Dr. Sondos Fadl

Assignment: Intro to CyberSecurity (CSC3104)

2025/2026

Scenario 1 — Unknown Device Appears on the Company Wi-Fi

During routine monitoring, the network security team sees an unfamiliar device connected to the secure Wi-Fi network. The router logs show multiple deauth frames sent from the same MAC address.

Tasks

1. Explain why an unknown device on Wi-Fi is a serious risk.
2. Explain reason why an unknown device generating deauth frames is a high-risk event.
3. Provide the command used to list all visible Wi-Fi networks and clients.
4. Provide the command used to lock onto the target router and capture a WPA/WPA2 handshake.

Scenario 2 — ARP Table Tampering on the Local Network

Users report strange network behavior. The gateway IP is intermittently unreachable and packet loss increases. ARP tables on several machines show unexpected MAC addresses associated with the router's IP.

Tasks

1. Identify the attack responsible for this behavior.
2. Identify which two parts of the CIA triad this attack targets.
3. Provide the command used to inspect the ARP table on the workstation.
4. Provide the Bettercap command used to launch the attack seen in the logs.

Scenario 3 — Port 4444 Generating Suspicious Outbound Traffic

The SOC alerts that one workstation is constantly sending encrypted outbound packets to external servers through TCP port 4444. This behavior is commonly associated with remote control malware.

Tasks

1. Identify the malware type likely responsible for this behavior.
2. Briefly describe how this kind of malware operates.

3. Provide the command used to check the service version running on port 4444.
4. Provide the Wireshark filter used to isolate all traffic on this port.

Scenario 4 — Unexpected Open Port on a Server

An instructor notices unusual outbound traffic from a university server. They suspect an unauthorized service was enabled. They decide to scan the system using Nmap.

Tasks

1. Explain why Nmap is the correct tool here.
2. Provide the command to scan all TCP ports.
3. Provide the command to detect service versions.
4. State one reason why unknown open ports are dangerous.

Scenario 5— Gateway MAC Address Change

Multiple users suddenly lose internet access. Checking their ARP tables shows the gateway IP mapped to a student laptop's MAC address.

Tasks

1. Explain what ARP spoofing is.
2. Provide the command to show ARP table entries.
3. Provide the Bettercap command to enable ARP spoofing.
4. State why ARP spoofing is dangerous.

Scenario 6 — Suspicious Open Ports on a Database Server

The SOC receives an alert showing that a production database server has multiple unexpected open ports. The server should only expose port 5432, but scans show port 21 and 445 are also open.

Tasks

1. Explain why exposing unnecessary services increases the attack surface.
2. State why scanning all 65,535 ports is sometimes necessary during incident response.
3. Provide the Nmap command to scan all ports on the server.
4. Provide the Nmap command to enumerate service versions on ports 21, 445, and 5432.

Scenario 7 — Man-in-the-Middle Attack on Internal Network

Employees complain about slow connections. Investigation reveals that the attacker's MAC address is being reported as the router's MAC inside several ARP tables, indicating ARP spoofing.

Tasks

1. Explain how ARP spoofing enables full MITM control over victim traffic.
2. State which part of the CIA triad is violated when traffic is intercepted.
3. Provide the Bettercap command to enable ARP spoofing.
4. Provide the Bettercap command to sniff the victim's traffic.

Scenario 8 - DNS Hijacking on Internal Network

The IT department receives multiple complaints that company websites redirect to unfamiliar pages. Investigation shows that DNS queries are being intercepted and returning fraudulent IP addresses for legitimate domains.

Tasks

1. Explain how DNS spoofing undermines network trust and security.
2. State which CIA triad component is primarily compromised by DNS spoofing.
3. Provide the Bettercap command to enable DNS spoofing.
4. Provide the command used by the attacker to redirect a specific domain to the attacker's server.

Scenario 9 - Encrypted Network Traffic Analysis

A security analyst suspects data exfiltration but notices all suspicious traffic is encrypted. They need to capture and analyze packet metadata to identify the communication pattern.

Tasks

1. Explain why capturing packets is useful even when traffic is encrypted.
2. State what metadata can still be analyzed in encrypted traffic.
3. Provide the tcpdump command to capture all traffic on interface eth0 and save it to a file.
4. Provide the tcpdump command to filter and display only HTTPS traffic.

Scenario 10 - Rogue Access Point Detection

Network monitoring reveals a new Wi-Fi access point with a similar SSID to the corporate network (e.g., "CompanyWiFi" vs "Company-WiFi"). Several employee devices have connected to this rogue AP.

Tasks

1. Explain why rogue access points are dangerous.
2. State what attack technique uses rogue APs to intercept credentials.
3. Provide the command to scan for all nearby Wi-Fi networks and their signal strength.
4. Provide the command to capture traffic from a specific BSSID.

Scenario 11 - Backdoor Hidden in System Updates

After a system update, IT discovers an unauthorized remote access service listening on port 31337. The service has no legitimate business purpose and provides shell access without authentication.

Tasks

1. Identify the malware type that provides unauthorized remote access.
2. Explain why backdoors are often placed on non-standard ports.
3. Provide the Nmap command to scan the top 1000 most common ports.
4. Provide the Nmap command to perform aggressive detection including OS and service versions.

Scenario 12 - DNS Cache Poisoning Attack

Users report that legitimate banking websites are displaying SSL certificate warnings. Investigation reveals that internal DNS servers are returning incorrect IP addresses for several financial institutions.

Tasks

1. Explain how DNS cache poisoning differs from DNS spoofing.
2. State what security measure can prevent DNS cache poisoning.
3. Provide the Bettercap command to view current DNS spoofing targets.
4. Provide the command to flush the DNS cache on a Windows system.

Best Wishes