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?

IDS is passive and focuses on detecting and alerting, while an IPS is proactive and can block threats as they are detected in real-time.

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

IOA looks for the signs of the attack in progress, and it focuses on the detection and stopping of threats early. IOC looks for the evidence after the attack has happened, assisting in the confirmation that a system has already been compromised.

The Cyber Kill Chain

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

1. Stage 1:

Reconnaissance

2. Stage 2:

Weaponization

3. Stage 3:

Delivery

4. Stage 4:

Exploitation

5. Stage 5:

```
Installation
```

6. Stage 6:

```
Command and Control
```

7. Stage 7:

```
Actions on 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 Snort rule header and explain what this rule does.

```
Action: alert - Tells Snort to generate an alert when the rule matches.

Protocol: tcp - The rule is applying to TCP Traffic

Source IP/Port: $EXTERNAL_NET any - this shows the IP address outside the
internal network, any applies to any of the source ports.

Direction: -> - Indicating the traffic flow, in this example the flow of
traffic is from external to internal.
```

```
Destination IP/ Port: $HOME_NET 5800:5820 - $HOME_NET represents the
destination on the internal network, 5800:5820 distinguishes the exact port
range on where this rule applies.

Rule Options: msg:"ET SCAN Potential VNC Scan 5800-5820"; - This is the
message to be logged / alerted that describes the rule.

flags:S,12; - Shows the specific TCP SYN Flag set and the TCP Header is 12
bytes.

threshold: type both, track by_src, count 5, seconds 60; - This sets a
threshold to trigger an alert if there are 5 matching packets detected
within 60 seconds from the same source.

reference:url,doc.emergingthreats.net/2002910; - This gives us a reference
URL to research more about the specific rule.

classtype:attempted-recon; - Categorizing of the alert that shows the
attempted reconnaissance activity.

sid:2002910; - The unique Snort ID for the rule.

rev:5; - The revision number of the rule above.

metadata:created_at 2010_07_30, updated_at 2010_07_30; - The metadata
indicates the date that the rule was created and also updated.
```

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

```
Reconnaissance, gathering information of the target network like scanning
ports that are open.
```

3. What kind of attack is indicated?

```
Those specific ports show that this is a potential VNC (Virtual Networking
Computing) scan. The rule is designed to alert and detect scans that target
these ports, they are scanned to discover if VNC services are running on an
internal network. This gives them avenues for further exploitation
```

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.

```
Action: Alert - Alert is triggers when the rule matches.

Protocol: tcp - Applies to TCP traffic

Source IP/ Port:   $EXTERNAL_NET - is for any external IP address.
$HTTP_PORTS - is a variable for HTTP ports (typically 80, 443, and more).

Direction: -> -Traffic direction from external to internal networks.

Destination IP/ Port: $HOME_NET any - $HOME_NET - represents the internal
network,  any  - says it is applicable to any destination port.

Rule Options: msg:"ET POLICY PE EXE or DLL Windows file download HTTP"; -
Description of the rule.

flow:established,to_client; - Applied to an established connection with data
flowing to the client.

flowbits:isnotset,ET.http.binary; - Checks if the flowbit. ET.http.binary -
is not set.

flowbits:isnotset,ET.INFO.WindowsUpdate; - Checks to see the flowbit.
ET.INFO.WindowsUpdate - is not set.

file_data;: File data analyzed that is within the HTTP payload.

content:"MZ"; within:2; - Searches for the "MZ" signature (indicating the
start of a Windows executable file) within the first 2 bytes of the file
data.
```

```
byte_jump:4,58,relative,little; -  Skipping 4 bytes then extracts the 58
bytes in a little-endian format.

content:"PE|00 00|"; distance:-64; within:4; - Searching for the "PE"
signature (indicating a Portable Executable file format) within 4 bytes
after a 64-byte offset from the previous match.

flowbits:set,ET.http.binary; - Sets the flowbit ET.http.binary if the
content matches.

metadata: former_category POLICY; - Indicating that the rule was changed
prior that was categorized under POLICY.

reference:url,doc.emergingthreats.net/bin/view/Main/2018959; - Shows the
linked URL for more information.

classtype:policy-violation; - Categorizes the alert as a policy violation.

sid:2018959; - The Snort ID that is unique for this rule.

rev:4;: Revision number of the rule.

metadata:created_at 2014_08_19, updated_at 2017_02_01; - Metadata indicating
creation and last update dates.
```

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

```
Delivery. Involving delivering malicious payload to the target, with this
example it would potentially be a .exe (Windows executable) or DLL file that
is being downloaded via HTTP.
```

3. What kind of attack is indicated?

```
Potentially a Policy Violation. The HTTP request is downloading a file where
the signature matches that of a .exe or DLL. Generally this is used to
detect suspicious or unauthorized file downloads that may be malicious.
Examples of malicious downloads include Trojans, malware and even backdoor
programs to remotely access the system.
```

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 any -> $HOME_NET 4444 (msg:"Inbound traffic on port
4444 detected"; sid:1000001; rev:1;)


Action: Alert - Alert generated when the rule gets triggered.

Protocol: TCP - Applies to TCP traffic.

Source IP/Port: $EXTERNAL_NET any- $EXTERNAL_NET - represents any IP address
that is external. Any -  represents this is applicable to any source port.

Direction: -> - Indicating traffic direction from external to internal.

Destination IP/Port: $HOME_NET 4444- $HOME_NET - represents the local
network, while 4444 dictates the specific traffic inbound to the port 4444.

Rule Options: msg:"Inbound traffic on port 4444 detected"; - Provides a
message describing the rule.

sid:1000001; - Unique Snort ID for the rule.

Rev:1; - Revision number of the rule above.



**This rule generates an alert when there is inbound traffic that is
detected on the port 4444 targeting any of the hosts on the internal
network.
```

Part 2: “Drop Zone” Lab

Set up.

Log into the web lab.

- Username: `sysadmin`
- Password: `cybersecurity`

Important: If your class started **BEFORE April 8, 2024,** You will need to do the following to start up the containers:

Open a terminal window and run the following command to start up the docker containers (Note: this should be one continuous line).

```
$  wget
https://gist.githubusercontent.com/jlow3939/904eb58af3605457255df35c649f9873
/raw/69bc0efdb38837ecce8db14662e9efffbfe15429/docker-compose.yml &&
docker-compose up -d
```

All classes that start **AFTER April 8, 2024**, will not need to do the previously indicated step. They will navigate to `cd ~/Cybersecurity-Lesson-Plans/11-NetSec` and type `docker-compose up.`

Run the following command to verify that the `firewalld` container is running:

```
$ docker ps
```

Start a session with the `firewalld` container using the following command:

```
$ docker exec -it firewalld bash
```

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 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 firewalld --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 firewalld --get-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 --permanent --zone=public --change-interface=eth0
sudo firewall-cmd --permanent --zone=web --change-interface=eth1
sudo firewall-cmd --permanent --zone=sales --change-interface=eth2
sudo firewall-cmd --permanent --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 --permanent --zone=public --add-service=http
sudo firewall-cmd --permanent --zone=public --add-service=https
sudo firewall-cmd --permanent --zone=public --add-service=pop3
sudo firewall-cmd --permanent --zone=public --add-service=smtp
```

- `web`:

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

- `sales`:

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

- `mail`:

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

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

```
HTTP/ HTTPS are public and web zones
SMTP/ POP3 are 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 -zone=drop —add-source=192.168.1.101
Sudo firewall-cmd -zone=drop —add-source=10.0.0.40
Sudo firewall-cmd -zone=drop —add-source=203.0.113.77
Sudo firewall-cmd -zone=drop —add-source=192.168.1.206
```

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-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” drop’
```

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

- 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.

Inline (In-band)- IDS positioned between the network traffic path, acting like a gatekeeper for the network segments. Monitoring and processing data packets as it flows through. This way the IDS can detect and prevent the threats.

Passive (Out-of-band) - IDS is set up to monitor traffic indirectly by receiving copies of the data packets through port mirroring or network taps. This analyzes the traffic without being in the direct path of the data flow, and does not interfere with the flow of network traffic.

2. Describe how an IPS connects to a network.

Inline (In-band Connection):
Inline Deployment- An IPS is directly placed in the data path between network segments. This means all network traffic must pass through the IPS before reaching its destination.
Traffic Inspection and Response- When the IPS is inline, it is able to inspect each packet for malicious activity or policy violations. If it detects a threat or attack, the IPS can block/ drop the malicious packets.
Implementation: Placing an IPS between the external firewall and the internal network.

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

Signature-Based IDS- operates using a database of predefined signatures/ patterns that correspond to known threats.

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- Establishes a baseline of normal network behavior or
system activity. Then it monitors traffic or activity in real-time, looking
for deviations from this established baseline.
```

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: Physical
```

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

```
Application
```

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

```
Data: Access Control
```

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

```
Host: Vulnerability Management
```

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

```
Network
```

    f. Data is classified at the wrong classification level.

```
Data: Data Governance
```

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

```
Network: Network Segmentation
```

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.

```
TLS/SSL
```

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

```
Tracking Software
```

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

```
BIOS/UEFI: Disable boot from USB or external device.
```

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.

```
Stateful 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?

```
MAC 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 Security Onion 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?*)

```
Stating that a Trojan (JS/Nemucod.M.gen) was downloading an executable (EXE)
payload from the source IP (188.124.9.56) to the destination (192.168.3.35)
on port 1035. I would say that this is malicious activity that is trying to
compromise the targeted system.
```

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

```
Install malware on target machine.
```

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?	May have scanned for open ports on targets IP ranged or used phishing to lure victims.
Weaponization	What was downloaded?	JavaScript Trojan payload
Delivery	How was it downloaded?	HTTP from source IP to destination port
Exploitation	What does the exploit do?	Downloads payload, allowing unauthorized access or control over the machine.

Installation	How is the exploit installed?	Malware is installed silently on victims machine without the users knowledge.
Command & Control (C2)	How does the attacker gain control of the remote machine?	Establishes a connection back to the attackers command and control server to receive further instructions
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	Software may capture sensitive data and allow remote access or serve as a gateway for future attacks on the network.

4. What are your recommended mitigation strategies?

Network segmentation, endpoint protection, security awareness training for employees, updating systems and monitoring network traffic for abnormalities.

5. List your third-party references.

https://attack.mitre.org, https://blog.malwarebytes.com, https://www.cisa.gov