| Cybersecurity |
| --- |
| Module 11 Challenge Submission File |

## Network Security Homework

Make a copy of this document to work in, and then fill out the solution for each prompt below. Save and submit this completed file as your Challenge deliverable.

### Part 1: Review Questions

#### Security Control Types

The concept of defense in depth can be broken down into three 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 Control |
| --- |

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

| Administrative Security Control |
| --- |

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

| Technical Security Control |
| --- |

#### Intrusion Detection and Attack Indicators

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

| IDS scans for potential vulnerabilities and attempts to detect any intrusions. IPS is more of a prevention system that can deny packets as they are incoming and can also stop intrusions. |
| --- |

1. What’s the difference between an indicator of attack (IOA) and an indicator of compromise (IOC)?

| IOA searches for any early attack indicators that would show a potential or possible intrusion and will work to prevent. Meanwhile IOC is more reactive and engages after it identifies that the system has been compromised and will use different protocols to begin recovery after an attack. |
| --- |

#### The Cyber Kill Chain

Name the seven stages of the cyber kill chain, and provide a brief example of each.

1. Stage 1:

| Reconnaissance: Gathering data and other information that could be used against a target, i.e. dumpster diving. |
| --- |

1. Stage 2:

| Weaponization: Preparing a file or script to be an exploitable method of attack. Loading malware or other malicious software onto thumbdrives. |
| --- |

1. Stage 3:

| Delivery: Sending the weaponized file or script in a manner that you think will help gain access. Using the thumbdrives as an example would be to randomly distribute them or drop them in high foot traffic areas where they could be easily seen and hopefully picked up and plugged in. |
| --- |

1. Stage 4:

| Exploitation: Execution of malicious code or script on the victim’s device. |
| --- |

1. Stage 5:

| Installation: The weaponized file will be installed on a device and ready for use. |
| --- |

1. Stage 6:

| Command and Control: A remote channel for an attacker to use the victim’s system. |
| --- |

1. Stage 7:

| Actions on Objective: Attacker proceeds towards the completion of their objective. |
| --- |

#### 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 and explain what this rule does.

| Header is “alert tcp $EXTERNAL\_NET any -> $HOME\_NET” and the rule is scanning the port range of 5800-5820. |
| --- |

1. What stage of the cyber kill chain does the alerted activity violate?

| Stage 1, Reconnaissance |
| --- |

1. What kind of attack is indicated?

| 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 this rule does.

| alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET warning that TCP packets were sent from the external net through HTTP on port 80. Rule: "ET POLICY PE EXE or DLL Windows file download HTTP" which states that an executable or dll file was downloaded to the home\_net. |
| --- |

1. What layer of the defense in depth model does the alerted activity violate?

| Host, since it is alerting to a download. |
| --- |

1. What kind of attack is indicated?

| Due to the metadata created message I believe that it’s a ransomware attack. |
| --- |

**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 -> $Home\_Net any (msg:”packet detected through port 4444”;) |
| --- |

### Part 2: “Drop Zone” Lab

#### Set up.

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 remove ufw |
| --- |

#### Enable and start firewalld.

By default, the firewalld service should be running. If not, then 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 the firewalld service is up and running.

| $ sudo systemctl status firewalld |
| --- |

#### List all firewall rules currently configured.

Next, list 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 ensuring that you don’t duplicate work that’s already done.

* 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 find out whether the service you need is available.

| $ sudo firewall-cmd -–get-services |
| --- |

* Notice 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 |
| --- |

* Notice that the public and drop zones are created by default. Therefore, you will need to create zones for web, sales, and mail.

#### Create zones for web, sales, and mail.

* Run the commands that create web, sales, and mail zones.

| $ firewall-cmd -–permanent -–new-zone=web  $ firewall-cmd --permanent --new-zone=sales  $ firewall-cmd --permanent --new-zone=mail |
| --- |

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

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

| $ sudo firewall-cmd --zone=web --interface=eth0  $ sudo firewall-cmd --zone=sales --interface=eth0  $ sudo firewall-cmd --zone=mail --interface=eth0  $ sudo firewall-cmd -–reload |
| --- |

#### 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 -–add-service=http -–zone=public -–permanent  $ sudo firewall-cmd -–add-service=https -–zone=public -–permanent  $ sudo firewall-cmd -–add-service=smtp -–zone=public -–permanent  $ sudo firewall-cmd -–add-service=pop3 -–zone=public -–permanent |
| --- |

* web:

| $ sudo firewall-cmd --add-service=http --zone=web --permanent |
| --- |

* sales:

| $ sudo firewall-cmd --add-service=https --zone=sales --permanent |
| --- |

* mail:

| $ sudo firewall-cmd --add-service=smtp --zone=mail --permanent  $ sudo firewall-cmd --add-service=pop3 --zone=mail --permanent |
| --- |

* What is the status of http, https, smtp and pop3?

| All services are active, ran sudo systemctl then searched list using / to verify apache smtp and pop3 were running. |
| --- |

#### 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=ipset:blacklist |
| --- |

#### 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 helps ensure that the network remains secure 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, 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 --list-services |
| --- |

#### 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 ehco replies.

* Run the command that blocks pings and icmp requests in your public zone.

| $ sudo firewall-cmd --zone=public --add-icmp-block=echo-request |
| --- |

#### 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=sales --list-all  $ sudo firewall-cmd --zone=mail --list-all  $ sudo firewall-cmd --zone=web --list-all  $ sudo firewall-cmd --zone=public --list-all  $ sudo firewall-cmd --zone=drop --list-all |
| --- |

* Are all of the 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, you’ll 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.

| Network Tap: A device that directly connects to network cabling to split or copy packet traffic for network management and monitoring. |
| --- |

| SPAN: Monitors network traffic through port mirroring and analyzing packets. Typically less effective due to only providing a single SPAN port. |
| --- |

1. Describe how an IPS connects to a network.

| With the flow of data in 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 IDS |
| --- |

1. What 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 IDS |
| --- |

#### 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.

| Perimeter |
| --- |

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

| Network |
| --- |

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

| Data |
| --- |

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

| Application |
| --- |

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

| Network |
| --- |

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

| Host |
| --- |

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

| Data |
| --- |

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

| Encryption |
| --- |

1. Name one method of protecting data-in-transit.

| Cryptography |
| --- |

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

| GPS tracking |
| --- |

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

| Multi Factor authentication or password protected BIOS |
| --- |

#### 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 considering only individual packets, these firewalls consider whole streams of packets at one time.

| Stateful Firewalls |
| --- |

1. Which type of firewall intercepts all traffic prior to forwarding it 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.

| Application Gateways |
| --- |

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?

| Stateless Packet Filtering Firewall |
| --- |

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

| Mac Firewall |
| --- |

### 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 junior 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 in to the Security Onion VM, and use the following **indicator of attack** to complete this portion of the assignment. |
| --- |

Locate the 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 questions:

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

| It states in the header that a download was initiated through port 80 on the home net with a trojan payload. |
| --- |

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

| Steal data, whether it be confidential, private, or personal. There could be various reasons as to why they wanted the data. |
| --- |

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? | Outbound SSH scan |
| **Weaponization** | What was downloaded? | Trojan |
| **Delivery** | How was it downloaded? | Through an email with an exe. |
| **Exploitation** | What does the exploit do? | Steals private information or possibly ransomware delivery. |
| **Installation** | How is the exploit installed? | In the background when a user opens pdf. |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | Provides access to the victim’s system. |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? | Steals the data, compresses, then sends it back to the attacker. |

1. What are your recommended mitigation strategies?

| Implementing a firewall or multiple firewalls and other detection systems at the right location within/ outside of the network. |
| --- |

1. List your third-party references.

| There is a reference in the packet to www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/ |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.