Cybersecurity

Module 11 Challenge Submission File

Network Security Homework

Make a copy of this document to work in, and then fill out the solution for each prompt below. Save and submit this completed file as your Challenge deliverable.

Part 1: Review Questions

Security Control Types

The concept of defense in depth can be broken down into three 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?

```
Physical
```

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

```
Administrative
```

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

```
Technical
```

Intrusion Detection and Attack Indicators

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

```
Intrusion Detection System VS Intrusion Prevention System
IDS can alert on an attack & notify the necessary team, but not really do
anything to prevent or mitigate the attack
IPS can actively block an attack by examining the packets & it can also act
as a defense mechanism while attack is taking place.
```

2. What's the difference between an indicator of attack (IOA) and an indicator of compromise (IOC)?

```
IOA focus on detecting the intent of what an attacker is trying to
accomplish or indicates an attack is occurng.
IOC could be used like forensic evidence to show an attack has occured
```

The Cyber Kill Chain

Name the seven stages of the cyber kill chain, and provide a brief example of each.

1. Stage 1:

```
Reconnaissance: the attacker gathers as much information on the target as
possible, nmap, socials, email etc.
```

2. Stage 2:

```
Weaponization: Start preparing your payload, malware or code/web-based
attack based on your findings.
```

3. Stage 3:

```
Delivery: Deliver your weaponized bundle via phishing, usbstick, web, or any
means possible
```

4. Stage 4:

```
Exploitation: Getting your newly crafted weapon to run on the system, code execution etc.
```

5. Stage 5:

```
Installation: Install malware on the asset
```

6. Stage 6:

```
Command and Control (C2): C&C method threat actors use to communicate with compromised devices for remote manipulation of victim
```

7. Stage 7:

```
Actions on Objectives: Pretty much “hands on keyboard” access the hacker is now able to perform any objectives they wish
```

Snort Rule Analysis

Use the provided Snort rules 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 this rule does.

```
Creates an alert to the HomeNetwork that applies to tcp packets on all IP addresses from ports 5800-5820 which would looks like VNC port range
```

2. What stage of the cyber kill chain does the alerted activity violate?

```
Stage 1: Reconnaissance
```

3. What kind of attack is indicated?

```
Scanning for a possible open VNC Server
```

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 this rule does.

```
Alert on TCP packets sent via HTTP Traffic sent on port 80
```

2. What layer of the defense in depth model does the alerted activity violate?

```
Application: It looks like a potential virus / .dll file downloaded trying
to be embedded into Windows Update
```

3. What kind of attack is indicated?

```
Malware / Virus attack
```

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 $EXT 4444 -> $HOME any (msg: "Info Damien Packet Detected on port
4444";)
```

Part 2: “Drop Zone” Lab

Set up.

Log into the Azure `firewalld` machine 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.

```
sudo apt remove ufw
```

Enable and start firewalld.

By default, the firewalld service should be running. If not, then run the commands that enable and start firewalld upon boots and reboots.

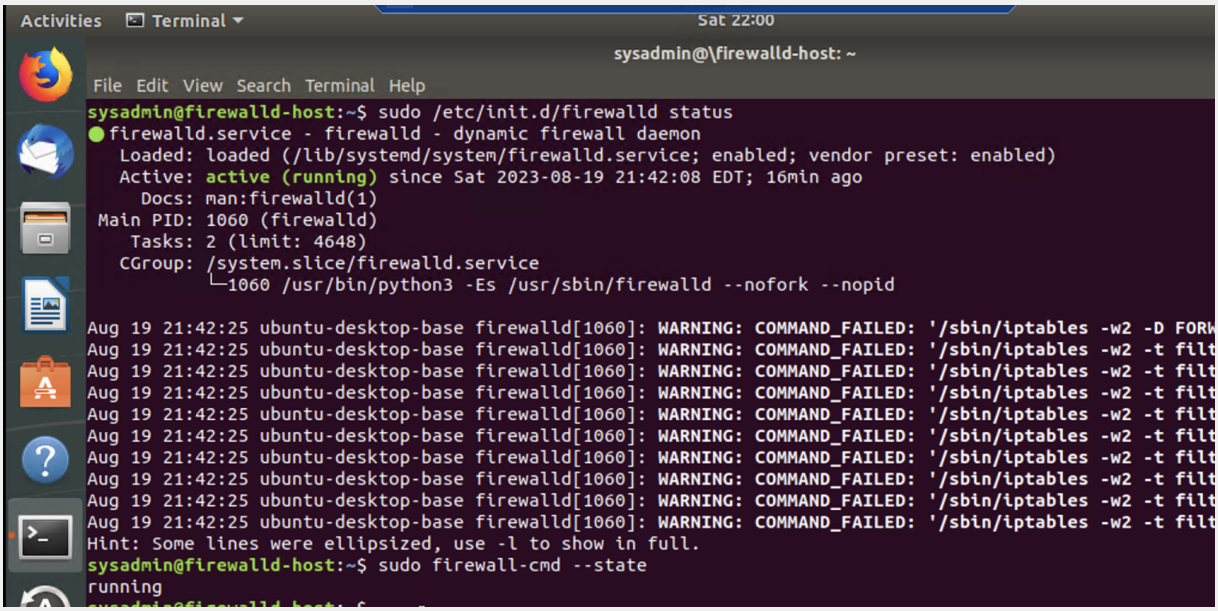
```
$sudo systemctl enable firewalld
$sudo systemctl start firewalld
```

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

Confirm that the service is running.

Run the command that checks whether the `firewalld` service is up and running.

```
$sudo firewall-cmd -state or $sudo /etc/init.d/firewalld status
```



List all firewall rules currently configured.

Next, list 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 ensuring that you don't duplicate work that's already done.

- Run the command that lists all currently configured firewall rules:

```
$sudo firewall-cmd –-list-all
```

- Take note of what zones and settings are configured. You may 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 find out whether the service you need is available.

```
$sudo firewall-cmd --get-services
```

- Notice that the `home` and `drop` zones are created by default.

Zone views.

- Run the command that lists all currently configured zones.

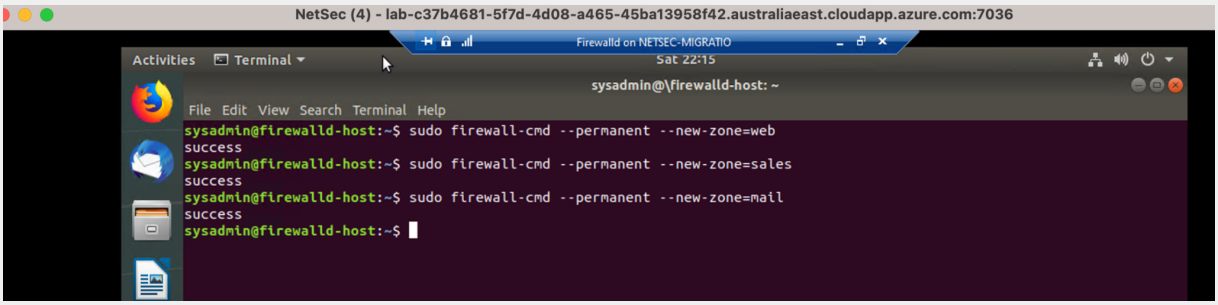
```
$ sudo firewall-cmd --list-all-zones
```

- Notice that the `public` and `drop` zones are created by default. Therefore, you will need to create zones for `web`, `sales`, and `mail`.

Create zones for `web`, `sales`, and `mail`.

- Run the commands that create `web`, `sales`, and `mail` zones.

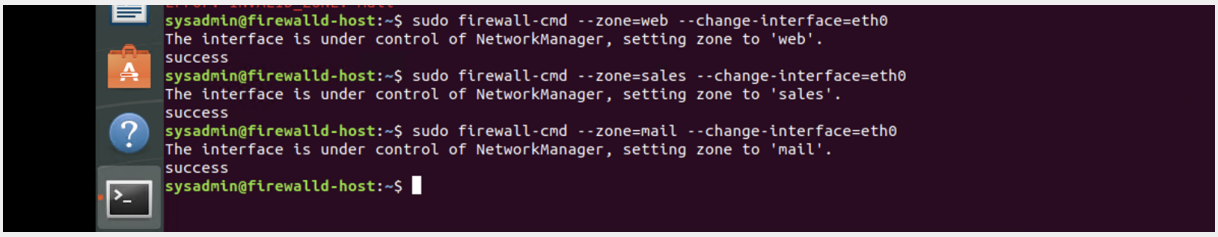
```
$ sudo firewall-cmd --permanent --new-zone=web
$ sudo firewall-cmd --permanent --new-zone=sales
$ sudo firewall-cmd --permanent --new-zone=mail
```



Set the zones to their designated interfaces.

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

```
$sudo firewall-cmd --zone=web --change-interface=eht0
$sudo firewall-cmd --zone=sales --change-interface=eht0
$sudo firewall-cmd --zone=mail --change-interface=eht0
```



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`:

```
$ 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`:

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

- `sales`:

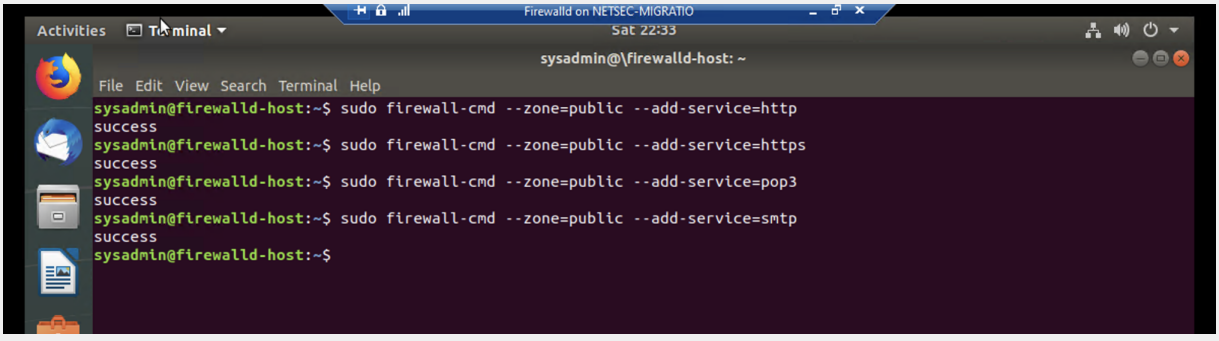
```
$ sudo firewall-cmd --zone=sales --add-service=https
```

- `mail`:

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

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

```
Active / success
```



Add your adversaries to the `drop` zone.

- Run the command that will add all current and any future blacklisted IPs to the `drop` zone.

```
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 helps ensure that the network remains secure after unplanned outages such as power failures.

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

```
$sudo firewall-cmd —-reload
```

View active zones.

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

- Run the command that displays all zone services.

```
$sudo firewall-cmd —-get-active-zones
```

Block an IP address.

- Use a rich-rule that blocks the IP address `138.138.0.3` on your `public` zone.

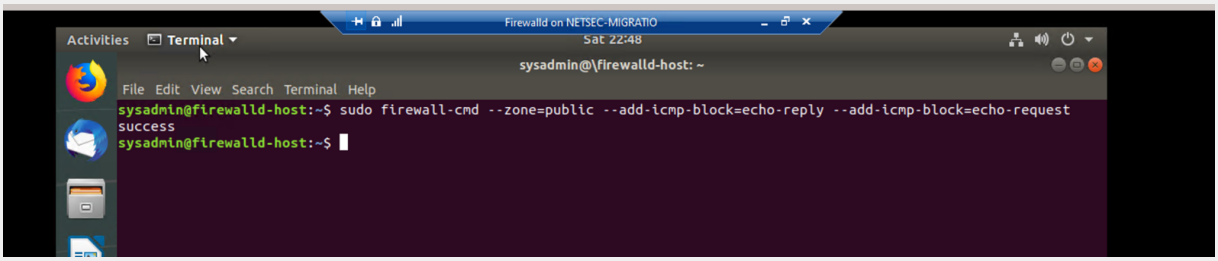
```
$ sudo firewall-cmd --add-rich-rule=’rule family=”ipv4” source
address=”138.138.0.3” drop’
```

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.

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



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 --zone=public --list-all
$ sudo firewall-cmd --zone=sales --list-all
$ sudo firewall-cmd --zone=mail --list-all
$ sudo firewall-cmd --zone=web --list-all
$ sudo firewall-cmd --permanent --zone=drop --list-all
```

- Are all of the 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, you'll 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.

```
Signature based intrusion detection: It allows IDSs to quickly identify
malicious behavior (SNORT)
```

```
SPAN, to allow port mirroring
```

2. Describe how an IPS connects to a network.

```
Inline with the flow of data, between the firewall and the network switch
```

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

```
Signature based
```

4. What 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?

```
Anomaly based detection
```

Defense in Depth

1. For each of the following scenarios, provide the layer of defense in depth that applies:

a. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.

```
Physical
```

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

```
Application
```

c. A criminal successfully gains access to HR's database.

```
Data
```

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

```
Application
```

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

```
Network
```

f. Data is classified at the wrong classification level.

```
Policies and Procedures
```

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

```
Data
```

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

```
Encryption
```

3. Name one method of protecting data-in-transit.

```
VPN
```

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

```
GPS, Geolocating
```

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

```
Bitlocker, or firmware password
```

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 firewall
```

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

```
Stateful
```

3. Which type of firewall intercepts all traffic prior to forwarding it 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.

```
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?

```
stateless
```

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

```
Mac filtering
```

Optional Additional Challenge Lab: “Green Eggs & SPAM”

In this activity, you will target spam, uncover its whereabouts, and attempt to discover the intent of the attacker.

- You will assume the role of a junior security administrator working for the Department of Technology for the State of California.
- As a junior administrator, your primary role is to perform the initial triage of alert data: the initial investigation and analysis followed by an escalation of high-priority alerts to senior incident handlers for further review.
- You will work as part of a Computer and Incident Response Team (CIRT), responsible for compiling **threat intelligence** as part of your incident report.

Threat Intelligence Card

Note: Log in to the Security Onion VM, and use the following **indicator of attack** to complete this portion of the assignment.

Locate the indicator of attack in Sguil based off of the following:

- **Source IP/port**: `188.124.9.56:80`
- **Destination address/port**: `192.168.3.35:1035`
- **Event message**: `ET TROJAN JS/Nemucod.M.gen downloading EXE payload`

Answer the following questions:

1. What was the indicator of an attack? (*Hint: What do the details reveal?*)

```
[Enter answer here]
```

2. What was the adversarial motivation (purpose of the attack)?

```
[Enter answer here]
```

3. Describe observations and indicators that may be related to the perpetrators of the intrusion. Categorize your insights according to the appropriate stage of the cyber kill chain, as structured in the following table:

TTP	Example	Findings
Reconnaissance	How did the attacker locate the victim?	
Weaponization	What was downloaded?	
Delivery	How was it downloaded?	
Exploitation	What does the exploit do?	
Installation	How is the exploit installed?	
Command & Control (C2)	How does the attacker gain control of the remote machine?	
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	

4. What are your recommended mitigation strategies?

```
[Enter answer here]
```

5. List your third-party references.

```
[Enter answer here]
```