## 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: Physical Security

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

Answer: Administrative Security

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

Answer: Operational Security

#### Intrusion Detection and Attack indicators

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

Answer: IDS is a monitoring while IPS is a control system, IDS does not alter the network packets in any way, IPS prevents packets from being delivered based on the contents of packet. This is similar to how a firewall prevents traffic from an IP address. False positives for IDS will only cause alerts, while false positives for IPS could cause the loss of important data or functions.

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

Answer: IOA focuses on spotting attempted attacks or reconnaissance and reducing the actors intent. IOC focuses on gathering conclusive evidence that a system has been breached, IOA is more reliable based on behaviors or contextual behaviors.

#### 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 – Gathering info on an individual in preparation for an attack.(Attackers probe for a weakness in the targets system)

2. Stage 2: Weaponization – Injecting the malicious software or installing some sort of backdoor on the intended targets machine.(Build a deliverable payload using an exploit and a backdoor)

3. Stage 3: Delivery – Attackers send a malicious payload by means of email or SMS, instant message.(Sending the weaponized bundle to the victim, malicious link in a legit looking email)

4. Stage 4: Exploit – Gaining access and compromising the user’s machine.(Executing code on the victim’s system)

5. Stage 5: Installation – Installing more malicious code such as granting your own user root access.(Installing malware on a target asset)

6. Stage 6: Command and Control – Command channel used to control another system.(Create a channel where the attacker can control a system remotely)

7. Stage 7: Actions – Accomplishing the final goal on the said target machine/system.(Attacker successfully carries out intended goal on the target)

#### 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: Alerts users of ANY inbound TCP traffic from ports 5800 to 5820 on the external network.

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

Answer: Reconnaissance (This is where the attacker probes for a weakness)

3. What kind of attack is indicated?

Answer: Potential VNC scan on ports 5800 to 5820 (Port mapping)

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: The remote host attempts to deliver a malicious payload through http ports, to any ports on the local machine. (Port 80)

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

Answer: Delivery,(Sending the weaponized bundle to the victim, malicious link in a legit looking email)this is Policies, procedures and awareness.

3. What kind of attack is indicated?

Answer: Cross site scripting(Threat for policy violation “EXE or DLL windows file 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 tcp $EXTERNAL\_NET any --> $HOME\_NET 4444 (msg: ”ET Possible Trojan or Crackdown”)

### 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 apt remove ufw**>

```

#### 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.service** >

$ < **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 systemctl status firewalld.service>

Text

Description automatically generated

```

#### 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>

Text

Description automatically generated

```

- Take note of what Zones and settings are configured. You many 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>

Text

Description automatically generated

```

- 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>

Text

Description automatically generated Text

Description automatically generated

```

- 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

$ <sudo firewall-cmd –-permanent –-new-zone=web>

$ <sudo firewall-cmd –-permanent –-new-zone=sales>

$ <sudo firewall-cmd –-permanent –-new-zone=mail>

Text

Description automatically generated Text

Description automatically generated

```

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

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

```bash

$ <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>

Text

Description automatically generated

```

#### 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

$ <sudo firewall-cmd –-permanent –-zone=public –-add-service=http>

$ <sudo firewall-cmd –-permanent –-zone=public –-add-service=https>

$ <sudo firewall-cmd –-permanent –-zone=public –-add-service=pop3>

$ <sudo firewall-cmd –-permanent –-zone=public –-add-service=smtp>

Text

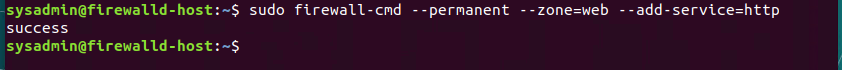
Description automatically generated

```

- Web:

```bash

$ <sudo firewall-cmd --permanent –-zone=web –-add-service=http>

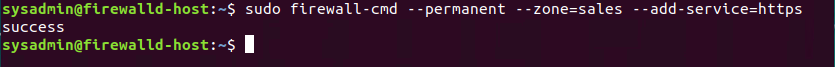


```

- Sales

```bash

$ <sudo firewall-cmd --permanent –-zone=sales –-add-service=https>



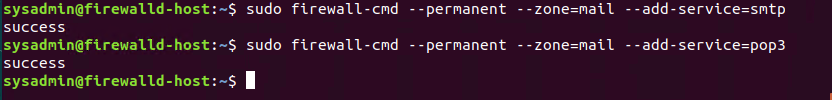
```

- Mail

```bash

$ < sudo firewall-cmd --permanent –-zone=mail –-add-service=smtp>

$ < sudo firewall-cmd --permanent –-zone=mail –-add-service=pop3>



```

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

Text

Description automatically generated

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

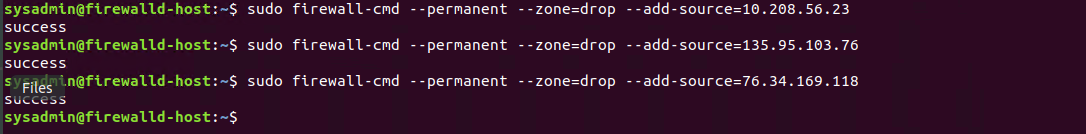
- Run the command that will add all current and any future blacklisted IPs to the Drop Zone.

```bash

$ <sudo firewall-cmd –-permanent –-zone=drop –-add-source=10.208.56.23>

$ < sudo firewall-cmd –-permanent –-zone=drop –-add-source=135.95.103.76>

$ < sudo firewall-cmd –-permanent –-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 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

$ <sudo firewall-cmd --reload>



```

#### View active Zones

Now, we'll want to provide truncated listings of all currently \*\*active\*\* zones. This a good time to verify your zone settings.

- Run the command that displays all zone services.

```bash

$ <sudo firewall-cmd –-get-active-zones>

Text

Description automatically generated

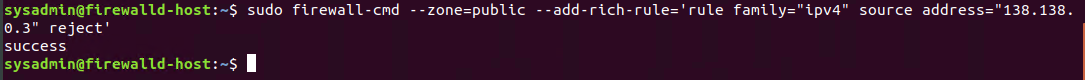
```

#### 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’>



```

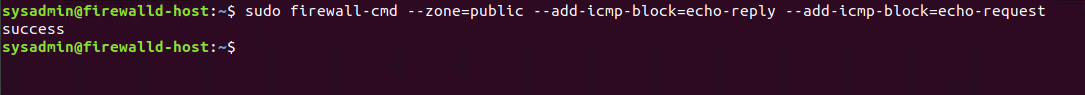
#### Block Ping/ICMP Requests

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-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.

```bash

$ <sudo firewall-cmd –-zone=public –-list-all>

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

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

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

$ < sudo firewall-cmd –-permanent –-zone=drop –-list-all>

Text

Description automatically generated Text

Description automatically generated Text

Description automatically generated

```

- 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: NIDS - Monitors traffic at network level from all devices coming in and out. It performs analysis on the traffic looking for patterns and abnormal behaviors upon which a warning is sent.

Answer 2: HIDS – Monitors the entire network for system data and looks for malicious activity on an individual host. This can take snapshots and if they change over time maliciously and alert is raised.

2. Describe how an IPS connects to a network.

Answer: An IPS usually connect to a mirror port or switch located directly behind the firewall and monitors traffic for suspicious behavior.

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

Answer: Signature-based IDS is unable to detect zero-days, this is because it compares traffic from a set of predefined lists. It lacks the functionality to filter anything outside of those domains.

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 network intrusion detection plays a vital role in protecting networks against malicious activities.

#### 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: Administrative Policy Physical Layer

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

Answer: Technical Software Application Layer

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

Answer: Technical Network Data Layer

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

Answer: Technical Software Data Layer

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

Answer: Technical Network Data Layer

6. Data is classified at the wrong classification level.

Answer: Administrative Procedures Physical Layer

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

Answer: Administrative Network Perimeter

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

Answer: Encrypting Drives

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

Answer: Data encryption

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

Answer: GPS, Geolocation, network cards and route tracing

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

Answer: Strong passwords and disk encryption you could also have a bios/uefi password policy in place

#### 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 Gateways, Stateful inspection firewalls, Proxy firewalls and next-gen firewalls

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 Inspection Firewalls (SIF)

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: 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: Packet-filtering firewalls

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

Answer: Next-gen Firewalls

### 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 Jr. 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 into the Security Onion VM and use the following \*\*Indicator of Attack\*\* to complete this portion of the homework.

Locate the following 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:

1. What was the indicator of an attack?

- Hint: What do the details of the reveal?

Answer: Trojan Downloader of JS.Nemucod which downloads and runs additional malicious onto the system.

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

Answer: Downloading malware including Teslacrypt, this is a variant of ransomware.

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 they attacker locate the victim? | Active reconnaissance – The hacker uses the system info to gain unauthorized access to protected digital or electronic materials and can even go around routers and firewalls.

| \*\*Weaponization\*\* | What was it that was downloaded?| Malware malicious software is injected into a system or network to do malicious things the owner would not want to be done.

| \*\*Delivery\*\* | How was it downloaded?| Adversary-controlled delivery, this involves directly hacking into an open port on the system.

| \*\*Exploitation\*\* | What does the exploit do?| Install malware and download additional malware from the internet which allows the attacker command execution.

| \*\*Installation\*\* | How is the exploit installed?| Through malware, ransomware and remote access trojans.

| \*\*Command & Control (C2)\*\* | How does the attacker gain control of the remote machine?| Through falsified/fake http headers that look legitimate.

| \*\*Actions on Objectives\*\* | What does the software that the attacker sent do to complete it's tasks?| Final goal could be extracting a ransom in exchange for sensitive data that has been encrypted by the attacker.

Answer: Attacker has sent a Trojan malware via HTTP port to gain access to the system, and install files to decrypt data and lock the system from providing any other access.

4. What are your recommended mitigation strategies?

Answer: Detect-determine attempts to scan or penetrate the organization. Deny-stop attacks as they happen. Disrupt data communications.

5. List your third-party references.

Answer: [IDS VS IPS](http://?), [IOA VS IOC](http://?)

[Port 5800](http://?)

---

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.