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

Answer: **Physical Security**

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

Answer: **Administrative Security Controls**

1. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?

Answer: **Technical Security**

**Intrusion Detection and Attack indicators**

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

Answer:

**An IDS requires an administrator to react to an alert by examining what has been flagged. An IPS can automatically take action by blocking and logging the threat.**

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

Answer:

**Indicators of attack indicate attacks happening in real time.**

1. Proactive approach to intrusion attempts.
2. Indicate that an attack is currently in progress but a full breach has not been determined or has not occurred yet.
3. Focus on revealing the intent and end goal of the attacker regardless of the exploit or malware used in the attack.

**Indicators of compromise** (**IOC**) indicate previous malicious activity.

1. Reactive approach to successful intrusions.
2. Indicate that an attack occurred, resulting in a breach.
3. Used to establish an adversary's techniques, tactics, and procedures (TTPs).
4. Expose all of the vulnerabilities used in an attack, giving network defenders the opportunity to revamp their defense as part

**The Cyber Kill Chain**

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

1. Stage 1: Reconnaissance:  packet sniffing, ping sweeping, port scanning, phishing, social engineering, and internet information queries
2. Stage 2: Weaponization: Inject malicious code into transiting TCP flows
3. Stage 3: Delivery: Luring a target with a spear phishing tactic
4. Stage 4: Exploitation: “Click here to donate”
5. Stage 5: Installation: Clicking a link provided in a spear phishing e-mail
6. Stage 6: Command and Control:  After the malicious code has been installed the hacker has the ability to control;  example would be a phone, listen, track and then use the info to attack
7. Stage 7: Actions on Objective:  Extraction of the information the attacker has been targeting.

**Snort Rule Analysis**

Use the Snort rule to answer the following questions:

Snort Rule #1

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. Break down the Sort Rule header and explain what is happening.

**Triggers an alert whenever a TCP packet from External\_Net any port, with source IP $HOME\_NET 5800:5200;  a message will print “ET SCAN Potential VNC Scan 5800-5820”**

1. What stage of the Cyber Kill Chain does this alert violate?

**Reconnaissance**

1. What kind of attack is indicated?

**Identify its vulnerabilities – any accessibility**

Snort Rule #2

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. Break down the Sort Rule header and explain what is happening.

**Triggers an alert whenever a TCP packet from External\_Net $HTTP\_Ports will print a message “ET Policy PE EXE or DLL  Windows file download HTTP”**

1. What layer of the Defense in Depth model does this alert violate?

**Delivery**

1. What kind of attack is indicated?

A download of the following files: **POLICY PE EXE or DLL Windows file download HTTP**

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.

alert tcp $EXTERNAL\_NET 4444 -> $HOME\_NET any (msg: "Traffic Detected on port 4444;”)

**Part 2: "Drop Zone" Lab**

**Uninstall ufw**

Before getting started, you should verify that you do not have any instances of ufw running. This will avoid conflicts with your firewalld service. This also ensures that firewalld will be your default firewall.

* Run the command that removes any running instance of ufw.

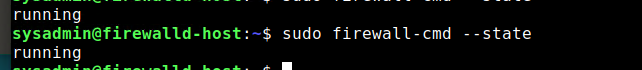
>

**Enable and start firewalld**

A screenshot of a computer

Description automatically generated with medium confidence





**List all firewall rules currently configured.**

Next, lists all currently configured firewall rules. This will give you a good idea of what's currently configured and save you time in the long run by not doing double work.

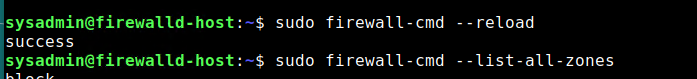
* Run the command that lists all currently configured firewall rules:
* Text

  Description automatically generated

**List all supported service types that can be enabled.**

* Run the command that lists all currently supported services to see if the service you need is available--- see below reload – success….

**Zone Views**

* Run the command that lists all currently configured zones.

**Create Zones for Web, Sales and Mail.**

* Run the commands that creates Web, Sales and Mail zones.

Text

Description automatically generated**Set the zones to their designated interfaces:**

* Run the commands that sets your eth interfaces to your zones.

Graphical user interface, text

Description automatically generated**Add services to the active zones:**

* Run the commands that add services to the **public** zone, the **web** zone, the **sales** zone, and the **mail** zone.

Graphical user interface, text

Description automatically generated

**Add your adversaries to the Drop Zone.**

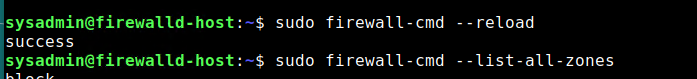
* Run the command that will add all current and any future blacklisted IPs to the Drop Zone.

Text

Description automatically generated**Make rules permanent then reload them:**

It's good practice to ensure that your firewalld installation remains nailed up and retains its services across reboots. This ensure that the network remains secured after unplanned outages such as power failures.

* Run the command that reloads the firewalld configurations and writes it to memory





**View active Zones**

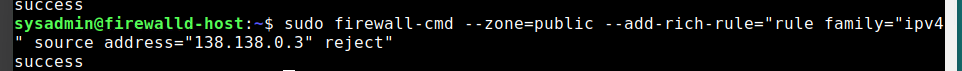
Now, we'll want to provide truncated listings of all currently **active** zones. This a good time to verify your zone settings.

* Run the command that displays all zone services.

Sudo firewall-cmd –list-all

**Block an IP address**

* Use a rich-rule that blocks the IP address 138.138.0.3.

**Block Ping/ICMP Requests**

Harden your network against ping scans by blocking icmp ehco replies.

* Run the command that blocks pings and icmp requests in your public zone.

Text

Description automatically generated**Rule Check**

Now that you've set up your brand new firewalld installation, it's time to verify that all of the settings have taken effect.

* Run the command that lists all of the rule settings. Do one command at a time for each zone.
* Sudo firewall-cmd –info-zone=public
* Sudo firewall-cmd –info-zone=web
* Sudo firewall-cmd –info-zone=sales
* Sudo firewall-cmd –info-zone=mail

Example below

Text

Description automatically generated

**Part 3: IDS, IPS, DiD and Firewalls**

Now, we will work on another lab. Before you start, complete the following review questions.

**IDS vs. IPS Systems**

1. Name and define two ways an IDS connects to a network.

Answer 1: Network Tap (Test Access Port)

Answer 2: SPAN/Mirrored Port – SPAN Port –

(Switched Port Analyzer) aka Port Mirroring

1. Describe how an IPS connects to a network.

Answer: Physically connects inline with the flow of data. An IPS is typically placed in between the firewall and network switch.

1. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?

Answer: Signature Based

1. Which type of 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?

Answer: Anomaly Based

**Defense in Depth**

1. For each of the following scenarios, provide the layer of Defense in Depth that applies:
   1. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.

**Perimeter defense**

1. A zero-day goes undetected by antivirus software.

**Application**

1. A criminal successfully gains access to HR’s database.

**Data Security**

1. A criminal hacker exploits a vulnerability within an operating system.

**Network**

1. A hacktivist organization successfully performs a DDoS attack, taking down a government website.

**Policy, Procedures, and Awareness**

1. Data is classified at the wrong classification level.

**Data Security**

1. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.

**Perimiter**

1. Name one method of protecting data-at-rest from being readable on hard drive.

**Encryption**

1. Name one method to protect data-in-transit.

**VPN or …. a tracking devise**

1. What technology could provide law enforcement with the ability to track and recover a stolen laptop.

**NIC**

1. How could you prevent an attacker from booting a stolen laptop using an external hard drive?

**Disable USB ports: BIOS setup disable USB**

**Firewall Architectures and Methodologies**

1. Which type of firewall verifies the three-way TCP handshake? TCP handshake checks are designed to ensure that session packets are from legitimate sources.

**Circuit level gateway:  Syn syn/ack ack**

1. Which type of firewall considers the connection as a whole? Meaning, instead of looking at only individual packets, these firewalls look at whole streams of packets at one time.

**Stateful inspection firewalls**

1. Which type of firewall intercepts all traffic prior to being forwarded to its final destination. In a sense, these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it?

**Host Based Network firewall**

1. Which type of 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?

**Packet Filtering Firewall**

1. Which type of firewall filters based solely on source and destination MAC address?

**MAC Filtering**