

Dr. Babasaheb Ambedkar Open University
Term End Examination January-2026

Course	: MSCCS	Date	: 19/02/2026
Subject Code	: MSCCS-304	Time	: 03:00PM TO 05:15PM
Subject Name	: Security Analysis and Reporting	Duration	: 2.15 Hours
		Max. Marks	: 70

Section A

Answer the following (Attempt any three) (30)

1. Write a short note on importance of firewall in network security.
2. Enlist and describe various types of Web Application Vulnerabilities.
3. Which are key recommendations for handling incidents?
4. Discuss various wireless threats in great details.
5. What do you mean by Credential Stealers ? Discuss in details.

Section B

Answer the following (Attempt any four) (20)

1. Explain various Steps of Penetration Testing Method.
2. What you will do when a Cyber security incident occurs and you are not prepared?
3. Enlist and explain seven principles of network security analysis strategy.
4. Describe each and every steps while handling crisis.
5. Which are various Weapons of a Social Engineer?
6. Discuss in short about polymorphic worms(PW).

Section C

Part – A (Multiple Choice Questions) (10)

- 1 In _____ , the attacker acts like someone else to trap the victim.

A Piggybacking	B Impersonation
C Eavesdropping	D Dumpster Driving
- 2 _____ from Faronics is an useful tool to use when performing malware analysis on physical hardware.

A Deep Freeze	B BinNavi
C BinDiff	D All of them
- 3 _____ is electronically and intentionally carrying out threatening acts against individuals.

A Hacking	B Cyber Laundering
C Cyber Harassment	D Cyber Theft
- 4 In _____ attack, devices are used to create interference with a valid RF of Wi-Fi network, thus leading to WLAN service degradation.

A Jamming	B Man – in – Middle
C War Driving	D Breaking WEP Encryption
- 5 _____ describes the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network.

A Packet Analysis	B Packet Sniffing
C Protocol analysis	D All of them

- 6 A _____ attack is done against an authentication mechanism such as passwords, CAPTCHAS or digital signatures.
 A Daniel of Service B Brute force
 C Phishing D Injection
- 7 _____ is a security standard in the world of wireless networking.
 A WEP B WPA2
 C WPA D All of them
- 8 _____ involves mass amounts of email being sent in order to promote and advertise products and websites.
 A Spamming B Pharming
 C Bombing D Phishing
- 9 _____ is a tool that creates virtual hosts on the network.
 A Kismet B SNORT
 C Honeyd D Fragroute
- 10 _____ phishers target selected groups of people with something in common.
 A Spear B Phone
 C Clone D None of them

Part – B (Do as Directed)

(10)

- 1 A botnet is a collection of compromised hosts, known as zombies, which are controlled by a server known as a botnet controller. True / False
- 2 Pharming is a type of attack intended to redirect traffic to a fake Internet host. True / False
- 3 Identifying the worms in the network is an example of Anomaly detection. True / False
- 4 Foot-printing is the technique of accumulating information regarding the target and the surrounding environment. True / False
- 5 cloud computing means "a type of Internet- based computing," where different services are delivered to an organization through the Internet. True / False
- 6 Passive monitoring transmits probes into the network to collect measurements between at least two endpoints in the network. True / False
- 7 Stream Cipher converts plain-text into cypher text in a bit-by-bit fashion. True / False
- 8 Mumble attacks are telephonic social engineering attacks targeted at call center agents. True / False
- 9 Incident handling is the process of detecting and analyzing incidents and limiting the incident's effect. True / False
- 10 An Intrusion Detection System(IDS) is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. True / False
