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?

```
Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS)
serve distinct roles. While IDS operates as a passive, stateless network
monitor, simply observing and logging potential threats without modifying
packets or frames, IPS takes on a more proactive stance in network
monitoring. Functioning as a stateful control system, IPS not only logs and
notifies but also has the capability to actively block suspicious traffic
and trigger additional security measures.
```

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

```
Real-time indicators known as "Indicators of Attack" (IOA) and signs of
potential breaches known as "Indicators of Compromise" (IOC). IOCs gather
solid proof that a system has been infiltrated. IOAs hone in on attempted
attacks or reconnaissance activities, trying to figure out what the bad
actors are up to. Cutting-edge security tools often prioritize keeping an
eye on these indicators of attack to stay one step ahead of potential
threats.
```

The Cyber Kill Chain

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

1. Stage 1:

```
Reconnaissance: A hacker gathers information about their target(s), like
their employee name, email address, and network structure; using public
resources, social media, physically gathering the information, or other
means.
```

2. Stage 2:

```
Weaponization: An attacker creates a malicious payload, such as a
malware-infected document, to use in the next stage of the attack.
```

3. Stage 3:

```
Delivery: The attacker attempts different delivery methods, such as a phishing email, to send the malicious document to an employee within the target organization.
```

4. Stage 4:

```
Exploitation: The target opens the infected document, triggering an exploit that takes advantage of a vulnerability to execute the malware.
```

5. Stage 5:

```
Installation: The malware is installed on the system, leaving it compromised, providing the attacker with an established foothold and a way to return later.
```

6. Stage 6:

```
Command and Control (C2): The compromised system establishes a connection to a remote server controlled by the attacker. This allows the attacker to send commands and receive information.
```

7. Stage 7:

```
Actions on Objective/ Exfiltration: The attacker has achieved their goals, which could involve exfiltration of sensitive information, disrupting operations (DDoS), or maintaining a “back-door” for them to have access again in the future.
```

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.

Snort flagged a significant event: a remote host probed $HOME_NET on ports 5800-5820 via TCP/IP, hinting at port mapping and possible reconnaissance with tools like nmap or metasploit. The broad port usage suggests an exploratory approach, focusing on VNC-related services. TCP/IP inclusion underscores the detection's TCP specificity. Such scans, concentrated on a port range, suggest reconnaissance. The rule's threshold mechanism minimizes false alerts, activating only if a single source IP exceeds defined counts within a timeframe. Crafting rules tailored for such scans empowers administrators to preemptively counter potential threats, bolstering overall system resilience against malicious activities.

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

```
1, Reconnaissance
```

3. What kind of attack is indicated?

```
Port Mapping is indicated.
```

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.

```
This Snort rule signals potential policy breaches, detecting the HTTP
download of Windows PE files (EXE or DLL). It observes TCP traffic from
external to internal networks, concentrating on established connections to
the client. The rule pinpoints potentially harmful downloads. The rule aids
in monitoring and responding to unauthorized Windows file downloads.
```

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

```
3, Delivery
```

3. What kind of attack is indicated?

```
I believe cross-site scripting is indicated, a person could be on a site
inputting information and they click something that could start the
download. The rule is focused on recognizing potential malicious downloads
of Windows executable files over HTTP.
```

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 -> $HOME_NET 4444 (msg:"Inbound traffic on port 4444
detected"; sid:1000001;)
```

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 -y remove ufwD
```

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 (or ufw instead of firewalld)
sudo systemctl start firewalld (or ufw instead of 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 systemctl status firewalld
```

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 --zone=home. I added the --zone=home because it was giving me an error without it.
```

- 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
```

- 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=eth0
sudo firewall-cmd -zone=mail -change-interface=eth0
sudo firewall-cmd -zone=sales -change-interface=eth0
```

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=public --add-service=http
```

- `sales`:

```
sudo firewall-cmd --zone=public --add-service=https
```

- `mail`:

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

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

```
I used this command to obtain the status. nc -zv localhost port#

HTTP (PORT 80) OPEN
HTTPS (PORT 443) CLOSED
SMTP (PORT 25) OPEN
POP3 (PORT 110) OPEN
```

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 -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 --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.

```
Network Intrusion Detection Systems: monitors network traffic, uses
signature-based detection, anomaly-based detection, packet inspection,
generates alerts, does logging and reporting, passive monitoring, integrates
with other security measures, and stays up-to-date with the latest known
threats and attack patterns.
```

```
Host-based Intrusion Detection System: Focus on individual hosts such as
servers, workstations, or other endpoints. It uses system-centric monitoring
all events and activities that occur on the host itself, signature-based
detection, anomaly based detections, log analysis, File Integrity Monitoring
checking changes made to certain system/configuration files, generates
alerts, allows for response action in being able to identify and isolate the
threat or block certain activities for example. It also monitors utilization
such as cpu usage, memory, network activity, etc. It adds to the endpoint
protection by working with other parameters that are in place.
```

2. Describe how an IPS connects to a network.

```
Intrusion Prevention System is typically positioned immediately behind the
firewall, actively monitoring network traffic to detect and respond to any
```

```
suspicious activities.connects to a network by being strategically placed within the network architecture, either inline or in passive mode, and configured to monitor, analyze, and prevent malicious activities. It utilizes Physical or virtual deployment, configuration and integration of software, Network interface configuration, routing and switching configuration, load balancing, monitoring and maintenance, logging and reporting.
```

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

```
A stateless IDS is limited in its ability to identify zero-day exploits because it relies on predefined hot and cold lists to analyze traffic. It lacks the capability to recognize anything beyond the parameters set by these lists, making it less effective in detecting emerging threats and unknown vulnerabilities.
```

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?

```
Stateful IDS proves valuable in identifying new exploits, despite typically having a larger footprint compared to stateless counterparts. Its improved capabilities provide a set of tools for analyzing system traffic with increased effectiveness.
```

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 Security
```

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

```
Endpoint Security
```

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

```
Identity and Access Management
```

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

```
Endpoint Security.
And possibly Application Security and possibly Network Security.
```

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.

```
Data Classification and Handling
```

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

```
Network Security
```

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

```
Drive Encryption
```

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

```
Data Encryption
```

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

```
Endpoint security technologies,(Trackers) tracking and remote management features, such as GPS, Wi-Fi or IP geolocation.
```

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

```
Use Full Disk Encryption, Secure Boot, or set up a BIOS/UEFI 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.

```
Stateless Network 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.

```
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?*)

```

```

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]
```