### **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: Management 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 passive system that logs and documents info from attacks, IPS does everything an IDS does, but it can also respond to attacks.
2. What's the difference between an Indicator of Attack and an Indicator of Compromise?  
   Answer: Indicator of attack indicates an attack that happens in real time, Indicator of Compromise indicates a previous malicious attack.

#### **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 - harvesting email addresses
2. Stage 2: Weaponization - Coupling Exploint with backdoor into deliverable payload
3. Stage 3: Delivery: Delivering weaponized bundle to the victim via some form of access
4. Stage 4: Exploitation: Exploiting a vulnerability to execute code on the victim’s system
5. Stage 5: Installation: Installing malware on the asset
6. Stage 6: Command & Control: Command channel for remote manipulation of the victim
7. Stage 7: Actions on Objectives: With “Hands on Keyboard” access, intruders accomplish their goals.

#### **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 is catching an attempted recon from a url and flagging it
2. What stage of the Cyber Kill Chain does this alert violate?  
   Answer: Reconnaissance
3. What kind of attack is indicated?  
   Answer: Attempted Recon

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: It's catching a policy violation on a url and flagging it.
2. What layer of the Defense in Depth model does this alert violate?  
   Answer: Application
3. What kind of attack is indicated?  
   Answer: Policy Violation

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 any 4444 -> any (msg:”Traffic on port 4444 detected”;sid:2000019)

### 

### **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 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.  
$sudo systemctl enable firewalld

* $ sudo systemctl start firewalld  
  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.  
  $ sudo firewall-cmd –state

#### **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 may 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
* 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 –new-zone=web –permanent

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

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

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

Run the commands that sets your eth interfaces to your zones.  
$ sudo firewall-cmd –zone=web –change-interface=eth0

$ sudo firewall-cmd –zone=sales –change-interface=eth0

$sudo firewall-cmd –zone=mail –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:  
$ sudo firewall-cmd --zone=public --add-service=http

$ sudo firewall-cmd --zone=public --add-service=https

$ sudo firewall-cmd --zone=public --add-service=smtp

$ sudo firewall-cmd --zone=public --add-service=pop3

Web:  
$ sudo firewall-cmd --zone=web --add-service=http

Sales  
$ sudo firewall-cmd --zone=sales --add-service=https

Mail  
$ sudo firewall-cmd --zone=mail --add-service=smtp

$ sudo firewall-cmd --zone=mail --add-service=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 –zone=drop –add-rich-rule=”rule blacklist reject”

#### **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 is a good time to verify your zone settings.

* Run the command that displays all zone services.  
  $ 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=drop –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 echo replies.

* Run the command that blocks pings and icmp requests in your public zone.  
  $ sudo firewall-cmd –zone=drop –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 –list-all –zone=public

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

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

$ sudo 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 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: a hardware device that provides access to a network.

Answer 2: SPAN: a mirror image of all network data to another physical port, where the packets can be captured and analyzed.

1. Describe how an IPS connects to a network.  
   Answer: Connects inline with the flow of data, typically between the firewall and network switch.
2. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?  
   Answer: Signature-Based IDS
3. 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 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: Technical
   3. A criminal successfully gains access to HR’s database.  
      Answer: Technical
   4. A criminal hacker exploits a vulnerability within an operating system.  
      Answer: Technical
   5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.  
      Answer: Technical
   6. Data is classified at the wrong classification level.  
      Answer: Administrative
   7. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.  
      Answer: Technical
2. Name one method of protecting data-at-rest from being readable on hard drive.  
   Answer: Encrypting the hard drive.
3. Name one method to protect data-in-transit.  
   Answer: Encrypt data Prior to moving it from the device.
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.  
   Answer: Something that lets you track the MAC address of the device in real time, similar to a GPS.
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?  
   Answer: Hard Disk Encryption is one way. Making sure to use a good password to login to the computer is another way.

#### **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 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: Packet Filtering (Stateful) firewall

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: Application Gateway Firewall

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(Stateless)

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

Answer: MAC Firewall