| 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?

| Management or Administrative |
| --- |

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

| Technical or Operational |
| --- |

#### Intrusion Detection and Attack Indicators

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

| IDS == Intrusion Detection System   * This is a passive system, which will provide documentation and logs for someone to review and respond to later.   IPS == Intrusion Prevention System   * Will do everything an IDS does, but also provides a level of protection by blocking perceived malicious traffic, thus preventing it from being delivered to an endpoint on the network. |
| --- |

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

| Indicator of Attack (IoA) indicates attacks that happen in real time. It is a proactive result and can let you know when something is currently happening.  Indicator of Compromise (IoC) indicates that a compromise has already happened. This is good for research to find the adversary’s techniques, tactics, and procedures (TTPs) to find the vulnerabilities that were used get inside the network. |
| --- |

#### The Cyber Kill Chain

Utilized the information on Crowdstrike to get more in depth details for the examples. <https://www.crowdstrike.com/cybersecurity-101/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 where the attacker identifies the target and starts to explore potential vulnerabilities and weaknesses of the target. Additionally, the attacker could start to harvest credentials, email addresses, physical locations, operating systems and application details. |
| --- |

1. Stage 2:

| Weaponization - This is where the attacker would find an exploit already in the wild, or create an exploit (or malware, ransomware, virus, or worm) to use against the vulnerabilities that were found during Recon. |
| --- |

1. Stage 3:

| Delivery - This is where the attacker actually launches the attack, either by using a backdoor they may have created (or found) in the previous stages, or utilizing phishing, email links/attachments, or social engineering. |
| --- |

1. Stage 4:

| Exploitation - This is where the code/malware is executed on the targets system(s) |
| --- |

1. Stage 5:

| Installation - Once the code/malware is executed, it’s installed onto the target system.  According to Crowdstrike, “This is a turning point in the attack lifecycle, as the threat actor has entered the system and can now assume control.” |
| --- |

1. Stage 6:

| Command and Control (C2) - This is where the attacker now has control of the target’s system. Additionally, the attacker can move around in the network, infecting more systems and creating more entry points. |
| --- |

1. Stage 7:

| Actions on Objectives - This is where the attacker does what they came to do, be it steal information, destroy information, or encrypt the systems (potentially for payment). |
| --- |

#### 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.

| alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"  alert: When the rule is triggered, send an alert  tcp: Apply the rule to all TCP packets  $EXTERNAL\_NET: Applies the rule to any address in the $External\_Net (source)  any: Applies the rule to any source port  ->: Direction of traffic  $HOME\_NET: Applies the rule to any address in the $Home\_Net (destination)  5800:5820: Applies the rule to ports 5800 through 5820  (msg:"ET SCAN Potential VNC Scan 5800-5820": This is the message that is printed when the alert occurs |
| --- |

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

| Reconnaissance |
| --- |

1. What kind of attack is indicated?

| 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.

| alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"  alert: When the rule is triggered, send an alert  tcp: Apply the rule to all TCP packets  $EXTERNAL\_NET: Applies the rule to any address in the $External\_Net (source)  $HTTP\_PORTS: Applies the rule to ports stored in the $HTTP\_Ports  ->: Direction of traffic  $HOME\_NET: Applies the rule to any address in the $Home\_Net (destination)  any: Applies the rule to any destination ports  (msg:"ET POLICY PE EXE or DLL Windows file download HTTP": This is the message that is printed when the alert occurs |
| --- |

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

| This question, in itself, is tricky, as it entirely depends on what you are qualifying as Layers in the Defense in Depth. You look at one source, they will tell you there are 3 layers.. Another says 5.. And another says 7. Then there is the OSI that we could look at. Or even just common sense.  In general, this violates multiple layers. Since a .exe was likely downloaded that had malicious software either as a whole or in part with it, there is the User end that you have to deal with. No one should be downloading a file that they don’t know about, and especially within a corporation. This would require some education to take place on that end users part.  Then there is the AV/Firewall that let the file through. It should have stopped it but didn’t.   What about the IDS? Did it detect something wrong with the packet?  Is the network segmented so that the infected system doesn’t compromise the entire business?  Was the system not properly updated/patched and that allowed for the exploit to come in?  Without knowing more of the circumstances (and the model you are referring to for the Defense in Depth), there are multiple answers that could be given. |
| --- |

1. What kind of attack is indicated?

| An .exe for .dll file was downloaded from a HTTP site |
| --- |

**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 ip any 4444 -> $LOCAL\_NET any (msg:"ET SCAN Traffic Detected Inbound on Port 4444" |
| --- |

### Part 2: “Drop Zone” Lab

Much of my information for this part of the homework came from either the Week 11, Day 1 student guide (<https://utsa.bootcampcontent.com/utsa-bootcamp/UTSA-VIRT-CYBER-PT-08-2022-U-LOLC/-/blob/main/Module%2011-Network-Security/1/StudentGuide.md>), or from the firewall man pages (<https://manpages.debian.org/testing/firewalld/firewall-cmd.1.en.html>).

#### Set up.

Log in 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.

| $ service 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  \*Note: this only shows you the information in the default (public) zone.  \*In order to see the currently configured rules for all zones, you would have to use the following:  $ sudo firewall-cmd --list-all-zones |
| --- |

* 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?

| Since we just added them to the various zones, they are active, but in order to verify that information, you can run:  $ sudo firewall-cmd --get-active-zones  This command will give you the active zones, and the interfaces and sources used on those zones.  Or, for complete information on all the zones, you can run:  $ sudo firewall-com --list-all-zones |
| --- |

#### 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  If you want a command for ‘future’ IP’s, I could write you a script so that when you type in “blacklist <ipaddress>”, it will add the IP the same as above.   Otherwise, I don’t really know how you can write a command for something you don’t know yet.  If this is something you would like to see, please let me know and I will get it written up for you and attach it. |
| --- |

#### 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  \*Notes: The idea, according to the man pages, is to work on and test the configuration in the runtime environment, and once you’re happy with it, then you can save the configuration to make it 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 --get-active-zones  Again, this command will give you the active zones, and the interfaces and sources used on those zones (as shown in the following image):    For complete information on all the zones, you can run:  $ sudo firewall-com --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=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 ehco 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 –info-zone=public  $ sudo firewall-cmd –info-zone=web  $ sudo firewall-cmd –info-zone=sales  $ sudo firewall-cmd –info-zone=mail  $ sudo firewall-cmd –info-zone=drop  Additionally, you could also run the following, as it will show the same information:  $ 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 (Test Access Port) |
| --- |

| SPAN (Switched Port Analyzer) |
| --- |

1. Describe how an IPS connects to a network.

| An IPS physically connects in line with the flow of data between the firewall and network switch. |
| --- |

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

| Signature-based |
| --- |

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 |
| --- |

#### Defense in Depth

As stated before, there are a slew of resources that give different layers and meanings for the Defense in Depth. For this, I’m going to utilize the following sites:

<https://learn.microsoft.com/en-us/training/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth>

and

<https://www.wallarm.com/what/defense-in-depth-concept>

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 |
| --- |

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

| Host (malware protection) / Compute |
| --- |

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

| Data (though it could be argued Application / App, depending on how they got the access) |
| --- |

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

| Host / Compute |
| --- |

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

| Internal Network / Network |
| --- |

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

| Policies, procedures, and awareness / (no associated one on the Microsoft page |
| --- |

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

| Perimeter |
| --- |

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

| HDD/SSD Encryption, or encrypting the specific sensitive files |
| --- |

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

| Utilizing encrypted connections (HTTPS, SSL, TLS, etc) |
| --- |

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

| Geo-Location |
| --- |

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

| Full Disk Encryption, Secure Boot, BIOS Password Protection |
| --- |

#### 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.

| Circuit-Level Gateway Firewall work by verifying the three-way TCP handshake.  However, there is also the Stateless Firewall, which ensures the delivery of data through a successful three-way handshake before transmitting the data.   Also, there is Stateful Firewalls, which uses a combination of the TCP handshake verification and packet inspections. |
| --- |

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 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.

| 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 (or Stateless) Firewalls |
| --- |

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

| MAC Layer Filtering Firewall |
| --- |

### Bonus 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?*)

| First IoA is that a Snort rule was activated and the activity was captured. But to go further, the specific rule that was activated was that a file was downloaded from an external http port onto an home network that contained a TROJAN JS/Nemucod.M.gen .exe payload, as indicated by the event message |
| --- |

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

| Per the resource found in SGUIL on this attack (<https://www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/>): “...the executable files downloaded by Nemucod are used to retrieve a Trojan Downloader called Fareit or Pony Downloader, which in turn downloads another set of executable files containing the Gozi infostealer…”  So, it would appear that they are trying to steal some information from the victim. |
| --- |

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? | Email campaign targeting Italian’s |
| **Weaponization** | What was downloaded? | Initially, a JavaScript file was downloaded which then started the attack. Depending on the campaign (there were 3 or 4), either an .exe or a .dll, which then in turn went and got the Trojan Downloader |
| **Delivery** | How was it downloaded? | By opening the .zip file on the email |
| **Exploitation** | What does the exploit do? | Steals information |
| **Installation** | How is the exploit installed? | The JavaScript opens a IE browser and goes to the location of the Trojan, which downloads and installs in the background. |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | Once installed, per the writer of the article, the system will start to ‘phone home’, though it may be because they were in a sandbox environment. |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? | Sends files back to the attacker |

1. What are your recommended mitigation strategies?

| First, education. Your users are always going to be your weakest point, so the more that you educate them, the better you might be.   Additionally, an IPS might have caught and prevented the file from reaching the target machine.  A good AV might also have caught the file as well. |
| --- |

1. List your third-party references.

| https://www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/ |
| --- |

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