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

Answer: Physical Security

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

Answer: Administrative Security

3. 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 is a network monitor that logs and notifies about network traffic while an IPS is more active and is able to monitor the network and block traffic.

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

Answer: An Indicator of compromise focuses on finding evidence that a breach has occured while an indicator of attack looks for any signs of attempted attacks.

**#### 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

2. Stage 2: Weaponization

3. Stage 3: Delivery

4. Stage 4: Exploitation

5. Stage 5: Installation

6. Stage 6: Command and control

7. Stage 7: Actions on Objectives

**#### Snort Rule Analysis**

Use the Snort rule to answer the following questions:

Snort Rule #1

```bash

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.

Answer: a remote host is scanning the local host on ports 5800-5820 using tcp/IP protocols.

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

Answer: Reconnaissance

3. What kind of attack is indicated?

Answer: Port Mapping

Snort Rule #2

```bash

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.

Answer: the remote host tried to deliver malicious content to any port of the local machine through http ports

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

Answer: Delivery

3. What kind of attack is indicated?

Answer: site scripting

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 any -> $HOME\_NET 4444 (msg:"Traffic Detected")

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

**#### Log into the Azure `firewalld` machine**

Log in using the following credentials:

- Username: `sysadmin`

- Password: `cybersecurity`

**#### 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`.

```bash

$ sudo ufw disable && sudo killall ufw ; sudo systemctl disable ufw

```

**#### Enable and start `firewalld`**

By default, these service should be running. If not, then run the following commands:

- Run the commands that enable and start `firewalld` upon boots and reboots.

```bash

$ sudo systemctl enable firewalld.service

$ sudo /etc/init.d/firewalld start

```

Note: This will ensure that `firewalld` remains active after each reboot.

**#### Confirm that the service is running.**

- Run the command that checks whether or not the `firewalld` service is up and running.

```bash

$ sudo systemctl status firewalld.service

```

**#### 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:

```bash

$ sudo firewall-cmd --list-all

```

- Take note of what Zones and settings are configured. You many need to remove unneeded services and settings.

**#### 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

```bash

$ <sudo firewall-cmd --get-services>

```

- We can see that the `Home` and `Drop` Zones are created by default.

**#### Zone Views**

- Run the command that lists all currently configured zones.

```bash

$ sudo firewall-cmd --get-zones

```

- We can see that the `Public` and `Drop` Zones are created by default. Therefore, we will need to create Zones for `Web`, `Sales`, and `Mail`.

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

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

```bash

$ sudo firewall-cmd --permanent --new-zone=web

$ sudo firewall-cmd --permanent --new-zone=sales

$ sudo firewall-cmd --permanent --new-zone=mail

```

**#### Set the zones to their designated interfaces:**

- Run the commands that sets your `eth` interfaces to your zones.

```bash

$ sudo firewall-cmd --zone=public --change-interface=eth0

$ sudo firewall-cmd --zone=web --change-interface=eth0

$ sudo firewall-cmd --zone=sales --change-interface=eth0

$ sudo firewall-cmd --zone=mail --change-interface=eth0

```

**#### 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.

- Public:

```bash

$ sudo firewall-cmd --zone=public --add-service=http

$ sudo firewall-cmd --zone=public --add-service=https

$ sudo firewall-cmd --zone=public --add-service=pop3

$ sudo firewall-cmd --zone=public --add-service=smtp

```

- Web:

```bash

$ sudo firewall-cmd --zone=web --add-service=http

```

- Sales

```bash

$ sudo firewall-cmd --zone=sales --add-service=https

```

- Mail

```bash

$ sudo firewall-cmd --zone=mail --add-service=smtp

$ sudo firewall-cmd --zone=mail --add-service=pop3

```

- What is the status of `http`, `https`, `smtp` and `pop3`?

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

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

```bash

$ sudo firewall-cmd --permanent --zone=drop --add-source=10.208.56.23

$ sudo firewall-cmd --permanent --zone=drop --add-source=135.95.103.76

$ sudo firewall-cmd --permanent --zone=drop --add-source=76.34.169.118

```

**#### 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

```bash

$ sudo firewall-cmd --reload> - if 'permanent' flags not used

$ sudo firewall-cmd --runtime-to-permanent && sudo firewall-cmd --reload

```

**#### 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.

```bash

$ sudo firewall-cmd -list-all-zones

```

**#### Block an IP address**

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

```bash

$ <sudo firewall-cmd --permanent --add-rich-rule="rule family='ipv4' source

address='138.138.0.3' reject

```

#### 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.

```bash

$ sudo firewall-cmd --zone=public --add-icmp-block=echo-reply

```

**#### 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.

```bash

$ <sudo firewall-cmd --zone=public --list-all>

$ <sudo firewall-cmd --zone=web --list-all>

$ <sudo firewall-cmd --zone=sales --list-all>

$ <sudo firewall-cmd --zone=mail --list-all>

$ <sudo firewall-cmd --zone=drop --list-all>

```

- Are all of our rules in place? If not, then go back and make the necessary modifications before checking again.

Congratulations! You have successfully configured and deployed a fully comprehensive `firewalld` installation.

---

**### 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: NIDS - Monitors network traffic for patterns and behaviors

Answer 2: HIDS - Looks for malicious activity

2. Describe how an IPS connects to a network.

Answer: It is placed inline between the source and destination usually placed behind the firewall to monitor traffic

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

Answer: a stateless IDS cant detect zero-days.

4. 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: a stateful IDS is able to detect new exploits.

**#### 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.

Answer: administrative Policy

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

Answer: Technical Software

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

Answer: Technical Network

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

Answer: Technical Software

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

Answer: Technical Network

6. Data is classified at the wrong classification level.

Answer: Administrative Procedures

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

Answer: Administrative Network

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

Answer: Drive encryption

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

Answer: Data Encryption

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

Answer: GPS

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

Answer: Encrypting the harddrive with strong passwords.

**#### 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.

Answer: Stateless Network firewall

2. 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.

Answer: Stateful Firewall

3. 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?

Answer: Proxy Firewall

4. 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?

Answer: Packet-Filtering firewall

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

Answer: Data-link Firewall