Unit 11 Submission File: Network Security Homework

Part 1: 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?

   Physical Control

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

   Administrative Control

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

   Technical Control

Intrusion Detection and Attack indicators

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

   Answer: IDS (Intrusion Detection Service) Will document and log attacks for analysis, it does not respond to an attack. IPS (Intrusion Prevention System) Can do everything IDS does. It has the ability to respond to attacks.

2. What's the difference between an Indicator of Attack and an Indicator of Compromise?
   Answer: Indicator of Attack (IOA) detects attacks in real time. (IOC) Shows attacks after the incident occurred.

The Cyber Kill Chain

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

Stage 1: Reconnaissance (Gaining access to email or other personal information.

Stage 2: Weaponization (Cybercriminal creates malware to attack target.)

Stage 3: Delivery (Attack delivered by USB, email Attachments, or a website.)

Stage 4: Exploitation (Activating the payload (Malware on the targeted system.)

Stage 5: Installation (Malware install access point “Backdoor”.)

Stage 6: Command and control (Cybercriminal using remote access to control targeted system.)

Stage 7: Actions and Objectives (Cybercriminal gains access to data and system.)

Snort Rule Analysis

Use the Snort rule 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 is happening.

Answer:

- tcp = applies the rule to all TCP packets.
- $EXTERNAL_NET = applies the rule to packets whose source IPs are in the external network.
- any = applies the rule to packets coming from any port.
- -> = indicates the direction of traffic, from source to destination.
- $HOME_NET = applies the rule to packets whose destination IPs are in the home network.

- 5800:5820 = applies the rule to traffic whose destination port number in the range of 5800-5820.
- Snort generated an alert and logged the message “ET SCAN Potential VNC Scan 5800- 5820” when it detects TCP packets coming from the external network on any ports traveling into the local network on ports 5800 to 5820.”
- This rule logs the message “ET SCAN Potential VNC Scan 5800-5820” when it detects TCP packet coming from the external network on any ports going into the local network on ports 5800 to 5820.

What stage of the Cyber Kill Chain does this alert violate?

Answer: Stage 4 (Exploitation)

What kind of attack is indicated?

Answer: Indicator of Attack (IOA)

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 is happening.

Answer:

- tcp = applies the rule to all TCP packets
- $EXTERNAL_NET = applies the rule to packets whose source IPs are in the external network.
- $HTTP_PORTS = applies the rule to packets coming from any HTTP ports
- -> = indicates the direction of traffic, from source to destination.
- $HOME_NET = applies the rule to packets whose destination IPs are in the home network
- any = applies the rule to traffic to any destination port.
- msg:"ET POLICY PE EXE or DLL Windows file download HTTP" = the message Snort will print when it generates an alert.

- Snort generated an alert and logged the message “ET POLICY PE EXE or DLL Windows file download HTTP” when it detected TCP packets coming from the external network on HTTP ports going into the local network on any ports, or essentially when a file is downloaded from an external source.
- TCP packets coming from IP addresses in the external network whose ports were HTTP traveling to IP addresses in the home network, to any port.” (The message “ET POLICY PE EXE or DLL Windows file download HTTP” is announcing that someone has downloaded a Windows executable file or DLL over HTTP, where “ET POLICY” refers to an action that might violate corporate policy.)

2. What layer of the Defense in Depth model does this alert violate?

Layer 7 (Application)

3. What kind of attack is indicated?

IOC (Indicator of Compromise)

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 detected from port 4444”)

Part 2: "Drop Zone" Lab

Log into the Azure firewalld machine

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, these service should be running. If not, then run the following commands:

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

  sudo systemctl enable firewalld
  sudo systemctl state firewalld

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.

  sudo firewall-cmd --state

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:

  sudo firewall-cmd --list-all

- Take note of what Zones and settings are configured. You many need to remove unneeded services and settings.

  sudo firewall-cmd -zone=public --remove-service=ssh

  sudo firewall-cmd --zone=public --remove-service=dhcpv6-client

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

  sudo firewall-cmd --get-services

We can see 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

- 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.

Run the commands that creates 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
```

Set the zones to their designated interfaces:

Run the commands that sets 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 --permanent --add-service=http

  sudo firewall-cmd --zone=public --permanent --add-service=https

  sudo firewall-cmd --zone=public --permanent --add-service=pop3

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

Web:

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

Sales:

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

Mail:

sudo firewall-cmd --zone=mail --permanent --add-service=smtp

sudo firewall-cmd --zone=mail --permanent --add-service=pop3

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

  sudo firewall-cmd --list-all-zones

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=ipset:10.208.56.23
  sudo firewall-cmd --permanent --zone=drop --add-source=ipset:135.95.103.76
  sudo firewall-cmd --permanent --zone=drop --add-source=ipset: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 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

  sudo firewall-cmd --complete-reload

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.

  sudo firewall-cmd --get-active-zone

Block an IP address

- Use a rich-rule that blocks the IP address 138.138.0.3.

  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 ehco 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=sales --list-all
  sudo firewall-cmd --zone=mail --list-all

Are all of our rules in pace? 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, we will work on another lab. Before you start, complete the following review questions.

IDS vs. IPS Systems

Name and define two ways an IDS connects to a network.

Network TAP (Test Access Port) Transit both inbound and outbound data streams on separate channels at once, all data will arrive at the monitoring device in real time.

SPAN (Switched Port Analyzer). Sends a mirror image of all network data to another physical port, so packets can be captured and analyzed, like port mirroring.

Describe how an IPS connects to a network.

"IPS physically connects in line with the flow of data. An IPS are typically placed in between the firewall and network switch." *-Student Guide*

What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?

Signature based

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?

Anomaly based

Defense in Depth

For each of the following scenarios, provide the layer of Defense in Depth that applies:

A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.

Perimeter access measures

A zero-day goes undetected by antivirus software.

Endpoint Protection

A criminal successfully gains access to HR's database.

Application

A criminal hacker exploits a vulnerability within an operating system.

Host

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

Network

Data is classified at the wrong classification level.

Policy

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

Perimeter

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

Encryption

Name one method to protect data-in-transit.

VPN

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

GPS

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

Firmware password

Firewall Architectures and Methodologies

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 firewalls

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.

Stateful

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?

Application and Proxy

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

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

MAC layering

Bonus 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 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.

Threat Intelligence Card

Note: 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 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:

- What was the indicator of an attack?

  Alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:”ET TROJAN JS/Nemucod.M.gen downloading EXE payload”

- What was the adversarial motivation (purpose of attack)?

  To install malware on the target system to get personal information, with a ransom demand for decryption.

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	Harvesting of email.	
Weaponization	A zip file.	
Delivery	Email attachment.	
Exploitation	Targets users through malware spam campaigns, malware and execute it without the user's consent. Also found a PDF that looks like an invoice.	
Installation	Opening the zip and double clicking the file.	
Command & Control (C2)	Malware will get personal info found on the victim's system.	
Actions on Objectives	It will send stolen info back to criminals, they will demand money.	

- What are your recommended mitigation strategies?

  Better employee training.

  Keep operating software up to date.

  Stronger password policy.

  The use of VPN and VPC.

- List your third-party references.

  Google.com

  https://www.f-secure.com/v-descs/trojan-downloader_js_nemucod.shtml

  Trojan.JS.NEMUCOD.THBBFAI - Threat Encyclopedia (trendmicro.com)