Practical Experience Report

Lab 3: Linux system hardening

Name:

StudentID:

System hardening is the proactive process of securing an IT system by reducing its attack surface and eliminating potential vulnerabilities. It involves configuring systems, applications, and networks to minimize security risks through patching, removing unnecessary software, and enforcing strict access controls to prevent unauthorized access or malware exploitation. In this lab we are going to harden your Linux system. We will need:

- Ubuntu VM: the target Linux system that need to be hardened
- Google, GenAI (e.g.: ChatGPT) to assist in hardening task
- *It would be more convenient if you work by ssh to the VM instead of using the VM GUI.

Task 1: Install OpenSSH server on the VM

1.1. Research with Google or GenAI to find out how to install OpenSSH server on your Ubuntu

1.2. List all commands in chronological order that help you to install OpenSSH:

Seq	Command	Description
1	`sudo apt update`	Update the package list from repositories
2	`sudo apt upgrade -y`	Upgrade installed packages to latest versions (optional but recommended)
3	`sudo apt install openssh-server -y`	Install OpenSSH server
4	`dpkg -l | grep openssh-server`	Verify that OpenSSH server is installed
5	`sudo systemctl start ssh`	Start the SSH service
6	`sudo systemctl enable ssh`	Enable SSH service at boot
7	`sudo systemctl status ssh`	Check SSH service status
8	`sudo systemctl restart ssh`	Restart SSH service
9	`ss -tlnp | grep ssh`	Check which port SSH is listening on

10	`sudo ufw allow ssh`	Allow SSH through firewall
11	`sudo ufw enable`	Enable firewall
12	`sudo ufw status`	Check firewall status
13	`ip a`	Show IP address of the machine
14	`ssh username@your_ip_address`	Connect to SSH server from another machine
15	`sudo nano /etc/ssh/sshd_config`	Edit SSH configuration file
16	`sudo systemctl reload ssh`	Reload SSH configuration without stopping service
17	`ps aux | grep sshd`	Check if SSH daemon (sshd) is running

1.3. Answer the following questions:

Q1. How to stop and start ssh server? (Show commands that work)

Answer:

The command `sudo systemctl start ssh` is used to start the SSH server so that it can accept incoming connections.

To stop the SSH service, the command `sudo systemctl stop ssh` is used, which terminates all active SSH sessions.

In addition, `sudo systemctl restart ssh` can be used to restart the SSH service.

Q2. How to know the status (start/stop) of ssh server?

Answer:

To check the status of the SSH server, the command `sudo systemctl status ssh` is used. This command displays whether the SSH service is currently running or stopped. If the output shows “active (running)”, it means the SSH server is running and accepting connections. If it shows “inactive (dead)”, it indicates that the SSH service has been stopped and is not currently active.

Q3. How to know what port number SSH server is listening at?

Answer:

To know which port the SSH server is listening on, there are two common methods. First, the configuration file can be checked using the command `grep ^Port /etc/ssh/sshd_config`, which shows the port defined in the SSH configuration.

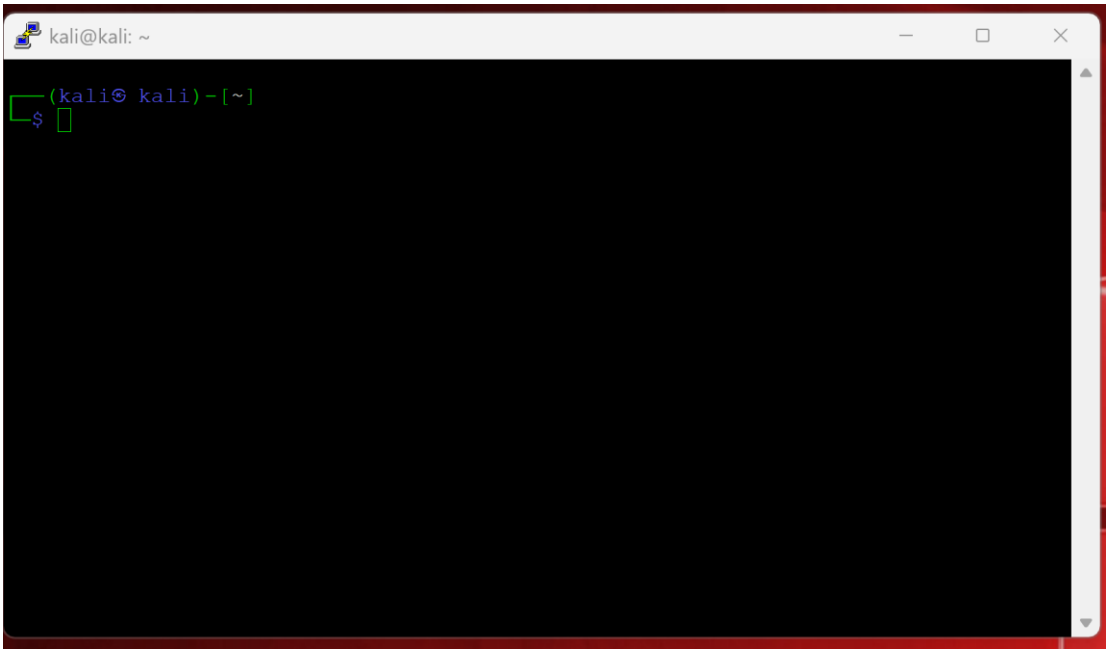
Second, the actual listening port can be verified by running `sudo ss -tlnp | grep ssh`, which displays active network sockets and confirms the port currently in use by the SSH service.

By default, the SSH server listens on port 22 unless it has been changed in the configuration. My server listens on port 22 too.

Q4. List the name of the ssh client software that you are using. Insert of a screenshot that you successfully access the VM with the ssh client software

Answer:

- SSH client software: PuTTY
- Connection details:
    - Host Name (IP): <VM_IP>
    - Port: 22
    - Connection type: SSH
- Screenshot:



    - This is my PuTTY terminal window.
    - I have successfully logged in.

Task 2: Install Lynis

Research with Google/GenAI to know how to install Lynis on your VM. Actually install Lynis and answer the following questions:

2.1. Introduce Lynis in writing form (what is it, what is it for, who should you it, how it works, ... Be concise but informative).

Lynis is an security auditing and system hardening tool designed for Linux, Unix, and macOS systems. It is primarily used to analyze the security posture of a system by scanning for vulnerabilities, misconfigurations, and outdated components. The main purpose of Lynis is to help administrators improve system security by providing detailed reports and practical recommendations.

Lynis is commonly used by system administrators, security professionals, and auditors who need to assess and maintain the security of servers, virtual machines, or personal systems. It is especially useful in environments where security compliance and regular auditing are required.

The tool works by performing a set of predefined tests on the system. These tests examine such as system configuration, installed software, authentication mechanisms, file permissions, and network settings. After the scan, Lynis generates a report that includes warnings, detected issues, and suggestions for improvement.

Task 3: Use Lynis to check your Ubuntu VM

3.1. Use Lynis to check your Ubuntu VM. With the following command:

lynis audit system –quick

The command will produce a report of system checking to the console.

The command also produces a file lynis-report.dat (in the current directory)

3.2. Read the output and analyze lynis-report.dat file and list all warnings and suggestions into the following table. Do some research (with Google/GenAI) on those items and provide short notes on “Notes” column.

Type	Code	Content	Notes
Suggestion	DEB-0280	Install libpam-tmpdir	Automatically creates a separate /tmp directory for each user → reduces the risk of

			privilege escalation attacks
Suggestion	DEB-0810	Install apt-listbugs	Displays critical bugs before installing packages → helps avoid installing unstable or vulnerable software
Suggestion	DEB-0811	Install apt-listchanges	Shows important changes before updates → helps administrators monitor and control updates
Suggestion	DEB-0831	Install needrestart	Checks which services need to be restarted after updates → prevents using outdated libraries (security risk)
Suggestion	DEB-0880	Install fail2ban	Blocks IP addresses after multiple failed login attempts → protects against SSH brute-force attacks
Suggestion	BOOT-5122	Set password on GRUB	Prevents unauthorized users from booting into single-user mode → avoids password bypass
Suggestion	BOOT-5180	Determine runlevel and services	Reviews services that start at boot → helps reduce the system's attack surface

Suggestion	BOOT-5264	Consider hardening system services	Use systemd-analyze security to evaluate service security levels
Suggestion	(multiple services)	Many services running	Multiple services are running (e.g., NetworkManager, SSH, etc.) → disable unnecessary services to reduce risk
Suggestion	General	System not hardened fully	The system is not fully hardened → additional security measures (firewall, logging, IDS, etc.) are recommended

Task 4: Implement 3 to 5 items in the above table (task 3)

Fixing [DEB-0280]:

```
└─$ sudo apt install libpam-tmpdir -y
Installing:
  libpam-tmpdir

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1788
  Download size: 11.9 kB
  Space needed: 60.4 kB / 3,018 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 libpam-tmpdir amd64 0.11 [11.9 kB]
Fetched 11.9 kB in 3s (3,854 B/s)
```

```
Selecting previously unselected package libpam-tmpdir.
(Reading database ... 422488 files and directories currently
installed.)
Preparing to unpack .../libpam-tmpdir_0.11_amd64.deb ...
Unpacking libpam-tmpdir (0.11) ...
Setting up libpam-tmpdir (0.11) ...
Processing triggers for man-db (2.13.1-1) ...
```

Fixing [DEB-0810]:

```
└─$ sudo apt install apt-listbugs -y
Installing:
  apt-listbugs

Installing dependencies:
  distro-info  ruby-debian  ruby-gettext  ruby-locale  ruby-soap4r
ruby-sys-proctable  ruby-text  ruby-unicode  ruby-xmlparser

Suggested packages:
  reportbug  shunit2

Summary:
  Upgrading: 0, Installing: 10, Removing: 0, Not Upgrading: 1784
  Download size: 732 kB
  Space needed: 6,427 kB / 3,010 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ruby-debian
amd64 0.3.12 [20.3 kB]
```

```
Get:3 http://kali.download/kali kali-rolling/main amd64 ruby-text all
1.3.1-1 [13.4 kB]

Get:5 http://kali.download/kali kali-rolling/main amd64 ruby-xmlparser
amd64 0.7.3-7 [75.7 kB]

Get:6 http://kali.download/kali kali-rolling/main amd64 ruby-soap4r
all 2.0.5-9 [180 kB]

Get:7 http://http.kali.org/kali kali-rolling/main amd64 ruby-unicode
amd64 0.4.4.5-1+b3 [83.5 kB]

Get:8 http://kali.download/kali kali-rolling/main amd64 distro-info
amd64 1.15 [19.2 kB]

Get:9 http://kali.download/kali kali-rolling/main amd64 apt-listbugs
all 0.1.47 [88.6 kB]

Get:10 http://kali.download/kali kali-rolling/main amd64 ruby-sys-
proctable all 1.3.0-1 [33.1 kB]

Get:2 http://mirror.kku.ac.th/kali kali-rolling/main amd64 ruby-locale
all 2.1.4-1 [89.2 kB]

Get:4 http://mirror.kku.ac.th/kali kali-rolling/main amd64 ruby-
gettext all 3.4.9-1 [129 kB]

Fetched 732 kB in 9s (77.2 kB/s)

Selecting previously unselected package ruby-debian.

(Reading database ... 422619 files and directories currently
installed.)

Preparing to unpack .../0-ruby-debian_0.3.12_amd64.deb ...

Unpacking ruby-debian (0.3.12) ...

…
```

Fixing [DEB-0811]:

```
└─$ sudo apt install apt-listchanges -y

Upgrading:

  debconf  debconf-i18n
```

```
Installing:
  apt-listchanges

Installing dependencies:
  python3-debconf

Suggested packages:
  default-mta  | mail-transport-agent

Summary:
  Upgrading: 2, Installing: 2, Removing: 0, Not Upgrading: 1782
  Download size: 493 kB
  Space needed: 591 kB / 2,998 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 debconf-i18n
all 1.5.92 [217 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 debconf all
1.5.92 [123 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 python3-
debconf all 1.5.92 [4,252 B]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 apt-
listchanges all 4.8+nmu1 [149 kB]
Fetched 493 kB in 2s (208 kB/s)
Retrieving bug reports... Done
Parsing Found/Fixed information... Done
Preconfiguring packages ...
Deferring configuration of apt-listchanges until /usr/bin/python3
and python's debconf module are available
```

```
(Reading database ... 424730 files and directories currently
installed.)

Preparing to unpack .../debconf-i18n_1.5.92_all.deb ...

…
```

Fixing [DEB-0831]:

```
└─$ sudo apt install needrestart -y

Installing:

  needrestart


Installing dependencies:

  libintl-perl  libintl-xs-perl  libmodule-find-perl  libproc-
processtable-perl  libsort-naturally-perl


Summary:

  Upgrading: 0, Installing: 6, Removing: 0, Not Upgrading: 1782

  Download size: 846 kB

  Space needed: 4,994 kB / 2,993 MB available


Get:2 http://kali.download/kali kali-rolling/main amd64 libintl-xs-
perl amd64 1.37-1 [16.0 kB]

Get:3 http://kali.download/kali kali-rolling/main amd64 libmodule-
find-perl all 0.17-1 [10.7 kB]

Get:4 http://http.kali.org/kali kali-rolling/main amd64 libproc-
processtable-perl amd64 0.637-1+b1 [42.3 kB]

Get:5 http://kali.download/kali kali-rolling/main amd64 libsort-
naturally-perl all 1.03-4 [13.1 kB]

Get:6 http://kali.download/kali kali-rolling/main amd64 needrestart
all 3.11-1 [68.6 kB]
```

```
Get:1 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libintl-
perl all 1.37-1 [696 kB]

Fetched 846 kB in 5s (182 kB/s)

Retrieving bug reports... Done

Parsing Found/Fixed information... Done

Selecting previously unselected package libintl-perl.

(Reading database ... 424797 files and directories currently
installed.)

…
```

Fixing [DEB-0880]:

```
└─$ sudo apt install fail2ban -y


Installing:

  fail2ban


Installing dependencies:

  python3-systemd


Suggested packages:

  mailx  system-log-daemon  monit


Summary:

  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1782

  Download size: 510 kB

  Space needed: 2,602 kB / 2,987 MB available


Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-
systemd amd64 235-1+b7 [43.3 kB]
```

```
Get:2 http://kali.download/kali kali-rolling/main amd64 fail2ban all
1.1.0-9 [467 kB]

Fetched 510 kB in 3s (198 kB/s)

Retrieving bug reports... Done

Parsing Found/Fixed information... Done

Selecting previously unselected package python3-systemd.

(Reading database ... 425277 files and directories currently
installed.)

Preparing to unpack .../python3-systemd_235-1+b7_amd64.deb ...

Unpacking python3-systemd (235-1+b7) ...

Selecting previously unselected package fail2ban.

Preparing to unpack .../fail2ban_1.1.0-9_all.deb ...

Unpacking fail2ban (1.1.0-9) ...

Setting up python3-systemd (235-1+b7) ...

Setting up fail2ban (1.1.0-9) ...

update-rc.d: We have no instructions for the fail2ban init script.

update-rc.d: It looks like a network service, we disable it.

fail2ban.service is a disabled or a static unit, not starting it.

Processing triggers for kali-menu (2025.4.3) ...

Processing triggers for man-db (2.13.1-1) ...

Scanning processes...

Scanning linux images...


Running kernel seems to be up-to-date.


No services need to be restarted.
```

```
No containers need to be restarted.


No user sessions are running outdated binaries.


No VM guests are running outdated hypervisor (qemu) binaries on this
host.


┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable fail2ban


Synchronizing state of fail2ban.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
Created symlink '/etc/systemd/system/multi-
user.target.wants/fail2ban.service' →
'/usr/lib/systemd/system/fail2ban.service'.


┌──(kali㉿kali)-[~]
└─$ sudo systemctl start fail2ban
```

Task 5 (optional): Produce readable report for lynis

You can use ansi2html or this github https://github.com/d4t4king/lynis-report-converter

Summarize your steps :

- to build/install tools
- commands to create report.

Answer:

1. Steps to build/install the tool
    - Install required dependencies:
      ```
      sudo apt install -y git perl make wget htmldoc \
      libxml-writer-perl libarchive-zip-perl libjson-perl
      ```

- Install required dependencies:
```
cd /tmp
git clone https://github.com/d4t4king/lynis-report-converter.git
cd lynis-report-converter
```
- Clone the repository:
```
cd /tmp
git clone https://github.com/d4t4king/lynis-report-converter.git
cd lynis-report-converter
```
- Install additional Perl modules (required for full features like Excel/PDF):
```
# HTML::HTMLDoc
wget http://search.cpan.org/CPAN/authors/id/M/MF/MFRANKL/HTML-HTMLDoc-0.10.tar.gz
tar xvf HTML-HTMLDoc-0.10.tar.gz
cd HTML-HTMLDoc-0.10
perl Makefile.PL
make
sudo make install
cd ..

# Excel::Writer::XLSX
wget http://search.cpan.org/CPAN/authors/id/J/JM/JMCNAMARA/Excel-Writer-XLSX-0.95.tar.gz
tar xvf Excel-Writer-XLSX-0.95.tar.gz
cd Excel-Writer-XLSX-0.95
perl Makefile.PL
make
sudo make install
```

2. Commands to create report
    - Copy Lynis report file (avoid permission issues):
    ```
    sudo cp /var/log/lynis-report.dat ~/lynis-report.dat
    ```
    - Generate HTML report
    ```
    perl lynis-report-converter.pl -i ~/lynis-report.dat -o report.html
    ```
    - View the report
    ```
    xdg-open report.html
    ```