**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?

Answer: Physical

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

Answer: Administrative

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

Answer: Technical

**Intrusion Detection and Attack indicators**

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

Answer: Intrusion Detection Systems (IDS) analyses and monitors network traffic for packets and other signs of potential network invasion, and then flags any known threats & hacking methods.   
  
Intrusion Preventive Systems (IPS) proactively aims to deny network traffic based on a security profile if that packet represents a known security threat. This is the difference between IDS and IPS as IPS can control and shut potential threats out and not deliver any malicious packets, while IDS simply monitors for known threats.

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

Answer: Indicator of Attack (IOA) aims on detecting the intent of what an attacker is attempting to accomplish, regardless of what exploit, or malware is utilised in the attack.  
  
Indicator of Compromise (IOC) is a form of digital evidence to demonstrate that a cyber incident has occurred. This intelligence is consolidated by security response teams when a network breach has occurred, or during a scheduled security audit.

**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: Deceived users by having them click on malicious links that contain Trojan ransomware

Stage 2: Weaponization: The creation of a Trojan attack

Stage 3: Delivery: Delivered the Trojan attack via link that downloads an executable file with malicious code

Stage 4: Exploitation: Hidden malicious code within legitimate software

Stage 5: Installation: Trojan malware can be installed through social engineering, spear phishing, and exploit kits

Stage 6: Command and Control: Opens a secret communication tunnel, allowing the local malware deployment to communicate with an attacker’s Command & Control centre

Stage 7: Action on Objectives: Attacker gains the users system access

**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: This Snort Rule header will create an alert that applies to TCP packets coming from any IP address on the external network, ranging from ports 5800 – 5820 on the home network

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

Answer: Reconnaissance

1. What kind of attack is indicated?

Answer: Potential VNC Scan

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: Snort Header Rule looks to create an alert that applies to all TCP packets coming from all IP address through an external network from HTTP\_PORT 80 to all ports on the home network

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

Answer: Host

1. What kind of attack is indicated?

Answer: Ransomware

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.

Answer: alert tcp $External\_Network 4444 -> $Home\_Network any {msg “TCP packet Detected through port 4444”}

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

**Log into the Azure firewalld machine**

Log in 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 -y 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 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 or not the firewalld service is up and running.

sudo /etc/init.d/firewalld

**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 --direct --get-all-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

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

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

* Run the commands that sets your eth interfaces to your zones.
* sudo firewall-cmd --zone=Web --change-interface=eth1
* sudo firewall-cmd --zone=Sales --change-interface=eth2
* sudo firewall-cmd --zone=Mail --change-interface=eth3
* sudo firewall-cmd --zone=Public --change-interface=eth0

**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=smtp
* sudo firewall-cmd –zone=public add-service=pop3

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

What is the status of http, https, smtp and 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.
* 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

**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

firewall-cmd --permanent --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-zones

**Block an IP address**

* Use a rich-rule that blocks the IP address 138.138.0.3.
* sudo firewall -cmd --zone=Drop --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-requests

**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=Web –list-all
* $ sudo firewall-cmd –zone=Sales –list-all
* $ sudo firewall-cmd –zone=public –list-all
* $ sudo firewall-cmd –zone=Mail –list-all
* $ sudo firewall-cmd –zone=drop –list-all
* Are all of our 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, 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.

Answer 1: Network Tap – provides access to a network by transiting inbound & outbound data streams on separate channels simultaneously to ensure that all data will be delivered at the monitoring device in real time.

Answer 2: Switched Port Analyzer (SPAN) – transmits a mirror image of all network data to a different physical port, where the packets can be captured and examined

1. Describe how an IPS connects to a network.

Answer: IPS connects to the network by having physical connections inline with the flow of data, as the IPS is generally placed in between the firewall & network switch.

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

Answer: Signature based intrusion detection system

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?

Answer: Anomaly-based intrusion detection system

**Defense in Depth**

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: Perimeter

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

Answer: Network

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

Answer: Data

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

Answer: Application

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: Host

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

Answer: Data

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

Answer: Encryption

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

Answer: Public Key Encryption/Cryptography

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

Answer: GPS tracking

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

Answer: Block unauthorised external devices from connecting to your device via USB ports

**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.

Answer: Circuit-level Gateway Firewall

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.

Answer: Stateful Firewall

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?

Answer: Application-level Gateway

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?

Answer: Stateless/Packet Filtering Firewall

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

Answer: MAC Layer Filtering Firewall