are samples of these services.

Attackers can use these services to use backdoors in given times. For example, using Cron table of an UNIX machine, a back door can start to work in 4 O'clock of morning and let attacker to connect to system, the time which there is no administrator in the office.

1.13 Protecting Against Trojans and Backdoors

Now, this is a time to know how we can protect our systems from Trojans and Backdoors and how we can defend these kinds of attacks.

Several ways could be suitable for this defending. We discuss briefly about these methods.

1.13.1 Antivirus

Running an update antivirus on all client systems with Real-time protection can be a very good way against popular Backdoors and Trojans. Antivirus can easily find Backdoors or Trojans before running them on the system, but the important thing is to keep any antivirus update. If an attacker use a new backdoor or Trojan which is not exists in antivirus database, it can run on victim machine easily and without any warning.

1.13.2 Signatures

Before using software you should be in sure about the application which you want to run. Many of developers use MD5 algorithm to make a hash string from their final application. After downloading any application and before running you can calculate the hash string of executable application and compare it with given hash string which is exists on developer’s website. If hash strings were same you can understand nobody changes executable file and you can execute it. But before execution you should have trust to developer.

There are many third-party companies, like verisign, which they give some keys for signing applications to the developers. If any application had this signature you can be in sure that the company is trusted and application is valid and safe for execution. If you do not know all of trusted software companies, you can trust to your trusted third-party company which guarantees the software company.

1.13.3 Training

It is very important to train the users about security problems which may happens in whole system. In most of times attackers use social engineering to deceit users. Users have to know what they should do and what they should not. If any user do something wrong, whole the corporation may become reachable for an attacker.

1.14 Case Study

In this unit, we use Back Orifice 2000 as a sample to show how a backdoor can work on a system. Back Orifice 2000 (also called Bo2k) is one of oldest and most popular backdoors which is widely used for training issues on Windows machines.

Bo2k is open source and it can be reachable from Source forge website.

1.14.1 Back Orifice and its History

Back Orifice is written by Dildog on of the members of ‘Cult of the dead cow’ group. It introduced in DefCon 7 conference in 1999.

After a while they made a more powerful version of Back Orifice in the name of Back Orifice 2000 or Bo2k as an open source project. They called this system a remote administration system but because it can be installed on client machine without any prompt, many of peoples used this application for bad reasons. That is why whenever you want to execute a Bo2k application on your system, your antivirus shows an alert. Bo2k is a tool which you can use it in both good and bad tasks. Many of companies use Bo2k as a cheap solution for managing their systems remotely.

1.14.2 Abilities of BO2K

Bo2k is very small but very complete in abilities. The client code of Bo2k is about 100 KB and it can be installed very easily even with old modems and limited bandwidth. You can also change the size of client with adding more features to it to have more control on remote machine. It can use different kinds of authentication, cryptography algorithms and protocols. In recent versions you can also run it as a reverse client or you can add kernel root kit features to hide the tasks. You can Improve the Bo2k abilities with adding some plug-ins to both client and server part of this application. Even you can develop your own plug-ins to work under Bo2k system.

1.14.3 Making A Trojan Using BO2K

You can use many binder applications to bind Bo2k client to any other program. After running the result program, Bo2k will start to work and user cannot understand that bo2k is running in parallel. Elite Wrap, Saran Wrap and Silk Rope are some sample programs which is widely used for binding the Bo2k client to other applications.

1.15 Viruses and Worms

Viruses and worms can be used to infect a system and modify a system to allow a hacker to gain access. Many viruses and worms carry Trojans and backdoors. In this way a virus or worm is a carrier and allows malicious code such as Trojans and backdoors to be transferred from system to system much in the way that contact between people allows germs to spread.

1.15.1 Understand the Types of Viruses

Viruses are classified according to two factors: what they infect and how they infect. A virus can infect the following components of a system:

- System sectors
- Files
- Macros (such as Microsoft Word macros)
- Companion files (supporting system files like DLL and INI files)
- Disk clusters
- Batch files (BAT files)
- Source code

1.15.2 How a Virus Spreads and Infects the System

A virus infects through interaction with an outside system. Viruses are categorized according to their infection technique, as follows:

- **Polymorphic viruses:** These viruses encrypt the code in a different way with each infection and can change to different forms to try to evade detection.
- **Stealth viruses:** These hide the normal virus characteristics, such as modifying the original time and date stamp of the file so as to prevent the virus from being noticed as a new file on the system.
- **Fast and slow infectors:** These can evade detection by infecting very quickly or very slowly.
- **Sparse infectors:** These viruses infect only a few systems or applications.
- **Armored viruses:** These are encrypted to prevent detection.
- **Multipartite viruses:** These advanced viruses create multiple infections.
- **Cavity (space-filler) viruses:** These viruses attach to empty areas of files.

- **Tunneling viruses:** These are sent via a different protocol or encrypted to prevent detection or allow it to pass through a firewall.
- **Camouflage viruses:** These viruses appear to be another program.
- **NTFS and Active Directory viruses:** These specifically attack the NT file system or Active Directory on Windows systems.

1.16 Understand Antivirus Evasion Techniques

An attacker can write a custom script or virus that won’t be detected by antivirus programs. Virus detection and removal is based on a signature of the program. Until the virus is detected and antivirus companies have a chance to update virus definitions, the virus goes undetected. This allows an attacker to evade antivirus detection and removal for a period of time.

1.17 Understand Virus Detection Methods

The following techniques are used to detect viruses:

- Scanning
- Integrity checking with checksums
- Interception based on a virus signature

The process of virus detection and removal is as follows:

1. Detect the attack as a virus. Not all anomalous behavior can be attributed to a virus.
2. Trace processes using utilities such as handle.exe, listdlls.exe, fport.exe, netstat.exe, and pslist.exe, and map commonalities between affected systems.
3. Detect the virus payload by looking for altered, replaced, or deleted files. New files, changed file attributes, or shared library files should be checked.
4. Acquire the infection vector and isolate it. Then, update your antivirus definitions and rescan all systems.
5. A test virus can be created by typing the following code in Notepad and saving the file as EICAR.COM. Your antivirus program should respond when you attempt to open, run, or copy it.X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

1.18 What’s the difference between a Virus, Worm, and Trojan horse?

Very commonly we hear about these three types of computer problems and although the terms get used interchangeably, each is vastly different. They are all various types of malicious software but differ in their affects and how they spread. Being informed on the cause and effects will better prepare you in keeping your computer safe.

Virus

A computer Virus is embedded code or attached to a file where it infects the computer when the file is executed. Viruses are spread through users transferring files, usually unknowingly, through e-mail or file sharing. Even if you download the infected file the

Virus cannot act until the malicious file is executed, which means it won’t harm your computer until you run it. Note that the only way a Virus can spread is through user involvement; it cannot execute or transfer itself independently. It can infect other files on your machine however, it cannot replicate itself.

Worm

A computer Worm is similar to a Virus by design and is considered a sub-class of a Virus. The difference is that a Worm gains access to your systems transport features and is able to travel unaided by the user. A Worm also has the added ability to replicate itself, so instead of sending out a single Worm it can send out hundreds and thousands of copies of itself creating a vicious cycle. Because of its ability to reproduce it can end up using tons of system memory and bandwidth causing servers and individual systems to crash. Unlike a Virus, it cannot infect other files on your computer.

Trojan horse (aka Adware/Spyware)

Typically a Trojan will appear to be a useful and legitimate application from a legitimate source and could possibly promise to clean your system of viruses or search your registry for spyware. When you execute a Trojan the results could vary from as little as changing your desktop wallpaper, creating annoying pop-ups, or to the extreme of deleting and destroying files and programs. Trojans are also known for creating backdoors to your system that allows malicious users to gain access to files and information. Unlike a Virus or Worm, a Trojan cannot infect other files or replicate.

1.19 Let Us Sum Up

This unit is written to have an overview on Trojans and Backdoors. It is good to know how Backdoors and Trojans work and how they can harm our systems with studying their behaviors we can design more secure systems and we can protect our information against these attacks.

1.20 References

a. Counter Hack, Ed Skoudis, ISBN: 0130332739

b. Maximum Security, Anonymous, ISBN: 0672318717

c. Firewalls and Backdoors, Bob Rudis and Phil Kostenbader, Security Focus d. Bo2k official website, http://www.bo2k.com, Last visit: October 24, 2006

e. Serpent (Cipher), Wikipedia, http://en.wikipedia.org/wiki/Serpent_(cipher), Last visit: October 24, 2006

Frequently Asked Questions

Where does the name "Trojan horse" come from?

It originates from the Greek story of the Trojan War in which the Greeks gave a wooden horse to their foes the Trojans as a peace offering. Once the gift was brought inside the city walls, the Greek troops from the hollow belly of the horse snuck out and opened the city gates allowing their fellow troops to invade and capture Troy. This is similar to how users would accept a Trojan horse thinking it is something good, but once inside it unleashes malicious code which attacks your machine.

I hear a lot about spyware, what is it? How is it different?

Spyware is a Trojan horse distributed to your machine through pop-ups or spam messages that log information such as sites you visit, terms you search, or more extreme things like credit card numbers and passwords. Through the backdoor that Trojan's create, it sends this information to malicious users who can use it for annoying things like pop-ups and advertisements to very severe things like identity theft.

How do you know if your system is infected?

The only sure way of knowing is by running an antivirus or antispyware scan of your system with the most up-to-date definitions. However there are symptoms you can look for that may indicate your system is infected:

- Your system suddenly runs much slower
- Your system begins crashing or freezing abruptly
- You start receiving lots of pop-ups or weird error messages
- You see shortcuts to programs that you don't remember installing
- Your Internet Explorer settings change without your knowledge ie. Your home page is different.

What should I do if I think my system is infected?

If you think your system is infected the first thing to do is disconnect your network cable from the back of your machine or from the wall. This will ensure that if the infection is a Worm it will not be able to transfer to any other machine, and if it's a Trojan, no backdoors will be open to malicious users. Next you should contact a member of AHS Computing to take a further investigation into the problem. If no support is available you should run an antivirus/antispyware scan on your machine using the most up-to-date definitions. Since your machine is not connected to the internet you will have to download the newest definitions from another machine and transfer them to the suspected machine via memory stick or CD. If an infection is found through a scan, let the software try to remove it (if it can find an infection usually it will be able to remove it). You can also search your findings in Google to see if there are any removal tools. Quite often Symantec http://www.symantec.com will have a useful tool available.

How can I prevent my system from being infected?

Make sure your Windows operating system is up to date. Be sure to install all high priority updates and any security updates in the software section from the Microsoft site http://windowsupdate.microsoft.com. These will update security features and fix vulnerabilities that can be exploited by malicious users and software. Be sure to run an up-to-date and trusted antivirus program. Antivirus programs will continually update with new definitions as new viruses are found. This will be your best bet of preventing infections. Make sure to set your preferences so the programs will auto- update and auto-protect. This way it will constantly check new programs being installed, files transferring from the internet, and e-mails being received or sent. You should only ever be running one antivirus program, running more than one could cause major problems. With the uproar of spyware it is recommended to have a separate antispyware program; a lot of these can be downloaded for free via the web. Maintain your antispyware software the same as your antivirus software as they both operate similarly. Be sure to run scans periodically after updating in case the new definitions find files the old definitions missed.

Lastly, surf smart. When you’re on the World Wide Web you are bombarded with links, files, advertising, and many other “free” services. Be suspicious of all content, whether it be from a web site you’re visiting or a best friend forwarding you a program or joke. You could potentially be downloading an infected file. Keep in mind a simple Google search of any suspicious file or program name can reveal much useful information and possible prevention of an infection.

Unit-2
Session Hijacking

Learning Objectives:

After learning this unit you should be able to

- Know about Session Hijacking.
- Know about how sessions can be tracked.
- Understand Different Types of Session Hijacking.
- Know about Session Hijacking Cheat Sheet.
- Study about Session puzzle attacks.
- Know about Understood Form Of Internet Data Theft And How To Avoid It.
- Study about Methods to Hijack Sessions.
- Know about Session Hijacking Involves.
- How to Protecting against Preventing an Attack**.**
- Know about UDP Session Hijacking.

Structure

2.8 What Session Hijacking Involves

- 2.8.1 Active and Passive Attacks
- 2.8.2 Compromising Session Tokens

2.9 Tools Employed by Attackers

2.10 Preventing an Attack

- 2.10.1 Encryption
- 2.10.2 Connections
- 2.10.3 Anti-Virus Software
- 2.10.4 Employee Education

2.11 Countermeasures for Session Hijacking

2.12 Hijacking Application Levels

2.1 Introduction

Web applications communicate using HTTP protocol. HTTP is stateless, which means there is no support at the protocol level to identify the state of a particular request. In other words, web servers don’t have any mechanism to know whether the request is coming from a new client from a client which is already communicating with it. So from the server perspective, every request it receives is a new request. For instance, let us say a client logged into his Facebook account by sending his credentials. Now if he wishes to see his messages, he has to send his credential information again, because the server doesn’t normally know that he was already authenticated in the previous request. This is something that developers have to do themselves. This is called ‘Session Tracking’.

2.2 How Can Sessions Be Tracked?

Sessions are tracked by developers primarily through the use of session identifiers (SIDs). Once the user is successfully authenticated, a session ID is created by the server and maintained by the server. From there on, for every request this value is checked to track the user. In other words, session IDs are used as an authentication token so that user does not have to re-enter the credential information with every request.

Based on how this SID this sent and received, there are 3 mechanisms to track sessions.

Cookies:

The SID is created and maintained in the server and sent to the user through cookies. A cookie is stored in the user’s hard disk and goes with each request. The server verifies the same before executing the request. This is the most widely used mechanism and we are going to talk more about this in the below sections.

URL Rewriting:

In this the SID value actually goes in the URL of each request. This kind of session tracking is difficult, as we need to keep track of the parameter as a chain link until the conversation completes.

Hidden Fields:

Hidden fields are elements which are not directly visible to the user. They can be viewed by looking at the page source. Interestingly, they can also be used for session management, as SID values can be stored in hidden fields and can be sent to the server with each request. This sort of mechanism is rarely used these days.

2.3 What is Session Hijacking?

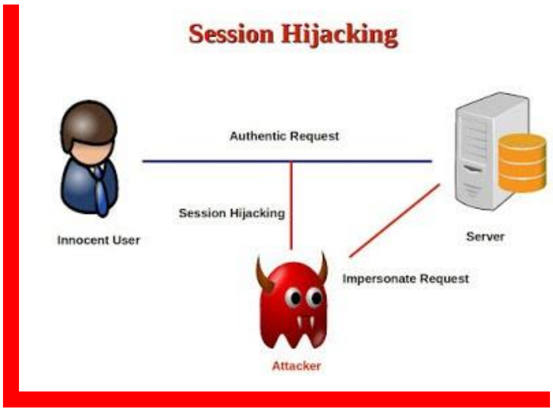
Let’s discuss them in common term’s, Session Hijacking by the name only it suggests that we are hacking someone’s active session and trying to exploit it by taking the unauthorized access over their computer system or Network. So Session Hijacking is the exploitation of valid computer or network session. Sometimes technical guys also call this HTTP cookie theft or more correctly Magic Cookie Hack. Now you guys surely be thinking what Magic Cookie is.

Magic cookie is simply a cookie that is used to authenticate the user on remote server or simply computer. In general, cookies are used to maintain the sessions on the websites and store the remote address of the website. So in Session Hijacking what Hacker does is that he tries to steal the Magic cookies of the active session that’s why it’s called HTTP cookie Theft. Nowadays several websites has started using HTTPS cookies simply called encrypted cookies.

Session Hijacking is the process of taking over a existing active session. One of the main reasons for hijacking the session is to bypass the authentication process and gain the access to the machine. Since the session is already active so there is no need of re-authenticating and the hacker can easily access the resources and sensitive information like passwords, bank details and much more.

2.4 Session Hijacking Cheat Sheet

When a user authenticates himself in a web server, the session is maintained with a HTTP cookie. And the cookie is placed in the user's computer. Session Hijacking is an attack in which an attacker exploits a valid session of a user and gets unauthorized access to the web server for malicious purposes.



There are couple of methods using which a Session Hijacking is performed:

Let us now take a look at different ways or scenarios in which active sessions can be hijacked.

2.4.1 Session Sidejacking

In this attack, the attacker mainly does packet sniffing and reads the network traffic between the victim's machine and the server to steal the session cookie.

It normally follows these steps:

- The victim logs in to the server and starts communicating.
- The attacker uses a packet sniffer and reads the network traffic between them.
- The attacker steals the session cookie.
- The attacker uses the same session cookie to log in to the server and impersonate

the victim.

If the application does not use SSL and transports the data in plain text, then anyone within the same network can grab the cookie values just by sniffing the traffic using tools such as Wireshark. There are a few cases worth mentioning here:

SSL only for login page: Of course if there is no SSL then the credentials too would be gone (forget about cookies!), but there are some developers who use SSL for the login page alone, assuming that the credentials are transported safely. But once the user is authenticated, it is the cookies (that go with each request) that identify him. All the requests that are done after logging in contain cookies, and if they are not protected with SSL, the session can be easily hijacked. Thus the password may not be stolen, but the session can be hijacked.

Single URL is enough to hijack a user: There are several cases where the application uses HTTP to fetch image or JS files that belong to same domain. The problem is when you send a request to a domain in which you are already signed in, the cookies would automatically go. That is how the cookies work. So in simple words, even if there is a single link which goes to the server without HTTPS, the cookies would go along with it and can be grabbed by an attacker who is sniffing the network.

2.4.2 Session Fixation

In this attack, an attacker sets a user's session id to one known to him. And, when the user falls in trap and logs in to the server, the attacker impersonates him.

It normally follows these steps:

- An attacker uses social engineering and sends the victim a link containing the predefined session id.
- The victim clicks on the link and a log in screen pops up. When he logs on to the server, the server assigns that session id to the victim (because of vulnerabilities in the web application)
- But, this session id is known to the attacker. So, the attacker now logs in to the server impersonating the victim.

Session fixation is an attack where the attacker fixes the session in advance and just waits for the user to login in order to hijack it. This is very much applicable to the SIDs in the URL scenario. If the application associates a user with an incoming SID without checking if it is generated by the server, then this attack is possible.

An attacker logs into the site www.vulnerablesite.com. The server sets a cookie value and returns it to him, say Set-Cookie:

SID=adfajkdfjer23411sdfadf

The attacker now sends a link to the victim,

http://www.vulnerablesite.com/test.php?SID= adfajkdfjer23411sdfadf

The victim logs on and the server now assigns the SID value to him. (Why? Due to bad coding, the server does not check if it is generated by itself and tags it with the users).

The attacker, who already knows the SID value he used, can now just use the same and access the victim's account.

2.4.3 Generating Cookies Before Authentication

Cookies are supposed to be generated (or at least changed) after successful authentication. If the same cookie which is generated before authentication is used after authentication, then session hijacking is possible, as explained here with a simple example. This is mostly exploitable in a public café or shared computers scenario.

An attacker visits the site www.vulnerablesite.com. The server sets a cookie value and returns it to him, say Set-Cookie: SID=randomqrrqwer234234234

The attacker notes down this value and leaves the system, keeping the page open.

The victim now logs into the same site. Cookie value does not change after authentication.

The attacker, who already has the cookie value, can access the victim's account.

2.4.4 Predictable Session Ids

By analyzing the pattern of session IDs, an attacker can predict the session ID of a logged in user and thus hijack his account. For example, consider the below session cookie set by an application.

Set-Cookie: sessionid=dG9tOm1hbmFnZXI=

Although this seems to be random at first look, it is not actually! Base 64 decoding of the above value gives the below data.

Base64 Decode [dG9tOm1hbmFnZXI=] = tom:manager

Thus an attacker can study this pattern and construct a valid cookie, for instance something like Base64 Decode [admin:admin]. Similarly, if the session IDs are not random enough, an attacker can try to brute force them to gain access to the application.

2.4.4 Using Cross Site Scripting Vulnerability

In this attack, the attacker exploits a victim and inject client side scripts into web pages viewed by the victim to do malicious activities like steal sensitive information etc.

It normally follows these steps:

- The attacker writes a script such that when a user is already logged in to the server and clicks on the link of the script, the session information is transferred to the attacker.
- The attacker uses some social engineering and sends the link to the victim.
- The victim logs in to the server and clicks on the link.

- Session information placed in the cookie is transferred to the attacker.
- The attacker now exploits the session information to log in to the server impersonating the victim.

Hear is aware of what an XSS attack is about. So we are going to take a look at how XSS can be used to steal SID or cookie value. In simple words, XSS allows an attacker to execute scripts (such as JavaScript) on an end user's browser. Hence an attacker just needs to write a script that can access the cookie value and send it to a server he owns. The below script does the same thing. It hits the attacker's site with the cookie value. Accessing the cookie on the client side is possible through use of document.cookie.

2.4.5 Session Puzzle Attacks

This vulnerability occurs when an application uses the same session variable for more than one purpose. Here an attacker tries to access the pages in a particular order so that the session variable is set in one context and then used in another. This is best explained in the below scenario.

An attacker visits the application and clicks on the 'Forgot Password' link.

Now he enters some other user's ID (say admin) and clicks submit.

After this the attacker just requests some internal page such as viewprofile.jsp and he logs in as admin.

This worked because the application wrongly sets the session attribute when the forgot password process is initiated. The attacker takes advantage of this and exploits it by requesting it in a sequence. These types of vulnerabilities are more difficult to identify through normal testing, and hence source code reviews are the best way to look out for such vulnerabilities.

2.4.6 Improper Logout Implementation

When a user clicks on the logout button, the application is supposed to destroy all the session variables that are handled on the server side. But instead, some developers just delete the cookies from the client side using client side code. This seems to work fine when you browse normally, because once the cookies are removed from the machine it will redirect to login page, but the session on the server is active indefinitely. This means that an attacker who can grab this value can still access the application. This scenario increases the time period an attacker can launch attacks over valid sessions.

2.4.7 Lack of Session Expiration Mechanism

All applications should track idle sessions and automatically redirect the user to a login page upon session timeout. Failure to do so would not only increase the time period an attacker can launch attacks, but also grant access to the application if he has physical access to that machine. Once again, this session expiration must be done at the server level and not just at the client level.

2.4.8 Using Malware

Here, the attacker infects the victim's computer with a malware and then steals the session cookie.

Just to give an example:

- The victim installs a software from an untrusted source.
- The victim's computer is infected with a Browser Hijacker.
- The malware changes the security settings of the attacker's browser.
- When the victim logs in to the server, the malware steals the session cookie and transfers it to the attacker.
- The attacker can now log in to the server impersonating the victim.

2.5 Different Types of Session Hijacking

Session Hijacking involves two types of attacks:

1. Active attack

2. Passive attack

In Passive attack, the hacker Hijacks a session, but just sits back and watches and records all the traffic that is being sent from the computer or received by the computer. This is useful for finding the sensitive information like username passwords of websites, windows and much more.

In Active attack, hacker finds the active session and takes over it. This is done by forcing one of the parties' offline which is usually achieved by DDOS attack (Distributed Denial of service attack). Now the hacker takes control over the active session and executes the commands on the system that either give him the sensitive information such as passwords or allow him to login at later time.

There are also some hybrid attacks, where the attacker watches a session for while and then becomes active by taking it over. Another way is to watch the session and periodically inject data into the active session without actually taking it over.

2.6 Methods to Hijack Sessions

There are four main methods used to perpetrate a session hijack. These are:

Session fixation, where the attacker sets a user's session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in.

Session sidejacking, where the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie. Many web sites use SSL encryption for login pages to prevent attackers from seeing the password, but do not use encryption for the rest of the site once authenticated. This allows attackers that can read the network traffic to intercept all the data that is submitted to the server or web pages viewed by the client. Since this data includes the session cookie, it allows him to impersonate the victim, even if the password itself is not compromised. Unsecured Wi-Fi hotspots are particularly vulnerable, as anyone sharing the network will generally be able to read most of the web traffic between other nodes and the access point.

Alternatively, an attacker with physical access can simply attempt to steal the session key by, for example, obtaining the file or memory contents of the appropriate part of either the user’s computer or the server.

Cross-site scripting, where the attacker tricks the user’s computer into running code which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie or perform other operations.

2.7 Understood form of Internet Data Theft and How to Avoid it.

Session hijacking involves the theft of another’s internet session, thereby allowing the attacker to impersonate the original user. Falling victim to a session hijacking attack could prove catastrophic because it may enable the attacker to perform any task that you, the victim, would be able to perform.

In this article I explain what session hijacking entails, and detail some of the more favored methods for compromising a session token. I also discuss three of the tools most commonly used to perform such attacks and outline some prevention measures that you might implement, in either your home or place of business, in order to avoid becoming a victim of such an attack.

2.8 What Session Hijacking Involves

At its most basic level, session hijacking involves the taking over of a victim’s active internet session by covertly obtaining the victim’s session token. Once the victim’s session token has been accessed, the attacker can masquerade as the victim, and perform any tasks that the victim is authorized to perform.

The session token required to perform a hijack is normally stored within an internet cookie or URL. For most communications, authentication procedures are carried out at start up. The process of session hijacking takes advantage of this practice by intruding into the web session in real time. The ability to detect such an intrusion is dependent on both the technical knowledge of the victim and the specific nature of the attack.

2.8.1 Active and Passive Attacks

There are two broad forms of session hijack attacks which are known respectively as an active and a passive attack. An active attack involves the identification, attack, and successful takeover of an active internet session. It is regarded as the more advanced form of attack, due to the higher level of skill which it entails.

A passive attack involves the attacker monitoring the traffic being sent across the victim’s network and, as such, is nothing more than an advanced form of network sniffing. The attacker gathers information, such as login information, and then uses that information to authenticate in a separate session.

2.8.2 Compromising Session Tokens

Common methods employed in stealing a valid session token are session sniffing; client-side attacks; man-in-the-middle attacks; and session prediction. Each of these is discussed below.

Session sniffing is the easiest approach to capturing a valid session token. It involves the monitoring of network traffic being sent between the victim's terminal and the server that the victim is connecting to Monitoring this traffic allows the attacker to easily gather a wide range of sensitive data, including information regarding the session token as well as login details to various websites and services.

Another common means of gaining access to a session token, and other personal data is for the attacker to use a client-side attack. One of the most common client-side-attacks involves infecting the intended victim's terminal with a malware application, such as a Trojan or Virus. This application then gives the attacker access to the target's data and allows the copying, editing and deletion of any file on the target's computer. The cross-site script (XSS) attack is another example of a client-side attack. An XSS attack occurs when an attacker sends a URL containing malicious Javascript code to a potential victim. If the target navigates to the link, the malicious Javascript code will be executed, resulting in a copy of the target's session token being sent to the attacker.

A man-in-the-middle attack (MITM) occurs when the attacker intercepts communications between two systems, and then assumes the role of a proxy between both parties. The attacker does this by splitting the connection into two new links: one between the server and the attacker, and the other between the attacker and the victim. By acting as a proxy for all communications between the two parties, the attacker is able to read and modify the data that is sent between the victim and the server, including the session token.

A session prediction attack, which is, in my opinion, the most amateurish of attack methods, involves the attacker trying to guess the active session's token. The attacker does this by analyzing both the means by which the session token is generated and the algorithms that are used to protect it. Once an attacker understands this process, they are able to predict a valid session token value and gain access to that session. Some simple, highly vulnerable session tokens may comprise predictable information such as timestamps and usernames. Employing such basic session token assignment schemes is extremely dangerous and should be avoided!

2.9 Tools Employed by Attackers

There are a variety of applications that can be used to sniff networks and hijack active sessions. Three of the most commonly employed applications are as follows.

Juggernaut is a network sniffer that was developed for Linux operating systems. Juggernaut allows the user to monitor all network traffic, or alternatively, to scan network traffic for specific keywords, such as usernames, website addresses or passwords. Juggernaut also allows the user to view information regarding all active network sessions, and provides the user with the option of hijacking any of these sessions. Juggernaut is a free-to-use application and installation guides are available on a variety of websites; a basic Google search should be sufficient to find one of these guides.

A second application is T-Sight, which is a network scanning and session hijacking tool designed for use within the Microsoft Windows environment. T-Sight allows the user to monitor all data being passed over a network. When a session id has been captured, a single button click allows the attacker to hijack the session. In an attempt to prevent T-Sight being used for illegal purposes, Engarde, the company that produces and distributes T-Sight, only licenses the software to pre-determined IP addresses.

Finally, Ettercap is a free and open source network security tool that allows the user to perform man-in-the middle attacks over Local Area Networks (LANs). Ettercap is compatible with a range of operating systems, including Linux, Mac OS X, Solaris and Microsoft Windows. It was ranked number 11 on the Top 100 Network Security Tools list of 2006. Ettercap is one of the most advanced sniffing tools available. It allows the attacker to analyse traffic using a variety of different methods, and enables the efficient location of information in the shortest possible timeframe. While Ettercap is arguably the most advanced of the three applications I have outlined, there are some known issues with its stability when operating within a Windows environment. However, it operates perfectly in Kali, a Linux distribution designed for penetration testers.

2.10 Preventing an Attack

The following preventative measures can be taken to minimize the risk of being subjected to a session hijacking attack.

2.10.1 Encryption

The encryption of data, including the session token, passing between both parties can significantly reduce the chances of a successful session hijack attack. Encryption can be employed using a cryptographic protocol such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL). Encryption is heavily relied upon by most web-based banking applications and e-commerce services, including eBay and Freelancer. A relatively effortless means of employing encryption is to download and install the browser add-on, HTTPS Everywhere. This is the same software that is used by the Tor Project to enforce browser encryption within the Tor network. It should be noted that while encryption will dramatically reduce the effectiveness of sniffing-style attacks, there is still the potential for a session hijack to occur if the attacker uses a different method to gain access to the session token.

2.10.2 Connections

Another way to mitigate the risk of having your session hijacked is to limit the number of remote connections to your network. This can be done by using a Virtual Private Network (VPN) server. This enable authorized users to connect to your network from an offsite location. Employing a VPN server adds an extra layer of protection between users and your network. When combined with SSL encryption, a VPN server, acting as a middleman between your users' personal terminals and your network, should offer sufficient protection against session hijacks in the majority of cases.

2.10.3 Anti-Virus Software

Making sure that up-to-date anti-virus software is installed on networked computers will help prevent the network being infected by malware. As discussed, malware can be used by an attacker to steal a session token.

2.10.4 Employee Education

Educating employees as to procedures for safe internet use can be boring but nonetheless highly effective in preventing a range of attacks. Educating your employees about the different types of malware, how malware is spread (spam email, infected files etc.) and proper browsing habits, will assist in preventing infections that could spread across your network and reap havoc.

2.11 Countermeasures for Session Hijacking

We can take couple of steps to prevent Session Hijacking.

- Web applications should use SSL/TLS to transfer sensitive data. This will encrypt the data making it difficult for the attacker to steal session cookie or any other information.
- Web applications should use very long random numbers as session key, so that it becomes difficult for the attacker to guess the session key and exploit that.
- After a user authenticates himself, the server should regenerate the session key. It will become difficult for the attacker to guess the session key after the user logs in.
- Web applications should use secondary checks like matching the IP address with that of the previous session etc, to increase the security.
- Web applications can change the cookie with each and every request made by the user's computer. This will limit the attacker to a great extent.
- And, users should always log out of the web applications, as soon as they are done using them.

2.12 Hijacking Application Levels

At this level a hijacker can not only hijack already existing sessions but can also create new sessions from the stolen data.

HTTP Session Hijack

Hijacking HTTP sessions involves obtaining Session ID's for the sessions, which is the only unique identifier of the HTTP session. Session ID's can be found at three places

1. In the URL received by the browser for the HTTP GET request.

2. With cookies which will be stored in clients computer.

3. Within the form fields.

Obtaining Session ID's

One way to obtain the Session ID is by sniffing, which is same as the Man in middle attack. Cookies and URL's can be sniffed from the packets and if unencrypted can provide critical user logon information.

Another way is by Brute Forcing the Session ID's which involves trying a set of session id's based on some pattern. Brute forcing is a time consuming task but worked on some algorithm can produce results rather quickly.

2.13 Conclusion

Whether you are operating on your personal, home, or business network, the threat of session hijacking attacks is very real. While a successful attack can be devastating to you and your business, the measures outlined in this article can assist in reducing the likelihood of an attack being effective.

Session hijacking is a serious threat to Networks and Web applications on web as most of the systems are vulnerable to it. Although above explanation and countermeasures will give insight to the defender to protect his /her network, but it will also raise the security bar and will force the hijackers to apply more complex attacks to compromise the system. Networks should be tested and monitored continuously in order to make them impenetrable by the intruders.

2.14 Reference

http://www.bindview.com/Services/Razor/Papers/2001/tcpseq.cfm

Unit-3
Social Engineering

Learning Objectives :

After learning this unit you should be able to

- Know about Social Engineering.
- Know about how Effective Is Social Engineering.
- Know about different type Social Engineering.
- Study about Insider Threat and Insider Attack.
- Know about Identity andHow Identities Are Stolen.
- Know about General Tips for Social Engineering.
- Know about The Social Engineer’s Toolkit.
- How Can You Use Social Engineering in Your Everyday Life?
- Understand about Mitigation advice.
- Study about Counteracting Social Engineering.

Structure

3.1 Introduction

In cyber-security, social engineering refers to the manipulation of individuals in order to induce them to carry out specific actions or to divulge information that can be of use to an attacker. Social engineering in itself does not necessarily require a large amount of technical knowledge in order to be successful. Instead, social engineering preys on common aspects of human psychology such as courtesy, gullibility, greed, thoughtlessness, shyness and apathy. Social engineering techniques are commonly used to deliver malicious software (malware2) but in some cases only form part of an attack, as an enabler to gain additional information, commit fraud or obtain access to secure systems. Social engineering techniques range from indiscriminate wide scale attacks, which are crude and can normally, be easily identified, through to sophisticated multi-layeredtailored attacks which can be almost indistinguishable from genuine interactions.Social engineers are creative, and their tactics can be expected to evolve to take advantage of new technologies and situations. This unit outlines some of the most common and effective forms of social engineering.

3.2 What is Social Engineering?

Social engineering is using the common tendencies of how people interact with others in order to gain information or a benefit of some kind. Effectively, social engineering can be referred to as the hacking of people. Before the Internet age, social engineering would more likely be referred to as conning, but the scope of social engineering's applications goes beyond tricking people out of money. It is about causing people to act according to your wishes. Getting someone to say yes to a date is social engineering. So is getting your company a contract from a tough client. In regards to information security, social engineering is getting people to give up protected information.

3.3 How Effective is Social Engineering?

Even companies that place a high focus on securing their information networks can prove extremely vulnerable to social engineering attacks. DefCon, one of the largest hacking conferences in the world, routinely features a social engineering competition that has demonstrated over and over again that simple tactics can be used to get enough information to potentially do harm to a company. Position in the company also seems to have almost no effect on how susceptible a person is to social engineering; a big wig is just as likely to give up information as a cashier, but the big wig also usually has access to more pertinent info.

Social engineering is gaining attention for its insidious effectiveness, and is starting to get recognized in the media and the corporate world. Check out these news articles for an idea of how it is being perceived:

Smooth-Talking Hackers Test Hi-Tech Titan's Skills – A look at DefCon hacking competitions, utilizing social engineering within legal boundaries to ferret out intelligence designed to weaken a company's security.

Social engineering to blame in Syrian Electronic Army hijack of the Onion – The targets of these sorts of attacks aren't always the ones you might expect, the Onion was a recent victim of a phishing scheme.

Facebook Social Engineering Attack Strikes NATO – Often, the targets are important, such as this attack against NATO. Every organization contains a human element, the target of savvy social engineers.

How a lying 'social engineer' hacked Wal-Mart – Many people are naturally biased to trust based on a set of subtle criteria; a tone of voice, a style of dress, even word choices can lead people to give credence to otherwise nonsensical ideas or situations, like this Wal-Mart store manager being duped into giving away company data in exchange for a non-existent contract possibility.

3.4 Social Engineering Types

Commonly referred to as the non-technical method of hacking, social engineering is a method of data intrusion that relies on human interaction. In a social engineering attack, bad actors prey upon people's natural proclivity for trust. Hackers may present themselves as a friend or familiar acquaintance in order to trick people into giving them typically confidential information or access to personal accounts. There are two common classifications of social engineering:

- *Internal*: In this type of attack, someone from inside the business has found a vulnerability and decided to take advantage. He or she may use the access to email lists and employee addresses to send out an email prompting users to engage in a call to action containing malicious software.
- *External*: This is when an outside source, perhaps a competitor or criminal hacker, wants to gain access to your data, so they employ similar tactics as the internal threat using information gathered off a public site.

The best cyber defense is understanding your vulnerabilities and doing what you can to correct them.

3.4.1 Insider Threat

- *Intentional*: This occurs when anyone who has or has had access to a company's network uses this access for malicious purposes. This can mean that the confidentiality of records was compromised, data was stolen or financial damage was one.
- *Unintentional*: Like intentional insider threat, this type of cyberthreat is the fault of a company's employee. However, unintentional insider threats are unplanned. The individuals involved were usually socially engineered into allowing a bad actor to have access to the network.

3.5 Insider Attack

An **insider attack** is one of the biggest threats faced by modern enterprises, where even a good working culture might not be sufficient to prevent it. Companies implement sophisticated technology to monitor their employees but it's not always easy for them to distinguish between an insider and an outside attack.

Those who target and plan attacks from the outside might create strategies for obtaining insider knowledge and access by either resorting to an existing employee, or by making one of their own an insider.

Understanding the attacker types might serve as a stepping stone in selecting effective security measures to prevent threats to the company. According to Bruce Schneier, author of *Beyond Fear*, the categories of attackers are:

Opportunists:

The most common type of attacker. As the category indicates, they spot and seize an "opportunity" and are convinced that they will not get caught. It is easy to deter such attackers via cursory countermeasures.

Emotional Attackers:

They may accept a high level of risk and usually want to make a statement through their attack. The most common motivation for them is revenge against an organization due to actual or perceived injustice. Although emotional attackers feel powerful when causing harm, they sometimes "hope to get caught" as a way of solving the issues they were unhappy with but were unable to change from the beginning.

Cold Intellectual Attackers:

Skilled and resourceful professionals who attack for their own gain or are employed to do so. They target information, not the system, and often use insiders to get it. Unlike opportunists, cold intellectual attackers are not discouraged by cursory countermeasures.

Terrorists:

They accept high risk to gain visibility and make a statement. They are not only hard to deter by cursory countermeasures, but can even see them as a thrill.

Friends and relations:

They may introduce a problem to both individuals (in the form of financial fraud, for example) and companies (by abusing authorization credentials provided to legitimate employees). In this scenario, a victim and an attacker are sharing physical space, which makes it very easy to gain login and other sensitive information.

There are a number of precursors of insider attacks that can help to identify and prevent them:

- **Deliberate markers** – These are signs which attackers leave intentionally. They can be very obvious or very subtle, but they all aim to make a statement. Being able to identify the smaller, less obvious markers can help prevent the "big attack."
- **Meaningful errors** – Skilled attackers tend to try and cover their tracks by deleting log files but error logs are often overlooked.
- **Preparatory behavior –** Collecting information, such as testing countermeasures or permissions, is the starting point of any social engineering attack.
- **Correlated usage patterns –** It is worthwhile to invest in investigating the patterns of computer usage across different systems. This can reveal a systematic attempt to collect information or test boundaries.
- **Verbal behavior** – Collecting information or voicing dissatisfaction about the current working conditions may be considered one of the precursors of an insider attack.
- **Personality traits –** A history of rule violation, drug or alcohol addiction, or inappropriate social skills may contribute to the propensity of committing an insider attack.

3.6 Identity Thieves

Identity theft is the use of information such as a person's name, bank account number, birth date or social security number without the individual's knowledge. This can range from putting on a uniform to impersonate someone, or even an elaborate scam involving DNS poisoning, as well as phishing scams.

3.6.1 Phishing

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Gartner research firm, estimates that 57 million U.S. adults received a "phishing" attack email within the past year. More than half of those that responded were victims of identity theft. This scam is carried out by sending legitimate looking emails to

unsuspecting individuals. The emails are designed to make the recipient believe that they are from an institute they trust, such as their banking institutions or any other company that may require you to provide personal information for authentication. As the unsuspecting person hands over this information they have opened up themselves or their businesses to attack. Even seemingly benign information can lead to something severe. Divulging even personal information can lead to an attack being launched, as shown in the story about AOL mentioned in our framework .

3.6.2 Dumpster Diving

Another commonly used method to gather information about someone's identity is by dumpster diving. Individuals and businesses throw away lots of sensitive information containing addresses, phone numbers, credit card receipts, and even social security numbers. This information can be used to build the identity that the thief wants. The identity thief can also find birthday cards, addresses of family members and of businesses that are used by the individual to gain a foothold into their identity. If the identity thief finds that someone one is using a cleaning service frequently and paying them for services, this could be used as a way into the organization. Using this information the identity thief could pose as a janitor and use that as a way into an organization to either carry out the attack or gain even more valuable inform

3.6.3 Skimming

Another method used by identity thieves is called skimming. Skimming is an example of a low tech technique used to scan or swipe your credit or bank card and get the information off the magnetic strip. This scam is fairly easy to carry out in restaurants or any place that you give someone your card and they walk out of sight to run the charges. The thief runs the card through a hand held scanner and is then able to capture the card information off it and use it at another time to run up charges on the account. The Center for Identity Management and Information Protection says that mail theft, dumpster diving, stolen wallets, and other low-tech or no-tech methods are used far more often, with only 10 percent of scammers using the Internet exclusively.

3.6.4 Pharming

Another method used with Identity theft is Pharming. These scams use basically two methods, in the first, the attacker modifies the computers hosts file and uses links in emails that look like they send you to a legitimate site for a financial institution. The web site is actually correct but you have made their system go to a fraudulent IP for that URL. The second attack exploits vulnerabilities in DNS servers that redirect victim's to the fake websites. The erroneous site enables the attacker to collect user-names, password, account information, and anything else that is entered in the web site. The Drive-by Pharming attack is a fairly sophisticated attack that involves modifying the configuration of the external router as opposed to the computer's local host file or the DNS server. Again it is the same principle but the thief is modifying the settings for an entire network rather than just a single host.

3.6.5 Tombstone Theft

A less thought of attack that can really be vicious is Tombstone Theft. Tombstone Theft involves stealing someone's identity that has passed away. The thief can assume this individuals identity and likely get away with the deceit for some time. Because of someone's death people often forget about notifying banks and other credit card companies right away after their loved ones death. As far as the financial companies know, the individual is alive and using their cards or accounts as normal. The thief typically gets this information through funeral home notices or obituaries. Funeral homes can be careless in their handling of personal information about their customers and information can be gained from newspaper obituaries. An example of this crime can be found in Atlanta Georgia. Personal identity information of some 80 people were sold for $600 US apiece. That information was used to secure over $1.5 million in loans._

3.7 How Identities are Stolen

There are six key ways identity theft occurs and these are all discussed in depth in our framework:

1. **Dumpster Diving:** Rummaging through your trash or your company's trash an identity thief can find enough information about you to launch an attack. [Dumpster Diving section in wiki]
2. **Skimming**: This is where an attacker uses a special device to store your personal information when you buy something from a store. This is the type of attack that was used against TJ Maxx.
3. **Phishing:** Pretending to be a financial institution or company a malicious email is sent trying to encourage you to visit a very realistic looking site and enter your personal info.
4. **Changing Your Address**: It has been done where an identity thief can divert your bills after they order high ticket items, to another location simply by filling out a "change of address" form.
5. **Stealing**: Still viable, but an identity thief who steals a purse or wallet can take the theft further by now taking your identity.

6. **Pretexting:**Using false pretenses, they obtain personal information from you that can lead to your identity being used falsely.

3.8 Famous Identity Thieves

Frank Abagnale

One recent popular example of identity theft is shown in the movie "Catch Me if you Can" based on Frank Abagnale. Frank impersonated a doctor, lawyer, prison inspector, maybe most famously an air line pilot. His airline scams alone cost Pan AM Airlines untold sums as Frank flew over 1 million miles to over 26 countries and stayed at various hotels along his way. Another more popular example of Franks scams was in the form of fraudulent checks. Frank used impersonation, pretexting, and other techniques to carry out some extraordinary scams.

In the example above Frank used a pilot's uniform and some prior knowledge of airports to carry out this scam. Another trick that he used is pretexting. In other words you use a position of authority to get things that you need or pretend that you are in real need of something of importance or urgent. Impersonation is used in the same way. Through observation, and using the jargon, the attire, or uniform, and some general knowledge to impersonate someone, a thief can steal a person's identity in the literal sense of the word. An identity thief can take a picture of an ID card and print it out and paste their own picture on "Tom Smith's" access badge and now the thief has become "Tom" The thief can dye his hair or put in false teeth to disguise himself as the individual he is trying to impersonate.

An example of ID Theft

Original source: YouTube.

3.9 General Tips for Social Engineering

These are common guidelines and methods used by social engineers before and during any assignment on which they are working. These focus more on the preparation and mindset of the social engineer than the actual attack methods that are used.

3.9.1 Do Your Research

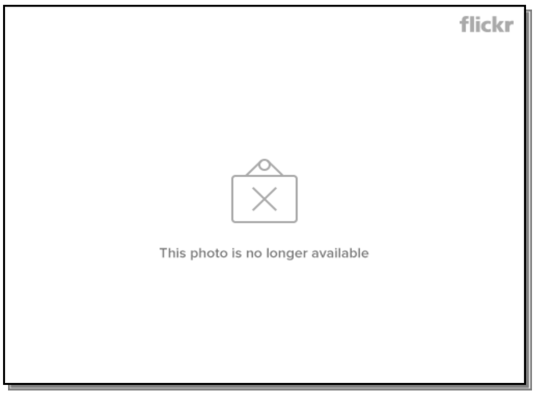
Take a look at this seminar on social engineering strategies.

Information is everywhere. If there is a topic you want to know about, you usually only need to glance at the Internet. Reading the news and press releases from a company can give you a firm background history from which to work. A social media site may give you insights into the temperament of a person or give you an idea of the social scene in which they operate. If you are trying to infiltrate a group or become closer to a person with any notable focus, then the Internet can be used to familiarize yourself with the topic.

Hackers may go above and beyond in this regard. If they manage to gain access to someone’s email account or messaging service, there may be records of conversations that can be used to mimic the person in electronic communications or learn about key topics that anyone on the inside should know about.

3.9.2 Look the Part

Imagine for a moment that you are watching a movie set in modern times and focused on the happenings in a government or business office. If there was someone dressed in jeans and a hoodie in the middle of a meeting of executives or elected officials, you would likely immediately feel the character was out of place or at least question why they were there. The same holds true whenever you want to interface with another social group, whether it is a company or a club.



Also worth noting is that looking professional – wearing a nicely tailored and well-kept business suit – can generate an obscene level of trust in your social interactions. The suit conveys a lot of subtle messages: this person is a successful member of society, they likely have money, and you can trust then a bit more than the average person. You may not gain complete trust and unlimited access, but the difference between the trust levels shown to someone in a suit and someone in casual clothing is palpable.

3.9.3 Learn to Read People

This article gives you a glimpse into the advancement of research into the integration of robotics and emotions.

If computers are getting to the point that they can recognize and react to the emotional displays of people, then there is no reason that a person should not be able to better do the same task. Taking the time to read on facial expression theory and other psychological articles can help point you in the right direction, but the only way to really learn is to go out and talk with people. Doing this with new people consistently will also give you practice on learning how to pick up the subtleties in a new person’s expression and tone.

3.9.4 Backup Your Backup Plans

Just having an idea of how to work a plan does not mean you should ignore contingency plans. Even if a failure in one portion of a plan only leaves breaking off the attempt, you should be prepared for the possibility and have a clear idea of how you will break it off. This is not going to eliminate having to think on your feet, but having a guideline for your actions can mean the difference between a smooth response and something haphazard that sends the wrong signal.

3.9.5 Strength in Numbers

Unlike the world of open conflict, more numbers on the side of the target can be a firm advantage. Working your way into a small firm can be a dogged task, but it can be easy to turn into “just another suit” at larger offices. It is almost always easier to work your way into social situations when the target has a larger number of people involved.

3.9.6 Take the Time to Do It Right

If you were to take movies and shows as fact, you would think social engineers waltz into a business with a suit and savvy and somehow manage to make their way into the confidence of the boss or gain access to sensitive areas within a few minutes. A real social engineering effort may take weeks or months to accomplish properly.

3.10 The Social Engineer’s Toolkit

A number of techniques have become common practice for social engineers. The list here is not exhaustive, and the variations on these techniques makes covering them all a task better suited for a textbook.

3.10.1 Phishing, Vishing, and SMiShing

This rainbow of techniques is typically meant to refer to scenarios where the attacker poses as a person or service the target already knows via electronic communications. One of the most common phishing emails is one that mimics the company’s style and email address while telling the target that their account has been locked out due to potentially malicious activity. A link is supplied to the target to reset their password. The site looks like the company’s to the smallest degree, but the reset instead sends your old and new passwords to the phisher.

The delineation between the terms is based on the attack vector. Phishing is done through the computer, vishing is done through the phone, and SMiShing is done through text messaging.

3.10.2 Pretexting

Pretexting is the art of constructing a scenario in which the target is more inclined to go along with the wishes of the attacker. The most common example of this in action might be taken from the ways people try to convince traffic cops to not give them tickets: “My friend is in the hospital”, “My wife is delivering our baby”, or “I’m on my way to stop the love of my life from getting on a plane and never coming back.” In the movie Live Free or Die Hard, a character uses the pretext of his grandfather in the hospital to get an OnStar agent to activate a car he wants to steal.

3.10.3 Sex Appeal

When dealing with a pretty face, a person can become distracted and lose focus on the things that matter. Not every social engineer will be a model, but you can expect the ones that have been favored with good looks and charm to use the advantage.

3.10.4 Tech Support

Most people simply have no idea what is going on with their computers beyond interfacing with the applications they use to work. Computers also have an unfortunate tendency to break down due to misuse or just over time. In larger companies, it may not be uncommon for the IT department to be behind on fixing all the computer issues that are active. By masquerading as tech support, savvy social engineers can troubleshoot for the employee while also placing themselves in a trusted position to ask for personal information like passwords.

3.10.5 The Indirect Approach

Coming up to a person directly and asking them about secure, private topics may immediately trigger warning signals. If the social engineer instead approaches a person via a secondary topic and befriends them, then later probing for the information has a higher chance of success due to the longer time for which trust has developed. As an example, if the target is an avid golfer, then a social engineer might find a way to arrange for them to end up playing together. This would let the engineer strike up a conversation naturally due to the common event.

3.11 Spy Versus Spy: Counteracting Social Engineering

It is nigh on impossible to stamp out the threat that social engineering represents even when utilizing proper security methods at a business or simply trying to avoid falling victim to it yourself. Much of the research and the supported methods for handling the threat of social engineering are to educate people on the dangers of it, develop security policies based on what needs to be protected, install Data Leak Prevention (DLP) software, and do penetration testing to get a real idea of the level of security in place.

3.11.1 Enforce Strict Information Release Policies

Both in your personal life and in the business world, sensitive information should be treated with respect and controlled properly. That does not mean you have to give someone trouble every time they ask for personal information, but taking the time to double check that the person is who they say they are and that you can feel comfortable handing over sensitive information can be done with a high degree of trust.

3.11.2 Education

To use an analogy, the human minds that reside within a social group can be thought of as computers on that social network. Where you would patch a computer, you would educate a mind. The ways in which you can be educated are numerous: you could have an article on social engineering (like this one) made mandatory reading, make social engineering news part of your company newsletter, or hold a class every couple of months. At the very least, people should be aware of the information policy on which you decide. The patch may not take on every person, but you should at least try.

3.11.3 Data Leak Prevention Software

An up and coming type of software is joining the ranks of applications like antivirus and firewalls on the list of things any network trying to be secure should have: Data Leak Prevention (DLP) tools. The software can monitor data in storage, in use, or going over the network, and it can perform tasks like preventing the data from sending or triggering an alert if something is sent. This is limited to just helping to prevent social engineering mishaps on computer networks, but social engineers are likely to use a combination of methods to try and gain access to the most valuable information.

3.11.4 Penetration Testing

Just like your hardware and software, you people can benefit from penetration testing in order to ascertain their awareness of social engineering as a threat and the information security policies that protect from it. This usually requires the aid of an outside entity to get a proper simulation of an attack from someone currently outside the company.

3.12 How Can You Use Social Engineering in Your Everyday Life?

You may not want to con someone out of their account passwords or savings fund, but that does not mean that the methods of social engineering cannot find their place in your life. They can even be used effectively for altruistic purposes. For example, making new friends can benefit from the inclusion of social engineering information.

Social engineering as a way to gain access to secure information is a threat of which everyone should be aware. Like almost any form of science or technology, it can be used for good and for evil. Taking the time to learn social engineering methods is the best way to use them to your benefit and know how to defend against them. Unless you move to deserted island with no technology, you are going to be subject to the designs of social engineering, so you may as well stay informed on the subject.

3.13 Mitigation Advice

Technical solutions such as spam filters, anti-virus software and blocking known phishing/baiting websites can help prevent some phishing attacks. To some extent blocking the use of non-authorized USB devices and disabling CD/DVD drives can do the same for baiting attacks. However, a successfulsocial engineer will attempt to get around these protections. As a result, the best prevention against social engineering is raising user education and awareness:

- Make sure users are aware of the signs of phishing emails – good advice is available from Cyber Streetwise (https://www.cyberstreetwise.com/common-scams) and Get Safe Online (https://www.cyberstreetwise.com/common-scams)
- If your organization is a member of CiSP, you can seek advice from other CiSP members on improving user awareness. See here for more information about joining CiSP: https://www.cert.gov.uk/cisp/
- Consider holding user awareness sessions, potentially as part of training or induction days, and including a demonstrative penetration test, showing a successful social engineering attack against an (anonymous) member of the organization
- Encourage users to verify any strange requests or messages by calling the originator on an already confirmed number
- Make users aware of their online presence and caution them to be aware of how much information they make available on social media
- Assess how much information your organization makes available publicly, and whether any of this could be used in a social engineering attack
- Implement policies that reduce the risk of a successful phishing (e.g. to never send sensitive information outside your organization’s network), and give users the confidence they won’t be punished for sticking to the rules
- Encourage users to share their concerns over strange emails or other potential social engineering events with colleagues and IT support
- Ensure as an organization you inform others of potential social engineering attempts through CiSP – you may not be the only one being targeted, but you may be the first who realizes it’s a social engineering attack
- Prepare for the fact that you are highly likely to eventually be compromised, and ensure you have in place an incident response and disaster recovery capability
- In general, if your organization adheres to the ‘10 Steps to Cyber Security’ 9 and the ‘20 Critical Controls for Cyber Defense’ 10 you will be in a good place to

prevent, respond and recover from a range of cyber related incidents, including those that involve social engineering.

3.14 Let Us Sum Up

Social engineering is one of the most prolific and effective means of gaining access to secure systems and obtaining sensitive information, yet requires minimal technical knowledge. Attacks vary from bulk phishing emails with little sophistication through to highly targeted, multi-layered attacks which use a range of social engineering techniques. Social engineering works by manipulating normal human behavioral traits and as such there are only limited technical solutions to guard against it. As a result, the best defense is to educate users on the techniques used by social engineers, and raising awareness as to how both humans and computer systems can be manipulated to create a false level of trust. This can be complemented by an organizational attitude towards security that promotes the sharing of concerns, enforces information security rules and supports users for adhering to them. Even so, a determined attacker with sufficient skill, resources and ultimately, luck, will be able to retrieve the information they are seeking. For this reason, organisations and individuals should have measures in place to respond to, and recover from, a successful attack.

3.15 Self-Assessment Questions

1. **What Is Social Engineering?**

   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………

2. **What is Insider Attack?**

   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………

3. **What is Phishing?**

   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………

4. **What is Skimming?**

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………

5. **What is Insider Threat?**

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
………..…………………………………………………………………………………

3.15 Model Questions

1. How Effective Is Social Engineering?
2. Explain about different types of Social Engineering.
3. Explain about Penetration Testing.
4. How to back up your Backup Plans?
5. How Can You Use Social Engineering in Your Everyday Life?

3.16 References & Further Readings

1. https://www.ncsc.gov.uk
2. http://www.nationalcybersecurityinstitute.org/awareness-month-2015/case-study-i-social-engineering-and-insider-threat/are covered.
3. https://www.tripwire.com/state-of-security/incident-detection/identifying-and-preventing-insider-threats/

Answer of Self-Assessment Questions (Unit-3)

1. **What Is Social Engineering and Explain it?**

   Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

   Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

2. **What is Insider Attack?**

   An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access.

   Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.

3. **What is Phishing?**

   Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.The information is then used to access important accounts and can result in identity theft and financial loss.

4. **What is Skimming?**

   Fraudsters use skimming to copy the data stored on the magnetic stripe of your bank card (at the back of the card) when you put your card in a cash dispenser. They use an almost invisible device installed right in front of the card slot on the cash dispenser in order to copy the data without the customer being aware of this. At the same time, they try to see your secret code, for instance by making use of a minicamera or via shoulder surfing. The data that have been stolen, will be used for making a false card.

5. **What is Pharming?**

   Pharming (pronounced farming) is a cracker's attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses - they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred to as "poisoned". The term pharming is a word play on farming and phishing. The term phishing refers to social engineering attacks to obtain access credentials such as user names and passwords. In recent years both pharming and phishing have been used to steal identity information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.

Unit- 4
Denial of Service

Learning Objectives:

After learning this unit you should be able to

- Know about Denial-of-Service and his History.
- Know about different types of DoS attacks.
- Know about what are the physical infrastructures in DoS Attack.
- Study about Distributed DoS Attack.
- Know about what smurf attack is and how to protect.
- Know about Protecting Microsoft Windows From A SYN Flood Attack.
- Know about Bots and Botnets and what is it and how its work.
- How Can You Use Life cycle of a Botnet in Your Everyday Life?
- Understand aboutflooding.
- Study about How to Protect Yourself.

Structure

4.1 Introduction

Denial of Service (or DoS for short) attacks are a kind of attacks against computers connected to the Internet. DoS attacks exploit bugs in a specific operating system or vulnerabilities in TCP/IP implementation. Unlike a privacy attack, where an adversary is trying to get access to resources to which it has no authorization, the goal of DoS attacks is to keep authorized users from accessing resources. The infected computers may crash or disconnect from the Internet. In some cases they are not very harmful, because once you restart the crashed computer everything is on track again; in other cases they can be disasters, especially when you run a corporate network or ISP.

In this unit, you will find many useful and definition which not only give you a general introduction to DoS attacks, but also present you specific types of DoS attacks and their possible solutions.

4.2 About Denial-of-Service (DoS)

A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoSattack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

The Denial of Service module delivers an in-depth analysis on the availability of info in terms of Penetration Testing and specifically to Denial of Service attacks. It clearly articulates the relationships of the network and to business, and discusses the two types of attacks you’ll face: regular Denial of Service (DoS) and Distributed Denial of Service (DDoS).

A DoS attack can be done in a several ways. The basic types of DoS attack include:

1. Flooding the network to prevent legitimate network traffic
2. Disrupting the connections between two machines, thus preventing access to a service
3. Preventing a particular individual from accessing a service.
4. Disrupting a service to a specific system or individual
5. Disrupting the state of information, such resetting of TCP sessions

Another variant of the DoS is the smurf attack. This involves emails with automatic responses. If someone emails hundreds of email messages with a fake return email address to hundreds of people in an organization with an autoresponder on in their email, the initial sent messages can become thousands sent to the fake email address. If that fake email address actually belongs to someone, this can overwhelm that person's account.

DoS attacks can cause the following problems:

1. Ineffective services
2. Inaccessible services
3. Interruption of network traffic
4. Connection interference

The motivation for DoS attacks is not to break into a system. Instead, it is to deny the legitimate use of the system or network to others who need its services. One can say that this will typically happen through one of the following means:

1. Crashing the system.
2. Deny communication between systems.
3. Bring the network or the system down or have it operate at a reduced speed which affects productivity.
4. Hang the system, which is more dangerous than crashing since there is no automatic reboot. Productivity can be disrupted indefinitely.

4.3 History of Denial-of-Service Attacks

DoS attacks on internet-connected systems have a long history, arguably started with the Robert Morris worm attack in 1988. In that attack, Morris, a graduate student at MIT, released a self-reproducing piece of malware (a worm) that quickly spread through the global internet and triggered buffer overflows and DOS attacks on affected systems. Mostly research and academic institutions were connected to the internet at the time, but it was estimated that as many as 10% of the 60,000 systems in the U.S. were affected.

Damages were estimated to be as high as $100 million, according to the U.S. General Accounting Office, and Morris was successfully prosecuted under the 1986 Computer Fraud and Abuse Act and sentenced to three years' probation, 400 hours of community service and fined $10,000.

DoS attacks can also be major components of other type of attacks.

4.4 Types of DoS Attacks

In addition to differentiating between a single-source denial-of-service attack and a distributed denial-of-service (DDoS) attack, DoS attacks can also be categorized by the methods the attack uses.

In an amplified DNS denial-of-service attack, the attacker generates crafted domain name system (DNS) requests that appear to have originated at the victim's network and sends them to misconfigured DNS servers managed by third parties. The amplification occurs as the intermediate DNS servers respond to the faked DNS requests. The responses from intermediate DNS servers to the crafted attack requests may contain far greater volume of data than ordinary DNS responses, requiring more resources to process, with the result being to deny legitimate users access to the service.

Application layer attacks generate fake traffic to internet application servers, especially DNS servers or HTTP servers. While some application-layer denial-of-service attacks rely simply on flooding the application servers with network data, others depend on exploiting weaknesses or vulnerabilities in the victim's application server or in the application protocol itself.

A buffer overflow attack is a catchall description most commonly applied to DoS attacks that send more traffic to a network resource than was ever anticipated by the developers who designed the resource. One example of such an attack sent, as email attachments, files that have 256-character file names to recipients using Netscape or Microsoft email clients; the longer-than-anticipated file names were sufficient to crash those applications.

In a DDoS attack, the attacker may use computers or other network-connected devices that have been infected by malware and made part of a botnet. Distributed denial-of-service attacks, especially those using botnets, use command-and-control (C&C) servers to direct the actions of the botnet members. The C&C servers dictate what kind of attack to launch, what types of data to transmit and what systems or network resources are to be targeted in the attack.

The ping-of-death attack abuses the Packet Inter-Network Groper (ping) protocol by sending request messages with oversized payloads, causing targeted systems to become overwhelmed, stop responding to legitimate requests for service and possibly crashing the victim systems.

A SYN flooding attack abuses TCP's handshake protocol by which a client establishes a TCP connection with a server. In a SYN flooding attack, the attacker directs a high-volume stream of requests to open TCP connections with the victim server, with no intention of actually completing the circuits. The cost of generating the stream of SYN requests is relatively low, but responding to such requests is resource-intensive for the victim. The result is a successful attacker is able to deny legitimate users access to the targeted server.

TCP, or Transmission Control Protocol, also called state exhaustion attacks occur when an attacker targets the state tables held in firewalls, routers and other network devices by filling them with attack data. When these devices incorporate state full of network circuits, attackers may be able to fill state tables by opening more TCP circuits than the victim system can handle at once, preventing legitimate users from accessing the network resource.

The teardrop attack exploits flaws in the way older operating systems handled fragmented Internet Protocol (IP) packets. The IP specification allows packet fragmentation when the packets are too large to be handled by intermediary routers, and it requires packet fragments specify fragment offsets; in teardrop attacks, the fragment offsets are set to overlap each other. Hosts running affected OSes are unable to reassemble the fragments and the attack may also crash the system.

Volumetric DoS attacks aim to interfere with legitimate access to network resources by using up all the bandwidth available to reach those resources. In order to do this, attackers must direct a high volume of network traffic against the victim's systems. Volumetric DoS attacks flood victim devices with network packets using the User Datagram Protocol or the Internet Control Message Protocol, in large part because those protocols require relatively little overhead to generate large volumes of traffic, while, at the same time, requiring nontrivial computation on the part of the victim's network devices to process the incoming malicious datagram’s.

4.5 Physical Infrastructure Denial-of-Service Attacks

A denial-of-service attack can also exploit vulnerabilities in a physical infrastructure to deny legitimate users access to computer or network resources. While many service interruptions are disrupted by network attacks, the same result can also be achieved by physically severing wiring or preventing power and cooling resources from being accessed. In such cases, the physical attack may also be referred to as sabotage.

4.6 What is a Distributed DoS?

A Distributed DoS (DDoS) is the combined effort of several machines to bring down victim. In many cases there is a master machine that launches the attack to zombie machines that are part of a bot network, as shown below in Figure 1. Some bot networks contain many thousands of machines used to launch an attack.

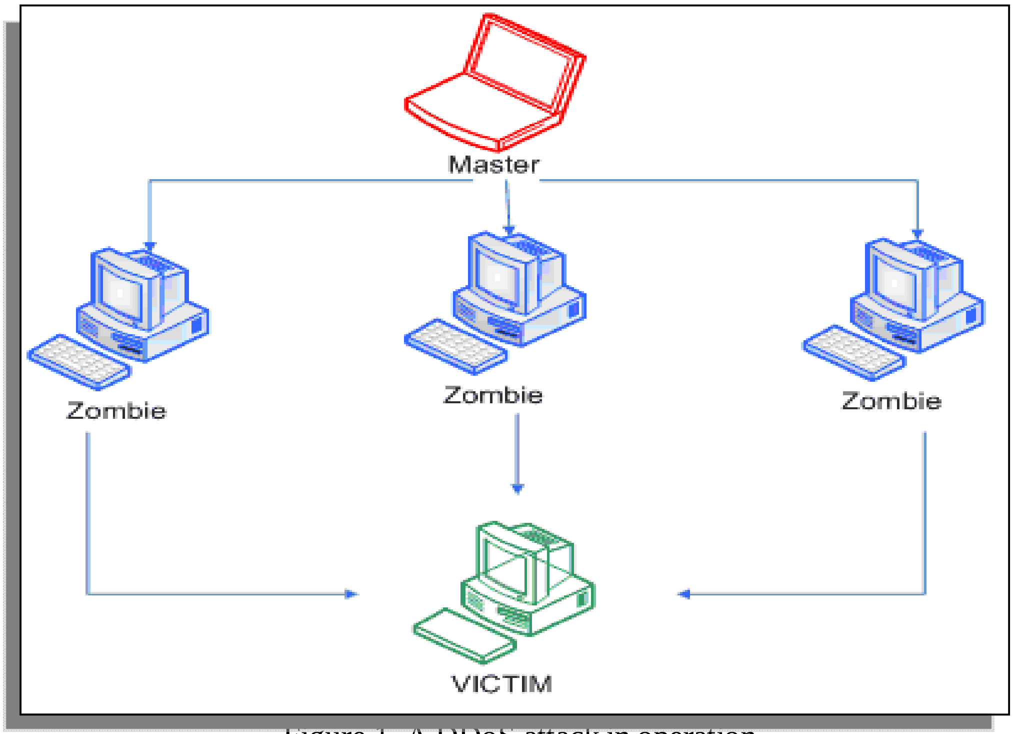


Figure 1. A DDoS attack in operation.

With DoS and DDos defined, we'll now take a look at attacks that affect the consumption of resources, such as Smurf attacks, and then address attacks like SYN Flood that affect network connectivity.

Note that the consumption of resources is most evident when it involves the exploitation of bandwidth, CPU usage, memory, disk space, or access to other computers and resources.

4.7 Bandwidth Exhaustion Attacks

A bandwidth exhaustion attack is where an attacker tries to consume the available bandwidth of a network by sending a flood of packets. This is most often accomplished with the help of several other machines. There is soon a flood of malicious nonsense packets on the network in large quantity, whereby the chances of survival of any good, legitimate packets becomes remote. Eventually the network becomes choked with these packets, and the network is effectively cutoff from the Internet and services are denied.

An ideal example of a bandwidth exhaustion attack would be Smurf attacks. Consider a scenario with an ISP and three clients, as shown below in Figure 2. In this scenario, the ISP receives extensive traffic for client 2 on its backbone. Since the connection to client 2 is of limited capacity and smaller than the ISP's backbone, it can't push all the data received for client 2 through the link to client 2. Therefore it will start to drop packets, and the TCP connections will lead to retransmissions of the lost/dropped packets. There will be a time when a legitimate host wants to connect to Client 2's network, but this will timeout and hence a DoS will occur.

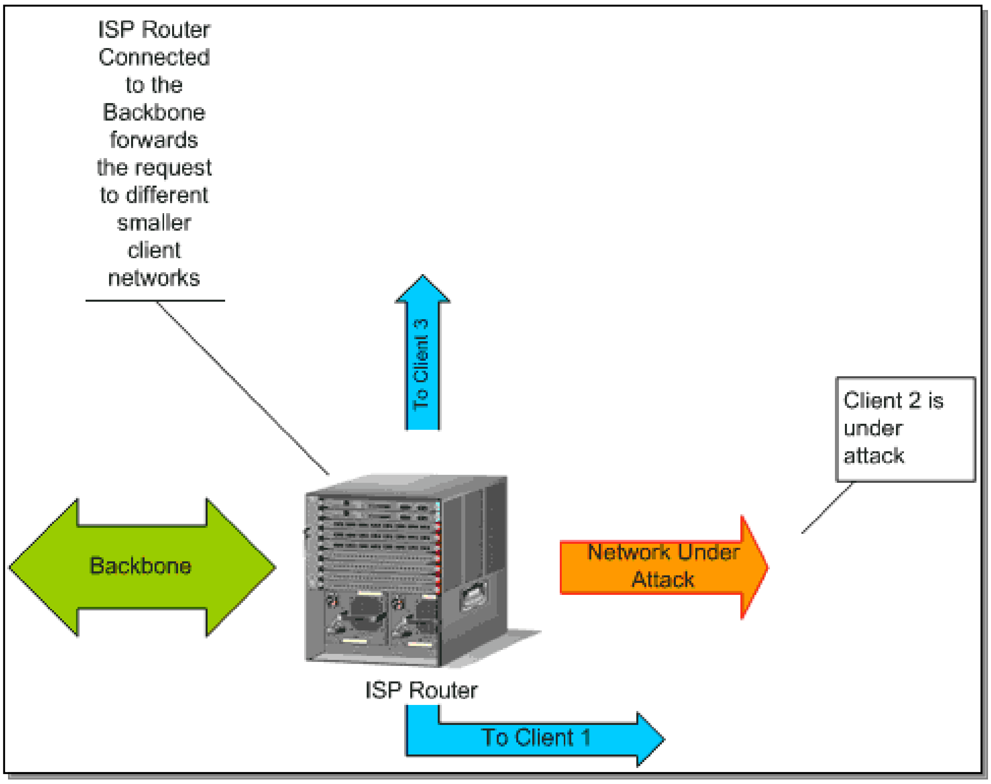

ISP Router Connected to the Backbone forwards the request to different smaller client networks
To Client 3
Client 2 is under attack
Backbone
Network Under Attack
ISP Router
To Client 1

Figure 2. Scenario for a bandwith exhaustion attack.

4.7.1 Smurf Attack

Named after a popular program which generates this attack, an ICMP echo request is sent to a broadcast network address (acting as an amplifying agent) with the source address of the victim spoofed. This results in a storm of replies from that network which, if large enough, has the power to take the victim's network down. It is to be noted that there is not much a victim can do about this attack since the link is simply overloaded with packets.

There are always three parts of a Smurf Attack:

1. Attacker
2. Amplifier - a router
3. Victim

This attack succeeds because the amplifier is misconfugred to forward the directed broadcasts.

Suppose the address range 172.30.164.0 to 172.30.164.255 is assigned to a company which has an amplifier, and an attacker sends packets with destination 172.20.164.255. All the routers and systems from attacker to the amplifier will not see the difference between this IP and 172.30.164.10 (an IP from the range). The packet reaches the amplifier and the amplifier notices that this is the broadcast address, so it forwards the request to all the systems on the network/subnet. This is known as directed broadcast.

The two crucial components of this attack were:

1. A misconfigured router forwarding the broadcast request to the subnet.
2. Machines that will respond to this ICMP broadcast request.

Going deeper we can see that the amplifier also makes itself and its network a victim of this attack.

Victims are typically chosen by attackers from IRC where bots (automated programs) are kept to look for the address of victims. Hackers often exchange the information about amplifiers with each other so when a mass attack takes place it usually appears to come from all over the globe.

Powertech provides real-time statistics of the top amplifiers currently on the Internet.

Below is a typical depiction of the dumps at the Victim. These are ICMP Echo replies received at the Victim's end. Then Figure 3 provides an overview of a Smurf attack.

```
10:10:17.100000 172.30.164.1  >victim:  icmp: echo reply

10:10:18.300000   172.30.164.76   >   victim:    icmp:   echo   reply   10:10:18.310000
172.30.164.10  >  victim:  icmp:  echo  reply  10:10:19.110000  172.30.164.223  >  victim:
icmp:   echo   reply   10:11:09.190000   172.30.164.51   >   victim:   icmp:   echo   reply
10:11:09.240000   172.30.164.18   >   victim:    icmp:   echo   reply   10:11:10.110000
172.30.164.98 > victim:  icmp: echo reply 10:11:10.600000 172.30.164.18 > victim:

icmp: echo reply 10:11:10.790000 172.30.164.240>victim:  icmp: echo reply
```

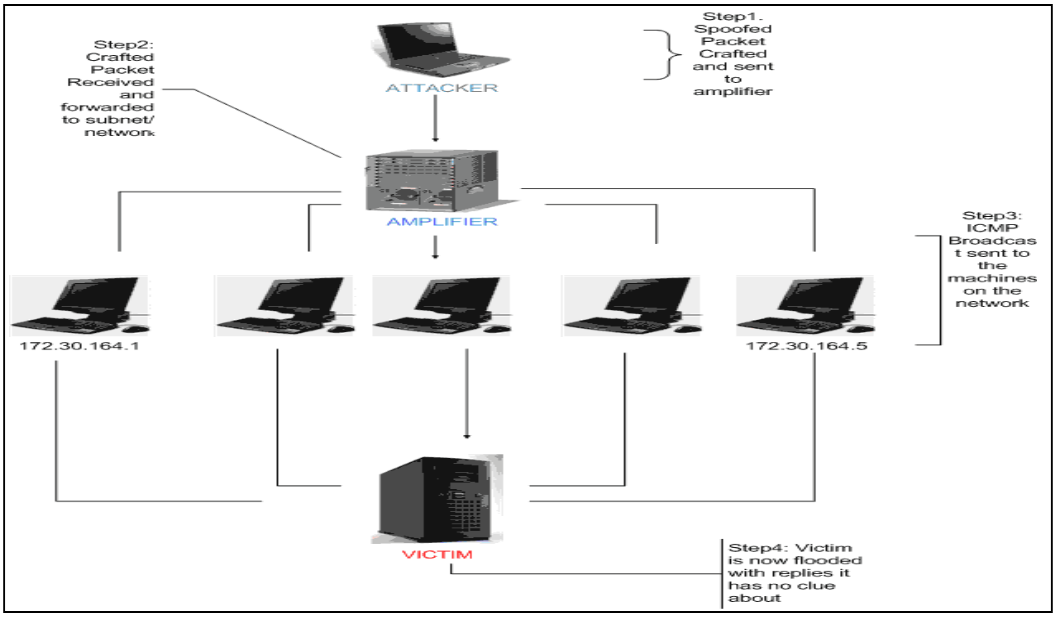

Step2: Crafted Packet Received and forwarded to subnet/ network
ATTACKER
Step1. Spoofed Packet Crafted and sent to amplifier
AMPLIFIER
Step3: ICMP Broadcas t sent to the machines on the network
172.30.164.1
172.30.164.5
VICTIM
Step4: Victim is now flooded with replies it has no clue about

Figure 3. Typical directed broadcast Smurf attack.

4.7.2 How to Protect Against Smurf Attacks

Step 1. Amplifier Configuration. The router should be configured so that it does not forward directed broadcasts onto networks. It is important to note that the broadcast has to be disabled on all the routers and not merely just the external ones. Command "no ip directed-broadcast" on Cisco routers should do the job in most cases. This will also ensure that employees on the internal network won't be able to launch Smurf attacks. However it is also advisable that one has a filtering device (such as a firewall) on the perimeter, thereby providing an extra layer of security.

Step 2. Configure the server operating systems. Servers should be configured so that they will not respond to a directed broadcast request. FreeBSD is one such system which by default does not respond to this request. Other systems can be similarly configured, and this will be discussed in the next section.

Step 3. Victim issues. As mentioned earlier, not much can be done at the victim's end and damage will be done unless victim's ISP takes some actions to block these ICMP Echo Reply floods. Even if the victim's parameter router denies the ICMP Echo Reply, the link from the ISP to the victim's site will suffer.

4.7.3 ICMP Ping Flood Attacks

Ping Floods are where an attacker floods the victim's network with large number of ICMP Echo Requests - such as by flooding the network as fast as possible. In this scenario, filtering the incoming packets might help, however, if the victim is on a modem instead of a high-speed connection, nothing can be done. However the catch in this attack is that if not done properly the attacker can also be counter-attacked, so he needs to be on a faster network than the victim. In most cases, mitigating this attack involves isolating spoofed IPs. This attack is easy to perform since there are many tools on Internet and little knowledge is required to execute a ping flood.

4.7.4 FraggleAttacks

A Fraggle attack is a Smurf variant that uses UDP instead of ICMP. In this case, the ports echo, chargen, daytime, qotd are used to trigger responses. These ports are also susceptible to a pingpong attack, and therefore these serves should be turned off or blocked.

4.8 Network Connectivity Attacks

These attacks overload the victim so that its TCP/IP stack is not able to handle any further connections, and processing queues are completely full with nonsense malicious packets. As a consequence of this attack, legitimate connections are denied. One classic example of a network connectivity attack is a SYN Flood.

4.8.1 SYN Flood Attacks

A SYN Flood is where an attacker sends packets with a spoofed source IP Address and a TCP SYN Flag set to the server (victim). Let's first assume that the attacker knows which ports are open on the server. Since the source IP is spoofed, the response sent to the SYN packet by the server will never receive a reply back. The server will keep waiting until it times out. If this happens for a very large number of connections the result will be a DoS, since the server won't be available for any legitimate connections and its resources will be choked.

As will be shown, this attack exploits a vulnerability of the TCP protocol, by the way in which the TCP three-way connection is established. This is shown below in Figure 4.

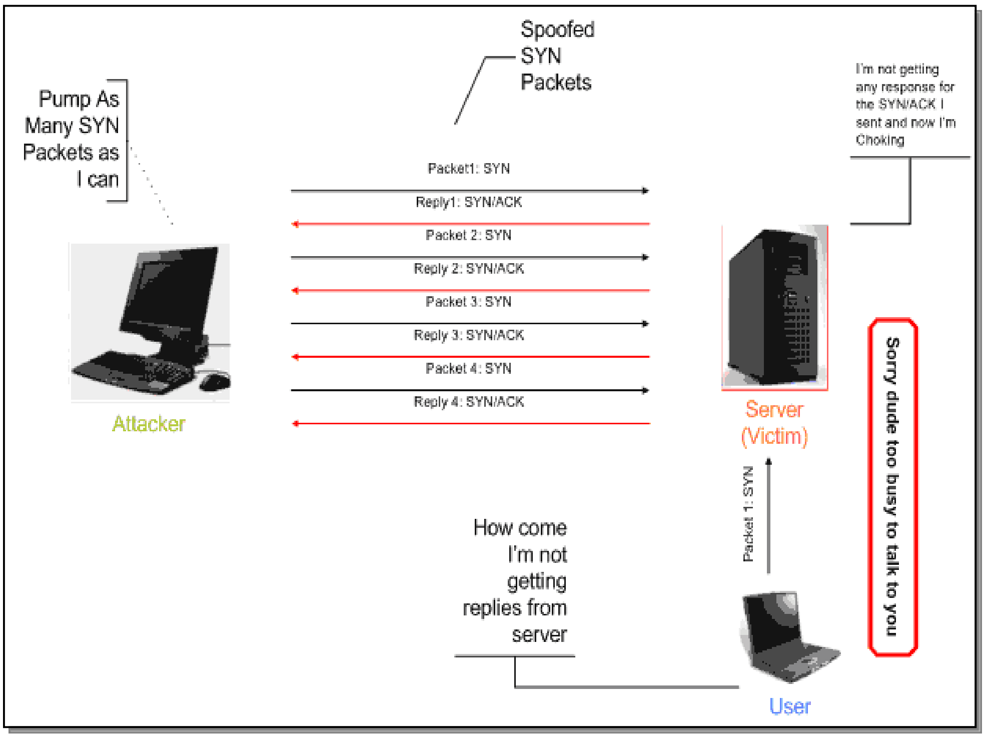

Spoofed SYN Packets
Pump As Many SYN Packets as I can
I'm not getting any response for the SYN/ACK I sent and now I'm Choking
Packet1: SYN
Reply1: SYN/ACK
Packet 2: SYN
Reply 2: SYN/ACK
Packet 3: SYN
Reply 3: SYN/ACK
Packet 4: SYN
Reply 4: SYN/ACK
Attacker
Server (Victim)
Sorry dude too busy to talk to you
Packet 1: SYN
How come I'm not getting replies from server
User

Figure 4. SYN Flood attack.

4.8.2 Protecting Against SYN Flood Attacks

There are several things that can be done to protect against SYN Flood attacks.

1. Decrease the TCP Connection Timeout on the victim server.
2. Use a filtering device, like a firewall, at the perimeter which works as an intermediary in forwarding the connections to the server.
3. Use of a server farm: this can also help in fighting the SYN Flood since you will have number of the servers to answer the request, but this also has limitations and overhead considerations.

4.8.2.1 Protecting Microsoft Windows from a SYN Flood Attack

Microsoft Windows has a mechanism to detect and start SYN Flood protection. The SYN flooding attack protection feature detects symptoms of SYN flooding and responds by reducing the time the server spends on connection requests that it cannot acknowledge.

Specifically, TCP shortens the required interval between SYN-ACK (connection request acknowledgements) retransmissions. TCP retransmits SYN-ACKS when they are not answered. As a result, the allotted number of retransmissions is consumed more quickly and the unacknowledgeable connection request is discarded faster.

When enabled, the system monitors the connections maintained by TCP and starts the SYN attack flooding protection when the any of the following conditions, symptomatic of SYN flooding, are found:

- The total number of connections in the half-open (SYN-RCVD) state exceeds the value of **TcpMaxHalfOpen**
- The number of connections that remain in the half-open (SYN-RCVD) state even after a connection request has been retransmitted exceeds the value of **TcpMaxHalfOpenRetried**
- The number of connection requests the system refuses exceeds the value of **TcpMaxPortsExhausted**. The system must refuse all connection requests when its reserve of open connection ports runs out.

4.8.2.2 Check Point Protections Against a SYN Flood Attack

We look at Check Point as a simple proxy to the victim server. This is shown below in Figure 5.

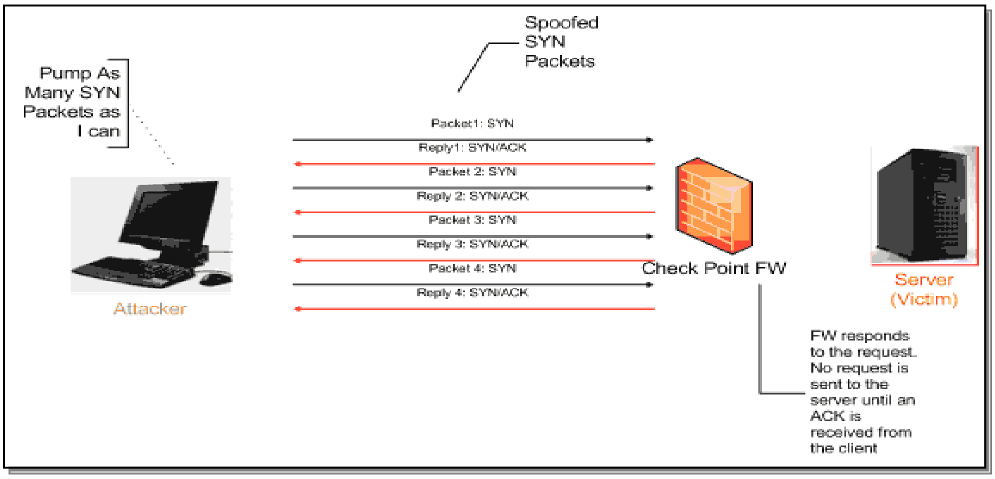


Figure 5. Check Point firewall acting as a proxy.

In this scenario Check Point acts a proxy to the server and responds to all the requests sent to the server. A request is forwarded to the server only if there is a corresponding ACK. The drawback of this configuration is that normally a perimeter firewall is very heavily loaded and this configuration will induce further load on it. The advantage is that the server will always be free to only take legitimate connections.

As we look at Check Point preventing a SYN Flood attack while residing in a transparent proxy configuration. This is shown below in Figure 6.

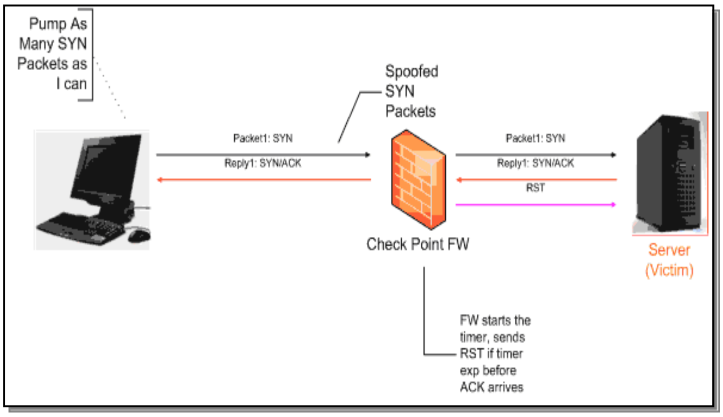


Figure 6. Check Point in transparent mode.

Here Check Point passes all the connections, irrespective of whether they are legitimate or not, to the server but also starts a timer once it sees an ACK/SYN from the server. If there is no corresponding ACK from the Client and the timer expires, the firewall will send a RST to the server thereby preventing its queue from overflowing with illegitimate connections. The advantage of this configuration is that load on firewall is reduced considerably as compared to previous configuration. The drawback, however, is that now the server sees all the connection attempts.

4.9 Bots and Botnets

When computers get infected with malware bots, they could be included to a network of infected computers, forming botnets. These botnets will be orchestrated by a command and control center that instructs them on specific malicious actions. A computer infected with a malware bot or virus can spread the same in their intranet, creating massive botnets. In most cases, the users of these computers are not aware that theirs is a part of a botnet, performing malicious activities.

Botnets are created to perform malicious activities such as Distributed Denial of Service (DDoS) attacks, phishing scams, spam emails, ransomware, click fraud and a lot more.

In most cases, computers become infected and turn into botnets because of a weak end-point security system. This can be taken care of by having the virus and malware programs and definitions updated and patched. Also, users of these computers should be educated on the perils of opening unknown attachments and clicking on suspicious executables.4.10 What is a Bot?

A "bot" is a type of malware that allows an attacker to take control over an affected computer. Also known as “Web robots”, bots are usually part of a network of infected machines, known as a “botnet”, which is typically made up of victim machines that stretch across the globe.

Since a bot infected computer does the bidding of its master, many people refer to these victim machines as “zombies.” The cybercriminals that control these bots are called botherders or botmasters**.**

Some botnets might have a few hundred or a couple thousand computers, but others have tens and even hundreds of thousands of zombies at their disposal. Many of these computers are infected without their owners' knowledge. Some possible warning signs? A bot might cause your computer to slow down, display mysterious messages, or even crash.

4.10.1 How Bots Work

Bots sneak onto a person's computer in many ways. Bots often spread themselves across the Internet by searching for vulnerable, unprotected computers to infect. When they find an exposed computer, they quickly infect the machine and then report back to their master. Their goal is then to stay hidden until they are instructed to carry out a task.

After a computer is taken over by a bot, it can be used to carry out a variety of automated tasks, including the following:

Sending	**Stealing**	**DoS** (Denial of Service)	**Clickfraud**
They send - spam - viruses -spyware	They steal personal and private information and communicate it back to the malicious user: - credit card numbers - bank credentials - other sensitive personal information	Launching denial of service (DoS) attacks against a specified target. Cybercriminals extort money from Web site owners, in exchange for regaining control of the compromised sites. More commonly, however, the systems of everyday users are the targets of these attacks -- for the simple thrill of the botherder.	Fraudsters use bots to boost Web advertising billings by automatically clicking on Internet ads.

4.10.2 Protect Against Bots

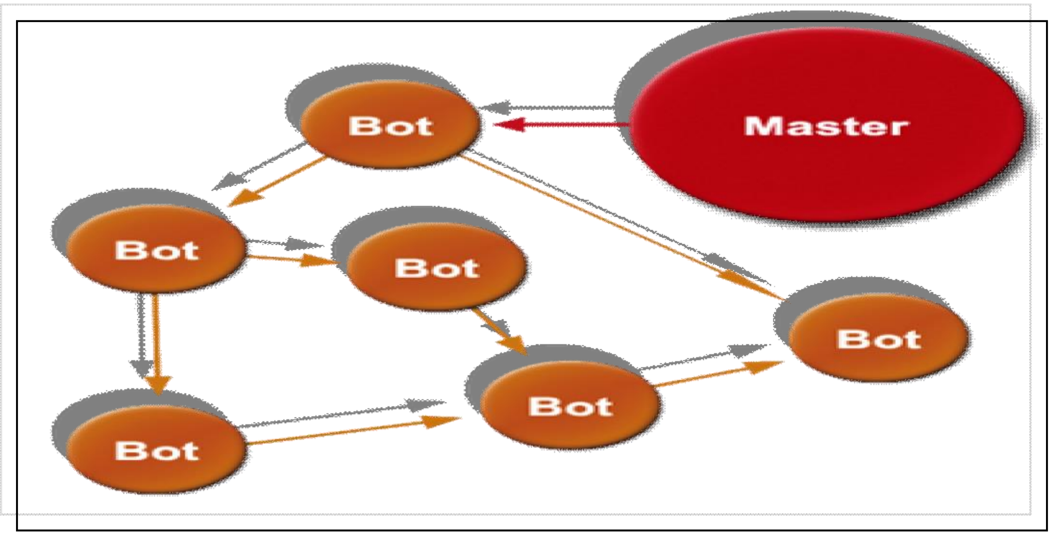
To safeguard against malicious bots, security experts at Symantec offer the following advice:

1. Install top-rated security software.
2. Configure your software's settings to update automatically.
3. Increase the security settings on your browser.
4. Limit your user rights when online.
5. Never click on attachments unless you can verify the source.

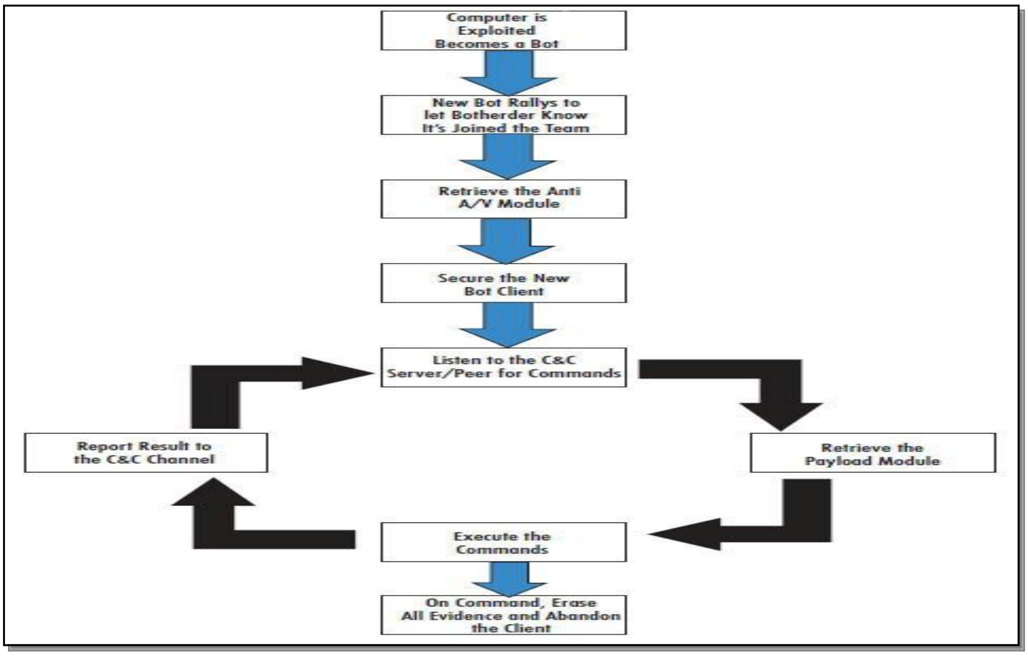
6. Ensure that your system is patched with the most current Microsoft Windows Update.
7. Set your computer's security settings to update automatically, toensure you always have the most current system patches.

4.11 Botnet? What is it? How it works?

A Botnet consists of a Bot server connected to one or more Bot clients. This set of zombie machines (infected PC's) are used in a network to create a more powerful and sophisticated invasion technique then the one's knew before. Each Bot can distribute orders and commands from the Bot Herder to others PC's that come in contact in a certain way with this PC. This leads to the exponentially grow characteristic of Botnets.



4.11.1 Life cycle of a Botnet


Computer is Exploited Becomes a Bot
New Bot Rallys to let Botherder Know It's Joined the Team
Retrieve the Anti A/V Module
Secure the New Bot Client
Listen to the C&C Server/Peer for Commands
Retrieve the Payload Module
Execute the Commands
Report Result to the C&C Channel
On Command, Erase All Evidence and Abandon the Client

4.11.2Schematic time line of a Botnet

- Initial setup of configuration settings of the Bot parameters such as infection vectors, payload, stealth, C&C details
- Register a dynamic DNS (DDNS)
- Register a static IP
- Bot Herder infect PC's with the Bot(s)
- Bot propagates the infection according to the configuration settings
- Bot scans for vulnerabilities that it may encounter
- Idle
- Performs actions received by other Bots above it in the chain of command
- Bot dies:
- Bot may be taken over by another Botnet
- The owner of an infected PC with a Bot realizes the PC is a zombie so it kills the Bot.
- The chain of command may be compromised above the level.

This invasion technique has evolved not only to an illegal way of profit, but also to a way of violating people's information privacy privilege. What have been Botnets being used for? Is the whole concept of Botnet Evil? What actions are being taken to control this terrible plague? On the following sections, this article will discuss how has this threat being used (mainly as one effective malicious way of breaking into data integrity, availability and confidentialityof a computer network) and ways to detain it.

4.12 Steps to Lead Smurf Attack

A smurf attack is a type of denial of service attack in which a system is flooded with spoofed ping messages. This creates high computer network traffic on the victim’s network, which often renders it unresponsive.

Smurfing takes certain well-known facts about Internet Protocol and Internet Control Message Protocol (ICMP) into account. ICMP is used by network administrators to exchange information about network state, and can also be used to ping other nodes to determine their operational status. The smurf program sends a spoofed network packet that contains an ICMP ping. The resulting echo responses to the ping message are directed toward the victim’s IP address. Large number of pings and the resulting echoes can make the network unusable for real traffic.

The following steps lead to a smurf attack:

1. Huge numbers of ICMP requests are sent to the victim's IP address
2. The source destination IP address is spoofed

3. The hosts on the victim's network respond to the ICMP requests
4. This creates a significant amount of traffic on the victim’s network, resulting in consumption of bandwidth and ultimately causing the victim’s server to crash.

To prevent a smurf attack, individual hosts and routers can be configured to be non-responsive to external ping requests or broadcasts. Routers can also be configured to ensure that packets directed to broadcast addresses are not forwarded.

4.13 How to Protect Yourself

The Smurf Attack sounds cute but poses real risks if servers are overwhelmed. Disabled IP broadcasting and reliable detection tools help limit the chance and impact of this attack. Here are a couple of steps to for Smurf attack mitigation:

- Make sure to block directed broadcast traffic coming into the network
- Configure hosts and routers not to respond to ICMP echo requests.

A variation to the Smurf attack is the Fraggle attack. The attack is essentially the same as the Smurf attack but instead of sending an ICMP echo request to the direct broadcast address, it sends UDP packets. For the Fraggle attack, it is the same mitigation process.

4.14 Flooding

Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host is memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

Flooding is a simple routing technique in computer networks where a source or node sends packets through every outgoing link.

Flooding, which is similar to broadcasting, occurs when source packets (without routing data) are transmitted to all attached network nodes. Because flooding uses every path in the network, the shortest path is also used. The flooding algorithm is easy to implement.

Network routing data is not initially included in data packets. A hop count algorithm is used to track network topology, or visited network routes. A packet tries to access all available network routes and ultimately reaches its destination, but there is always the potential for packet duplication. Hop count and some selective flooding techniques are used to avoid communication delay and duplication. Flooding is also used as a denial of service attack by flooding network traffic to bring down a network service. The service is flooded with many incomplete server connection requests. Due to the number of flooded requests, the server or host is not able to process genuine requests at the same time. A flooding attack fills the server or host memory buffer; once it is full, further connections cannot be made, which results in denial of service.

4.15 Let Us Sum Up

While there have been instances where DoS attackers demand payment from victims to end the attacks, financial profit is not usually the motive behind this type of attack. In many cases, the attackers wish to cause harm to the organization or individual targeted in the attack; in other cases, the attackers are simply attempting to sabotage the victim, causing the greatest damage or inconvenience to the greatest number of victims. When a perpetrator of a DoS attack is identified, the reasons for an attack may also be revealed.

Many high-profile DoS attacks are actually distributed attacks, meaning the attack traffic is directed from multiple attack systems. While DoS attacks originating from a single source can be easier to mitigate because defenders can block network traffic from the offending source, attacks directed from multiple attacking systems are far more difficult to detect and defend against because it can be difficult to differentiate legitimate traffic from malicious traffic and filter malicious packets when they are sent from all over the internet.

4.16 Self Assessment Questions

1. What Is Denial-of-Service?

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

2. Discuss about Smurf Attack.

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

3. What is a Distributed DoS?

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

4. What areBot and Botnets?

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

5. What you mean by Flooding and explain it?

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
…………………………………………………………………………………...…………

4.17 Model Questions

1. Discuss about different types of DoS Attacks?
2. What is Bot and how its work?
3. Discuss about the SYN Flood Attacks.
4. What is Smurf Attack and how to Lead Smurf Attack?
5. How to Protect Against Smurf Attacks?
6. Write the steps how to protect yourself.

4.18 References & Further Readings

1. Symantec Corporation Internet Security Threat Report 2014, Volume 19, 2013 Trends, Volume 19, Published April 2014.
2. KhushbooSawant et al Int. Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 4, Issue 5(Version 6), May 2014, pp.110-115.
3. https://us.norton.com/botnet.
4. https://www.symantec.com/connect/articles/demystifying-denial-service-attacks-part-one.

Answer of Self Assessment Questions (Unit-4)

1. **What Is Denial-of-Service?**
   In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. It shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.
2. **Discuss about Smurf Attack.**
   A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service. The attacker uses a program called Smurf to cause the attacked part of a network to become inoperable. The exploit of smurfing, as it has come to be known, takes advantage of certain known characteristics of the Internet

Protocol (IP) and the Internet Control Message Protocol (ICMP). The ICMP is used by network nodes and their administrators to exchange information about the state of the network. ICMP can be used to ping other nodes to see if they are operational. An operational node returns an echo message in response to a ping message.

3. What is a Distributed DoS?

A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

4. What are Bot and Botnets?

A bot is a computer that has been compromised through a malware infection and can be controlled remotely by a cybercriminal. The cybercriminal can then use the bot (also known as a zombie computer) to launch more attacks, or to bring it into a collection of controlled computers, known as a botnet.

Short for "robot," the term "bot" originally had a positive connotation, especially in Internet Relay Chat circles. These bots were programs that were designed to run as a user in the various chat rooms. They could proctor a room, booting out people who used foul language, or referee a trivia game, giving out point and declaring the winner.

5. What you mean by Flooding and explain it?

Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

❑❑❑

Block

3 HACKING WEB APPLICATIONS AND WIRELESS NETWORKS

UNIT-1 Web Application Hacking

Unit Structure

1.0 Introduction

Web application hacks refer to attacks on applications themselves, as opposed to the web server software upon which these applications run. Web application hacking involves many of the same techniques as web server hacking, including input-validation attacks, source code disclosure attacks, and so on. The main difference is that the attacker is now focusing on custom application code and not on off-the-shelf server software. As such, the approach requires more patience and sophistication. We will outline some of the tools and techniques of web application hacking in this section.

1.1 Learning Objective

After learning this unit you should be able to

- Know about the assessment of web applications.
- Identify the Web Server Vulnerabilities.
- Know about different type of Web Servers.
- Study about types of attacks against Web Servers
- Know about Web Server attack Tools.
- Study about how to avoid Attacks on Web Server.
- Know about types of Web Application Vulnerabilities.
- How to protect against Google Hacking.
- Understand Virus Detection Methods of Web Application Threats.
- Know about different types of Authentication.

1.2 Web Application Assessment

Once the target application content has been crawled and thoroughly analysed, the attacker will typically turn to more in-depth probing of the main features of the application. The ultimate goal of this activity is to thoroughly understand the architecture and design of the application, pinpoint any potential weak points, and logically break the application in any way possible.

To accomplish this goal, each major component of the application will be examined from an unauthenticated point of view as well as from the authenticated perspective if appropriate credentials are known (for example, the site may permit free registration of new users, or perhaps the attacker has already gleaned credentials from crawling the site). Web application attacks commonly focus on the following features:

- Authentication
- Session management
- Database interaction
- Generic input validation

- Application logic

We will discuss how to analyse each of these features in the upcoming units. Because many of the most serious web application flaws cannot be analysed without the proper tools, we begin with an enumeration of tools commonly used to perform web application hacking, including: Browser plug-ins, Free tool suites, Commercial web application scanners.

1.3 Browser Plug-ins

Browser plug-ins allows you to see and modify the data you send to the remote server in real time as you navigate the website. These tools are useful during the discovery phase, when you're trying to figure out the structure and functionality of the web application, and they are invaluable when you're trying to confirm vulnerabilities in the verification phase.

The concept behind browser plug-in security tools is ingenious and simple: install a piece of software into the web browser that monitors requests as they are sent to the remote server. When a new request is observed, pause it temporarily, show the request to the user, and let them modify it before it goes out on the wire. As an attacker, these tools are invaluable for identifying hidden form fields, modifying query arguments and request headers, and inspecting the response from the remote server.

The vast majority of security plug-ins are developed for the Mozilla Firefox browser, which provides an easy mechanism to create cross-platform, feature-rich plug-ins. For Internet Explorer, security tool developers have focused on proxy-based tools.

1.4 Web Server Vulnerabilities

A web server is a program that stores files (usually web pages) and makes them accessible via the network or the internet. A web server requires both hardware and software. Attackers usually target the exploits in the software to gain authorized entry to the server. Let's look at some of the common vulnerabilities that attackers take advantage of.

- **Default settings:** These settings such as default user id and passwords can be easily guessed by the attackers. Default settings might also allow performing certain tasks such as running commands on the server which can be exploited.
- **Mis-configuration of operating systems and networks:** certain configuration such as allowing users to execute commands on the server can be dangerous if the user does not have a good password.

- **Bugs in the operating system and web servers:** discovered bugs in the operating system or web server software can also be exploited to gain unauthorized access to the system.

In additional to the above-mentioned web server vulnerabilities, the following can also led to unauthorized access

- **Lack of security policy and procedures:** lack of a security policy and procedures such as updating antivirus software, patching the operating system and web server software can create security loop holes for attackers.

1.5 Types of Web Servers

The following is a list of the common web servers

- **Apache** – This is the commonly used web server on the internet. It is cross platform but is it's usually installed on Linux. Most PHP websites are hosted on Apache servers.
- **Internet Information Services (IIS)** – It is developed by Microsoft. It runs on Windows and is the second most used web server on the internet. Most asp and aspx websites are hosted on IIS servers.
- **Apache Tomcat** – Most Java server pages (JSP) websites are hosted on this type of web server.
- **Other web servers** – These include Novell's Web Server and IBM's Lotus Domino servers.

1.6 Types of Attacks Against Web Servers

Directory traversal attacks – This type of attacks exploits bugs in the web server to gain unauthorized access to files and folders that are not in the public domain. Once the attacker has gained access, they can download sensitive information, execute commands on the server or install malicious software.

- **Denial of Service Attacks** – With this type of attack, the web server may crash or become unavailable to the legitimate users.
- **Domain Name System Hijacking –** With this type of attacker, the DNS setting are changed to point to the attacker's web server. All traffic that was supposed to be sent to the web server is redirected to the wrong one.
- **Sniffing** – Unencrypted data sent over the network may be intercepted and used to gain unauthorized access to the web server.

- **Phishing** – With this type of attack, the attack impersonates the websites and directs traffic to the fake website. Unsuspecting users may be tricked into submitting sensitive data such as login details, credit card numbers, etc.
- **Pharming** – With this type of attack, the attacker compromises the Domain Name System (DNS) servers or on the user computer so that traffic is directed to a malicious site.
- **Defacement** – With this type of attack, the attacker replaces the organization’s website with a different page that contains the hacker’s name, images and may include background music and messages.

1.6.1 Effects of Successful Attacks

- An organization’s reputation can be ruined if the attacker edits the website content and includes malicious information or links to a porn website
- The web server can be used to install malicious software on users who visit the compromised website. The malicious software downloaded onto the visitor’s computer can be a virus, Trojan or Botnet Software, etc.
- Compromised user data may be used for fraudulent activities which may lead to business loss or lawsuits from the users who entrusted their details with the organization

1.6.2 Web Server Attack Tools

Some of the common web server attack tools include;

- **Metasploit** – this is an open source tool for developing, testing and using exploit code. It can be used to discover vulnerabilities in web servers and write exploits that can be used to compromise the server.
- **MPack** – this is a web exploitation tool. It was written in PHP and is backed by MySQL as the database engine. Once a web server has been compromised using MPack, all traffic to it is redirected to malicious download websites.
- **Zeus** – this tool can be used to turn a compromised computer into a bot or zombie. A bot is a compromised computer which is used to perform internet-based attacks. A botnet is a collection of compromised computers. The botnet can then be used in a denial of service attack or sending spam mails.
- **Neosplit** – this tool can be used to install programs, delete programs, replicating it, etc.

1.6.3 How to Avoid Attacks on Web Server

An organization can adopt the following policy to protect itself against web server attacks.

- Patch management – this involves installing patches to help secure the server. A patch is an update that fixes a bug in the software. The patches can be applied to the operating system and the web server system.
- Secure installation and configuration of the operating system
- Secure installation and configuration of the web server software
- Vulnerability scanning system – these include tools such as Snort, NMap, Scanner Access Now Easy (SANE)
- Firewalls can be used to stop simple DoS attacks by blocking all traffic coming the identify source IP addresses of the attacker.
- Antivirus software can be used to remove malicious software on the server
- Disabling Remote Administration
- Default accounts and unused accounts must be removed from the system
- Default ports & settings (like FTP at port 21) should be changed to custom port & settings (FTP port at 5069)

1.7 Types of Web Application Vulnerabilities

The Open Web Application Security Project Foundation, the not for profit organization that is focused on improving software security, has a list of the top Web application vulnerabilities and what to do about them. Here are 10 of the most common.

1. Invalidated inputs

Definition: Not checking whether text a user types into a field on a website is appropriate for that field.

Problem: Hackers use these fields to type commands that allow them to scan for vulnerabilities and gain access.

What you can do: Validate that each field accepts only those characters that are common for that field (such as numbers for a post code field) and are an appropriate length. Run the inputs against a small library of post codes and addresses to confirm that the information is valid.

2. Broken access control

Definition: Access controls determine what a user can access after logging in to his personal account and blocks access to other accounts.

Problem: About half of all websites have serious access problems because of poor testing during development.

What you can do: Test all possible permutations of what a user may do to try to access information that is not his own.

3. Broken authentication and session management

Definition: After logging into a website with a user name and password, you receive a cookie that works like a hand stamp at a night club, authenticating your identity as you go through the site.

Problem: Sometimes companies will customize authentication, inadvertently allowing hackers to infiltrate sessions and use the ID cookie to access the legitimate user's account.

What you can do: Rely on the built-in authentication schemes in the application; use secured sockets layer (SSL) to encrypt the session.

4. Cross-site scripting

Definition: When a hacker sends commands embedded in queries to a website.

Problem: A hacker types JavaScript into any text field, such as a change-of-address field. When legitimate user types information into that field, the JavaScript is activated, which allows the hacker to take control of the session and grants him all the user's session rights, enabling him to move money or steal credit card numbers.

What you can do: Make sure every text field will accept only those characters and length of characters that are suitable for that field--for example, five numbers in a ZIP code field and five numbers only.

5. Buffer overflow

Definition: Allows an attacker to input more information than the buffer can manage.

Problem: Attacker can take control of application server, gaining access to all the data that the server manages.

What you can do: Move away from C++ programming language, which is most vulnerable, to Java or .Net languages. If you must use C++, use static analysis tools to find overflow vulnerabilities.

6. Injection flaws

Definition: Web applications that use interpreters, specific so-called stake words that are instructions for a database to return specific information, are susceptible to commands written in the middle of a query, thereby changing the nature of the query.

Problem: Hacker can send a specific command in a user name and password field so that instead of accessing one file or account attached to that user name and password, the database is commanded to send back all accounts.

What you can do: Use parameter queries, in which the command and data are separate. Each command is associated with certain files, so that a hacker has no way to manipulate the command.

7. Improper error management

Definition: Purposefully inputting errors into fields to receive an error message or to open up a secure area.

Problem: Error messages contain information about the information that may lie underneath, such as receiving an "access denied" message, which indicates a file is associated with the data the hacker input.

What you can do: Keep track of errors and log users out after three errors. Do not provide specific information about the infrastructure or directory in error messages.

8. Unsecured storage

Definition: Not protecting stored data using encryption, not properly securing the keys for accessing encrypted data, and not using effective randomness for passwords.

Problem: Once a hacker gains access to a system, non-encrypted data is easily accessed or hacker can find unsecured encryption keys to gain access to encrypted data.

What you can do: Do not store data that is not absolutely necessary for the operation of the business, and minimize use of encryption. If encryption is used, store the master secret to open the encryption in two locations (say, a configuration file and an external sever) and assemble it at runtime.

9. Denial of Service

Definition: Sending thousands of queries to a Web server to overload the system, slowing it down or causing it to crash.

Problem: While not an attack meant to steal personal information, the attack is meant to be purely malicious by slowing down a business's online services and commerce.

What you can do: Require users to log on to your site so that you process queries only from legitimate users. Limit the number of queries within a certain time frame per user. After three log-in failures, lock out the user for a certain amount of time to thwart a DNS attack on the log-in app.

10. Insecure configuration management

Definition: Unpatched security flaws on server, use of default passwords or improperly secured passwords, improper file and directory permissions, and others.

Problem: A hacker scans for these vulnerabilities, and if found, gains access to administrative and other sensitive accounts.

What you can do: Create configuration security guidelines that lay out the specific steps that developers and Web operations staff must check off. Removes the debate between staff on how to set up proper configuration.

1.8 IIS Unicode Exploit Explanation

Microsoft Internet Information Server (IIS) versions 4.0 and 5.0 which usually run on Windows NT4 and Windows 2k all have the Unicode extensions installed by default. Unicode allows characters that are not used in the English language to be recognized by Web Servers. The Unicode IIS Exploit allows users to run arbitrary commands on the target web servers. The Unicode extensions loaded on IIS Servers are known to be vulnerable unless they are running the current patches within the server.

1.8.1 Unicode Exploit Usage

The Unicode Exploit is mostly found with Microsoft's IIS, but it don't really matter what Operating System you are using on the machine. The reason why is because The Unicode Exploit is a Web Server specific hole. As long as you're running Microsoft IIS 4.0 or 5.0 Web Server the hole will be exploitable.

1. It can be used when a writeable or executable directory is available; this allows attacks to upload malicious code.

2. Or when a system executable such as cmd.exe or cmd2.exe is available on the root, which doesn’t have an access control listing written to it.

The Microsoft ISS Unicode exploit uses the **H**yper **T**ext **T**ransfer **P**rotocol (HTTP) and malformed URLs to execute arbitrary commands and transverse directories on vulnerable web servers. Unicode exploit uses Unicode representation of a directory delimiter (/) to fool IIS. The reason why this works so well is because you can use it right from your web browsers address bar, the reason why you can do this is because it uses the Hyper Text Transfer Protocol (HTTP). The only thing that the exploit lacks is its program usage. Programs such as the File Transfer Protocol (FTP) or Telnet don’t work very well with this exploit reasoning are because this is a non-interactive exploit.

1.8.2 Patch Management Techniques

Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks, including Ringmaster’s Automated Patch Management, Patch Link Update, and Gibraltar's Ever guard.

1.9 Web Application Threats

Cross-site scripting - Injecting lines of Java Script into web pages. If not defended against, a hacker can submit malicious code through the search bar, for example, or post it in a user comment.

Session Hijacking - Each unique user is assigned a "session" when they log in to a website. Session hijackers will jump into the session of another user, reading information as it passes between the user and the server.

Parameter Manipulation - Websites often pass information from one web page to the next through URL parameters. For example, if you search on Google, your search terms will be passed to the results page through the

URL. A hacker can take advantage of this fact to rewrite these parameters in harmful ways.

Buffer Overflow - A buffer is a small amount of space allotted to store data. If a buffer is overloaded, the extra data will overwrite data in other areas. Hackers have exploited this knowledge to overfill a buffer, than overwrite other data with their own malicious code.

Denial of Service - Denial of Service attacks are simple but effective. They operate by overwhelming a site with requests for information, severely slowing the operation of a website or bringing it down entirely.

SQL Injection - SQL injection works similarly to cross-site scripting; in this case, however, it is malicious SQL statements that are inserted into the site. These statements are intended to manipulate the database in some way - accessing sensitive data, or deleting it entirely, causing major headaches for the owners.

1.9.1 Google Hacking

Google hacking, sometimes, referred to as Google dorking is an information gathering technique used by an attacker leveraging advanced Google searching techniques. Google hacking search queries can be used to identify security vulnerabilities in web applications, gather information for arbitrary or individual targets, discover error messages disclosing sensitive information, and discover files containing credentials and other sensitive data.

The advanced search string crafted by an attacker could be searching for the vulnerable version of a web application, or a specific file-type (.pwd,.sql etc.) in order to further restrict the search. The search can also be restricted to pages on a specific site, or it can search for specific information across all websites, giving a list of sites that contain the information.

1.10 Web Based Countermeasures

- Choose passwords that have at least eight characters
- Passwords should have a combination of lower-and upper-case letters, numbers, special characters, etc.
- Do not use words that can be easily found in a dictionary as passwords
- Do not use public information, such as social security number, credit card number, and ATM card number as passwords
- Never use personal information as passwords
- User names and passwords should be different

1.10.1 About Authentication

Authentication is the process of determining if a user or entity is who he/she claims to be.

In a web application it is easy to confuse authentication and session management. Users are typically authenticated by a username and password or similar mechanism. When authenticated, a session token is usually placed into the user's browser (stored in a cookie). This allows the browser to send a token each time a request is being made, thus performing entity authentication on the browser. The act of user authentication usually takes place only once per session, but entity authentication takes place with every request.

1.10.2 Types of Authentication

As mentioned there are principally two types of authentication and it is worth understanding the two types and determining which you really need to be doing.

User Authentication is the process of determining that a user is who he/she claims to be.

Entity authentication is the process of determining if an entity is who it claims to be.

Imagine a scenario where an Internet bank authenticates a user initially (user authentication) and then manages sessions with session cookies (entity authentication). If the user now wishes to transfer a large sum of money to another account 2 hours after logging on, it may be reasonable to expect the system to re-authenticate the user!

1.11 Browser Limitations

When reading the following sections on the possible means of providing authentication mechanisms, it should be firmly in the mind of the reader that ALL data sent to clients over public links should be considered "tainted" and all input should be rigorously checked. SSL will not solve problems of authentication nor will it protect data once it has reached the client. Consider all input hostile until proven otherwise and code accordingly.

1.11.1 HTTP Basic

There are several ways to do user authentication over HTTP. The simplest is referred to as HTTP Basic authentication. When a request is made to a URI, the web server returns a HTTP 401 unauthorized status code to the client:

HTTP/1.1 401 Authorization Required

This tells the client to supply a username and password. Included in the 401 status code is the authentication header. The client requests the username and password from the user, typically in a dialog box. The client browser concatenates the username and password using a ":" separator and base 64 encodes the string. A second request is then made for the same resource including the encoded username password string in the authorization headers.

HTTP authentication has a problem in that there is no mechanism available to the server to cause the browser to 'logout'; that is, to discard its stored credentials for the user. This presents a problem for any web application that may be used from a shared user agent.

The username and password of course travel in effective clear-text in this process and the system designers need to provide transport security to protect it in transit. SSL or TLS are the most common ways of providing confidentiality and integrity in transit for web applications.

Entity Authentication

Using Cookies

Cookies are often used to authenticate the user's browser as part of session management mechanisms. This is discussed in detail in the session management section of this unit.

A Note about the Referer

The referer [sic] header is sent with a client request to show where the client obtained the URI. On the face of it, this may appear to be a convenient way to determine that a user has followed a path through an application or been referred from a trusted domain. However, the referrer is implemented by the user's browser and is therefore chosen by the user. Referrers can be changed at will and therefore should never be used for authentication purposes.

Infrastructure Authentication

DNS Names

There are many times when applications need to authenticate other hosts or applications. IP addresses or DNS names may appear like a convenient way to do this. However the inherent insecurities of DNS mean that this should be used as a cursory check only, and as a last resort.

IP Address Spoofing

IP address spoofing is also possible in certain circumstances and the designer may wish to consider the appropriateness. In general use gethostbyaddr () as opposed to gethostbyname (). For stronger authentication you may consider using X.509 certificates or implementing SSL.

Password Based Authentication Systems

Usernames and passwords are the most common form of authentication in use today. Despite the improved mechanisms over which authentication information can be carried (like HTTP Digest and client side certificates), most systems usually require a password as the token against which initial authorization is performed. Due to the conflicting goals that good password maintenance schemes must meet, passwords are often the weakest link in authentication architecture. More often than not, this is due to human and policy factors and can be only partially addressed by technical remedies. Some best practices are outlined here, as well as risks and benefits for each countermeasure. As always, those implementing authentication systems should measure risks and benefits against an appropriate threat model and protection target.

Usernames

While usernames have few requirements for security, a system implement or may wish to place some basic restriction on the username. Usernames that are derivations of a real name or actual real names can clearly give personal detail clues to an attacker. Other usernames like social security numbers or tax ID's may have legal implications. Email addresses are not good usernames for the reason stated in the Password Lockout section.

Storing Usernames and Passwords

In all password schemes the system must maintain storage of usernames and corresponding passwords to be used in the authentication process. This is still true for web applications that use the built in data store of operating systems like Windows NT. This store should be secure. By secure we mean the passwords should be stored in such a way that the application can compute and compare passwords presented to it as part of an authentication scheme, but the database should not be able to be used or read by administrative users or by an adversary who manages to compromise the system. Hashing the passwords with a simple hash algorithm like SHA-1 is a commonly used technique.

Ensuring Password Quality

Password quality refers to the entropy of a password and is clearly essential to ensure the security of the users' accounts. A password of "password" is obviously a bad thing. A good password is one that is impossible to guess. That typically is a password of at least 8 characters, one alphanumeric, one mixed case and at least one special character (not A-Z or 0-9). In web applications special care needs to be taken with meta-characters.

Password Lockout

If an attacker is able to guess passwords without the account becoming disabled, then eventually he will probably be able to guess at least one password. Automating password checking across the web is very simple! Password lockout mechanisms should be employed that lock out an account if more than a preset number of unsuccessful login attempts are made. A suitable number would be five.

Password lockout mechanisms do have a drawback, however. It is conceivable that an adversary can try a large number of random passwords on known account names, thus locking out entire systems of users. Given that the intent of a password lockout system is to protect from brute-force attacks, a sensible strategy is to lockout accounts for a number of hours. This significantly slows down attackers, while allowing the accounts to be open for legitimate users.

Password Aging and Password History

Rotating passwords is generally good practice. This gives valid passwords a limited life cycle. Of course, if a compromised account is asked to refresh its password then there is no advantage.

Automated Password Reset Systems

Automated password reset systems are common. They allow users to reset their own passwords without the latency of calling a support organization.

They clearly pose some security risks in that a password needs to be issued to a user who cannot authenticate himself.

There are several strategies for doing this. One is to ask a set of questions during registration that can be asked of someone claiming to be a specific user. These questions should be free form, i.e., the application should allow the user to choose his own question and the corresponding answer rather than selecting from a set of predetermined questions. This typically generates significantly more entropy.

Sending Out Passwords

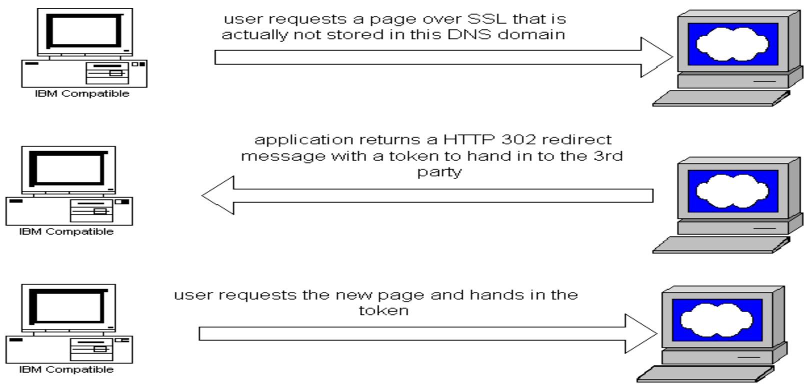
In highly secure systems passwords should only be sent via a courier mechanism or reset with solid proof of identity. Processes such as requiring valid government ID to be presented to an account administrator are common.

Single Sign-On Across Multiple DNS Domains

With outsourcing, hosting and ASP models becoming more prevalent, facilitating a single sign-on experience to users is becoming more desirable.

Many web applications have relied on SSL as providing sufficient authentication for two servers to communicate and exchange trusted user information to provide a single sign on experience. On the face of it this would appear sensible. SSL provides both authentication and protection of the data in transit.

However, poorly implemented schemes are often susceptible to man in the middle attacks. A common scenario is as follows:


IBM Compatible
user requests a page over SSL that is actually not stored in this DNS domain
IBM Compatible
application returns a HTTP 302 redirect message with a token to hand in to the 3rd party
IBM Compatible
user requests the new page and hands in the token

The common problem here is that the designers typically rely on the fact that SSL will protect the payload in transit and assumes that it will not be modified. He of course forgets about the malicious user. If the token consists of a simple username then the attacker can intercept the HTTP 302 redirect in a Man-in-the-Middle attack, modify the username and send the new request. To do secure single sign-on the token must be protected outside of SSL. This would typically be done by using symmetric algorithms and with a pre-exchanged key and including a time-stamp in the token to prevent replay attacks.

1.12 Let Us Sum Up

Web server stored valuable information and are accessible to the public domain. This makes them targets for attackers. The commonly used web servers include Apache and Internet Information Service IIS. Attacks against web servers take advantage of the bugs and Misconfiguration in the operating system, web servers, and networks. Popular web server hacking tools include Neosploit, MPack, and ZeuS. A good security policy can reduce the chances of been attacked. As the online world has integrated itself into our lifestyles, web hacking has become an increasingly more visible and relevant threat to global commerce. Nevertheless, despite its cutting-edge allure, web hacking is based on many of the same techniques for penetrating the confidentiality, integrity, and availability of similar technologies that have gone before, and thus mitigating this risk can be achieved by adhering to some simple principles. As you saw in this chapter, one critical step is to ensure that your web platform (that is, the server) is secure by keeping up with patches and best-practice configurations. Finally, we can’t overemphasize the necessity to regularly audit your own web apps. The state of the art in web hacking continues to advance, demanding ongoing diligence to protect against the latest tools and techniques. There is no vendor service pack for custom code!

1.13 Self Assessment Questions

1. How organizations avoid attacks on web server?

....
....
....
....
....
....
....
....
....
....

....

2. Write a short note on IIS Unicode Exploit Explanation.

....

....

....

....

....

....

....

....

....

....

....

3. What is patch management technique?

....

....

....

....

....

....

....

....

....

....

....

....

....

4. Write down web application threats.

....

....

....

....

....

....

....

....

....

....

....

....

....

5. What is password based Entity authentication?

....
....
....
....
....
....
....
....
....
....
....
....

1.14 Model Questions

1. What are the types of web application vulnerabilities?
2. What are the web application threats?
3. What is the Difference between User Authentication and Entity authentication?
4. Explain Types of Attacks Against Web Servers.
5. What is Google Hacking

1.15 References & Further Readings

1. http://www.cgisecurity.com/owasp/html/ch06.html
2. https://en.wikipedia.org/wiki/Internet_Information_Services
3. https://www.computerworlduk.com/tutorial/infrastructure/the-top-10-web-vulnerabilities-and-what-to-do-about-them-424/
4. https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access

UNIT-2 SQL Injection

Unit Structure

2.0 Introduction

SQL injection attacks are simple in nature – an attacker passes string input to an application in hopes manipulating the SQL statement to his or her advantage. The complexity of the attack involves exploiting a SQL statement that may be unknown to the attacker. Open-source applications and commercial applications delivered with source code are more vulnerable since an attacker can find potentially vulnerable statements prior to an attack.

2.1 Learning Objective

After learning this unit you should be able to

- Know about SQL Injection.
- Know about how SQL Injection works.
- Understand different types of SQL Injection techniques.
- Know about categories of SQL injection attack.
- Know about different types of SQLi.
- Study about Automation Tools for SQL Injection.
- Know about how to prevent against SQL Injection Attacks.
- Know about Buffer Overflow Countermeasures.

2.2 SQL Injection Overview

SQL injection is a basic attack used either to gain unauthorized access to a database or to retrieve information directly from the database. The basic principles underlying SQL injection are simple and these types of attacks are easy to execute and master.

Any program or application may be vulnerable to SQL injection including stored procedures executed with a direct database connection, Oracle Forms applications, web applications, etc. Numerous SQL injection vulnerabilities have been found in the standard Oracle Database packages such as DBMS_DATAPUMP, DBMS_REGISTRY, and DBMS**_METADATA (see Oracle Critical Patch Update January 2006).**

Web applications are at highest risk to attack since often an attacker can exploit SQL injection vulnerabilities remotely without any database or application authentication. Web applications using Oracle as a back-end database are more vulnerable to SQL injection attacks than most application developers think. Our application audits have found many web applications vulnerable to SQL injection even though well-established coding standards were in place during development of many of these applications. Function-based SQL injection attacks are of most concern, since these attacks do not require knowledge of the application and can be easily automated.

Fortunately, SQL injection attacks are easy to defend against with simple coding practices. However, every parameter passed to every dynamic SQL statement must be validated or bind variables must be used.

2.3 What are SQL Injections?

An SQL injection is a kind of injection vulnerability in which the attacker tries to inject arbitrary pieces of malicious data into the input fields of an application, which, when processed by the application, causes that data to be executed as a piece of code by the back end SQL server, thereby giving undesired results which the developer of the application did not anticipate. The backend server can be any SQL server (MySQL, MSSQL, ORACLE, and POSTGRESQL etc.)

The ability of the attacker to execute code (SQL statements) through vulnerable input parameters empowers him to directly interact with the back end SQL server, thereby leveraging almost a complete compromise of system in most cases.

2.4 Different Types of SQL Injections

SQL injections can be classified and categorized in different ways, based on the type of data extraction channel, the response received from server, how server responses aid in leveraging the successful exploitation, impact point, etc.

Based on the data extraction channel

- In band or inline
- Out-of-band

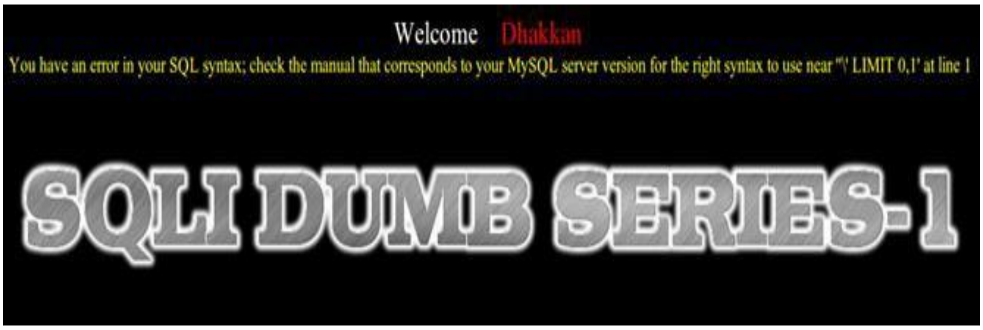
SQL injections that use the same communication channel as input to dump the information back are called inband or inline SQL Injections. This is one of the most common methods, readily explained on the Internet in different posts. For example, a query parameter, if injectable, leads to the dumping of info on the web page.

Injections that use a secondary or different communication channel to dump the output of queries performed via the input channel are referred to as out-of-band SQL injections. For example, the injection is made to a web application and a secondary channel such as DNS queries is used to dump the data back to the attacker domain.

Based on the response received from the server

- Error-based SQL injections
    - Union query type.
    - Double query Injections.
- Blind SQL Injections
    - Boolean-based blind injections.
    - Time based blind injections.

Error-based SQL injections are primarily those in which the SQL server dumps some errors back to the user via the web application and this error aids in successful exploitation. In the image below, the yellow line displays the error. These will be discussed further in this post and in related posts to come.



```
Welcome Dhakkan
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''\' LIMIT 0,1' at line 1
```

Blind SQL injections are those injections in which the backend database reacts to the input, but somehow the errors are concealed by the web application and not displayed to the end users. Or the output is not dumped directly to the screen. Therefore, the name "blind" comes from the fact that the injector is blindly injected using some calculated assumptions and tries.

Based on how the input is treated in SQL query (what data type)

- String-based
- Numeric- or integer based

Based on how the input parameter would be treated in the back end SQL query, an injection can be classified as string- or integer-based.

Based on the degree/order of injections (where the impact happens)

- First-order injections.
- Second-order injections.

The degree or the order of injection identifies the way in which the injection yields the output. If the injection directly delivers the result, it is considered to be a first-order injection, but if the injection input yields no successful result in extraction, but instead impacts some other result which the attacker can take advantage of on some other place/page, it is called a second-order injection. Consider second-order injections similar to stored XSS injections, where the input is stored in the application and later rendered on some other page, thereby impacting that page indirectly because of initial malicious input.

Based on the injection point location

- Injection through user input form fields.
- Injection through cookies.
- Injection through server variables. (headers-based injections)

2.5 Categories of SQL Injection Attacks

There are four main categories of SQL Injection attacks against Oracle databases –

1. SQL Manipulation
2. Code Injection
3. Function Call Injection
4. Buffer Overflows

The first two categories, SQL manipulation and code injection, should be well known to the reader, as these are the most commonly described attacks for all types of databases (including SQL Server, MySQL, PostgreSQL, and Oracle).

SQL manipulation typically involves modifying the SQL statement through set operations (e.g., UNION) or altering the WHERE clause to return a different result. Many documented SQL injection attacks are of this type. The most well known attack is to modify the WHERE clause of the user authentication statement so the WHERE clause always results in TRUE.

Code injection is when an attacker inserts new SQL statements or database commands into the SQL statement. The classic code injection attack is to append a SQL Server EXECUTE command to the vulnerable SQL statement. Code injection only works when multiple SQL statements per database request are supported. SQL Server and PostgreSQL have this capability and it is sometimes possible to inject multiple SQL statements with Oracle.

Oracle code injection vulnerabilities involve the dynamic execution of SQL in PL/SQL.

The last two categories are more specific attacks against Oracle databases and are not well known or documented. In the vast majority of our application audits, we have found applications vulnerable to these two types of attacks.

Function call injection is the insertion of Oracle database functions or custom functions into a vulnerable SQL statement. These function calls can be used to make operating system calls or manipulate data in the database.

SQL injection of buffer overflows is a subset of function call injection. In several commercial and open-source databases, vulnerabilities exist in a few database functions that may result in a buffer overflow. Patches are available for most of these vulnerabilities, but many production databases remain un-patched.

2.6 What Is Vulnerable?

An application is vulnerable to SQL injection for only one reason – end user string input is not properly validated and is passed to a dynamic SQL statement without any such validation. The string input is usually passed directly to the SQL statement. However, the user input may be stored in the database and later passed to a dynamic SQL statement, referred to as a second-order SQL injection. Because of the stateless nature of many web applications, it is common to write data to the database or store it using some other means between web pages. This indirect type of attack is much more complex and often requires in-depth knowledge of the application.

2.7 What Is Not Vulnerable?

SQL Statements using bind variables are generally protected from SQL Injection as the Oracle database will use the value of the bind variable exclusively and not interpret the contents of the variable in any way. PL/SQL and JDBC allow for bind variables. Bind variables should be extensively used for both security and performance reasons.

2.8 Types of SQL Injection (SQLi)

SQL Injection can be used in a range of ways to cause serious problems. By levering SQL Injection, an attacker could bypass authentication, access, modify and delete data within a database. In some cases, SQL Injection can even be used to execute commands on the operating system, potentially allowing an attacker to escalate to more damaging attacks inside of a network that sits behind a firewall.SQL Injection can be classified into three major categories – *In-band SQLi*, *Inferential SQLi* and *Out-of-band SQLi*.

In-band SQLi (Classic SQLi)

In-band SQL Injection is the most common and easy-to-exploit of SQL Injection attacks. In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.

The two most common types of in-band SQL Injection are *Error-based SQLi* and *Union-based SQLi*.

Error-based SQLi

Error-based SQLi is an in-band SQL Injection technique that relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database. While errors are very useful during the development phase of a web application, they should be disabled on a live site, or logged to a file with restricted access instead.

Union-based SQLi

Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

Inferential SQLi (Blind SQLi)

Inferential SQL Injection, unlike in-band SQLi, may take longer for an attacker to exploit; however, it is just as dangerous as any other form of SQL Injection. In an inferential SQLi attack, no data is actually transferred via the web application and the attacker would not be able to see the result of an attack in-band (which is why such attacks are commonly referred to as “blind SQL Injection attacks”). Instead, an attacker is able to reconstruct the database structure by sending payloads, observing the web application’s response and the resulting behavior of the database server.

The two types of inferential SQL Injection are *Blind-boolean-based SQLi* and *Blind-time-based SQLi.*

Boolean-based (content-based) Blind SQLi

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.

Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database, character by character.

Time-based Blind SQLi

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

Out-of-band SQLi

It is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

2.9 How SQL Injection Works

The types of attacks that can be performed using SQL injection vary depending on the type of database engine. **The attack works on dynamic SQL statements**. A dynamic statement is a statement that is generated at run time using parameters password from a web form or URI query string.

Let’s consider a simple web application with a login form. The code for the HTML form is shown below.

```
 <form action=‘index.php’ method="post">
<input type="email" name="email" required="required"/>
<input type="password" name="password"/>
<input type="checkbox" name="remember_me" value="Remember me"/>
<input type="submit" value="Submit"/>
</form>
```

Here,

- The above form accepts the email address, and password then submits them to aPHP file named index.php.
- It has an option of storing the login session in a cookie. We have deduced this from the remember_me checkbox. It uses the post method to submit data. This means the values are not displayed in the URL.

Let’s suppose the statement at the backend for checking user ID is as follows

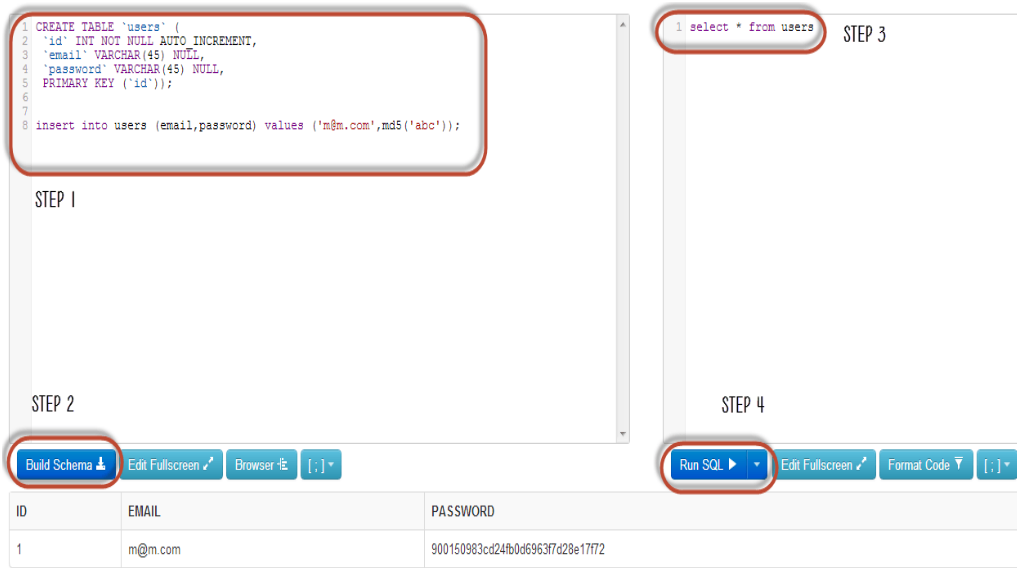
```
SELECT * FROM users WHERE email = $_POST['email'] AND password =
md5($_POST['password']);
```

Here,

- The above statement uses the values of the $_POST[] array directly without sanitizing them.
- The password is encrypted using MD5 algorithm.

We will illustrate SQL injection attack using sqlfiddle. Open the URL http://sqlfiddle.com/in your web browser. You will get the following window.

Note: you will have to write the SQL statements



```
CREATE TABLE `users` (
 `id` INT NOT NULL AUTO_INCREMENT,
 `email` VARCHAR(45) NULL,
 `password` VARCHAR(45) NULL,
 PRIMARY KEY (`id`));


insert into users (email,password) values ('m@m.com',md5('abc'));
```

```
select * from users
```

ID	EMAIL	PASSWORD
1	m@m.com	900150983cd24fb0d6963f7d28e17f72

Step 1) Enter this code in left pane

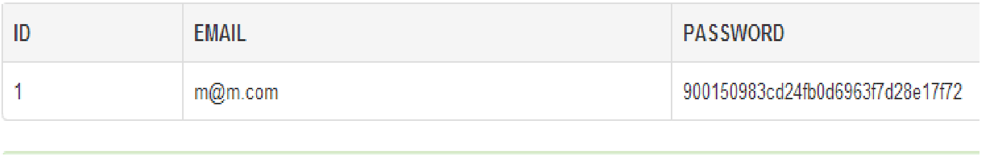
CREATE TABLE `users` (
 `id` INT NOT NULL AUTO_INCREMENT,
 `email` VARCHAR(45) NULL,
 `password` VARCHAR(45) NULL,
 PRIMARY KEY (`id`));
 insert into users (email,password) values ('m@m.com',md5('abc'));

Step 2) Click Build Schema

Step 3) Enter this code in right pane

select * from users;

Step 4) Click Run SQL. You will see the following result



ID	EMAIL	PASSWORD
1	m@m.com	900150983cd24fb0d6963f7d28e17f72

Suppose user supplies **admin@admin.sys** and **1234** as the password. The statement to be executed against the database would be

SELECT * FROM users WHERE email = 'admin@admin.sys' AND password = md5('1234');

The above code can be exploited by commenting out the password part and appending a condition that will always be true. Let’s suppose an attacker provides the following input in the email address field.

xxx@xxx.xxx' OR 1 = 1 LIMIT 1 -- ']

xxx for the password.

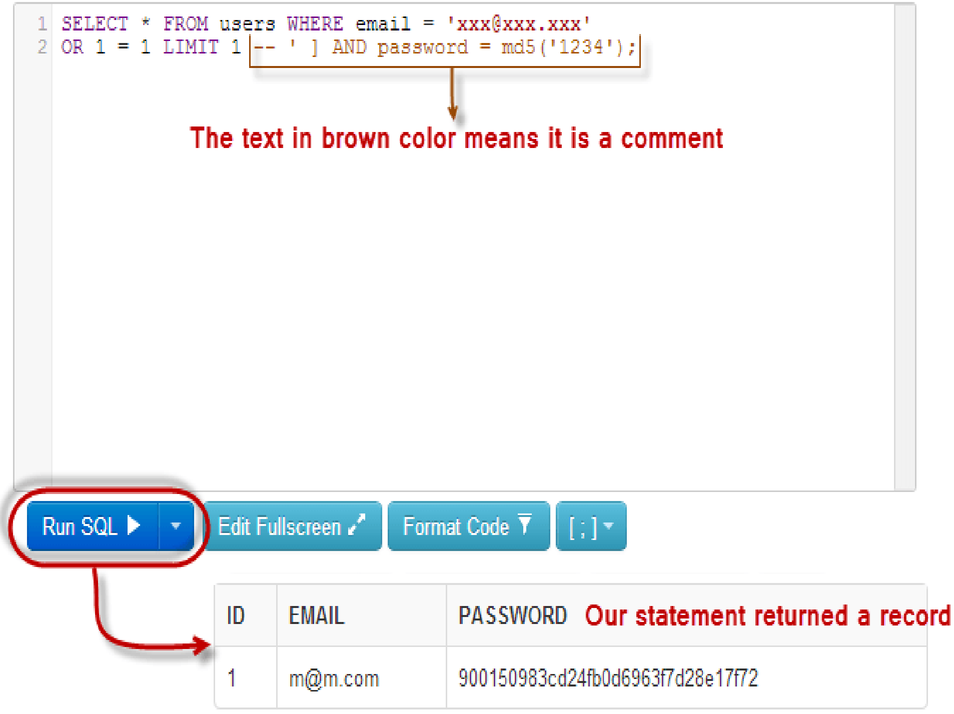
The generated dynamic statement will be as follows.

SELECT * FROM users WHERE email = 'xxx@xxx.xxx' OR 1 = 1 LIMIT 1 -- '] AND password = md5('1234');

Here,

- **xxx@xxx.xxx** ends with a single quote which completes the string quote
- OR 1 = 1 LIMIT 1 is a condition that will always be true and limits the returned results to only one record.
- -- ' AND … is a SQL comment that eliminates the password part.

Copy the above SQL statement and paste it in SQL FiddleRun SQL Text box as shown below



```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx'
OR 1 = 1 LIMIT 1 -- ' ] AND password = md5('1234');
```

The text in brown color means it is a comment

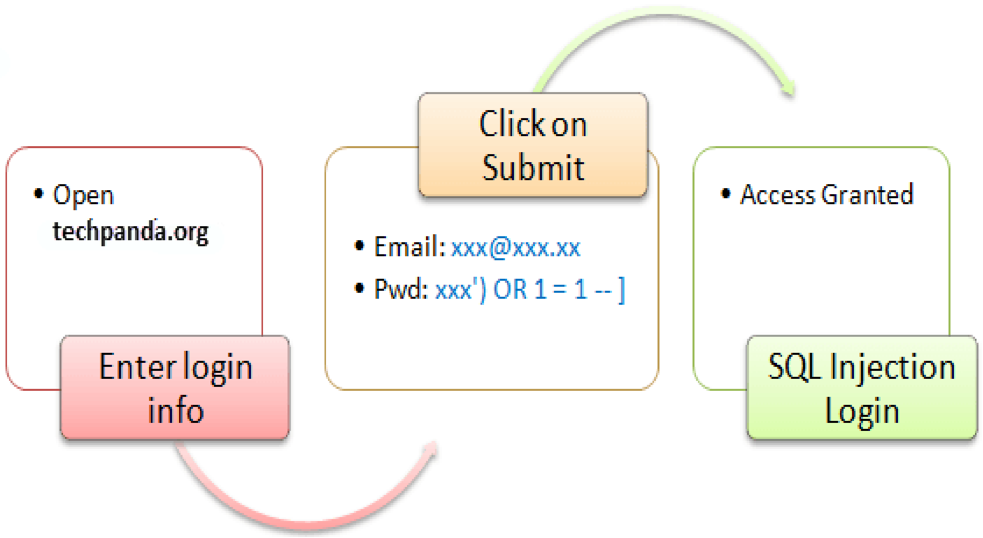
Our statement returned a record

ID	EMAIL	PASSWORD
1	m@m.com	900150983cd24fb0d6963f7d28e17f72

2.10 Hacking Activity: SQL Inject a Web Application

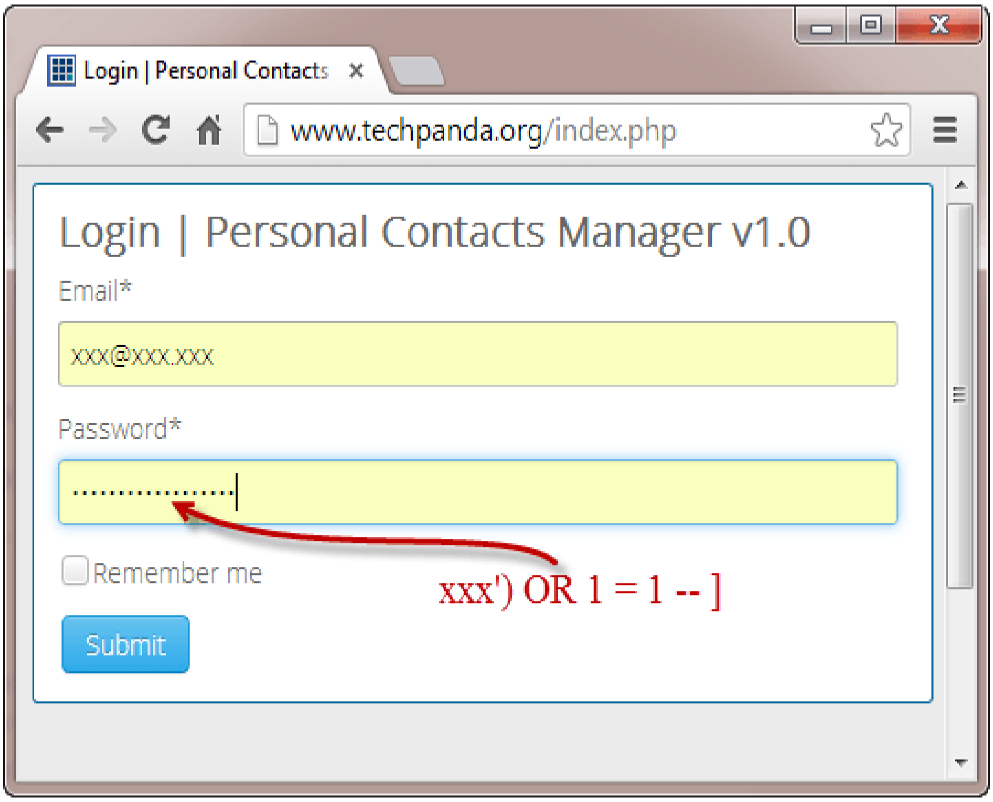
We have a simple web application at http://www.techpanda.org/ **that is vulnerable to SQL Injection attacks for demonstration purposes only.** The HTML form code above is taken from the login page. The application provides basic security such as sanitizing the email field. This means our above code cannot be used to bypass the login.

To get round that, we can instead exploit the password field. The diagram below shows the steps that you must follow



Let's suppose an attacker provides the following input

- Step 1: Enter xxx@xxx.xxx as the email address
- Step 2: Enter xxx') OR 1 = 1 --]



Login | Personal Contacts Manager v1.0

Email*

xxx@xxx.xxx

Password*

••••••••••••••••••

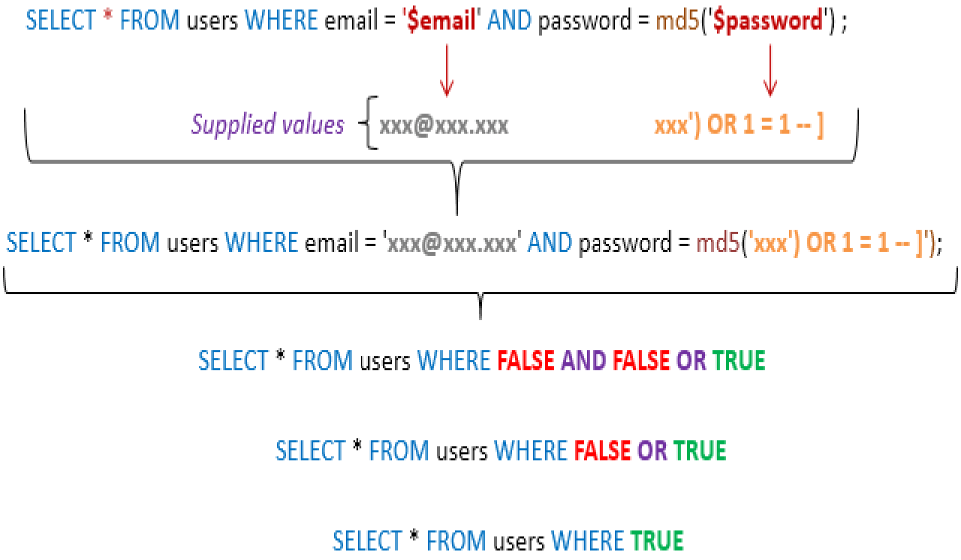
☐ Remember me

- Click on Submit button
- You will be directed to the dashboard

The generated SQL statement will be as follows

SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 --]');

The diagram below illustrates the statement has been generated.



SELECT * FROM users WHERE email = '$email' AND password = md5('$password') ;

xxx@xxx.xxx

xxx') OR 1 = 1 --]

SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 --]');

SELECT * FROM users WHERE FALSE AND FALSE OR TRUE

SELECT * FROM users WHERE FALSE OR TRUE

SELECT * FROM users WHERE TRUE

Here,

- The statement intelligently assumes md5 encryption is used
- Completes the single quote and closing bracket
- Appends a condition to the statement that will always be true

In general, a successful SQL Injection attack attempts a number of different techniques such as the ones demonstrated above to carry out a successful attack.

2.11 SQL Injection Attack Types

SQL Injections can do more harm than just by passing the login algorithms. Some of the attacks include

- Deleting data
- Updating data
- Inserting data
- Executing commands on the server that can download and install malicious programs such as Trojans
- Exporting valuable data such as credit card details, email, and passwords to the attacker's remote server
- Getting user login details etc

The above list is not exhaustive; it just gives you an idea of what SQL Injection

2.10.1 Automation Tools for SQL Injection

In the above example, we used manual attack techniques based on our vast knowledge of SQL. There are automated tools that can help you perform the attacks more efficiently and within the shortest possible time. These tools include

- SQLSmack - http://www.securiteam.com/tools/5GP081P75C.html
- SQLPing 2 - http://www.sqlsecurity.com/downloads/sqlping2.zip?attredirects=0&d=1
- SQLMap - http://sqlmap.org/

2.10.2 How to Prevent against SQL Injection Attacks

An organization can adopt the following policy to protect itself against SQL Injection attacks.

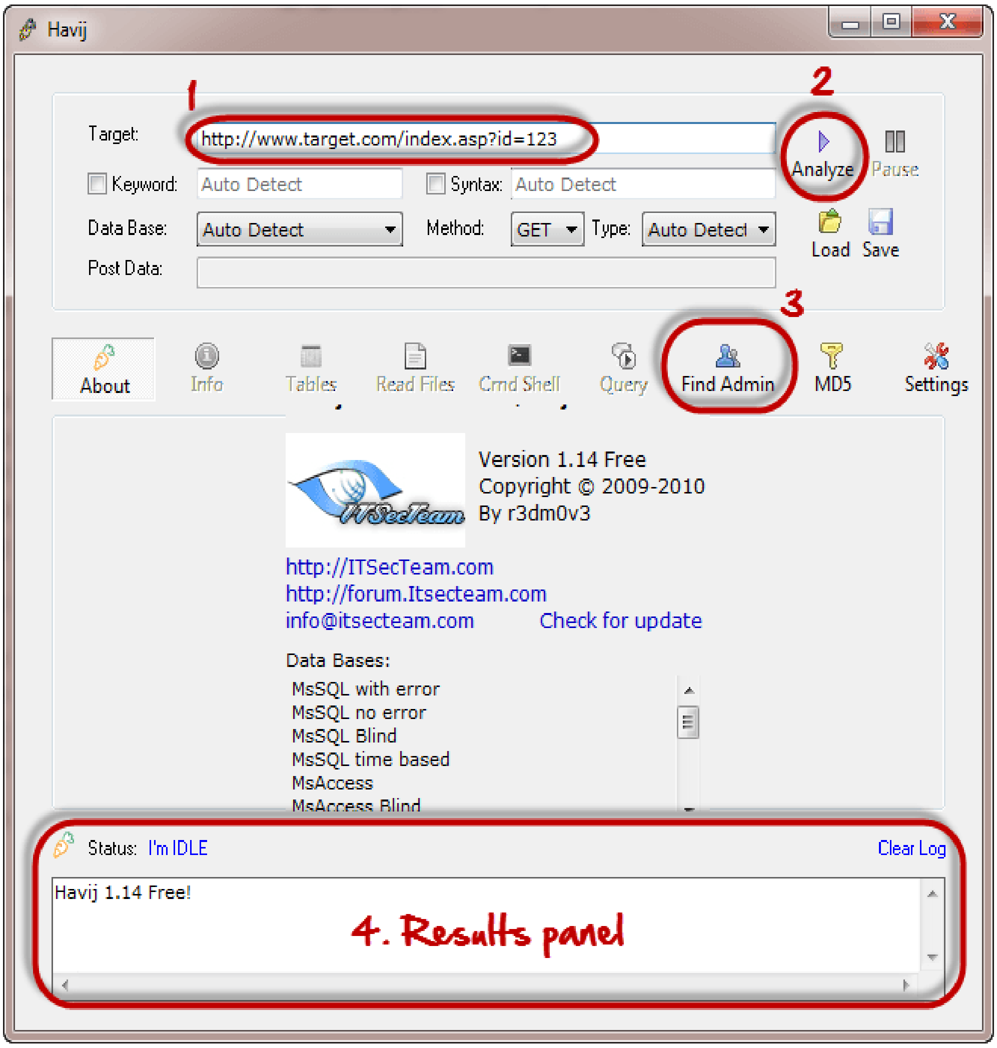
- **User input should never be trusted -** It must always be sanitized before it is used in dynamic SQL statements.
- **Stored procedures** – these can encapsulate the SQL statements and treat all input as parameters.
- **Prepared statements** –prepared statements to work by creating the SQL statement first then treating all submitted user data as parameters. This has no effect on the syntax of the SQL statement.
- **Regular expressions** –these can be used to detect potential harmful code and remove it before executing the SQL statements.
- **Database connection user access rights** –only necessary access rights should be given to accounts used to connect to the database. This can help reduce what the SQL statements can perform on the server.
- **Error messages** –these should not reveal sensitive information and where exactly an error occurred. Simple custom error messages such as "Sorry, we are experiencing technical errors. The technical team has been contacted. Please try again later" can be used instead of display the SQL statements that caused the error.

Hacking Activity: Use Havij for SQL Injection

In this practical scenario, we are going to use Havij Advanced SQL Injection program to scan a website for vulnerabilities.

Note: your anti-virus program may flag it due to its nature. You should add it to the exclusions list or pause your anti-virus software.

The image below shows the main window for Havij.



Version 1.14 Free
Copyright © 2009-2010
By r3dm0v3

http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com Check for update

Data Bases:
MsSQL with error
MsSQL no error
MsSQL Blind
MsSQL time based
MsAccess
MsAccess Blind

```
Havij 1.14 Free!
```

2.11 Buffer Overflow

Buffer overflow problems always have been associated with security vulnerabilities. In the past, lots of security breaches have occurred due to buffer overflow. This article attempts to explain what buffer overflow is, how it can be exploited and what countermeasures can be taken to avoid it.

Knowledge of C or any other high level language is essential to this discussion. Basic knowledge of process memory layout is useful, but not necessary. Also, all the discussions are based on Linux running on x86 platform. The basic concepts of buffer overflow, however, are the same no matter what platform and operating system is used.

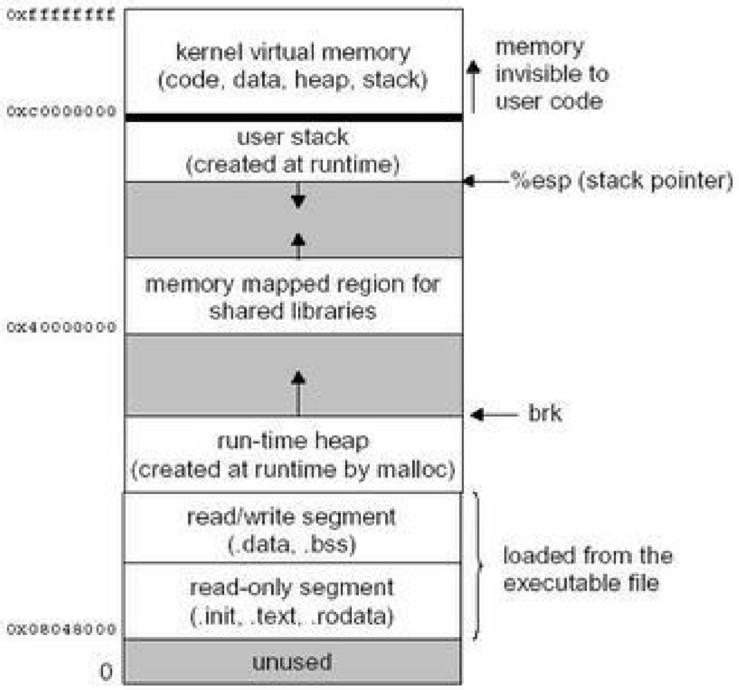
Buffer Overflow: the Basics

A buffer is a contiguous allocated chunk of memory, such as an array or a pointer in C. In C and C++, there are no automatic bounds checking on the buffer, which means a user can write past a buffer. For example:

```
int main ()
{
   int buffer[10];
   buffer[20] = 10;
}
```

The above C program is a valid program, and every compiler can compile it without any errors. However, the program attempts to write beyond the allocated memory for the buffer, which might result in unexpected behavior. Over the years, some bright people have used only this concept to create havoc in the computer industry. Before we understand how they did it, let's first see what a process looks like in memory.

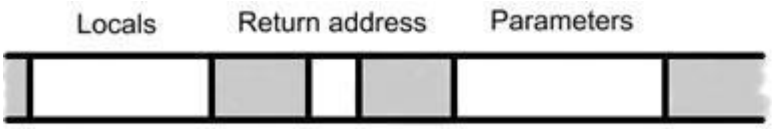
A process is a program in execution. An executable program on a disk contains a set of binary instructions to be executed by the processor; some read-only data, such as printf format strings; global and static data that lasts throughout the program execution; and a brk pointer that keeps track of the malloced memory. Function local variables are automatic variables created on the stack whenever functions execute, and they are cleaned up as the function terminates.



The figure above shows the memory layout of a Linux process. A process image starts with the program's code and data. Code and data consists of the program's instructions and the initialized and uninitialized static and global data, respectively. After that is the run-time heap (created using malloc/calloc), and then at the top is the users stack. This stack is used whenever a function call is made.

The Stack Region

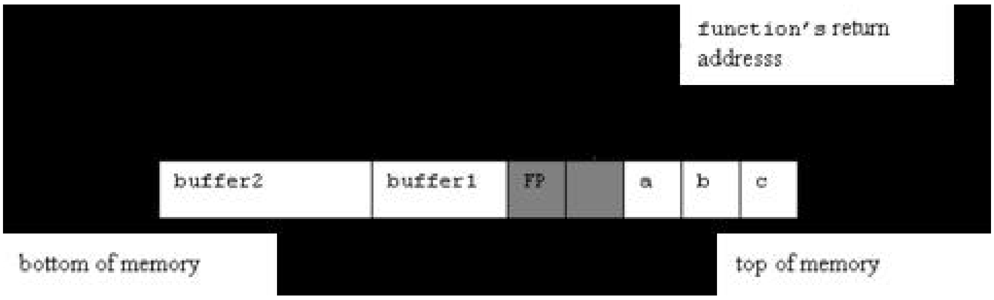
A stack is a contiguous block of memory containing data. A stack pointer (SP) points to the top of the stack. Whenever a function call is made, the function parameters are pushed onto the stack from right to left. Then the return addresses (address to be executed after the function returns), followed by a frame pointer (FP), is pushed on the stack. A frame pointer is used to reference the local variables and the function parameters, because they are at a constant distance from the FP. Local automatic variables are pushed after the FP. In most implementations, stacks grow from higher memory addresses to the lower ones.



This figure depicts a typical stack region as it looks when a function call is being executed. Notice the FP between the local and the return addresses. For this C example,

```
void function (int a, int b, int c) {
   char buffer1[5];
   char buffer2[10];
}
int main() {
  function(1,2,3);
}
```

the function stack looks like:



As you can see, buffer1 takes eight bytes and buffer2 takes 12 bytes, as memory can be addressed only in multiples of word size (four bytes). In addition, an FP is needed to access a, b, c, buffer1 and buffer2 variables. All these variables are cleaned up from the stack as the function terminates. These variables take no space in the executable disk copy.

Buffer Overflow: the Details

Consider another C example:

```
void function (char *str) {
  char buffer[16];
  strcpy (buffer, str);
}
int main () {
 char *str = "I am greater than 16 bytes"; // length of str = 27 bytes
 function (str);
}
```

This program is guaranteed to cause unexpected behavior, because a string (str) of 27 bytes has been copied to a location (buffer) that has been allocated for only 16 bytes. The extra bytes run past the buffer and overwrite the space allocated for the FP, return address and so on. This, in turn, corrupts the process stack. The function used to copy the string is strcpy, which completes no checking of bounds. Using strcpy would have prevented this corruption of the stack. However, this classic example shows that a buffer overflow can overwrite a function's return address, which in turn can alter the program's execution path. Recall that a function's return address is the address of the next instruction in memory, which is executed immediately after the function returns.

2.12 Buffer Overflow Countermeasures

The solutions proposed for buffer overflow problems mainly target the prevention of large-scale system attacks through the loopholes described above. None of the methods described below can claim to prevent all possible attacks. These methods, however, can make it more difficult to access buffer overflows and, hence, destroy the consistency of stacks.

1. **Write secure code:** Buffer overflows are the result of stuffing more code into a buffer than it is meant to hold. C library functions such as strcpy (), strcat (), sprintf () and vsprintf () operate on null terminated strings and perform no bounds checking. gets () is another function that reads user input (into a buffer) from stdin until a terminating newline or EOF is found. The scanf () family of functions also may result in buffer overflows. Hence, the best way to deal with buffer overflow problems is to not allow them to occur in the first place.

Developers should be educated about how to minimize the use of these vulnerable functions.

2. **Stacks execute invalidation:** Because malicious code (for example, assembly instructions to spawn a root shell) is an input argument to the program, it resides in the stack and not in the code segment. Therefore, the simplest solution is to invalidate the stack to execute any instructions. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation. However, the solution is not easy to implement. Although possible in Linux, some compilers (including GCC) use trampoline functions (see Resources) to implement taking the address of a nested function that works on the system stack being executable. A trampoline is a small piece of code created at run-time when the address of a nested function is taken. It normally resides in the stack, in the stack frame of the containing function and thus requires the stack to be executable. However, a version of the Linux kernel that enforces the non executable stack is freely available.
3. **Compiler tools:** Over the years, compilers have become more and more aggressive in optimizations and the checks they perform. Various compiler tools already offer warnings on the use of unsafe constructs such as gets (), strcpy () and the like. For example, this code

   ```
   int main ()
   {
      char *str = (char *)malloc(10);// allocate 10 bytes for str
      gets (str); // reads input from stdin and store into str
   }
   ```

   when compiled with GCC, returns the following warning:

   ```
   /tmp/cc203ViF.o: In function "main":
   /tmp/cc203ViF.o(.text+0x1f): the "gets" function is dangerous and
   should
   not be used.
   ```

   Apart from offering warnings, modern compiler tools change the way a program is compiled, allowing bounds checking to go into compiled code automatically, without changing the source code. These compilers generate the code with built-in safeguards that try to prevent the use of illegal addresses. Any code that tries to access an illegal address is not allowed to execute.

These kind of tools, however, require the source code to be recompiled with a newer compiler. This requirement may be a problem if the application is not open source. Furthermore, it may affect the application's performance to a great extent. In some case, executable size and execution time may increase two-fold.

A patch for GCC that does bounds checking can be found **here**. Recently, however, most of the tools have concentrated on preventing the return address from being overwritten, as most attacks occur this way. **StackShield** is a freely available tool that copies the return address of a function to a safe place (usually to the start of the data segment) at the start of the function. When the function terminates, it compares the two function return address, the one in the stack and the one stored in data segment. In the case of a mismatch, the function aborts immediately.

Because a function also can call another function, it needs to maintain a stack kind of structure for storing return addresses. Another tool available is**StackGuard**, which detects and defeats smash stacking attacks by protecting the return address on the stack from being altered. It places a canary word next to the return address whenever a function is called. If the canary word has been altered when the function returns, then some attempt has been made on the overflow buffers. It responds by emitting an alert and halting.

4. **Dynamic run-time checks:** In this scheme, an application has restricted access in order to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions, or it can ensure that return addresses are not overwritten. One example of such a tool is **libsafe**. The libsafe library provides a way to secure calls to these functions, even if the function is not available. It makes use of the fact that stack frames are linked together by frame pointers. When a buffer is passed as an argument to any of the unsafe functions, libsafe follows the frame pointers to the correct stack frame. It then checks the distance to the nearest return address, and when the function executes, it makes sure that address is not overwritten.

2.13 Let Us Sum Up

SQL Injection is an attack type that exploits bad SQL statements. SQL injection can be used to bypass login algorithms, retrieve, insert, and update and delete data. SQL injection tools include SQLMap, SQLPing, and SQLSmack, etc. A good security policy when writing SQL statement can help reduce SQL injection attacks. All the methods/tools described above are limited in one manner or another. No tool can solve completely the problem of buffer overflow, but they surely can decrease the probability of stack smashing attacks. However, code scrutiny (writing secure code) is still the best possible solution to these attacks. Programmers should be educated to prevent/minimize the use of standard unsafe functions. In addition, no warning given by the compiler should be taken lightly. With time and increasing awareness among developers, buffer overflow problems are predicted to decrease in importance and frequency. Security-related issues are still expected to be around, though, by various other means.

2.14 Self Assessment Questions

1. What do you mean by SQL Injection?

   ....
   ....
   ....
   ....
   ....
   ....
   ....

2. Explain Categories of SQL Injection Attacks.

....
....
....
....
....
....
....

3. What is vulnerable in SQL Injection?

....
....
....
....
....
....
....

4. Write down about Buffer Overflow.

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
…………………………………………………………………………………………

5. What is Boolean-Based (Content-Based) Blind SQLi?

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
…………………………………………………………………………………………

2.15 Model Questions

1. How to Prevent against SQL Injection Attacks?
2. Explain about SQL Injection Attack Types
3. What is the Difference between Vulnerable and Not Vulnerable?
4. Explain Buffer Overflow Countermeasures.
5. What are the automation tools for SQL Injection?

1.16 References & Further Readings

1. https://www.codeproject.com/Articles/9378/SQL-Injection-Attacks-and-Some-Tips-on-How-to-Prev
2. https://dzone.com/articles/sqli-part-3-in-band-and-inferential-sqli
3. https://www.integrigy.com/files/Integrigy_Oracle_SQL_Injection_Attacks.pdf
4. http://ethicalhacking11.blogspot.in/p/sql-injection.html

UNIT-3 Hacking Wireless Networks - I

Unit Structure

3.0 Introduction

Wireless networks are convenient and popular, but poor configuration and encryption leave them open to attack. Hackers can use Wi-Fi vulnerabilities to infiltrate your entire network. Security professionals need to know how to detect, prevent, and counter these kinds of attacks using the latest tools and techniques—the subject of this course with cyber security expert Malcolm Shore. Malcolm covers everything from configuring basic security to understanding how hackers extract passwords, harvest connections at rogue access point, and attack networks via Bluetooth. He also explains how to select the right antennae for testing and introduces some sophisticated Windows and Linux tools to scan for vulnerabilities, including Acrylic, Ekahau, and Wireshark. By the end of this unit, you should be able to ensure protection your wireless connections and gain confidence that your local network is safe to use.

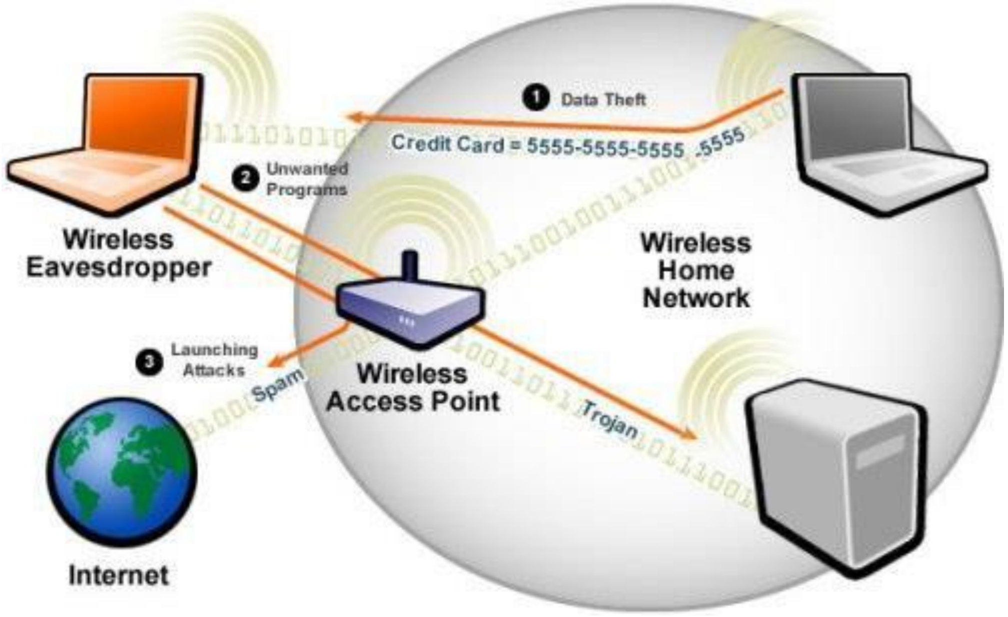
3.1 Learning Objective

After learning this unit you should be able to

- Know about Wireless Network.
- Know about How to access a wireless network.
- Know about different type Wireless Network Authentication.
- Study about WEP Authentication, weakness and cracking.
- Know about WPA, its Weaknesses and Cracking.
- Know about Benefits of using 802.11 Wireless Networks.
- Know about How to secure wireless networks.
- Understand How Can You Use Social Engineering in Your Everyday Life?
- Understand about WLAN Scanners in advice.
- Study about Tools for Detecting Packet Sniffers.

3.2 Overview on Wireless Network

A wireless network is a network that uses radio waves to link computers and other devices together. The implementation is done at the Layer 1 (physical layer) of the OSI model.



3.3 How To Access A Wireless Network?

You will need a wireless network enabled device such as a laptop, tablet, smartphones, etc. You will also need to be within the transmission radius of a wireless network access point. Most devices (if the wireless network option is turned on) will provide you with a list of available networks. If the network is not password protected, then you just have to click on connect. If it is password protected, then you will need the password to gain access.

3.3.1 Wireless Network Authentication

Since the network is easily accessible to everyone with a wireless network enabled device, most networks are password protected. Let’s look at some of the most commonly used authentication techniques.

3.4 WEP

WEP is the acronym for Wired Equivalent Privacy. It was developed for IEEE 802.11 WLAN standards. Its goal was to provide the privacy equivalent to that provided by wired networks. WEP works by encrypting the data been transmitted over the network to keep it safe from eavesdropping.

3.4.1 WEP Authentication

Open System Authentication (OSA) – this methods grants access to station authentication requested based on the configured access policy.

Shared Key Authentication (SKA) – This method sends to an encrypted challenge to the station requesting access. The station encrypts the challenge with its key then responds. If the encrypted challenge matches the AP value, then access is granted.

3.4.2 WEP Weakness

WEP has significant design flaws and vulnerabilities.

- The integrity of the packets is checked using Cyclic Redundancy Check (CRC32). CRC32 integrity check can be compromised by capturing at least two packets. The bits in the encrypted stream and the checksum can be modified by the attacker so that the packet is accepted by the authentication system. This leads to unauthorized access to the network.
- WEP uses the RC4 encryption algorithm to create stream ciphers. The stream cipher input is made up of an initial value (IV) and a secret key. The length of the initial value (IV) is 24 bits long while the secret key can either be 40 bits or 104 bits long. The total length of both the initial value and secret can either be 64 bits or 128 bits long. The lower possible value of the secret key makes it easy to crack it.
- Weak Initial values combinations do not encrypt sufficiently. This makes them vulnerable to attacks.
- WEP is based on passwords; this makes it vulnerable to dictionary attacks.
- Keys management is poorly implemented. Changing keys especially on large networks is challenging. WEP does not provide a centralized key management system.
- The Initial values can be reused

Because of these security flaws, WEP has been deprecated in favour of WPA

3.4.3 WEP Cracking

Cracking is the process of exploiting security weaknesses in wireless networks and gaining unauthorized access. WEP cracking refers to exploits on networks that use WEP to implement security controls. There are basically two types of cracks namely;

- **Passive cracking**– This type of cracking has no effect on the network traffic until the WEP security has been cracked. It is difficult to detect.
- **Active cracking**– This type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking. It is more effective compared to passive cracking.

3.4.4 WEP Cracking Tools

- **Aircrack**– Network sniffer and WEP cracker. Can be downloaded from http://www.aircrack-ng.org/
- **WEPCrack**– This is an open source program for breaking 802.11 WEP secret keys. It is an implementation of the FMS attack. http://wepcrack.sourceforge.net/
- **Kismet**- This can include detector wireless networks both visible and hidden, sniffer packets and detect intrusions. http://www.kismetwireless.net/
- **WebDecrypt**– This tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters. http://wepdecrypt.sourceforge.net/

3.5 WPA

WPA is the acronym for Wi-Fi Protected Access. It is a security protocol developed by the Wi-Fi Alliance in response to the weaknesses found in WEP. It is used to encrypt data on 802.11 WLANs. It uses higher Initial Values 48 bits instead of the 24 bits that WEP uses. It uses temporal keys to encrypt packets.

3.5.1 WPA Weaknesses

- The collision avoidance implementation can be broken
- It is vulnerable to denial of service attacks
- Pre-shares keys use passphrases. Weak passphrases are vulnerable to dictionary attacks.

3.5.2 WPA Cracking

WPA uses a 256 pre-shared key or passphrase for authentications. Short passphrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords. The following tools can be used to crack WPA keys.

- **CowPatty**– this tool is used to crack pre-shared keys (PSK) using brute force attack.

  http://wirelessdefence.org/Contents/coWPAttyMain.htm

- **Cain & Abel**– this tool can be used to decode capture files from other sniffing programs such as Wireshark. The capture files may contain WEP or WPA-PSK encoded frames.

  http://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml

General Attack types

- **Sniffing**– this involves intercepting packets as they are transmitted over a network. The captured data can then be decoded using tools such as Cain & Abel.
- **Man in the Middle (MITM) Attack**– this involves eavesdropping on a network and capturing sensitive information.
- **Denial of Service Attack**– the main intent of this attack is to deny legitimate users network resources. FataJack can be used to perform this type of attack.

3.5.3 Cracking Wireless network WEP/WPA keys

It is possible to crack the WEP/WPA keys used to gain access to a wireless network. Doing so requires software and hardware resources, and patience. The success of such attacks can also depend on how active and inactive the users of the target network are.

We will provide you with basic information that can help you get started. Backtrack is a Linux-based security operating system. It is developed on top of Ubuntu. Backtrack comes with a number of security tools. Backtrack can be used to gather information, assess vulnerabilities and perform exploits among other things.

Some of the popular tools that backtrack has includes;

- Metasploit
- Wireshark
- Aircrack-ng
- NMap
- Ophcrack

Cracking wireless network keys requires patience and resources mentioned above. At a minimum, you will need the following tools

A wireless network adapter with the capability to inject packets (Hardware)

- **Kali Operating System**. You can download it from here https://www.kali.org/downloads/
- **Be within the target network's radius**. If the users of the target network are actively using and connecting to it, then your chances of cracking it will be significantly improved.
- Sufficient **knowledge of Linux based operating systems and working knowledge of Aircrack** and its various scripts.
- **Patience**, cracking the keys may take a bit of sometime depending on a number of factors some of which may be beyond your control. Factors beyond your control include users of the target network using it actively as you sniff data packets.

UNIT-4 Hacking Wireless Networks - II

Unit Structure

Hacking Wireless Network – I and II

4.1 How to Secure Wireless Networks

In minimizing wireless network attacks; an organization can adopt the following policies

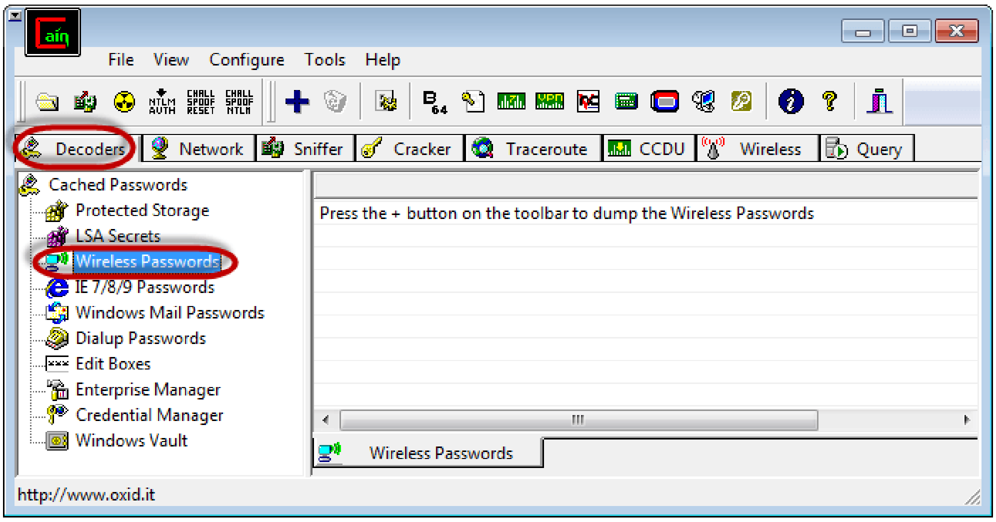
- Changing default passwords that come with the hardware
- Enabling the authentication mechanism
- Access to the network can be restricted by allowing only registered MAC addresses.
- Use of strong WEP and WPA-PSK keys, a combination of symbols, number and characters reduce the chance of the keys been cracking using dictionary and brute force attacks.
- Firewall Software can also help reduce unauthorized access.

Hacking Activity: Crack Wireless Password

In this practical scenario, we are going to use Cain and Abel to decode the stored wireless network passwords in Windows. We will also provide useful information that can be used to crack the WEP and WPA keys of wireless networks.

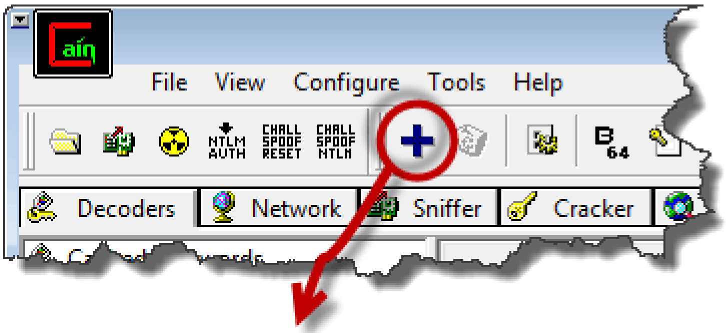
Decoding Wireless network passwords stored in Windows

- Download Cain & Abel from the link provided above.
- Open Cain and Abel



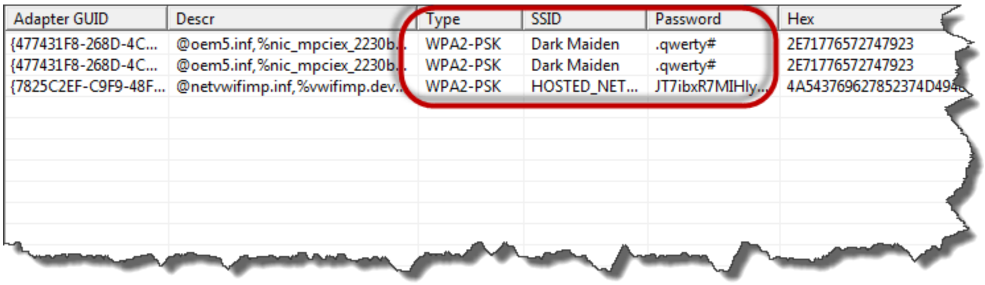
Press the + button on the toolbar to dump the Wireless Passwords

- Ensure that the Decoders tab is selected then click on Wireless Passwords from the navigation menu on the left-hand side
- Click on the button with a plus sign



Click on the plus (+) button

- Assuming you have connected to a secured wireless network before, you will get results similar to the ones shown below



Adapter GUID	Descr	Type	SSID	Password	Hex
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{7825C2EF-C9F9-48F...	@netvwifimp.inf,%vwifimp.dev...	WPA2-PSK	HOSTED_NET...	JT7ibxR7MIHly...	4A543769627852374D494

- The decoder will show you the encryption type, SSID and the password that was used.

4.2 An Introduction to 802.11 (Wi-Fi) Technologies

The WLAN (Wireless Local Area Network) protocol, IEEE 802.11, allows wireless and mobile network access to a network infrastructure. Before the 802.11b protocol (which was coined Wi-Fi) was widely adopted in the early 2000s, to get high speed network access to your LAN you had to be physically connected via a cable. The family of 802.11 protocols is made up of an arrangement of over-the-air modulation techniques that use the same basic principles. The most widely used protocols are the 802.11b, 802.11g and 802.11n for 2.4GHz networks and the 802.11a, 802.11n and 802.11ac for 5GHz networks.

4.3 Benefits of using 802.11 Wireless Networks

Wireless connections can replace wired infrastructure or extend existing networks

For applications in which it is impractical to lay cables or it is too costly, 802.11 Wireless Networks can be used in the following situations:

When connecting two networks in separate buildings with a critical obstacle obstructing you, an 802.11 WLAN connection can be used to avoid purchasing a leased line from a telecommunications vendor providing significant savings.

Temporary 802.11 WLAN networks can be set up instantly reducing deployment times for applications such as conventions.

802.11 WLAN networks do not require the laying of cables in homes and offices where aesthetics are critical.

Mobile computer users can connect to 802.11 WLAN networks in changing locations and always remain connected to the network without being near a network socket or router.

802.11 "Hot Spot" areas can provide internet access for the public in places such as airports, hotels and retail centres.

4.3.1 802.11 Operating Modes

Infrastructure Mode is used when there is at least one Wireless Access Point and client. The client connects to the network through the Access Point to gain internet access.

Ad Hoc Mode is used when wireless clients want to directly communicate with each other without going through an Access Point. This is also called peer-to-peer mode.

4.3.2 Popular 802.11 Standards

802.11a

The 802.11a protocol standard uses the same data link layer protocol and frame format as the original 802.11-1997 standard but instead uses an OFDM air interface for the physical layer. Its operating frequency range is in the 5GHz band and has a maximum bandwidth of 54mbps. Due to the 2.4GHz range becoming overcrowded using the 802.11a standard has a significant advantage. However, the effective range of the 5GHz 802.11a is lower than that of the 802.11b, g and n protocols as, in theory, the signal is more easily absorb by solid objects such as walls due to the smaller wavelength which reduces its penetration. Nevertheless, due to the lack of interference in the 5GHz range, 802.11a often has a similar or even greater range in practice.

802.11b

802.11b was the first widely adopted standard wireless networking products. It has a maximum bandwidth of 11Mbps and uses the same media access method as that of the original 802.11-1997 standard. Working on the 2.4GHz frequency range, 802.11b suffers greatly from interference with other consumer items such as Bluetooth devices, DECT & VoIP Wireless phones, wireless keyboards and mice and also microwave ovens etc.

802.11g

802.11g was the next step on from 802.11b still operating a 2.4GHz but using OFDM based transmission. It has a maximum bandwidth of 54Mbps and is backwards compatible with 802.11b hardware. It was the next industrial standard and was, again, widely adopted for WLAN applications due to the increased data transfer rates. Much similar to 802.11b, 802.11g devices can suffer badly from interference from other 2.4GHz consumer products.

OFDM is enabled at speeds above 20Mbps which greatly increases NLOS (Non-Line-of-Sight) capabilities.

802.11n

802.11n is a revision that improves on the previous standards by adding MIMO (Multiple-In-Multiple-Out) capabilities can operate not just on the 2.4GHz frequency range but also at 5GHz, 40 MHz channels to the physical layer and frame aggregation to the MAC layer. 802.11 is backwards compatible with 802.11a, b and g. OFDM is enabled across the whole speed range which greatly increases NLOS (Non-Line-of-Sight) capabilities.

MIMO uses multiple antennas to intelligently resolve a larger amount of data than possible when using a single antenna. It does this by using SDM (Spatial Division Multiplexing) which uses multiple but independent data streams that are transferred simultaneously inside one channel of bandwidth. This increases the throughput bandwidth as the number of resolved streams is increased.

Doubling the channel size from 20MHz to 40MHz can be enabled on 802.11n compatible equipment which allows for twice the data rate on the physical layer relative to a 20MHz channel.

These two features combined give the 802.11n standard increased bandwidth capabilities when compared to 802.11g at 2.4GHz and 802.11a at 5GHz of up to 600Mbps (in theory) when using 4 spatial streams and a 40MHz channel and an increase in range over previous standards when put in practice. It seems that with 802.11 Wi-Fi chip manufactures applying market pressure to move onto this protocol, 802.11 should become the new standard over the next few years.

802.11ac

802.11ac operates at 5GHz using OFDM based modulation. The specification expects WLAN throughput of at least 1Gbp/s and a single link throughput of at least 500Mbp/s. This is achieved by extending concepts from the 802.11n standard such as wider RF bandwidth (up to 160MHz, mandatory 80MHz), more MIMO spatial streams (up to 8), mulit-user MIMO and high-density modulation (up to 256-QAM).

4.4 IEEE 802.11 Architecture

The difference between a portable and mobile station is that a portable station moves from point to point but is only used at a fixed point. Mobile stations access the LAN during movement.

When two or more stations come together to communicate with each other, they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block.

A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is referred to as an Ad-Hoc Network. An ad-hoc network is a network where stations communicate only peer to peer. There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-Hoc or IBSS networks are characteristically limited both temporally and spatially.

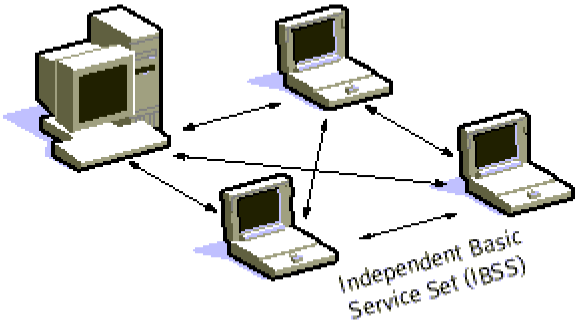


Fig 1: "Adhoc Mode"

When BSS's are interconnected the network becomes one with infrastructure. 802.11 infrastructures have several elements. Two or more BSS's are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points.

Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, the Extended Service Set or ESS. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSS′s transparently to the LLC.

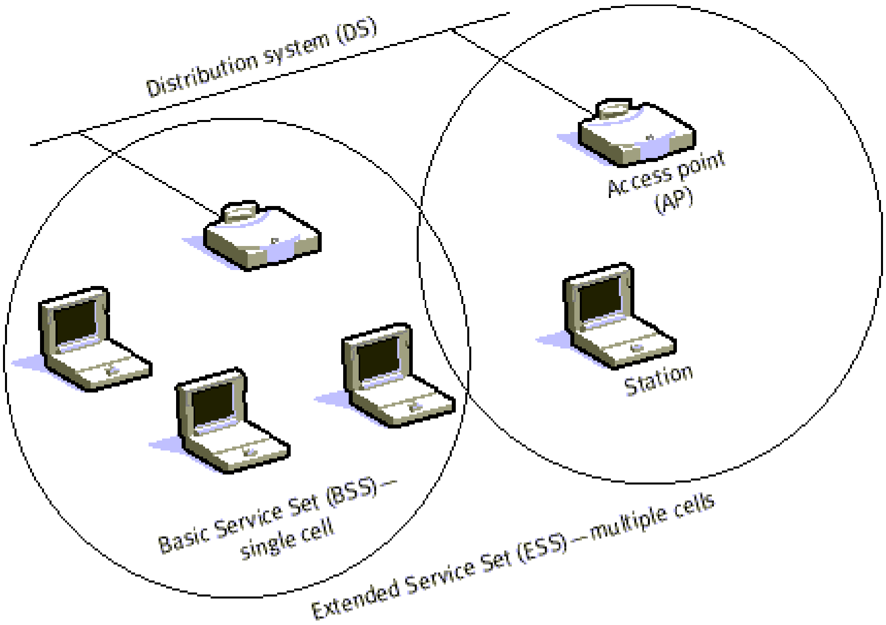

Distribution system (DS)
Access point (AP)
Station
Basic Service Set (BSS)—single cell
Extended Service Set (ESS)—multiple cells

Fig 2: Infrastructure Mode

One of the requirements of IEEE 802.11 is that it can be used with existing wired networks. 802.11 solved this challenge with the use of a Portal. A portal is the logical integration between wired LANs and 802.11. It also can serve as the access point to the DS. All data going to an 802.11 LAN from an 802.X LAN must pass through a portal. It thus functions as bridge between wired and wireless.

The implementation of the DS is not specified by 802.11. Therefore, a distribution system may be created from existing or new technologies. A point-to-point bridge connecting LANs in two separate buildings could become a DS.

While the implementation for the DS is not specified, 802.11 does specify the services, which the DS must support. Services are divided into two sections

1. Station Services (SS)
2. Distribution System Services (DSS).

There are five services provided by the DSS

1. Association
2. Re-association
3. Disassociation
4. Distribution
5. Integration

The first three services deal with station mobility. If a station is moving within its own BSS or is not moving, the stations mobility is termed No-transition. If a station moves between BSS's within the same ESS, its mobility is termed BSS-transition. If the station moves between BSS's of differing ESS's it is ESS transition. A station must affiliate itself with the BSS infrastructure if it wants to use the LAN. This is done by associating itself with an access point. Associations are dynamic in nature because stations move, turn on or turn off. A station can only be associated with one AP. This ensures that the DS always knows where the station is.

Association supports no-transition mobility but is not enough to support BSS-transition. Enter Re-association. This service allows the station to switch its association from one AP to another. Both association and re-association are initiated by the station. Disassociation is when the association between the station and the AP is terminated. This can be initiated by either party. A disassociated station cannot send or receive data. ESS-transition are not supported. A station can move to a new ESS but will have to reinitiate connections.

Distribution and Integration are the remaining DSS's. Distribution is simply getting the data from the sender to the intended receiver. The message is sent to the local AP (input AP), then distributed through the DS to the AP (output AP) that the recipient is associated with. If the sender and receiver are in the same BSS, the input and out AP's are the same. So the distribution service is logically invoked whether the data is going through the DS or not. Integration is when the output AP is a portal. Thus, 802.x LANs are integrated into the 802.11 DS.

Station services are:

1. Authentication
2. De-authentication
3. Privacy
4. MAC Service Data Unit (MSDU) Delivery.

With a wireless system, the medium is not exactly bounded as with a wired system. In order to control access to the network, stations must first establish their identity. This is much like trying to enter a radio net in the military.

Before you are acknowledged and allowed to converse, you must first pass a series of tests to ensure that you are who you say you are. That is really all authentication is. Once a station has been authenticated, it may then associate itself. The authentication relationship may be between two stations inside an IBSS or to the AP of the BSS. Authentication outside of the BSS does not take place.

There are two types of authentication services offered by 802.11. The first is Open System Authentication. This means that anyone who attempts to authenticate will receive authentication. The second type is Shared Key Authentication. In order to become authenticated the users must be in possession of a shared secret. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm. The shared secret is delivered to all stations ahead of time in some secure method (such as someone walking around and loading the secret onto each station).

De-authentication is when either the station or AP wishes to terminate a stations authentication. When this happens the station is automatically disassociated. Privacy is an encryption algorithm, which is used so that other 802.11 users cannot eavesdrop on your LAN traffic. IEEE 802.11 specifies Wired Equivalent Privacy (WEP) as an optional algorithm to satisfy privacy. If WEP is not used then stations are "in the clear" or "in the red", meaning that their traffic is not encrypted. Data transmitted in the clear are called plaintext. Data transmissions, which are encrypted, are called cipher text. All stations start "in the red" until they are authenticated. MSDU delivery ensures that the information in the MAC service data unit is delivered between the medium access control service access points.

4.4.1 Wireless DOS

Despite recent 802.11 security advances, WLANs remain very vulnerable to Denial of Service attacks. While you may not be able to prevent DoS attacks, a WIDS can help you detect when DoS attacks occur and where they come from, so that you can track the intruder down and bring him to justice -- or at least scare him away. This tip offers practical advice on how to recognize and respond to DoS attacks launched against your WLAN.

4.4.2 Wireless Security Lunchtime Learning

Despite recent 802.11 security advances, WLANs remain very vulnerable to denial-of-service (DoS) attacks. While you may not be able to prevent DoS attacks, a wireless intrusion detection system (WIDS) can help you detect when DoS attacks occur and where they come from, so that you can bring the intruder to justice -- or at least scare him away. This tip offers practical advice on how to recognize and respond to DoS attacks launched against your WLAN.

4.5 How DoS Happens?

Most WLAN interference is accidental. While an attacker could use an RF jammer, like a high-powered RF signal generator, there are many less expensive ways to intentionally DoS your WLAN. For example:

802.11 Control frames can be used to "busy out" a channel so that no other station can transmit. Entering this continuous transmit mode is known as a Queensland DoS attack.

- 802.11 Deauthenticate frames can be used to disconnect an individual station, or every station associated with a given AP. Sending a continuous stream of these forged frames is known as a Deauth Flood.
- 802.11 Associate frames consume AP resources by creating entries in the AP's association table. Flooding an AP with Associate frames from random station MAC addresses can make the AP too busy to service real users.
- Similar attacks can be launched using forged 802.1X packets -- for example, 802.1X EAP Logoff Flood, EAP Start Flood, and EAP-of-Death attacks.

These and many other wireless DoS attacks are possible because only 802.11 data frames carry integrity check codes used to detect forged messages. These attacks can be launched using off-the-shelf wireless cards and readily-available shareware or open source tools, like air jack and void11. The attacker just needs to be close enough to your WLAN to capture a little traffic to identify victims.

4.6 WLAN Scanners

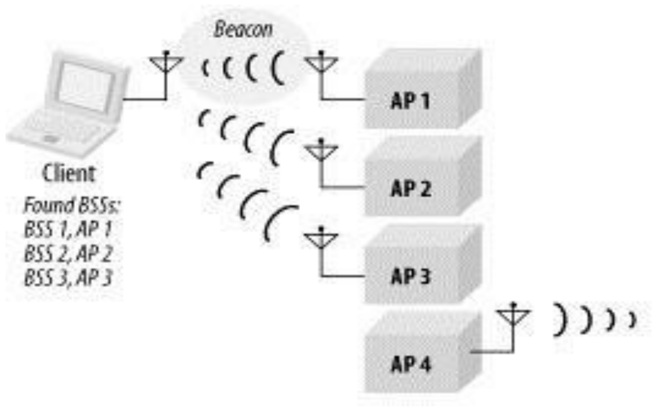
Real-time WLAN information and network analysis. Acrylic Wi-Fi Home is a Free WiFi scanner that displays WiFi access points and shows information of the security mechanisms and obtains generic WiFi passwords thanks to a plugins system. Our WiFi scanner is able to gather information from 802.11/a/b/g/n/ac networks.

As we know before joining any network first client or stations or mobile stations need to find it first. In the wired world, just plugging the cable or jack will find the network. In the wireless world, this is challenging and requires identification of the compatible network before joining process can begin. This identification process of the network is referred as scanning.

Several parameters are needed in the scanning process. These parameters are specified by the user. The few of them are set as default in the WLAN client driver software.

The parameters are BSSType, BSSID, SSID, ScanType, ChannelList, ProbeDelay, MinChannelTime and MaxChannelTime.

WLAN Passive Scanning

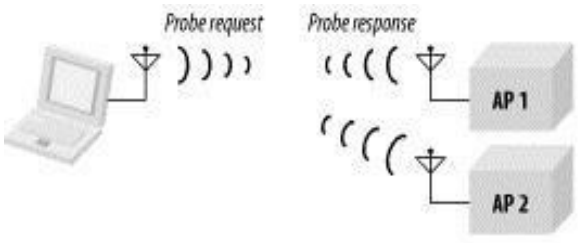


WLAN Passive Scanning

In **Passive Scanning**, WLAN station moves to each channel as per channel list and waits for beacon frames. These frames are buffered and are used to decode and extract information about BSSs.

This passive scanning will save battery power as it does not need to transmit. As shown in the fig-1 WLAN client receives beacon frames from three access points and hence it will declare that it has found only three BSSs.

WLAN Active Scanning



WLAN active scanning

Station plan active role in **Active Scanning**. On each of the channels. Probe request frames are used to obtain responses from the network of choice. In active scanning station finds out network rather than waiting for network to announce its availability to all the stations.

4.7 What is a Wireless Sniffer?

A wireless sniffer is a type of packet analyzer. A packet analyzer (also known as a packet sniffer) is a piece of software or hardware designed to intercept data as it is transmitted over a network and decode the data into a format that is readable for humans. Wireless sniffers are packet analyzers specifically created for capturing data on wireless networks. Wireless sniffers are also commonly referred to as wireless packet sniffers or wireless network sniffers.

Wireless sniffer tools have many uses in commercial IT environments. Their ability to monitor, intercepts, and decode data as it is in transit makes them useful for:

- Diagnosing and investigating network problems
- Monitoring network usage, activity, and security
- Discovering network misuse, vulnerabilities, malware, and attack attempts
- Filtering network traffic
- Identifying configuration issues and network bottlenecks

4.7.1 Wireless Packet Sniffer Attacks

While wireless packet sniffers are valuable tools for maintaining wireless networks, their capabilities make them popular tools for malicious actors as well. Hackers can use wireless sniffer software to steal data, spy on network activity, and gather information to use in attacking the network. Logins (usernames and passwords) are very common targets for attackers using wireless sniffer tools. Wireless network sniffing attacks usually target unsecure networks, such as free WiFi in public places (coffee shops, hotels, airports, etc).

Wireless sniffer tools are also commonly used in “spoofing” attacks. Spoofing is a type of attack where a malicious party uses information obtained by a wireless sniffer to impersonate another machine on the network. Spoofing attacks often target business’ networks and can be used to steal sensitive information or run man-in-the-middle attacks against network hosts.

There are two modes of wireless sniffing: monitor mode and promiscuous mode. In monitor mode, a wireless sniffer is able to collect and read incoming data without sending any data of its own. A wireless sniffing attack in monitor mode can be very difficult to detect because of this. In promiscuous mode, a sniffer is able to read all data flowing into and out of a wireless access point. Since a wireless sniffer in promiscuous mode also sniffs outgoing data, the sniffer itself actually transmits data across the network. This makes wireless sniffing attacks in promiscuous mode easier to detect. It is more common for attackers to use promiscuous mode in sniffing attacks because promiscuous mode allows attackers to intercept the full range of data flowing through an access point.

4.7.2 Preventing Wireless Sniffer Attacks

There are several measures that organizations should take to mitigate wireless packet sniffer attacks. First off, organizations (and individual users) should refrain from using insecure protocols. Commonly used insecure protocols include basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be used in place of their insecure alternatives when possible. Secure protocols ensure that any information transmitted will automatically be encrypted. If an insecure protocol must be used, organizations themselves need to encrypt any data that will be sent using that protocol. Virtual Private Networks (VPNs) can be used to encrypt internet traffic and are a popular tool for organizations today.

In addition to encrypting information and using secure protocols, companies can prevent attacks by using wireless sniffer software to sniff their own networks. This allows security teams to view their networks from an attacker’s perspective and discover sniffing vulnerabilities and attacks in progress. While this method will not be effective in discovering wireless network sniffers in monitor mode, it is possible to detect sniffers in promiscuous mode (the preferred mode for attackers) by sniffing your own network.

4.7.3 Tools for Detecting Packet Sniffers

Wireless sniffer software programs frequently include features such as intrusion and hidden network detection for helping organizations discover malicious sniffers on their networks. In addition to using features that are built into wireless sniffer tools, there are many aftermarket tools available that are designed specifically for detecting sniffing attacks. These tools typically perform functions such as monitoring network traffic or scanning network cards in promiscuous mode to detect wireless network sniffers. There are dozens of options (both paid and open source) for sniffer detection tools, so organizational security teams will need to do some research before selecting the right tool for their needs.

4.8 Let Us Sum Up

Wireless network transmission waves can be seen by outsiders, this possesses many security risks.WEP is the acronym for Wired Equivalent Privacy. It has security flaws which make it easier to break compared to other security implementations.WPA is the acronym for Wi-Fi Protected Access. It has security compared to WEP. Intrusion Detection Systems can help detect unauthorized access. A good security policy can help protect a network. 802.11 Wireless transmissions can be encrypted to improve the security and confidentiality of the data that is being transferred. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2 are the three types of security available with WPA2 using AES (Advanced Encryption Standard) technology. If wireless is critical to your business, create a fallback plan. Wired networks routinely employ high-availability measures like link diversity, redundant routers, and uninterruptible power supplies. Apply this thinking to your WLAN as well by considering where and how wired alternatives should be applied.

4.9 Self Assessment Questions

2. What is WEP?

....
....
....
....
....
....
....

2. Explain about WEP Cracking.

....
....
....
....
....
....
....

3. List out the different WEP Cracking Tools

....
....
....
....
....
....
....

4. What are the general attack types in WPA?

....
....
....
....
....
....
....

5. How to Secure Wireless Networks?

....
....
....
....
....
....
....

4.10 Model Questions

1. Explain Different between WEP Cracking and WPA Cracking
2. Write the benefits of using 802.11 Wireless Networks
3. What is WLAN Scanners and explain it.
4. What is a Wireless Sniffer?
5. What are the tools for Detecting Packet Sniffers?

References & Further Readings

1. https://www.veracode.com/security/wireless-sniffer
2. https://www.developersindia.in/hacking/best-methods-get-access-wireless-network/
3. https://www.sans.org/reading-room/whitepapers/protocols/understanding-security-osi-model-377
4. https://www.quora.com/How-are-wireless-connections

UNIT-5 IDS, Firewalls and Honeypots - I

Unit Structure

4.0 Introduction

Threats to wireless local area networks (WLANs) are numerous and potentially devastating. Security issues ranging from misconfigured wireless access points (WAPs) to session hijacking to Denial of Service (DoS) can plague a WLAN. Wireless networks are not only susceptible to TCP/IP-based attacks native to wired networks, they are also subject to a wide array of 802.11-specific threats. To aid in the defense and detection of these potential threats, WLANs should employ a security solution that includes an intrusion detection system (IDS). Even organizations without a WLAN are at risk of wireless threats and should consider an IDS solution. This paper will describe the need for wireless intrusion detection, provide an explanation of wireless intrusion detection systems, and identify the benefits and drawbacks of a wireless intrusion detection solution.

4.1 Learning Objective

After learning this unit you should be able to

- Understand the concepts of Wireless Intrusion Detection.
- Identify different types of wireless local area networks.
- Know about the working of wireless intrusion detection systems.
- Study about Architecture of IDS.
- Learn about the threats Detection using IDS
- To point out the limitations of Wireless IDS.
- Study how to implement Wireless Intrusion Detection Systems.
- Know about Proxy Firewalls and Definition of Honeypot.
- Understand the purposes of a Honeypot and how it work.
- Remember the types of Honeypots and advantages of honeypots.
- Learn about the ethical issues concerning Honeypots.

4.2 Wireless Intrusion Detection Concept

In order to protect our network we need to ensure that we know:

- Where all access points reside on our network
- What actions to take to close down any un-authorized access points that do not conform to the company security standards
- What wireless users are connected to our network

- What unencrypted data is being accessed and exchanged by those users

To do this we must monitor our air space using a Wireless Intrusion Detection System.

4.2.1 What is Intrusion Detection?

Let’s firstly start with the principle and to do this I found the following quote from Ant Allen, research director at Gartner. “For an enterprise to protect itself from abuse of its information, it must monitor the events occurring in its computer system or network and analyze them for signs of intrusion. To do this, the enterprise must install an Intrusion Detection System (IDS).”

First thing to clarify here is that an IDS is not a firewall! Firewalls are designed to be outward looking and to limit access between networks in order to prevent an intrusion happening. IDS watch the wired and wireless network from the inside and report or alarm depending on how they evaluate the network traffic they see.

4.2.2 Threats to Wireless Local Area Networks

Wireless local area networks are subject to a variety of threats. The standard 802.11 encryption method, Wired Equivalent Privacy (WEP) is weak. As documented in the paper "Weaknesses in the Key Scheduling Algorithm of RC-4", the WEP key of a wireless transmission can be acquired via brute force attack. So even if WEP encryption is utilized on a WLAN, an attacker can potentially intercept and decrypt sensitive data from wireless communications.

Hackers can also attack a WLAN and gather sensitive data by introducing a rogue WAP into the WLAN coverage area. The rogue WAP can be configured to look like a legitimate WAP and, since many wireless clients simply connect to the WAP with the best signal strength, users can be "tricked" into inadvertently associating with the rogue WAP. Once a user is associated, all communications can be monitored by the hacker through the rogue WAP. In addition to hackers, rogue WAPs can also be introduced by users. Low cost and easy implementation coupled with the flexibility of wireless network communications makes WLANs highly desirable to users. By installing a WAP on an established LAN, a user can create a backdoor into the network; subverting all the hard-wired security solutions and leaving the network open to hackers. It is for this reason that even organizations without a WLAN implementation must strongly consider deploying a wireless IDS solution. It is very possible that users can and will install a rogue WAP, exposing even an exclusively hard-wired organization to the risks of WLANs.

4.3 Intrusion Detection Systems (IDSs)

Intrusion detection systems (IDSs) attempt to identify computer system and network intrusions and misuse by gathering and analyzing data. IDSs have traditionally been developed to detect intrusions and misuse for wired systems and networks. More recently, IDSs have been developed for use on wireless networks. These wireless IDSs can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs. Wireless IDSs gather all local wireless transmissions and generate alerts based either on predefined signatures or on anomalies in the traffic.

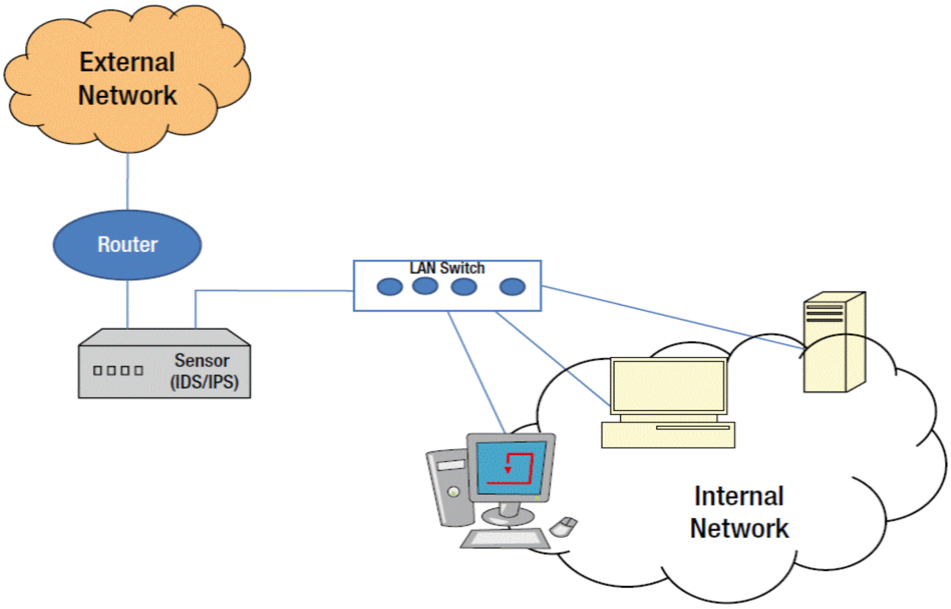
A Wireless IDS is similar to a standard, wired IDS, but has additional deployment requirements as well as some unique features specific to WLAN intrusion and misuse detection.

4.3.1 Wireless Intrusion Detection Systems

Wireless IDSs can be purchased through a vendor or developed in-house. There are currently only a handful of vendors who offer a wireless IDS solution - but the products are effective and have an extensive feature set. Popular wireless IDS solutions include Air defense Rogue Watch and Air defence Guard, and Internet Security Systems Real secures Server sensor and wireless scanner products. A home grown wireless IDS can be developed with the use of the Linux operating system, for example, and some freely available software. Open source solutions include Snort-Wireless and WIDZ, among others.

4.3.2 Architecture of IDS

A wireless IDS can be centralized or decentralized. A centralized wireless IDS is usually a combination of individual sensors which collect and forward all 802.11 data to a central management system, where the wireless IDS data is stored and processed. Decentralized wireless intrusion detection usually includes one or more devices that perform both the data gathering and processing/reporting functions of the IDS. The decentralized method is best suited for smaller (1-2 WAP) WLANs due to cost and management issues. The cost of sensors with data processing capability can become prohibitive when many sensors are required. Also, management of multiple processing/reporting sensors can be more time intensive than in a centralized model.



WLANs typically encompass a relatively large physical coverage area. In this situation, many WAPs can be deployed in order to provide adequate signal strength to the given area. An essential aspect of implementing a wireless IDS solution is to deploy sensors wherever a WAP is located. By providing comprehensive coverage of the physical infrastructure with sensors at all WAP locations, the majority of attacks and misuse can be detected. Another benefit of positioning the sensors in close proximity to the WAPs is the enhanced ability to physically pinpoint the geographical location of an attacker.

4.3.3 Physical Response of IDS

Physical location detection is a pivotal aspect of a wireless IDS. 802.11 attacks are often carried out in close proximity to the WAP and can be performed in an extremely short timeframe. Therefore, the response to attacks needs to not only be logical, like standard IDSs (i.e. Block the offending IP address), the response also needs to incorporate the physical deployment of individuals to identify the attacker - and the response must be timely. Unlike wired attacks where the hacker is usually great physical distances from the victim network, wireless attackers are often physically located on the local premises. A wireless IDS can aid in detecting the attacker's location by providing at least a general estimate of their physical location. By correlating the captured 802.11 data with the sensor location as well as the location of the victim WAP, the physical location of the attacker can be more easily identified. An even more ambitious approach to physical location identification would be to also use directional antennae in an effort to triangulate the 802.11 attacker signal source.

4.3.4 Policy Enforcement of IDS

A wireless IDS not only detects attackers, it can also help to enforce policy. WLANs have a number of security-related issues, but many of the security weaknesses are fixable. With a strong wireless policy and proper enforcement, a wireless network can be as secure as the wired equivalent - and a wireless IDS can help with the enforcement of such a policy.

Suppose policy states that all wireless communications must be encrypted. A wireless IDS can continually monitor the 802.11 communications and if a WAP or other 802.11 device is detected communicating without encryption, the IDS will detect and notify on the activity. If the wireless IDS is pre-configured with all the authorized WAPs and an unknown (rogue) WAP is introduced to the area, the IDS will promptly identify it. Features such as rogue WAP detection, and policy enforcement in general, go a long way to increase the security of the WLAN.

4.3.5 Threat Detection in IDS

A wireless IDS can also aid in the detection of a number of attacks. Not only can a wireless IDS detect rogue WAPS, identify non-encrypted 802.11 traffic, and help isolate an attacker's physical location, as mentioned earlier - a wireless IDS can detect many of the standard (and not-so standard) wireless attacks and probes as well .

In an effort to identify potential WAP targets, hackers commonly use scanning software. Hackers or curious individuals will use tools such as Netstumbler or Kismet to map out a given area's WAPs. Used in conjunction with a Global Positioning System (GPS) these scans not only locate WAPs, but also log their geographical coordinates. These tools have become so popular that there are web sites dedicated to mapping the world's WAP geography. A wireless IDS can detect these and other scans, helping to improve awareness of the threats to the WLAN.

More critical than probe detection, a wireless IDS can also detect some DoS attacks. DoS attacks are relatively common with wireless networks, as many DoSs occur from signal loss due to a frequency conflict or a building that just went up across the street. Sometimes though, as mentioned earlier, hackers can attack the WLAN with the intent of denying it service. A wireless IDS can detect many of the attacks used to DoS WLANs, such as flooding authentication requests or disassociation/de-authentication frames.

In addition to the aforementioned attacks and probes, a wireless IDS can spot many of the other 802.11 threats as well. MAC address spoofing, one of the more common attacks, can be used by an attacker to masquerade as a WAP or wireless client. MAC address spoofing is also used in several tools including HostAP and WLAN-jack.

These features can add a strong layer of security to a WLAN. In addition to threat detection, merely letting people know that an IDS is in operation can add an element of deterrence and therefore, enhance security.

4.3.6 Wireless IDS drawbacks

The benefits to a wireless IDS are numerous, but there are several drawbacks to consider before deploying such a system. Wireless intrusion detection is a rather new technology. Caution should be taken before applying any new technology to an operational network. Because the technology is new, there may be bugs, or worse vulnerabilities which could potentially *weaken* the WLAN security. Wireless IDS technology is developing at a rapid pace though, and this caveat may not be a deterrent in the future. A potential turn-off to a wireless IDS solution may be cost.

The expense of the vendor solutions may be prohibitive. In such a case, a home grown solution can be developed, but this approach may prove costly as well due to the extensive human capital that may be required to develop such a solution. Also, the cost of the wireless IDS solution (vendor-based or home grown) will grow in conjunction with the size of the WLAN to be monitored, due to the requirement for a greater number of sensors. Therefore, the larger the WLAN, the more expensive the wireless IDS deployment will be.

A wireless IDS is only as effective as the individuals who analyze and respond to the data gathered by the system. A wireless IDS, like standard IDS, can require vast human resources to analyze and respond to threat detection. In fact, it can be argued that a wireless IDS will require more human resources than a standard IDS because with a wireless IDS, individuals will be required to both attend to the logical (alert data) and physical aspects (finding and catching the hackers) of an attack.

4.3.7 Limitations of Intrusion Detection Systems

To be effective, IDS must be run online, in real time. Offline, or after-the-event IDS, is useful for audit trail but will not prevent an attack from taking place. Real time IDS needs to be able to stream data across a network from sensors to a central point where it can be stored and analysed, sometimes known as a correlation server. This ‘additional’ network traffic running concurrently can significantly impact network performance so sufficient bandwidth is a prerequisite, though certain tools such as Air Defence Guard allow you to “set rate throttles on each sensor to bring transfer rates to the server as low as 9.6 Kbps.”

4.3.8 Implement Wireless Intrusion Detection Systems

Wireless intrusion detection systems will monitor a WLAN using a mixture of hardware and software called intrusion detection sensors. The sensor will sit on the 802.11 network and will examine all network traffic. The first challenge to be faced when installing IDS is to decide on the best place to locate the sensors. To help make this decision, some detailed analysis must first be carried out on the site of the WLAN:

What kind of a building or location is it? Steel framed or wooden? (A steel framed building will limit the wireless transmitter’s range)

Are there areas of the site that have to be kept segregated? (In a built up area there will be mixed businesses, or it may be that a payroll department may want to be segregated in a large company for example.)

What MAC addresses are in use? (This list can be used as a baseline for comparison)

What authorised Access Points already exist? (Again, this list can be used as a baseline for future comparisons) Based on this information and from information gathered from sniffing the wireless network - using open source software such as Kismet we can easily build up a picture of what our WLAN looks like – where our AP’s are located who uses them, from where and how strong the radio signals are and how strong the radio signals need to be.

We are now in a position to determine where our IDS sensors need to be and to determine how many we need. A ‘warwalk’ can then be carried out to verify and test the implementation.

A **firewall** is a network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or corporate network). It acts as the demarcation point or “traffic cop” in the network, as all communication should flow through it and it is where traffic is granted or rejected access. They enforce access controls through a positive control model, which states that only traffic defined in the security policy is allowed onto the network; all other traffic is denied (known as “default deny”).

4.4 Access Control Lists

Early on, the firewall function was initially performed by Access Control Lists (ACLs), often on routers. ACLs are essentially rules written out that determine whether network access should be granted or rejected to specific

IP addresses. For example, an ACL can have a line that states all traffic from IP 172.168.2.2 must be rejected, or to allow all traffic on port 80 from 172.168.2.2 to the web server at 10.10.10.201.

ACLs are advantageous due to scalability and high-performance, but cannot read past packet headers, which provides only rudimentary information about the traffic. Thus, ACL packet filtering alone does not have the capacity to keep threats out of the network.

4.4.1 Proxy Firewalls

Proxy firewalls act as middlemen; they accept all traffic requests coming into the network by impersonating the true recipient of the traffic within the network. After an inspection, if it decides to grant access, the proxy sends the information to the destination computer. The destination computer's reply is sent to the proxy, which repackages the information with the source address of the proxy server. Through this process, the proxy breaks (or terminates) the connection between two computers so that it is the only machine on the network that talks to the outside world.

Proxy firewalls can inspect content fully and make access decisions based on more specific, granular information. Access control this nuanced is attractive to network administrators; however each application needs its own proxy at the application-level. These networks also suffer degraded traffic performance and many limitations in application support and general functionality. This ultimately leads to scalability issues that make successful implementation tricky to pull off. For this reason, proxies have not been widely adopted. In fact, even at the peak of their popularity in the 90s, performance and scalability issues limited adoption to select verticals in niche deployments.

UNIT-6 IDS, Firewalls and Honeypots - II

Unit Structure

IDS, Firewalls and Honeypots – I and II

6.0 Stateful Inspection Firewalls

Stateful inspection, or stateful filtering, is regarded as the third generation of firewalls. Stateful filtering does two things:

1. 1. Classifies traffic by looking at the destination port (e.g., tcp/80 = HTTP)
2. 2. Tracks the state of the traffic by monitoring every interaction of each particular connection until that connection is closed

These properties add more functionality to access control as they have the ability to grant or reject access based not only on port and protocol, but also the packet's history in the state table. When a packet is received, they check the state table to find if a connection has already been established or if a request for the incoming packet has been made by an internal host. If neither is found, the packet's access becomes subject to the ruling of the security policy.

Though stateful filtering is scalable and transparent to users, the extra layer of protection adds complexity to network security infrastructure, and stateful firewalls face difficulty in handling dynamic applications such as SIP or H.323.

6.1 Unified Threat Management

Unified Threat Management (UTM) solutions were initially defined as the consolidation of stateful inspection firewalls, antivirus, and IPS into a single appliance. Over time, the UTM definition has expanded to include many other network security functions.

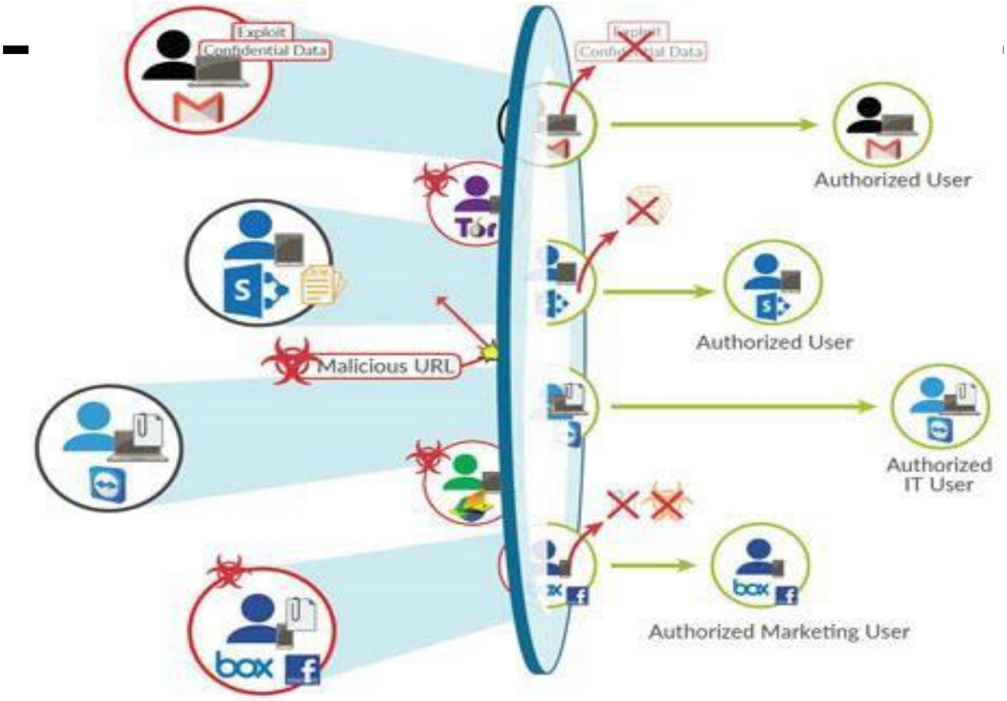
It is important to note that the success of UTMs relies on the effectiveness of the stateful inspection-based firewall decision that precedes all of its component functions. This is because UTM components, while in a single device, are effectively downstream security services. Thus, the workload of all security components inside the network will be determined by the strength of its access control. Though UTMs provide a number of security functions in one product, the fundamental access control technology remains unchanged.

Next-Generation Firewalls

Next-generation firewalls (NGFWs) were created in response to the evolving sophistication of applications and malware. Application and malware developers have largely outwitted the long-standing port-based classification of traffic by building port evasion techniques into their programs. Today, malware piggybacks these applications to enter networks and became increasingly networked themselves (connected to each other on the computers they individually infected).

NGFWs act as a platform for network security policy enforcement and network traffic inspection. Per technology research firm Gartner Inc., They are defined by the following attributes:

- **Standard capabilities of the first-generation firewall**: This includes packet filtering, stateful protocol inspection, network-address translation (NAT), VPN connectivity, etc.
- **Truly integrated intrusion prevention**: This includes support for both vulnerability-facing and threat-facing signatures, and suggesting rules (or taking action) based on IPS activity. The sum of these two functions collaborating via the NGFW is greater than the individual parts.
- **Full stack visibility and application identification**: Ability to enforce policy at the application layer independently from port and protocol.
- **Extra intelligence**: ability to take information from external sources and make improved decisions. Examples include creating blacklists or whitelists and being able to map traffic to users and groups using active directory.
- **Adaptability to the modern threat landscape**: support upgrade paths for integration of new information feeds and new techniques to address future threats.
- **In-line support** with minimum performance degradation or disruption to network operations.



6.2 Introduction to Honeypot

The role of decoy-based intrusion-detection technology, or "honeypots," is evolving. Once used primarily by researchers as a way to attract hackers to a network system in order to study their movements and behaviour, honeypots are now beginning to play an important part in enterprise security. Indeed, by providing early detection of unauthorized network activity, honeypots are proving more useful to IT security professionals than ever.

This unit looks at how honeypots work and how the technology is emerging as a key component in a layered approach to intrusion protection.

6.2.1 Definitions of Honeypot

A honeypot is a system that's put on a network so it can be probed and attacked. Because the honeypot has no production value, there is no "legitimate" use for it. This means that any interaction with the honeypot, such as a probe or a scan, is by definition suspicious.

6.2.2 There Are Two Types of Honeypots

- **Research:** Most attention to date has focused on research honeypots, which are used to gather information about the actions of intruders. For example, the Honeynet Project is a volunteer, non-profit security research organization that uses honeypots to collect information on cyber threats.
- **Production:** Less attention has been paid to production honeypots, which are actually used to protect organizations. Increasingly, however, production honeypots are being recognized for the detection capabilities they can provide and for the ways they can supplement both network- and host-based intrusion protection.

6.2.3 How Honeypots Work

Honeypots can also be described as being either low interaction or high interaction, a distinction based on the level of activity that the honeypot allows an attacker. A low-interaction system offers limited activity; in most cases, it works by emulating services and operating systems. The main advantages of low-interaction honeypots are that they are relatively easy to deploy and maintain and they involve minimal risk because an attacker never has access to a real operating system to harm others.

In contrast, high-interaction honeypots involve real operating systems and applications, and nothing is emulated. By giving attackers real systems to interact with, organizations can learn a great deal about an attacker's behaviour. High-interaction honeypots make no assumptions about how an attacker will behave, and they provide an environment that tracks all activity. Such conditions allow organizations to learn about behavior they would not otherwise have access to.

High-interaction systems are also flexible, and IT security professionals can implement as much or as little of them as they want. In addition, this type of honeypot provides a more realistic target, capable of detecting a higher calibre of attacker. High-interaction honeypots can be complex to deploy, however, and they require additional technologies to prevent attackers from using the honeypot to launch attacks on other systems.

6.2.4 What Are The Purposes Of A Honeypot?

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.

The hacker can be caught and stopped while trying to obtain root access to the system.

By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

6.2.5 What Are The Types Of Honeypots?

Although most honeypots have a similar general purpose, there are actually different types of honeypots that fulfill different functions. According to Windowsecurity.com, there are two main types of honeypots:

- Production - A production honeypot is one used within an organization's environment to help mitigate risk.
- Research – A research honeypot add value to research in computer security by providing a platform to study the threat

Honeypots can generally be divided into different categories, low-interaction, medium-interaction and high-interaction honeypots respectively.

- honeyd (low-interaction) - a GPL licensed daemon, that is able to simulate big network structures on a single host.
- mwcollect, nepenthes (medium-interaction) - Honeypot where malware infects a simulated environment
- Spam honeypots - Honeypot programs created by administrators which masquerade as abusable resources in order to discover the activities of spammers.
- E-mail trap - An e-mail address that is not used for any other purpose than to receive spam can also be considered a spam honeypot.

6.2.6 What Are The Ethical Issues Concerning Honeypots?

The use of honeypots is a very controversial topic and although deemed legal to use, how ethical are they really? Some experts deem honeypots as a cause for entrapment and according to *M.E. Kabay*, author of 'liability and ethics of honeypots' , "As for entrapment, although this is not a legal problem, this does not mean that the way a honeypot entices attackers is not unethical." The argument is that since it is both unethical and illegal to lure someone into stealing an object, why is it legal or ethical to lure an individual into committing a computer crime?

Other experts consider honeypots not only unethical, but a disadvantage to the computer world since they are in essence "building the better hacker" because more and more hackers are training themselves to be aware of honeypots and working around them, thus making secure systems a difficult ideal to achieve.

On the other hand some system security experts voice their opinion on the premise that honeypots merely use the "Attack first, before being attacked" approach. According to *B. Scottberg*, author of 'Internet Honeypots: Protection or Entrapment?' "Tracking an intruder in a honeypot reveals invaluable insights into attacker techniques and ultimately motives so that production systems can be better protected. You may learn of vulnerabilities before they are exploited." This viewed is a valid support concerning the ethics of honeypot applications for organizations that use them.

6.2.7 Advantages of Honeypots

Security experts say that honeypots can succeed in a number of areas where traditional intrusion-detection systems (IDS) have been found wanting. In particular, they point to:

4.6.6.1 **Too much data:** One of the common problems with the traditional IDS is that it generates a huge amount of alerts. The sheer volume of this "noise" makes it time-consuming, resource-intensive and costly to review the data. In contrast, honeypots collect data only when someone is interacting with them. Small data sets can make it easier and more cost-effective to identify and act on unauthorized activity.

4.6.6.2 **False positives:** Perhaps the biggest drawback of an IDS is that so many of the alerts generated are false. False positives are a big problem even for organizations that spend a lot of time tuning their systems. If an IDS continually creates false positives, administrators may eventually begin to ignore the system. Honeypots sidestep this problem because any activity with them is, by definition, unauthorized. That allows organizations to reduce, if not eliminate, false alerts.

4.6.6.3 **False negatives:** IDS technologies can also have difficulty identifying unknown attacks or behavior. Again, any activity with a honeypot is anomalous, making new or previously unknown attacks stand out.

4.6.6.4 **Resources:** An IDS requires resource-intensive hardware to keep up with an organization's network traffic. As a network increases in speed and generates more data, the IDS has to get bigger to keep up. Honeypots require minimal resources, even on large networks. According to Lance Spitzner, founder of the Honeynet Project, a single Pentium computer with 128MB of RAM can be used to monitor millions of IP addresses.

4.6.6.5 **Encryption:** More organizations are moving to encrypt all their data, either because of security issues or regulations, such as the Health Insurance Portability and Accountability Act. Not surprisingly, more and more attackers are using encryption as well. That blinds an IDS's ability to monitor the network traffic. With a honeypot, it doesn't matter if an attacker is using encryption; the activity will still be captured.

6.2.8 How Honeypots Augment IDSs

The evolution of honeypots can also be understood by looking at the ways these systems are being used in association with IDSs to prevent, detect and help respond to attacks. Indeed, honeypots are increasingly finding their place alongside network- and host-based intrusion-protection systems.

Honeypots are able to prevent attacks in several ways. The first is by slowing down or stopping automated attacks, such as worms or auto rooters. These are attacks that randomly scan an entire network looking for vulnerable systems. (Honeypots use a variety of TCP tricks to put an attacker in a "holding pattern.") The second way is by deterring human attacks. Here Honeypots aim to sidetrack an attacker, making him devote attention to activities that cause neither harm nor loss while giving an organization time to respond and block the attack.

As noted above, honeypots can provide early detection of attacks by addressing many of the problems associated with traditional IDSs, such as false positives and the inability to detect new types of attacks, or zero-day attacks. But increasingly, honeypots are also being used to detect insider attacks, which are usually more subtle and more costly than external attacks.

Honeypots are also helping organizations respond to attacks. A hacked production system can be difficult to analyze, since it's hard to determine what's normal day-to-day activity and what's intruder activity. Honeypots, by capturing only unauthorized activity, can be effective as an incident-response tool because they can be taken off-line for analysis without affecting business operations. The newest honeypots boast stronger threat-response mechanisms, including the ability to shut down systems based on attacker activity and frequency-based policies that enable security administrators to control the actions of an attacker in the honeypot.

6.2.9 How Honeypots Secure Computer Systems

A Honeypot is a computer connected to a network. These can be used to examine the vulnerabilities of the operating system or the network. Depending on the kind of setup, one can study security holes in general or in particular. These can be used to observe activities of an individual which gained access to the Honeypot.

Honeypots are generally based on a real server, real operating system, along with data that looks like real. One of the chief differences is the location of the machine in relation to the actual servers. The most vital activity of a honeypot is to capture the data, the ability to log, alert, and capture everything the intruder is doing. The gathered information can prove to be quite critical against the attacker.

6.3 Let Us Sum Up

Wireless intrusion detection systems are important additions to the security of wireless local area networks. While there are drawbacks to implementing a wireless IDS, the benefits will most likely prove to outweigh the downsides. With the capability to detect probes, DoSs, and variety of 802.11 attacks, in addition to assistance with policy enforcement, the benefits of a wireless IDS can be substantial. Of course, just as with a wired network, an IDS is only one part of a greater security solution. WLANs require a number of other security measures to be employed before an adequate level of security can be reached, but the addition of a wireless IDS can greatly improve the security posture of the entire network. With the immense rate of wireless adoption, the ever-increasing number of threats to WLANs, and the growing complexity of attacks, a system to identify and report on threat information can greatly enhance the security of a wireless network. Like all technologies, honeypots have their drawbacks, the greatest one being their limited field of view. Honeypots capture only activity that's directed against them and will miss attacks against other systems.

6.4 Self Assessment Questions

1. What is Intrusion Detection?

....

....

....

....

....

....

....

....

....

....

....

....

....

....

3. What is Proxy Firewalls?

....

....

....

....

....

....

....

....

....

....

....

4. Write the definition of Honeypot.

....

....

....

....

....

....

....

....

....

....

....

....

5. What is the purpose of a Honeypot?

....

....

....

....

....

6.5 Model Questions

1. Explain about Architecture of IDS
2. How threat Detection in IDS?
3. What are the types of Honeypots?
4. What are the Ethical issues Concerning Honeypots?
5. How Honey pots secure Computer Systems?

6.6 References & Further Readings

1. https://www.sans.org/reading-room/whitepapers/wireless/wireless-intrusion-detection-systems-1543
2. https://www.symantec.com/connect/articles/wireless-intrusion-detection-systems
3. WIRELESS INTRUSION DETECTION SYSTEMS (IDS) SOLUTION TO WLAN THREATS, K R Patil 1 A A Sawant 2 P.D. Sheba Kezia Malarchelvi 3
4. https://www.sans.org/reading-room/whitepapers/wireless/overview-wireless-intrusion-detection-system-1599

Answer of Self Assessment Questions

1. How organizations avoid attacks on web server?

An organization can adopt the following policy to protect itself against web server attacks.

- Patch management – this involves installing patches to help secure the server. A patch is an update that fixes a bug in the software. The patches can be applied to the operating system and the web server system.
- Secure installation and configuration of the operating system
- Secure installation and configuration of the web server software
- Vulnerability scanning system – these include tools such as Snort, NMap, Scanner Access Now Easy (SANE)
- Firewalls can be used to stop simple DoS attacks by blocking all traffic coming the identify source IP addresses of the attacker.
- Antivirus software can be used to remove malicious software on the server
- Disabling Remote Administration
- Default accounts and unused accounts must be removed from the system
- Default ports & settings (like FTP at port 21) should be changed to custom port & settings (FTP port at 5069)

2. Write a short note on IIS Unicode Exploit Explanation.

The Unicode Exploit is a Web Server specific hole.

i. It can be used when a writeable or executable directory is available; this allows attacks to upload malicious code.

ii. Or when a system executable such as cmd.exe or cmd2.exe is available on the root, which doesn’t have an access control listing written to it.

The Microsoft ISS Unicode exploit uses the **H**yper **T**ext **T**ransfer **P**rotocol (HTTP) and malformed URLs to execute arbitrary commands and transverse directories on vulnerable web servers. Unicode exploit uses Unicode representation of a directory delimiter (/) to fool IIS. The reason why this works so well is because you can use it right from your web browsers address bar, the reason why you can do this is because it uses the Hyper Text Transfer Protocol (HTTP). The only thing that the exploit lacks is its program usage. Programs such as the File Transfer Protocol (FTP) or Telnet don’t work very well with this exploit reasoning are because this is a non-interactive exploit.

3. What is patch management technique?

Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks, including Ringmaster’s Automated Patch Management, Patch Link Update, and Gibraltar's Ever guard.

4. Write down web application threats.

Cross-site scripting - Injecting lines of JavaScript into web pages. If not defended against, a hacker can submit malicious code through the search bar, for example, or post it in a user comment.

Session Hijacking - Each unique user is assigned a "session" when they log in to a website. Session hijackers will jump into the session of another user, reading information as it passes between the user and the server.

Parameter Manipulation - Websites often pass information from one web page to the next through URL parameters. For example, if you search on Google, your search terms will be passed to the results page through the URL. A hacker can take advantage of this fact to rewrite these parameters in harmful ways.

Buffer Overflow - A buffer is a small amount of space allotted to store data. If a buffer is overloaded, the extra data will overwrite data in other areas. Hackers have exploited this knowledge to overfill a buffer, than overwrite other data with their own malicious code.

Denial of Service - Denial of Service attacks are simple but effective. They operate by overwhelming a site with requests for information, severely slowing the operation of a website or bringing it down entirely.

SQL Injection - SQL injection works similarly to cross-site scripting; in this case, however, it is malicious SQL statements that are inserted into the site. These statements are intended to manipulate the database in some way - accessing sensitive data, or deleting it entirely, causing major headaches for the owners.

5. What is password based Entity authentication?

Usernames and passwords are the most common form of authentication in use today. Despite the improved mechanisms over which authentication information can be carried (like HTTP Digest and client side certificates), most systems usually require a password as the token against which initial authorization is performed. Due to the conflicting goals that good password maintenance schemes must meet, passwords are often the weakest link in authentication architecture. More often than not, this is due to human and policy factors and can be only partially addressed by technical remedies. Some best practices are outlined here, as well as risks and benefits for each countermeasure. As always, those implementing authentication systems should measure risks and benefits against an appropriate threat model and protection target.

Answer of Self Assessment Questions (Unit-2)

1. **What do you mean by SQL Injection?**

SQL injection is a code injection technique that might destroy your database. It is one of the most common web hacking techniques. It is the placement of malicious code in SQL statements, via web page input. SQL Injections can manipulate data (delete, update, and add etc.) and corrupt or delete tables of the database.

2. Explain Categories of SQL Injection Attacks.

There are four main categories of SQL Injection attacks against Oracle databases –

1. SQL Manipulation

2. Code Injection

3. Function Call Injection

4. Buffer Overflows

The first two categories, SQL manipulation and code injection, should be well known to the reader, as these are the most commonly described attacks for all types of databases (including SQL Server, MySQL, PostgreSQL, and Oracle).

SQL manipulation typically involves modifying the SQL statement through set operations (e.g., UNION) or altering the WHERE clause to return a different result. Many documented SQL injection attacks are of this type. The most well known attack is to modify the WHERE clause of the user authentication statement so the WHERE clause always results in TRUE.

Code injection is when an attacker inserts new SQL statements or database commands into the SQL statement. The classic code injection attack is to append a SQL Server EXECUTE command to the vulnerable SQL statement. Code injection only works when multiple SQL statements per database request are supported. SQL Server and PostgreSQL have this capability and it is sometimes possible to inject multiple SQL statements with Oracle.

Oracle code injection vulnerabilities involve the dynamic execution of SQL in PL/SQL.

The last two categories are more specific attacks against Oracle databases and are not well known or documented. In the vast majority of our application audits, we have found applications vulnerable to these two types of attacks.

Function call injection is the insertion of Oracle database functions or custom functions into a vulnerable SQL statement. These function calls can be used to make operating system calls or manipulate data in the database.

SQL injection of buffer overflows is a subset of function call injection. In several commercial and open-source databases, vulnerabilities exist in a few database functions that may result in a buffer overflow. Patches are available for most of these vulnerabilities, but many production databases remain un-patched.

3. What is vulnerable in SQl Injection?

An application is vulnerable to SQL injection for only one reason – end user string input is not properly validated and is passed to a dynamic SQL statement without any such validation. The string input is usually passed directly to the SQL statement. However, the user input may be stored in the database and later passed to a dynamic SQL statement, referred to as a second-order SQL injection. Because of the stateless nature of many web applications, it is common to write data to the database or store it using some other means between web pages. This indirect type of attack is much more complex and often requires in-depth knowledge of the application.

4. Write down about Buffer Overflow.

Buffer overflow problems always have been associated with security vulnerabilities. In the past, lots of security breaches have occurred due to buffer overflow. This article attempts to explain what buffer overflow is, how it can be exploited and what countermeasures can be taken to avoid it.

Knowledge of C or any other high level language is essential to this discussion. Basic knowledge of process memory layout is useful, but not necessary. Also, all the discussions are based on Linux running on x86 platform. The basic concepts of buffer overflow, however, are the same no matter what platform and operating system is used.

5. What is Boolean-Based (Content-Based) Blind SQLi?

In-band SQLi (Classic SQLi)

In-band SQL Injection is the most common and easy-to-exploit of SQL Injection attacks. In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.

The two most common types of in-band SQL Injection are *Error-based SQLi* and *Union-based SQLi*.

Error-based SQLi

Error-based SQLi is an in-band SQL Injection technique that relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database. While errors are very useful during the development phase of a web application, they should be disabled on a live site, or logged to a file with restricted access instead.

Union-based SQLi

Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

Out-of-band SQLi

Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable.

Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

Answer of Self Assessment Questions

1. What is WEP

WEP is the acronym for Wired Equivalent Privacy. It was developed for IEEE 802.11 WLAN standards. Its goal was to provide the privacy equivalent to that provided by wired networks. WEP works by encrypting the data been transmitted over the network to keep it safe from eavesdropping.

2. Explain about WEP Cracking.

Cracking is the process of exploiting security weaknesses in wireless networks and gaining unauthorized access. WEP cracking refers to exploits on networks that use WEP to implement security controls. There are basically two types of cracks namely;

- **Passive cracking**– This type of cracking has no effect on the network traffic until the WEP security has been cracked. It is difficult to detect.
- **Active cracking**– This type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking. It is more effective compared to passive cracking.

3. List out the different WEP Cracking Tools

- **Aircrack**– Network sniffer and WEP cracker.
- **WEPCrack**– This is an open source program for breaking 802.11 WEP secret keys. It is an implementation of the FMS attack.
- **Kismet**- This can include detector wireless networks both visible and hidden, sniffer packets and detect intrusions. **WebDecrypt**– This tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters.

4. General Attack types in WPA

- **Sniffing**– this involves intercepting packets as they are transmitted over a network. The captured data can then be decoded using tools such as Cain & Abel.
- **Man in the Middle (MITM) Attack**– this involves eavesdropping on a network and capturing sensitive information.
- **Denial of Service Attack**– the main intent of this attack is to deny legitimate users network resources. FataJack can be used to perform this type of attack.

5. How to Secure Wireless Networks.

In minimizing wireless network attacks; an organization can adopt the following policies

- **Changing default passwords** that come with the hardware
- Enabling the **authentication mechanism**
- **Access to the network can be restricted** by allowing only registered MAC addresses.
- **Use of strong WEP and WPA-PSK keys**, a combination of symbols, number and characters reduce the chance of the keys been cracking using dictionary and brute force attacks.
- **Firewall** Software can also help reduce unauthorized access.

Answer of Self Assessment Questions

1. What is Intrusion Detection?

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.

2. What is Wireless Intrusion Detection System?

Intrusion detection systems (IDSs) attempt to identify computer system and network intrusions and misuse by gathering and analyzing data. IDSs have traditionally been developed to detect intrusions and misuse for wired systems and networks. More recently, IDSs have been developed for use on wireless networks. These wireless IDSs can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs. Wireless IDSs gather all local wireless transmissions and generate alerts based either on predefined signatures or on anomalies in the traffic.

A Wireless IDS is similar to a standard, wired IDS, but has additional deployment requirements as well as some unique features specific to WLAN intrusion and misuse detection.

3. What is Proxy Firewalls?

Just like a proxy server or cache server, a proxy firewall acts as an intermediary between in-house clients and servers on the Internet. The difference is that in addition to intercepting Internet requests and responses, a proxy firewall also monitors incoming traffic for layer 7 protocols, such as HTTP and FTP.

4. Write down the definition of Honeypot.

In computer terminology, a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked. This is similar to police sting operations, colloquially known as "baiting," a suspect.

5. What is the purpose of a Honeypot?

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.

The hacker can be caught and stopped while trying to obtain root access to the system.

By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

●