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 stands for Intrusion Detection Systems, which are passive devices that perform packet captures of all traffic that passes through a network interface. In other words, they are tools that are used to both analyze traffic and to look for malicious signatures. While being similar to firewalls, IDS do have additional capabilities that allow them to read the data in packets that it inspects, issue alerts and alarms, and, if configured to do so, to block malicious traffic. Snort is an example of an Intrusion Detection System (the world's most popular open-source solution, apparently).
IDS are not designed to respond to attacks, rather they are used to document and log attacks for future analysis. They are able to help organizations enforce the cyber kill chain by establishing situational awareness of adversaries, which can help the organizations harden their defenses.

IPS stands for Intrusion Prevention System. This can do everything that the IDS can do, with the added feature of being able to respond to attacks. They are able to react to packets by automatically logging and blocking any malicious traffic/threats without any administrative intervention (something that the IDS requires). In other words, IPS can detect and mitigate threats in real time. Moreover, while an IDS connects via a network TAP or mirrored SPAN port, an IPS connects inline with the flow of data (usually between the firewall and the network switch). As a result, more traffic flows through it, and this requires more robust hardware.

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

An indicator of attack (IOA) is an alert that is generated by the IDS when a Snort rule detects malicious traffic that matches a signature. This type of indicator shows an attack that is happening in real time. While the attack is currently in progress, a full breach has not been determined or has not occurred yet. The focus here is to reveal the intent and the end goal of the attacker, regardless of the exploit or malware that is used in the attack.

On the other hand, an indicator of compromise (IOC) specifies previous malicious activity. It is a reactive approach to successful intrusions, which indicates that an attack resulting in a breach has occurred. It is used to help determine an adversary's techniques, tactics, and procedures

```
(TTPs). Finally, it exposes all of the vulnerabilities that were used in an attack, with the goal of giving network defenders the opportunity to revamp their defense as part of their mitigation strategy and to learn from an attack so it does not happen again.
```

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 against the targeted victim. DNS registration websites, Facebook, LinkedIn, X, etc are information sources. VNC scans are used in the reconnaissance stage.
```

2. Stage 2:

```
Weaponization - Adversaries establish attack vectors and technical profiles of targets, for example logical and administrative security controls, infil/exfil points, etc.
```

3. Stage 3:

```
Delivery - Delivery of “weaponized payload” via email, USB, website, etc.
```

4. Stage 4:

```
Exploitation - where preparations for escalation during the next phase, installation, are done. This is accomplished by actively compromising the adversary’s applications and servers while averting logical, physical, and administrative controls. Also, exploiting employees through social engineering.
```

5. Stage 5:

```
Installation - otherwise known as the “persistence preparation phase”, includes activities such as malicious software installation, backdoor implants, and persistence mechanisms such as Cron Jobs, AutoRun keys, log file deletion, services, and timestamp manipulation.
```

6. Stage 6:

```
Command & Control (C2) - a command channel that is used for remote control of a victim’s computer, typically Internet Relay Chat (IRC).
```

7. Stage 7:

```
Actions on Objections - once the equivalent of “Hands on Keyboard access to a victim’s systems has been achieved, adversaries are able to act on their objectives. This could be copying data/files, and sending it back to the attacker.
```

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.

```
The Snort rule creates an alert for TCP traffic from any IP address outside the organization’s networks and any port, going to any destination IP address among the trusted internal networks and destination ports in the range of 5800-5820.
Snort then generates an alert and logs a message.
```

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

```
It appears to be a part of the reconnaissance stage of the cyber kill chain.
```

3. What kind of attack is indicated?

```
A potential VNC scan, which would be a reconnaissance tool.
```

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.

```
The rule creates an alert for TCP traffic from any IP address outside the
organization’s networks through source HTTP port (port 80) to any IP address
and ports among the trusted internal networks.
The message shows that a Windows executable file has been downloaded over
HTTP.
```

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

```
Delivery
```

3. What kind of attack is indicated?

```
It could be a virus that is disguised as a windows update.
```

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: “TCP packet detected through 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 -y 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 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
```

- 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 --new-zone=web --permanent
$ sudo firewall-cmd --new-zone=sales --permanent
$ sudo firewall-cmd --new-zone=mail --permanent
```

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 --permanent
$ sudo firewall-cmd --zone=web --change-interface=eth1 --permanent
$ sudo firewall-cmd --zone=sales --change-interface=eth2 --permanent
$ sudo firewall-cmd --zone=mail --change-interface=eth3 --permanent
```

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`?

```
active
```

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-source=10.208.56.23
$ sudo firewall-cmd --zone=drop --add-source=135.95.103.76
$ sudo firewall-cmd --zone=drop --add-source=76.34.169.118
$ sudo firewall-cmd --zone=drop --add-rich-rule=”rule family=ipv4 source
address=’10.10.10.10’ 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 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 --runtime-to-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-services
```

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-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=drop --list-all
$ sudo firewall-cmd --zone=mail --list-all
$ sudo firewall-cmd --zone=public --list-all
$ sudo firewall-cmd --zone=sales --list-all
$ sudo firewall-cmd --zone=web --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) - a hardware device that provides access to a
network. TAPs transit both inbound and outbound data streams on separate
channels, at the same time. This allows all data to arrive at the monitoring
device in real time.
```

```
SPAN (Switched Port Analyzer) - sends a mirror image of all network data to
another physical port, where the packets can be captured and analyzed. This
is also known as port mirroring.
```

2. Describe how an IPS connects to a network.

```
Connects inline with the flow of data. The IPS is usually placed in between the firewall and network switch. Due to the amount of traffic flowing through it, an IPS requires more robust hardware.
```

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.

```
Perimeter
```

    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.

```
Host
```

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?

```
Using a firmware 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.

```
Circuit-level gateway
```

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/Packet-Filtering 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?*)

```
There is a red alert in the Sguil analyst console, leading to the discovery of a “Get /40.exe HTTP/1.1” request with a server response of “Http/1.1 200 OK” for an unauthorized file download.
```

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

```
The purpose of the attack was the theft of private sensitive data. Typical targets of this adversary are financial institutions.
```

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?	Email addresses, possibly exposed through vendor/customer mailing lists.
Weaponization	What was downloaded?	JavaScript downloaded called JS/Nemucod, which is attached to emails as a ZIP file
Delivery	How was it downloaded?	An unsolicited SPAM email
Exploitation	What does the exploit do?	Nemucod uses three different Activex controls: - WScript.Shell - MSXML2.XMLHTTP - ADODB.Stream An executable file is saved to the temporary folder %TEMP%. Nemucod will then open a legitimate PDF file in the browser, which is used as a decoy to let the user think that they are viewing the real invoice.
Installation	How is the exploit installed?	JavaScript file then downloads a simple EXE file which is installed in the background through the WScript.Shell ActiveX control. The malware then opens the decoy PDF document through the ADODB.
Command & Control (C2)	How does the attacker gain control of the remote machine?	Installed malware communicates with the Attacker's network, allowing them access to the system.
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	EXE files downloaded by Nemucod are used to retrieve a Trojan downloader called Fareit or Pony Downloader. They then download another

		set of executable files that contain the Gozi infostealer malware. The files are compressed, then sent to the attacker.

4. What are your recommended mitigation strategies?

```
Use an IDS to detect any anomalies that come into and out of the network. On top of that, use an IPS to detect and mitigate threats in real time.
```

5. List your third-party references.

```
https://www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/
```