

# Network Security

## 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

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

**Answer:** Administrative

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

**Answer:** Technical

### Intrusion Detection and Attack indicators

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

**Answer:** The difference between IDS (Intrusion Detection System and IPS (Intrusion Prevention System, is that IDS can only detect, alert, and log when an attack occurs which can help with hardening defense (gathering attack info), however, IPS does everything that IDS does with the added response to the attack by blocking the malicious traffic. Also, IPS requires more hardware than the IDS. IDS connects via mirrored SPAN port, and IPS connects inline with the flow of data.

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

**Answer:** The differences between IOA (Indicator of Attack) and IOC (Indicator of Compromise) are: **IOA** indicates malicious attack in real time, where **IOC** indicates previous malicious attacks. **IOA** has a proactive approach to intrusion attempts, where **IOC** indicates that an attack occurred which resulted in a breach. **IOA** focuses on revealing the intent and the goal of the attacker regardless of the means, where **IOC** exposes all vulnerabilities used in the attack, thus providing the network defenders the opportunity to learn how to revamp their defense as part of mitigation strategy.<sup>1</sup>

### 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:** Research, gathering names, titles, email addresses or any other useful information of the targets, which also includes a selection of desired targets. The hackers will identify a specific target, and plan their point of attack.
2. **Stage 2: Weaponization:** Hackers have a vast amount of code and types of exploit at their disposal, and they need to tweak their attack based on the networks, operating system, and software of their target/s. Identifying those components, they will be able to customize their malware payload.
3. **Stage 3: Delivery:** In this stage the hacker will deliver the malware payload to the targeted environment via email, websites, attachments, or any other available means of delivery. This part of the attack comes with a risk to the hacker by providing some digital fingerprinting in case the attack will be discovered at this stage.
4. **Stage 4: Exploitation:** At this stage, looking and finding weaknesses in the target's environment for manipulation is the main objective. the malware payload/code is activated and will start exploiting vulnerabilities.
5. **Stage 5: Installation:** At this stage, the hacker will install a remote access Trojan or backdoor in the target's environment, and by doing so the hacker will be able to maintain presence inside that environment at will. Some malware installation in the target's environment will require the target's unknown participation by enabling the malicious code.

6. **Stage 6: Command and Control:** Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network.<sup>2</sup>
7. **Stage 7: Actions & Objectives:** The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.<sup>3</sup>

## Snort Rule Analysis

Use the Snort rule 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;)
```

Break down the Sort Rule header and explain what is happening.

**Answer:** The sort rule will alert for any tcp protocol using source \$external\_net (ip), from any source ports, to \$home\_net (ip) destination with ports between 5800:5820.

**alert:** Generate an intrusion event when triggered.

**tcp:** Tests tcp traffic only.

**\$EXTERNAL\_NET:** Tests traffic coming from any host that is not on your internal network.

**any:** Tests traffic coming from any port on the originating host (source).

**->:** toward.

**\$HOME\_NET:** the destination ip address

**5800:5820:** apply the rule to traffic to the destination port

---

<sup>2</sup> [https://upload.wikimedia.org/wikipedia/commons/1/1d/Intrusion\\_Kill\\_Chain\\_-\\_v2.png](https://upload.wikimedia.org/wikipedia/commons/1/1d/Intrusion_Kill_Chain_-_v2.png)

<sup>3</sup> [https://upload.wikimedia.org/wikipedia/commons/1/1d/Intrusion\\_Kill\\_Chain\\_-\\_v2.png](https://upload.wikimedia.org/wikipedia/commons/1/1d/Intrusion_Kill_Chain_-_v2.png)

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

**Answer:** This violates the Reconnaissance kill chain stage by **classtype:** attempted-recon

3. What kind of attack is indicated?

**Answer:** This is a port scan attack since it looks like they were scanning for open ports (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 Sort Rule header and explain what is happening.

The sort rule will alert for any tcp protocol using source external ips with 80 source ports to internal ips destinations with any ports.

**Answer:** The sort rule will alert for any tcp protocol using source \$external\_net (ip) with \$http source port, to \$home\_net (ip) destination with any ports.

**alert:** Generates an intrusion event when triggered.

**tcp:** Tests TCP traffic only.

**\$EXTERNAL\_NET:** Tests traffic coming from any host that is not on your internal network.

**\$HTTP\_PORTS:** apply the rule to the source port.

**->:** towards

**\$HOME\_NET:** apply the rule to destination ip address

**any:** apply the rule to traffic to the destination port.

2. What stage of the Cyber Kill Chain does the alerted activity violate?

**Answer:** This violates the Installation cyber kill chain by **classtype:policy-violation**.

3. What kind of attack is indicated?

**Answer:** This is a download from http without admin approval. Threat of EXE or DLL file download.

#### 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 any any -> any 4444 (msg:"inbound traffic using port 4444")`

## Part 2: "Drop Zone" Lab

### Log into the Azure firewall 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 firewall 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, these services should be running. If not, then run the following commands:

Run the commands that enable(1) and start(2) firewalld upon boots and reboots.

1. `$sudo systemctl enable firewalld`

2. `$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.

`$sudo /etc/init.d/firewalld status`

- **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:

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

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

`block, dmz, drop, external, home, internal, public, trusted, work`

## 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.

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

```
sysadmin@\firewalld-host: ~
File Edit View Search Terminal Help
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 minidlina 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-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:~$
```

- We can see 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-active-zones`

```
sysadmin@\firewalld-host: ~
File Edit View Search Terminal Help
sysadmin@firewalld-host:~$ sudo firewall-cmd --get-active-zones
drop
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
mail
  interfaces: eth3
  sources: 201.45.105.12
public
  interfaces: eth0
sales
  interfaces: eth2
  sources: 201.45.15.48
web
  interfaces: eth1
  sources: 201.45.34.126
sysadmin@firewalld-host:~$
```

- 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 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 --change-interface=eth0  
$sudo firewall-cmd --permanent --zone=web --change-interface=eth1  
$sudo firewall-cmd --permanent --zone=sales --change-interface=eth2  
$sudo firewall-cmd --permanent --zone=mail --change-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  
  
$sudo firewall-cmd --permanent --zone=web --add-source=201.45.34.126
```

#### **Sales:**

```
$sudo firewall-cmd --permanent --zone=sales --add-service=https  
  
$sudo firewall-cmd --permanent --zone=sales --add-source=201.45.15.48
```

#### **Mail:**

```
$sudo firewall-cmd --permanent --zone=mail --add-service=smtp  
$sudo firewall-cmd --permanent --zone=mail --add-service=pop3  
$sudo firewall-cmd --permanent --zone=Mail --add-source=201.45.105.12
```



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

**Answer:** The status of services http, https, smtp, and pop3 is **(active)**.

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

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

Blacklisted ip addresses to be dropped:

10.208.56.23

135.95.103.76

76.34.169.118

```
$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
```

**or:**

```
$sudo firewall-cmd --permanent --zone=drop --add-source={10.208.56.23,  
135.95.103.76,76.34.169.118}
```

### **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 ensures 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

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

**--permanent:** The permanent option can be used to set options permanently. These changes are not effective immediately, only after service restart/reload, or system reboot. Without the --permanent option, a change will only be part of the runtime configuration.

## View active Zones

Now, we'll want to 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-zone Or  
$sudo firewall-cmd --list-all-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 --zone=public --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 echo replies.

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

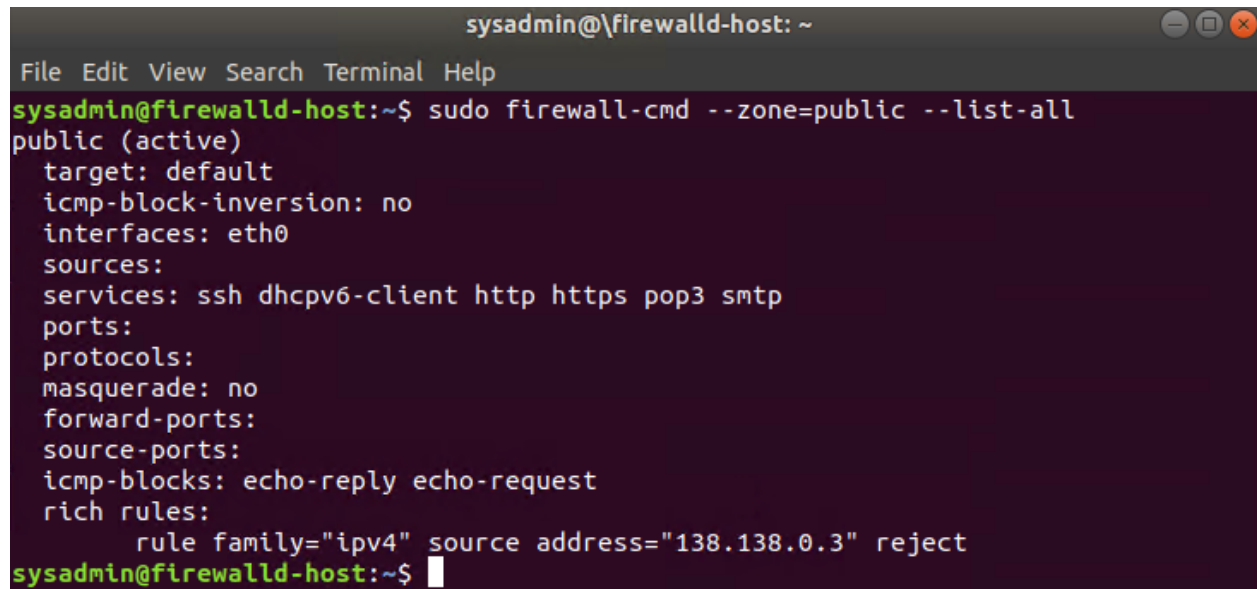
```
$sudo firewall-cmd --permanent --zone=public  
--add-icmp-block={echo-reply,echo-request}
```

## 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.

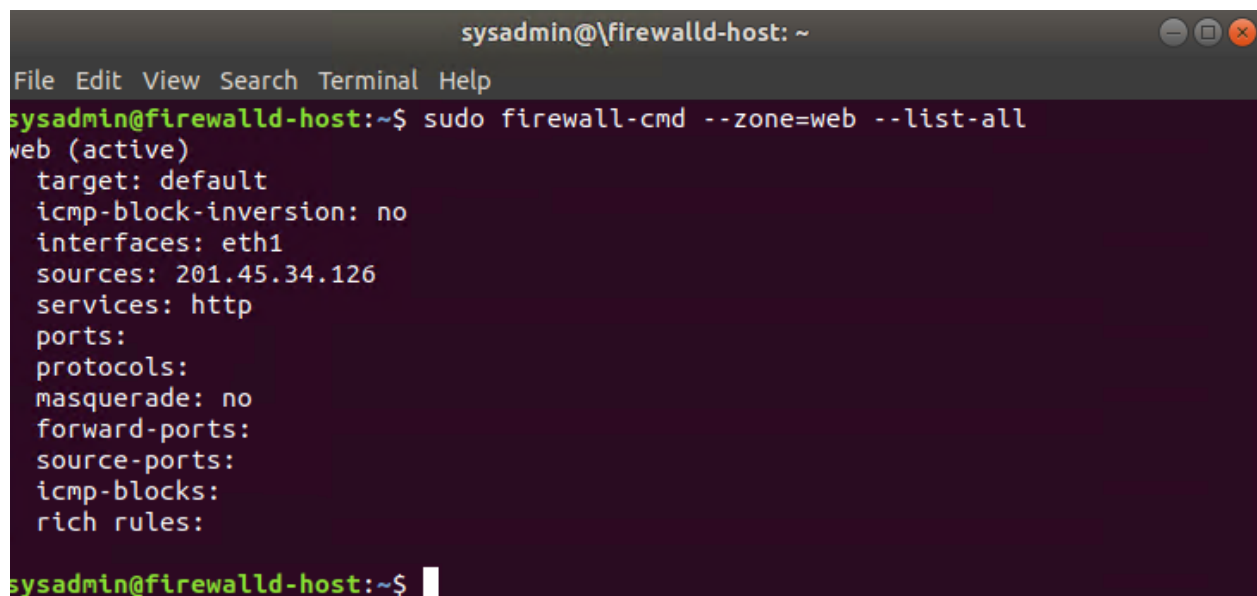
Run the command that lists all of the rule settings. Do one command at a time for each zone.

```
$sudo firewall-cmd --zone=public --list-all
```



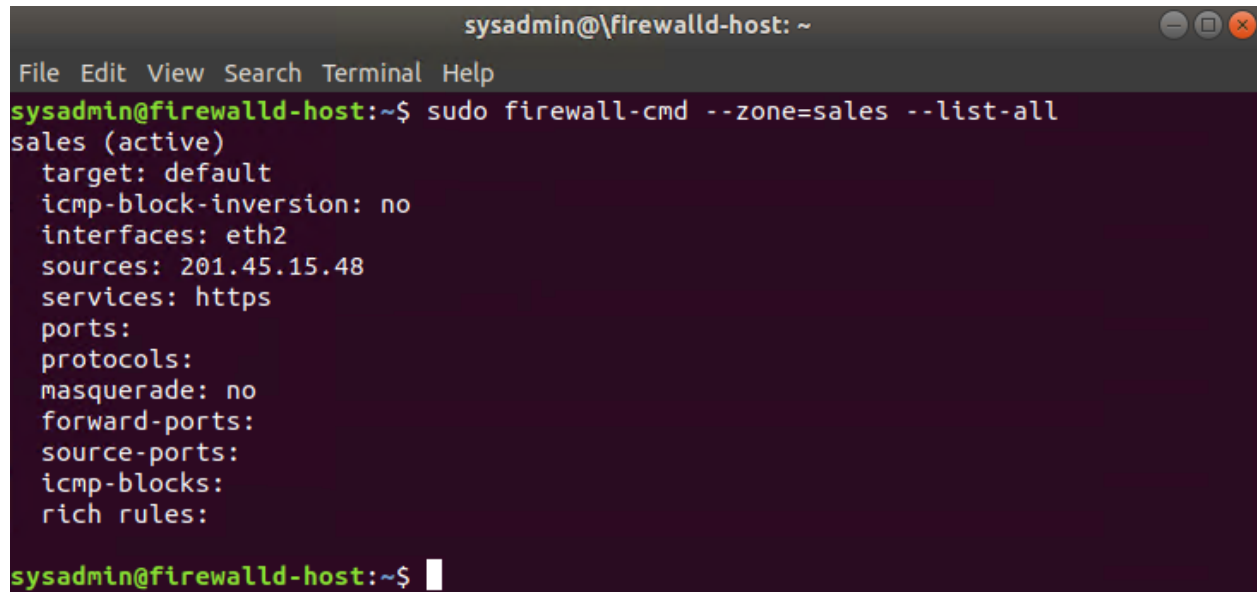
```
sysadmin@\firewalld-host: ~
File Edit View Search Terminal Help
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks: 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
```



```
sysadmin@\firewalld-host: ~
File Edit View Search Terminal Help
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=web --list-all
web (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1
  sources: 201.45.34.126
  services: http
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
sysadmin@firewalld-host:~$
```

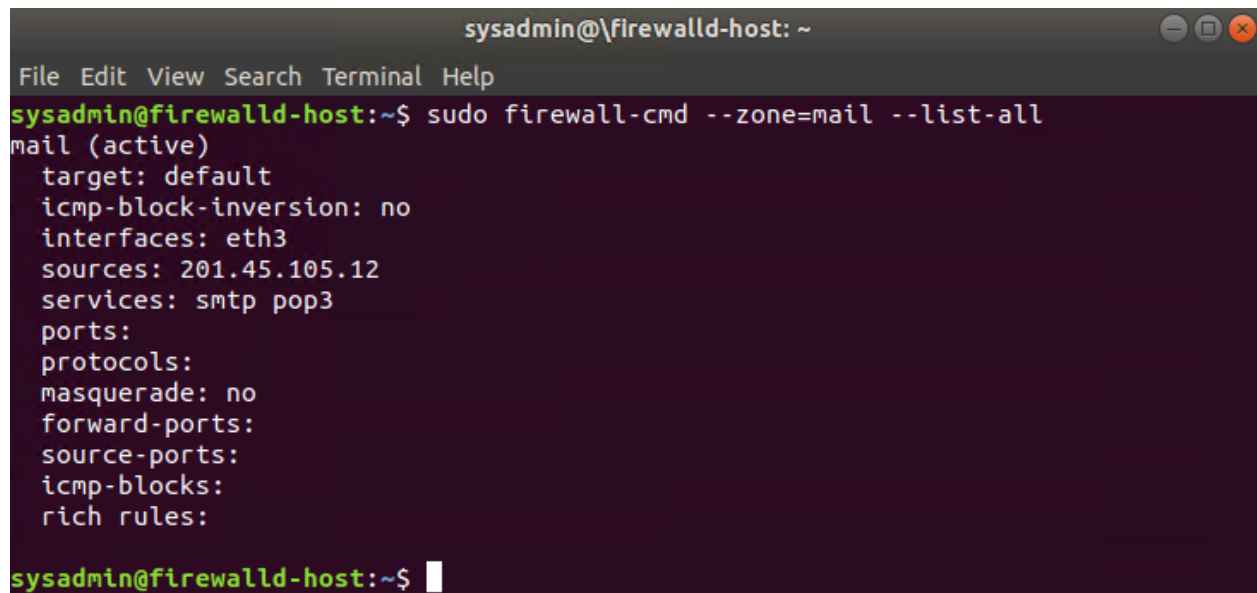
`$sudo firewall-cmd --zone=sales --list-all`

A terminal window titled 'sysadmin@\firewalld-host: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'sysadmin@firewalld-host:~\$'. The command 'sudo firewall-cmd --zone=sales --list-all' has been executed. The output shows the configuration for the 'sales' zone, which is active. The configuration includes: target: default, icmp-block-inversion: no, interfaces: eth2, sources: 201.45.15.48, services: https, ports: (empty), protocols: (empty), masquerade: no, forward-ports: (empty), source-ports: (empty), icmp-blocks: (empty), and rich rules: (empty). The prompt returns to 'sysadmin@firewalld-host:~\$' with a cursor.

```
sysadmin@\firewalld-host: ~
File Edit View Search Terminal Help
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=sales --list-all
sales (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth2
  sources: 201.45.15.48
  services: https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

sysadmin@firewalld-host:~$
```

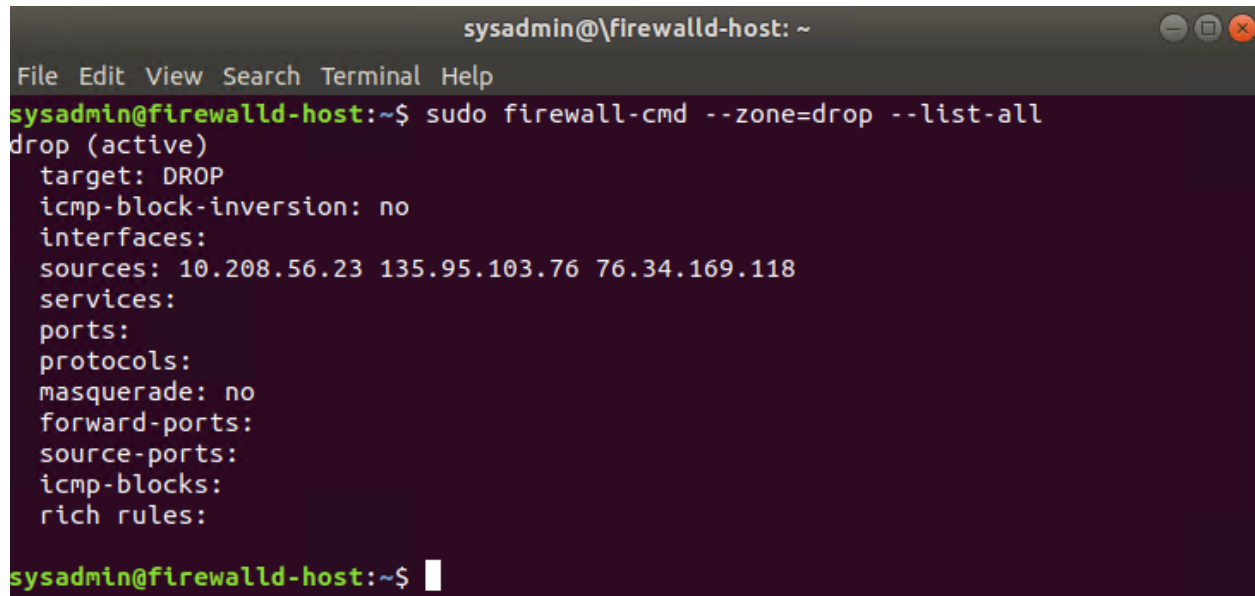
`$sudo firewall-cmd --zone=mail --list-all`

A terminal window titled 'sysadmin@\firewalld-host: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'sysadmin@firewalld-host:~\$'. The command 'sudo firewall-cmd --zone=mail --list-all' has been executed. The output shows the configuration for the 'mail' zone, which is active. The configuration includes: target: default, icmp-block-inversion: no, interfaces: eth3, sources: 201.45.105.12, services: smtp pop3, ports: (empty), protocols: (empty), masquerade: no, forward-ports: (empty), source-ports: (empty), icmp-blocks: (empty), and rich rules: (empty). The prompt returns to 'sysadmin@firewalld-host:~\$' with a cursor.

```
sysadmin@\firewalld-host: ~
File Edit View Search Terminal Help
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=mail --list-all
mail (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth3
  sources: 201.45.105.12
  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`



```
sysadmin@\firewalld-host: ~
File Edit View Search Terminal Help
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:

sysadmin@firewalld-host:~$
```

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

**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:** Network TAP (test access port), which is a hardware device that provides access to the network. it transit both inbound and outbound data streams on separate channels at the same time. all the data will arrive at the monitoring device at the same time.<sup>4</sup>

---

4

[https://docs.google.com/presentation/d/1I0MqNWSZaoKeWaVVuMAESJIROz3ZXbbPhrbnNlwQTpo/edit#slide=id.g713e0b84c3\\_0\\_71](https://docs.google.com/presentation/d/1I0MqNWSZaoKeWaVVuMAESJIROz3ZXbbPhrbnNlwQTpo/edit#slide=id.g713e0b84c3_0_71)

**Answer 2:** [Mirrored SPAN port \(switched port analyzer\)](#), which is known as port mirroring, sends a mirror image of all network data to another physical port where the packets are captured and analyzed.<sup>5</sup>

2. Describe how an IPS connects to a network.

**Answer:** [IPS connects inline with the flow of data, typically between the firewall and the network switch.](#)<sup>6</sup>

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

**Answer:** [Signature based IDS.](#)

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:** [Anomaly-based IDS.](#)

## 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:** [Perimeter](#)

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

**Answer:** [Application](#)

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

**Answer:** [Data](#)

---

<sup>5</sup>

[https://docs.google.com/presentation/d/1I0MqNWSZaoKeWaVVuMAESJIROz3ZXbbPhrbnNlwQTpo/edit#slide=id.g713e0b84c3\\_0\\_71](https://docs.google.com/presentation/d/1I0MqNWSZaoKeWaVVuMAESJIROz3ZXbbPhrbnNlwQTpo/edit#slide=id.g713e0b84c3_0_71)

<sup>6</sup>

[https://docs.google.com/presentation/d/1I0MqNWSZaoKeWaVVuMAESJIROz3ZXbbPhrbnNlwQTpo/edit#slide=id.g71707969e3\\_0\\_350](https://docs.google.com/presentation/d/1I0MqNWSZaoKeWaVVuMAESJIROz3ZXbbPhrbnNlwQTpo/edit#slide=id.g71707969e3_0_350)

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

**Answer:** Host

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

**Answer:** Network

6. Data is classified at the wrong classification level.

**Answer:** Data

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

**Answer:** Network

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

**Answer:** One method protecting data at rest is by encrypting the hard drive. More steps to increase security can help as well, such as storing data in different locations, which reduces the amount of data at risk if a security breach occurs.

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

**Answer:** One method to protect data-in-transit would be using private and public key based encryption when transmitting/moving data, individuals/or businesses will often encrypt sensitive data, and use encrypted connections for added security measures. Ideal secure connection will be as follows: HTTPS,SSL,TLS,FTPS.

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

**Answer:** A laptop-specific program that works closely with law enforcement to recover a stolen laptop. LoJack for Laptops is available for Mac OS X and Windows as far back as 2000. The Computrace Agent, part of the LoJack software, works in the background and

resists detection. LoJack gives you the ability to remote access your laptop to lock, delete sensitive files, and locate your stolen laptop.<sup>7</sup>

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

**Answer:** Disable bios boot options, and put a bios password, are one of best ways to prevent a stolen laptop from booting.

### 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:** Circuit-level firewalls.

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:** Packet-filtering firewall (stateful).

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:** Application (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 (stateless).

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

**Answer:** Mac layer firewall.

---

<sup>7</sup> [www.pcmag.com/news/six-security-apps-that-can-help-recover-a-stolen-laptop](http://www.pcmag.com/news/six-security-apps-that-can-help-recover-a-stolen-laptop)



## Bonus 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 into the Security Onion VM and use the following **Indicator of Attack** to complete this portion of the homework.

Locate the following 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:

1. What was the indicator of an attack?
  - Hint: What do the details of the reveal?

**Answer:** The indicator of attack (IOA) is an alert notifying us that a Trojan EXE file payload was downloaded.

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

**Answer:** The purpose of the attack was to download Command & Control files that would phone home after a reboot. The trojan file will download Gozi infostealer.

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
<b>Reconnaissance</b>	How did the attacker locate the victim? Through a malware spam campaign (email).	
<b>Weaponization</b>	What was it that was downloaded? JavaScript downloader file embedded in a zip file that is attached to an email.	
<b>Delivery</b>	How was it downloaded? When a user unsuspectingly clicks on the attached zip file and runs the JavaScript it contains.	
<b>Exploitation</b>	What does the exploit do? Nemucod will Install three different ActiveX controls.	
<b>Installation</b>	How is the exploit installed? Nemucod will use the ActiveX controls to save an executable file to a temporary folder %TEMP% and to run it.	
<b>Command &amp; Control (C2)</b>	How does the attacker gain control of the remote machine? Files downloaded by Nemucod are used to retrieve a Trojan Downloader called Fareit or Pony Downloader., which in turn downloads another set of executable files containing the Gozi infostealer. Once Gozi was installed, he started phoning home.	
<b>Actions on Objectives</b>	What does the software that the attacker sent do to complete it's tasks? The purpose of the attack is to gain access to the target's private data.	

4. What are your recommended mitigation strategies?

**Answer:** Block the domains used in the IOC for all the campaigns. Educate employees on not opening up emails, and clicking on attacked files from unknown sources. Implement snore signatures to detect both the decory pdf and the Nemucod execution.

5. List your third-party references.

Answer: [Italian spam campaigns using JS/Nemucod downloader | Certego](#)  
[Threat Spotlight: URSNIF Infostealer Malware \(blackberry.com\)](#)