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 Controls
```

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

```
Administrative Security Controls
```

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

```
Technical Security Controls
```

Intrusion Detection and Attack Indicators

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

IDS or Intrusion Detection Systems are tools that can both analyze traffic and look for malicious signatures. It is similar to a firewall but it also reads the data in the packets, sends alerts and blocks malicious traffic if configured to do so. It is different from an IPS or Intrusion Prevention System because an IPS can **respond** to attacks. An IPS also physically connects inline with the flow of data whereas an IDS physically connects through a network tap or mirrored port.

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

Indicators of Attack indicate attacks that are happening in real time. They focus on revealing the intent and end goal of the attacker regardless of the exploit or malware used in the attack. Indicators of compromise indicate previous malicious activity. IOC's are used to establish an adversary's techniques, tactics and procedures.

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 threat actor doing research on an organization on public websites, social media or other publicly available sources.

2. Stage 2:

Weaponization - a cybercriminal may create a malicious document, like a PDF or Word file, that contains malware.

3. Stage 3:

```
Delivery - a cybercriminal delivers the weaponized payload via phishing email attack method.
```

4. Stage 4:

```
Exploitation - a threat actor takes advantage of a vulnerability in a system to get access to a target system and plant malicious software or steal sensitive information.
```

5. Stage 5:

```
Installation - while inside a target system, an attacker may install malicious software that can give them persistent access to the system, like the installation of remote access control or a keylogger.
```

6. Stage 6:

```
Command and Control - while accessing a target machine, an attacker may deploy a c2 agent like Cobalt Strike Beacon that allows users to interact with compromised systems, execute commands and send back important data.
```

7. Stage 7:

```
Actions on Objectives - An attacker with a motive of stealing financial information obtains sensitive financial documents of a banking institution after gaining access to the organizations system.
```

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.

From the Xpert Learning Assistant…

alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820:
This part specifies that the alert will trigger on TCP traffic from any external network address to any port in the range 5800 to 5820 on the local network.

msg:"ET SCAN Potential VNC Scan 5800-5820":
This is the message associated with the alert. It indicates that the rule is related to detecting a potential VNC (Virtual Network Computing) scan targeting ports 5800 to 5820.

flags:S,12:
This part specifies the TCP flags that should be set for the alert to trigger. In this case, it looks for the SYN (S) flag and the ACK (12) flag set in the TCP header.

threshold: type both, track by_src, count 5, seconds 60:
This section sets a threshold for triggering the alert. It specifies that the alert should trigger if 5 events matching this rule are detected from the same source IP address within a 60-second window.

reference:url,doc.emergingthreats.net/2002910:
This is a reference URL to additional information related to this rule, often pointing to a specific threat intelligence source.

classtype:attempted-recon:
This classifies the alert as an attempted reconnaissance activity, indicating that the rule is designed to detect reconnaissance attempts.

Sid:2002910:
This is the unique identifier for the Snort rule, used to differentiate it from others.

Rev:5:
This is the revision number of the rule.

metadata:created_at 2010_07_30, updated_at 2010_07_30:
These metadata fields specify the creation and last update dates of the rule.

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

Reconnaissance

3. What kind of attack is indicated?

This is a scanning attack targeting VNC (Virtual Network Computing) services on ports 5800 - 5820.

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.

From the Xpert Assistant…

Alert tcp $EXTERMAN_NET $HTTP_PORTS -> $HOME_NET any
This part of the rule specifies that the alert will trigger an TCP traffic from any external network address to any port in the HTTP_PORTS range on the local network

msg:"ET POLICY PE EXE or DLL Windows file download HTTP"
The message associated with the alert. It indicates that the rule is related to detecting a potential policy violation involving the download of a Windows Portable Executable file over HTTP.

Flow:established,to_client:
This part specifies that the traffic flow should be established and directed towards the client (inbound traffic).

flowbits:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate:
Flowbits are used to track certain conditions in the traffic flow. In this case, it checks if the flowbits ET.http.binary and ET.INFO.WindowsUpdate are not set.

file_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4:
This section of the rule looks for specific patterns in the file data payload.It checks for the presence of the "MZ" header (indicating a DOS executable file) within 2 bytes and then jumps 58 bytes to check for the "PE" header followed by two null bytes (indicating a Windows PE file).

flowbits:set,ET.http.binary:
If the pattern matching is successful, this sets the flowbit ET.http.binary, indicating that a binary file has been detected in the HTTP traffic.

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:
These are additional metadata fields associated with the rule, including the former category, reference URL, classification type, signature ID (SID), revision number, and creation/update dates.

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

```
Delivery
```

3. What kind of attack is indicated?

```
Malware Delivery
```

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:"Alert - Inbound Traffic on Port 4444 Detected";)
```

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 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.

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

- `web`:

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

- `sales`:

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

- `mail`:

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

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

```
HTTP: Allowed
HTTPS: Allowed
SMTP: Allowed
POP3: Allowed
```

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
$ sudo firewall-cmd --permanent --zone=drop --add-source=64.57.183.85
```

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-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-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=web --list-all
$ sudo firewall-cmd --zone=sales --list-all
$ sudo firewall-cmd --zone=drop --list-all
$ sudo firewall-cmd --zone=mail --list-all
$ sudo firewall-cmd --zone=public --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.

```
The first way an IDS or Intrusion Detection System connects to a network is through a Network Tap (Test Access Port). A Network Tap is a hardware device that provides access to a network. It transits both inbound and outbound data streams on separate channels at the same time. All data will arrive at the monitoring device in real time.
```

```
The second way an IDS connects to a network is by utilizing a SPAN or a Switched Port Analyzer, also known as port mirroring. A SPAN sends a mirror image of all network data to another physical port, where packets can be captured and analyzed.
```

2. Describe how an IPS connects to a network.

```
An IPS or Intrusion Prevention System is typically placed between the firewall and a network switch. It physically connects inline with the flow of data.
```

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.

```
Physical security
```

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

```
Application security
```

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

```
Data security
```

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

```
Host 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 security
```

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

```
Perimeter security
```

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

```
Full Disk Encryption
```

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

```
Using a Virtual Private Network (VPN)
```

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

```
Remote Monitoring and Tracking Software
```

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

```
Set a BIOS or 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.

```
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 Packet 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 or Proxy Firewalls
```

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 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 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?*)

```
[Enter answer here]
```

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.

```
Xpert Learning Assistant

Module 11.1 - 11.3 Student Guides
Modele 2.1 - 2.3 Student Guides

To find blacklisted IP addresses -
https://whatismyipaddress.com/blacklist-check

To convert URL to IP
https://www.nslookup.io/domains/korea.services.net/webservers/

Worked on assignment in group setting with Tim Sottile and Isabel Rodriguez
```