**Unit 11 Homework: Network Security**

**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.**

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

Physical Security Controls

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

Administrative Controls.

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

Technical Controls.

**Intrusion Detection and Attack indicators**

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

An IDS sends alerts based on a ruleset when traffic triggers those rules. But it does not act on it.

IPS will actively block and react to the rules it has been configured with to traffic on the network.

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

Indicator of Attack is when you are currently being attacked while an indicator of compromise is after you have been attacked.

**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

Port scans on a network.

**Stage 2:**

Weaponization

Creating a deliverable payload such as a imbedded file in a word document.

**Stage 3:**

Delivery

Sending the corrupting files to the victim.

**Stage 4:**

Exploitation

The exploit executing the code, such as a executable script running.

**Stage 5:**

Installation

The exploit creating a pathway into the system such as a backdoor.

**Stage 6:**

Command & Control

The attacker's machine communicating with the tools installed on the host computer.

**Stage 7:**

Actions on Objective

The attacker working on the objective set such as

**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 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;)**

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

It is alerting to TCP traffic coming from the WAN connection to the internal “home net”. It has found that there is a potential VNC scan on the network.

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

This is stage 1, recon.

**What kind of attack is this rule monitoring?**

The classtype is attempted-recon.

**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;)**

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

Another TCP alert from the WAN connection to the “home net” over port 80. It is an alert for a file being downloaded MZ.

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

This is Stage 3, Delivery.

**What kind of attack is this rule monitoring?**

The attack the rule is monitoring is a windows Exe/DLL binary install.

**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\_Network 4444 -> any any (msg: “Traffic inbound on port 4444”

**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**](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**

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

An IDS can be connected either on the inside or the outside of the network. Inside being within the local LAN while outside being outward WAN facing.

**Describe how an IPS connects to a network.**

An IPS is best connected in-between the LAN and WAN and should act as the gatekeeper for traffic. It must be on the outer facing side of the network so it has the ability to block unwanted traffic.

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

A network based IDS will monitor and can look at the traffic signatures but it must be specifically set up to look at the packet information.

**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?**

A Host based IDS. It will monitor the end device to ensure that there is nothing on the machine that is not supposed to be there.

**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 laer/physical layer.

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

Endpoint security.

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

Data security layer

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

Host Layer

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

Application security layer.

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

Data Security layer

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

Perimeter Layer Security

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

Encryption such as bitlocker

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

VPN or transport layer security

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

Using the devices GPS functionality the asset could be tracked.

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

Using host based programs such as absolute to ensure the computer annot be used.

**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.**

A Stateful firewall will verify the TCP handshake.

**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.**

A Stateless firewall .

**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?**

An application firewall will intercept all traffic and verify the source.

**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?**

A Packet filtering firewall (network firewall) will perform a deep packet inspection on the incoming traffic.

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

A specific type of network based firewall can have rules set up to solely filter traffic by mac addresses.