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 control
```

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

```
Administrative control
```

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

```
Technical control
```

Intrusion Detection and Attack Indicators

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

```
An IDS actively scans for vulnerabilities and tries to detect intrusions. An IPS is a preventative system that denies incoming packets and stops intrusions.
```

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

```
An indicator of attack indicates an attack happening in real time and require active responses from personnel to identify the intent and end goal of the attack.
An indicator of compromise indicates that malicious activity has previously occurred and require reactive responses from personnel to identify the threat actors techniques and attack vectors allowing them to rebuild and fortify their defenses against future attacks.
```

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 and data on the target
```

2. Stage 2:

```
Weaponization - Preparing a script or file to become a means of attacking the target
```

3. Stage 3:

```
Delivery - Sending or uploading the malicious file or script using whatever methods will help gain access. Ex: malicious emails or USBs in the parking lot.
```

4. Stage 4:

```
Exploitation - executing the malicious script or file on the victim's system
```

5. Stage 5:

```
Installation - the weaponized file or script is installed onto the target
and ready to be deployed
```

6. Stage 6:

```
Command and Control - remote channels for an attacker to manipulate a
victims system are accessed
```

7. Stage 7:

```
Actions on Objectives - the attacker moves toward their end goal or
objective on the victims system
```

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 Sort rule header and explain what this rule does.

```
The header is “alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820” and it is generating TCP alerts for inbound traffic to the home network on ports 5800 to 5820 on the external network.
```

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

```
Reconnaissance
```

3. What kind of attack is indicated?

```
Emerging threats were found, possibly attempting reconnaissance on target
```

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 this rule does.

```
The header is “alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any” and it is warning that TCP packets were sent from the external net through the port 80. The rule is stating that an EXE or DLL was downloaded
```

2. What layer of the defense in depth model does the alerted activity violate?

```
Host since a file was downloaded
```

3. What kind of attack is indicated?

```
Emerging threat for an 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.

```
Alert tcp any any -> any [4444] (msg:”SAMPLE ALERT FOR TCP
TRAFFIC”;sid:1;rev:1;)
```

Part 2: “Drop Zone” Lab

Set up.

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
```

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
```

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
```

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
```

- 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 firewall-cmd --get-services
```

- 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
```

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

Set the zones to their designated interfaces.

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

```
firewall-cmd --permanent --zone=public --change-interface=eth0
firewall-cmd --permanent --zone=web --change-interface=eth1
firewall-cmd --permanent --zone=sales --change-interface=eth2
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 --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
```

- `web`:

```
Sudo firewall-cmd --zone=web --add-service=http
```

- `sales`:

```
Sudo firewall-cmd --zone=sales --add-service=https
```

- `mail`:

```
Sudo firewall-cmd --zone=mail --add-service=smtp
Sudo firewall-cmd --zone=mail --add-service=pop3
```

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

```
After reloading firewalld all of the services are up and running.
```

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
```

Make rules permanent, then reload them.

It's good practice to ensure that your firewalld installation remains nailed up and retains its services across reboots. This helps ensure that the network remains secure after unplanned outages such as power failures.

- Run the command that reloads the firewalld configurations and writes it to memory:

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

View active zones.

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

- Run the command that displays all zone services.

```
Sudo firewall-cmd --get-active-zones
```

Block an IP address.

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

```
sudo firewall-cmd --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 ehco` 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
```

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

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

Congratulations! You have successfully configured and deployed a fully comprehensive firewalld installation.

Part 3: IDS, IPS, DiD and Firewalls

Now, you'll work on another lab. Before you start, complete the following review questions.

IDS vs. IPS Systems

1. Name and define two ways an IDS connects to a network.

```
NIDS: These Network intrusion detection systems connect to a network hub,
network switch, or network tap.
```

```
HIDS: A Host-based intrusion detection system connects to a network via
```

2. Describe how an IPS connects to a network.

```
An IPS is placed inline directly in the flow of network traffic between source and destination, usually right behind the firewall.
```

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

```
A Signature-based Intrusion Detection System
```

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
```

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.

```
Policies and Procedures
```

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

```
Application
```

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

```
data
```

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

```
Application
```

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

```
Host
```

f. Data is classified at the wrong classification level.

```
Policies and procedures
```

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

```
Application
```

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

```
Encryption
```

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

```
Using a VPN
```

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

```
GPS Tracking
```

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

```
Encrypt the password
```

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 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.

```
A 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.

```
An Application-level Gateway
```

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?

```
MAC Layer Firewall
```

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 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?*)

```
The header states that through port 80 a download was initiated on the home network with an attached trojan payload.
```

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

```
To steal private, confidential, or PII data
```

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?	Outbound SSH scan

Weaponization	What was downloaded?	A Trojan
Delivery	How was it downloaded?	Through an email using exe
Exploitation	What does the exploit do?	Steals private information
Installation	How is the exploit installed?	Through the background when the user opens a pdf
Command & Control (C2)	How does the attacker gain control of the remote machine?	Gives the attack access to victims system
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	Steals data, compresses it, then sends it to the attacker.

4. What are your recommended mitigation strategies?

```
Install firewalls and detection systems
```

5. List your third-party references.

```

```