Unit 11 Homework: Network Security

Submission Guidelines

Please complete and submit the Submission File for your homework deliverable.

Part 1: Review Questions

Before diving into a lab exercise, complete the following review questions:

Security Control Types

The concept of defense in depth can be broken down into three different 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?
2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?

Intrusion Detection and Attack indicators

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

What's the difference between an Indicator of Attack and an Indicator of Compromise?

The Cyber Kill Chain

Name each of the seven stages for the Cyber Kill chain and provide a brief example of each.

1. Stage 1:
2. Stage 2:
3. Stage 3:

4. Stage 4:
5. Stage 5:
6. Stage 6:
7. Stage 7:

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 Potentia
l VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by_src, co
unt 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classty
pe:attempted-recon; sid:2002910; rev:5; metadata:created_at 2010_07_30, u
pdated_at 2010_07_30;)
```

1. Break down the Sort Rule header. What is this rule doing?
2. What stage of the Cyber Kill Chain does the alerted activity violate?
3. What kind of attack is this rule monitoring?

Snort Rule #2

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY PE E
XE or DLL Windows file download HTTP"; flow:established,to_client; flowbi
ts:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file
_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"P
E|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata:
 former_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Mai
```

1. Break down the Sort Rule header. What is this rule doing?
2. What stage of the Cyber Kill Chain does the alerted activity violate?
3. What kind of attack is this rule monitoring?

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.

Part 2: "Drop Zone" Lab

In this lab exercise, you will assume the role of a Jr. Security Administrator at an indoor skydiving company called Drop Zone.

- Your company hosts a web server that takes online reservations and credit card payments. As a result, your company must comply with PCI/DSS regulations which requires businesses who take online credit card payments to have a firewall in place to protect personally identifiable information (PII).
- Your network has been under attack from the following three IPs: `10.208.56.23`, `135.95.103.76`, and `76.34.169.118`. You have decided to add these IPs to the drop zone within your firewall.
- The first requirement of PCI/DSS regulations is to protect your system with firewalls. "Properly configured firewalls protect your card data environment. Firewalls restrict incoming and outgoing network traffic through rules and criteria configured by your organization." PCI DSS Quick Reference Guide

Set Up:

For this lab you will use the Network Security Lab located in Azure.

- Once logged in, launch an instance of the machine `firewalld` from the HyperV Manager and login with the following credentials:
  - Username: `sysadmin`
  - Password: `cybersecurity`

Reference: https://manpages.debian.org/testing/firewalld/firewall-cmd.1.en.html

Instructions:

The Senior Security Manager has drafted configuration requirements for your organization with the following specification.

You need to configure `zones` that will segment each network according to service type.

- **Public Zone**

    - Services: HTTP, HTTPS, POP3, SMTP
    - Interface: ETH0

- **Web Zone**

    - Source IP: 201.45.34.126
    - Services: HTTP
    - Interface: ETH1

- **Sales Zone**

    - Source IP: 201.45.15.48
    - Services: HTTPS
    - Interface: ETH2

- **Mail Zone**

    - Source IP: 201.45.105.12
    - Services: SMTP, POP3
    - Interface: ETH3

You also need to drop all traffic from the following blacklisted IPs: - `10.208.56.23` - `135.95.103.76` - `76.34.169.118`

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`.

Enable and start `firewalld`

By default, the `firewalld` service should be running. If not, then run the following commands:

- Run the commands that enable and start `firewalld` upon boots and reboots.

  Note: This will ensure that `firewalld` remains active after each reboot.

Confirm that the service is running.

- Run the command that checks whether or not the `firewalld` service is up and running.

List all firewall rules currently configured.

Next, lists 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 not doing double work.

- Run the command that lists all currently configured firewall rules:
- Take note of what zones and settings are configured. You many 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 see if the service you need is available
- We can see that the `Home` and `Drop` Zones are created by default.

Zone Views

- Run the command that lists all currently configured zones.
- We can see that the `Public` and `Drop` Zones are created by default. Therefore, we will need to create Zones for `Web`, `Sales`, and `Mail`.

Create Zones for `Web`, `Sales` and `Mail`. (Hint look at the manpage in the instructions)

- Run the commands that create Web, Sales and Mail zones.
- If needed, use the manpages link for assistance.
- Remember to reload the firewalld service in order to apply your new settings before moving on.

Set the zones to their designated interfaces.

- Run the command that sets your `eth` interfaces to your zones.
- Use the configurations provided at the beginning of the instructions.

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.
- Use the configurations provided at the beginning of the instructions.

Add your adversaries to the Drop Zone.

- Run the command that will add all the blacklisted IPs to the Drop Zone.

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 ensure that the network remains secured after unplanned outages such as power failures.

- Run the command that reloads the `firewalld` configurations and writes it to memory.

View active Zones

Now, we'll want to provide truncated listings of all currently **active** zones. This a good time to verify your zone settings.

- Run the command that displays all zone services.

Block an IP address

- Use a rich-rule that blocks the IP address `138.138.0.3` on your public zone.

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.

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. Run one command at a time for each

zone.

- Are all of the rules in place? If not, then go back and make the necessary modification before checking again.

Congratulations! You have successfully configured and deployed a fully comprehensive `firewalld` installation.

Part 3: IDS, IPS, DiD, and Firewalls

Answer the following review questions.

IDS vs. IPS Systems

1. Name and define two ways an IDS connects to a network.
2. Describe how an IPS connects to a network.
3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?
4. Which 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?

Defense in Depth

1. For each of the following scenarios, provide the layer of Defense in Depth that applies:
    1. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.
    2. A zero-day goes undetected by antivirus software.
    3. A criminal successfully gains access to HR's database.
    4. A criminal hacker exploits a vulnerability within an operating system.
    5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.
    6. Data is classified at the wrong classification level.

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

2. Name one method of protecting data-at-rest from being readable on hard drive.
3. Name one method to protect data-in-transit.
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.
5. How could you 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.
2. Which type of firewall considers the connection as a whole? Meaning, instead of looking at only individual packets, these firewalls look at whole streams of packets at one time.
3. Which type of firewall intercepts all traffic prior to being forwarded 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?
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?
5. Which type of firewall filters based solely on source and destination MAC address?

Bonus Lab: "Green Eggs & SPAM"

This bonus activity is a culmination of the topics and tools covered during the following Unit 11 activities:

- Alert - FTP File Extraction
- Alert - ET INFO Executable Download
- Alert - C2 Beacon
- Investigation, Analysis, and Escalation Activity
- Threat Hunting - Cyber Threat Intelligence

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 Jr. 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.

Instructions

Log into the Security Onion VM and use the following **Indicator of Attack** to complete this portion of the homework.

Locate the following Indicator of Attack in Sguil:

- **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 of the reveal?
2. What was the attacker's motivation?
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 they attacker locate the victim?	
Weaponization	What was it that 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 it's tasks?	

1. What are your recommended mitigation strategies?

2. Cite your references here.

Important Note Regarding Unit 12:

Please make sure that you are set up on your personal Azure accounts prior to the first day of the Cloud Security unit. Use the following set up guide for assistance: Set-up Guide.
