## **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.

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

Answer: **A Physical Control**

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

Answer: **A Administrative Control Type**

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

Answer: **A Technical Control Type**

#### **Intrusion Detection and Attack indicators**

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

Answer: **A IPS is a control system. It logs and takes action against potential threats. An IDS is a monitoring system. It does not alter the network packets.**

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

Answer: **Both are similar, only that Indicator of Attack focus on Identifying attacker while the attack is in progress.**

**(https://en.wikipedia.org/wiki/Intrusion\_detection\_system)**

**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**

**Attackers probe for weakness. This might include harvesting login credentials or information useful in a phishing attack.**

1. Stage 2: **Weaponization**

**Build a deliverable payload using an exploit and backdoor.**

1. Stage 3: **Delivery**

**Sending the weaponized bundle to the victim-for example, a malicious link in a legitimate-looking email.**

1. Stage 4: **Exploit**

**Executing code on the victim’s system.**

1. Stage 5: **Installation**

**Installing malware on the target asset.**

1. Stage 6: **Command and Control (C&C)**

**Creating a channel where the attacker can control a system remotely.**

1. Stage 7: **Actions**

**The attacker remotely carries out its intended goal.**

**(https://www.csoonline.com/article/2134037/strategic-planning-erm-the-practicality-of-the-cyber-kill-chain-approach-to-security.html)**

#### 

#### 

#### 

#### 

#### 

#### **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;)

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

**Answer: Alerts user of Any inbound TCP traffic from ports “5800 - 5820”.**

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

Answer: **Reconnaissance**

1. What kind of attack is this rule monitoring?

**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. What is this rule doing?

**Answer: Alerts for inbound TCP traffic on port 80, “HTTP”.**

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

**Answer: Policies, awareness, and procedures.**

1. What kind of attack is this rule monitoring?

**Answer: 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.

**Answer: alert tcp $EXTERNAL\_NET 4444 -> $HOME\_NET any (msg; “ET Possible Trojan or CrackDown)**

### **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 require 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](https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf)

#### **Set-Up:**

For this lab, you will use the Network Security Lab located in Azure.

* Once logged in, launch an instance of the machine firewall from the HyperV Manager and log in with the following credentials:
  + Username: sysadmin
  + Password: cybersecurity

**Reference:**<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 firewall service. This also ensures that the firewall will be your default firewall.

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

**$ sudo apt -y remove ufw**

#### **Enable and start the firewall**

By default, the firewall service should be running. If not, then run the following commands:

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

**$ sudo systemctl enable firewalld**

**$ sudo systemctl start firewalld**

Note: This will ensure that firewall remains active after each reboot.

#### 

#### **Confirm that the service is running.**

* Run the command that checks whether or not the firewall 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 may 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 firewalld-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. (Hint look at the manpage in the instructions)**

* Run the commands that create Web, Sales, and Mail zones.

**$ sudo firewall-cmd --permanent --new-zone=web**

**$ sudo firewall-cmd --permanent --new-zone=mail**

**$ sudo firewall-cmd --permanent --new-zone=sales**

* If needed, use the [manpages link](https://manpages.debian.org/testing/firewalld/firewall-cmd.1.en.html) for assistance.
* Remember to reload the firewall 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.

**$ sudo firewall-cmd --zone=public --change-interface=eth0**

**$ sudo firewall-cmd --zone=mail --change-interface=eth0**

**$ sudo firewall-cmd --zone=sales --change-interface=eth0**

**$ sudo firewall-cmd --zone=web --change-interface=eth0**

* 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.

**Public:**

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

**$ sudo firewall-cmd --zone=public --add-service=http**

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

**$ 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**

* 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.

**$ 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 firewall installation remains nailed up and retains its services across reboots. This ensures that the network remains secured after unplanned outages such as power failures.

* Run the command that reloads the firewall configurations and writes it to memory.

**$ sudo firewall-cmd --reload**

#### **View active Zones**

Now, we'll want to provide truncated listings of all currently **active** zones. This is 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 on your public zone.

**$ 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 echo 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 firewall 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.

**$ sudo firewall-cmd --zone=public --list-all**

**$ sudo firewall-cmd --zone=sales --list-all**

**$ sudo firewall-cmd --zone=mail --list-all**

**$ sudo firewall-cmd --zone=web --list-all**

**$ sudo firewall-cmd --permanent --zone=drop --list-all**

* 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 firewall installation.

### **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.

**Answer: IDS connects to a network through the Perimeter and its Host.**

1. Describe how an IPS connects to a network.

**Answer: An IPS connects to a network physically through a switch.**

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

**Answer: Signature Types**

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 Types**

(https://en.wikipedia.org/wiki/Intrusion\_detection\_system)

#### **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: Host**

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

**Answer: Network**

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

**Answer: Policy, Procedures, and Answers**

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

**Answer: Encryption**

* 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 a hard drive.

**Answer: One method to protect a readable hard drive could be by using Encryption.**

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

**Answer: To protect data-in-transit would be by using a VPN.**

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

**Answer: Law enforcement could track and recover a stolen laptop by using tracking software.**

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

**Answer: You can prevent an attacker from booting a stolen laptop by using an encrypted password.**

#### **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: A Circuit Level Proxy**

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: A Stateful Packet Filter**

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

**Answer: A Application of Proxy**

1. Which type of firewall examines data within a packet as it progresses through a network interface by examining the source and destination IP address, port number, and packet type- all without opening the packet to inspect its contents?

**Answer: Packet-filtering firewall**

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

**Answer: A Mac Firewall**

**(https://www.geeksforgeeks.org/firewall-methodologies/)**

### **Bonus Lab: "Green Eggs & SPAM"**

This bonus activity is a culmination of the topics and tools covered during the following Unit 11 activities:

* Alert - FTP File Extraction
* Alert - ET INFO Executable Download
* Alert - C2 Beacon
* Investigation, Analysis, and Escalation Activity
* Threat Hunting - Cyber Threat Intelligence

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.

#### **Instructions**

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:

* **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 questions:

1. What was the indicator of an attack?

**Answer: The indicator of the attack “msg:”ET TROJAN JS/Nemucod.Mgendownloading EXE payload”**

* + Hint: What do the details of the reveal?

1. What was the attacker's motivation?

**Answer: The attacker’s motivation was to steal passwords and info by use of a TROJAN.**

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 the attacker locate the victim?  **Answer: Physhing Emails** |  |
| **Weaponization** | What was it that was downloaded?  **Answer: ET TROJAN JS/Nemucod.Mgendownloading EXE payload** |  |
| **Delivery** | How was it downloaded?  **Answer: Trojan-Downloader.JS.Nemucod is distributed as a JavaScript file embedded in a ZIP file that is attached to an email message.** |  |
| **Exploitation** | What does the exploit do?  **Answer: Nemucod is usually used by attackers to distribute malware such as** [**Zeus**](https://www.f-secure.com/v-descs/trojan-spy_w32_zbot.shtml) **variants or various password- or info-stealers. In more recent malware distribution campaigns, the file observed being downloaded by Nemucod has been ransomware, typically either** [**TeslaCrypt**](https://www.f-secure.com/v-descs/trojan_teslacrypt.shtml) **or** [**Locky**](https://www.f-secure.com/v-descs/trojan-downloader_js_locky.shtml)**.** |  |
| **Installation** | How is the exploit installed?  **Answer: If an unsuspecting recipient opens the attached ZIP file and runs the JavaScript file it contains, Trojan-Downloader.JS.Nemucod will download a file to the %TEMP% folder and run it.** |  |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine?  **Answer: Once installed the attacker sits and steals sensitive info such as passwords and other data. Has also been known to install ransomware.** |  |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks?  **Answer: Automatically download and install malware. Steal any and all sensitive info and passwords.** |  |

1. What are your recommended mitigation strategies?

**Answer: Send out group policy to be folowed, and or decoy phshing emails. Install antivirus and use the proper port settings.**

1. Cite your references here.

**Answer: https://www.f-secure.com/v-descs/trojan-downloader\_js\_nemucod.shtml**