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?

An IDS is a detection system, it cannot act on the traffic coming through. An IPS can take action to block traffic based on info contained in the packet(s).

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

An IOA is an alert generated by an IDS when malicious traffic is detected. It happens in real time and is proactive. A full breach is perhaps not complete. Focus is to analyze intent. An IOC is an indication that there has been previous malicious activity. It is reactive, after a breach is complete. Focus is to analyze tactics.

The Cyber Kill Chain

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

1. Stage 1:

Reconnaissance. One example could be researching email addresses for employees of a company for a future phishing attack.

2. Stage 2:

Weaponization. This stage would include crafting a phishing campaign to be used along w/ the email addresses obtained during reconnaissance.

3. Stage 3:

Delivery. Sending the phishing emails with the malicious link.

4. Stage 4:

```
Exploitation. Getting someone to click the link in the malicious email, and
obtaining their credentials.
```

5. Stage 5:

```
Installation. Using the credentials obtained in stage 4, installing a
malicious program.
```

6. Stage 6:

```
Command and Control (C2). Remote control of a victim's machine/network,
obtained via the malicious program installed in stage 5.
```

7. Stage 7:

```
Actions on Objectives. Attacker can implement their end goal plan, using
access from C2 to pull the targeted data from the organization.
```

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.

```
This rule creates an alert based on TCP packets coming from an external IP
through any source port, inbound to an internal IP on destination ports 5800
through 5820 and generates the message, "ET SCAN Potentil VNC Scan
5800:5820"
```

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

```
Reconnaissance
```

3. What kind of attack is indicated?

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

```
This rule creates an alert based on TCP packets coming from an external IP
through an HTTP source port, inbound to an internal IP on any destination
port and generates the message, "ET POLICY PE EXE or DLL Windows file
download HTTP"
```

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

```
Delivery
```

3. What kind of attack is indicated?

```
An EXE or DLL file has been downloaded over HTTP. Potentially 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: "Inbound TCP Traffic
Detected on 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 killall 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.

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

*Must reload in order for new zones to show when running "sudo firewall-cmd
--list-all-zones"
```

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

*Can add "--permanent" to ensure your rules persist, but will require a
reload before they will be applied. Same goes for the following commands for
web, sales, and mail.
```

- `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`?

```
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-rich-rule='rule family="ipv4" source
address="10.208.56.23" reject'
sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" source
address="135.95.103.76" reject'
```

```
sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" source
address="76.34.169.118" reject'
sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" source
address="xx.xx.xx.xx" reject'

*Last command includes placeholder as this is the rule to be used for any
future blacklisted IPs, subbing in the specific address.
```

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-all-zones

*Command above will list out each zone and under each, those services
associated w/ the particular zone. If running "sudo firewall-cmd
--list-services" you would also need to include the "--zone=name" option for
the specific zone you would like to search for as without the "--zone=name"
addition, it will not show which services are associated with which 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" 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=public --list-all
sudo firewall-cmd --zone=web --list-all
sudo firewall-cmd --zone=mail --list-all
sudo firewall-cmd --zone=sales --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.

Network TAP (Test Access Port): a hardware device that taps into both in/outbound communication. Data arrival is in real time.

SPAN (Swiched Port Analyzer): AKA port mirroring. A mirror image of all traffic is sent to another device for capture/analysis.

2. Describe how an IPS connects to a network.

IPS is usually between the firewall and network switch, as part of the flow of data in/out of the network.

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.

```
Endpoint
```

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

```
Data
```

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

```
Endpoint
```

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
```

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.

```
Restrict access to files w/ data in question either to a pre-approved list
of persons, or to require a password to open the file.
```

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

```
Encryption
```

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?

```
Require two factor authentication. Unless the hacker also has the
phone/email tied to the 2 factor authentication method, they should be
unable to complete the boot.
```

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 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.

```
Packet-Filtering Firewall (Stateful)
```

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?

```
Packet-Filtering Firewall (Stateless)
```

5. Which type of firewall filters solely based on source and destination MAC address?

```
MAC Layer 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?*)

```
Download of EXE file over HTTP
```

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

```
Obtain access to data stored on the target machine, likely for ransom.
```

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 address
Weaponization	What was downloaded?	Executable file
Delivery	How was it downloaded?	Phishing email.
Exploitation	What does the exploit do?	Recipient of email opens attachment.
Installation	How is the exploit installed?	Upon opening what the user thinks is a PDF, the EXE file is downloaded/run and the dummy PDF opens as a decoy.
Command & Control (C2)	How does the attacker gain control of the remote machine?	EXE files are used to retrieve a Trojan downloader which allows the attacker to establish communication w/ the system and download the desired malware/ransomware.

Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	It depends on which particular malware is used. In some instances, info is encrypted and ransomed. In others, data and credentials can be stolen.

4. What are your recommended mitigation strategies?

Identify all downloaded files starting at the initial point of compromise and ensure complete removal. Follow steps of the organization's preferred antivirus software to adhere to the proper removal process. To prevent future attacks of a similar nature, use an extension in the email program if available from the current antivirus provider. If not available from the existing antivirus program, obtain means of scanning all email attachments before opening and trigger alert if the file name/type is suspicious.

5. List your third-party references.

https://certego.net/blog/blog-jsnemucode

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=JS/Nemucod

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.js.nemucod.ah

Sources:
For setting services on individual zones w/ firewalld:
https://www.linode.com/docs/guides/introduction-to-firewalld-on-centos/
Cyber Kill Chain:
https://www.youtube.com/watch?v=mMkonxKnqHI
Addl info on defense in depth layers definitions:
https://www.intrasource.co.uk/blog/it-security/7-layers-of-cyber-security/