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**

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: **IDS: Intrusion Detection Systems is passive and only detects, Intrusion Prevention Systems are active and detects along with preventing intrusions or prevents attacks**

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

   Answer: **An IOA is an alert message that is sent to an analysts console in the form of a Snort rule that detects malicious traffic that matches a signature. Happens in real time, currently in progress but a full breach has not been determined, focus on revealing the intent and end goal of an attacker regardless of exploit or malware used. An IOC tells that an attack has occurred and resulted in a breach. Was used to establish adversary's techniques, tactics, and procedures. Exposes all the vulnerabilities used in an attack, giving network defenders an opportunity to revamp the defenses(I swear that was what that floating droid says on Hoth, sry, lol)**

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 - finding intel or any info on the objective for an example DNS registration websites, facebook, twitter, etc**

2. Stage 2: **Weaponization - able to change code or hacking tools based on requirements to infiltrate objective, establishing attack vectors and profiles based on Reconnaissance**

3. Stage 3: **Delivery - the method of which the attack is carried out EX. Phishing email**

4. Stage 4: **Exploitation - a type of possible convincing or extortion that the hacker may use against the target or victim, actively compromising the applications to servers, done through social engineering**

5. Stage 5: **Installation - when a virus or malware is install / implemented on a network or system, the persistence of keeping a foothold in a computer while being stealthy and keep from being discovered**

6. Stage 6: **Command & Control - once malware or virus infiltrates a system then it will phone home to the attacker and wait to be commanded on what to do next, a command channel IRC, remote control of a victim's computer, botnet**

7. Stage 7: **Action on Objectives - attacker extracts desired intel or info from the network or system, because they have complete access**

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: **It generating an alert of inbound traffic of attempted Recon coming from outside the LAN, the ET scan is scanning their ports, took 60 seconds and there is a referenced url about the attack that can be explored for further information,**

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

   Answer: **Stage 1 Recon because they were scanning through ports and did not hack directly into the system yet, it also says classtype: attempted-recon**

3. What kind of attack is indicated?

Answer: **port sniffing, the emerging threat of the ET SCAN Potential VNC Scan 5800-5820**

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_NET went through port 80 (http) to download a DLL Windows file or corrupted update file and there is a referenced url about the attack that can be explored for further information, generated from anywhere on the LAN**

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

   Answer: **Policies, Procedures, and Awareness**

3. What kind of attack is indicated?

   Answer:**this would indicate the .EXE file or the DLL windows file that was downloaded and has an emerging threat, a supply chain attack or a corrupted update injected with 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:"ET POLICY Trojan possible")**

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 disable** and then checked with **sudo ufw status** “status: inactive”

```
sysadmin@firewalld-host:~$ sudo ufw disable
Firewall stopped and disabled on system startup
sysadmin@firewalld-host:~$ sudo ufw status
Status: inactive
```

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 /etc/init.d/firewalld start**

-
```
sysadmin@firewalld-host:~$ sudo /etc/init.d/firewalld start
[ ok ] Starting firewalld (via systemctl): firewalld.service.
sysadmin@firewalld-host:~$ sudo firewall-cmd --state
running
sysadmin@firewalld-host:~$
```

  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**

```
sysadmin@firewalld-host:~$ systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled
   Active: active (running) since Tue 2021-02-16 11:28:38 EST; 36min ago
     Docs: man:firewalld(1)
 Main PID: 922 (firewalld)
    Tasks: 2 (limit: 4648)
   CGroup: /system.slice/firewalld.service
           └─922 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid
```

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**

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- 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 --get-services**

```
sysadmin@firewalld-host:~$ firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp bitcoin bitcoin-rp
c bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp d
hcpv6 dhcpv6-client dns docker-registry docker-swarm dropbox-lansync elasticsearch freeip
a-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client ganglia-master
git high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target ka
dmin kerberos kibana klogin kpasswd kprop kshell ldap ldaps libvirt libvirt-tls managesie
ve mdns minidlna mosh mountd ms-wbt mssql murmur mysql nfs nfs3 nrpe ntp openvpn ovirt-im
ageio ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s pos
tgresql privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh
rsyncd samba samba-client sane sip sips smtp smtp-submission smtps snmp snmptrap spideroa
k-lansync squid ssh synergy syslog syslog-tls telnet tftp tftp-client tinc tor-socks tran
smission-client vdsm vnc-server wbem-https xmpp-bosh xmpp-client xmpp-local xmpp-server z
abbix-agent zabbix-server
```

- 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**

```
sysadmin@firewalld-host:~$ firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
```

- 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,sales,mail>

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=Web
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=Sales
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=Mail
success
```

  Then… **sudo firewall-cmd --relaod** and **firewall-cmd --list-all-zones** to verify

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --reload
success
sysadmin@firewalld-host:~$ firewall-cmd --list-all-zones
Mail
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


Sales
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


Web
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
```

Set the zones to their designated interfaces:
Run the commands that sets your eth interfaces to your zones.

- **sudo firewall-cmd --zones=** < … > **--change-interface=eth** 1,2,3

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Web --change-interface=eth1
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Sales --change-interface=eth2
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Mail --change-interface=eth3
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --reload
success
```

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:

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=http
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=https
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=pop3
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=smtp
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --reload
success
```

- Web, Sales, Mail commands: **sudo firewall-cmd --permanent --zone= <...> --add-service=<...>** and then reload

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=Web --add-service=http
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=Sales --add-service=https

success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=Mail --add-service=smtp
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=Mail --add-service=pop3
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --reload
success
```

- What is the status of http, https, smtp and pop3? **They are assigned to their proper zones as well as the public zone**

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 --zone=drop --add-rich-rule='rule family="ipv4" source address="<...>" reject' --permanent** and then reload

-
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" sou
rce address="10.208.56.23" reject' --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" sou
rce address="135.95.103.76" reject' --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" sou
rce address="76.34.169.118" reject' --permanent
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --reload
success
```

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 --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.

  $ **sudo firewall-cmd --get-active-zones**

Block an IP address

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

  $**sudo firewall-cmd --permanent --zone=public --add-rich-rule=’rule family=”ipv4” source address=”138.138.0.3” reject’** and then reload

Block Ping/ICMP Requests

Harden your network against ping scans by blocking icmp echo 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=Web --list-all**
- **sudo firewall-cmd --zone=Sales --list-all**
- **sudo firewall-cmd --zone=Mail --list-all**
- **sudo firewall-cmd --permanent --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: **HIDS host-based Intrusion Detection runs locally on a host-based system or users workstation or server, a network tap, port mirroring**

   Answer 2: **NIDS Network Intrusion Detection filters an entire subnet on a network**
2. Describe how an IPS connects to a network.

   Answer: **IPS connects inline with the flow of data, typically 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 IDS

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-base 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: **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, procedures and awareness**

    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: **password locked, bitlocker with encryption**

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

    Answer: **Using an encrypted connection like HTTPS, SSL, TLS, FTPS, VPN**

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

   Answer: **GPS Tracker or enabled devices**

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

   Answer: **Huge password with alot of special characters, 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 proxy or gateway verifies TCP handshake, OSI layer 4**

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, Rather than look at individual packets, stateful firewalls examine connection as whole, looking at streams of packets**

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, They intercept all traffic on its way to its final destination, without data source knowing**

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 these firewalls statically evaluate the contents of packs and do not keep track of the state of a network connection**

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

Answer: **MAC layer firewalls operate on layer 2 and filter based on source and destination**

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?
   A downloadable executable file that produces a PDF to look like an actual invoice but has several layers that steal info, even after a restart
   - Hint: What do the details of the reveal?

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

   Answer: **theft of private data from financial institutions**

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? Through email	
Weaponization	What was it that was downloaded? Corrupted Javascript that performed executibles in the background to access information on the system	
Delivery	How was it downloaded? Through a email and was installed in the TMP folder while a decoy PDF showed on display	**Spam email**
Exploitation	What does the exploit do? Copy and send back system	**Will use**

	information to the host	**3 different EXE's,**
Installation	How is the exploit installed? Downloaded through an email pdf attachment	**Java file downloads in the background and downloads a DLL**
Command & Control (C2)	How does the attacker gain control of the remote machine? Whatever sensitive information that is on the machine	**Use Gozi**
Actions on Objectives	What does the software that the attacker sent do to complete it's tasks? Sends found information back to the attacker's machine	

Answer:

4. What are your recommended mitigation strategies?
   Dont open bad emails, employee training with security layers
   Answer: **check the Raw email date before downloading attachments or have the download file scanned before opening and saving**

5. List your third-party references.

   Answer: **google, which was less than helpful, and i clicked on the blue link in squil which took me to certego.net, also checked virus total, and secureworks.com**