Dr. Babasaheb Ambedkar Open University

MSCCS-105

Software Lab for MSCCS-103, MSCCS-104

List of Practical

Practical-1:

- List out the ways to make policies more effective
- List out five basic differences between policies and procedures
- Explain IPSec.
- Explain working of PGP in detail along with diagram
- Differentiate between Malware, Botnet, Virus and Worms

Practical-2:

- List different types of insider attacks.
- How to prevent Insider attack?
- List different types of outsider attacks.
- How to prevent outsider attack?
- Write challenges of a cybercrime
- Explain various effects of cybercrime
- Differentiate between Active & Passive Attacks
- Explain distributed attack with example
- Write down steps to report an incident?

Practical-3:

- List characteristics of an IDS?

- Write the steps to install an IDS in an organization?
- Differentiate network and host based IDS?
- Make diagram of IDS Components
- Give examples of Misuse & Anomaly Detection IDS?
- Explain lifecycle of Incident Handling along with diagram

Practical-4:

- Differentiate between tangible and intangible assets
- Write down the steps for securing an asset
- List out key features and types of Hardware Security Module(HSM)?
- Explain firewalls along with its types and diagram
- When and where to implement hardware based firewall?
- Write down few points to prevent your network from anonymous attack?
- What are the security problems with WEP and WPA? Explain briefly

Practical-5:

- List different type of cyber exercises.
- Write an attack/ scenario for table-top exercise.
- Discuss various initiatives of Govt. of India for achieving information security assurance.
- Explain cyber security self-assessment.
- Write importance of cyber exercises.
- Discuss various parameters used for purpose of evaluation in cyber exercises

Practical-6:

- How does spyware exploit user information?
- As a responsible home user, how can you prevent getting infected with malware?
- Discuss the modus operandi of banking Trojan citing some notable malware as example?
- How exploit kit infect you? How one can prevent drive by download attacks in exploit kit scenario?

Practical-7:

- Explain application security.
- What is a web shell.
- Explain with an example malicious file upload.
- Security is a continuous process - explain.
- How to perform security integration within SDLC?
- Explain manual security testing.

Practical-8:

- What is social engineering? If my name is Sani Abhilash and I am working at Ministry of I.T. Explain the tools and techniques you could possibly use to get information to perform social engineering attack on me?
- Give an example of reverse social engineering
- What is spear phishing? How successful it as compared to generic phishing mails?
- List different types of social engineering attacks.
- How to defend against social engineering attack?

Practical-9:

- Explain process for conducting risk assessment.
- Discuss common methods of conducting riskassessment.
- Explain OCTAVE.
- Explain COBIT.
- Explain NIST cyber security framework.
- Explain Factor analysis of information risk (FAIR).

Practical-10:

- What is the purpose of a write block protection device?
- What types of digital media devices can potentially hold data?
- In computer forensics methodology, what do you infer metadata
- Does turning off a machine impact forensics analyst? If you think yes, Explain? If you think, No, justify

Practical-11:

- Explain cyber security initiatives in India.
- Discuss Roles and functions of CERT-In.
- Explain National cyber security exercises.
- Discuss user responsibilities specified in email policy by Government of India.

Practical-12:

- Discuss importance of national cyber security policies.
- Discuss vision and objective of the National cyber security policy of India.
- Discuss cyber index and wellness profile of the India.
- Explain categories and parameters on which cyber security index is calculated.

Practical-13:

- Discuss Current threat landscape.
- Discuss emerging threats to Cloud computing and Internet of Things.
- Discuss five common attacks possible on computer networks with example.
- What is MITM attack, discuss impact of MITM.
- Explain DoS/DDoS attack.
- What is SYN flooding and UDP flooding?
- Discuss tools and communication methods used by hacker groups.
- Website as a vector for propagating malware
- What are the possible attacks on Internet trust infrastructure?

Practical-14:

- Give an example of Application level firewall.
- What is Network Address Translation (NAT).
- Explain Network Intrusion Detection and Prevntion System.
- What is a honeypot? Discuss different type of honeypots.
- What is a difference between network based and host based intrusion detection and prevention system.
- Discuss the various placement of intrusion detection and prevention system in a network.
- What do you understand by log management, how it is different from security information and event management.
- Discuss honeypot technology and its applications.
- Distinguish between High-interaction and low-interaction honeypot.
- Discuss honeypot utilities known to you.

- What is a signature based detection, how it is different from anomaly detection.

Practical-15:

- Prepare list of network security best practices.
- Explain end-point security.
- Discuss any 4 critical security controls in detail.
- Why Maintenance, Monitoring and Analysis of Complete Audit Logs is critical control.
- What do you understand by Secure Network Engineering?
- Discuss importance of Penetration Tests and Red Team Exercises.
- Write a note on Network Device Resiliency and Survivability.

Practical-16:

- Explain TIA-942 standard.
- What is data center security?
- Explain importance of data backup.
- Discuss threats to ICT from manmade or natural disasters.
- Discuss common controls to protect ICT from Fire disaster