## Unit 11 Submission File: Network Security Homework

### Part 1: Review Questions

#### Security Control Types

The concept of defense in depth can be broken down into three different 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?

Answer: Preventative - Physical

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

Answer: Preventive - Administrative

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

Answer: Preventive - Technical

#### Intrusion Detection and Attack indicators

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

Answer: An IDS is a passive system that logs attacks. An IPS is an active system that does everything that an IDS can do, but can also respond to attacks.

2. What's the difference between an Indicator of Attack and an Indicator of Compromise?

Answer: Indicators of attack indicate attacks happening in real time. Indicators of compromise indicate previous malicious activity.

#### The Cyber Kill Chain

Name each of the seven stages for the Cyber Kill chain and provide a brief example of each.

1. Stage 1: Reconnaissance - The attacker gathers the necessary information during the reconnaissance step. Hackers select the victim, conduct in-depth research of the company, and look for weak points in the target network.

2. Stage 2: Weaponization - The attacker team found a weak point in the system and knows how to create an entry point. The criminal team now designs a virus or a worm to target the weakness. If attackers found a zero-day exploit, they typically work fast before the victim discovers and fixes the vulnerability.

3. Stage 3: Delivery - Criminals launch the attack into the target environment. This can often be through phishing attacks, exploiting a hardware or software flaw, compromised user accounts, a drive-by download that installs malware alongside a regular program. Direct hacking through an open port or other external access point.

The goal of this step is to breach the system and silently establish a foothold.

4. Stage 4: Installation - This is when the malware installs on the network. Once the malware installs, intruders get access to the network. Keeping their presence secret is critical for attackers. Intruders typically wipe files and metadata, overwrite data with false timestamps, and modify documents to remain undetected.

5. Stage 5: Lateral Move - Intruders move laterally to other systems and accounts on the network. The goal is to gain higher permissions and reach more data. Standard techniques during this stage are exploiting password vulnerabilities, brute force attacks, credential extraction, and/ or targeting further system vulnerabilities.

6. Stage 6: Command and Control - Complex malware requires manual interaction to operate, so attackers need keyboard access to the target environment. The last step before the execution phase is to establish a command-and-control channel (C2) with an external server. Hackers typically achieve C2 via a beacon over an external network path. Beacons are usually HTTP or HTTPS-based and appear as ordinary traffic due to falsified HTTP headers. If data exfiltration is the attack’s goal, intruders start placing target data into bundles during the C2 phase. A typical location for data bundles is a part of the network with little to no activity or traffic.

7. Stage 7: Execution - Intruders take action to fulfill the attack’s purpose. Immediately before an attack starts, intruders cover their tracks by causing chaos across the network. Some criminals also launch another DDoS attack to distract the security controls while extracting data.

#### Snort Rule Analysis

Use the Snort rule to answer the following questions:

Snort Rule #1

```bash

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 is happening.

Answer: An outside IP was looking to see if it could remotely control a computer on our Home Network ports 5800 and 5820.

2. What stage of the Cyber Kill Chain does this alert violate?

Answer: Reconnaissance

3. What kind of attack is indicated?

Answer: IOC

Snort Rule #2

```bash

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 is happening.

Answer: An external website downloaded a program that violated a Snort Policy.

2. What layer of the Defense in Depth model does this alert violate?

Answer: Application

3. What kind of attack is indicated?

Answer: Policy Violation “Exe or DLL download”

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.

Answer: alert ip any any -> any 4444 {msg: "Traffic on Port 4444 detected";}

### Part 2: "Drop Zone" Lab

#### Log into the Azure `firewalld` machine

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`.

```bash

$ sudo ufw disable

```

#### Enable and start `firewalld`

By default, these service should be running. If not, then run the following commands:

- Run the commands that enable and start `firewalld` upon boots and reboots.

```bash

$ sudo systemctl enable firewalld

$ 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 or not the `firewalld` service is up and running.

```bash

$ sudo /etc/init.d/firewalld status

```

#### List all firewall rules currently configured.

Next, lists 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 not doing double work.

- Run the command that lists all currently configured firewall rules:

```bash

$ 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 see if the service you need is available

```bash

$ sudo firewall-cmd --get-services

```

- We can see that the `Home` and `Drop` Zones are created by default.

#### Zone Views

- Run the command that lists all currently configured zones.

```bash

$ sudo firewall-cmd --list-all-zones

```

- We can see that the `Public` and `Drop` Zones are created by default. Therefore, we will need to create Zones for `Web`, `Sales`, and `Mail`.

#### Create Zones for `Web`, `Sales` and `Mail`.

- Run the commands that creates Web, Sales and Mail zones.

```bash

$ firewall-cmd --new-zone=Web --permanent

$ firewall-cmd --new-zone=Sales --permanent

$ firewall-cmd --new-zone=Mail --permanent

```

#### Set the zones to their designated interfaces:

- Run the commands that sets your `eth` interfaces to your zones.

```bash

$ sudo firewall-cmd --zone=Web --change-interface=eth1 --permanent

$ sudo firewall-cmd --zone=Sales --change-interface=eth1 --permanent

$ sudo firewall-cmd --zone=Mail --change-interface=eth1 --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:

```bash

$ firewall-cmd --zone=public --add-service=http --permanent

$ firewall-cmd --zone=public --add-service=https --permanent

$ firewall-cmd --zone=public --add-service=smtp --permanent

$ firewall-cmd --zone=public --add-service=pop3 --permanent

```

- Web:

```bash

$ firewall-cmd --zone=Web --add-service=https --permanent

```

- Sales

```bash

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

```

- Mail

```bash

$ firewall-cmd --zone=Mail --add-service=stmp --permanent

$ firewall-cmd --zone=Mail --add-service=pop3 --permanent

```

- What is the status of `http`, `https`, `smtp` and `pop3`? Open

#### Add your adversaries to the Drop Zone.

- Run the command that will add all current and any future blacklisted IPs to the Drop Zone.

```bash

$ firewall-cmd --new-ipset=blacklist --type=hash:net --option=family=inet --option=hashsize=4096 --option=maxelem=200000 --permanent

$ firewall-cmd --ipset=ipv4blacklist --add-entry=192.168.0.5 --permanent

$ firewall-cmd --zone=drop --add-source=ipset:blacklist --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 ensure that the network remains secured after unplanned outages such as power failures.

- Run the command that reloads the `firewalld` configurations and writes it to memory

```bash

$ firewall-cmd --reload

```

#### View active Zones

Now, we'll want to 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.

```bash

$ sudo firewall-cmd --list-services

```

#### Block an IP address

- Use a rich-rule that blocks the IP address `138.138.0.3`.

```bash

$ 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.

```bash

$ sudo firewall-cmd --zone=public --add-icmp-block={echo-request,echo-reply,timestamp-reply,timestamp-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.

```bash

$ 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=Zone --list-all

$ sudo firewall-cmd --zone=drop --list-all

```

- Are all of our 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, we will 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.

Answer 1: Mirror Port

Answer 2: Network Tap

2. Describe how an IPS connects to a network.

Answer: IPS physically connects inline with the flow of data. An IPS 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?

Answer: Signature-based

4. Which 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?

Answer: Anomaly-based

#### 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.

Answer: Physical

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

Answer: Application

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

Answer: Data

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

Answer: Host

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

Answer: Network

6. Data is classified at the wrong classification level.

Answer: Policy

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

Answer: Perimeter

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

Answer: Encryption Key

3. Name one method to protect data-in-transit.

Answer: TLS or VPN

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

Answer: GPS

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

Answer: Disable USB ports or a Firmware password

#### 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.

Answer: Circuit-Level Gateway Firewall

2. Which type of firewall considers the connection as a whole? Meaning, instead of looking at only individual packets, these firewalls look at whole streams of packets at one time.

Answer: Stateful Firewall

3. Which type of firewall intercepts all traffic prior to being forwarded 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?

Answer: Application or Proxy Firewalls

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?

Answer: Stateless Firewall

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

Answer: MAC Layer Filtering Firewall

### Bonus Lab: "Green Eggs & SPAM"

