| 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?

| The above are examples of physical security controls. |
| --- |

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

| The above are examples of administrative security controls. |
| --- |

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

| The above are examples of technical security controls. |
| --- |

#### Intrusion Detection and Attack Indicators

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

| An IDS (Intrusion Detection System) monitors network traffic and has alerts when it detects suspicious activity while an IPS (Intrusion Prevention System) detects and blocks/mitigates threats that are detected. |
| --- |

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

| An Indicator of Attack (IOA) indicates real time attacks that are either ongoing or happened recently and help to identify active threats while an Indicator of Compromise (IOC) indicates a system breach or if it has been compromised and gathering information/evidence of 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 information about a network that has been targeted for attack, as an example-looking for ports or services that are vulnerable. |
| --- |

1. Stage 2:

| Weaponization: Creating/using malicious software, such as a trojan, or back door into a targeted machine. |
| --- |

1. Stage 3:

| Delivery: Sending out malicious software to the target with phishing emails, compromised websites, or even instant messages. |
| --- |

1. Stage 4:

| Exploitation: Exploiting weaknesses in the target’s system to execute the malicious payload. |
| --- |

1. Stage 5:

| Installation: Installing/using code to grant root access to a created malicious user or ensuring that you can have an established presence within the network being targeted. |
| --- |

1. Stage 6:

| Command and Control (C2): Adding communication channels with the system that is compromised to be able to control them remotely. |
| --- |

1. Stage 7:

| Actions on Objectives: Achieving the desired goals on the targeted network/machine, such as data exfiltration or disrupting the system. (Accomplishing the goal that was intended.) |
| --- |

#### 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.

| It’s an alert of transmission control protocol (TCP) traffic on ports 5800 to 5820 and possibly using a VNC (virtual network computing) scan to identify VNC servers on a network. |
| --- |

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

| This activity violates the Reconnaissance stage of the cyber kill chain. |
| --- |

1. What kind of attack is indicated?

| This indicates an attempted reconnaissance 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.

| This alert shows a TCP connection from an external network to the targeted network on HTTP ports. A violation has occurred with policy regarding downloads from HTTP ports. It appears to be an attempt to deliver/download malicious files the download of Windows executable files |
| --- |

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

| This activity violates the Delivery stage of the cyber kill chain. |
| --- |

1. What kind of attack is indicated?

| This indicates a policy violated related to executable file downloads 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 any any -> $HOME\_NET 4444 (msg:"Inbound Traffic on Port 4444") |
| --- |

### 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-get 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 --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=public --change-interface=ETH0 --permanent  $ sudo firewall-cmd --zone=web --add-source=201.45.34.126 --permanent  $ sudo firewall-cmd --zone=sales --add-source=201.45.15.48 --permanent  $ sudo firewall-cmd --zone=mail --add-source=201.45.105.12 --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  $ 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?

| They are all enabled.  $ sudo firewall-cmd –zone=public –list-services  ssh dhcpv6-client http https pop3 smtp |
| --- |

#### Add your adversaries to the drop zone.

* Run the command that will add all current and any future blacklisted IPs to the drop zone.

| $ <ADD COMMAND HERE>  $ <ADD COMMAND HERE>  $ <ADD COMMAND HERE>  $ <ADD COMMAND HERE> |
| --- |

#### 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.

| Network Tap = An IDS can connect to a network via a network tap, which can monitor network traffic without disrupting the network's operations. |
| --- |

| Span port = An IDS can connect to a network through a span port on a network switch, receiving copies of network traffic without disrupting the network’s operations. |
| --- |

1. Describe how an IPS connects to a network.

| IPS connects behind the firewall and typically connects to a network inline, between the internal network and the external network. It intercepts and analyzes network traffic in real-time. It can then block or prevent traffic based on rules or policies that are in place. |
| --- |

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

| Signature-based IDS: Signature-based IDS operates by comparing observed network traffic, system activity, or file content against a database of predefined signatures or patterns that represent known malicious behavior. |
| --- |

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 : Instead of relying on predefined signatures of known threats, anomaly-based IDS looks for deviations from normal behavior, which may include unusual network traffic patterns, unexpected system resource usage, or abnormal user activity. |
| --- |

#### 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.

| Access control |
| --- |

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

| Operating system security |
| --- |

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

| Network security |
| --- |

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

| Security awareness training |
| --- |

* 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 |
| --- |

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

| SSL/TLS encryption |
| --- |

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?

| Enabling BIOS password protection and configuring secure boot options |
| --- |

#### 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 Inspection 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.

| Proxy 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?

| Stateful Inspection Firewall |
| --- |

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

| MAC Layer 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 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?*)

| A Trojan malware variant known as "JS/Nemucod.M.gen" is attempting to download an executable (EXE) payload. |
| --- |

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

| The purpose of the attack is to download a malicious executable payload to the target’s system by exploiting a vulnerability. |
| --- |

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? | The attacker may have performed reconnaissance to identify vulnerabilities. |
| **Weaponization** | What was downloaded? | A malicious JavaScript file (JS/Nemucod.M.gen) was used to download an executable (EXE) payload. |
| **Delivery** | How was it downloaded? | It was delivered via HTTP protocol from the source IP to the destination IP |
| **Exploitation** | What does the exploit do? | It takes advantage of vulnerabilities to execute the payload |
| **Installation** | How is the exploit installed? | Most likely remote exploitation |
| **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?

| Maintain up-to-date antivirus and anti-malware solutions to detect and remove malicious files and activities. |
| --- |

1. List your third-party references.

| Boot camp resources, slides, notes, zoom classes, and also chatgpt for definitions of terms. |
| --- |

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