### **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: These are all examples of a physical control type
2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control? Are a type of Administrative security control and their function  
   Answer: Are a type of Administrative control
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?  
   Answer: these are all examples of a technical control type

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

1. What's the difference between an IDS and an IPS?  
   Answer: The Subtle difference between the two are; An intrusion detection system IDS: Has a human element that is required for deciphering The output of data. In an Intrusion prevention system that human element has been automated to read and take preventative action against attacks.
2. What's the difference between an Indicator of Attack and an Indicator of Compromise?  
   Answer:Indicators of attack are preventative measures in identifying the motivations behind threat actors regardless of the malicious exploit used. Indicators of Compromise: post attack makes available evidence of possible threat actors on a local network or host machine.

#### **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: This can happen both online and offline in the corporate setting or in a militarized operation. For purposes of gathering Intelligence on an employee or specific target.
2. Stage 2: Weaponization Stage 2 allows companies to prepare and communicate with staff preemptively in order to mitigate potential risks.
3. Stage 3: Delivery This refers to the method in how a potential threat or attack is carried out
4. Stage 4: Exploitation attacking known vulnerabilities to gain access to a target machine.
5. Stage 5: Installation at this step Malware has been installed onto a system allowing threat actors to gain complete control.
6. Stage 6: Command & Control at this phase of the kill chain access has been granted privilege escalated with the control of a users machine being relinquished to a threat actor
7. Stage 7: Actions on objective The final phase of the kill chain is when a threat actor is able to achieve their desired outcome of stealing PII or any other valuable data from a targeted user.

#### **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: The sort rule header alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5800:5820 is asking snort to alert for any tcp protocols outside of the home network coming inbound to the home or host IP using ports 5800:5820.
2. What stage of the Cyber Kill Chain does this alert violate?  
   Answer: Reconnaissance
3. What kind of attack is indicated?  
   Answer: VNC scan

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: the snort rule header alert tcp “$EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any” is asking snort to alert for any Tcp traffic externally specifying http port incoming to the home or host network
2. What layer of the Defense in Depth model does this alert violate?  
   Answer: Administrative
3. What kind of attack is indicated?  
   Answer: "ET POLICY PE EXE or DLL Windows file download HTTP"

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 ip $EXTERNAL\_NET 4444 -> $HOME\_NET (msg:”EXCELSIOR! Network traffic inbound!”; sid:1000001; rev;1)

### **Part 2: "Drop Zone" Lab**

#### **Log into the Azure firewalld machine**

Log in using the following credentials:

* Username: sysadmin
* Password: cybersecurity

In this lab exercise, you will assume the role of a Jr. Security Administrator at an indoor skydiving company called Drop Zone.

* Your company hosts a web server that takes online reservations and credit card payments. As a result, your company must comply with PCI/DSS regulations which requires businesses who take online credit card payments to have a firewall in place to protect personally identifiable information (PII).
* Your network has been under attack from the following three IPs: 10.208.56.23, 135.95.103.76, and 76.34.169.118. You have decided to add these IPs to the drop zone within your firewall.
* The first requirement of PCI/DSS regulations is to protect your system with firewalls. "Properly configured firewalls protect your card data environment. Firewalls restrict incoming and outgoing network traffic through rules and criteria configured by your organization." [PCI DSS Quick Reference Guide](https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf)

**Public Zone**

* Services: HTTP, HTTPS, POP3, SMTP
* Interface: ETH0

**Web Zone**

* Source IP: 201.45.34.126
* Services: HTTP
* Interface: ETH1

**Sales Zone**

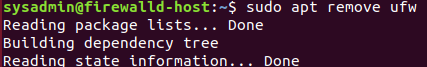
* Source IP: 201.45.15.48
* Services: HTTPS
* Interface: ETH2

**Mail Zone**

* Source IP: 201.45.105.12
* Services: SMTP, POP3
* Interface: ETH3

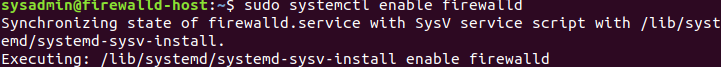
#### **Uninstall ufw**

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.  
  $ 

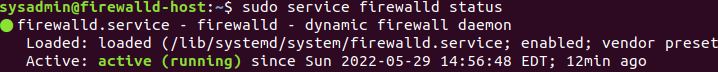
#### **Enable and start firewalld**

By default, these services should be running. If not, then run the following commands:

Run the commands that enable and start firewalld upon boots and reboots.  
$ <

* $ <>  
  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.  
  $ <>

#### **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:  
  $ <>
* 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  
  $ s>
* We can see that the Home and Drop Zones are created by default.

#### **Zone Views**

* Run the command that lists all currently configured 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 create Web, Sales and Mail zones.  
$ <>

$ <>

$ <>

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

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

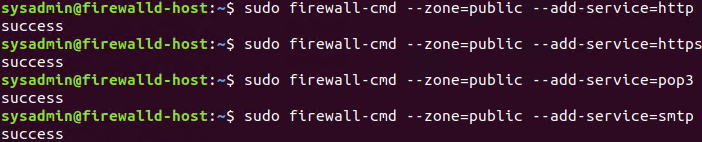
$ <>

$ <>

>

#### **Add services to the active zones:**

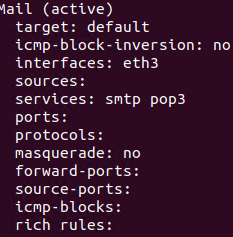
* Run the commands that add services to the **public** zone, the **web** zone, the **sales** zone, and the **mail** zone.

Public:  
$ <

* Web:  
  $ <>
* Sales  
  $ <>

Mail  
$ <>

* $ < >
* What is the status of http, https, smtp and pop3?



Currently active is smtp and pop3 inactive is http and https

#### **Add your adversaries to the Drop Zone.**

Run the command that will add all current and any future blacklisted IPs to the Drop Zone.  
$ <>





#### **Make rules permanent then reload them:**

It's good practice to ensure that your firewall installation remains nailed up and retains its services across reboots. This ensures 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  
  $ <

#### **View active Zones**

Now, we'll want to provide truncated listings of all currently **active** zones. This is to verify your zone settings.

* Run the command that displays all zone services.  
  $ <>

#### **Block an IP address**

* Use a rich-rule that blocks the IP address 138.138.0.3 in the public zone.  
  $ <=>

#### **Block Ping/ICMP Requests**

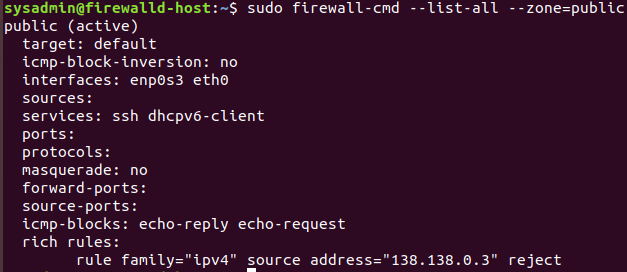
Harden your network against ping scans by blocking icmp echo replies.

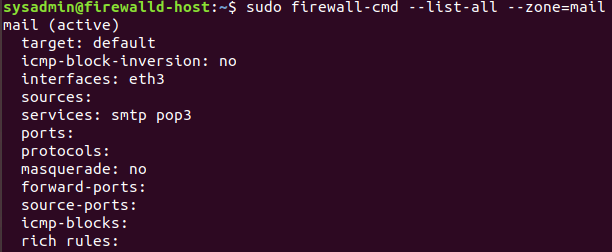
* Run the command that blocks pings and icmp requests in your public zone.  
  $ <>

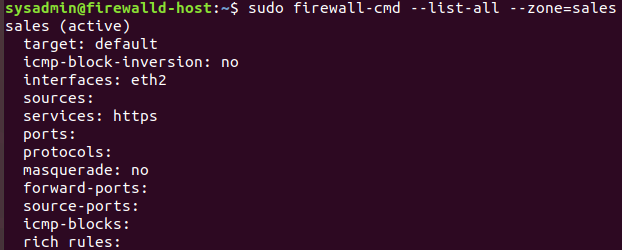


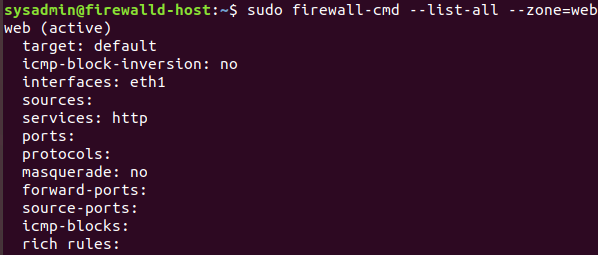
#### **Rule Check**

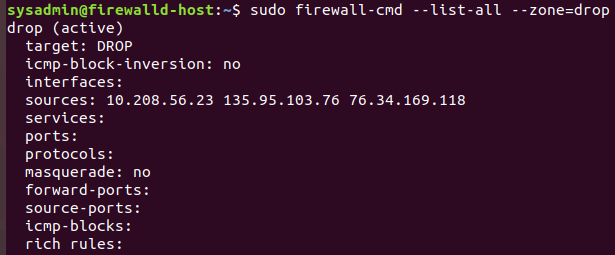
Now that you've set up your brand new firewalld installation, it's time to verify that all of the settings have taken effect.

Run the command that lists all of the rule settings. Do one command at a time for each zone.  
$ <>

$ >

$ <>

$ <>

* $ <>
* 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 Test Access Port is a physical device that creates a copy of network traffic.   
   Answer 2: switched port analyzer is a resolute port on a switch that utilizes a copy of data from the network that will be sent to a target
2. Describe how an IPS connects to a network.  
   Answer: IPS connects in the direct data path of the Host and Client
3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?  
   Answer: signature based Intrusion detection system where a specific pattern of malware or other malicious attack is noticed within the network activity followed by an analysis of the data.
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 when a contrast is made between patterns against well known references

#### **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: perimeter layer
   2. A zero-day goes undetected by antivirus software.  
      Answer: application
   3. A criminal successfully gains access to HR’s database.  
      Answer: data layer
   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 Layer
   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: perimeter
2. Name one method of protecting data-at-rest from being readable on hard drive.  
   Answer: using AES-256 encryption
3. Name one method to protect data-in-transit.  
   Answer: using TLS or transport layer security
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.  
   Answer: Geo locating the stolen laptop
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?  
   Answer: password protecting the bios, or 2 factor authentication

#### **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 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, do these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it?

Answer: 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: Packet filtering

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

Answer: MAC Layer 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?
2. Answer:
3. What was the adversarial motivation (purpose of attack)?  
   Answer:
4. 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 the 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:
2. List your third-party references.  
   Answer:

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.