**Linux Network Configuration**

**1. Goal and Deliverable**

Getting familiar with Linux network and firewall configuration.

At the end, you need to submit the screenshot of Linux commands you tried to the D2L Dropbox.

**2. Network Configuration**

Network configuration is the process of assigning network settings, policies, flows, and controls.

Step 1: finding the distro of the current Linux system

Different Linux distro uses different files and commands for network configuration. So, our first step is to find out the Linux distro on your system. Please connect to badgerctf.cs.wcupa.edu through ssh, and then use the following command to check the distro: cat /etc/\*-release

Please attach the screenshot of the Linux distro information here.

Text

Description automatically generated

Step 2: gather information about the current network setting

TCP/IP configuration files are important for network administrators to configure the network. Let’s read three of them by command: cat *filename*

|  |  |
| --- | --- |
| *filename* | Description |
| /etc/resolv.conf | List DNS servers for internet domain name resolution. |
| /etc/hosts | List hosts to be resolved locally |
| /etc/nsswitch.conf | List order of host name search. Typically look at local files, then NIS server, then DNS server. |

Here is an example

Graphical user interface, text

Description automatically generated

Please read attach screenshots for /etc/hosts and /etc/nsswitch.conf.

Text

Description automatically generated

Step 3: show IP addresses

The command “ip addr show” displays the ip addresses of all interfaces.

Please show the screenshot of first two interfaces’ ip addresses.

The first two IP addresses are 127.0.0.1/8 and 172.17.0.8/16.

Text

Description automatically generated

Step 4: show network route

The command “ip route show” displays the network flow.

Please show the screenshot that displays the network route.

Text

Description automatically generated

**3. Firewall Configuration**

Step 5: enable UFW

UFW, or Uncomplicated Firewall, is an interface to iptables that is geared towards simplifying the process of configuring a firewall. Let us start from checking the status of UFW using command “sudo ufw status”. If the status is inactive, please use the command “sudo ufw enable” to activate the firewall, and check the status again.

Please attach a screenshot of active ufw status.

Text

Description automatically generated

Step 6: where to find help

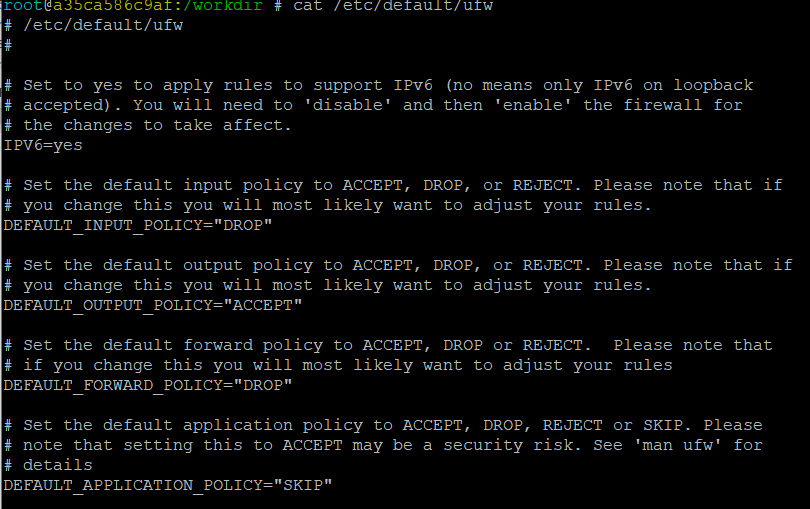
If you are new to UFW, the first thing to do is to refer the help section and man page of UFW to get the basic idea about UFW usage. Please use “ufw --help” and “man ufw” to check the syntax and feature of ufw. These two command are very handy.

Step 7: default rules

Using UFW, you can create firewall rules (or policies) to allow or deny a specific service. There are default policies that come with ufw. The default policy drops all incoming connections and allow all outgoing connection.

Please use the command “cat /etc/default/ufw” to check the default rule.

Please attach the screenshot of the default rules and highlight the default incoming and outgoing policies.



Step 8: add rules

Now, let us create our own rules. Currently, all incoming traffic is denied. Let us allow the ssh connection by using command

(1)“sudo ufw allow ssh”: allows all access to ssh service. UFW knows by default ssh listens to port 22.

(2)“sudo ufw allow 22”: explicitly tell UFW to allow incoming connections for port 22

(3)“sudo ufw allow 22/tcp”: allows all access to tcp port 22

(4)“sudo ufw allow 2222/tcp”: allows a custom ssh port (i.e. 2222) to accept the incoming connections

After executing these four commands, if you check the ufw status again, here is what you should have

Text

Description automatically generated

Please show the screen shot of allowing http, and https.

As you can see, ports 80 and 443 (http and https) are now allowed :D

Graphical user interface, text

Description automatically generated

Step 9: delete UFW firewall rules

To remove a rule or policy, you can use ufw delete command. For example, if you no longer with to allow ssh traffic, simply run

Text

Description automatically generated

Please show the screenshot of deleting http.

A screenshot of a computer

Description automatically generated with medium confidence

Whenever you want to disable ufw, simply run “sudo ufw disable”. The firewall will be stopped and disabled on the system startup.

**3. Network mapping**

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks. To run Nmap, we need to first install it.

Step 10: install snaps and nmap

Snaps are applications packaged with all their dependencies to run on all popular Linux distributions from a single build. Let’s installed it from command line “sudo pacman -S snapd”.

Once installed, the system unit that manages the main snap communication socket needs to be enabled by “sudo systemctl enable –now snapd.socket”.

To enable classic snap support, enter the following to create a symbolic link between /var/lib/snapd/snap and /snap: “sudo ln -s /var/lib/snapd/snap /snap”

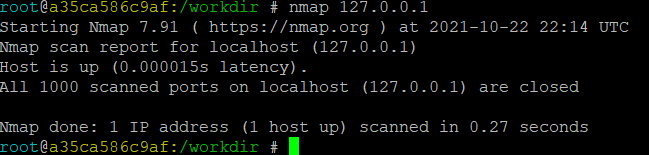
Finally, please use command “sudo snap install nmap” to install nmap.

Step 11: Perform network mapping (enumeration and identification of network components) use Nmap

There are many useful Nmap command.

|  |  |  |
| --- | --- | --- |
| Syntax | Example | Function |
| nmap IPaddress | nmap 127.0.0.1 | Basic Nmap scan against IP or host |
| nmap -p portnumberrange localhost | nmap -p 1-65535 localhost | Scan specific ports or scan entire port ranges on a local or remote server |
| nmap IPaddress IPaddress | nmap 1.1.1.1 8.8.8.8 | Scan multiple IP addresses |
| nmap -p IPaddress/subnet mask | nmap -p 8.8.8.8/28 | Scan entire CIDR IP ranges |
| nmap --top-ports TopX IPaddress | nmap --top-ports 20 192.168.1.106 | Scan top 20 most common ports for IP address 192.168.1.106 |

Please attach the screenshot of nmap on your localhost.



Please use command “ifconfig -a” to check your ip address then attach the screenshot of nmap this ip address, the top 10 most common ports for this IP address

See next page!

Text

Description automatically generated

References:

<https://ostechnix.com/how-to-setup-firewall-with-ufw-on-linux/>

<https://www.secur.cc/how-to-implement-and-manage-a-linux-firewall/>

<https://blog.resellerclub.com/a-step-by-step-guide-on-how-to-configure-firewall-in-linux/>

<http://www.yolinux.com/TUTORIALS/LinuxTutorialNetworking.html>

<https://snapcraft.io/install/nmap/manjaro>