NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment Solution- Week 9

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which mode allows a network interface card (NIC) to capture all traffic on the network segment regardless of the destination?

a. Monitor mode
b. Transparent mode
c. Promiscuous mode
d. Hypervisor mode

Correct Answer: c

Detail Solution: When using sniffing tools like Wireshark, the NIC is set to promiscuous mode, allowing it to capture all packets on the segment, not just those destined for the host.

The correct option is (c).

QUESTION 2:

Which of the following is/are not a feature of Wireshark?

a. Captures and analyzes packets
b. Generates statistical reports
c. Manipulates live network traffic
d. Carries out SQL injection attack

Correct Answer: c, d

Detail Solution: Wireshark can capture, analyze, and display packets with GUI support, and also generate statistical reports. But it cannot manipulate live traffic — tools like Ettercap or BurpSuite are used for that, SQL injection is not a feature of Wireshark.

The correct options are (c) and (d).

QUESTION 3:

Which of the following protocols are vulnerable to sniffing attack?

a. HTTP
b. FTP
c. HTTPS
d. SSL

Correct Answer: a, b

Detail Solution: HTTPS and SSL exchange data in secure channel. HTTP and FTP protocol exchange data in plain text (unsecured form), and thus they are vulnerable to sniffing attack.

The correct options are (a) and (b).

QUESTION 4:

Which of the following countermeasures is effective against sniffing attacks?

a. Use switch instead of hub
b. Use Telnet instead of SSH
c. Disable HTTPS
d. Allow ARP broadcasts

Correct Answer: a

Detail Solution: A switch forwards packets only to intended recipients, limiting the scope for sniffing. Using telnet and disabling HTTPS can increase the risk of sniffing.

The correct option is (a).

QUESTION 5:

Which of the following features are present in Ettercap?

a. IP-based and MAC-based filtering
b. Character injection
c. Packet filtering and dropping
d. SQL injection

Correct Answer: a, b, c

Detail Solution: The Ettercap tool can carry out IP-based filtering, MAC-based filtering, and character injection in a packet, packet filtering & dropping. However, it cannot be used to mount SQL injection attacks.

The correct options are (a), (b) and (c).

QUESTION 6:

Which of the following is an example of reverse social engineering?

a. Attacker pretends to be IT support so victim voluntarily provides information
b. Attacker steals password by shoulder surfing
c. Attacker sends phishing mail
d. Attacker sneaks in through tailgating

Correct Answer: a

Detail Solution: In reverse social engineering, the attacker acts as an authority, and the victim approaches the attacker for help, revealing sensitive info.

The correct option is (a).

QUESTION 7:

Which of the following is NOT a human-based social engineering attack?

a. Impersonation
b. Shoulder surfing
c. Piggybacking
d. Phishing

Correct Answer: d

Detail Solution: Phishing is a computer-based social engineering attack. The others are example of direct human-based attacks.

The correct option is (d).

QUESTION 8:

A DoS attack that exploits the TCP three-way handshake is called:

a. SYN Flooding
b. ICMP Flood
c. Ping of Death
d. UDP Flood

Correct Answer: a

Detail Solution: SYN Flooding sends repeated SYN requests without completing handshakes, exhausting server listen queues.

The correct option is (a).

QUESTION 9:

Which tool performs a DoS attack by sending partial HTTP requests and never completing them?

a. Hydra
b. Wireshark
c. Slowloris
d. Crunch

Correct Answer: c

Detail Solution: Slowloris opens many connections with partial requests, keeping them alive and exhausting server resources.

The correct option is (c).

QUESTION 10:

Which of the following best defines a Botnet?

a. A network of legitimate IoT devices
b. A protocol for DoS mitigation
c. A security feature in switches
d. A group of compromised systems remotely controlled by an attacker

Correct Answer: d

Detail Solution: A botnet is a large network of compromised machines under attacker control, often used to launch DDoS attacks.

The correct option is (d).

**********END*******