| 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 |
| --- |

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

| Administrative control |
| --- |

3. 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?

| One is a monitoring system (IDS) and the other is a control system (IPS) |
| --- |

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

| One is detecting the attack in real time (IOA) while the other shows the intrusion after the fact (IOC) |
| --- |

The Cyber Kill Chain

Name the seven stages of the cyber kill chain, and provide a brief example of each. 1. Stage 1:

| Reconnaissance (ex:searching targets, hackers collect information about possible victims over a longer period of time by searching common platforms and normal company website) |
| --- |

2. Stage 2:

| Weaponize (ex:Prepare attacks, attackers specifically search for vulnerabilities withing the entire company through which they can then strike) |
| --- |

3. Stage 3:

| Delivery (ex: delivering the payload bundle to the target via email or web) |
| --- |

4. Stage 4:

| Exploitation (ex: activating the attackers payload on the target system |
| --- |

5. Stage 5:

| Installation (ex: installing a backdoor and maintaining persistence; installing malware) |
| --- |

6. Stage 6:

| Command and Control (ex:attacker now has permanent access and can start specific actions like establishing a connecting to CC servers to obtain further instructions, install malware or updates) |
| --- |

7. Stage 7:

| Actions on Objectives (ex:attacker has access and can encrypt documents and manipulate them.) |
| --- |

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 = the action Snort will take when triggered  Tcp = applies the rule to all TCP packets  $EXTERNAL\_NET = applies the rule to packets whose source IPs are in external network  Any = applies the rule to packets coming from any port  -> = indicated the direction of traffic, from source to destination |
| --- |

| $HOME\_NET = applies the rule to packet whose destination IPs are in the home network  5800:5820 = applies the rule to traffic whose destination port number in the range of 5800-5820  “Et Scan Potential VNC Scan 5800 - 5820” = Snort generated alert and logged the message.  This rule generates TCP alerts for inbound traffic on ports 5800 to 5820 on the external network |
| --- |

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

| Stage 1 - Reconnaissance |
| --- |

3. What kind of attack is indicated?

| Indicator of attack is emerging threat on ports 5800-5820 |
| --- |

**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 = the action Snort will take when triggered  Tcp = applies the rule to all TCP packets  $EXTERNAL\_NET = applies the rule to packets whose source IPs are in the external network  HTTP\_PORTS = applies the rule to packets coming from any HTTP ports -> = indicated the direction of traffic from source to destination |
| --- |

| $HOME\_NET = applies the rule packets whose destination IPs are in the home network  Any = applies the rule to traffic to any destination port  msg:”ET POLICY PE EXE or DLL Windows file download HTTP” = the message snort will print when it generated an alert  Snort generated an alert and logged the message “ET POLICY PE EXE or DLL Windows file download HTTP” when it detected TCP packets coming from the external network on HTTP ports going into the local network on any ports, or essentially, when a file is downloaded from an external source.  Generates a TCP alert for inbound traffic outside the external network on port 80 to all ports |
| --- |

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

| Layer 7, Application |
| --- |

3. What kind of attack is indicated?

| Indicator of attack is emerging threat for EXE or DLL file download violation. |
| --- |

**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 any –> $HOME\_NET 4444 (msg:”Traffic detected from port 4444”) |
| --- |

**Part 2: “Drop Zone” Lab**

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 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 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 firewall-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 --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>

| $sudo firewall-cmd --reload |
| --- |

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>  $ <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 --permanent --add-service=http> |
| --- |

● sales:

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

● mail:

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

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

| 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.

| $ <ADD COMMAND HERE>  $ <sudo firewall-cmd --permanent --zone=drop  --add-source=ipset:10-.208.56.23>  $ <sudo firewall-cmd --permanent --zone=drop  --add-source=ipset:135.95.103.76>  $ <sudo firewall-cmd --permanent --zone=drop  --add-source=ipset: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 --complete-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 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 --zone=public --list-all>

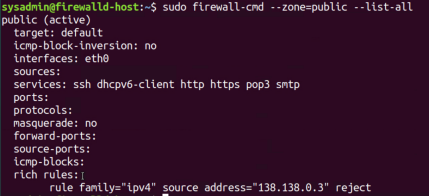
$ <sudo firewall-cmd --zone=web --list-all>

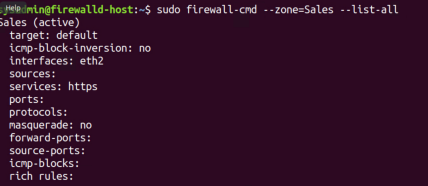
$ <sudo firewall-cmd --zone=sales --list-all>

$ <sudo firewall-cmd --zone=mail --list-all>

$ <ADD COMMAND HERE>

● 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). Network TAPs transit both inbound and outbound data streams on separate channels at the same time therefore all the data will arrive at the monitoring device in real time |
| --- |

| SPN (Switched Port Analyzer). A span sends a mirror image of all network data to another physical port where the packets can be captured and analyzed. |
| --- |

2. Describe how an IPS connects to a network.

| IPS physically connects inline with the flow of data and is typically placed in between the firewall and network switch. |
| --- |

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

| signature-based |
| --- |

4. 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

1. For each of the following scenarios, provide the layer of defense in depth that applies:

a. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.

| Perimeter/access measures |
| --- |

b. A zero-day goes undetected by antivirus software.

| Endpoint protection |
| --- |

c. A criminal successfully gains access to HR’s database.

| application |
| --- |

d. A criminal hacker exploits a vulnerability within an operating system.

| host |
| --- |

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

| network |
| --- |

f. Data is classified at the wrong classification level.

| data |
| --- |

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

| perimeter |
| --- |

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

| Encryption |
| --- |

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

| VPN |
| --- |

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

| GPS |
| --- |

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

| hard disk encryption |
| --- |

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 firewalls |
| --- |

2. 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 |
| --- |

3. 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 /application |
| --- |

4. 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?

| Stateless firewalls |
| --- |

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

| MAC layering filtering |
| --- |

**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?*)

| Downloading files that contain malware on port 80 |
| --- |

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

| Most attacks happen because the criminal wants access to sensitive information to exploit and most likely benefit from it. |
| --- |

3. 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 attacker gathers  information that might reveal  the victim?  vulnerabilities and comes up  with tactics for attack through  email. |
| **Weaponization** | What was downloaded? Zip files attached to emails |
| **Delivery** | How was it downloaded? Drive-by downloads expose users to different threats. |
| **Exploitation**  **Installation** | What does the exploit do? An exploitation is an act of taking advantage of someone  or a group of people in order  to benefit oneself.  Ransomware  How is the exploit  They find vulnerabilities in the  operating system,  installed?  applications, networks, or  hardware. |
| **Command & Control (C2)** | How does the attacker gain  A remote attack is a harmful  operation directed at one or  control of the remote  more computers. The attacker  machine?  will look for weaker areas  within the security software or  network in order to gain  access. |
| **Actions on Objectives** | What does the software  Nemucod will use files such as  WScript.Shell,  that the attacker sent do to  MSXML2.XMLHTTP and  complete its tasks?  ADODB.Stream to save an |

|  | executable file to the  temporary folder and to run it.  Nemucod will then opens a  PDF files that shows to be an  invoice is used a decoy |
| --- | --- |

4. What are your recommended mitigation strategies?

| Reduction is a way to mitigate risks in the way that tools are used to identify risks and reduce the probability of being attacked. |
| --- |

5. List your third-party references.

| https://www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-down loader/  https://www.f-secure.com/v-descs/trojan-downloader\_js\_nemucod.shtml |
| --- |

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