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

Intrusion Detection and Attack indicators

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

   IDS is passive, detected traffic and creates alerts so that administrators have to action whereas IPS is an active, will do everything IDS can but does an extra step by responding to attacks

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

   Indicator of Attack (IOA) happens in real time, it is proactive and will focus on revealing the intent of the attacker.

   Indicator of Compromise (IOC) indicates previous malicious activity. It is a reactive response to attack as an attack has occured. Therefore there is a need to fix vulnerabilities and learn from the attacker so that a breach will not happen again

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, gathering information from sources such as social media
2. Stage 2:Weaponization, the development of malware or program for intended target
3. Stage 3:Delivery, to deliver the weaponised payload, via email or USB
4. Stage 4:Exploitation, once the payload has been opened and downloaded, attackers can then use the device of its host

5. Stage 5:Installation, the installation of software or backdoor implants
6. Stage 6:Command and control, will security being compromised attackers will gain full access of network
7. Stage 7:Actions on objective, attackers will act out their objectives such as stealing information, hold for ransom and disrupt systems.

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;)

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

   External host using any port attempted to scan local network on ports ranging from 5800-5820 using a TCP protocol. This can be triggered by using nmap.

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

   Stage 1, reconnaissance

3. What kind of attack is indicated?
   Answer:

   Port scanning

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.
   Answer:

External host is using HTTP is attempting to deliver a malicious file/software to local host through any port

2. What layer of the Defense in Depth model does this alert violate?
   Answer:

   Stage 3, delivery

3. What kind of attack is indicated?
   Answer:

   Cross Site Scripting, malicious script

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 $EXERNAL_NET any -> $HOME_NET 4444 {msg: “Traffic detected at 4444”}

Part 2: "Drop Zone" Lab

Log into the Azure firewalld machine

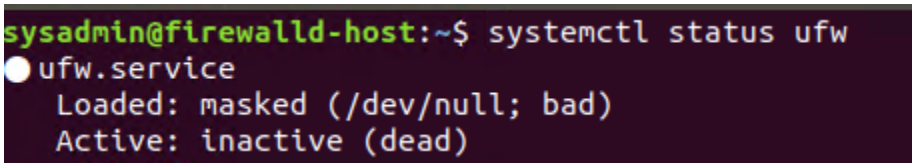
Log in using the following credentials:

- 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 firewalld service. This also ensures that firewalld will be your default firewall.

- Run the command that removes any running instance of ufw.
  $ <sudo apt remove ufw> followed by <systemctl status ufw> to check it is inactive.



Enable and start firewalld

By default, these service should be running. If not, then run the following commands:

Run the commands that enable and start firewalld upon boots and reboots.
$ <service firewalld status>
$ <service firewalld start, 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 firewall-cmd --state>

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

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>
- 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 see if the service you need is available
  $ <sudo firewall-cmd --get-services>
- 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 --list-all-zone>
- 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 creates 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 sets your eth interfaces to your zones.
$ <sudo firewall-cmd --zone=public --change-interface=eth0>
$ <sudo firewall-cmd --zone=Web --change-interface=eth1>
$ <sudo firewall-cmd --zone=Sales --change-interface=eth2>
$ <sudo firewall-cmd --zone=Mail --change-interface=eth3>

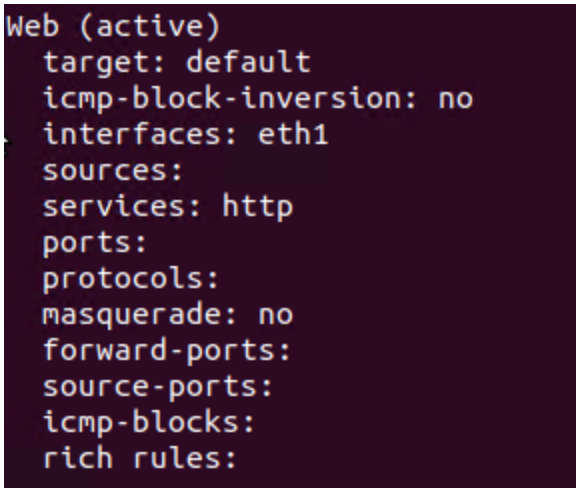
Add services to the active zones:

- Run the commands that add services to the **public** zone, the **web** zone, the **sales** zone, and the **mail** zone.

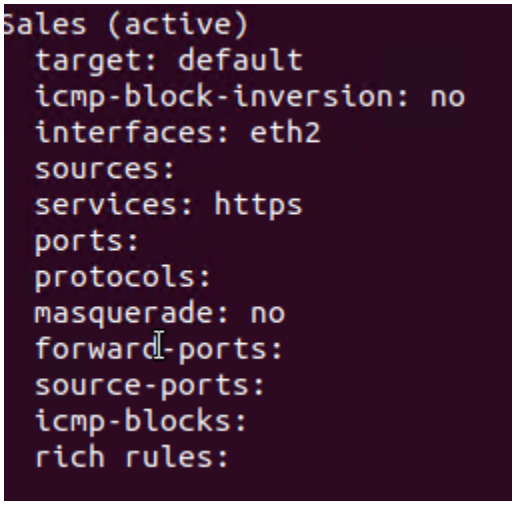
Public:
$ <sudo firewall-cmd --permanent -zone=public --add-service=http>
$ <sudo firewall-cmd --permanent -zone=public --add-service=https>
$ <sudo firewall-cmd --permanent -zone=public --add-service=pop3>
$ <sudo firewall-cmd --permanent -zone=public --add-service=smtp>

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

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=pop3>

$ <sudo firewall-cmd --permanent -zone=Mail --add-service=smtp>

```
Mail (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth3
  sources:
  services: pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

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

By running the command <sudo firewall-cmd --list-service --zone=(zone)>, it shows a list of active services running on firewalld. Evidently the screenshot below indicates which services are active for each zone.

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

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-rich-rule='rule family="ipv4" source address="10.208.56.23" reject' --permanent>
$ <sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" source address="135.95.103.76" reject' --permanent>
$ <sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" source address="76.43.169.118" reject' --permanent>

```
drop
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" source address="76.34.169.118" reject
        rule family="ipv4" source address="135.95.103.76" reject
        rule family="ipv4" source address="10.208.56.23" reject
```

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 ensure 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>

View active Zones

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

- Run the command that displays all zone services.
  $ <sudo firewall-cmd --list-all-zone>

Block an IP address

- Use a rich-rule that blocks the IP address 138.138.0.3.
  $ <sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="138.138.0.3" reject' --permanent>

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        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 --zone=public --add-icmp-block=echo-reply
  --add-icmp-block=echo-request --permanent>

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>

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: 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
```

$ <sudo firewall-cmd --zone=Web --list-all>

```
Web (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1
  sources:
  services: http
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

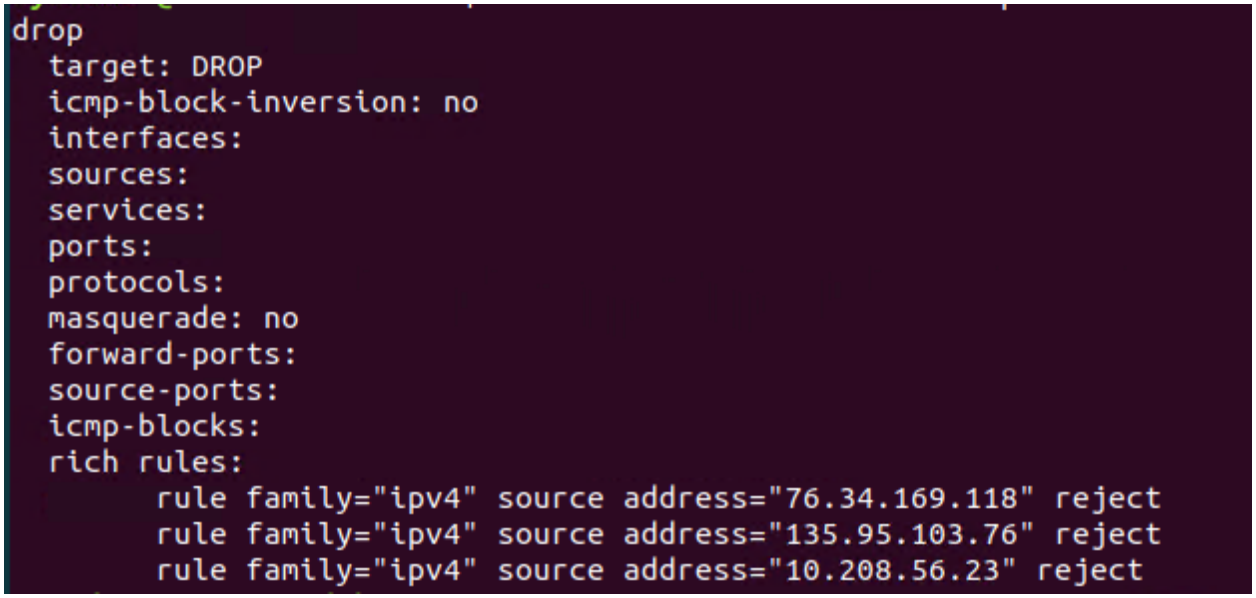
$ <sudo firewall-cmd --zone=Sales --list-all>

```
Sales (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth2
  sources:
  services: https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

$ <sudo firewall-cmd --zone=Mail --list-all>

```
Mail (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth3
  sources:
  services: pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

$ <sudo firewall-cmd --zone=drop --list-all>



Are all of our 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, 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: Connecting to network hub
   Answer 2:Network switch that is configured for port mirroring or network tap
2. Describe how an IPS connects to a network.
   Answer: physically connects inline with flow of data
3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?
   Answer: Signature-based IDS cannot detect zero-day attacks
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 will compare traffic against well-known baseline so those deviate from it will be flagged.

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: Physical
    2. A zero-day goes undetected by antivirus software.
       Answer: Technical
    3. A criminal successfully gains access to HR's database.
       Answer: Administrative
    4. A criminal hacker exploits a vulnerability within an operating system.
       Answer:Technical
    5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.
       Answer: Technical
    6. Data is classified at the wrong classification level.
       Answer: Administrative
    7. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.
       Answer: Administrative
2. Name one method of protecting data-at-rest from being readable on hard drive.
   Answer: Encrypting hard drive
3. Name one method to protect data-in-transit.
   Answer: Symmetric encryption
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.
   Answer: Installation of software called Lojack software, it can provide GPS tracking or monitoring software. IP address could be used for general location.
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?
   Answer: Disk Encryption with strong passwords.

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 gateways

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: Stateful Firewall

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 gateways (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: Stateless Firewall

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

Answer: MAC layer

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 Jr. 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 event message shows that an external host using HTTP has tried to download/install malware onto the local host's network. More specifically the adversary is trying to use a trojan to conduct the attack.

2. What was the adversarial motivation (purpose of attack)?
   Answer: To install malware onto a targeted host motivation can vary depending on goal, but some examples include stealing information or holding for ransom. In this incident it appears that the target is to gain information.
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 they attacker locate the victim?	Company website (airfiber.com.tr) can contain email addresses of employers.
Weaponization	What was it that was downloaded?	Trojan download using JavaScript where malware is downloaded
Delivery	How was it downloaded?	Delivered through HTTP so it can be sent via email.
Exploitation	What does the exploit do?	Remain unsuspected the file that contains the JS which contains the malware can be installed.
Installation	How is the exploit installed?	JS/Nemucod will download additional malware and execute it without consent. This can be done by opening the file as it is EXE file.
Command & Control (C2)	How does the attacker gain control of the remote machine?	After the targeted victim's machine is rebooted, it will enable the malware to send information to an adversary/allow the adversary to gain access remotely to the machine.
Actions on Objectives	What does the software that the attacker sent do to complete it's tasks?	The malware installed can remotely send all information that is

		obtained back to the adversary.

Answer:

4. What are your recommended mitigation strategies?
   Answer: Installation of Antivirus software that will include removal of Trojans. Raise awareness of not downloading from untrusted websites.
5. List your third-party references.
   Answer:

https://www.f-secure.com/v-descs/trojan-downloader_js_nemucod.shtml
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/91000/KB91905/en_US/McAfee_Labs_Threat_Advisory_JS-Nemucod.pdf
https://www.bullguard.com/blog/2014/10/watch-out-an-exe-is-about