**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 Security

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

Administrative Security

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

Technical Security

**Intrusion Detection and Attack indicators**

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

The Intrusion Detection System detects when intrusions have already happened on a network. On the other hand, an Intrusion Prevention System actively works to stop network intrusions before they happen.

1. What’s the difference between an Indicator of Attack and an Indicator of Compromise?

An Indicator of Attack indicates that a network is under attack from a malicious actor, while an Indicator of Compromise indicates that an attacker has gained access to and has compromised a network.

**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: Reconnaissance
2. Stage 2: Weaponization
3. Stage 3: Delivery
4. Stage 4: Exploitation
5. Stage 5: Install
6. Stage 6: Command and Control
7. Stage 7: Actions and Obections

**Snort Rule Analysis**

Use the Snort rule to answer the following questions:

Snort Rule #1

1. Break down the Sort Rule header and explain what is happening.

This rule creates alerts for traffic coming from any port in the range of 5800 to 5820 on the external net heading to home net.

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

This violates stage one.

1. What kind of attack is indicated?

VNC Scan

Snort Rule #2

1. Break down the Sort Rule header and explain what is happening.

Alerts when TCP traffic originates from the http ports stored on the network external net and going to any port on the network homenet.

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

Endpoint

1. What kind of attack is indicated?

Malware

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: "Traffic detected inbound on port 4444")

**Part 2: "Drop Zone" Lab**

**Uninstall ufw**

* Run the command that removes any running instance of ufw.

$ sudo apt remove ufw

**Enable and start firewalld**

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

$ sudo systemctl start firewall

$ sudo systemctl enable firewall

**Confirm that the service is running.**

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

$ systemctl status firewall

**List all firewall rules currently configured.**

* Run the command that lists all currently configured firewall rules:

$ sudo firewall-cmd --list-all

**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

**Zone Views**

* Run the command that lists all currently configured zones.

$ sudo firewall-cmd --get-zones

**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

**Set the zones to their designated interfaces:**

* Run the commands that sets your eth interfaces to your zones.

$ sudo firewall-cmd --reload

$ sudo firewall-cmd --zone=web --add-interface=eth1

$ sudo firewall-cmd --zone=sales --add-interface=eth2

$ sudo firewall-cmd --zone=mail --add-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=public --add-service=https

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

$ sudo firewall-cmd --zone=public --add-service=smtp

* 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=smtp

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

**Add your adversaries to the Drop Zone.**

* Run the command that will add all current and any future 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

$ sudo firewall-cmd --runtime-to-permanent

**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-zones

**Block an IP address**

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

$ sudo firewall-cmd --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 --permanent --add-icmp-block=echo-request --add-icmp-block=echo-reply

**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 --info-zone=public

$ sudo firewall-cmd --info-zone=mail

$ sudo firewall-cmd --info-zone=drop

$ sudo firewall-cmd --info-zone=web

$ sudo firewall-cmd --info-zone=sales

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

**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**

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

Test Access Port and Switched Port Analyzer

1. Describe how an IPS connects to a network.

In line with the flow of data, typically between the firewall and network switch.

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

Signature-based

1. 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**

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.

Answer: Physical

* 1. A zero-day goes undetected by antivirus software.

Answer: Application

* 1. A criminal successfully gains access to HR’s database.

Answer: Data

* 1. A criminal hacker exploits a vulnerability within an operating system.

Answer: Endpoint

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

Answer: Network

* 1. Data is classified at the wrong classification level.

Answer: Policy-Management

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

Answer: Perimeter

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

Answer: Encryption of Hardware

1. Name one method to protect data-in-transit.

Answer: Transport Layer Security

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

Answer: Geo-tracking

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

Answer: Secure-boot or a password in the BIOS / UEFI

**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 Gateways

1. 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.

Packet-Filtering

1. Which type of firewall intercepts all traffic prior to being forwarded to its destination. In a sense, these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it.

Proxy

1. 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

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

**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:

1. What was the indicator of an attack?
   * Hint: What do the details of the reveal?

Answer:

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

Answer:

1. 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? |  |

Answer:

1. What are your recommended mitigation strategies?

Answer:

1. List your third-party references.

Answer: