Network Security Homework Submission File

Part 1
Security Control Types

With the understanding that Defense in Depth can be broken down into three different security control types, answer the following questions:

1. Walls, bollards, fences, guard dogs, cameras, and lighting are what type of security control?

Answer: Physical

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

Answer: Administrative

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

Answer: Technical

Intrusion Detection and Attack indicators

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

Answer: An IDS is a monitoring system, while IPS is a control system. IDS doesn't alter the network packets in any way, whereas IPS prevents the packet from delivery based on the contents of the packet, much like how a firewall prevents traffic by IP address.

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

Answer: IoA indicates attacks happening in real time. IoC indicates 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 – info gathering state against targeted victim

2. Stage 2: Weaponization – establishing attack vectors and technical profiles of targets.

3. Stage 3: Delivery – delivering the weaponized payload through email, websites, USB…

4. Stage 4: Exploitation – actively compromising adversary's applications and server while avoiding physical, logical, and administrative controls.

5. Stage 5: Installation – includes malicious software installation, backdoor implants, and persisten mechanisms.

6. Stage 6: Command and Control – a command channel, typically Internet Relay Chat, used to remotely control a victim's computer

7. Stage 7: Actions on objectives – after achieving the equivalent of hands-on keyboard access to a victim's systems, adversaries can now act their objectives.

Snort Rule Analysis **NOTE: alert -> alerts and logs packet when triggered**

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: Action is alert. Applies rules to all TCP packets. All IP addresses and all ports -→ applies rule to all destination IP addresses. Applies rule to traffic to destination ports 5800 and 5820

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

Answer: Reconnaissnace

3. What kind of attack is indicated?

Answer: Unauthorized port scan

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: Action is alert. Applies rules to all TCP packets, from any source IP address, from all HTTP ports → to all destination IP addresses and applies rule to traffic to any destination port.

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

Answer: Host

4. What kind of attack is indicated?

Answer: A downloaded file was registered.

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 any 4444 -> $HOME_NET any (msg:”Traffic detected from port 4444”;)

Lab: "Drop Zone"

Log into the Azure `firewalld` machine

Log in using the following credentials:

- Username: `sysadmin`
- Password: `cybersecurity`

Uninstall `ufw`

Before you get started, it's generally best practice to ensure that you do not have any instances of `ufw` running in order to avoid conflicts with your `firewalld` service. Additionally, this 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, these service should be running. If not, then run the following commands:

- Run the commands that enables and starts `firewalld` upon boots and reboots.

```bash
$ <ADD COMMAND TO enable firewalld systemctl enable firewalld
$ <ADD COMMAND TO  start firewalld systemctl start firewalld
```

Note: This will ensure that `firewalld` service 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.

systemctl status firewalld

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:

Firewall-cmd --list-all

- 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

sudo firewall-cmd --zone --get-services

Note: that we can see 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

- 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
firewall-cmd --new-zone=Sales
firewall-cmd --new-zone=Mail
```

Set the zones to their designated interfaces:

- Run the command that sets your `eth0` interface to your zones.

```bash
firewall-cmd --zone=Web --change-interface=eth0
firewall-cmd --zone=Sales --change-interface=eth0
firewall-cmd --zone=Mail --change-interface=eth0
firewall-cmd --zone=Public --change-interface=eth0
```

```

#### 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 --zone=public --change-interface=eth0
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:

```bash
sudo firewall-cmd --zone=web --change-interface=eth1
sudo firewall-cmd --zone=web --add-service=http
sudo firewall-cmd --permanent --zone=web --add-source=201.45.34.126
```

- Sales

```bash
sudo firewall-cmd --permanent --zone=sales --add-source=201.45.15.48
sudo firewall-cmd --zone=sales --add-service=http
Sudo firewall-cmd --zone=sales --change-interface=eth2
```

- Mail

```
sudo firewall-cmd --zone=mail --add-source=pop3
sudo firewall-cmd --zone=mail --add-service=smtp
sudo firewall-cmd --zone=mail --change-interface=eth3
sudo firewall-cmd --zone=mail --add-source=201.45.105.12
```

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
1. Sudo firewall-cmd –permanent –zone=drop –add-rich-rule=”rule family= ‘ipv4’ source address=’10.208.56.73’ reject”
2. sudo firewall-cmd –permanent –zone=drop -add-rich-rule=”rule family=’ipv4’ source address=’135.95.103.76’ reject”
3. sudo firewall-cmd –permanent –zone=drop –add-rich-rule=”rule family=’ipv4’ source address=’76.34.169.118’ reject”
```

Source: access.redhat.com/discussions/1342573

```
firewall-cmd --permanent --add-rich-rule="rule family='ipv4' source address='192.168.0.11' reject"
```
```

Make rules permanent then reload them:

It's good practice to ensure that your `firewalld` installation remains nailed up and services across reboots. This ensures 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**
   **firewall-cmd --runtime-to-permanent**
    ```

View active Zones

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

- Run the command that displays all zone services.

    ```bash
    **firewall-cmd --get-active-zones**
    ```

Block an IP address

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

    ```bash
    **firewall-cmd --permanent –add-rich-rule=”rule family=’ipv4’ source address=’192.168.0.11’ reject”**
    ```

Block Ping/ICMP Requests

You've decided to 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
    **firewall-cmd --zone=public --add -icmp-block=echo-reply**
    ```

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
    **Public: firewall-cmd --list-all –zone=public**
    ```

Web: firewall-cmd --list-all -zone=web
Sales: firewall-cmd --list-all -zone=sales
Mail: firewall-cmd --list-all -zone=mail
```

- 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 2

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: Network tap (test access port)**

**Answer 2: SPAN (switched port analyzer)**

2. Describe how an IPS connects to a network.

**Answer: It physically connects inline with the flow of data. Typically placed 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

- 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: Policies, procedures, and awareness**

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

**Answer: Application**
```

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

Answer: Host

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

Answer: Application

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

Answer: Perimeter

6. Data is classified at the wrong classification level.

Answer: Data

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

Answer: Physical

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

Answer: Encrypting the hard drive

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

Answer: There are many to choose from. (HTTPS, SSL, TLS, FTPS)

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

Answer: LoJack

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

Answer: change CMOS settings

Lab: "Green Eggs & SPAM" **(According to the assignment documentation, this is a Bonus)**

In this activity, you will target spam, discover its whereabouts, and uncover the malicious deeds that the sender is intending.

- 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 producing a **Threat Intelligence Card** 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 in Sguil?
   - Hint: Do the packet details tell you anything?

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

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?
Weaponization	What was it that 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 it's tasks?

___

4. What are your recommended mitigation strategies?

5. List your third-party references.

For the final part of the homework, complete a set of review questions about firewall architecture and methodologies:

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**

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: Proxy firewall (aka 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?

Answer: Stateless firewall

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

Answer: MAC Layer Filtering firewall

GAVIN'S CORNER

Top 10 Indicators of Compromise

1. Unusual outbound network traffic
2. Anomalies in privileged user account activity
3. Geographical irregularities (for example, traffic between countries that a company doesn't do business with offers reason for pause.)
4. Other log-in red flags (log-in irregularities and failures can provide clues of network and system probing by attackers.)
5. Swells in database read volume
6. HTML Response Sizes (if attackers use SQL injection to extract data through a Web application, the request issued by them will usually have a larger HTML response size than a normal request)
7. Large number of requests for the same file
8. Mismatched port-application traffic (attackers often take advantage of obscure ports to get around more simple Web filtering techniques. So if an application is using an unusual port, it could be sign of command-and-control traffic masquerading as "normal" application behavior)
9. Suspicious registry or system file changes
10. DNS request anomalies

Source: https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647