



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 security

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

Management security

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

Operational security

Intrusion Detection and Attack Indicators

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

IDS waits for an administrator to react to an alert, where IPS automatically takes action.

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

An IOA is an indicator of current ongoing attacks where an IOC indicates that an attack already occurred.

The Cyber Kill Chain

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

1. Stage 1:

Reconnaissance-Information gathering against targeted victims. DNS registration websites and social media websites.

2. Stage 2:

Weaponization-using reconnaissance to attack logical security controls such as passwords, IDS, and firewalls. Administrative security controls as well.

3. Stage 3:

Delivery-delivery of weaponization payload via email, website, or USB.

4. Stage 4:

Exploitation-compromising servers or applications through social engineering exploiting employees or personnel.

5. Stage 5:

Installation-malicious software installation, backdoor attacks, or backlog attacks such as cron jobs.

6. Stage 6:

Command and Control (C2)-command control such as IRC to get remote control of the victim's computer.

7. Stage 7:

Actions on objectives- access to take actions on objectives such as steal data to ransom for monetary incentives.

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.

An alert that applies to all tcp packets, that comes from any source IP address that isn't in the HOME_NET, from any port, going into the HOME_NET, and applies to portswith in the range of 5800 to 5820 in the HOME_NET. The message is referring to a VNC scan that is looking for a VNC server without password configured.

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

Reconnaissance

3. What kind of attack is indicated?

A VNC scan that is a metasploit.

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.

An alert that applies to all tcp packets, from any source IP address outside of the HOME_NET that applies to configured HTTP ports to all IP addresses protected whether private or public on any port. The message is referring to a policy that may have been violated due to the downloading of a windows executable file.

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

Delivery

3. What kind of attack is indicated?

Policy 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 any 4444 -> HOME_NET any (msg: "
```

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 ufw reset
```

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 /etc/init.d/firewalld enable  
$ sudo /etc/init.d/firewalld start
```

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 is-active 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-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 --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 --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=pop3 --add-service=smtp
--add-service=http --add-service=https --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=pop3 --add-service=smtp --permanent
```

- 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.

```
$ sudo firewall-cmd --zone=drop --add-source=10.208.56.23 --permanent  
$ sudo firewall-cmd --zone=drop --add-source=135.95.103.76 --permanent  
$ sudo firewall-cmd --zone=drop --add-source=76.34.169.118 --permanent
```

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-services
```

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' --permanent
```

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 --permanent
```

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- a hardware device that provides access to a network. Sending inbound and outbound data at the same time through different channels.

Mirrored Span port- sends a mirrored image of all network data to another physical port where packets can be captured and analyzed.

2. Describe how an IPS connects to a network.

Connects inline with the flow of data typically after the firewall.

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

Signature-based IDS

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 IDS

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.

Physical

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

Endpoint

- c. A criminal successfully gains access to HR's database.

Data

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

Application

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

Perimeter

- 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.

Network

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

Full-disk encryption

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

Transport Layer Security

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

Remote desktop software

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

Disable booting from external media under BIOS/UEFI settings.

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 firewall

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.

Packet-Filtering Firewalls(stateful)

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.

Application firewall

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?

Uncomplicated firewall(UFW)

5. 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?*)

[Enter answer here]

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

[Enter answer here]

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 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?	

4. What are your recommended mitigation strategies?

[Enter answer here]

5. List your third-party references.

[Enter answer here]