### **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 controls
2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?  
     
    Answer: administrative controls
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?  
     
    Answer: technical controls

#### **Intrusion Detection and Attack indicators**

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

Answer: Both can detect an intrusion, but and IPS also moves to protect and respond. IDS are passive, they do not respond to attacks, they only log and document information for future analysis while Intrusion Prevention System (IPS) can do everything an IDS can but can also respond to attacks.

2. What's the difference between an Indicator of Attack and an Indicator of Compromise?  
  
 Answer: IOC will indicate that an attack occurred, but and IOA alerts in real time. Indicators of attack indicate attacks happening in real time while Indicators of compromise indicate 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 (information gathering on LinkedIn, harvesting of email accounts)
2. Stage 2: Weaponization (finding a weak point to infiltrate, coupling an exploit with a backdoor)
3. Stage 3: Delivery (sending a virus via email or web)
4. Stage 4: Exploitation (phishing email link clicked, exploit a vulnerability to execute code)
5. Stage 5: Installation (virus installs malware, establishes presence)
6. Stage 6: Command and Control (hacker using root on a infiltrated system, command channel for remote manipulation)
7. Stage 7: Actions on Objectives (exfiltration of data, access for intruder to accomplish goal)

#### **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 from an external TCP packet sent to the internal home network on ports 5800-5820
2. What stage of the Cyber Kill Chain does this alert violate?  
     
    Answer: Stage 4, Exploitation
3. What kind of attack is indicated?
4. Answer: Scanning for open VNC server to gain access to system via VNC or Indicator of 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: Alert on external TCP packet sent from an HTTP port to the home network
2. What layer of the Defense in Depth model does this alert violate?  
     
    Answer: Application

3. What kind of attack is indicated?  
  
 Answer: Potential virus hidden as windows update or DLL or Indicator of Compromise

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:”APP-DETECT I2P 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.  
    
   $ sudo apt-get 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 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:  
    
   $ sudo firewall-cmd --list-all-zones
* 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
* 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 --get-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

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

Run the command that sets your eth0 interface 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 --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:  
    
   $ 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

* What is the status of http, https, smtp and pop3?
* active

#### **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-source=10.208.56.23

$ sudo firewall-cmd --zone=drop --add-source=135.95.103.76

$ sudo firewall-cmd --zone=drop --add-source=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

#### **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 --add-rich-rule=’rule family=”ipv4” source address=”138.138.0.3” drop’

#### **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 -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.  
  
$ 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 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:Network tap - transmits both inbound and outbound traffic on separate channels  
     
    Answer 2: SPAN - mirrors all network traffic to another physical port
2. Describe how an IPS connects to a network.  
     
    Answer: connects inline with the flow of data
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-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: Polices and Procedures
   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: Policies and Procedures
   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: encryption
3. Name one method to protect data-in-transit.  
     
    Answer: VPN
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.  
     
    Answer: GPS tracking
5. 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-Level Gateway Firewall

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 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 or Proxy 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: Stateless Firewall

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

Answer: MAC Layer Filtering Firewall

### 

### **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:

Alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:”ET TROJAN JS/Nemucod.M.gen downloading EXE payload”

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

The attacker to install malware to encrypt data that is stored on the targeted user’s computer then harvest personal information such as passwords or demand ransoms in exchange for the decryption tool.

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?  Harvesting of email accounts and sent a spam email. |  |
| **Weaponization** | What was it that was downloaded?  A zip file containing a JavaScript file. |  |
| **Delivery** | How was it downloaded?  It was downloaded via email attachment. |  |
| **Exploitation** | What does the exploit do?  JS/Nemucod is a JavaScript downloader trojan that targets users through malware spam campaigns. JS/Nemucod downloads additional malware and executes it without the user’s consent. It also opens a PDF document as a decoy to let the victim believe they're actually viewing a real invoice. |  |
| **Installation** | How is the exploit installed?  Upon opening the attached .zip file, and double-clicking the JavaScript file inside it, the default browser opens and executes the JavaScript which downloads other malware. |  |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine?  The malware will access and obtain your personal information and passwords found on the victim’s computer. |  |
| **Actions on Objectives** | What does the software that the attacker sent do to complete it's tasks?  The malware will send the obtained personal information back to the attacker or the malware will encrypt the data stored on the victim’s computer and will demand ransoms in exchange for a decryption tool. |  |

4. What are your recommended mitigation strategies?   
  
 Answer:

---- Be wary of emails with JavaScript attachments. It is uncommon and quite suspicious for people to send legitimate applications in pure JavaScript file format (files with .js or .jse extension) via email. Do not click or open it.

----- I recommended office 365 Advanced Threat Protection. It has a machine learning capability to help your network administrators block dangerous email threats. See the Overview of Advanced Threat Protection in Exchange: new tools to stop unknown attacks, for details.

---- Keep your software up-to-date to mitigate possible software exploits.

---- Ensure that a strong password policy is implemented throughout the enterprise

---- Secure your code integrity with Device Guard for Windows 10 Enterprise.

* + 5. List your third-party references.  
      
     Answer: ---<https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/91000/KB91905/en_US/McAfee_Labs_Threat_Advisory_JS-Nemucod.pdf>
  + <https://www.f-secure.com/v-descs/trojan-downloader_js_nemucod.shtml>
  + <https://www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/>