| 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 |
| --- |
|  |

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

| Administrative |
| --- |

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

| Technical |
| --- |

#### Intrusion Detection and Attack Indicators

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

| An IDS (Intrusion Detection System) will alert a SOC analyst about a potential incident, the analyst will then manually look at it and decide if it requires further action or not. An IPS (Intrusion Prevention System) does the same as and IDS, but can actively stop attacks happening automatically itself. |
| --- |

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

| IOA (Indicator of Attacks) identifies suspicious activity during an attack. IOC (Indicator of Compromise) analyzes evidence after an attack or system has been compromised. |
| --- |

#### The Cyber Kill Chain

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

1. Stage 1:

| Reconnaissance: where the attacker is information gathering on the target. This is passive as it is collecting information that is already public knowledge. Might scour LinkedIn for example. |
| --- |

1. Stage 2:

| Weaponization: which method of attack to use based on the information gathered in the reconnaissance stage. Finding a weak point to infiltrate. |
| --- |

1. Stage 3:

| Delivery: how the weapon identified in the weaponization stage will be delivered. Via email, website, USB etc. |
| --- |

1. Stage 4:

| Exploitation: Prepares for escalation during the installation phase. Getting the weapon to run on the system. Phishing email may have been clicked. |
| --- |

1. Stage 5:

| Installation: Getting the weapon installed on to the target’s system. Could be malware install, or backdoor implants. |
| --- |

1. Stage 6:

| C2 (Command and Control): When the attacker has command and control of the target system remotely. Most typically used is Internet Relay Chat (IRC). |
| --- |

1. Stage 7:

| Actions on Objectives: The attacker has achieved “hands on keyboard” access to the target, and can now act on their objectives. Could be to encrypt files for financial gain, or DDoS for ransom. |
| --- |

#### 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.

| This will create an ET Scan (Emerging Threats) alert for all tcp packets coming from any IP address on the internet (or external network) from any port to ports numbered 5800 - 5820 on the home network. |
| --- |

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

| Reconnaissance |
| --- |

1. What kind of attack is indicated?

| Penetration testing by using potential VNC (Virtual Network Computing) scan to gain remote access. |
| --- |

**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.

| This will create an alert that applies to all tcp packets coming from any IP address from the internet or external network through port 80 (HTTP) to any ports on the home network. This indicates that a Windows file has been attempted to be downloaded, but it was blocked as it violates the policy. |
| --- |

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

| Installation |
| --- |

1. What kind of attack is indicated?

| This could be ransomware or malware hidden in the downloadable Windows file. |
| --- |

**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: “TCP packet 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 apt remove ufw  Could also use the disable function  $ sudo ufw disable |
| --- |

#### 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 /etc/init.d/firewalld start |
| --- |

| **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 /etc/init.d/firewalld status |
| --- |

#### 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=public --change-interface=eth0  $ sudo firewall-cmd --zone=web --change-interface=eth1  $ sudo firewall-cmd --zone=sales --change-interface=eth2  $ sudo firewall-cmd --zone=mail --change-interface=eth3 |
| --- |

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

* 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?

| Enabled or active |
| --- |

#### 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 –-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 --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-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 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=web --list-all  $ sudo firewall-cmd --zone=sales --list-all  $ sudo firewall-cmd --zone=mail --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.

| SPAN Port (Switched Port Analyzer) or a Mirrored Port: mirrors all network traffic to another physical port. |
| --- |

| Network TAP (Test Access Point): hardware device providing access to a network. Allows data streams to be transmitted to monitoring devices in real time for all inbound and outbound traffic on separate channels simultaneously. |
| --- |

1. Describe how an IPS connects to a network.

| An IPS (Intrusion Prevention System) is connected inline with the flow of network traffic between the firewall and the network switch. This way, all network traffic must pass through the IPS. |
| --- |

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.

| Physical Security |
| --- |

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

| Application Security |
| --- |

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

| Data Security |
| --- |

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

| Host Security |
| --- |

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

| Perimeter Security |
| --- |

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

| Data Security |
| --- |

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

| Network Security |
| --- |

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

| Encryption of the data-at-rest will stop it being readable on hard drives. |
| --- |

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

| Other than encryption, the use of a VPN (Virtual Private Network) would protect data-in-transit. |
| --- |

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

| To track and recover a stolen laptop, GPS technology should be employed. |
| --- |

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

| The use of a strong firmware password would prevent hackers accessing the stolen laptop. |
| --- |

#### 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 Firewalls verify the three-way TCP handshake. |
| --- |

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 Packet Filtering Firewall will consider whole streams of packets instead of individual packets. |
| --- |

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 Firewall inspect the traffic and apply security policies before forwarding the traffic to its final destination. |
| --- |

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 Firewalls will inspect the header information of each packet without inspecting the contents of the packet. |
| --- |

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

| MAC Layer Firewalls inspect the source and destination MAC addresses in the ethernet frames. |
| --- |

### 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?*)

| Shows an email being downloaded on the home network that has an EXE file which contains trojan malware. |
| --- |

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

| Gain access to the network to 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 reconnaissance |
| **Weaponization** | What was downloaded? | Trojan malware |
| **Delivery** | How was it downloaded? | Email through EXE files |
| **Exploitation** | What does the exploit do? | Steals private information |
| **Installation** | How is the exploit installed? | Background installation when user opens PDF file |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | Installed malware communicates with hacker network giving them access to the system. Most likely through IRC (Internet Relay Chat) |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? | Compresses the files before sending it back to the hacker. |

1. What are your recommended mitigation strategies?

| Implement an IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) to detect anomalies in traffic both inbound and outbound, and mitigate these in real time. Use MFA (Multi Factor Authentication) if not already in use. Train the employees on good cyber security hygiene. Apply software updates and upgrades immediately. |
| --- |

1. List your third-party references.

| National Security Agency (NSA) 2018, “NSA’s Top Ten Cybersecurity Mitigation Strategies”, viewed Friday 10th May 2024, <https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf>  Sophos 2024, “Intrusion Protection System and Intrusion Detection System”, viewed Saturday 11th May 2024, <https://www.sophos.com/en-us/cybersecurity-explained/ips-and-ids>  edX UWA 2024, course content, module 11. |
| --- |

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