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
```

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

```
Administrative Security
```

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

```
Operational Security
```

Intrusion Detection and Attack Indicators

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

An IDS main purpose is to monitor the network or system for any suspicious patterns or behaviors. An IDS is a stateless network meaning it does not alter packets/frames but creates logs which can be investigated.

An IPS does not only detect threats but also actively prevents and blocks them. An IPS is a stateful system as it's capable of implementing security protocols to control traffic.

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

Indicators of attack (IOA) are used as signs or a pattern that suggest an ongoing imminent attack or an attack in progress.

Indicator of compromise (IOC) is a piece of evidence/characteristic that suggests that the system had been compromised or affected by the 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 on the target to prepare for an attack

2. Stage 2:

Weaponization

- Create some kind of harmful software such as malware or a virus and install it on the target's computer.
- Example: Creating a backdoor via malware.

3. Stage 3:

```
Delivery
   -  Attacker sends the malicious software/payload to target.
   -  Example: Sending an email with a link to malicious software.
```

4. Stage 4:

```
Exploitation
   -  Having access to system and having the ability to breach the user’s
      machine
```

5. Stage 5:

```
Installation
   -  Installing malware to be able gain back door access to the system
```

6. Stage 6:

```
Command and Control (C2)
   -  Attackers communicated with the breached system to give orders
```

7. Stage 7:

```
Actions on Objectives
   -  The attacker would be achieving their main goal
   -  Example: Stealing data or damaging the network
```

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.

```
An alert is made that applies to TCP traffic, the traffic direction is from
an external IP to an internal network on ports 5800:5820, using TCP/IP
protocol.
```

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

```
Reconnaissance
```

3. What kind of attack is indicated?

```
Port Mapping
```

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.

```
An alert is made that applies to tcp traffic, the traffic direction is from
an external IP to any internal network on any port, an attempt to download
ET POLICY PE EXE or DLL Windows file download via HTTP (malicious payload).
```

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

```
Delivery
```

3. What kind of attack is indicated?

```
Malware Delivery
```

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

Part 2: “Drop Zone” Lab

Set up.

Log into the Azure `firewalld` machine using the following credentials:

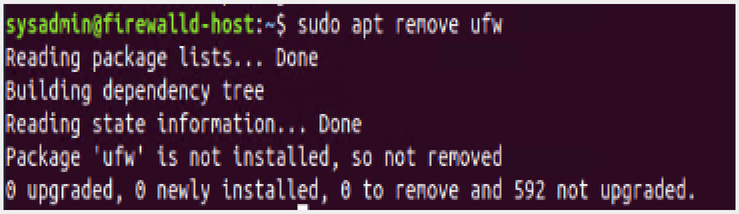
- Username: `sysadmin`
- Password: `cybersecurity`

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-get remove ufw
```

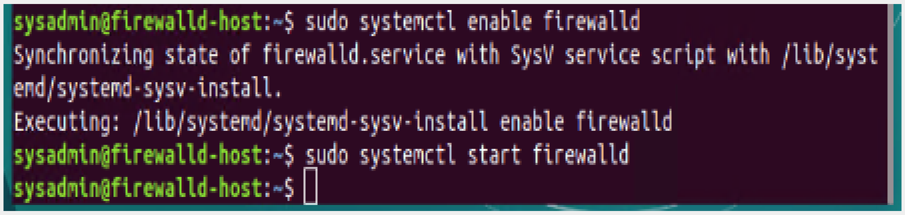


```
sysadmin@firewalld-host:~$ sudo apt remove ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'ufw' is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 592 not upgraded.
```

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
```



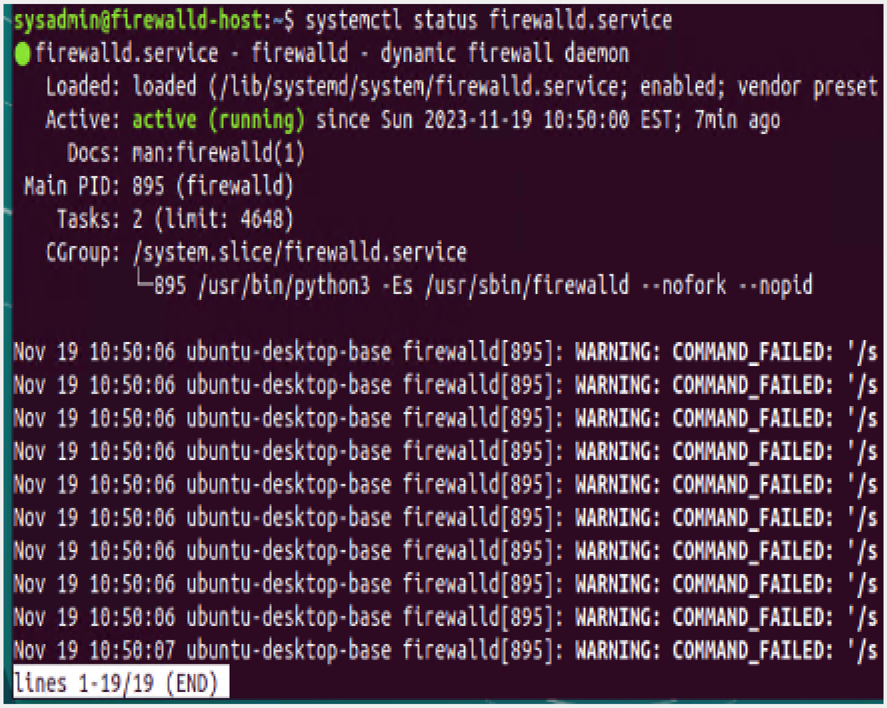
```
sysadmin@firewalld-host:~$ sudo systemctl enable firewalld
Synchronizing state of firewalld.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable firewalld
sysadmin@firewalld-host:~$ sudo systemctl start firewalld
sysadmin@firewalld-host:~$ 
```

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.

```
$ systemctl status firewalld.service
```



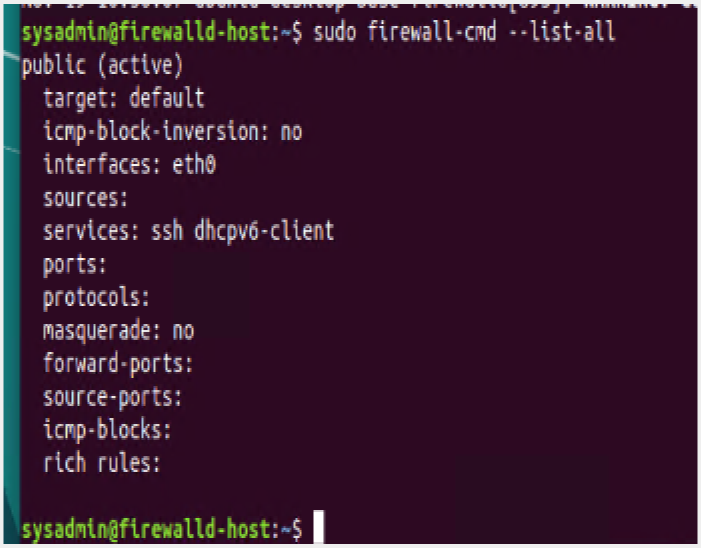
```
sysadmin@firewalld-host:~$ systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/lib/systemd/system/firewalld.service; enabled; vendor preset
     Active: active (running) since Sun 2023-11-19 10:50:00 EST; 7min ago
       Docs: man:firewalld(1)
   Main PID: 895 (firewalld)
      Tasks: 2 (limit: 4648)
     CGroup: /system.slice/firewalld.service
             └─895 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid

Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:06 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
Nov 19 10:50:07 ubuntu-desktop-base firewalld[895]: WARNING: COMMAND_FAILED: '/s
lines 1-19/19 (END)
```

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
```



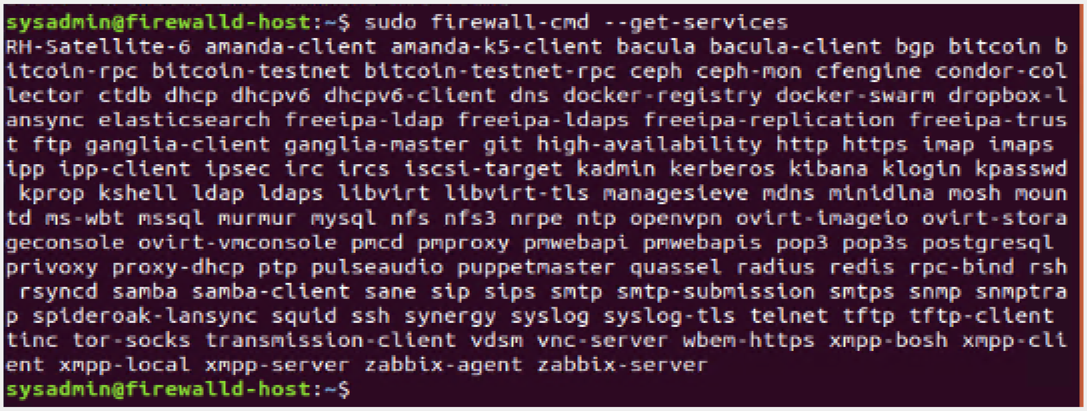
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

sysadmin@firewalld-host:~$
```

- 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 firewalld-cmd --get-services
```



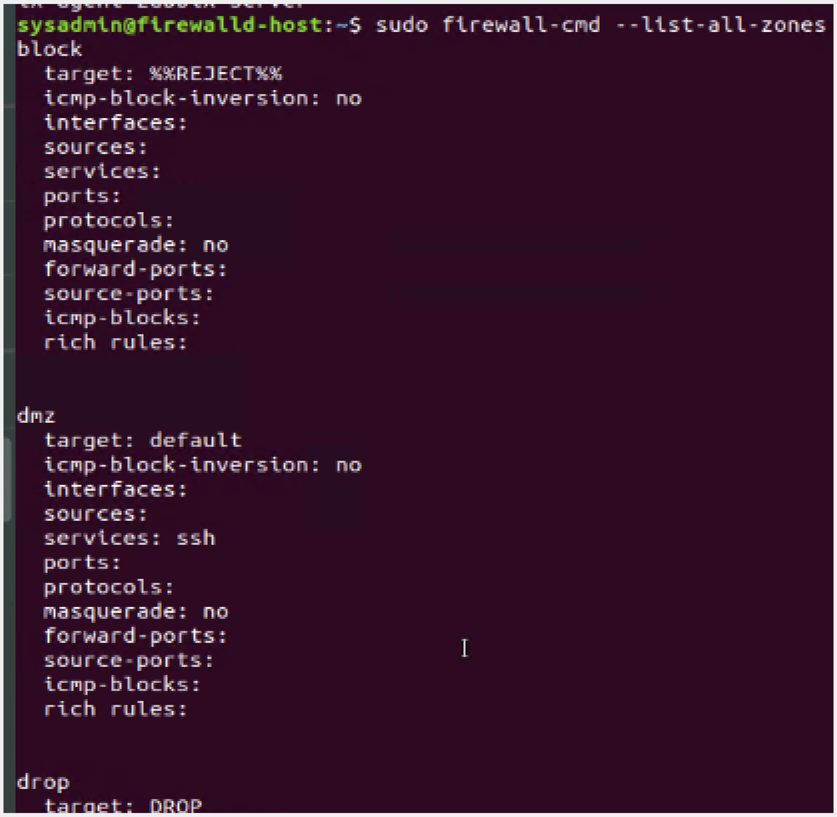
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp bitcoin b
itcoin-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-col
lector ctdb dhcp dhcpv6 dhcpv6-client dns docker-registry docker-swarm dropbox-l
ansync elasticsearch freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trus
t ftp ganglia-client ganglia-master git high-availability http https imap imaps
ipp ipp-client ipsec irc ircs iscsi-target kadmin kerberos kibana klogin kpasswd
 kprop kshell ldap ldaps libvirt libvirt-tls managesieve mdns minidlna mosh moun
td ms-wbt mssql murmur mysql nfs nfs3 nrpe ntp openvpn ovirt-imageio ovirt-stora
geconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql
privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh
 rsyncd samba samba-client sane sip sips smtp smtp-submission smtps snmp snmptra
p 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-cli
ent xmpp-local xmpp-server zabbix-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
```



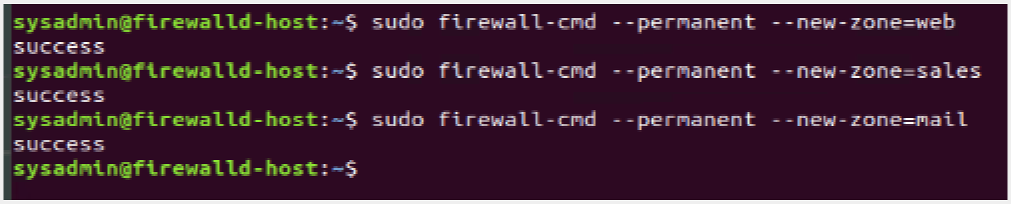
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


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
```

- 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
```

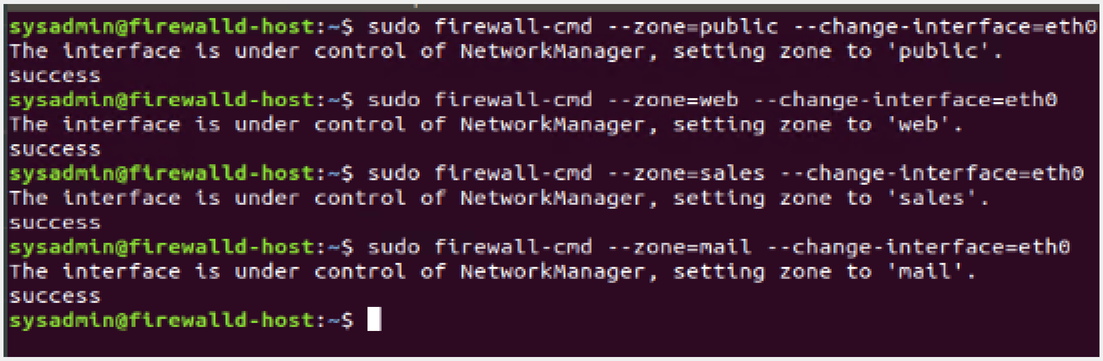


```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=web
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=sales
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=mail
success
sysadmin@firewalld-host:~$
```

Set the zones to their designated interfaces.

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

```
$ 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
```



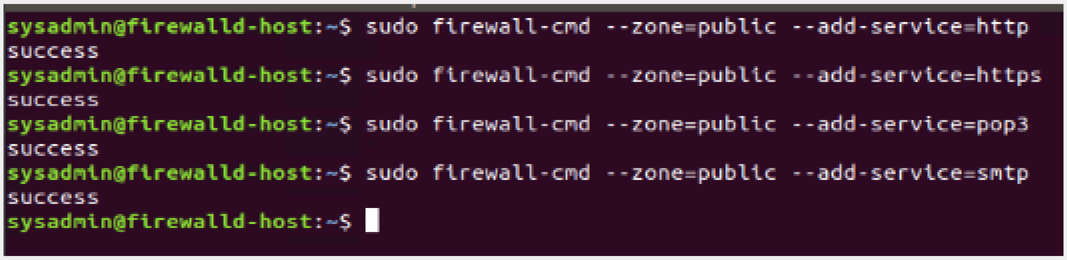
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --change-interface=eth0
The interface is under control of NetworkManager, setting zone to 'public'.
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=web --change-interface=eth0
The interface is under control of NetworkManager, setting zone to 'web'.
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=sales --change-interface=eth0
The interface is under control of NetworkManager, setting zone to 'sales'.
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=mail --change-interface=eth0
The interface is under control of NetworkManager, setting zone to 'mail'.
success
sysadmin@firewalld-host:~$
```

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`:

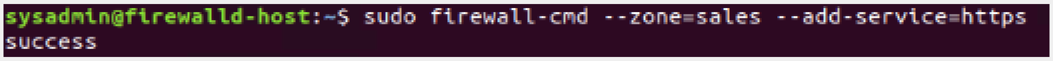
```
$ sudo firewall-cmd --zone=public --add-service=http
$ sudo firewall-cmd --zone=public --add-service=https
$ sudo firewall-cmd --zone=public --add-service=pop3
$ sudo firewall-cmd --zone=public --add-service=smtp
```



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

- `web`:

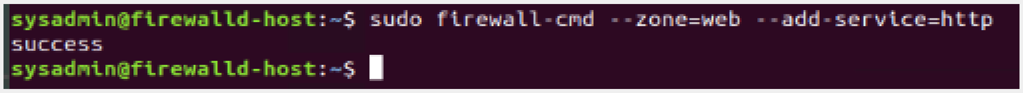
```
$ sudo firewall-cmd --zone=web --add-service=http
```



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=sales --add-service=https
success
```

- `sales`:

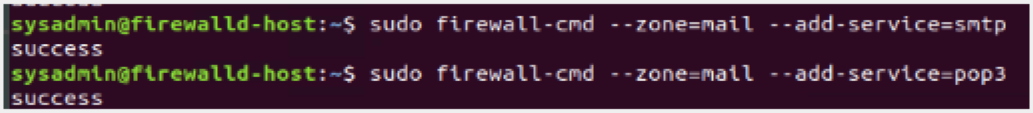
```
$ sudo firewall-cmd --zone=sales --add-service=https
```



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=web --add-service=http
success
sysadmin@firewalld-host:~$
```

- `mail`:

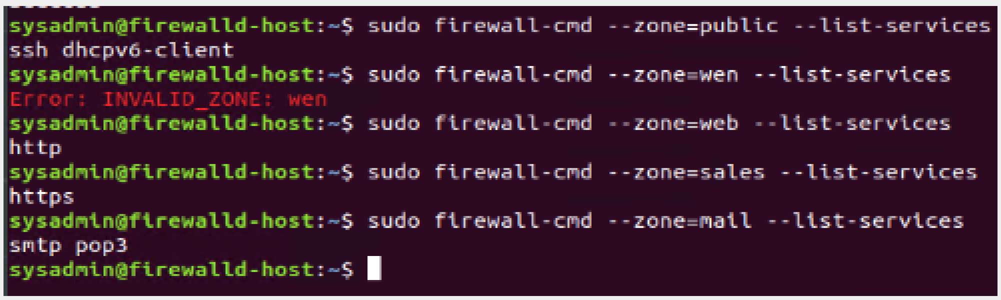
```
$ sudo firewall-cmd --zone=mail --add-service=smtp
$ sudo firewall-cmd --zone=mail --add-service=pop3
```



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

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

```
sudo firewall-cmd --zone=public --list-services
sudo firewall-cmd --zone=web --list-services
sudo firewall-cmd --zone=sales --list-services
sudo firewall-cmd --zone=mail --list-services
```

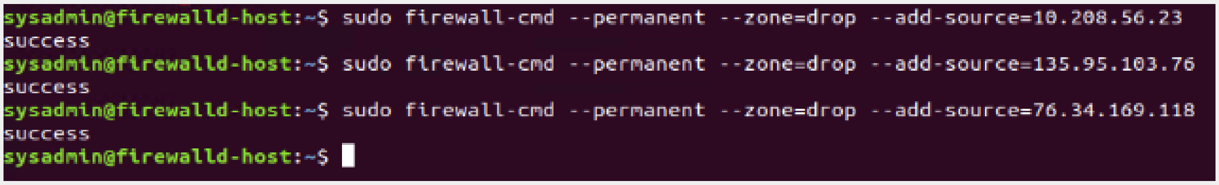


```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --list-services
ssh dhcpv6-client
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=wen --list-services
Error: INVALID_ZONE: wen
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=web --list-services
http
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=sales --list-services
https
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=mail --list-services
smtp pop3
sysadmin@firewalld-host:~$
```

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
```



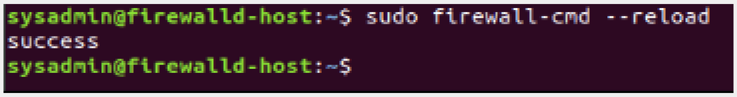
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=drop --add-source=10.208.56.23
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=drop --add-source=135.95.103.76
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=drop --add-source=76.34.169.118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

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
```



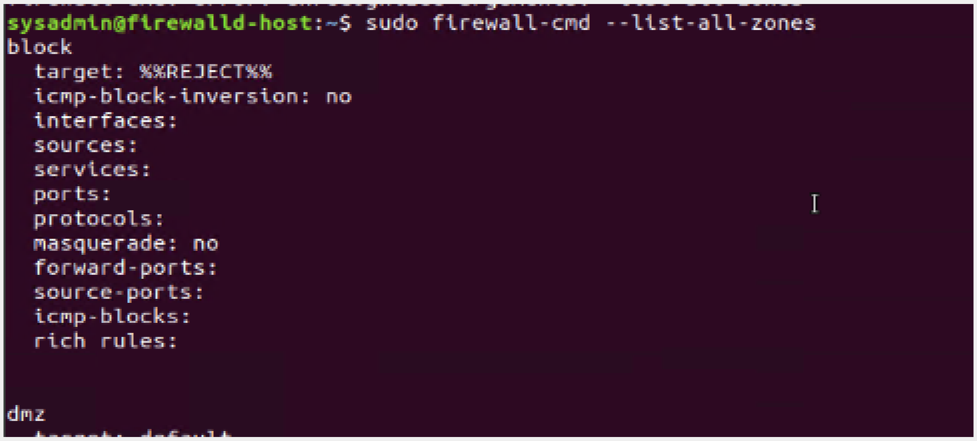
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --reload
success
sysadmin@firewalld-host:~$
```

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 -list-all-zones
```

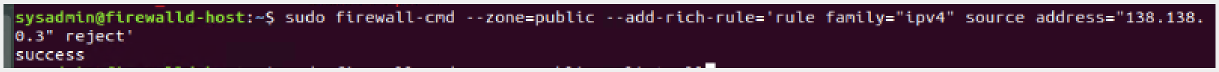


```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


dmz
```

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'
```



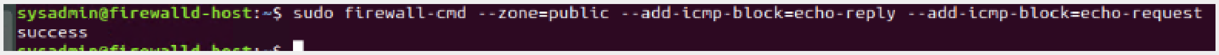
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="138.138.
0.3" reject'
success
```

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
```



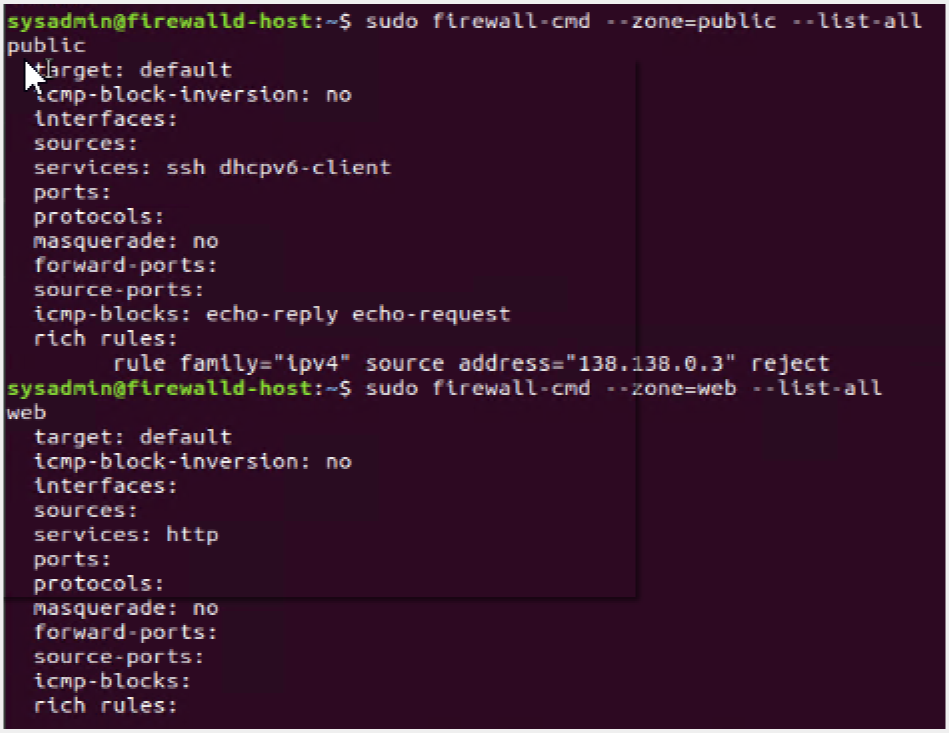
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --add-icmp-block=echo-reply --add-icmp-block=echo-request
success
sysadmin@firewalld-host:~$
```

Rule check.

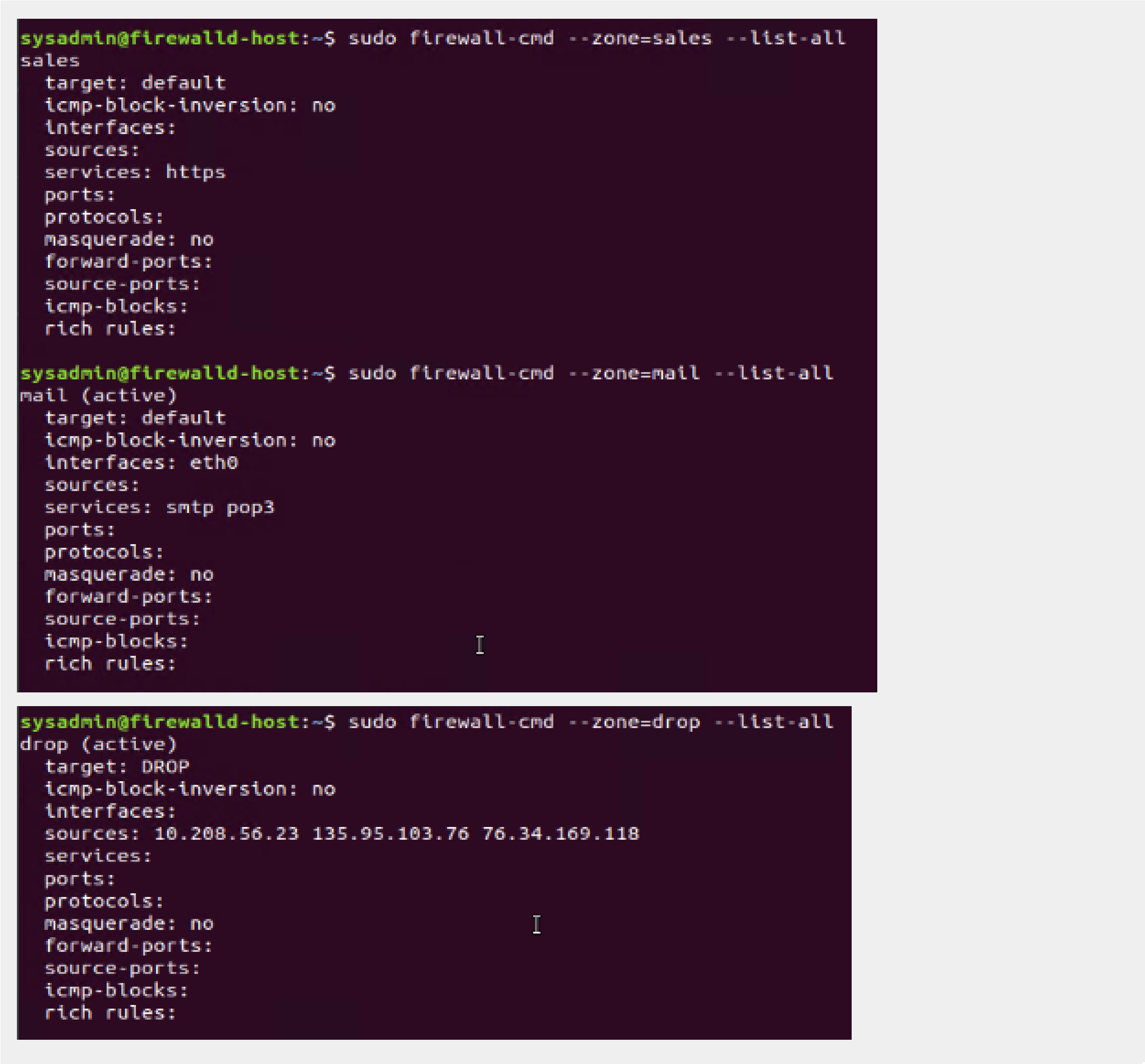
Now that you've set up your brand new firewalld installation, it's time to verify that all of the settings have taken effect.

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



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks: echo-reply echo-request
  rich rules:
        rule family="ipv4" source address="138.138.0.3" reject
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=web --list-all
web
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: http
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```



```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=sales --list-all
sales
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=mail --list-all
mail (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: smtp pop3
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --list-all
drop (active)
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- 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.

HIDS (Host based detection system) - A Host based detection system. It monitors the system for malicious activity.

NIDS (Network based detection system) - Monitors networking traffic for suspicious patterns.

2. Describe how an IPS connects to a network.

An IPS is placed behind the firewall and monitors traffic for any abnormal behavior

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

A stateless IDS is unable to detect zero-day attacks. It compares patterns of traffic to predefined signatures and is unable to do anything out of that domain. An example would be a 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?

A stateful IDS is able to detect suspicious traffic and is excellent at detecting when an attacker probes or sweeps a network. Stateful tends to have more features making it a good tool for analyzing traffic.An example would be an 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.

```
Administrative Policy
```

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

```
Technical Software
```

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

```
 Network Security
```

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

```
Technical Software, Patch Management
```

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.

```
Administrative Procedures
```

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

```
Administrative Network
```

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

```
Drive/Disk Encryption
```

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

```
Data Encryption/TLS
```

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

```
Trackers/GPS
```

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

```
BIOS/UEFI Password or Disk Encryption
```

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 gateways
```

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?

```
Packet filtering firewall
```

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

```
Data link 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]
```