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 Controls
```

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

```
Administrative Controls
```

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

```
Technical Controls
```

Intrusion Detection and Attack Indicators

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

```
IDS are tools that can analyze traffic and look for malicious signatures. IPS can do everything an IDS can do, but it can also respond to attacks by blocking malicious traffic, preventing it from being delivered to a host network.
```

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

```
An IOA indicates attacks happening in real time while an IOC indicated previous malicious activity.
```

The Cyber Kill Chain

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

1. Stage 1:

```
Reconnaissance: Information gathering stage.
```

2. Stage 2:

```
Weaponization: Establish attack vectors and technical profiles of targets.
```

3. Stage 3:

```
Delivery: Delivery of the weaponized payload.
```

4. Stage 4:

```
Exploitation: Actively compromise adversary's applications and servers.
```

5. Stage 5:

```
Installation: Persistence preparation phase.
```

6. Stage 6:

```
Command and Control: Remote control of a victim’s computer.
```

7. Stage 7:

```
Actions on Objectives: After gaining full control of target computer,
adversaries can now act on their objectives.
```

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.

```
Send alert when an external tcp packet from any port from $EXTERNAL_NET
attempts to access $HOME_NET on ports 5800:5820
```

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

```
Reconnaissance
```

3. What kind of attack is indicated?

```
Scanning for open VNC port
```

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.

```
Send alert when an external tcp packet from $EXTERNAL_NET on $HTTP_PORTS
attempts to access $HOME_NET on any port
```

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

```
Administrative
```

3. What kind of attack is indicated?

```
Malware attack
```

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 4444 -> $LOCAL_NETWORK any {msg: “TCP packet detected”;}
```

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:

```
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 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 --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 --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`?

```
Active 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-zone
```

Block an IP address.

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

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

```
SPAN or Mirrored Port: enterprise-level switch that allows you to mirror one or more physical switch ports to another port
```

```
Network TAP: a cable connects the TAP monitor port with the NIC on the sensor
```

2. Describe how an IPS connects to a network.

```
Inline with the flow of data.
```

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

```
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?

```
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.

```
Physical
```

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

```
Application
```

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

```
Data Link
```

    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.

```
Network
```

    f. Data is classified at the wrong classification level.

```
Policy Procedure Awareness
```

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

```
Perimeter
```

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

```
Hard drive Encryption
```

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

```
VPN
```

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

```
GPS enabled device
```

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

```
Disable boot from external and implement a BIOS password to keep them from
re-enabling
```

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 Firewalls
```

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.

```
Packet-Filtering Firewalls (Stateful)
```

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.

```
Application (Proxy) Firewalls
```

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 Firewalls (Stateless)
```

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

```
MAC layer Firewalls
```

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?*)

```
An alert was triggered indicating a download of a trojan attack through port 80
```

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

```
Gain access to the target's computer through an inconspicuous trojan attack.
```

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?	Random
Weaponization	What was downloaded?	A trojan exe payload
Delivery	How was it downloaded?	Downloading pirated media Clicking unknown links Clicking on pop-up Failing to read the user agreement Not updating
Exploitation	What does the exploit do?	Disguises malware to gain access to the victim's computer
Installation	How is the exploit installed?	User download

Command & Control (C2)	How does the attacker gain control of the remote machine?	When executed, the trojan may set up a backdoor to allow the attacker access to the target machine.
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	When executed, run scripts.

4. What are your recommended mitigation strategies?

```
Do not click on unknown links
Use strong passwords.
Only use encrypted https.
Log in to websites through official log in page, not link.
Use a strong password manager.
Use a spam filter.
Enable two-way authentication.
Always update everything
Back up files regularly in case of an attack.
```

5. List your third-party references.

```
https://www.crowdstrike.com/cybersecurity-101/malware/trojans/#:~:text=A%20Trojan%20Horse%20(Trojan)%20is,the%20contents%20of%20the%20device.
```