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?

```
These are physical security controls.
```

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

```
These are administrative security controls.
```

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

```
All examples of technical security controls.
```

Intrusion Detection and Attack Indicators

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

```
An IDS is designed to only provide an alert about a potential incident which can be investigated so it can be determined if it needs further action. An IPS takes action to block the attempted intrusion or otherwise remediate the incident..
```

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

```
An IOA focuses on detecting the intent of what an attacker is trying to accomplish. An IOC is described as evidence that the security of a network has been breached and that the attack was successful.
```

The Cyber Kill Chain

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

1. Stage 1:

```
Reconnaissance: this is the planning phase for the adversary. They will discover and collect information.
```

2. Stage 2:

```
Weaponization: The attacker would use the information gathered about the target and then decide what is the best tool to use to break into a target's defense. This could mean buying malware, using an exploit to deliver a payload to the target.
```

3. Stage 3:

```
Delivery:  Choosing a method to distribute the malicious content to a targets computer or server.
```

4. Stage 4:

```
Exploitation: During this phase once a person is successfully targeted and the adversary gets into the computer they may find ways to exploit the network. They could use lateral movement to move deeper into the network.
```

5. Stage 5:

```
Installation: The attacker would install malicious scripts, a back door, or modify services so that they can have persistent access to the target computer.
```

6. Stage 6:

```
Command and Control: The adversary server would be able to communicate with the infected host and this would turn the infected host into a beacon. Two common channels of communication are through the HTTP protocols and DNS.
```

7. Stage 7:

```
Exfiltration: Once the data is collected the attacker can then steal, hold ransom, delete copies and collect credentials. This is also known as the actions and objectives of 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 Sort rule header and explain what this rule does.

```
This is a TCP alert that monitors any TCP packets that come with any IP
through ports 5800:5820 on the home network.
```

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

```
This would be reconnaissance.
```

3. What kind of attack is indicated?

```
The alert message states that it is a VNC scan.
```

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.

```
This alert states that any TCP packers coming from any external IP and HTTP
ports that are listed should be monitored if sent to any port on the home
network.
```

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

Delivery on the Kill Chain.

3. What kind of attack is indicated?

```
This could be a malware or ransomware 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 $EXTERNAL_NET 4444 -> $HOME_NET any (msg: “potential buffer overflow attack”)
```

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-get 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 start firewalld

Sudo systemctl enable 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.

```
Service firewalld status
```

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

Set the zones to their designated interfaces.

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

```
Sudo firewall-cmd --zone=public --add-interface=eth0
sudo firewall-cmd --zone=Web --add-interface=eth1
 sudo firewall-cmd --zone=Sales --add-interface=eth2
sudo firewall-cmd --zone=Mail --add-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`:

```
Firewall-cmd --zone=public--add-service=smtp
Firewall-cmd --zone=public--add-service=http
Firewall-cmd --zone=public--add-service=https
Firewall-cmd --zone=public--add-service=pop3
```

- `web`:

```
Firewall-cmd --zone=web --add-service=http
```

- `sales`:

```
Firewall-cmd --zone=sales --add-service=https
```

- `mail`:

```
Firewall-cmd --zone=mail --add-service=smtp
Firewall-cmd --zone=mail --add-service=pop3
```

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

```
They are enable for specific zones web=http mail=smtp,pop3,
public=smtp,pop3,https,https, and sales-https.
```

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.

```
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
```

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.

```
$firewall-cmd --zone=public --remove-icmp-block-inversion --permanent
```

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.

```
$ firewall-cmd --list-all --zone=public
$ firewall-cmd --list-all --zone=web
$ firewall-cmd --list-all --zone=sales
$ firewall-cmd --list-all --zone=mail
```

- 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.

```
Signature-based detection use patterns by establishing a unique identifier for the detection of future cyber attacks, using the IDS sensors and consoles.
```

```
Statistical anomaly-based detection as an expert system, relies on the identification of anomalies in the network traffic comparing against established baselines.
```

2. Describe how an IPS connects to a network.

The IPS is placed inline, directly in the flow of network traffic between the source and destination.

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

Signature-based Intrusion Detection Systems

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?

```
statistical anomaly-based detection
```

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.

```
Reconnaissance
```

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

```
exploitation
```

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

```
installation
```

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

```
exploitation
```

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

```
Exfiltration
```

f. Data is classified at the wrong classification level.

```
Command and contorl
```

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

```
Exfiltration
```

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

```
Encryption and encrypt your back up data. Also if a hardrive is being
retired make the hard-drive unreadable. Bitlocker and an encryption based on
a block cipher.
```

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

```
Choose data protection solutions with policies that enable user prompting, blocking, or
automatic encryption for sensitive data in transit, such as when files are attached to
```

an email message or moved to cloud storage, removable drives, or transferred elsewhere.

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

A laptop-specific program, this works closely with law enforcement to recover a stolen laptop. LoJack for Laptops is available for Mac OS X and Windows as far back as 2000. The Computrace Agent, part of the LoJack software, works in the background and resists detection. LoJack for Laptops even survives wiped hard drives. Upon reporting a stolen laptop, the Absolute Theft Recovery Team does all of the work to recover the device

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

```
We would need to enter the BIOS and  go into the CD/DVD ROM Drive BBS Priorities and Network Device BBS Priorities and disable the options in there. Once you do that, they won't even show up as options anymore
```

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.

```
Statefull 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
```

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 event message is alerting a trojan attack and suspected payload.
```

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

```
The attack is trying to get access to a computers network and install
malware.
```

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]
```