Part 1:

Security Control Types

1. Physical
2. Administrative
3. Technical

Intrusion Detection and Attack Indicators

1. The difference between an IDS(Intrusion Detection System) and IPS(Intrusion Prevention System) primarily lies in passive versus active security. An IDS logs breaches in the network and serves only as a detection mechanism which will require a follow up by an admin while an IPS proactively attempts to block the intrusion/threats based off of the profile.
2. An IOA is a proactive system that indicates a pending breach while an IOC is evidence of a past breach and is reactive.

The Cyber Kill Chain

The Cyber Kill Chain consists of reconnaissance, weaponization, delivery, exploitation, installation, command & control, and actions on objectives.

Reconnaissance is the gathering of information on the victim. Some examples may include reading the victims emails, listening in on conversations and scouring publicly available data like social media.

Weaponization establishes attack vectors and primes the attacker for the delivery stage.

Delivery is the stage of sending the dangerous payload to the victim. Some methods may include malware via email or USB.

Exploitation is the stage of using a vulnerability to begin the execution of malware.

Installation is the stage where the malware is fully installed in the victim’s machine (malware, cron jobs).

Command & Control is when the attacker is able to remotely manipulate the target machine with something like an IRC.

Actions on Objectives is the final step when the attacker will execute his or her desired actions. This may include examples such as data deletion or data theft.

Snort Rule Analysis

[alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by\_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classtype:attempted-recon; sid:2002910; rev:5; metadata:created\_at 2010\_07\_30, updated\_at 2010\_07\_30;)]

1. This is an alert for TCP based traffic sourced externally from the LAN specifically targeting the port range of 5800 to 5820 within the network.
2. Recon
3. Threats are located within the port range.

[alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"; flow:established,to\_client; flowbits:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file\_data; content:"MZ"; within:2; byte\_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata: former\_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Main/2018959; classtype:policy-violation; sid:2018959; rev:4; metadata:created\_at 2014\_08\_19, updated\_at 2017\_02\_01;)]

1. An alert for TCP traffic funneling through port 80.
2. Policies
3. Threat is the executable files that was downloaded

Part 2:

IDS vs IPS Systems

1. A network TAP receives and sends data on separate channels. The network TAP is able to transmit data in real time and fully copy all traffic without altering data. Another one is the switch port analyzer which sends duplicate network packets to another for analysis.
2. An IPS is installed in the form of a firewall.
3. Signature
4. Anomaly

Defense in Depth

1. Physical
2. Application
3. Data
4. Host
5. Network
6. Admin
7. Perimeter
8. Encryption
9. Encrypting traffic and regularly updating the key/certificate
10. GPS tracking
11. Harddrive encryption

Firewall Architectures and Methodologies

1. Stateful firewall
2. Stateful firewall
3. Proxy firewall
4. Stateless firewall
5. MAC layer firewall