| 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?

| These types of security control are ‘Physical’ control. |
| --- |

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

| These types of security control are ‘Administrative’ control. |
| --- |

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

| These types of security control are ‘Technical’ control. |
| --- |

#### Intrusion Detection and Attack Indicators

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

| The difference between an IDS and an IPS is that an IDS does not mitigate an attack, but rather alerts when an attack is occuring and an IPS is a defensive system that will actively stop attacks when one occurs. |
| --- |

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

| The difference between an IOA and an IOC is that an IOA tells us that an attack is happening in real time and an IOC lets us know an attack happened and that there is a breach into our network. |
| --- |

#### The Cyber Kill Chain

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

1. Stage 1:

| Reconnaissance - this is when a threat actor is gathering information on a target on how best to approach an attack. |
| --- |

1. Stage 2:

| Weaponization - this is when a threat actor generates an attack of sorts going off of what they learned from their reconnaissance. |
| --- |

1. Stage 3:

| Delivery - this is when the threat actor implements the weapon being used into a victim's network. |
| --- |

1. Stage 4:

| Exploitation - this is when the weapon is being run on to the vulnerable victm’s system. |
| --- |

1. Stage 5:

| Installation - this is when the weapon is being installed into the network. |
| --- |

1. Stage 6:

| Command & Control - this is when the threat actor has absolute ‘command’ over the system and can ‘control’ it wherever they are. |
| --- |

1. Stage 7:

| Actions on Objectives - this is when the threat actor is able to perform ‘actions’ on their desired ‘objectives’, since they now have full control. |
| --- |

#### 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.

| This Snort Rule header is related to TCP packets, creating an alert on these packets that derive from any IP address from ports 5800-5820 within the home network. |
| --- |

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

| The stage of the cyber kill chain that this alerted activity violates the ‘Reconnaissance’ stage. |
| --- |

1. What kind of attack is indicated?

| The attack indicated is the ‘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.

| The Snort rule header generates an alert applying to all of the TCP packets coming through ‘HTTP\_PORT 80’ to any port on the network. |
| --- |

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

| This layer of the defense in depth model that this alerted activity violates is the ‘Host’. |
| --- |

1. What kind of attack is indicated?

| This kind of attack is called ‘Ransomware’. |
| --- |

**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\_Network any {msg: “TCP packet Detected through 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 -y 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.

| $ 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 --add-interface=eth0  $ sudo firewall-cmd --zone=Web --add-interface=eth0  $ sudo firewall-cmd --zone=Sales --add-interface=eth0  $ sudo firewall-cmd --zone=Mail --add-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 --add-service=http --permanent  $ sudo firewall-cmd --zone=public --add-service=https --permanent  $ sudo firewall-cmd --zone=public --add-service=smtp --permanent  $ sudo firewall-cmd --zone=public --add-service=pop3 --permanent |
| --- |

* web:

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

* sales:

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

* mail:

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

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

| The status of ‘not found’ has been applied to the services http, https, 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 --zone=drop --add-source=10.208.56.23  $ sudo firewall-cmd --zone=drop --add-source=135.95.103.76  $ sudo firewall-cmd --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 --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-all-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=drop --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 –list-all –zone=public  $ sudo firewall-cmd –list-all –zone=Web  $ sudo firewall-cmd –list-all –zone=Sales  $ sudo firewall-cmd –list-all –zone=Mail  $ sudo firewall-cmd –list-all –zone=drop |
| --- |

* 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.

| An IDS connects to a network by Network TAP that monitors all data that is incoming and outgoing on a network. |
| --- |

| An IDS connects to a network by SPAN that sends flagged data to a different port so it can be reviewed by a sysadmin. |
| --- |

1. Describe how an IPS connects to a network.

| An IPS connects to a network in the middle of a network switch and the firewall in regards to data traveling through a network. |
| --- |

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

| The type of IDS comparing patterns of traffic to predefined signatures and is unable to detect zero-day attacks is the signature based intrusion detection system. |
| --- |

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?

| The type of IDS that 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 is an anomaly based intrusion detection system. |
| --- |

#### 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.

| This layer of defense in depth is ‘Physical’. |
| --- |

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

| This layer of defense in depth is ‘Network’. |
| --- |

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

| This layer of defense in depth is ‘Data’. |
| --- |

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

| This layer of defense in depth is ‘Application’. |
| --- |

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

| This layer of defense in depth is ‘Network’. |
| --- |

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

| This layer of defense in depth is ‘Host’. |
| --- |

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

| This layer of defense in depth is ‘Data’. |
| --- |

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

| One method of protecting data-at-rest from being readable on a hard drive is through ‘Encryption’. |
| --- |

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

| One method of protecting data-in-transit is a ‘Data Encryption’. |
| --- |

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

| Technology that can provide law enforcement with the ability to track and recover a stolen laptop is through ‘GPS Tracking’. |
| --- |

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

| A way you can prevent an attacker from booting a stolen laptop using an external hard drive is through ‘2-Factor Authentication;. |
| --- |

#### 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.

| The type of firewall that verifies the three-way TCP handshake are ‘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.

| The type of firewall that considers the connection as a whole are ‘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.

| The type of firewall that intercepts all traffic prior to forwarding it to its final destination are ‘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?

| The type of firewall that 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 are ‘Stateless/Packet Filtering’ firewalls. |
| --- |

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

| The type of firewall filters solely based on source and destination MAC addresses are ‘MAC’ 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?*)

| It appears that this is a Trojan malware attack that is executed by the victim opening an EXE file in an email and the malware is automatically downloaded into the victim’s home network for future access and control. |
| --- |

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

| The purpose of the attack was to steal private 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? | Passive Reconnaissance |
| **Weaponization** | What was downloaded? | Trojan Malware |
| **Delivery** | How was it downloaded? | Email |
| **Exploitation** | What does the exploit do? | Steals private data |
| **Installation** | How is the exploit installed? | Installs malware when the PDF file is opened |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | Malware links with attacker’s network and gives the attacker access into the victim’s system |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? | Compresses the files before it sends it back to the attacker |

1. What are your recommended mitigation strategies?

| We need to implement an intrusion detection system to reveal any and all abnormal traffic being sent and received within the network. Also, never open an attachment from an email from somebody that you do not know or trust. |
| --- |

1. List your third-party references.

| https://www.webroot.com/us/en/resources/tips-articles/what-is-trojan-virus#:~:text=Never%20download%20or%20install%20software,and%20running%20on%20your%20computer |
| --- |

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