**Getting Familiar with Linux System Administration**

**1. Goal and Deliverables**

Getting familiar with Linux system administration.

Deliverables: Please answer all of the question inside this lab report and submit it to the D2L submission folder.

Note that different Linux distribution may have different commands for the same purpose. So, the first thing you want to do is to check the distribution of the Linux system using command “***cat /etc/\*-release***”. Then, you could search specific commands like “ubuntu command for adding a user” or “redhat command for adding a group” or “manjaro command for update”. Here, “ubuntu, redhat, manjaro” are different Linux distrubtions, and “adding a user, adding a group, update” are the functions you want to reach.

**2. System Administration and Hardening**

Step 1: Set up user accounts

Setting up user accounts is the very basic operation you need to conduct, since you are not the only user for the Linux system. There are three steps: (1) Open the terminal application; (2) To add a new user in Ubuntu run ***sudo adduser username***; (3) Enter password and other needed information to create a user account on Ubuntu server.

Text

Description automatically generated

Enter optional user information here

To overwrite the regular expression, you need to use –force-badname

Enter password here

System information about this user

Enter password (can be found in Lab 1) here

If you want to delete a user account, please use command ***sudo deluser username*** or ***sudo userdel username***

Step 2: Set up groups

Please create at least three users (follow the above steps) before setting up groups. Use command ***sudo addgroup groupname*** or ***sudo groupadd groupname*** to create groups.

Text

Description automatically generated

If you want to delete a personalized group, user command ***sudo delgroup groupname*** or ***sudo groupdel groupname***

Please show all of the users in the system by using command *cat /etc/passwd*

A screen shot of a computer screen

Description automatically generated

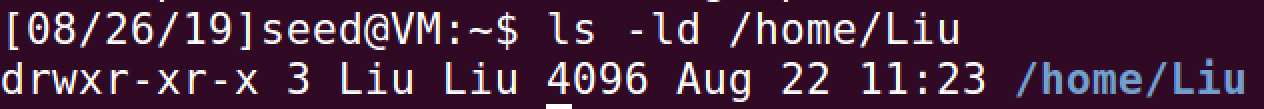
Please show all of the groups in the system by using command *cat /etc/group*

A screen shot of a computer screen

Description automatically generated

Step 3: Configure authorization policies

When a new user is created, the adduser utility creates a brand new home directory named /home/username. If your server will be home to multiple users, you should pay close attention to the user home directory permissions to ensure confidentiality. By default, user home directories in Ubuntu are created with world read/execute permission. This means that all users can browse and access the contents of other users home directories. This may not be suitable for your environment. Let’s configure appropriate authorization policies from verify current user home directory permissions by using following syntax: *ls –ld /home/username*



The above output shows that the directory /home/Liu has world-readable permission. To learn how to modify the permission on a file or a folder, please use command ***man chmod***. It shows everything about the permission modification that you need to know. ***man*** is the abbreviation of manual. You could use the syntax ***man commandname*** to check manuals for all commands.

Please remove the world executable permission to one of your user’s home directory, and attach the screenshot of ls - ld /home/username to show the result.

A screen shot of a computer screen

Description automatically generated

Step 4: appropriate authentication policies

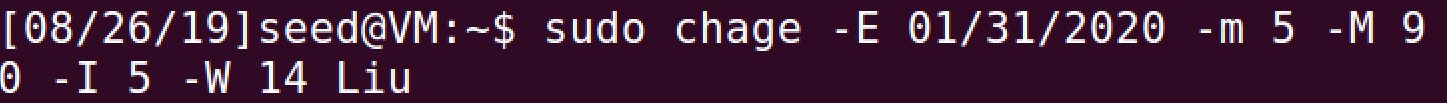
A strong password policy is one of the most important aspects of your security posture. By default, Ubuntu requires a minimum password length of 6 characters, as well as some basic entropy checks. If you want to check the password requirements, please go to files -> etc -> pam.d -> passwd.

When creating user accounts, you should make it a policy to have a minimum and maximum password age forcing users to change their passwords when they expire. Before enforcing the limits, please check the current status of a user account by using syntax: *sudo chage -l username*. You will get information such as last password change, password expires, password inactive, etc. Please see the following figure as an example

Text

Description automatically generated

If you want to change the expiration date (-E) to 01/31/2020, minimum password age(-m) of 5 days, maximum password age (-M) of 90 days, inactivity period (-I) of 5 days after password expiration, and a warning time period (-W) of 14 days before password expiration:



Then, use sudo chage -l username to verify changes. Please attach the screenshot here.

A screen shot of a computer screen

Description automatically generated

Step 5: Install patches and updates, ensure all patches and updates are applied

One of the important operating system hardening practice is to install all patches and updates.

First, let us apply updates and patches on Linux by using command ***sudo apt-get upgrade*** or ***sudo pacman -Syu***.

Then, we need to get updated software list for Ubuntu by using command *sudo apt-get update* or *sudo pacman -Syu.* It will show you the number of upgradable packages. If you want to read the details, please use command *apt --list upgradeable*. It marks the package names in different colors. To upgrade individual packages, please use command *sudo apt install packagename*. For example, if you need to upgrade firefox, you can use command *sudo apt install firefox* to do that.

Please updates and patches your Ubuntu systems and show that you have 0 upgradeable packages.

A screen shot of a computer screen

Description automatically generated

Step 6: Remove or shutdown unnecessary components and services

Removing and shutdown unnecessary components and services reduce the attack surface. So, attackers have less opportunity to compromise your system.

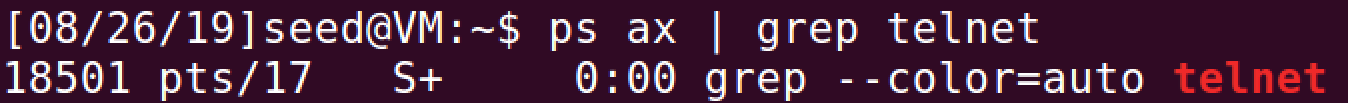
First, we need to know what kind of services are running on the system using command *ps ax*.

Text

Description automatically generated

In the above output, you notice that some of the applications you may not needed on your server but they are still running. Some examples are: Telnet which is a bidirectional interactive text-oriented communication over internet or local area network; rlogin which allows you to log in to another host over network; automount which mounts different file systems automatically to bring up network file system, etc.

If you want to kill a process in Linux (you don’t need to actually do it in this lab, but you need to know how to do it), you need to get the process ID (PID) of the process by command *ps ax | grep telnet.*



Here, 18501 is the PID of “telnet”. To kill that PID, run command *kill -9 18501*.

**3. Network Configuration**

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

Step 7: 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.

A computer screen with white text

Description automatically generated

Step 8: 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.

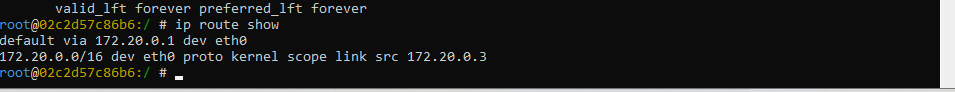
A computer screen with text on it

Description automatically generated

Step 9: show network route

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

Please show the screenshot that displays the network route.



**4. Firewall Configuration**

Step 10: 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.

A computer screen shot of a program

Description automatically generated

Step 11: 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 et 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 12: 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 rule and highlight the default incoming and outgoing policies.

A screenshot of a computer program

Description automatically generated

Step 13: 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.

A screenshot of a computer

Description automatically generated

Step 14: 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

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 15: 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

A screen shot of a computer screen

Description automatically generatedA computer screen shot of a black screen

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>