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 security controls
```

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

```
Security awareness programs educate employees on policies. BYOD policies set
guidelines for personal device use in work, managing associated security
risks. Ethical hiring practices verify qualifications and align individuals
with trustworthy behavior, contributing to overall security.
```

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

Encryption safeguards data by converting it into code, requiring a specific decryption key. Biometric fingerprint readers verify identity using unique physical traits. Firewalls regulate network traffic based on security rules. Endpoint security secures individual devices from threats. Intrusion detection systems monitor activities for anomalies and alert administrators to policy violations.

Intrusion Detection and Attack Indicators

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

Indicator Detection System (IDS) monitors network activities, generating alerts for potential security incidents. In contrast,
An Intrusion Prevention System (IPS) not only detects but actively blocks or mitigates threats in real-time, providing a more proactive defense by automatically taking predefined actions to prevent unauthorized or malicious activities.

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

An Indicator of Attack (IOA) signifies potential malicious activity based on tactics and techniques, offering proactive detection. An Indicator of Compromise (IOC) indicates a confirmed security breach or compromise, providing evidence of unauthorized access or a successful attack.

The Cyber Kill Chain

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

1. Stage 1:

Reconnaissance:
Gathering information about the target.

2. Stage 2:

```
Weaponization:
Developing or acquiring malicious tools
```

3. Stage 3:

```
Delivery:
Transmitting the weaponized payload to the target
```

4. Stage 4:

```
Exploitation:
Taking advantage of vulnerabilities in the target's system
```

5. Stage 5:

```
Installation:
Placing the malware on the target system
```

6. Stage 6:

```
Command and Control:
Establishing communication channels between the attacker and the compromised
system
```

7. Stage 7:

```
Actions on Objectives:
The attacker accomplishes their main goals, like stealing important
information, causing chaos in operations, or keeping prolonged access for
spying.
```

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 Snort rule header and explain what this rule does.

```
The rule is like a security guard for computer networks. It watches for
suspicious behavior, like someone checking specific doors (ports 5800 to
5820). If it sees something strange, it raises an alert and logs a message.
It helps spot attempts to explore or scan for weaknesses in a VNC service.
```

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

```
The detected activity, scanning for VNC services on ports 5800 to 5820,
breaks the "Reconnaissance" stage of the Cyber Kill Chain. Attackers are in
the early phase, gathering info and identifying vulnerabilities in the
target system for potential future attacks
```

3. What kind of attack is indicated?

```
The Snort rule shows that someone is trying to check and learn about a
computer network. They're exploring to see if there's a VNC service on
ports 5800 to 5820. This kind of checking is usually the first step before
more serious cyber attacks might happen.
```

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 Snort rule header and explain what this rule does.

```
This Snort rule watches out for a certain thing: when someone tries to
download a special kind of file for Windows over the internet. It checks how
things are flowing, looks at the file, and uses certain tricks. If it
catches this happening, it writes a message saying someone broke the rules
by downloading a Windows file. They give it a special ID and version number
to keep track.
```

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

```
The alerted activity, where someone is trying to download a special kind of
file for Windows over the internet (as seen in the Snort rule), usually
breaks the "Delivery" stage of the Cyber Kill Chain. It's like someone
delivering a possibly harmful file to the target computer.
```

3. What kind of attack is indicated?

```
The Snort rule flags someone trying to download a suspicious Windows file
online, possibly intending to harm the computer.
```

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 any any -> $HOME_NET 4444 (msg:"Inbound Traffic on Port 4444";
sid:1000001;)
```

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 systemctl disable 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 disable 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 systemctl status firewalld
```

List all firewall rules currently configured.

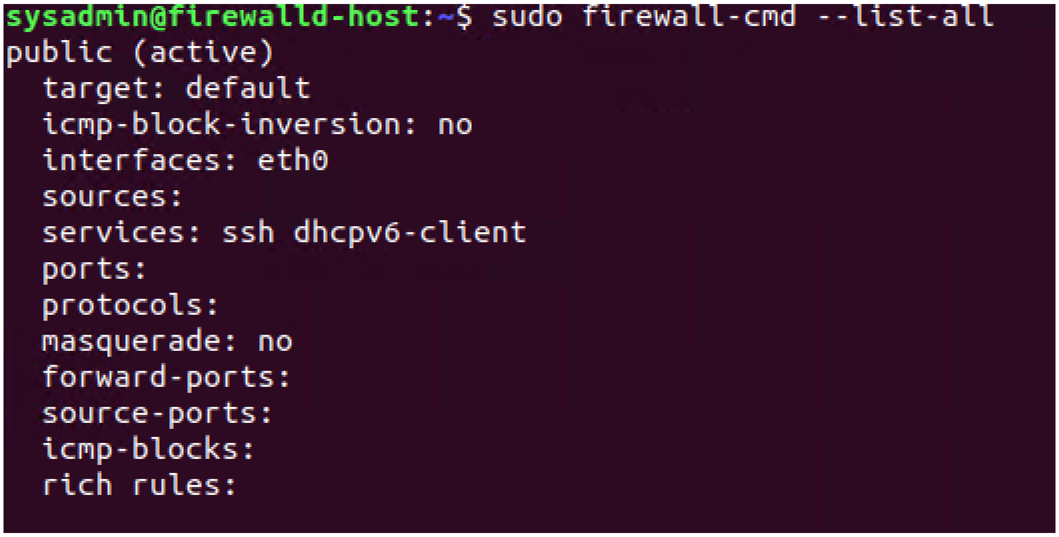
Next, list all currently configured firewall rules. This will give you a good idea of what's currently configured and save you time in the long run by ensuring that you don't duplicate work that's already done.

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

```
$ sudo systemctl disable firewalld
```

- 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.



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Run the command that lists all currently supported services to find out whether the service you need is available.

```
$ sudo firewall-cmd -get-service
```

- 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 --get-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 --permanent --zone=public --add-interface=eth0
$ sudo firewall-cmd --permanent --zone=web --add-interface=eth1
$ sudo firewall-cmd --permanent --zone=sales --add-interface=eth2
$ sudo firewall-cmd --permanent --zone=mail --add-interface=eth3
```

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 --permanent --zone=public --add-service=http
```

```
$sudo firewall-cmd --permanent --zone=public --add-service=https
$sudo firewall-cmd --permanent --zone=public --add-service=pop3
$sudo firewall-cmd --permanent --zone=public --add-service=smtp
```

- `web`:

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

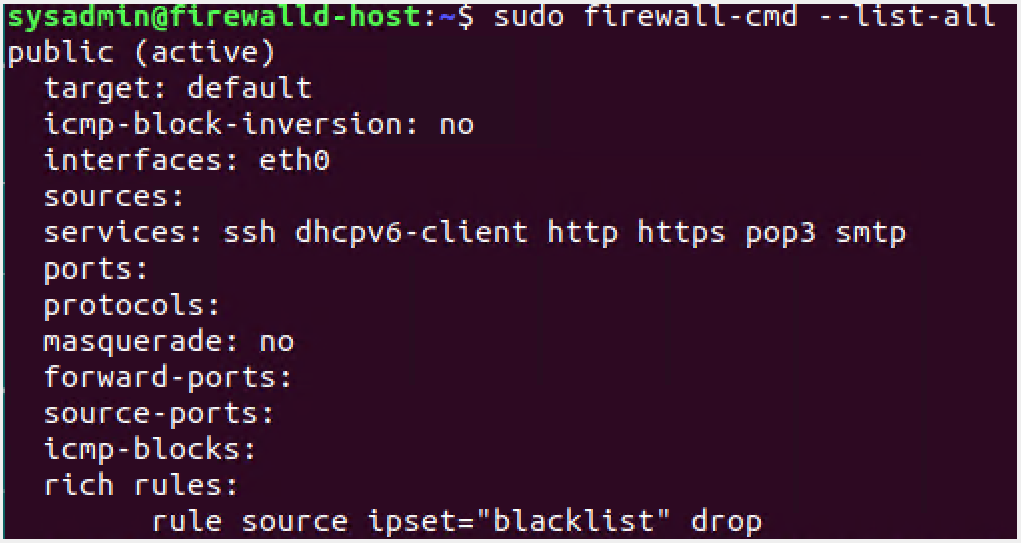
- `sales`:

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

- `mail`:

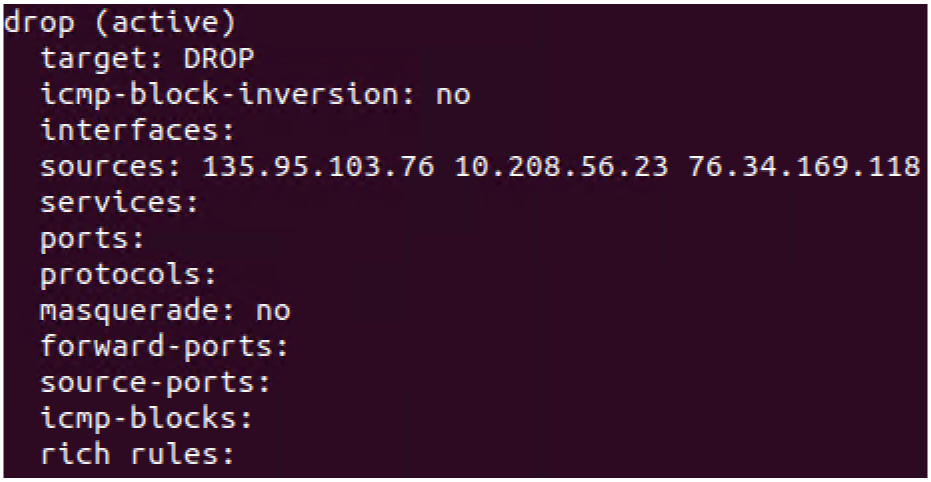
```
$sudo firewall-cmd --permanent --zone=mail --add-service=smtp
$sudo firewall-cmd --permanent --zone=mail --add-service=pop3
```

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



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule source ipset="blacklist" drop
```

Add your adversaries to the `drop` zone.



```
drop (active)
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources: 135.95.103.76 10.208.56.23 76.34.169.118
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

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

```
$sudo firewall-cmd --permanent --add-rich-rule='rule source ipset=blacklist drop'
$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
```

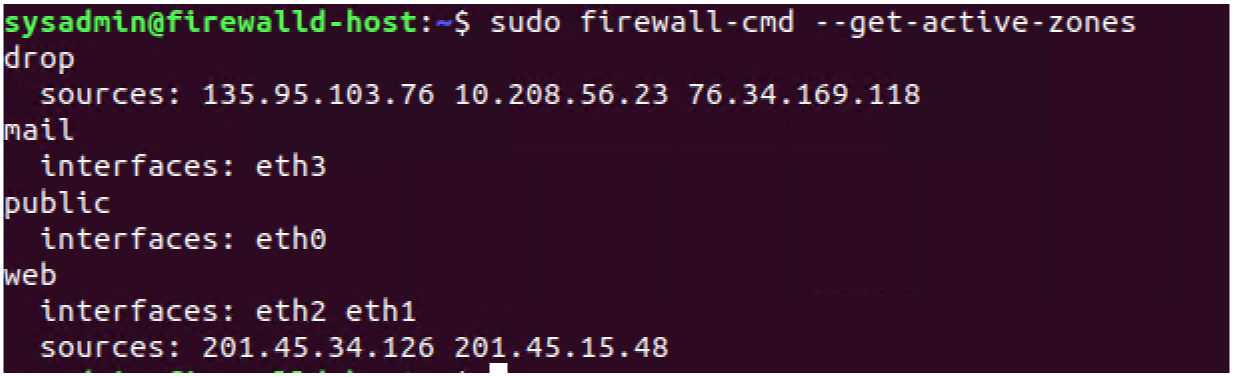
Make rules permanent, then reload them.

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.



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --get-active-zones
drop
  sources: 135.95.103.76 10.208.56.23 76.34.169.118
mail
  interfaces: eth3
public
  interfaces: eth0
web
  interfaces: eth2 eth1
  sources: 201.45.34.126 201.45.15.48
```

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 --permanent --zone=public --add-rich-rule='rule source
ipset=blacklist drop' --ipset=blacklist --add-entry=138.138.0.3
```

Block ping/ICMP requests.

Harden your network against `ping` scans by blocking `ICMP echo` replies.

- Run the command that blocks `pings` and `ICMP requests` in your `public` zone.

```
$ sudo firewall-cmd --permanent --zone=public --add-rich-rule='rule protocol
value="icmp" drop'
```

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=web --list-all
$sudo firewall-cmd --zone=service --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 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.

```
Network TAPs (test access point)
```

```
SPAN ports (Switched port analyzer)
```

2. Describe how an IPS connects to a network.

```
Inline Mode:
an IPS is placed directly in the network traffic path and actively block or
allows traffic based on its rules
```

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

```
Signature-based IDS
```

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 IDS
```

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 security layer
```

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

```
Application Security Layes
```

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

```
Database Security layer
```

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

```
Host security layer
```

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

```
Network security layer
```

f. Data is classified at the wrong classification level.

```
Data security layer
```

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

```
Network security Layer
```

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

```
Full Disk Encryption FDE
```

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

```
Transport layer security TLS
```

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

```
GPS tracking
```

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

```
BIOS/UEFI Password Protection
```

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.

```
Stateful 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 firewall
```

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?

```
Stateful firewall
```

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

```
MAC filtering firewall
```

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?*)

```
Red alert icon (RT)
```

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

```
Sensitive informations theft
```

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?	Email address has been compromised
Weaponization	What was downloaded?	JS/Nemucod was downloaded through a malicious JavaScript script.
Delivery	How was it downloaded?	SPAM Email
Exploitation	What does the exploit do?	Nemucod opens a legitimate PDF file in the browser, serving as a deceptive cover to make the user believe they are viewing a genuine invoice.
Installation	How is the exploit installed?	The installation process involves a JavaScript file downloading a straightforward EXE file, which is then silently executed in the background through the WScript_Shell ActiveX control.
Command & Control (C2)	How does the attacker gain control of the remote machine?	Gozi refrains from initiating communication with its command and control server until after the initial reboot
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	Nemucod fetches files, including Fareit or Pony Downloader, which then downloads additional executables housing the Gozi infostealer malware.

4. What are your recommended mitigation strategies?

```
Implement security awareness programs.
```

5. List your third-party references.

```
https://www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader
/

https://www.vimstotal.com/gui/fi1e/6cb50ecb44007c42666958ae58d724505fdd6414fd574ea
5cc6e5c03c640ecO/community

https://www.virustota1.com/gui/urVe0114a871f807bfff43161758dfaaffBcf458fd6c1fb242b
a79bc3f1d1c66d/detection
```

```
https://www.secureworks.com/research/gozipdf
```