Network Security

Security Control Types

- Physical – biometrics, security guards, and CCTV
- Administrative – policies, response plans, and training
- Technical – firewalls, SIEM, and IPS

Intrusion Detection & Attack Indicators

- Difference between IPS and IDS is that IPS logs and acts against potential threat traffic, IDS only monitors and reports malicious traffic.
- Indicator of attack is a real time indicator, indicator of compromise is not.

The Cyber Kill Chain Process

1. Stage 1: Recon - Gathering info on an individual in preparation for an attack.
2. Stage 2: Weaponization - Injecting the malicious software or installing some sort of back door on intended target's machine.
3. Stage 3: Delivery - Attacker sends malicious payload by means of email or instant message.
4. Stage 4: Exploitation - Gaining access & compromising the user's machine.
5. Stage 5: Installation - Installing more malicious code such as granting your own user root access.
6. Stage 6: C2 - Command channel used to control another computer.
7. Stage 7: Exfiltration - Accomplishing the final goal on the user's machine.

Snort Rule Analysis

Snort Rule #1:

- Rule 1 alerts user of ANY inbound TCP traffic from ports 5800:5820.
- This is part of the Reconnaissance Stage in the Cyber Kill Chain.
- This rule monitors for potential VNC scans.

Snort Rule #2:

- Rule 2 alerts for inbound TCP traffic on port 80, HTTP.
- Part of the Policies, Awareness, and Procedures.
- This rule monitors Policy PE EXE or DLL file download.

Snort Rule #3:

- alert tcp $EXTERNAL_NET 4444 -> $HOME_NET any (msg: "ET Possible Trojan or CrackDown)
- This rule alerts when traffic is detected on port 4444 to LAN on any port.

Part 3: IDS, IPS, DiD, and Firewalls

- An IDS connects to network via:
  - Perimeter
  - Host
- An IPS connects to network with a physical connection after a switch.
- Signature type IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks.
- Anomaly type IDS is beneficial for detecting all suspicious traffic that deviates from the well-known baseline and is excellent at detecting when an attacker probes or sweeps a network.

Defense Depth

1. Layers of Defense in Depth
   a. Physical
   b. Application
   c. Data
   d. Host
   e. Network
   f. Policy, Procedures, and Awareness
   g. Perimeter
2. Encryption
3. Spoofers or VPN
4. Trackers
5. Firewall encrypted passwords

Firewall Architectures & Methodologies

1. **Circuit level proxy** verifies the three-way TCP handshake. TCP handshake checks are designed to ensure that session packets are from legitimate sources.
2. **Stateful packet filter** looks at whole streams of packets at one time instead of individual packets.
3. An **application of proxy** intercepts all traffic prior to being forwarded to its final destination. This firewall acts on behalf of the recipient by ensuring the traffic is safe prior to forwarding it.
4. **Packet-filtering firewall** examines data within a packet as it progresses through a network interface by examining source and destination IP address, port number, and packet type- all without opening the packet to inspect its contents.
5. **MAC firewall** filters based solely on source and destination MAC address.