**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 Control** – These controls include security measures that prevent physical access to IT systems, such as security guards or locked doors.

1. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?

Answer: **Administrative Control** – are the policies and procedures put in place by an organization, directed at the employees.

1. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?

Answer: **Technical Control** – are the protection methods that secure network systems. Hardware, software, and network level protection is included within a company’s specific technical controls

**Intrusion Detection and Attack indicators**

1. What is the difference between an IDS and an IPS?

**Answer**: An Intrusion detection system **(IDS)** is either a hardware device or software application that uses known intrusion signatures to detect and analyze both inbound and outbound network traffic for abnormal activities. This is done through:

* System file comparisons against malware signatures.
* Scanning processes that detect signs of harmful patterns.
* Monitoring user behaviour to detect malicious intent.
* Monitoring system settings and configurations.
* IDS gain access to network traffic by connecting to a network hub, a network switch configured for **mirroring or a network** tap.

An Intrusion prevention system **(IPS**) complements an IDS configuration by proactively inspecting a system’s incoming traffic to weed out malicious requests. A typical IPS configuration uses web application firewalls and traffic filtering solutions to secure applications.

**In brief:** IPS logs & take action against potential threat traffic and IDS doesn’t take any action again threat, it is just show alert.

1. What is the difference between an Indicator of Attack and an Indicator of Compromise?

**Answer**: Indicators of attack **(IOA)**: focus on detecting the intent of what an attacker is trying to accomplish, regardless of the malware of exploit used in an attack. IOA focus on identifying attacker activity while an attack is in process.

Indicators of compromise **(IOCs)** used by legacy endpoint detection solutions. IOC is focusing on forensic analysis of a compromise that has already taken place.

**In brief**: IOA is real time indicator and before attack, IOC is indicators of compromise or it is already breach.

**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**: Attackers probe for a weakness. This might include harvesting login credentials or information useful in a pushing attack. (Research, Identification, and selection of targets)
2. Stage 2: **Weaponization**: Build a deliverable payload using an exploit and back-door. (Pairing remote access malware with exploit into a deliverable payload (e.g., Adobe PDF and MS office)
3. Stage 3: **Delivery**: Sending the weaponized bundle to the victim-for example, a malicious link in a legitimate-looking email. (Transmission of weapon to target (e.g., Via email attachment, websites, or USB drives)
4. Stage 4: **Exploitation**: Executing code on the victim’s system. (once delivered the weapon’s code is triggered, exploiting vulnerable applications or systems)
5. Stage 5**: Installation**: Installing malware on the target asset. (The weapon installs a backdoor on a target’s system allowing persistent access)
6. Stage 6: **Command & Control (C2):** creating a channel where the attacker can control a system remotely. (Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network.)
7. Stage 7: **Actions on objectives**: Attacker remotely carries out its intended goal. (The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

**Snort Rule Analysis**

Use the Snort rule to answer the following questions:

Snort Rule [#1](file:///C:\utoronto-bootcamp\utor-tor-cyber-pt-09-2020-u-c\-\issues\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 external port to inbound home network on port 5800 (VNC remote buffer RF protocol over http):5820

Remote host using any port, attempting to scan local host on port 5800:5820. Using TCP/IP protocol

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

**Answer**: Reconnaissance , Looking the port scanning or try to get access.

1. What kind of attack is indicated?

**Answer**: SCAN: Potential VNC,

Snort Rule [#2](file:///C:\utoronto-bootcamp\utor-tor-cyber-pt-09-2020-u-c\-\issues\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**: Remote host to http port (80), to local host on any port. Delivered the data on local host through web.

**Alert from external TCP traffic on port80, HTTP to internal home network (RC190) on any port**.

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

**Answer**: Delivery.

1. What kind of attack is indicated?

**Answer**: Policy-violation (Polices, awareness and Policy rule) it’s ‘s an attack per se. it ‘s just something which might vilate a corporate policy

**It’s just telling you that someone has downloaded a windows exe**. File or DLL over 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 $External\_Net any 4444 -> $Home\_Net any (msg: “ET Possible Trojan or CrackDown)

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

**Log into the Azure firewalld machine**

Log in using the following credentials:

* Username: sysadmin
* Password: cybersecurity

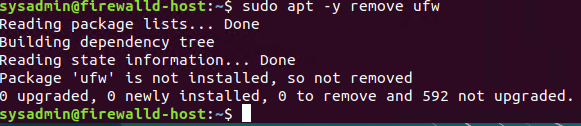
**Uninstall ufw**

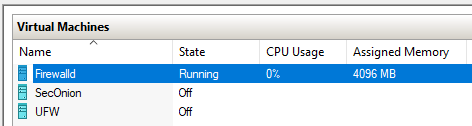
Before getting started, you should verify that you do not have any instances of ufw running. This will avoid conflicts with your firewalld service. This also ensures that firewalld will be your default firewall.

* Run the command that removes any running instance of ufw.

**$ sudo apt -y remove ufw**

**$ sudo ufw disable**



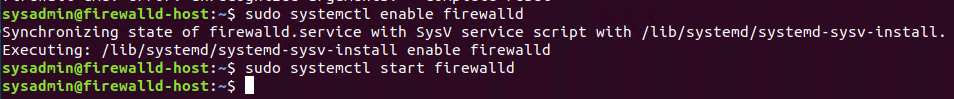


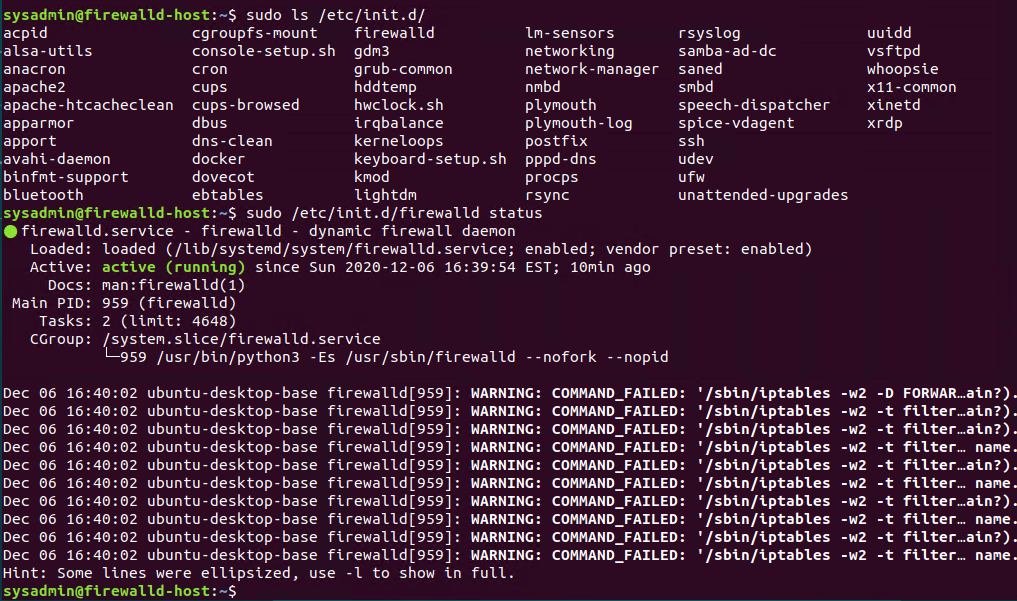
**Enable and start firewalld**

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.
* **$ sudo /etc/init.d/firewalld status**
* **$ Sudo /etc/init.d/firewalld enable**
* **$ sudo systemctl enable firewalld**
* **$ sudo systemctl start firewalld**

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



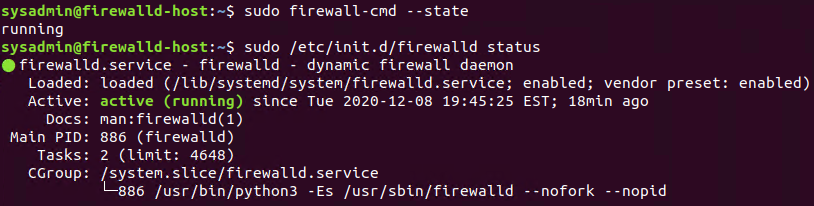


**Confirm that the service is running.**

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

**$ sudo firewall-cmd --state**

**$ sudo /etc/init.d/firewalld status**



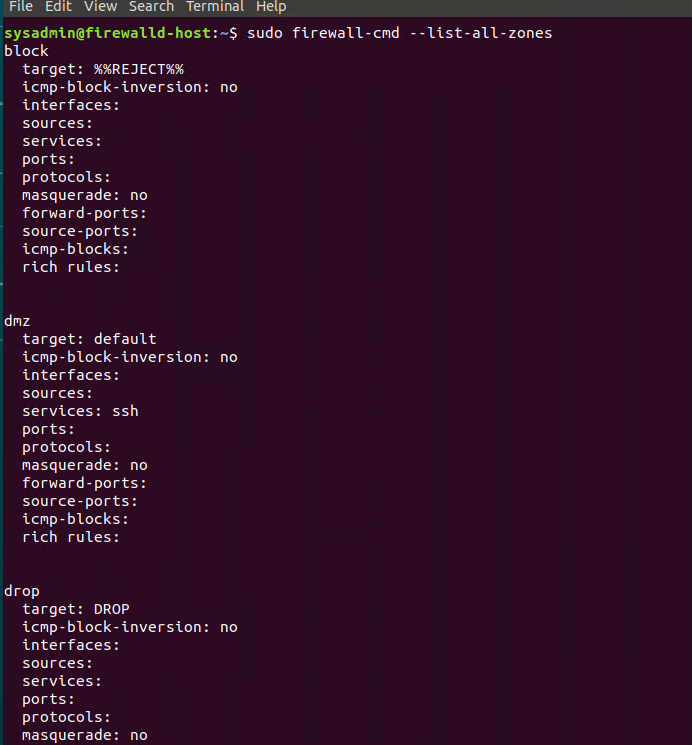
**List all firewall rules currently configured.**

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**

**Currently Firewall Zones are: Block, DMZ, Drop, External, Home, Internal, Public, Trusted, Work**



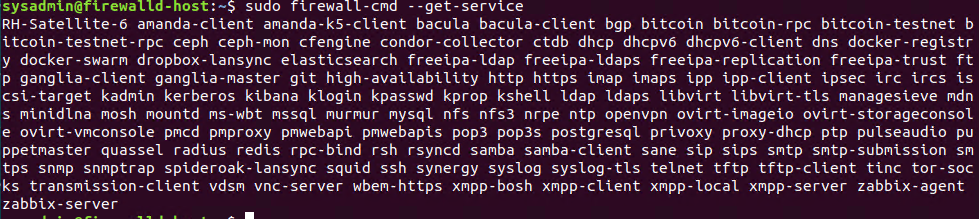
* Take note of what Zones and settings are configured. You many need to **remove unneeded** services and settings.
* 
* 

**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 firewalld-cmd –get-services**

**(Sorry I took screenshot after configured all 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**

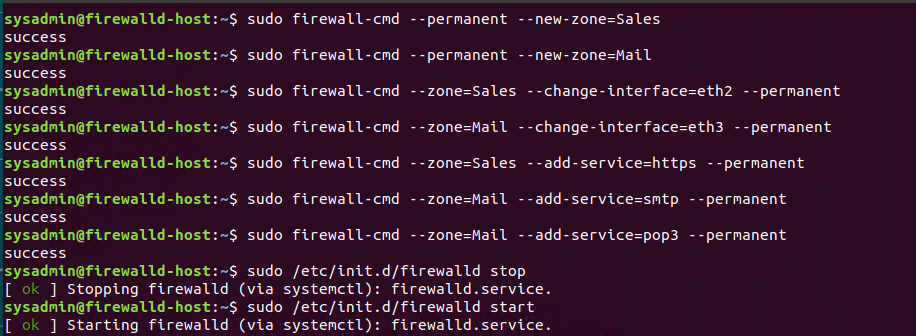
* We can see that the Public and Drop Zones are created by default. Therefore, we will need to create Zones for Web, Sales, and Mail.

**Create Zones for Web, Sales and Mail.**

* Run the commands that creates **Web, Sales and Mail zones**.
* **$** **sudo firewall-cmd –permanent –new-zone=WEB**
* **$ sudo firewall-cmd –permanent –new-zone=Sales**

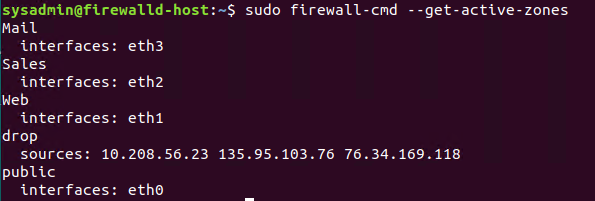
**$ sudo firewall-cmd –permanent –new-zone=Mail**



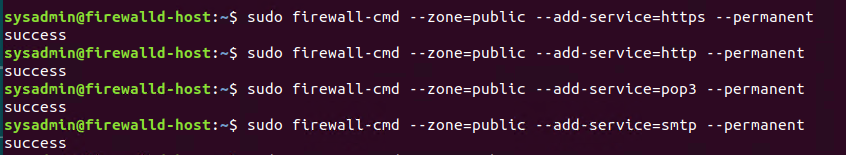


**Set the zones to their designated interfaces:**

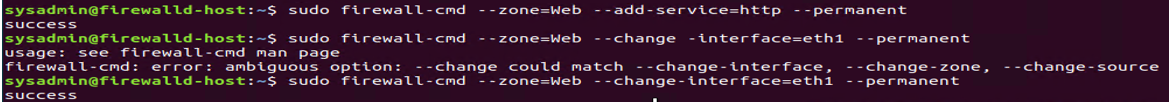
* Run the command that sets your eth0 interface to your zones.
* $ **sudo firewall-cmd –zone=Sales –change-interface=eth2 --permanent**
* **$ sudo firewall-cmd –zone=Mail –change-interface=eth3 --permanent**
* **$ sudo firewall-cmd –zone=Web –change-interface=eth1 --permanent**



**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=https --permanent**
* **$ sudo firewall-cmd –zone=public –add-service=http --permanent**
* **$ sudo firewall-cmd –zone=public –add-service=pop3 --permanent**
* **$ sudo firewall-cmd –zone=public –add-service=smtp --permanent**
* 
* **Web:**

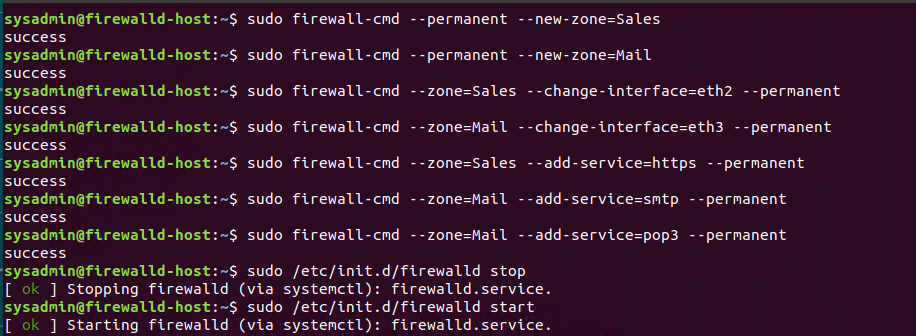
$ **sudo firewall-cmd –zone=Web –add-service=http --permanent**



* Sales

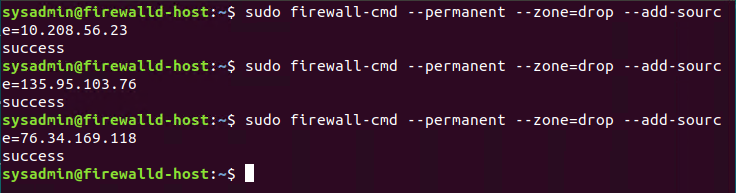
**$ sudo firewall-cmd –zone=Sales --change-interface=eth2 – permanent**

**$ sudo firewall-cmd –zone=Sales –add-service=https –permanent**

* **Mail**
* **S sudo firewall-cmd --zone=Mail --change-interface=eth3 --permanent**
* **$ sudo firewall-cmd --zone=Mail –add-service-smtp --permanent**
* **$ sudo firewall-cmd --zone=Mail -add-service-pop3 --permanent**
* **What is the status of http, https, smtp and 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 –permanent --zone=drop --add-source=10.208.56.23**
* **$ sudo firewall-cmd –permanent --zone=drop --add-source=135.95.103.76**
* **$ sudo firewall-cmd –permanent --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 –reload**

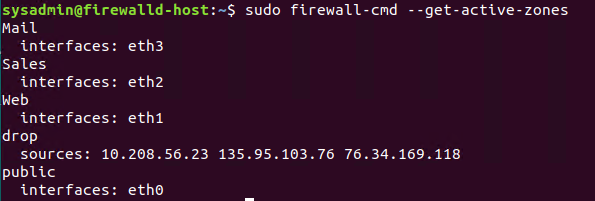


**View active Zones**

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.

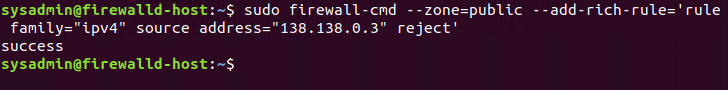
$ **sudo firewall-cmd –get-active-zones**



**Block an IP address**

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

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

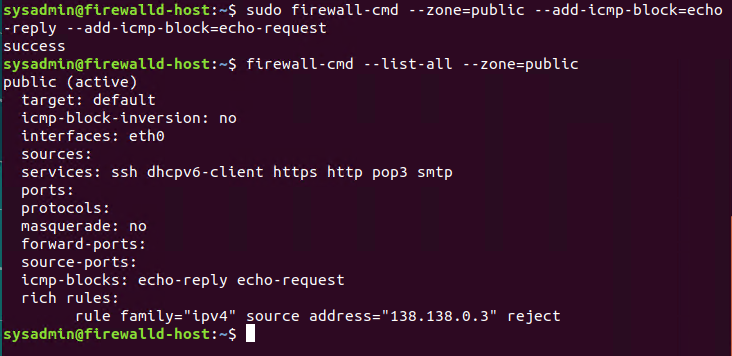


**Block Ping/ICMP Requests**

Harden your network against ping scans by blocking icmp ehco 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**



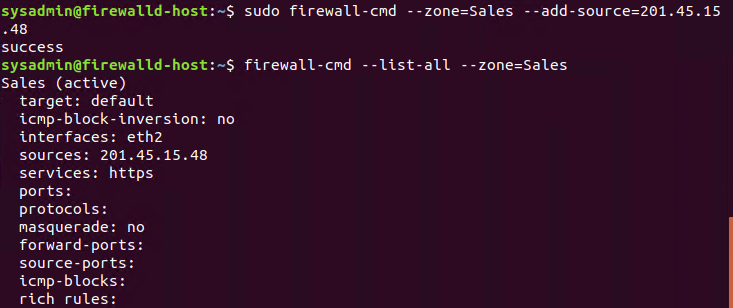
**Rule Check**

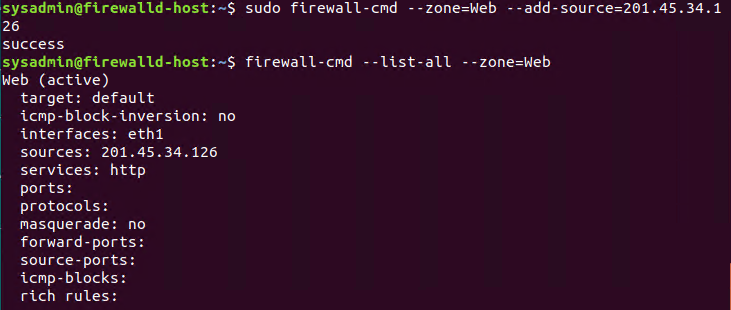
Now that you've set up your brand new firewalld installation, it's time to verify that all of the settings have taken effect.

* 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=Sales –list-all**
* **$ sudo firewall-cmd –zone=public –list-all**

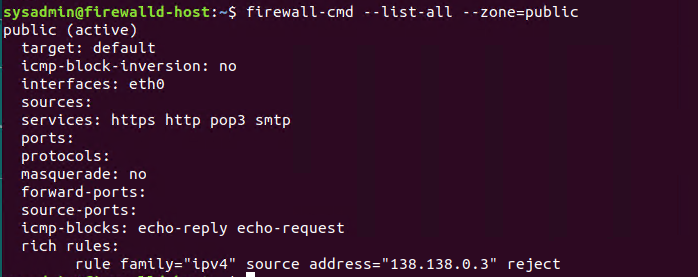
**$ sudo firewall-cmd –zone=public –list-all**

**$ 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.

Definition: An intrusion detection system (IDS) is a tool or software that works with your network to keep it secure and flag when somebody is trying to break into your system. Types of intrusion detection system:

Answer 1: **Network-based Intrusion Detection System (NIDS)**: it’s only applied to one host at a time, not an entire subnet. (Generally deployed or placed at strategic points throughout the network, intended to cover those places where traffic is most likely to be vulnerable to attack.) Its monitor traffic from all devices going in and out of the network. NIDS has two type of detection system. **A. Signature-Based IDS**: This type of IDS is focused on searching for a “signature, “patterns, or a known identity, of an intrusions or specific intrusion event. (Signature-based IDS is only as good as how up to date its database is at a given moment) **B. Anomaly-Based** **IDS** looks for the kinds of unknown attacks signature-based IDS finds hard to detect.

Answer 2: **Host Intrusion Detection System:** The HIDS runs on all devices in the network with access to the internet and other parts of the enterprise network. While host intrusion detection systems look at actions and files on the host devices.

1. Describe how an IPS connects to a network.

Answer: IPS usually located behind the firewall and monitors or scan the traffic for suspicious behaviour.

1. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?

Answer: Snort (The snort tool) is one of the popular rule-based and opensource IDSs. Its rules recognise malicious network packets by matching the current packet against predefined rules and cannot detect zero-day attack.

1. 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: Stateful IDS is useful in detecting new exploits.

**Defense in Depth**

1. For each of the following scenarios, provide the layer of Defense in Depth that applies:

Defense-in-depth (DiD) is an information assurance strategy that provides multiple, redundant defensive measures in case a security control fails, or a vulnerability is exploited. A computer network to protect the confidentiality, integrity, and availability of the network and the data within

* 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 Control** – These controls include security measures that prevent physical access to IT systems, such as security guards or locked doors. A hacker can try to access to any workstation inside the building and server room too.

* 1. A zero-day goes undetected by antivirus software.

Answer: **Technical Controls** - Zero-day antivirus software is capable of identifying known and unknown malicious files. The goal is to block them before they can cause damage to your computer or steal your data.

Zero-day exploits are dangerous because your antivirus software doesn’t have signature in place to identify them. Until the vulnerability is identified and patched, zero-day exploits can get through traditional antivirus software undetected

* 1. A criminal successfully gains access to HR’s database.

Answer: **Administrative Control** – are the policies and procedures put in place by an organization, directed at the employees. Training employees to make certain to label sensitive information as “confidential” or keep private files in proper folders are examples of administrative control

* 1. A criminal hacker exploits a vulnerability within an operating system.

Answer: **Technical Control** – are the protection methods that secure network systems. Hardware, software, and network level protection is included within a company’s specific technical controls. Cybersecurity efforts including layered security live in this category.

* 1. A hacktivist organization successfully performs a DDoS attack, taking down a government website.

Answer: Technical Control

* 1. Data is classified at the wrong classification level.

Answer: Data classification is broadly defined as the process of organizing data by data’s level of sensitivity. Generally, we find four levels data classification: A. Restricted, B. Confidential C. Internal D. Public.

* 1. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.

Answer: Administrate Control

1. Name one method of protecting data-at-rest from being readable on hard drive.

Answer: Encryption, Data encryption, which prevents data visibility in the event of its unauthorized access of theft. In commonly used to protect data in motion and increasingly promoted for protecting data at rest. Strong encryption methods should use such as AES or RSA

Data protection at rest aims to secure inactive data stored on any device or network.

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

Answer: To protect your data when it flows across an untrusted network(internet). You should put the appropriate security measures in effect. These measures include the Secure Sockets layer (SSL), IBM I Access for windows, and virtual private network (VPN) connections

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

Answer: **Lojack** for laptop can map and display your laptops current and past whereabouts. – a subscription service for Mac and PC. Few apps are here:

* 1. Lojack: A laptop-specific program, this works closely with law enforcement to recover a stolen laptop. The computrace agent, part of the Lojack software, works in the background and resists detection.
  2. Hidden: A Mac-specific tracking app, this provides a wealth of information for lost or stolen Macs.
  3. Prey: A cross-platform tracking app, this is available for both computer and mobile devices.
  4. GadgetTrak: A cross-platform tracking app, this provides information tailored to specific groups of devices. On laptops, Gadget Track provides Wi-Fi positioning and webcam support.
  5. LockitTight: A Windows-specific program, this provides location tracking, screenshots, webcam support, key logging, file tracking, and encrypted reports.
  6. Laptop Cop: installs invisibly and keeps a record of the laptop’s location. The owner can view location history online

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

Answer: User can protect data with Device **encryption and Bit locker**. Encryption is a mathematical process used to jumble up data. If important files or whole device are encrypted, there is no way to make sense of them without the key.

**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** operate at layer 5 (Session Layer) of OSI model. This firewall depends on the three-way TCP handshake. TCP uses a three-way handshake to establish a reliable connection. The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other. The exchange of these four flags is performed in three steps – **SYN, SYN-ACK, ACK**

These firewalls only look at the header of a packet. One the circuit is allowed to establish an end-to-end connection, all date is tunneled between parties.

Adv. Quickly and easily approve and deny traffic without consuming significant computing resources. Relatively inexpensive and provide anonymity to the private network.

DisAdv. Do not check the contents of the packet. If a packet contains malware but has the correct TCP information, the data is allowed to pass through.

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 filters firewall (stateful): operate on layer 3 and layer 4 of the OSI model. Stateful firewalls can determine if a packet is: trying to establish a new connection, know as a new state. Part of an existing connection know as an established state. IS neither a new or exiting connection, known as a rouge packet.

Rather than look at individual packets, stateful firewalls examine the connection as whole, looking at streams of packets. They inspect the packet’ conversation and routing tables and use a combination of TCP handshake verification and packet inspection technology.

Adv. Offer transparent mode, which allow direct connections between clients and servers

Dis Adv. Are resource-intensive systems.

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: **Proxy-based firewalls (Application Layer)**, these firewalls acts as a gateway between end users who request data and the source of that data. Host devices connect to the proxy, and the proxy makes a separate connection to the source of the data. In response, source device makes connections to the proxy, and the proxy make a separate connection to the host device. Before passing on packets to a destination address, the proxy can filter then to enforce polices and mask the location of the recipient’s device, but also to protect the recipient’s device and network.

These firewalls operate at layer 3 to layer 7 of OSI model. They inspect the actual contents of the packet, including authentication and encryption components. Proxy firewalls ue deep packet instepction and state inspection to determine if incoming traffic is safe or harmful. They intercept all traffic in its way too its final destination, without the data source knowing. A Connection is established to the proxy firewall, which inspects the traffic and forwards it if its determined to be safe, or drops it its’s determined to be malicious.

Proxy firewalls create an extra layer of protection between the traffic source and its destination behind the network by obscuring the destination from the source creting and additional layer of anonymity and protection for the network.

Adv. More secure than other implementations and provide simple log and file audit management for incoming traffic.

DisAdv. Resource intensive, requiring robust modern hardware and high costs. Bypassed with encryption.

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 filter firewall (stateless)**controls the network access by analyzing the outbound and incoming packets. It lets a packet pass or block its way by comparing it with pre-established criteria like allowed IP addresses, Packets type, port number, etc. it is suitable for small business.

These firewalls statically evaluate the contents of the packets and don’t keep track of the state of network connection. Rules based on individual packets. Source and destination IP address, Source and destination Port info, IP protocol, ingress, and egress interface.

Adv.: not resource intensive, meaning they are low cost and do not have a significant impact on system performance. Work best with small networks.

DisAdv.: Easy to subvert compared to more robust firewalls. Only operate at the network layer. They ae vulnerable to spoofing and don’t support custom based rule sets.

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

Answer: **Host-based firewall or Mac layer firewalls (Data link)**, they are installed on each server, control incoming and outgoing traffic, decide whether to allow traffic to individual devices, and protect the host.

Mac layer firewall filter based on source and destination mac address. Routers compare the mac address of a device against an approval list.

Adv.: Secure network from novice attackers

DisAdv. :can be easily bypass by mac spoofing

**Thank you,**

**Dhawal Pandya**