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?

```
An Intrusion Detection System (IDS) is a passive security control that
monitors network traffic and generates alerts when it detects suspicious or
potentially malicious activity. An Intrusion Prevention System (IPS) is an
active security control that not only detects but also takes action to
prevent or stop potential attacks
```

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

```
An Indicator of Compromise (IOC) is a sign or evidence that a system or
network has been breached or compromised. IOC is typically generated after
the fact, when an attack has already occurred, and it is used to investigate
and determine the scope and impact of the attack. An Indicator of Attack
(IOA) is a proactive security measure that aims to identify and prevent
attacks before they can cause damage. IOA’s are generated based on known
attack techniques or patterns, rather than on specific indicators of
compromise. IOC’s are used to detect and investigate past security incidents
while IOA’s are used to identify and prevent future attacks before they
occur.
```

The Cyber Kill Chain

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

1. Stage 1:

```
Reconnaissance
Example: scanning for open ports, identifying operating systems, discovering
vulnerabilities
```

2. Stage 2:

```
Weaponization
Example: creating a malicious email attachment or a malware-infected website
```

3. Stage 3:

```
Delivery
Example: social engineering tactics to trick a user into opening a malicious
email attachment or clicking on a link
```

4. Stage 4:

```
Exploitation
Example: using a known software vulnerability to gain remote access to the
target system
```

5. Stage 5:

```
Installation
Example: creating a backdoor or remote access tool to allow the attacker to
return to the system at a later time
```

6. Stage 6:

```
Command and Control
Example: using a remote access tool to connect to the compromised system and
issue commands
```

7. Stage 7:

```
Actions and Objectives
Example: stealing passwords or credit card numbers, encrypting files,
deleting critical system files
```

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.

- alert: This specifies that an alert should be generated if the rule is triggered.
- tcp: This indicates that the rule applies to TCP traffic.
- $EXTERNAL_NET: This is a variable representing the external network.
- any: This specifies any source port.
- ->: This symbol indicates the direction of the traffic, in this case, from any source in the external network to the destination in the Home network.
- $HOME_NET: This is a variable representing the home network.
- 5800:5820: This specifies the destination port range to be matched, which in this case is the range of VNC server ports.
- msg:"ET SCAN Potential VNC Scan 5800-5820"; This is the message that will be logged if the rule is triggered, indicating a potential VNC scan in the specified port range.
- flags:S,12; This specifies the TCP flags that should be set to trigger the rule, which in this case are the SYN and FIN flags.
- threshold: This specifies a threshold to reduce false positives and optimize the detection of VNC scans.
- type both: This specifies the type of threshold, in this case, both the count and time will be used to trigger the rule.
- track by_src: This specifies that the threshold will be tracked based on the source IP address.
- count 5: This specifies that the rule should trigger after five matching events.
- seconds 60: This specifies the time period in which five matching events must occur.
- reference:url,doc.emergingthreats.net/2002910: This provides a reference to more information about the rule.
- classtype:attempted-recon: This specifies the classification of the rule as attempted reconnaissance.
- sid:2002910: This is a unique identifier for the rule.
- rev:5: This specifies the revision number of the rule.

- metadata:created_at 2010_07_30, updated_at 2010_07_30: This provides metadata information about the rule, such as its creation and update dates.

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

```
Reconnaissance stage
```

3. What kind of attack is indicated?

```
The alert indicates a potential VNC scan 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 Sort rule header and explain what this rule does.

```
[Enter answer here]
```

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

```
Content filtering layer
```

3. What kind of attack is indicated?

```
This rule could indicate a potential malware infection or an attempt to
download and execute a Windows executable or DLL file via HTTP, which
violates organizational policy
```

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 any (msg:”Inbound traffic detected on port
4444”; dport:any; flags:S; sid:1000001; rev:1;)
```

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 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.

```
$ sudo 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.

```
$ service --status-all
```

- 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 --add-interface=eth0 --permanent
$ sudo firewall-cmd --zone=web --add-interface=eth1 --permanent
$ sudo firewall-cmd --zone=sales --add-interface=eth2 --permanent
$ sudo firewall-cmd --zone=mail --add-interface=eth3 --permanent
```

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

- `web`:

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

- `sales`:

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

- `mail`:

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

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

```
HTTP and HTTPS added to the public and web zones
SMTP and POP3 added to the public and mail zones
HTTPS added to the sales zone
```

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=$IP
```

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 --list-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 --permanent --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 ehco` replies.

- Run the command that blocks `pings` and `icmp requests` in your `public` zone.

```
$ sudo firewall-cmd --zone=public --permanent --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
```

- 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.

```
 1. Inline IDS: sits directly on the network path and intercepts all
    traffic flowing through it. It operates by analyzing network packets
    in real-time and blocking or allowing them based on predefined
    security policies. Inline IDS requires careful configuration to avoid
    network disruption and to ensure that it does not become a single
    point of failure.
```

```
  2. Passive IDS: A passive IDS (also known as a network-based IDS)
     operates by monitoring a copy of a network traffic rather than
     intercepting it directly. It usually connects to a network tap or a
     span port on a switch to capture a copy of network traffic. Passive
     IDS is less intrusive than inline IDS and can be installed without
     affecting the network’s normal operation. However, it cannot block
     traffic, and administrators must use other security tools to respond
     to detected threats.
```

2. Describe how an IPS connects to a network.

```
An Intrusion Prevention System (IPS) typically connects to a network through
a network tap or a port mirroring switch. This allows the IPS to monitor all
the traffic passing through the network and analyze it for any suspicious or
malicious activity. Once connected, the IPS can use various techniques such
as signature-based detection, anomaly-based detection, and behavioral
analysis to identify potential threats and take action to prevent them from
causing harm. This can include blocking traffic from specific IP
addresses,ports, or protocols, as well as alerting security administrators
about potential security breaches. It’s important to note that the exact
steps for connecting an IPS to a network may vary depending on the specific
device and network configuration being used. It’s always recommended to
consult the manufacturer’s documentation or seek assistance from a qualified
network security professional to ensure proper setup and configuration of an
IPS.
```

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

```
The type of IDS that compares patterns of traffic to predefined signatures
and is unable to detect zero-day attacks is called a signature-based IDS.
Signature-based IDS works by comparing incoming traffic against a database
of known attack patterns or signatures, and if a match is found, it triggers
an alarm. However, since signature-based IDS relies on previously identified
attack patterns, it is ineffective against zero-day attacks,which are
attacks that exploit vulnerabilities that are unknown to the security
community.
```

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?

The type of IDS that 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 is called an anomaly-based IDS. Anomaly-based IDS works by learning the normal patterns of traffic on a network over time and creating a baseline of “normal” behavior. It then flags any deviations from this baseline as suspicious, regardless of whether or not the traffic matches a known attack signature. Since anomaly-based IDS is based on identifying abnormal behavior, it is particularly effective at detecting zero-day attacks, as well as new and previously unknown types of attacks. Anomaly-based IDS can also detect attacks who are probing or scanning the network, as these activities often involve unusual traffic patterns. However, anomaly-based IDS can be more difficult to set up and maintain than signature-based IDS, as it requires continuous monitoring and fine-tuning of the baseline to prevent false positives.

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 layer

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

Technical security layer

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

Data security layer

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

System security layer

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

Network security layer

f. Data is classified at the wrong classification level.

Data security layer

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

Network security layer

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

Data encryption. By doing this, the data is transformed into a scrambled, unreadable format that can only be deciphered with a decryption key.

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

Transport Layer Security (TLS) or Secure Sockets Layer (SSL). TLS and SSL are cryptographic protocols that provide a secure, encrypted channel between two devices over a network. These protocols use public key cryptography to establish a secure connection between the sender and receiver, and to encrypt and decrypt data as it is transmitted. By using TLS or SSL, organizations can protect sensitive data, such as login credentials, credit card information, or personal information, as it travels between devices, such as between a web server and a web browser or between two email servers. Additionally, implementing strong access controls, network segmentation, and firewalls can further protect data-in-transit by limiting access to critical systems and detecting and blocking suspicious activity.

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

GPS tracking system. GPS tracking systems use GPS technology to pinpoint the location of a device, such as a laptop or mobile phone, and transmit that location data to a central monitoring system. If a laptop is stolen, a GPS tracking system could help law enforcement to locate and recover the device by providing real-time location data.

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

BIOS passwords. By setting a BIOS password, the attacker is prevented from changing the boot order of the laptop, which is necessary to boot from an external device. Secure Boot. Secure Boot is a feature that is available on some laptops, which ensures that only authorized software is loaded during the boot process. If secure boot is enabled, the attacker cannot boot from an external hard drive, as the laptop's firmware will only allow trusted software to load during the boot process. Full Disk Encryption. Full Disk Encryption (FDE) is a technique that encrypts the entire hard drive of a laptop, including the boot sector. This makes it impossible for an attacker to boot the laptop from an external hard drive, as they would need to decrypt the hard drive first.

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 firewalls verify the three-way TCP handshake. Stateful firewalls maintain information about active connections and session state, allowing them to distinguish legitimate traffic from unauthorized traffic. When a new TCP connection is initiated, the stateful firewall checks the three-way TCP handshake to ensure that the connection is legitimate before allowing the traffic to flow. This helps to prevent various types of attacks, such as SYN floods, where an attacker sends a flood of SYN packets to a victim's server to overwhelm it with connection requests.

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.

```
Deep packet inspection firewall. Deep packet inspection firewalls are
designed to examine and analyze entire streams of packets, from the initial
handshake to the end of the session. Unlike traditional packet-filtering
firewalls, which only examine individual packets based on basic criteria
such as source and destination IP address and port number, deep packet
inspection firewalls can inspect the payload of packets, looking for
specific patterns and signatures that indicate malicious activity.
```

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. Proxy firewalls act as an intermediary between a client and
a server, intercepting all traffic and performing security checks before
forwarding it to its final destination. In this way, the proxy firewall acts
on behalf of the recipient, ensuring that the traffic is safe before
allowing it to pass through. Proxy firewalls can inspect and filter traffic
at the application layer, which allows them to detect and prevent a wide
range of attacks, such as SQL injection, cross-site scripting (XSS), and
buffer overflow attacks.
```

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. Packet filtering firewalls are a type of network
security device that filters incoming and outgoing traffic based on a set of
predefined rules. These rules are typically based on criteria such as the
source and destination IP addresses, port numbers, and protocol type. The
firewall examines each packet as it passes through a network interface and
decides whether to forward or discard it based on the rules.
```

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

```
MAC filtering firewall or Layer 2 firewall. MAC filtering firewalls operate
at the data link layer of the OSI model and use MAC addresses to control
access to a network. They can filter traffic based on the source of the MAC
address, destination MAC address or both.
```

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?*)

```
ET TROJAN JS/Nemucod.M.gen downloading EXE payload. This message suggests
that a Trojan with the name JS/Nemucod.M.gen is being downloaded and
executed on the destination machine.
```

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

```
The purpose of the attack was to download and execute a Trojan on a victim
machine, which could potentially be used to steal sensitive information or
gain unauthorized access to the system.
```

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?	Network or port scans Phishing emails Online searches or social media profiling
Weaponization	What was downloaded?	Suspicious files or executables onto the victim machine
Delivery	How was it downloaded?	Downloaded via HTTP on port 80
Exploitation	What does the exploit do?	Unclear what the exploit does
Installation	How is the exploit installed?	Not specified
Command & Control (C2)	How does the attacker gain control of the remote machine?	Unclear how the attacker gains control of the remote machine
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	Unclear what the software that the attacker sent does to complete its tasks

4. What are your recommended mitigation strategies?

```
Block the IP address or port number associated with the attack to prevent
further communication with the attacker.
Install and update anti-virus software to detect and prevent the malware
from executing on the system.
```

```
Educate users on safe browsing habits and the dangers of opening suspicious
emails or downloading attachments.
Implement network segmentation to prevent lateral movement and limit the
damage caused by successful attacks
```

5. List your third-party references.

```
https://www.snort.org/downloads#rules
https://csrc.nist.gov/
https://www.cisecurity.org/
```