| 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 Controls |
| --- |

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

| Administrative Security Controls |
| --- |

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

| Technical Security Controls |
| --- |

#### Intrusion Detection and Attack Indicators

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

| IDS is a detection system and is passive. IPS is prevention/protection and is active/ intrusive to the network. |
| --- |

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

| IOA is proactive and used to focus on imminent attacks with potential tactics and behaviors, whereas IOC is reactive and evidence based, helping to identify previous attacks |
| --- |

#### The Cyber Kill Chain

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

1. Stage 1:

| Reconnaissance |
| --- |

1. Stage 2:

| Weaponization |
| --- |

1. Stage 3:

| Delivery |
| --- |

1. Stage 4:

| Exploitation |
| --- |

1. Stage 5:

| Installation |
| --- |

1. Stage 6:

| Command and Control |
| --- |

1. Stage 7:

| Actions on Objectives |
| --- |

#### 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 Snort rule header and explain what this rule does.

| An alert that was triggered due to a variable external networking IP attempting to contact the home network IPs via TCP connection on any port to ports within the range 5800-5820 |
| --- |

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

| This is the Reconnaissance stage of the Cyber Kill Chain, the attacker is trying to gather information about the target environment to identify potential vulnerabilities or entry points. |
| --- |

1. What kind of attack is indicated?

| A VNC Port Scan attack |
| --- |

**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 Snort rule header and explain what this rule does.

| The alert was triggered due to a download of an EXE over HTTP. The header shows that the external network IP is attempting to communicate over any HTTP based ports that the Home network might have open |
| --- |

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

| This is the Delivery stage of the Cyber Kill Chain, malicious files or payloads are delivered to the target system |
| --- |

1. What kind of attack is indicated?

| Remote Malware download -attempting Command and Control |
| --- |

**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:"Inbound traffic detected on port 4444";/) |
| --- |

### Part 2: “Drop Zone” Lab

#### Set up.

Log into the web lab.

* Username: sysadmin
* Password: cybersecurity

**Important:** If your class started **BEFORE April 8, 2024,** You will need to do the following to start up the containers:  
  
Open a terminal window and run the following command to start up the docker containers (Note: this should be one continuous line).

| $ wget https://gist.githubusercontent.com/jlow3939/904eb58af3605457255df35c649f9873/raw/69bc0efdb38837ecce8db14662e9efffbfe15429/docker-compose.yml && docker-compose up -d |
| --- |

All classes that start **AFTER April 8, 2024**, will not need to do the previously indicated step. They will navigate to cd ~/Cybersecurity-Lesson-Plans/11-NetSec and type docker-compose up.

Run the following command to verify that the firewalld container is running:

| $ docker ps |
| --- |

Start a session with the firewalld container using the following command:

| $ docker exec -it firewalld bash |
| --- |

#### 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 ufw disable && sudo apt-get remove --purge ufw -y |
| --- |

#### 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.

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

* web:

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

* sales:

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

* mail:

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

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

| Running / yes sudo firewall-cmd --zone=[zone-name] --query-service=[service] |
| --- |

#### 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  $ sudo firewall-cmd --zone=drop --permanent --add-source=[Blacklisted IP] |
| --- |

#### 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 --reload |
| --- |

#### 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 --get-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 --permanent --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 --permanent --add-rich-rule='rule family="ipv4" protocol value="icmp" drop' |
| --- |

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

| Host-based IDS |
| --- |

1. Describe how an IPS connects to a network.

| IPS can connect in two ways, inline deployment which is placed directly in a network path between two points or a tap/SPAN port deployment via a network tap or port mirroring configuration to monitor traffic without interfering with traffic |
| --- |

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?

| Behavior/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.

| Physical Security |
| --- |

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

| Endpoint Protection/ Intrusion Detection |
| --- |

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

| Data Access Controls and Encryption |
| --- |

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

| System and Application Hardening |
| --- |

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

| Network Security and DDoS Protection |
| --- |

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

| Data Classification and Management |
| --- |

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

| Network Security and Firewall Configuration |
| --- |

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

| Full Disk Encryption |
| --- |

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

| Transport Layer Security |
| --- |

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

| Anti-Theft Software |
| --- |

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

| Disable Booting from External Devices via BIOS settings or enabling Secure boot |
| --- |

#### 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.

| Stateful firewall |
| --- |

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 Firewall |
| --- |

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.

| Proxy / Application 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 solely based on source and destination MAC address?

| MAC Filtering Firewall |
| --- |

### Optional Additional Challenge 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 Security Onion 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?*)

| A network trojan detected |
| --- |

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

| Steal private information |
| --- |

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? | Passive recon |
| **Weaponization** | What was downloaded? | Trojan malware |
| **Delivery** | How was it downloaded? | Exe from email download |
| **Exploitation** | What does the exploit do? | Steals private info |
| **Installation** | How is the exploit installed? | Malware gets installed when the user opens the PDF |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | Installed malware gives access to the hacker communicating to the hacker’s network |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? | Compresses the files and sends it to the hacker |

1. What are your recommended mitigation strategies?

| Add an IDS in order to monitor for network abnormalities involving network communications or an IPS for realtime prevention based on known signatures. |
| --- |

1. List your third-party references.

| <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDownloader:JS/Nemucod> <https://www.f-secure.com/v-descs/trojan-downloader-js-nemucod.shtml> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malware-mystery-jsnemucod-downloads-legitimate-installer/> |
| --- |

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