Part 1: Review Questions

Security Control Types

The concept of defense in depth can be broken down into three different security control types. Identify the security control type of each set of defense tactics.

1. What type of security control are Walls, bollards, fences, guard dogs, cameras, and lighting?

Answer: Physical

1. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?

Answer: Administrative

1. What type of security control is encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems?

Answer: Technical

Intrusion Detection and Attack indicators

1. What's the difference between an IDS and an IPS?

Answer: IDS or Intrusion Detection System detects when intrusions have already happened, while an IPS also known as Intrusion Prevention System actively works to prevent network intrusions before they happen.

1. What's the difference between an Indicator of Attack and an Indicator of Compromise?

Answer: An Indicator of Attack indicates that a network is under attack from a malicious actor, while an Indicator of Compromise tells you when an attacker has gained access to and has compromised a network.

The Cyber Kill Chain

Name each of the seven stages for the Cyber Kill chain and provide a brief example of each.

Stage 1: Reconnaissance - running nmap to discover open ports.

Stage 2: Weaponization - exploit the vulnerabilities discovered in Stage 1 to make a deliverable payload.

Stage 3: Delivery - Deliver the weaponized bundle from Stage 2 to the victim.

Stage 4: Exploitation - Exploit a vulnerability using the delivered payload.

Stage 5: Installation - Using the exploit from Stage 4 to install malware.

Stage 6: Command and Control - Using the malware installed in Stage 5 to command and control the target machine.

Stage 7: Actions on Objective - To execute the desired actions on the target machine.

Snort Rule Analysis

Use the Snort rule to answer the following questions:

Snort Rule #1

1. Break down the Sort Rule header and explain what is happening.  
     
    Answer: Alerting of TCP traffic originating from any port on [$EXTERNAL\_NET], going to [$HOME\_NET] on any port in the range of 5800-5820.
2. What stage of the Cyber Kill Chain does this alert violate?  
     
    Answer: Reconnaissance
3. What kind of attack is indicated?  
     
    Answer: A potential VNC Scan.

Snort Rule #2

1. Break down the Sort Rule header and explain what is happening.  
     
    Answer: Alerts of any TCP traffic originating from the ports stored in [$HTTP\_PORTS] on the network [$EXTERNAL\_NET], and going to any port on the network [$HOME\_NET].
2. What layer of the Defense in Depth model does this alert violate?  
     
    Answer: Endpoint Security, specifically Content Security
3. What kind of attack is indicated?  
     
    Answer: A potential malware bundle being downloaded on the network described by [$HOME\_NET]

Snort Rule #3

* Your turn! Write a Snort rule that alerts when traffic is detected inbound on port 4444 to the local network on any port. Be sure to include the msg in the Rule Option.  
    
   Answer: alert tcp [$EXTERNAL\_NET] 4444 -> [$HOME\_NET] any (msg: "Traffic detected inbound on port 4444")