Network Security

Security Control Types

- Physical
- Administrative
- Technical

Intrusion Detection & Attack Indicators

- IPS logs and takes action against potential threat traffic, IDS do not.
- Indicator of attacks are real time indicators, indicator of compromise does 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:

- Alerts user of ANY inbound TCP traffic from ports 5800:5820.
- Reconnaissance
- Potential VNC scan

Snort Rule #2:

- Alerts for inbound TCP traffic on port 80, HTTP.
- Policies, awareness, and procedures.
- Policy PE EXE or DLL file download

Snort Rule #3:

- alert tcp $EXTERNAL_NET 4444 -> $HOME_NET any (msg: "ET Possible Trojan or CrackDown)

Part 3: IDS, IPS, DiD, and Firewalls

- IDS connects to network via:
    - Perimeter
    - Host
- A physical connection after a switch.
- Signature type.
- Anomaly type.

Defense Depth

1. Layer of Defense Depths
    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
2. Stateful packet filter
3. Application of proxy
4. Packet-filtering firewall
5. MAC firewall