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.

Walls, bollards, fences, guard dogs, cameras, and lighting are what type of security control?

**Answer: Physical**

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

**Answer: Administrative**

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

**Answer: Technical**

Intrusion Detection and Attack indicators

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

**Answer: An IDS is a monitoring system that detects suspicious activities and generates alerts when they are detected. An IPS, however, is a control system that accepts and rejects packets based on a ruleset.**

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

**Answer: Indicators of Compromise is a reactive system that looks at events in retrospect, while an Indicator of Attack is more of a real time detection system.**

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. This is the stage at which hackers will search and gather information for suitable attack targets.**

**Stage 2: Weaponization. The hackers will search for vulnerabilities and prepare their attack.**

**Stage 3: Delivery. This is the stage where the attack starts typically by emails or USBs to deliver the malware/attack.**

**Stage 4: Exploitation. This is the stage where the attacker will exploit the vulnerabilities that they found prior to gain full access to the computer or network.**

**Stage 5: Installation. In this stage, the attacker will persist their malware to gain more access such as getting root access.**

**Stage 6: Command and Control. Now that the attacker has access, they can do specific actions such as establishing a connection to another computer.**

**Stage 7: Actions on Objectives. This is where the attacker finishes the attack and can do things such as encryption.**

**Snort Rule Analysis**

Use the Snort rule to answer the following questions:

Snort Rule #1

1. Break down the Sort Rule header. What is this rule doing?

**The rule is alerting when there is any TCP traffic from ports 5800 to 5820.**

1. What stage of the Cyber Kill Chain does the alerted activity violate?

**Reconnaissance**

1. What kind of attack is this rule monitoring?

**Potential VNC Scan**

Snort Rule #2

1. Break down the Sort Rule header. What is this rule doing?

**The rule is alerting when there is any TCP traffic on port 80.**

1. What stage of the Cyber Kill Chain does the alerted activity violate?

**Delivery**

1. What kind of attack is this rule monitoring?

**Policy PE EXE or DLL file download**

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 on port 4444”)**

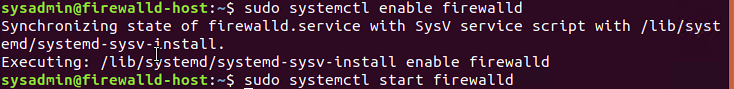
**Part 2: "Drop Zone" Lab**

**Uninstall ufw**

Text

Description automatically generated

**Enable and start firewalld**



**Confirm that the service is running.**

****

**List all firewall rules currently configured.**

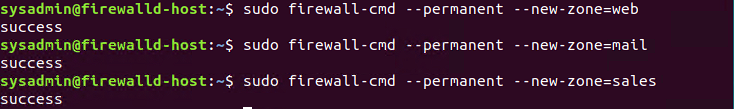
Text

Description automatically generated

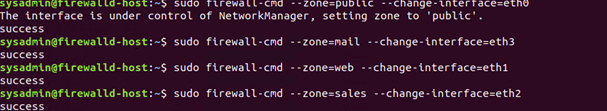
**Zone Views**



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

****

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

****

**Add services to the active zones.**

* **Public**

Text

Description automatically generated

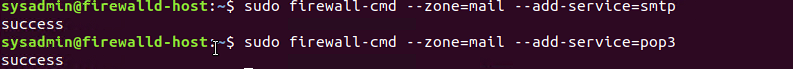
* **Web**



* **Sales**



* **Mail**



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

A screenshot of a computer

Description automatically generated with medium confidence

**Make rules permanent then reload them**



**View active Zones**

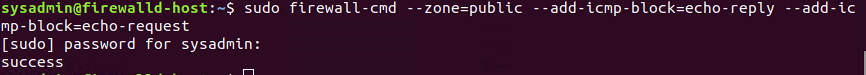
Text

Description automatically generated

**Block an IP address**



**Block Ping/ICMP Requests**



**Rule Check**











### 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.

**The two ways an IDS connects to a network is: Network and Host.**

**A network IDS enacts intrusion detection over a network by using all packet metadata and contents to determine threats.**

**A host IDS enacts intrusion detection through a particular endpoint, and monitors network traffic and system logs to and from a particular device.**

1. Describe how an IPS connects to a network.

**An IPS is usually placed behind the firewall and inspects every packet that passes through it. It usually is given access to this information by connecting to a network hub, a network switch, or a network tap.**

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

**Signature Based Intrusion Detection**

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 Intrusion Detection**

#### 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.

**Physical**

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

**App**

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

**Data**

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

**Host**

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

**Internal Network**

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

**Policies, Procedures, and Awareness**

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

**Perimeter**

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

**Encryption**

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

**Encrypted connections such as HTTPS or SSL**

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

**A tracker such as LoJack.**

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

**BitLocker**

#### 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 Gateway**

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.

**Stateful Inspection Firewalls**

1. 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?

**Proxy Firewall**

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 Firewall**

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

**MAC Address-Filtering**