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
```

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

```
Administrative
```

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

```
Technical
```

Intrusion Detection and Attack Indicators

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

```
An IDS and IPS can both detect and alert to a potential attack, but only IPS can respond. IDS only logs the incident.
```

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

```
IOA indicates an attack is happening in real time, whereas an IOC indicates that malicious activity has already occurred.
```

The Cyber Kill Chain

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

1. Stage 1:

```
Reconnaissance: In this phase, the attacker develops as much information about their target in order to plan the attack. This can be login credentials, potential weaknesses to exploit, user ID's and OS details, to name a few.
```

2. Stage 2:

```
Weaponization: An attack vector is created to exploit the known vulnerability established in stage 1. This is when the malware, worm or virus is created as well as potential backdoors in order to regain access to the target.
```

3. Stage 3:

```
Delivery: In this phase, the attack itself is launched. Depending on the type of attack, the steps will vary. For example, this is when the attacker would send out their malicious phishing emails.
```

4. Stage 4:

```
Exploitation: The malicious code has successfully been executed in the
target system.
```

5. Stage 5:

```
Installation: The malware is successfully installed on the victim machine
and the attacker can now take control of their target.
```

6. Stage 6:

```
Command and Control: Remote control is taken of the target device and from
here the attacker can begin to move laterally throughout the target system.
From here they can expand their access to the system and create more
backdoors for future entry.
```

7. Stage 7:

```
Actions on Objective: The attacker executes their intended mission. This can
include encryption, data exfiltration and theft and destruction.
```

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.

alert: this is the action snort will take when triggered.
tcp: the rule is applied to all TCP packets.
$EXTERNAL_NET any -> $HOME_NET 5800:5820: When a TCP packet is sent from an external network on any port to the home network on ports 5800-5820 the rule will be triggered.

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

This violates Stage 1, Reconnaissance because the attacker is performing a scan.

3. What kind of attack is indicated?

The attacker may be attempting a VNC scan to check for an open VNC server. VNC allows remote desktop control.

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.

alert: This is the action snort will take when triggered.
tcp: the rule is applied to incoming TCP packets.
$EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any: When a TCP packet is sent from an external network on an HTTP port to the home network on any port, the rule will be triggered.

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

```
Stage 3: Delivery because an EXE or DLL file has been attempted to be
downloaded.
```

3. What kind of attack is indicated?

```
A potential malware attack disguised as a windows update if the file
downloaded over HTTP contains malicious code.
```

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 $EXTERNAL_NET 4444 -> $HOME_NET any (msg: inbound tcp from port
4444)
```

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 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.

```
$ systemctl enable firewalld
$ 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.

```
$ 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-zones
```

- 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 --get-active-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 --permanent
$ sudo firewall-cmd --zone=public --add-service=https --permanent
$ sudo firewall-cmd --zone=public --add-service=pop3 --permanent
$ sudo firewall-cmd --zone=public --add-service=smtp --permanent
```

- `web`:

```
$ sudo firewall-cmd --zone=web --add-service=http --permanent
```

- `sales`:

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

- `mail`:

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

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

```
http is enabled in the public and web zones, https is enabled in the public
and sales zones, smtp is enabled in the public and mail zones and pop3 is
enabled in the public and mail zones.
```

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 (the rules were added as permanent during
configuration so reloading firewalld will make them active and permanent.)
```

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 --permanent --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
--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 Tap (Test Access Port): This is a piece of hardware that provides
access to a network and monitors both inbound and outbound traffic
simultaneously and sends the data to a monitoring device in real time.
```

```
SPAN (Switch Port Analyser): A mirror image of all network data is sent to
another physical port for packet analysis.
```

2. Describe how an IPS connects to a network.

```
An IPS usually connects inline with the data flow. Most often it is located
between a firewall and a switch.
```

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

```
This is known as a “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?

```
This is known as an “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 layer
```

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

```
Endpoint layer
```

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

```
Data layer
```

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

```
Application layer
```

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

```
Data layer
```

f. Data is classified at the wrong classification level.

```
Identity and Access Management layer
```

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

```
Network layer
```

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

```
Password protection
```

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

```
encryption
```

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

```
GPS
```

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

```
Configure the laptop to shutdown or hibernate when not in use and require
software like Bitlocker to prompt you for a PIN upon powering up/restoring
the laptop or 2FA.
```

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 gateway 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.

```
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?

```
Stateless firewall
```

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

```
MAC layer filtering 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?*)

```
In this instance a snort rule was triggered: an external network using the
http protocol port connected to the home network via any port. Furthermore,
a malicious payload matching the signature of a known Trojan virus was
detected. Upon further investigation we were able to uncover that this
payload is related to an Italian spam campaign.
```

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

```
The motivation here is to infect target machines for the purpose of stealing
info and installing ransomware.
```

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?	Victims are found through phishing.
Weaponization	What was downloaded?	A malicious .exe file is hidden in a phishing email attachment posing as a pdf document.
Delivery	How was it downloaded?	The victim clicks the decoy pdf attachment to download.
Exploitation	What does the exploit do?	Attempts to steal passwords and PII, installs ransomware and records info about you and your PC.
Installation	How is the exploit installed?	When the victim clicks the decoy email attachment, the malware/ransonware is installed.

Command & Control (C2)	How does the attacker gain control of the remote machine?	The malicious payload connects to a remote host allowing the attacker control over the system.
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	This malware can encrypt your data, steal your password info and monitor your activities on your PC.

4. What are your recommended mitigation strategies?

```
Education on the dangers of phishing, anti-malmare software, up to date
security patches for OS’s.
```

5. List your third-party references.

```
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-descriptio
n?Name=JS/Nemucod
```