**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/Tangible controls**

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

Answer: **Situational/business controlls**

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

Answer: **Online/intangible controls**

**Intrusion Detection and Attack indicators**

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

Answer: **IDS monitors a network, while IPS works to prevent packets based on the contents of the packet.**

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

Answer: **IoA focuses towards the intent where as IoC is how the attacks are happening.**

**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: Recon – Monitoring the system and gathering informaiton**
2. **Stage 2: Weaponization – creating a plan and how to execute**
3. **Stage 3: Delivery – attack on source**
4. **Stage 4: Exploit – the attack is successful**
5. **Stage 5: Install – malware is administered onto the system**
6. **Stage 6: Command/Control – successful login from hacker/s and ability to move across the system**
7. **Stage 7: Action – Complete the task set out to do.**

**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: **External tcp alert to the home network ports 5800:5820**

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

Answer: **Recon**

1. What kind of attack is indicated?

Answer: **Port checking attack**

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: **External TCP alert to the home network. Packet was sent attempting to be downloaded**

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

Answer: **applications**

1. What kind of attack is indicated?

Answer: **malware**

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:”DETECTED\_TRAFFIC”)**

**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.

$ <ADD COMMAND HERE>

**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.
* $ <ADD COMMAND TO enable firewalld HERE>

$ <ADD COMMAND TO start firewalld HERE>

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.

$ <ADD COMMAND HERE>

**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:

$ <ADD COMMAND HERE>

* 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

$ <ADD COMMAND HERE>

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

**Zone Views**

* Run the command that lists all currently configured zones.

$ <ADD COMMAND HERE>

* 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.
* $ <ADD COMMAND HERE>
* $ <ADD COMMAND HERE>

$ <ADD COMMAND HERE>

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

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

$ <ADD COMMAND HERE>

**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:
* $ <ADD COMMAND HERE>
* $ <ADD COMMAND HERE>
* $ <ADD COMMAND HERE>

$ <ADD COMMAND HERE>

* Web:

$ <ADD COMMAND HERE>

* Sales

$ <ADD COMMAND HERE>

* Mail
* $ <ADD COMMAND HERE>

$ <ADD COMMAND HERE>

* 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.
* $ <ADD COMMAND HERE>
* $ <ADD COMMAND HERE>

$ <ADD COMMAND HERE>

**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

$ <ADD COMMAND HERE>

**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.

$ <ADD COMMAND HERE>

**Block an IP address**

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

$ <ADD COMMAND HERE>

**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.

$ <ADD COMMAND HERE>

**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.
* $ <ADD COMMAND HERE>
* $ <ADD COMMAND HERE>
* $ <ADD COMMAND HERE>
* $ <ADD COMMAND HERE>

$ <ADD COMMAND HERE>

* 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: **Network Tap – transmits the data onto different channels**.

Answer 2: **SPAN – mirrors network onto another port**

1. Describe how an IPS connects to a network.

Answer: **IPS connects to the data flow and monitors for packets which it can check and not send through**.

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

Answer: **Signature IDS**

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 IDS**

**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: **policies and procedures**

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

Answer: **applications**

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

Answer: **data**

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

Answer: **applications**

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

Answer: **hosts**

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

Answer: **policies and procedures**

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

Answer: **applications**

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: **VPN**

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

Answer: **GPS tracking**

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

Answer: **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 Gateway 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: **Stateful 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 or** **Application 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: **Stateless Firewalls**

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

Answer: **MAC Layer Filtering 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:

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

Answer:

1. 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? |  |

Answer:

1. What are your recommended mitigation strategies?

Answer:

1. List your third-party references.

Answer: