| 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 Control |
| --- |

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

| Administrative Control |
| --- |

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

| Technical Control |
| --- |

#### Intrusion Detection and Attack Indicators

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

| * IDS: An IDS is a system that monitors for any type of malicious activity, it then alerts the administrator of the machine of any malicious activity. An IDS only detects malicious activity it does not prevent it * IPS: An IPS is a system that also monitors for any type of malicious activity it also acts against it by trying to block the attack or mitigate the attack as much as possible. AN IPS detects malicious activity but also acts against it preventing it from entering the machine. |
| --- |

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

| * IOC: IOCs are specific pieces of information that indicate a system has been hacked.IOCs detect this by specific patterns in what a malicious activity would look like. IOCs can be implemented as file hashes which is a unique identifier for a file if this changes it may indicate malicious activity. They can also be used in IPs and domain names IOCs will take note of known malicious IPs and domain names and won't accept information from those specific IPs or Domain names. * IOA: IOAs detect ongoing attacks by observing the activity and looking at the tactics techniques and procedures (TTP) in the attack they observe an attack rather than gather information about a previous attack. IOAs can be implemented into a system and detect patterns in a system like a hacker gaining access to the system and trying to move from machine to machine by escalating privileges or attacking vulnerabilities in a system. * IOCs (Indicator of a compromise)   + Focus: Detects previous attacks and relies on known patterns   + Implementation: On file hashes, IPs, and domain names to recognize known malicious entities   + Utilization: It is reactive and works on data from previous attacks * IOAs (Indicator of Attack)   + Focus: Detects ongoing attacks and observes the tactics, techniques, and procedures of an attack   + Implementation: Monitors system activities for patterns associated with an attack such as privilege escalation and taking advantage of vulnerabilities   + Utilization: It is proactive and adaptive against evolving threats. |
| --- |

#### The Cyber Kill Chain

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

1. Stage 1:

| * Reconnaissance:   + Example: Gathering information about a target, such as looking at online forums to find vulnerabilities |
| --- |

1. Stage 2:

| * Weaponization:   + Example: Creating malicious software made to target the victim's vulnerabilities |
| --- |

1. Stage 3:

| * Delivery:   + Example: Sending out phishing emails or using corrupted USB drives on the victim's computer |
| --- |

1. Stage 4:

| * Exploitation:   + Example: Making use of the information you got from the information you gathered about the victim by exploiting a vulnerability in the system and gaining access |
| --- |

1. Stage 5:

| * Installation:   + Example: Once in the target machine a hacker deploys malware in the victim's machine and creates a backdoor so the hacker can have consistent access to the machine |
| --- |

1. Stage 6:

| * Command & Control (C2):   + Example: A Hacker has a connection between the machine and a remote server for data exchange and control of the system |
| --- |

1. Stage 7:

| * Actions On Objectives:   + Example: Acheiving the desired goal set in the attackers mind such as data theft, stealing money, black mail, or service disrption all depends on the attackers 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 Snort rule header and explain what this rule does.

| * Alert:   + Sends an alert when the specific rules and conditions are   Met   * Tcp:   + Specifies the protocol to which the rule applies, in this case, TCP * $EXTERNAL\_NET any -> $HOME\_NET 5800:5820:   + IP Address and Port Definition   + Defines source and destination IP addresses.   + $EXTERNAL\_NET: External network addresses.   + $HOME\_NET: Internal network.   + Triggers traffic on ports 5800 to 5820. * (msg:"ET SCAN Potential VNC Scan 5800-5820";:   + Provides a human-readable output related to the rule indicating that the rule conditions are met when there is a VNC scan on ports 5800 to 5820 * Flags: s,12;   + Specifies the TCP flags that must be set for the rule to trigger. In this case, it requires the SYN (S) and RST (12) flags to be set. * threshold: type both, track by\_src, count 5, seconds 60;   + Implements thresholding to prevent excessive alerts.   + Triggers rule if five events occur within 60 seconds. * reference: url,doc.emergingthreats.net/2002910;   + Provides a URL with additional information about the snort and in this case its emergingthreats.net * Classtype: attempted-recon   + Sets a type of classification for the rule which indicates attempted association with reconnaissance * sid: 2002910;   + A unique identifier for the Snort rule. * Rule Revision: 5   + Specifies rule revision number. * metadata: created\_at 2010\_07\_30, updated\_at 2010\_07\_30;   + Provides metadata indicating when the rule was created and last updated. |
| --- |
|  |
|  |

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

| It violates the reconnaissance cyber kill chain because it attempts to gather information about VNC Services |
| --- |

1. What kind of attack is indicated?

| The attacker is initiating a VNC scan and is scanning for VNC services on ports 5800 to 5820. VNC scans can lead to larger exploitation |
| --- |

**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.

| * Alert:   + Sends an alert when the specific rules and conditions are   Met   * Tcp:   + Specifies the protocol to which the rule applies, in this case, TCP * $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any:   + $EXTERNAL\_NET: External network addresses.   + $HTTP\_PORTS: Typically associated with HTTP traffic.   + ->: Specifies the direction of the traffic flow, indicating that the traffic is going from the external network to the internal network.   + $HOME\_NET any: Represents any destination address in the local (home) network, and "any" indicates that the destination port can be any. |
| --- |

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

| The Snort rule detects an HTTP download attempt of a potentially harmful Windows PE file, aligning with the "Delivery" phase of the Cyber Kill Chain. |
| --- |

1. What kind of attack is indicated?

| * Attack Type:   + The rule indicates a potential download of a malicious executable or DLL file over HTTP, which is characteristic of various malware delivery methods or potentially unwanted activities |
| --- |

**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 any any -> $HOME\_NET 4444 (msg:"Inbound Traffic on Port 4444"; sid:1000001;) |
| --- |

### Part 2: “Drop Zone” Lab

#### Set up.

Log into the Azure firewalld machine 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 firewalld-cmd –state |
| --- |

#### 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 --get-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 --permanent  $ sudo firewall-cmd --zone=sales --change-interface=ETH2 --permanent  $ sudo firewall-cmd --zone=mail --change-interface=ETH3 --permanent |
| --- |

#### 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  --add-service=https  --add-service=pop3  --add-service=smtp  --permanent |
| --- |

* web:

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

* sales:

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

* mail:

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

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

|  |
| --- |

#### 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 |
| --- |

#### 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 --permanent --zone=public --add-rich-rule='rule family="ipv4" source address="138.138.0.3" drop' |
| --- |

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

| * Inline Mode of IDS   + Positioned directly in network traffic flow.   + Actively blocks or allows traffic based on analysis. |
| --- |
|  |

| * IDS Promiscuous Mode Overview   + Connected passively to the network via tap or mirror port.   + Analyzes network traffic copies without active participation within the traffic flow |
| --- |

1. Describe how an IPS connects to a network.

| * IPS Network Connection   + IPS deployed in-line, directly monitoring network traffic flow.   + Actively analyzes network/system activities.   + Can take automated actions like blocking/altering traffic based on findings. |
| --- |

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

| * IDS Types: Signature-Based and Zero-Day   + Signature-Based IDS: Relies on predefined patterns of known threats.   + Detects malicious activities by matching observed traffic patterns against these signatures.   + Less effective against novel or zero-day attacks. |
| --- |

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 Overview   + Monitors network/system activities.   + Establishes baseline of normal behavior.   + Flags/alerts on significant deviations.   + Effective in detecting unknown threats.   + Includes probing and scanning activities. |
| --- |
|  |

#### 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.

| * Layer of Defense: Physical Security   + Technical Control: Access Control Systems (Keycard access, Biometric authentication).   + Physical Control: Security Guards, Turnstiles.   + Administrative Control: Employee Training on Tailgating Prevention, Strict Access Policies. |
| --- |

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

| * Layer of Defense: Network Security   + Technical Control: Intrusion Detection/Prevention Systems (Network-based and Host-based IDS/IPS).   + Technical Control: Application Whitelisting.   + Administrative Control: Regular Security Audits, Incident Response Plan. |
| --- |

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

| * Layer of Defense: Database Security   + Technical Control: Access Controls (Role-based access, Least Privilege).   + Technical Control: Encryption of sensitive data.   + Physical Control: Server Room Access Controls.   + Administrative Control: Database Security Policies, Employee Background Checks |
| --- |

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

| * Layer of Defense: Host-based Security   + Technical Control: Patch Management.   + Technical Control: Antivirus Software.   + Technical Control: Network Firewalls.   + Administrative Control: Regular Security Training, Incident Response Plan. |
| --- |

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

| * Layer of Defense: Network Security   + Technical Control: Firewalls.   + Technical Control: Intrusion Prevention Systems (IPS).   + Technical Control: DDoS Mitigation Services.   + Administrative Control: Incident Response Plan, Communication Plan. |
| --- |

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

| * Layer of Defense: Data Classification Policies   + Administrative Control: Clear Data Classification Policies and Procedures.   + Administrative Control: Employee Training on Data Handling.   + Technical Control: Data Loss Prevention (DLP) Tools. |
| --- |

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

| * Layer of Defense: Network Security   + Technical Control: Firewalls.   + Technical Control: Intrusion Detection Systems (IDS).   + Technical Control: Network Segmentation.   + Administrative Control: Regular Security Audits, Incident Response Plan. |
| --- |

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

| * Method: Encryption   + (Full Disk Encryption, File-level Encryption). |
| --- |

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

| * Method: SSL/TLS Encryption   + (Secure Sockets Layer/Transport Layer Security). |
| --- |

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

| * Technology:   + GPS Tracking Software or Hardware. |
| --- |

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

| * Method:   + Disable booting from external devices in laptop's BIOS or UEFI settings to prevent theft, even if the attacker has physical possession. |
| --- |

#### 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 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 Firewalls |
| --- |

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

| MAC Layer Firewalls |
| --- |

### 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 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?*)

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

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? |  |
| **Weaponization** | What was downloaded? |  |
| **Delivery** | How was it downloaded? |  |
| **Exploitation** | What does the exploit do? |  |
| **Installation** | How is the exploit installed? |  |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? |  |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? |  |

1. What are your recommended mitigation strategies?

| [Enter answer here] |
| --- |

1. List your third-party references.

| [Enter answer here] |
| --- |

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