**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 Control

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

Answer: Administrative/Management Security Controls

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

Answer: Operational/Technical Security Control

**Intrusion Detection and Attack indicators**

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

Answer: IDS operates in ‘passive/offline’ mode in a sense that it’s not actively in the path of traffic. You use port mirroring or tap to detect traffic and perform analysis. IDS can detect and alert users and log traffic. Since it’s not sitting inline, it can’t respond to attack or protect from an attack in real time. IPS is considered an ‘Active’ device. It sits inline in the path of traffic, actively monitor the traffic and based on user’s policies, it can block malicious traffic or alert the user.

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

Answer: IOA

* Is a proactive approach to intrusion attempts.
* Indicate that an attack is currently in progress but a full breach has not been determined or has not occurred yet.
* Focus on revealing the intent and end goal of the attacker regardless of the exploit or malware used in the attack.

IOC

* Reactive approach to successful intrusions.
* Indicate that an attack occurred, resulting in a breach.
* Used to establish an adversary's techniques, tactics, and procedures (TTPs).
* Expose all of the vulnerabilities used in an attack, giving network defenders the opportunity to revamp their defense as part of their mitigation strategy, and learn from an attack so it won't happen again.

**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**: In this step, the attacker / intruder chooses their target. Then they conduct an in-depth research on this target to identify its vulnerabilities that can be exploited.
2. **Stage 2: Weaponization:** In this step, the intruder creates a malware weapon like a virus, worm or such in order to exploit the vulnerabilities of the target.
3. **Stage 3: Delivery:** This step involves transmitting the weapon to the target. The intruder / attacker can employ different methods like USB drives, e-mail attachments and websites.
4. **Stage 4: Exploitation:** In this step, the malware starts the action. The program code of the malware is triggered to exploit the target’s vulnerability/vulnerabilities.
5. **Stage 5: Installation:** In this step, the malware installs an access point for the intruder / attacker. This access point is also known as the backdoor.
6. **Stage 6: Command and Control:** The malware gives the intruder / attacker access to the network/system.
7. **Stage 7: Actions on Objective:** Once the attacker / intruder gains persistent access, they finally take action to fulfill their purpose, such as encryption for ransom, data exfiltration or even data destruction.

**Snort Rule Analysis**

Use the Snort rule 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 is happening.

Answer:

Alert = action taken by snort

Tcp = protocol (tcp)

$EXTERNAL\_NET = source IP

Any= any source port (tcp)

$HOME\_NET = Destination IP

5800:5820 = destination port in the range (5800-5820)

Create an alert and logged the message “ET SCAN Potential VNC Scan 5800- 5820” when it detects TCP packets in the range specified. This is likely the result of port scanning.

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

Answer: Port scanning is active information gathering and Reconnaissance stage of Cyber Kill Chain.

1. What kind of attack is indicated?

Answer: Port Mapping, IOA.

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 is happening.

Answer: Generate an alert (with the message :"ET POLICY PE EXE or DLL Windows file download HTTP") when IP (= $EXTERNAL\_NET) is sending traffic on http port to any internal network (= $HOME\_NET) at any port. This may be because someone is downloading http file or someone pushing malicious file to a target inside “EXTERNAL\_NET”.

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

Answer: IOA, Stage 3 (Delivery) of Cyber Kill Chain

1. What kind of attack is indicated?

Answer: Application Layer, possibly Cross Site Scripting

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 4444 --> $HOME\_NET any (msg:” Inbound traffic detected on port 4444”)

**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.

$ < sudo ufw reset>

$ <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.
* $ <sudo udw enable>
* $ < 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.

$ < systemctl status firewalld.service >

$ < sudo ufw status > --🡪 Shows active or inactive

$ < sudo firewall-cmd –state > 🡪 shows running or not

**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:

$ < sudo firewall-cmd --list-all >

* Take note of what Zones and settings are configured. You many need to remove unneeded services and settings.

$ < sudo firewall-cmd --zone=public --remove-service=dhcpv6-client >

**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 --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.

$ < 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.

* $ < sudo firewall-cmd --permanent --new-zone=web >
* $ < sudo firewall-cmd --permanent --new-zone=sales >
* $ < sudo firewall-cmd --permanent --new-zone=mail >

Note: You must reload the firewall to see new zones. Command to reload the firewall.

* $ < sudo firewall-cmd –reload >

After creating Zones, verify that zones have been created. Command to verify zones have been created.

* $ < firewall-cmd --get-zones >

block dmz docker drop external home internal mail public sales trusted web work.

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

* Run the commands that sets your eth interfaces to your zones.
* $ < 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 >

**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 --permanent --add-service=http >
* $ < sudo firewall-cmd --zone=public --permanent --add-service=https >
* $ < sudo firewall-cmd --zone=public --permanent --add-service=pop3 >

$ < sudo firewall-cmd --zone=public --permanent --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?

**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 --permanent --zone=drop --add-source=ipset:10.208.56 >
* $ < 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 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.

$ < sudo firewall-cmd --runtime-to-permanent > 🡪 Make setting permanent before reloading

$ < 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.

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

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

**Block an IP address**

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

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

$ < sudo firewall-cmd --zone=public --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: It can be deployed using port mirroring. It ca

Answer 2: It can be deployed using TAPS.

It can be deployed as HIDS or NIDS.

1. Describe how an IPS connects to a network.

Answer: IPS is deployed inline of traffic path. It performs inspection and can take actions in real time.

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

Answer: Book answer is Signature Based IDS however, in real life it’s not true.

1. 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 Access/ Perimeter Security

* 1. A zero-day goes undetected by antivirus software.

Answer: End Point Security

* 1. A criminal successfully gains access to HR’s database.

Answer: Application Security

* 1. A criminal hacker exploits a vulnerability within an operating system.

Answer: End Point / Host Protection

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

Answer: Network Protection

* 1. Data is classified at the wrong classification level.

Answer: Administrative Protection / Human Firewall

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

Answer: Network

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

Answer: Encryption

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

Answer: Encryption e.g., VPN

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

Answer: LoJack, Location Based Services, Laptop Jack (and many others)

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

Answer: Disk Encryption, Firmware Boot Password and DLP

**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: Stateful Firewalls

1. 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: Circuit Level Firewalls

1. 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

1. 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

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

Answer: MAC Layer Filtering Firewall