# 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?

```
These are all examples of Physical Security Controls, measures taken to
protect physical assets, such as buildings, facilities, and the people and
resources within them, from unauthorized access, theft, vandalism, or other
physical threats.
```

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

```
Administrative or Procedural Security Controls.
```

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

```
Technical Security Controls.Technical controls are an integral part of an
organization's overall security strategy.
```

## Intrusion Detection and Attack Indicators

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

```
The difference between an IDS and an IPS is in their response capabilities.
An IDS is primarily focused on detection and alerting, while an IPS takes an
active role in preventing and blocking security threats in real-time.
```

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

```
The difference between IOAs and IOCs is their timing and purpose. IOAs are
focused on identifying potential threats or attacks in progress to prevent
them, while IOCs are used to confirm that a compromise has occurred and to
investigate and respond to incidents that have already taken place.
```

## The Cyber Kill Chain

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

1. Stage 1:

```
Reconnaissance:an attacker might scan a company's website to identify
employee names and email addresses.
```

2. Stage 2:

```
Weaponization: a cybercriminal may create a phishing email with a weaponized
PDF attachment.
```

3. Stage 3:

```
Delivery:the attacker sends the phishing email to the target's employees,
containing the weaponized attachment or a link to a malicious website.
```

4. Stage 4:

```
Exploitation: a vulnerability in an outdated software application could be
exploited to establish a connection with the attacker's command and control
server.
```

5. Stage 5:

```
Installation:a Trojan horse might be installed to provide the attacker with
persistent access to the victim's network.
```

6. Stage 6:

```
Command and Control (C2): malware on the victim's system connects to a
remote server controlled by the attacker.
```

7. Stage 7:

```
Actions on Objectives: For instance, in a data breach, the attacker
exfiltrates sensitive data from the compromised systems.
```

## 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.

```
This Snort rule is designed to generate an alert when it detects TCP traffic
from an external network to an internal network on ports 5800 to 5820 with
specific TCP flag settings, which are indicative of a potential VNC scan.
```

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

```
 this alerted activity primarily corresponds to the "Reconnaissance" stage.
```

3. What kind of attack is indicated?

```
indicative of a potential port scanning or reconnaissance attack.
```

### 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 is designed to detect the download of Windows executable
(PE) files or DLLs over HTTP.
```

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

```
The alerted activity violates the "Delivery" stage of the Cyber Kill Chain.
```

3. What kind of attack is indicated?

```
the indicated attack the potential download of Windows executable files or
DLLs over an HTTP connection. Such downloads can be a vector for malware
delivery, including viruses, Trojans, and other malicious software, or the
delivery of potentially unwanted software to a target system.
```

**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 ufw disable
Sudo apt -y 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.

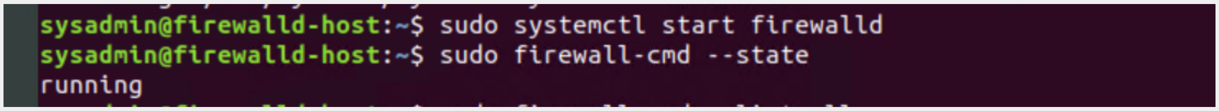
```
sudo apt-get install firewalld
sudo systemctl enable firewalld
sudo systemctl start firewalld
```

**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
```



```
sysadmin@firewalld-host:~$ sudo systemctl start firewalld
sysadmin@firewalld-host:~$ sudo firewall-cmd --state
running
```

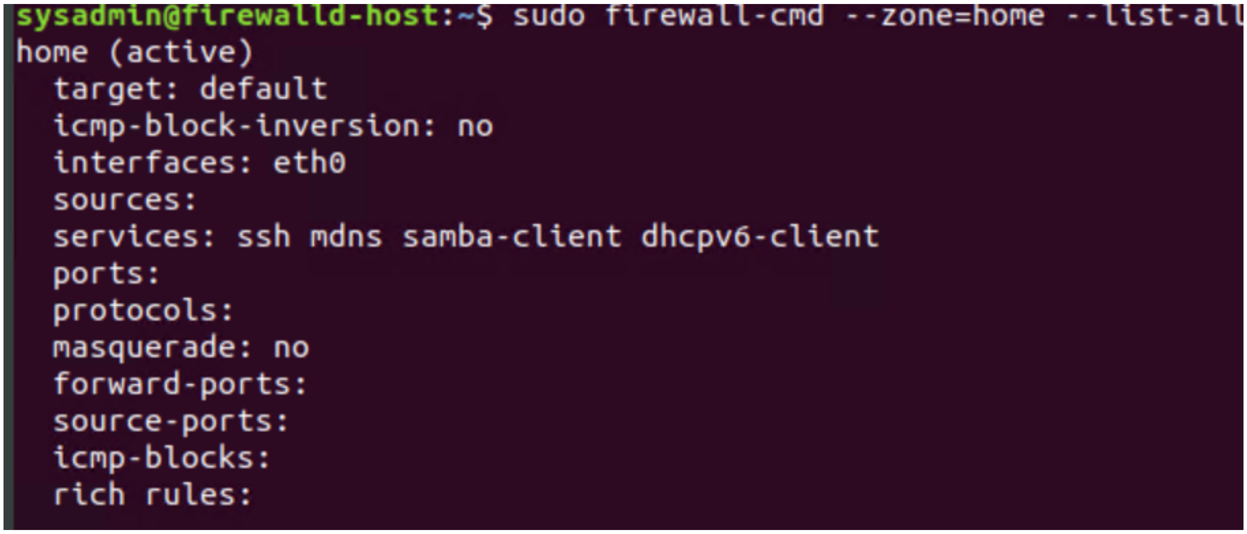
## List all firewall rules currently configured.

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 --zone-home --list-all
```

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

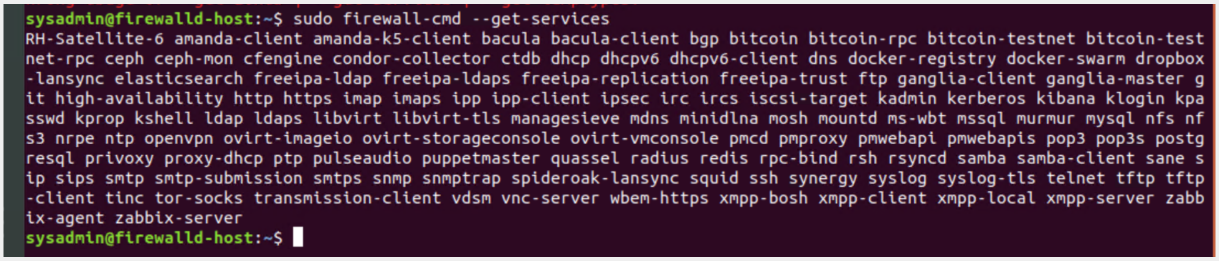


```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=home --list-all
home (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh mdns samba-client dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich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

## 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
```



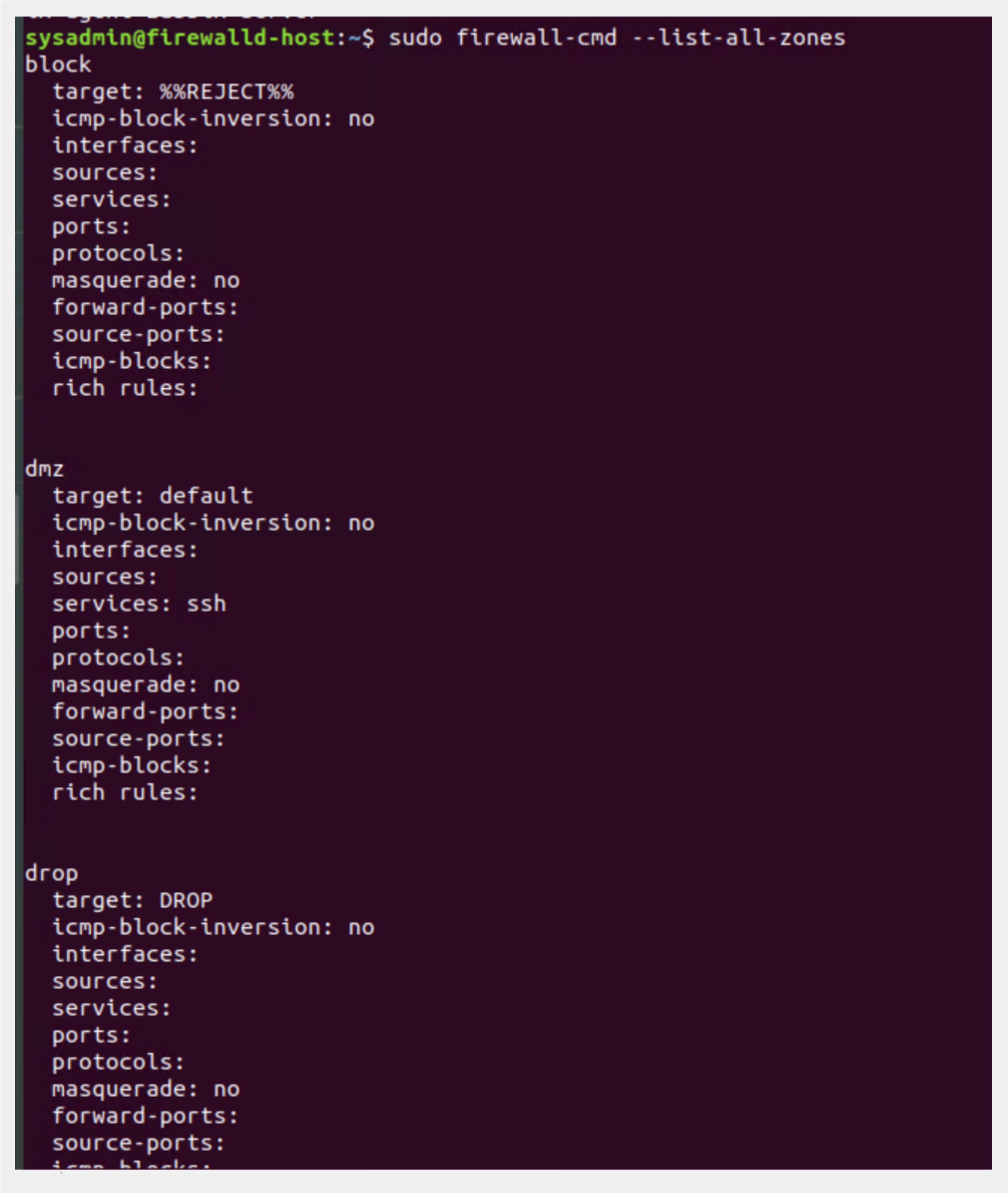
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-test
net-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp dhcpv6 dhcpv6-client dns docker-registry docker-swarm dropbox
-lansync elasticsearch freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client ganglia-master g
it high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target kadmin kerberos kibana klogin kpa
sswd kprop kshell ldap ldaps libvirt libvirt-tls managesieve mdns minidlna mosh mountd ms-wbt mssql murmur mysql nfs nf
s3 nrpe ntp openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postg
resql privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh rsyncd samba samba-client sane s
ip sips smtp smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh synergy syslog syslog-tls telnet tftp tftp
-client tinc tor-socks transmission-client vdsm vnc-server wbem-https xmpp-bosh xmpp-client xmpp-local xmpp-server zabb
ix-agent zabbix-server
sysadmin@firewalld-host:~$ 
```

- 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
```



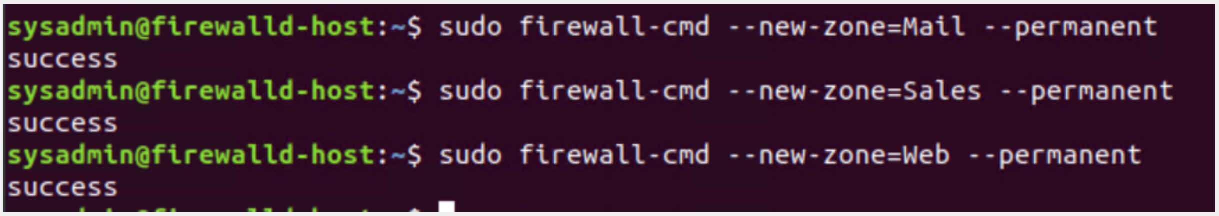
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


dmz
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


drop
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
```

- 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 --new-zone=Mail --permanent
sudo firewall-cmd --new-zone=Sales --permanent
sudo firewall-cmd --new-zone=Web -permanent
```

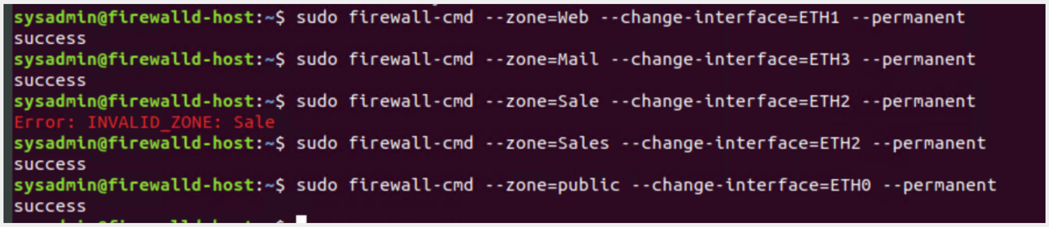


```
sysadmin@firewalld-host:~$ sudo firewall-cmd --new-zone=Mail --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --new-zone=Sales --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --new-zone=Web --permanent
success
```

## Set the zones to their designated interfaces.

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

```
sudo firewall-cmd --zone=Mail --change interface=ETH3 --permanent
sudo firewall-cmd --zone=Sale --change interface=ETH2 --permanent
sudo firewall-cmd --zone=Web --change interface=ETH1 --permanent
sudo firewall-cmd --zone=public --change interface=ETH0
--permanent
```



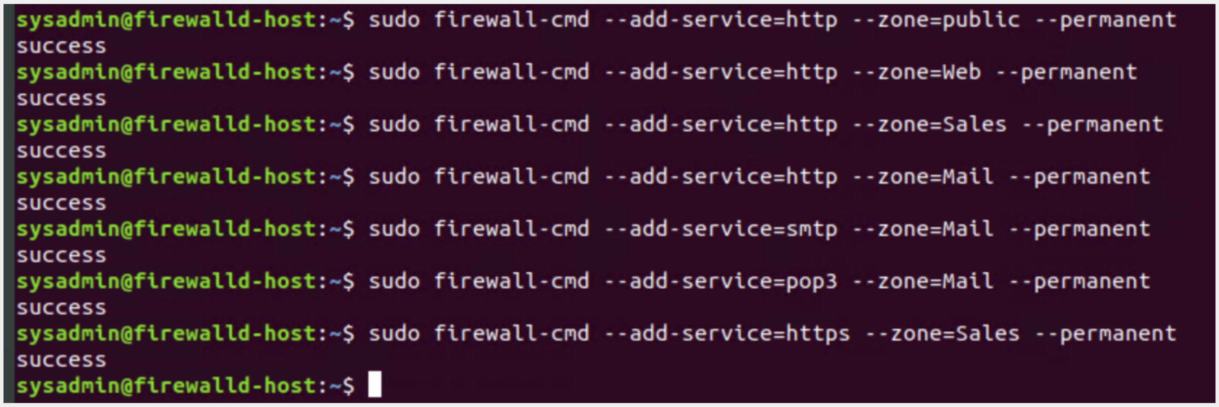
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Web --change-interface=ETH1 --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Mail --change-interface=ETH3 --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Sale --change-interface=ETH2 --permanent
Error: INVALID_ZONE: Sale
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Sales --change-interface=ETH2 --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --change-interface=ETH0 --permanent
success
```

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



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=http --zone=public --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=http --zone=Web --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=http --zone=Sales --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=http --zone=Mail --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=smtp --zone=Mail --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=pop3 --zone=Mail --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=https --zone=Sales --permanent
success
sysadmin@firewalld-host:~$ 
```

- `web`:

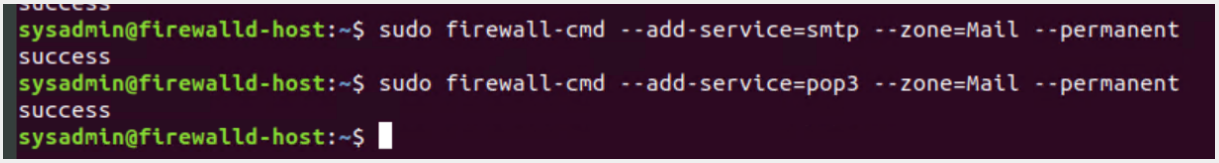
```
sudo firewall-cmd --add-service=http --zone=Web --permanent
```

- `sales`:

```
sudo firewall-cmd --add-service=http --zone=Sales --permanent
```

- `mail`:

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



```
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=smtp --zone=Mail --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --add-service=pop3 --zone=Mail --permanent
success
sysadmin@firewalld-host:~$ 
```

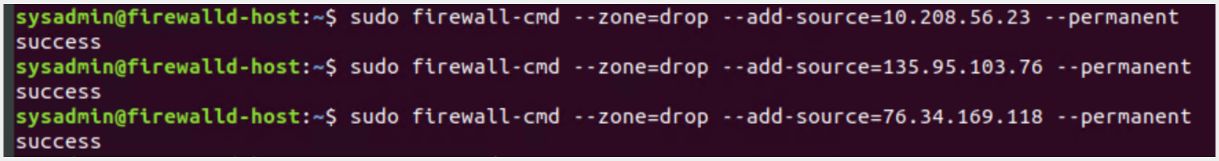
- What is the status of `http`, `https`, `smtp` and `pop3`?

```
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 --zone=drop --add-source=10.208.56.23 --permanent
sudo firewall-cmd --zone=drop --add-source=135.95.103.76 --permanent
sudo firewall-cmd --zone=drop --add-source=76.34.169.118 --permanent
```



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --add-source=10.208.56.23 --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --add-source=135.95.103.76 --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --add-source=76.34.169.118 --permanent
success
```

## 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:

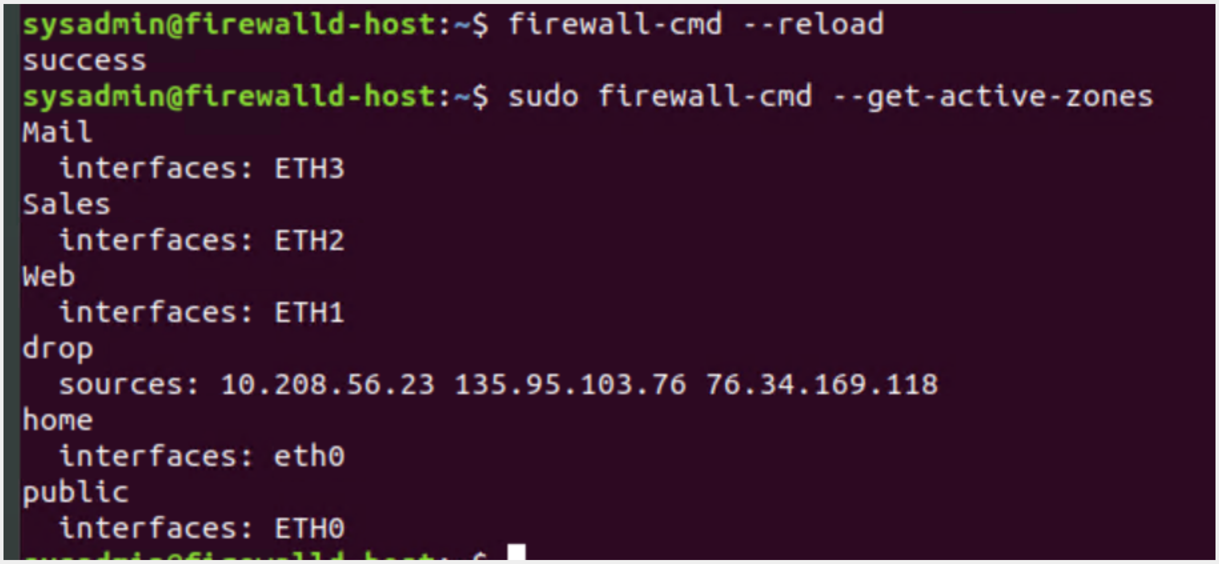
```
$  firewall-cmd --reload
```

## 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
```

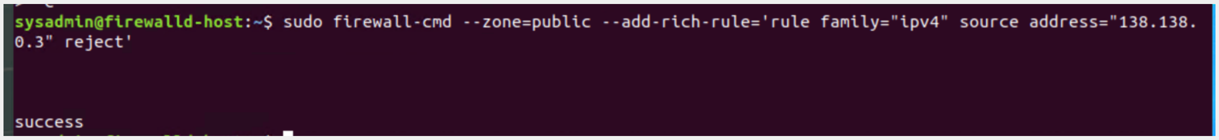


```
sysadmin@firewalld-host:~$ firewall-cmd --reload
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --get-active-zones
Mail
  interfaces: ETH3
Sales
  interfaces: ETH2
Web
  interfaces: ETH1
drop
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
home
  interfaces: eth0
public
  interfaces: ETH0
```

## Block an IP address.

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

```
$ sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source
address="138.138.0.3" reject'
```



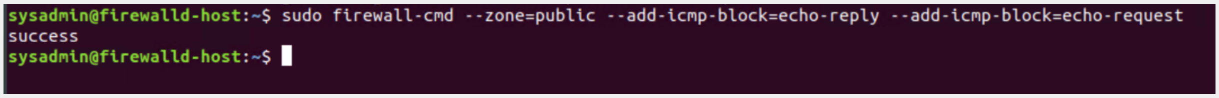
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="138.138.
0.3" reject'


success
```

## 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 --zone=public --add-icmp-block=echo-reply
--add-icmp-block=echo-request
```



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --add-icmp-block=echo-reply --add-icmp-block=echo-request
success
sysadmin@firewalld-host:~$
```

### 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=Web --list-all
sudo firewall-cmd --zone=Mail --list-all
sudo firewall-cmd --zone=Sales --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.

```
Promiscuous Mode:IDS is connected to a network segment via a network tap, a network switch's mirrored port, or a network hub.
```

```
In-line Mode:the IDS is positioned as a network gateway or bridge and
actively inspects all incoming and outgoing traffic.
```

2. Describe how an IPS connects to a network.

```
TAP or SPAN Port: Similar to IDS, an IPS can also be connected to a network
using a network tap or a switch's mirrored (SPAN) port.
```

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

```
Signature-Based IDS or Pattern-Matching 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 or Behavior-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.

```
The Physical Security Layer.
```

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

```
Security Monitoring and Incident Response.
```

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

```
Access Control and Authorization Layer.
```

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

```
the Host-Based Security Layer.
```

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

```
Network Security
```

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; hardening and configuration management 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.

```
Vpn
```

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

```
Location Tracking Software.  "Find My Device" or "Find My Laptop"
```

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

```
Set a BIOS/UEFI Password, Use Full Disk Encryption, Enable Secure Boot.
```

## 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 or a Stateful Inspection 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.

```
Application Layer Firewall or a Proxy 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 or simply a Proxy Server
```

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?

```
Packet Filtering Firewall or a Network Layer Firewall.
```

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

```
 MAC Filtering Firewall or a MAC Address 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?*)

```
[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]
```

Sources used: UTSA Bootcamp Module 11, Gitlab activities, Presentation slides, google, Chat gpt, PI.AI