## **Unit 11 Submission File: Network Security Homework**

### **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 System) - are passive and they don’t respond to attacks, they log and document information for future analysis
   1. IPS (Intrusion Prevention System) - are the same as IDS but they ALSO respond to attacks.
2. What's the difference between an Indicator of Attack and an Indicator of Compromise?  
     
    Answer: Indicator of Attack - proactive approach and indicates attacks happening in real time. Focuses on revealing the intent and the end goal of an attacker, regardless of the exploit or malware used in the attack.
   1. Indicator of Compromise - reactive approach stating that an attack already happened, and exposes vulnerabilities used in an attack, giving the network defenders the opportunity to rebuild their defenses

#### **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: Action Snort will take when triggered, it applies to all TCP packets, applies any External Network, applies to any port, OUR Home network will then move the traffic to port 5800:5820
2. What stage of the Cyber Kill Chain does this alert violate?  
     
    Answer: Reconnaissance
3. What kind of attack is indicated?  
     
    Answer: ET Scan and Potential 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: Snort Action will take place and will apply to all TCP packets, applies to the External network and applies to all HTTP ports (Port 80), Destination Home Network, and applies to any Ports.
2. What layer of the Defense in Depth model does this alert violate?  
     
    Answer: Application
3. What kind of attack is indicated?  
     
    Answer: The attacker is trying to download an executable file that will have connections with Windows properties to help the attacker succeed. 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 tcp $EXTERNAL\_NET 4444 -> $HOME\_NET any ( msg:"Incoming tcp connection, may allow remote access"; flags:S; sid:10001)

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

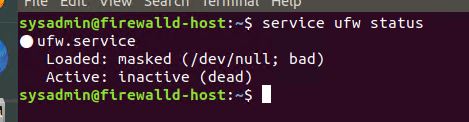
#### **Log into the Azure firewalld machine**

Log in using the following credentials:

* Username: sysadmin
* Password: cybersecurity

#### **Uninstall ufw**

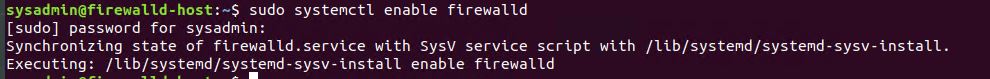
Before getting started, you should verify that you do not have any instances of ufw running. This will avoid conflicts with your firewalld service. This also ensures that firewalld will be your default firewall.

* Run the command that removes any running instance of ufw.  
    
   $ <service ufw status>  
  

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

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

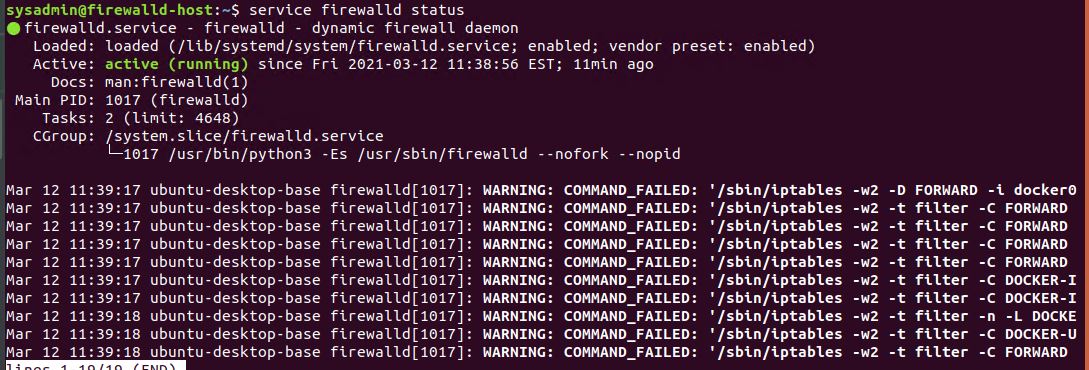
Run the commands that enable and start firewalld upon boots and reboots.  
  
 $ <sudo systemctl enable firewalld >



* $ <sudo systemctl start firewalld>

Note: This will ensure that firewalld remains active after each reboot.

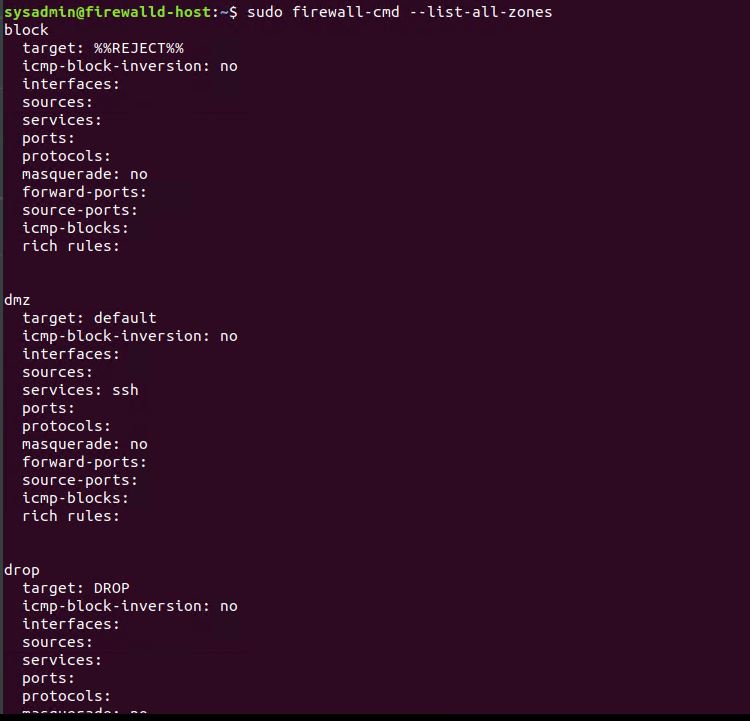
#### **Confirm that the service is running.**

* Run the command that checks whether or not the firewalld service is up and running.  
    
   $ <service firewalld status>  
  

#### **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.

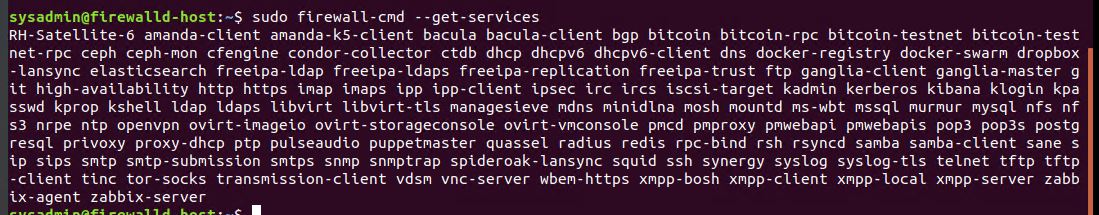
* Run the command that lists all currently configured firewall rules:  
    
   $ <sudo firewall-cmd --list-all-zones >



* 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 --permanent --new-zone=web

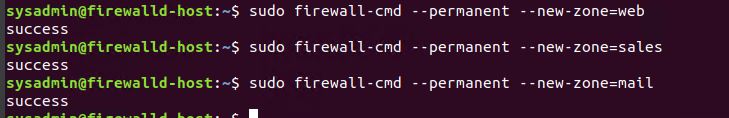
sudo firewall-cmd --permanent --new-zone=sales

sudo firewall-cmd --permanent --new-zone=mail>

* 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.  
  
 $ <See Above>



#### **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=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=smtp>

* Web:  
    
   $ <sudo firewall-cmd --zone=public --add-service=http>
* Sales  
    
   $ <sudo firewall-cmd --zone=public --add-service=http>

Mail

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

* What is the status of http, https, smI tp and pop3?
  + I don’t know what this question is asking

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

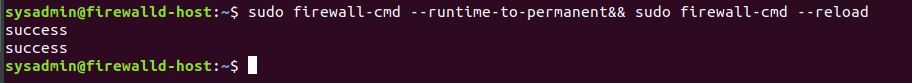
Run the command that will add all current and any future blacklisted IPs to the Drop Zone.  
  
 $ <ADD COMMAND HERE>

$ <ADD COMMAND HERE>

* $ <ADD COMMAND HERE>

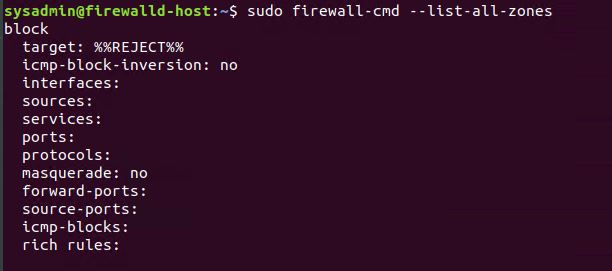
#### **Make rules permanent then reload them:**

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  
    
   $ <sudo firewall-cmd --runtime-to-permanent&& 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 --list-all-zones >  
  

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

* Use a rich-rule that blocks the IP address 138.138.0.3.  
    
   $ <sudo firewall-cmd --zone=home --ad-rich-rule=’rule family=”ipv4” source address=”138.138.0.3” reject’>

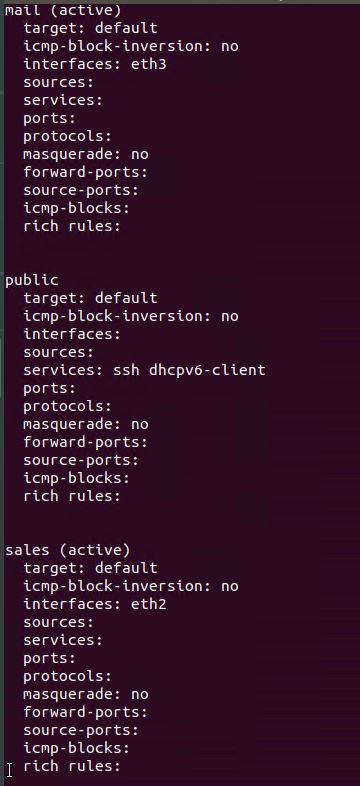
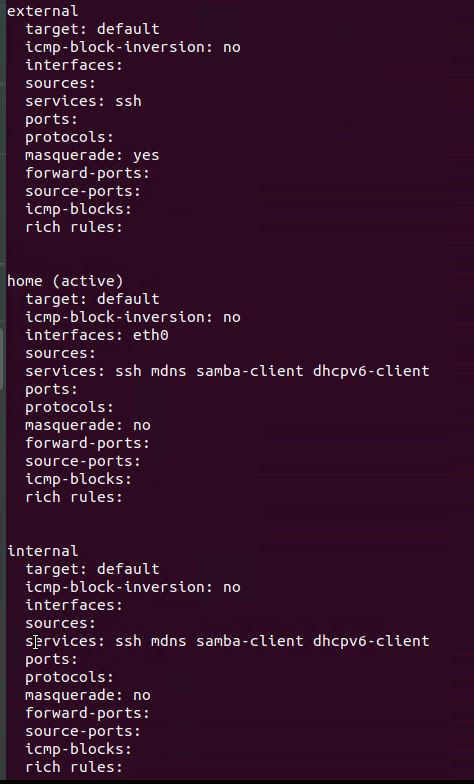
#### **Block Ping/ICMP Requests**

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=home --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.  
  


* 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: Signature-based IDS  
     
    Answer 2: Anomaly-based IDS
2. Describe how an IPS connects to a network.  
     
    Answer: Through Network Tap or Mirrored SPAN port
3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?  
     
    Answer: Snort
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 Type

#### **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
   2. A zero-day goes undetected by antivirus software.  
        
       Answer: Application & Data because the Application could have flaws in it and that the criminal found them. The data would be in trouble and thus the data defenses would need to be heightened.
   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 & Application because the host is what the operating system could be considered and the application could also be what the operating system could be called.
   5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.  
        
       Answer: Host because the host of the network or the site will be attacked and thus the defense would need to be fixed.
   6. Data is classified at the wrong classification level.  
        
       Answer: Data
   7. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.  
        
       Answer: Network
2. Name one method of protecting data-at-rest from being readable on hard drive.  
     
    Answer: MAC Layer Firewall
3. Name one method to protect data-in-transit.  
     
    Answer: Packet Filtering Fire
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.  
     
    Answer: LoJack?
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?  
     
    Answer: Don’t lose it in the first place? If they stole it from you, you could use a Bitlocker that encrypts the harddrive on the computer

#### **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 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 Firewalls (Stateful)

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/Proxy 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: Packet-Filtering Firewalls (Stateless)

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

Answer: MAC Layer Firewall

## **Optional**

#### **The Cyber Kill Chain**

Name each of the seven stages for the Cyber Kill chain and provide a brief example of each.

<https://www.lepide.com/blog/what-is-the-cyber-kill-chain-and-how-it-works/>

1. Stage 1: Reconnaissance: Attackers are selecting their victim and researching their security vulnerabilities.
2. Stage 2: Weaponization: Attackers got done with their reconnaissance and they have selected the vulnerabilities
3. Stage 3: Delivery: the attack is delivered from the attackers to give them a step forward to get the attack executed
4. Stage 4: Exploitation: Malicious code has been inserted and/or the vulnerabilities have been targeted, found and exploited.
5. Stage 5: Installation: malware installs the backdoor or way for the attacker to access the target environment
6. Stage 6: Command and Control: the attacker has control and can be manipulated by the attacker
7. Stage 7: Actions and Objective: the original goals for the attack can be used and completed successfully