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?

All those are examples of physical security controls.

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

All are examples of administrative security controls.

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

All are examples of technical security controls.

Intrusion Detection and Attack Indicators

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

Intrusion detection systems (IDS) analyze traffic and look for malicious signatures, in other words an IDS reads the data in the packets it inspects, issues alerts/alarms, and blocks malicious traffic. IDS doesn't alter or react to packets as they enter the network.

An intrusion prevention system (IPS) does everything that an IDS can do, but can also respond to attacks. An IPS does this by blocking malicious traffic and preventing it from being delivered to a host on the network.

Another difference between IDS and IPS is how these two systems connect.
An IDS physically connects via a network tap (Test Access Port) or mirrored port/Switched Port Analyzer (SPAN).
An IPS physically connects inline with the flow of data, An IPS is typically placed in between the firewall and network switch.

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

Indicators of attack (IOA) indicate attacks happening in real time (currently in progress) but a full breach has not been determined or has not occurred yet. IOA's focus is on revealing the intent and end goal of the attacker regardless of the exploit or malware used in the attack.

Indicators of compromise (IOC) indicate previous malicious activity in other words it indicates that an attack occurred, resulting in a breach.
IOC expose all of the vulnerabilities used in an attack, giving network defenders the opportunity to revamp their defense as part of their mitigation strategy, and learn from an attack so it won't happen again

IOA takes a preventive stance, actively searching for and stopping intrusion attempts before they can compromise the system. IOCs, on the other hand, come into play after a successful intrusion, helping to identify and mitigate the damage.

The Cyber Kill Chain

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

1. Stage 1:

Reconnaissance

Reconnaissance is the first stage of the cyber kill chain, where cybercriminals gather information about their target from publicly available sources like: social media, company website, search engines (this is called Open-Source Intelligence).

Also cybercriminals might use automated tools to scan the target network and identify: Live IP addresses, open ports, network configurations (this is called Scanning and Enumeration).

Cybercriminals might use social engineering tactics to trick employees into revealing sensitive information, such as: Phishing emails, Vishing attacks etc

2. Stage 2:

Weaponization

In Cyber Kill Chain Weaponization techniques attackers use to create malicious payloads, ex Cybercriminals often use exploit kits, pre-packaged collections of exploits targeting specific software vulnerabilities.

3. Stage 3:

Delivery

Delivery is a crucial phase - it focuses on how the cybercriminals transmit malicious code or exploits to the target system. Example:
-Social engineering tactics are used during delivery to trick users into downloading or interacting with malicious payloads.
- Malicious Websites: cybercriminals can compromise legitimate websites or create fake ones designed to exploit vulnerabilities in a user's browser or software.
- USB Drives: Leaving infected USB drives in places where targets might find them can be a delivery method.

- Cybercriminals can use zero-day exploits to deliver malware without users being aware of the security weaknesses.

4. Stage 4:

Exploitation

In the exploitation step of the Cyber Kill Chain, cybercriminals take advantage of the vulnerabilities they have discovered in previous stages or weakness in software to further infiltrate a target's network and achieve their objectives.
Example:

- Exploiting Software Vulnerabilities: Unpatched Systems, Zero-Day Exploits, Buffer Overflow Attacks.
- Exploiting System Misconfigurations: Weak Passwords, Unnecessary Permissions, Disabled Security Features etc

5. Stage 5:

Installation

After cybercriminals have exploited their target's vulnerabilities to gain access to a network, they begin the installation stage of the Cyber Kill Chain: attempting to install malware and other cyberweapons onto the target network to take control of its systems and exfiltrate valuable data.
Example: In this step, cybercriminals may install cyberweapons and malware using Trojan horses, backdoors, or command-line interfaces.

6. Stage 6:

Command and Control

In the C2 stage of the Cyber Kill Chain, cybercriminals communicate with the malware they've installed onto a target's network to instruct cyberweapons or tools to carry out their objectives.

For example, cybercriminals may use communication channels to direct computers infected with the Mirai botnet malware to overload a website with traffic or C2 servers to instruct computers to carry out cybercrime objectives.

7. Stage 7:

Actions on Objectives

Actions on Objectives is the final stage of the Cyber Kill Chain carrying out their cyberattack objectives.
Examples: Data Theft Disruption/Denial-of-Service (DoS) attack, Privilege Escalation, ransomware etc

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.

Rule Header: alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820

This is suspicious TCP traffic coming from the $EXTERNAL_NET (probably internet or untrusted network) and any source port. Going to the $HOME_NET (internal network) specifically looking for traffic targeting ports in the range 5800 to 5820.

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

Reconnaissance

3. What kind of attack is indicated?

It might be a potential scan for a VNC (Virtual Network Computing) server targeting ports 5800 to 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.

Rule Header: alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any

This Snort rule header is designed to trigger an alert for TCP traffic coming from any external network ($EXTERNAL_NET) on any HTTP port ($HTTP_PORTS) and going to any IP address within the local network ($HOME_NET) on any port.
It is a generic rule that can be used to detect various types of HTTP-related traffic, and can detect potential suspicious or malicious activity involving TCP traffic over HTTP ports within the network.

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

Delivery stage of the cyber kill chain.

3. What kind of attack is indicated?

Policy violation related to the download of Windows executable (potential malicious PE EXE or DLL) files over HTTP.

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 traffic on port 4444")
```

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 ufw disable
```

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: “systemctl start firewalld” is the command suggested to use if we want
to start firewalld, but unfortunately it failed to start firewalld in our
VM.

To start firewalld I used the command from the user guide
“11-Network-Security” (to be more precise I ran the script in the
/etc/init.d directory).

$ sudo /etc/init.d/firewalld start
```

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 firewall-cmd --state
```

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

- `web`:

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

- `sales`:

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

- `mail`:

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

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

```
- In public zone status is YES for http, https, smtp and pop3
- In web zone status is YES only for http, and status is NO for https, smtp and pop3
- In sales zone status is YES only for https, and status is NO for http, smtp and pop3
- In mail zone status is YES for smtp and pop3, and status is NO for http, and 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.

```
$ sudo firewall-cmd --get-active-zones
```

Note: the request “Run the command that displays all zone services” doesn't much with the activity title “View Active Zone” and activity description where it is specified that we should run the command to display “active zones”.

The request “Run the command that displays all zone services” is asking us to display all zone services and the command for this is “sudo firewall-cmd --get-services” that doesn’t make sense in this specific activity. So, I believe we should display all active zone instead:
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" 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.

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

Network tap (Test Access Port) is a hardware device that replicates the entire network traffic flowing through a specific cable segment. Network taps transit both inbound and outbound data streams on separate channels at the same time, so all data will arrive at the monitoring device in real time.

2. Describe how an IPS connects to a network.

IPS physically connects inline with the flow of data. An IPS is typically placed in between the firewall and network switch.

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

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.

Host

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

Network

f. Data is classified at the wrong classification level.

Policy, procedures, & awareness

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

Perimeter

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.

One method of protecting data-in-transit is by using secure communication protocols such as SSL/TLS (Secure Sockets Layer/Transport Layer Security). These protocols encrypt the data exchanged between devices over a network, ensuring that it remains confidential and secure during transmission.

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

GPS (Global Positioning System) tracking.
GPS tracking software utilizes the Global Positioning System (GPS) to determine the precise location of a device, such as a laptop, in real-time.

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

Setting a BIOS password can restrict the boot options and prevent an attacker from booting a stolen laptop using an external hard drive.

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 firewalls, also known as packet-filtering firewalls

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?*)

The indicator of an attack is in the name of this event:
- "JS/Nemucod" - is known for malicious activity.
- "downloading EXE payload" - executable files can be used to install malware, steal data, or take control of the system.

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

First of all the purpose of this attack was the downloading of an EXE payload.
“JS/Nemucod” is a downloader script, the main goal is to download and execute other malicious payloads/malware such as Ransomware or Trojans.
The attacker's goals could be: stealing data, financial gain, disrupting the system, or gain access for later attacks.

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?	Nemucod malware is frequently delivered through spam or phishing emails that contain harmful attachments.. Also that’s what we have in Security Onion for this alert event: field rule.rule - “Spam campaigns using js nemucod downloader” that indicate that the attacker located the victim through phishing emails or

		malicious websites.
Weaponization	What was downloaded?	Downloaded was probably a Javascript file called JS/Nemucode.
Delivery	How was it downloaded?	Because this malware is frequently delivered through spam or phishing emails the user opens the attachment, malicious code is run and further malware is downloaded on the affected machine.
Exploitation	What does the exploit do?	The attacker is trying to use this exploit to get a malicious executable running on the victim's machine as a result the he could gain access for later attacks, access sensitive data etc
Installation	How is the exploit installed?	The JS/Nemucod once executed initiates the download of the EXE payload. This payload usually contains the real malware the attacker wants to install on the victim's machine.
Command & Control (C2)	How does the attacker gain control of the remote machine?	After the installation stage the attacker has direct connection to the infected machine, and can now control it. Through this connection, the attacker can freely steal data, install more malware or do other malicious actions on the victim's machine
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	Here are some potential actions that the software may perform to achieve its objectives: - steal data - install additional malware - establish a remote

		connection (backdoor) to the victim's machine. - encrypt files on the victim's system and demand a ransom for decryption

4. What are your recommended mitigation strategies?

```
   - Conduct regular cybersecurity awareness training for employees
   - Implement email filtering solutions
   - Use web filtering tools to block access to known malicious websites
   - Regularly update operating systems, software applications, and
     security tools
   - Regularly back up critical data and ensure that backups are stored
     securely.
And much more …
```

5. List your third-party references.

https://any.run/report/fb98c3221d1a8a4d43636b19307a61d13baa210d35d925dbeab197833b13f1c5/2b8cbb75-e7c0-4771-a1e2-f9e5411acb2c

https://www.cisecurity.org/insights/blog/malware-analysis-report-nemucod-ransomware

https://www.hybrid-analysis.com/sample/81e5669b060efa4d5977f8132d1b5b36b32bf80b74f79334ae2904a6540e3b0d/5f4f5775f37710425f1186d6