

Coursework Project:

# **“Defending an Online System”**

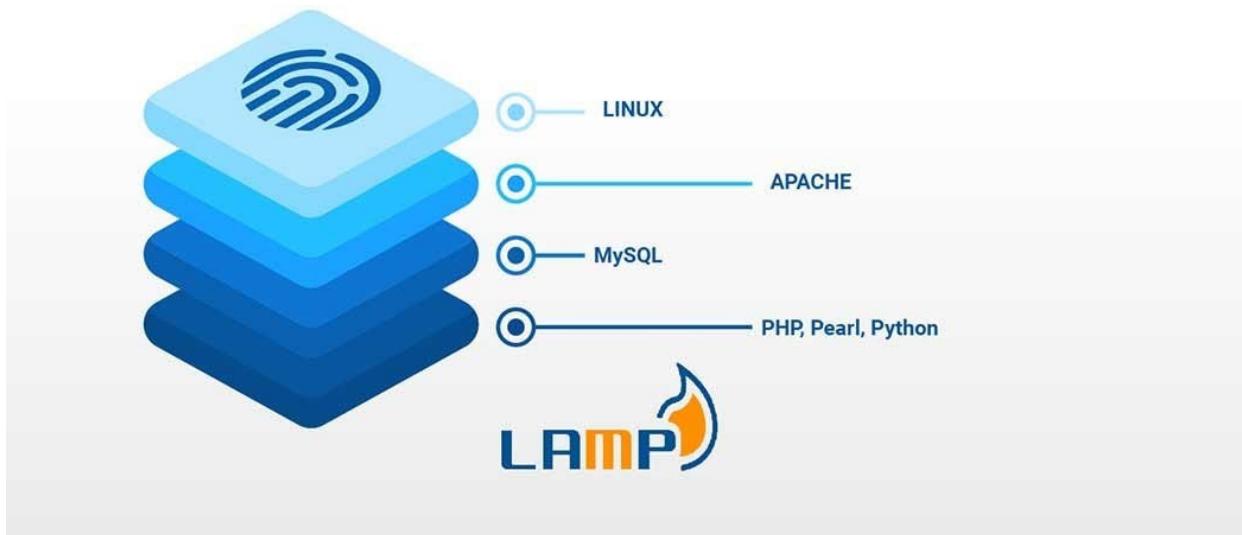


- 1. Research a working cyber security system 3**
  - 1.1 I can investigate a working system to determine the main components 3
  - 1.2 I can explain the main system components [3](#)
  - 1.3 I can describe how the components fit together [4](#)
  - 1.4 I can make detailed notes of my findings 5
  - 1.5 I can present my notes to an audience for feedback 6
  - 1.6 I can list some of the key objectives of the system I will design 6
- 2. Plan to build a cyber safe web server 7**
  - 2.1 I can make a working skeletal plan of a system 8
  - 2.2 I can set clear objectives and outcomes to build a system against 9
  - 2.3 I can list the main safety features for success 9
  - 2.4 I can explain the main hardware requirements needed 10
  - 2.5 I can explain the main software aspects of the system 10
  - 2.6 I can make a final plan for a system 10
- 3. Develop a cyber safe web server 12**
  - 3.1 A system in terms of specifications 12
  - 3.2 The specification in terms of performance needs 12
  - 3.3 Describe the way a web site functions 13
  - 3.4 Describe the main pieces of software required 13
  - 3.5 Describe the configuration settings for a working system 14
  - 3.6 We can recommend final adjustments before going live 24
- 4. Test the system against common threats [37](#)**
  - 4.1 I can develop a basic test regime 37
  - 4.2 I can explain the purpose of the main test procedures [38](#)
  - 4.3 I can explain the expected results from the test [38](#)
  - 4.4 I can describe the test results and what they mean 39
  - 4.5 We can adjust the system in light of test results 65
  - 4.6 We can document the test results for third party support people 66
- 5. Evaluate the effectiveness of the system 69**
  - 5.1 I can analyse the results in terms of the objectives 69
  - 5.2 I can evaluate some of the features of the system and their purpose 69
  - 5.3 I can justify some design decisions in terms of objectives 70
  - 5.4 I can analyse possible improvements to the system based on usage 71
  - 5.5 I can analyse the effectiveness of the system by viewing the different log files 87
  - 5.6 I can recommend improvements to the system for future-proofing 88

## **1.Research a working cyber security system**

### **1.1 I can investigate a working system to determine the main components**

LAMP is a server-based software stack designed for websites and web applications. LAMP is an acronym that stands for: Linux, Apache, MySQL and PHP.



### **1.2 I can explain the main system components**

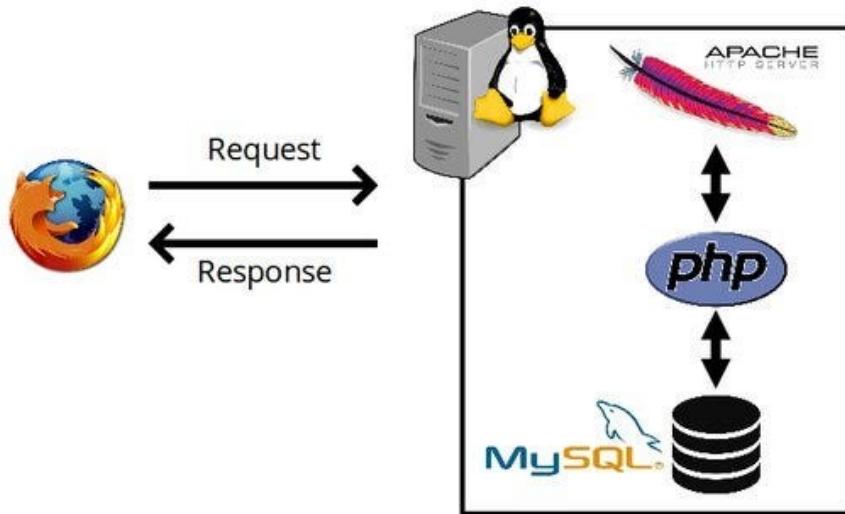
LAMP elements:

1. Linux is used as the OS on the server, often various Ubuntu and Debian distributions.
2. Apache is a web server. It processes all requests to site pages and issues appropriate responses. Apache HTTP Server is a free web server software package made available under an open-source license and offers a secure and extendable Web server that's in sync with current HTTP standards. Web servers are responsible for translating from web browsers to their correct website.
3. MySQL is a DBMS (database management system). MySQL is a relational database management system used to store application data. MySQL stores details that can be queried by scripting to construct a website. MySQL usually sits on top of the Linux layer alongside Apache.
4. PHP is a scripting language for generating pages. The PHP open-source scripting language works with Apache to create dynamic web pages. We cannot use HTML to perform dynamic processes such as pulling data out of a database. To provide this type of functionality, we drop PHP code into the parts of a page that you want to be dynamic. Websites and Web Applications run within this layer. PHP is designed for efficiency. It makes programming easier and allowing to write new code, hit refresh, and immediately see the resulting changes without the need for compiling.

### 1.3 I can describe how the components fit together

LAMP has classic layered architecture, with Linux at the lowest level.

## LAMP architecture



The next layer is Apache and MySQL, followed by PHP.

#### Request Flow:

1. A user makes a request by accessing a web page through their browser.
2. The request is sent to the Apache web server running on the Linux operating system.
3. Apache, based on its configuration, may handle static content directly or forward requests for dynamic content to the PHP interpreter.
4. PHP processes the request, interacting with the MySQL database if necessary to fetch or update data.
5. The processed content is returned to Apache, which then sends the response back to the user's browser.

#### Database Interaction:

- PHP scripts use MySQL queries to interact with the database.
- MySQL processes these queries, retrieves or modifies data, and sends the results back to PHP.
- PHP then uses this data to generate dynamic content for the web page.

## **Communication:**

Communication between components happens via protocols like HTTP (between the browser and Apache) and MySQL protocol (between PHP and MySQL).

- Inter-process communication is essential for the seamless flow of data and requests throughout the stack.

## **Integration:**

- Configuration files for each component (e.g., Apache's httpd.conf, MySQL's my.cnf, and PHP's php.ini) define how these components behave and interact.
- Proper integration ensures that each component plays its role effectively in serving web applications.

In summary, the LAMP stack is a cohesive unit where Linux provides the operating system, Apache serves as the web server, MySQL manages the database, and PHP handles server-side scripting. These components work together to deliver dynamic, database-driven web applications to end-users.

## **1.4 I can make detailed notes of my findings**

Advantages of assembly:

1. assembly is great for quick application deployment due to simple configuration, but it still provides few features in terms of scalability and component isolation.
2. LAMP installation (Linux + Apache + MySQL + PHP / Perl / Python) is a fairly widely used option for configuring servers with Ubuntu;
3. there are a large number of applications that are open source and written using the LAMP application stack. For example, popular LAMP applications: wiki encyclopedias, content management systems (CMS) and management applications, for example, phpMyAdmin;
4. flexibility in selecting databases, web servers and script languages;
5. uses sets of open software, which significantly speeds up the development process;
6. PostgreSQL and SQLite serve as an actual replacement for MySQL. Python, Perl and Ruby can be substituted for PHP. And Nginx, Cherokee and Lighttpd are an alternative to Apache;
7. tasksel is used for fast LAMP installation. Tasksel is a Debian/Ubuntu tool that installs multiple dependent packages on your system as a single task.

Disadvantages of LAMP:

1. The application and database use the same server resources (CPU, memory, I/O, etc.), which results in poor performance and makes it difficult to determine the source (application or database) of this problem.
2. There are also obstacles in the implementation of horizontal scaling.

## **1.5 I can present my notes to an audience for feedback**

Open-source alternatives are:

1. **LEMP**(Linux, NGINX, MySQL/MariaDB, PHP/Perl/Python)
2. **LAPP**(Linux, Apache, PostgreSQL, PHP)
3. **LEAP**(Linux, Eucalyptus, AppScale, Python)
4. **LLMP**(Linux, Lighttpd, MySQL/MariaDB, PHP/Perl/Python)

While non-open source alternatives include:

1. **WAMP**(Windows, Apache, MySQL/MariaDB, PHP/Perl/Python)
2. **WIMP**(Windows, Internet Information Services, MySQL/MariaDB, PHP/Perl/Python)
3. **MAMP**(Mac OS x, Apache, MySQL/MariaDB, PHP/Perl/Python)

## **1.6 I can list some of the key objectives of the system I will design**

Linux, Apache, MySQL and PHP, all of them add something unique to the development of high-performance web applications. Originally popularized from the phrase Linux, Apache, MySQL, and PHP, the acronym LAMP now refers to a generic software stack model.

The key objectives of system will be to follow the fundamental concept in information security - CIA triad that consists of three core principles: Confidentiality, Integrity, and Availability. Here's a brief overview of each component:

- **Confidentiality:**
  - Confidentiality involves protecting data from unauthorized access, disclosure, or exposure.
  - Methods to achieve confidentiality include encryption, access controls, and secure communication protocols.
- **Integrity:**
  - The goal is to prevent unauthorized or malicious alteration of data.
  - Techniques to maintain integrity include checksums, digital signatures, access controls, and version control.

- **Availability:**

- Availability involves preventing and mitigating disruptions to services and ensuring timely access to data.
- Measures to support availability include redundant systems, backups, disaster recovery plans, and fault-tolerant architectures.

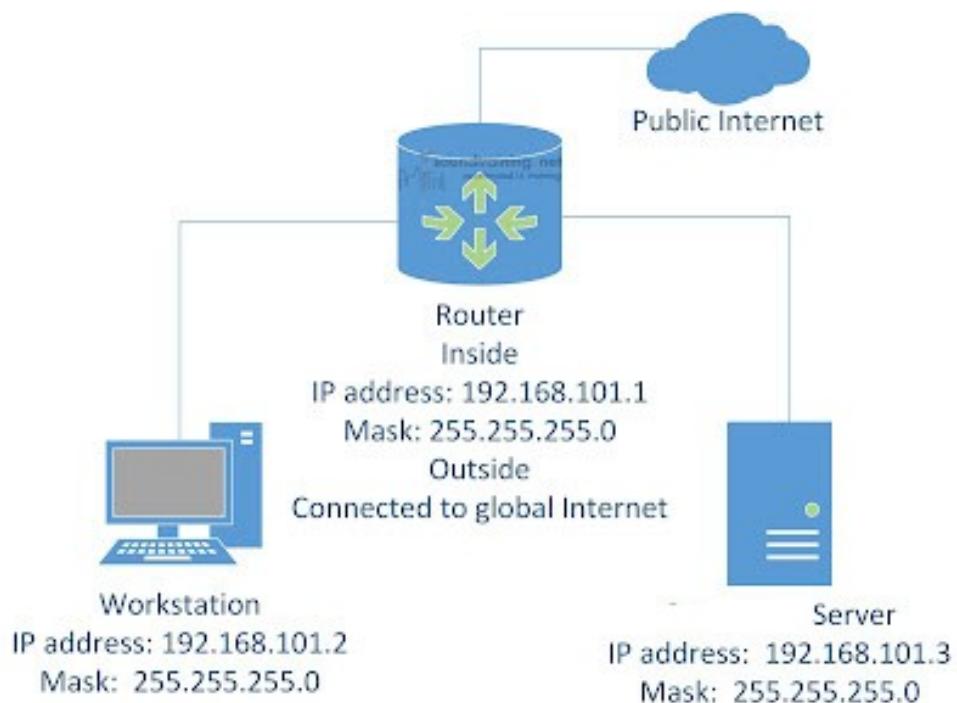
## **2. Plan to build a Cyber safe website or server**

### **2.1 I can make a working skeletal plan of a system**

Key objectives of the system LAMP are:

1. **Optimal Access Speed:** Achieve fast page load times through efficient code, optimized database queries, and proper server resource allocation. Utilize testing facilities to gauge and improve access speed.
2. **Security Against Common Threats:** Implement robust security measures to protect against a defined percentage (X%) of common cyber threats. Regularly update and patch software components to address vulnerabilities. Root Access Security: Ensure the LAMP system is secure against unauthorized root access by implementing strong authentication mechanisms, monitoring user activities, and restricting privileged access.
3. **Compatibility with Current Technologies:** Stay abreast of emerging technologies and ensure compatibility with the latest standards. Regularly update and adapt the LAMP stack components to integrate seamlessly with modern technologies.

**The visual representing of working skeletal plan of a system is:**



We need to make sure that only authorized people can access our server by locking it behind a door, and trying to place the server in a safe place.

LAMP stands for Linux, Apache, MySQL, and PHP/Python/Perl.

## 2.2 I can set clear objectives and outcomes to build a system against

We think that objectives for building the LAMP system:

- **Prevent Injection Attacks:** Implement robust input validation and secure coding practices to thwart injection attacks and protect the integrity of the system.
- **Mitigate Spam Postings:** Develop mechanisms to detect and prevent spam postings, safeguarding the site's content and user experience.
- **Block Unauthorized PHP Mail Server Use:** Configure the system to prevent unauthorized access and usage as a PHP mail server, ensuring the server's resources are not exploited for malicious purposes.

For our opinion, outcomes indicating system success:

- **Log Exclusion of Specific IP Addresses:** Successful configuration to block undesirable IP addresses, as evidenced by their absence in log files.

**Effective Access Denial:** Log entries reflecting unsuccessful attempts to access restricted areas, demonstrating the system's ability to thwart unauthorized access.

## 2.3 I can list the main safety features that will need to be addressed for success

To ensure the success and security of a LAMP-based site, several key safety features must be addressed. Firstly, robust user authentication and authorization mechanisms should be implemented to prevent impersonation and unauthorized access. Configuring well-defined roles and permissions ensures users only have access to the resources they need, preventing abuse.

Database and web server security is paramount to prevent attacks and data theft. Employing encryption, input validation, and secure coding practices helps safeguard against SQL injection and other vulnerabilities. Regular software updates and patches are crucial to address emerging threats.

Addressing the challenge of user-friendly yet secure passwords is essential. Implementing a strong password policy, as exemplified by Moodle, ensures that users adopt secure practices without compromising usability. Regularly educating users on security best practices further enhances the site's resilience against hacking attempts.

In summary, the success of a LAMP-based site relies on a holistic approach to security encompassing user authentication, database and server protection, and a sensible password policy that balances security with user convenience. Continuous monitoring, updates, and user education are key elements in maintaining a secure online environment.

## **2.4 I can explain the main hardware requirements needed**

1. I can install and run Ubuntu 22.04 on any system with a 2GHz, 2-core 64-bit processor, 4GBs of RAM, and 25GBs of storage.
2. The machines that will run the Management Server and MySQL database must meet the following requirements : operating system: CentOS/RHEL 7.2+ or Ubuntu 16.04(.2) or higher , 64-bit x86 CPU (more cores results in better performance), 4 GB of memory, 250 GB of local disk, (more results in better capability; 500 GB recommended), at least 1 NIC, statically allocated IP address,fully qualified domain name as returned by the hostname command.
3. I can install and run PHP with processor: x86 or x64, RAM : 512 MB (minimum), 1 GB (recommended),Hard disk: up to 200 MB of available space may be required. However, 50 MB free space is required in boot drive even if you are installing in other drive.

## **2.5 I can explain the main software aspects of the system**

The main software aspects of the LAMP system comprise the Linux operating system, Apache web server, MySQL database, and PHP scripting language. The choice of specific versions impacts system functionality and security. For example, PHP 7 is required in the latest releases of applications like WordPress. Understanding the trade-offs between newer versions, stability, and security is crucial. Debian-based Linux systems, like Ubuntu, update components such as the kernel, and LTS versions provide long-term support with stability, although they may not feature the latest Apache or PHP versions. Balancing the advantages of newer software against the need for a stable and secure environment is key, especially when considering dependencies within the system.

## **2.6 I can make a final plan for a system**

Our project will consist of 6 main stages:

1. Research a working cyber security system (LAMP).
2. Plan to build a cyber safe web server.
3. Installation of the components of the server.
4. Develop a cyber safe web server.
5. Test the system against common threats.
6. Evaluate the effectiveness of the system

Time plan for building my LAMP server:

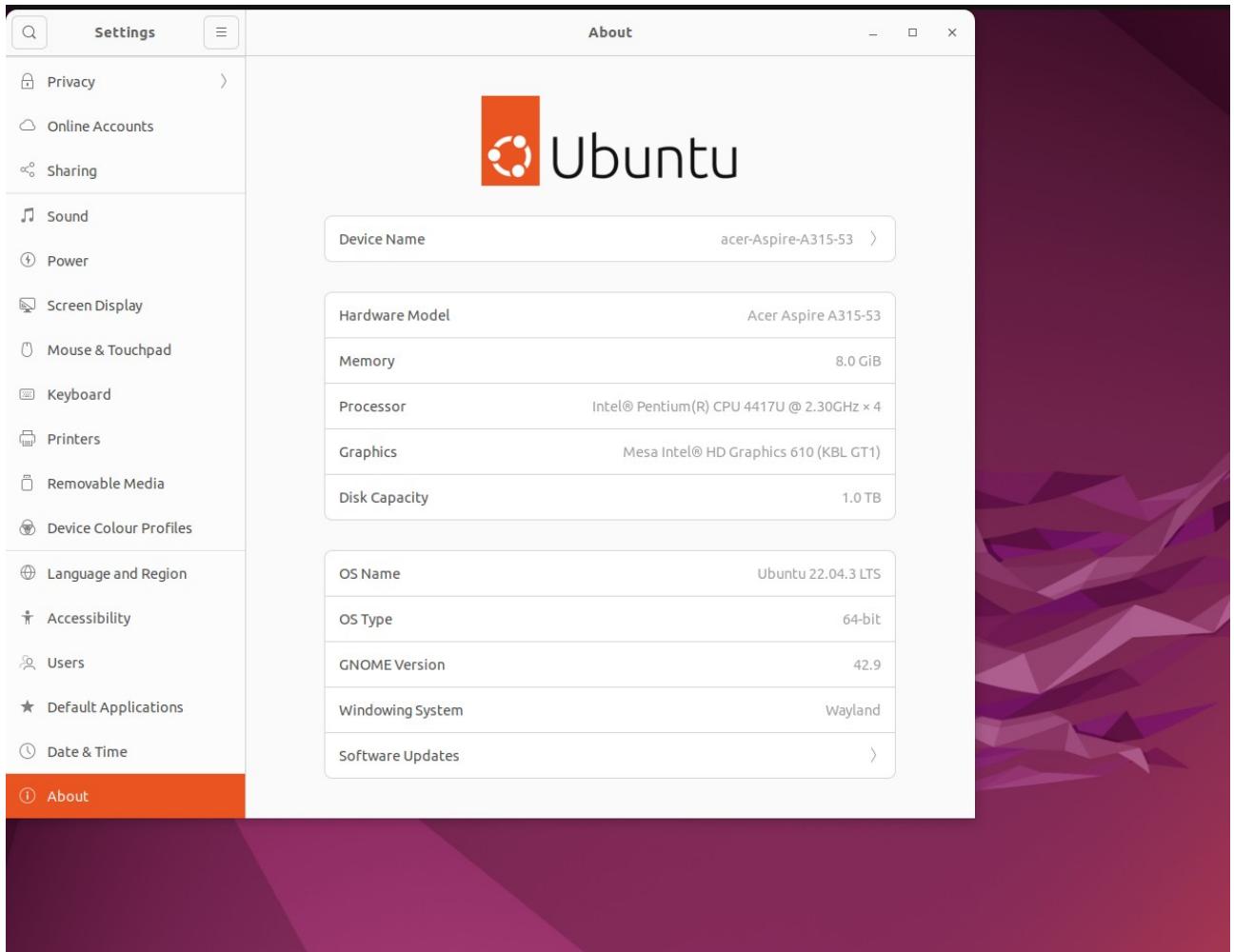
| Name of Task | Week 1    | Week 2 | Week 3 | Week 4 | Week 5 |
|--------------|-----------|--------|--------|--------|--------|
| Researching  | Week<br>1 |        |        |        |        |
| Planning     |           | Week2  |        |        |        |
| Installation |           | Week2  |        |        |        |
| Developing   |           |        | Week3  |        |        |
| Testing      |           |        | Week3  | Week4  |        |
| Evaluating   |           |        |        | Week4  | Week5  |

### 3. Develop a cyber safe web site or server

#### 3.1 A system in terms of specifications:

For this project I used Ubuntu 22.04 because it is a Long-Term Support (LTS) release and will receive ongoing app updates and critical security fixes for five years from release.

I installed Ubuntu 22.04 LTS on the PC acer – Aspire – A315 – 53 according the recommended system requirements for Ubuntu 22.04:



My machine also meet the recommended system requirements for running Apache, MySQL, PHP (LAMP) Stack.

#### 3.2 The specification in terms of performance needs

The LAMP server offers a complete flexibility to build and deploy applications considering unique business needs. LAMP technology is secure and stable. It possesses a powerful security feature to mitigate vulnerable attacks and if any error occurs it can be fixed quickly in a financially savvy approach.

### **3.3 Describe the way a web site functions**

I had built a flexible foundation for serving PHP websites and applications, using Apache as a web server and MySQL as a database system.

### **3.4 Describe the main pieces of software required**

The main pieces of software for this project are:

1. A “LAMP” stack is a group of open source software that is typically installed together in order to enable a server to host dynamic websites and web apps written in PHP.
2. Uncomplicated Firewall is an easy-to-use program for managing a netfilter firewall. It uses a command-line interface consisting of a small number of simple commands and uses iptables for configuration.
3. Mod\_security is a web application firewall (WAF) which can be installed as an additional module for Apache. It can be used to protect the web server from numerous attacks like SQL injections, session hijacking, cross site scripting, bad user agents and many others.
4. Fail2Ban is an intrusion prevention framework written in Python that protects Linux systems and servers from brute-force attacks. Setting up Fail2Ban provides brute-force protection for SSH on your Linode. It also allows you to monitor the strength of brute-force attacks in regards to the number of authentication attempts.
5. Anti-Virus Protection ClamAV. Scanning with ClamAV is simple and can be invoked by running the clamscan command in the terminal.
6. MySAT for audit the security of my MySQL server. MySAT performs several test to analyze database configurations and security policies. MySAT can help to assess and therefore increase MySQL database security.
7. Lynis as an extensible security audit tool for computer systems running Linux, FreeBSD, macOS, OpenBSD, Solaris, and other Unix derivatives. It assists system administrators and security professionals with scanning a system and its defenses, with the final goal being system hardening.
8. Chkrootkit is also another free, open-source rootkit detector that locally checks for signs of a rootkit on Unix-like systems. It helps to detect hidden security holes.  
The chkrootkit package consists of a shell script that checks system binaries for rootkit modification and a number of programs that check various security issues.
9. RootKit Hunter is a free, open-source, powerful, simple to use, and well-known tool for scanning backdoors, rootkits, and local exploits on POSIX-compliant systems such as Linux. As the name implies, it is a rootkit hunter, a security monitoring and analyzing tool that thoroughly inspects a system to detect hidden security holes.

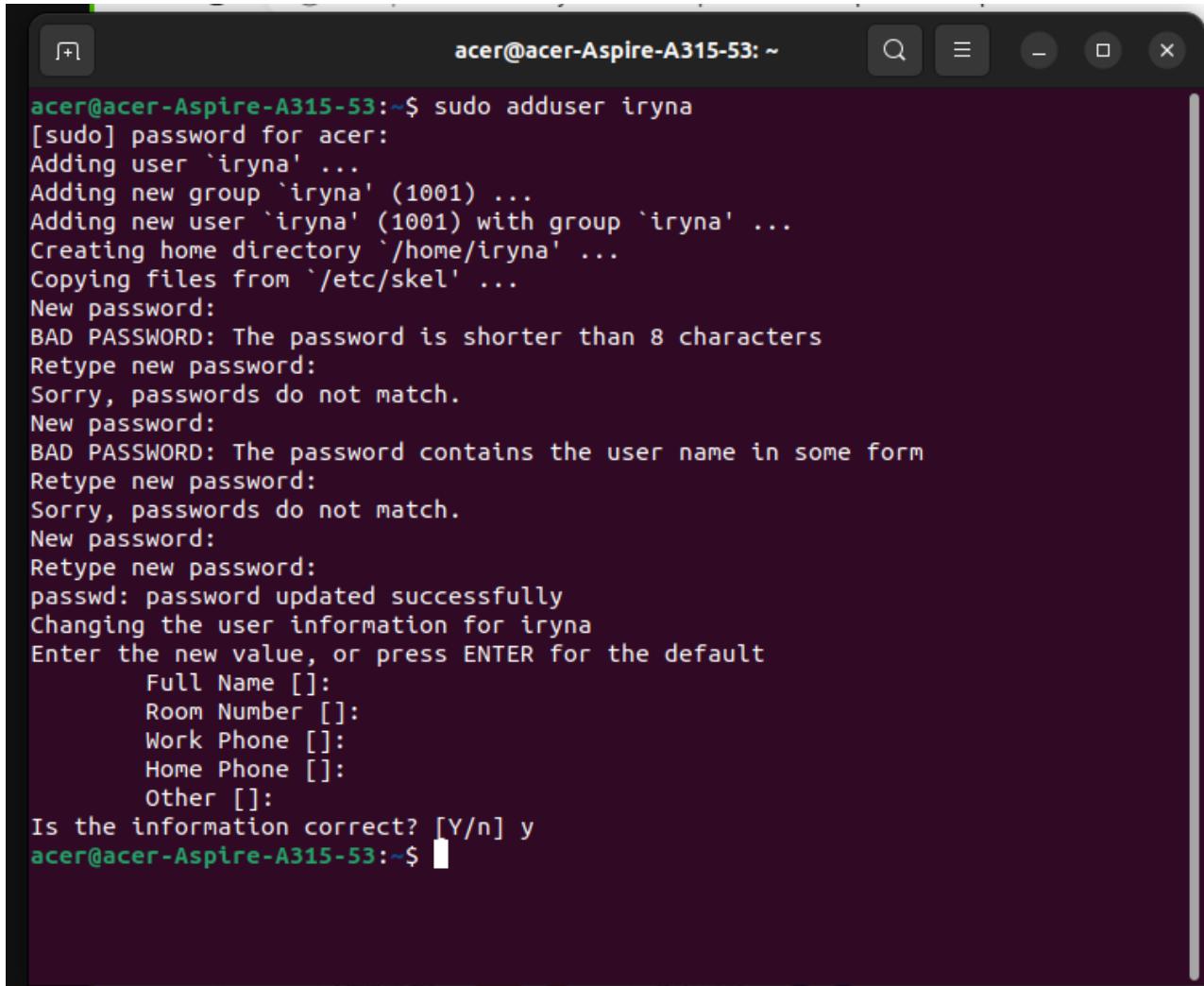
10. Nmap (an acronym of Network Mapper) is an open-source command-line utility to securely manage the network. Nmap command has an extensive list of options to deal with security auditing and network exploration.

### 3.5 Describe the configuration settings for a working system

#### Initial Server Setup with Ubuntu 22.04

These steps will increase the security and usability of server:

Step 1 — Creating a New User



The screenshot shows a terminal window titled "acer@acer-Aspire-A315-53: ~". The user is running the command "sudo adduser iryna". The terminal output is as follows:

```
acer@acer-Aspire-A315-53:~$ sudo adduser iryna
[sudo] password for acer:
Adding user `iryna' ...
Adding new group `iryna' (1001) ...
Adding new user `iryna' (1001) with group `iryna' ...
Creating home directory `/home/iryna' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for iryna
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
acer@acer-Aspire-A315-53:~$
```

Step 2 — Setting Up a Firewall

Ubuntu 22.04 servers can use the UFW firewall to ensure only connections to certain services are allowed. I set up a basic firewall using this application.

```
acer@acer-Aspire-A315-53:~$ ufw app list
ERROR: In order to run this script, you need to be root
acer@acer-Aspire-A315-53:~$ sudo ufw app list
[sudo] password for acer:
Available applications:
 Apache
 Apache Full
 Apache Secure
 CUPS
acer@acer-Aspire-A315-53:~$ ufw allow OpenSSH
ERROR: In order to run this script, you need to be root
acer@acer-Aspire-A315-53:~$ sudo ufw allow OpenSSH
ERROR: Could not find a profile matching 'OpenSSH'
acer@acer-Aspire-A315-53:~$ sudo ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)
acer@acer-Aspire-A315-53:~$ ufw enable
ERROR: In order to run this script, you need to be root
acer@acer-Aspire-A315-53:~$ sudo ufw enable
Firewall is active and enabled on system startup
acer@acer-Aspire-A315-53:~$ ufw status
ERROR: In order to run this script, you need to be root
acer@acer-Aspire-A315-53:~$ sudo ufw status
Status: active
```

## Install Linux, Apache, MySQL, PHP (LAMP) Stack on Ubuntu 22.04

### Step 1 — Installing Apache and Updating the Firewall:

I started by updating the package manager cache and then, installed Apache. Once the installation is finished, I adjusted my firewall configuration tool is called Uncomplicated Firewall (UFW) settings to allow HTTP traffic.

To only allow traffic on port 80, I used the Apache profile.

```
acer@acer-Aspire-A315-53:~$ To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
acer@acer-Aspire-A315-53:~$ sudo apt update  
[sudo] password for acer:  
Hit:1 http://gb.archive.ubuntu.com/ubuntu jammy InRelease  
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]  
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]  
Hit:4 http://gb.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Fetched 229 kB in 1s (159 kB/s)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
4 packages can be upgraded. Run 'apt list --upgradable' to see them.  
acer@acer-Aspire-A315-53:~$ sudo apt install apache2  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap  
Suggested packages:  
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom  
The following NEW packages will be installed:  
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap  
0 to upgrade, 8 to newly install, 0 to remove and 4 not to upgrade.  
Need to get 1,919 kB of archives.  
After this operation, 7,718 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

```
acer@acer-Aspire-A315-53:~$ sudo ufw app list  
[sudo] пароль до acer:  
Доступні програми:  
  Apache  
  Apache Full  
  Apache Secure  
  CUPS  
acer@acer-Aspire-A315-53:~$ sudo ufw allow in "Apache"  
Пропуск додавання правила що існує  
Пропуск додавання правила що існує (v6)  
acer@acer-Aspire-A315-53:~$ sudo ufw status  
Стан: активний  
  
До          Дія      З  
--          ---      -  
Apache      ALLOW    Anywhere  
Anywhere    ALLOW    94.197.150.147  
22/tcp      ALLOW    Anywhere  
Apache (v6)  ALLOW    Anywhere (v6)  
22/tcp (v6) ALLOW    Anywhere (v6)  
  
acer@acer-Aspire-A315-53:~$ ip addr show ens3 | grep inet | awk '{ print $2; }'  
| sed 's/\.*$//'  
Device "ens3" does not exist.  
acer@acer-Aspire-A315-53:~$ curl http://icanhazip.com  
94.197.150.147  
acer@acer-Aspire-A315-53:~$
```

```
[n] Unpacking libaprutil1-ldap_1.6.1-5ubuntu4.22.04.2_amd64.deb ...
Selecting previously unselected package apache2-bin.
Preparing to unpack .../4-apache2-bin_2.4.52-1ubuntu4.7_amd64.deb ...
Unpacking apache2-bin (2.4.52-1ubuntu4.7) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../5-apache2-data_2.4.52-1ubuntu4.7_all.deb ...
Unpacking apache2-data (2.4.52-1ubuntu4.7) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../6-apache2-utils_2.4.52-1ubuntu4.7_amd64.deb ...
Unpacking apache2-utils (2.4.52-1ubuntu4.7) ...
Selecting previously unselected package apache2.
Preparing to unpack .../7-apache2_2.4.52-1ubuntu4.7_amd64.deb ...
Unpacking apache2 (2.4.52-1ubuntu4.7) ...
Setting up libapr1:amd64 (1.7.6-8ubuntu0.22.04.1) ...
Setting up apache2-data (2.4.52-1ubuntu4.7) ...
Setting up libaprutil1:amd64 (1.6.1-Subuntu4.22.04.2) ...
Setting up libaprutil1-ldap:amd64 (1.6.1-Subuntu4.22.04.2) ...
Setting up libaprutil1-db:amd64 (1.6.1-Subuntu4.22.04.2) ...
Setting up apache2-utils (2.4.52-1ubuntu4.7) ...
Setting up apache2-bin (2.4.52-1ubuntu4.7) ...
Setting up apache2 (2.4.52-1ubuntu4.7) ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module authn_dbsql.
Enabling module authn_file.
Enabling module authn_socache.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libfc-bin (2.35-0ubuntu3.6) ...
acer@acer-Aspire-A315-53: ~
```

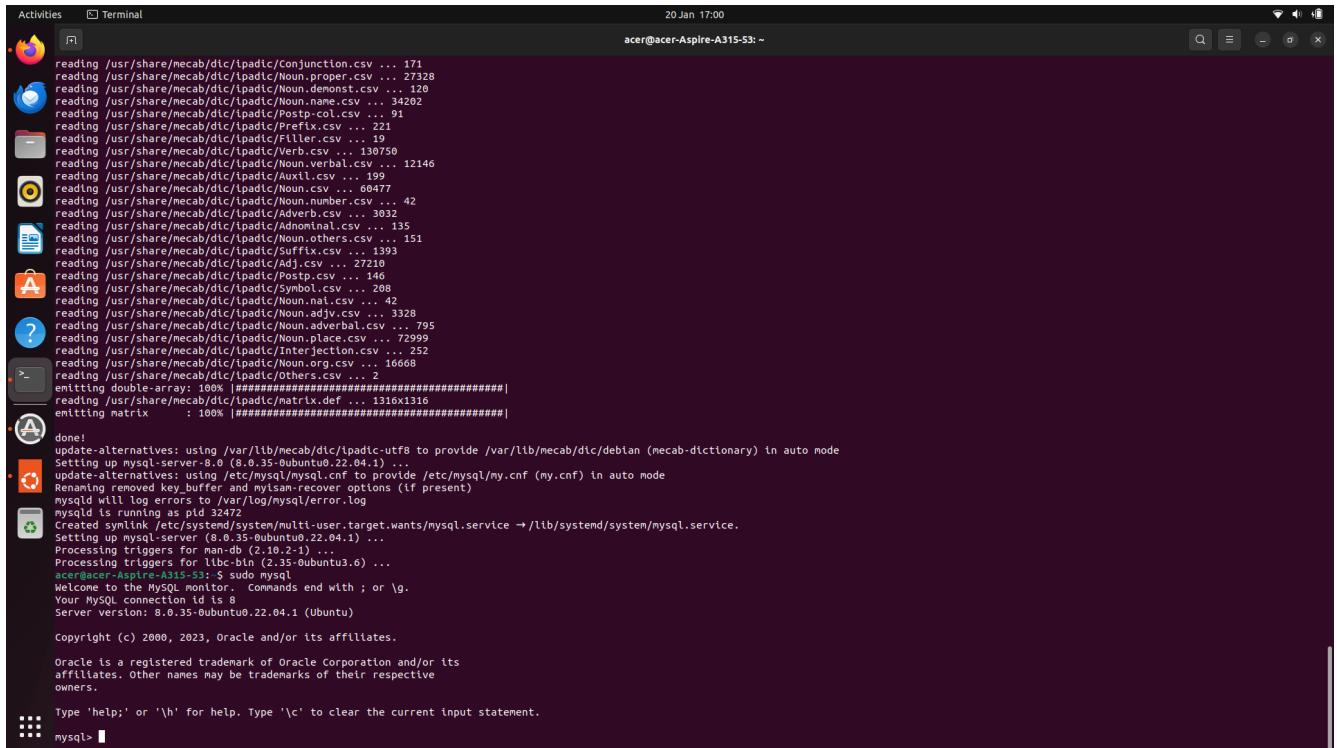
## Step 2 — Installing MySQL

Now that I had a web server up and running, I used apt to acquire and install MySQL:

```
Activities Terminal 20 Jan 16:57
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcache-clean.service → /lib/systemd/system/apache-htcache-clean.service.
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for liblc-bin (2.35-0ubuntu3.6) ...
acer@acer-Aspire-A315-53:~$ sudo ufw app list
Available applications:
Apache
Apache Full
Apache Secure
CUPS
[...] (redacted)
acer@acer-Aspire-A315-53:~$ sudo ufw allow in "Apache"
#sudo: ufw: command not found
acer@acer-Aspire-A315-53:~$ #sudo ufw allow in "Apache"
acer@acer-Aspire-A315-53:~$ sudo ufw status
Status: inactive
acer@acer-Aspire-A315-53:~$ ^C
acer@acer-Aspire-A315-53:~$ sudo ufw allow in "Apache"
Rules updated
Rules updated (v0)
acer@acer-Aspire-A315-53:~$ sudo ufw status
Status: inactive
acer@acer-Aspire-A315-53:~$ ^[[200~lp addr show ens3 | grep inet | awk '{ print $2; }' | sed 's/.*://'
sed: -e expression #1, char 10: unknown option to 's'
lp: command not found
acer@acer-Aspire-A315-53:~$ ip addr show ens3 | grep inet | awk '{ print $2; }' | sed 's/.*://'
Device "ens3" does not exist.
acer@acer-Aspire-A315-53:~$ ip addr show ens3 | grep inet | awk '{ print $2; }' | sed 's/.*://'
Device "ens3" does not exist.
acer@acer-Aspire-A315-53:~$ curl http://icanhazip.com
Command "curl" not found, but can be installed with:
sudo snap install curl # version 8.1.0-ubuntu1.14
See 'snap info curl' for additional versions.
acer@acer-Aspire-A315-53:~$ ^C
acer@acer-Aspire-A315-53:~$ sudo snap install curl # version 8.1.2-1
curl/8.1.2 from Wouter van Bonnel (woutervb) [installed]
acer@acer-Aspire-A315-53:~$ curl http://icanhazip.com
94.197.150.147
acer@acer-Aspire-A315-53:~$ ^C
acer@acer-Aspire-A315-53:~$ sudo apt install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libatoi1 libfcgi-fast-perl libfcgi-perl libevent-core-2.1.7 libevent-pthreads-2.1.7 libfcgi-bin libfcgi-perl libfcgioldbl libhtml-template-perl libmecab2 libprotobuf-lite23 mecab-ipadic
meCab-ipadic-utf8 mecab-util mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server mysql-server-8.0 mysql-server-core-8.0
Suggested packages:
libfcgi-sharedache-perl mailx tinyca
The following NEW packages will be installed:
libatoi1 libfcgi-fast-perl libfcgi-perl libevent-core-2.1.7 libevent-pthreads-2.1.7 libfcgi-bin libfcgi-perl libfcgioldbl libhtml-template-perl libmecab2 libprotobuf-lite23 mecab-ipadic
meCab-ipadic-utf8 mecab-util mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server mysql-server-8.0 mysql-server-core-8.0
0 to upgrade, 20 to newly install, 0 to remove and 4 not to upgrade.
Need to get 29.3 MB of archives.
After this operation, 242 MB of additional disk space will be used.
Do you want to continue? [Y/n] [
```

When the installation is finished, I run a security script that comes pre-installed with MySQL. This script removed some insecure default settings and lock down access to your database system.

I run the following ALTER USER command to change the root user's authentication method to one that uses a password.



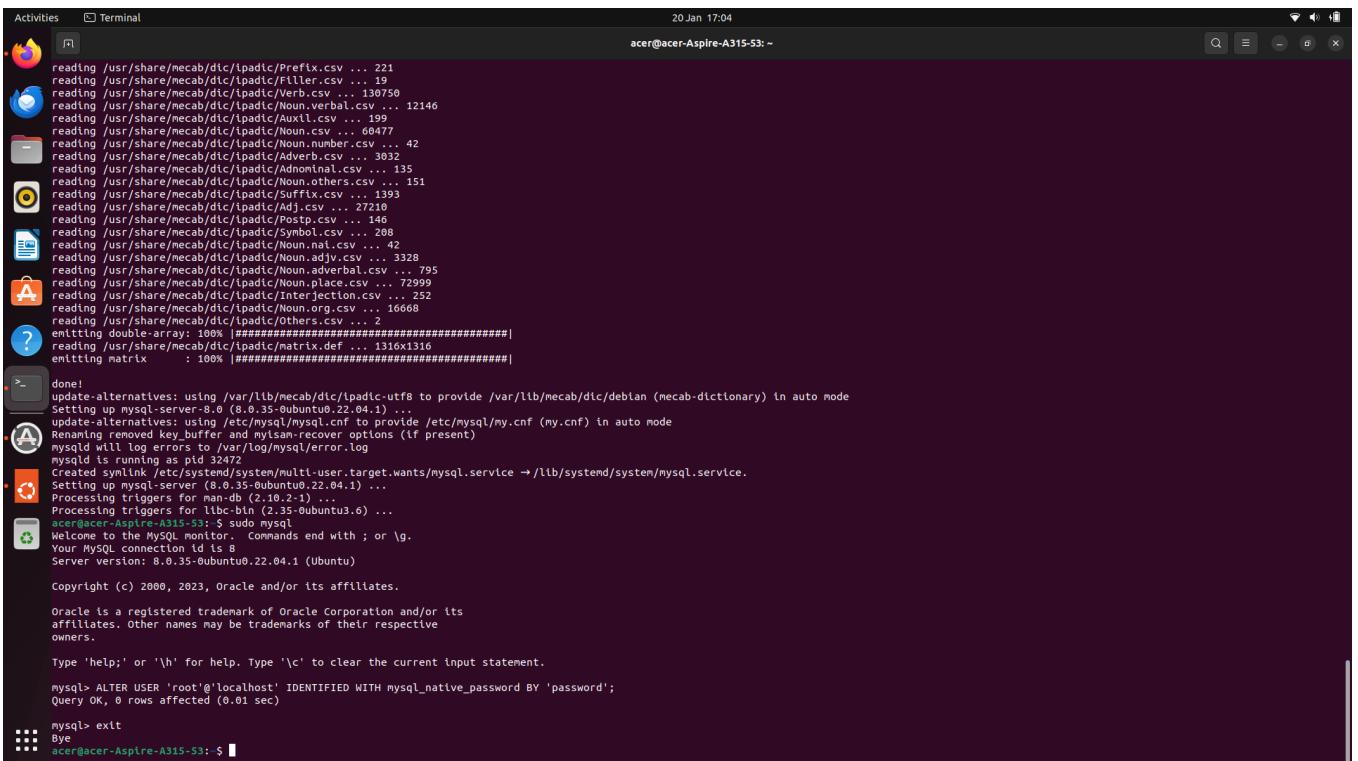
```
Activities Terminal 20 Jan 17:00 acer@acer-Aspire-A315-53: ~
reading /usr/share/mecab/dic/ipadic/Cjunction.csv ... 171
reading /usr/share/mecab/dic/ipadic/Noun_proper.csv ... 27328
reading /usr/share/mecab/dic/ipadic/Noun_nemawashi.csv ... 120
reading /usr/share/mecab/dic/ipadic/Noun_name.csv ... 34202
reading /usr/share/mecab/dic/ipadic/Postp_col.csv ... 91
reading /usr/share/mecab/dic/ipadic/Prefix.csv ... 221
reading /usr/share/mecab/dic/ipadic/Filler.csv ... 19
reading /usr/share/mecab/dic/ipadic/Verb.csv ... 130750
reading /usr/share/mecab/dic/ipadic/Noun_verbal.csv ... 12146
reading /usr/share/mecab/dic/ipadic/Auxil.csv ... 199
reading /usr/share/mecab/dic/ipadic/Noun_namida.csv ... 60477
reading /usr/share/mecab/dic/ipadic/Noun_nemawashi.csv ... 42
reading /usr/share/mecab/dic/ipadic/Adverb.csv ... 332
reading /usr/share/mecab/dic/ipadic/Adnominal.csv ... 135
reading /usr/share/mecab/dic/ipadic/Noun_others.csv ... 151
reading /usr/share/mecab/dic/ipadic/Suffix.csv ... 1393
reading /usr/share/mecab/dic/ipadic/Adj.csv ... 27210
reading /usr/share/mecab/dic/ipadic/Postp.csv ... 146
reading /usr/share/mecab/dic/ipadic/Symbol.csv ... 208
reading /usr/share/mecab/dic/ipadic/Noun_natal.csv ... 42
reading /usr/share/mecab/dic/ipadic/Advcl.csv ... 3328
reading /usr/share/mecab/dic/ipadic/Noun_adverbial.csv ... 795
reading /usr/share/mecab/dic/ipadic/Noun_place.csv ... 72999
reading /usr/share/mecab/dic/ipadic/Interjection.csv ... 252
reading /usr/share/mecab/dic/ipadic/Noun_org.csv ... 16668
reading /usr/share/mecab/dic/ipadic/Others.csv ... 2
emitting double-array: 100% #####| reading /usr/share/mecab/dic/ipadic/matrix.def ... 1316x1316
emitting matrix : 100% #####| reading /usr/share/mecab/dic/ipadic/matrix.def ... 1316x1316
done!
update-alternatives: using /var/lib/mecab/dic/ipadic-utf8 to provide /var/lib/mecab/dic/debian (mecab-dictionary) in auto mode
Setting up mysql-server-8.0 (8.0.35-0ubuntu0.22.04.1) ...
update-alternatives: using /etc/mysql/mysql.cnf to provide /etc/mysql/my.cnf (my.cnf) in auto mode
Renaming removed key_buffer and myisam-recover options (if present)
mysqld will log errors to /var/log/mysql/error.log
mysqld is running as pid 32472
Created symlink /etc/systemd/system/multi-user.target.wants/mysql.service → /lib/systemd/system/mysql.service.
Setting up mysql-server (8.0.35-0ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for liblc-bin (2.35-0ubuntu3.6) ...
acer@acer-Aspire-A315-53: ~$ sudo mysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.35-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```



```
Activities Terminal 20 Jan 17:04 acer@acer-Aspire-A315-53: ~
reading /usr/share/mecab/dic/ipadic/Prefix.csv ... 221
reading /usr/share/mecab/dic/ipadic/Filler.csv ... 19
reading /usr/share/mecab/dic/ipadic/Verb.csv ... 130750
reading /usr/share/mecab/dic/ipadic/Noun_verbal.csv ... 12146
reading /usr/share/mecab/dic/ipadic/Auxil.csv ... 199
reading /usr/share/mecab/dic/ipadic/Noun_namida.csv ... 60477
reading /usr/share/mecab/dic/ipadic/Noun_nemawashi.csv ... 42
reading /usr/share/mecab/dic/ipadic/Adverb.csv ... 332
reading /usr/share/mecab/dic/ipadic/Adnominal.csv ... 135
reading /usr/share/mecab/dic/ipadic/Noun_others.csv ... 151
reading /usr/share/mecab/dic/ipadic/Suffix.csv ... 1393
reading /usr/share/mecab/dic/ipadic/Adj.csv ... 27210
reading /usr/share/mecab/dic/ipadic/Postp.csv ... 146
reading /usr/share/mecab/dic/ipadic/Symbol.csv ... 208
reading /usr/share/mecab/dic/ipadic/Noun_natal.csv ... 42
reading /usr/share/mecab/dic/ipadic/Advcl.csv ... 3328
reading /usr/share/mecab/dic/ipadic/Noun_adverbial.csv ... 795
reading /usr/share/mecab/dic/ipadic/Noun_place.csv ... 72999
reading /usr/share/mecab/dic/ipadic/Interjection.csv ... 252
reading /usr/share/mecab/dic/ipadic/Noun_org.csv ... 16668
reading /usr/share/mecab/dic/ipadic/Others.csv ... 2
emitting double-array: 100% #####| reading /usr/share/mecab/dic/ipadic/matrix.def ... 1316x1316
emitting matrix : 100% #####| reading /usr/share/mecab/dic/ipadic/matrix.def ... 1316x1316
done!
update-alternatives: using /var/lib/mecab/dic/ipadic-utf8 to provide /var/lib/mecab/dic/debian (mecab-dictionary) in auto mode
Setting up mysql-server-8.0 (8.0.35-0ubuntu0.22.04.1) ...
update-alternatives: using /etc/mysql/mysql.cnf to provide /etc/mysql/my.cnf (my.cnf) in auto mode
Renaming removed key_buffer and myisam-recover options (if present)
mysqld will log errors to /var/log/mysql/error.log
mysqld is running as pid 32472
Created symlink /etc/systemd/system/multi-user.target.wants/mysql.service → /lib/systemd/system/mysql.service.
Setting up mysql-server (8.0.35-0ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for liblc-bin (2.35-0ubuntu3.6) ...
acer@acer-Aspire-A315-53: ~$ sudo mysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.35-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';
Query OK, 0 rows affected (0.01 sec)

mysql> exit
Bye
acer@acer-Aspire-A315-53: ~$ 
```

I started the interactive script by running:

```
sudo mysql_secure_installation
```

This asked to configure the VALIDATE PASSWORD PLUGIN.

I answered “yes”, and was asked to select a level of password validation. I entered **2** for the strongest level. In this case I will receive errors when attempting to set any password which does not contain numbers, upper and lowercase letters, and special characters.

I enabled password validation, and was shown the password strength for the root password . I was happy with my current password, enter **Y** for “yes” at the prompt. For the rest of the questions, I pressed **Y** and hit the **ENTER** key at each prompt. This removed some anonymous users and the test database, disable remote root logins, and load these new rules so that MySQL immediately respects the changes I had made.

```
Activities Terminal 20 Jan 17:18
Copyright (c) 2000, 2023, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';
Query OK, 0 rows affected (0.01 sec)

mysql> exit
Bye
acer@acer-Aspire-A315-53:~$ sudo mysql_secure_installation
sudo: mysql_secure_installation: command not found
acer@acer-Aspire-A315-53:~$ sudo mysql_secure_installation
A Securing the MySQL server deployment.

Enter password for user root:
? VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: y

A There are three levels of password validation policy:
LOW Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary      file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2
Using existing password for root.

Estimated strength of the password: 50
Change the password for root ? ((Press y|Y for Yes, any other key for No) : y
New password:
Re-enter new password:

Estimated strength of the password: 100
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) :
```

```
Activities Terminal 20 Jan 17:19
acer@acer-Aspire-A315-53:~$ file
LOW Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary      file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2
Using existing password for root.

Estimated strength of the password: 50
Change the password for root ? ((Press y|Y for Yes, any other key for No) : y
New password:
Re-enter new password:

Estimated strength of the password: 100
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

A Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y
- Dropping test database...
Success.

- Removing privileges on test database...
Success.

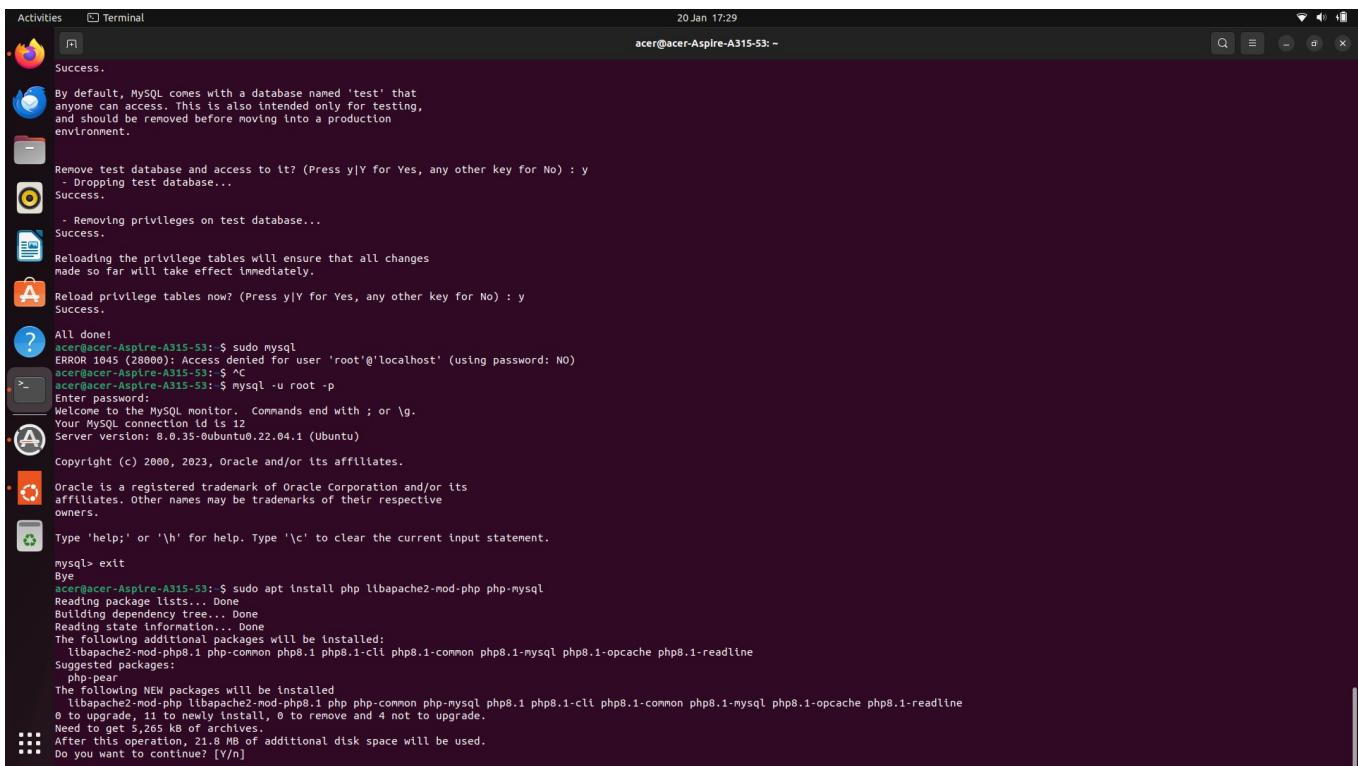
Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
acer@acer-Aspire-A315-53:~$
```

## Step 3 — Installing PHP

PHP is the component of our setup that will process code to display dynamic content to the final user. In addition to the `php` package, I installed `php-mysql`, a PHP module that allows PHP to communicate with MySQL-based databases. Also I installed `libapache2-mod-php` to enable Apache to handle PHP files. Core PHP packages automatically was installed as dependencies.



```
Activities Terminal 20 Jan 17:29 acer@acer-Aspire-A315-53: ~
Success.

By default, MySQL comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y
- Dropping test database...
Success.

- Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done! acer@acer-Aspire-A315-53: $ sudo mysql
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
acer@acer-Aspire-A315-53: $ ^C
acer@acer-Aspire-A315-53: $ mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.35-0ubuntu0.22.04.1 (Ubuntu)

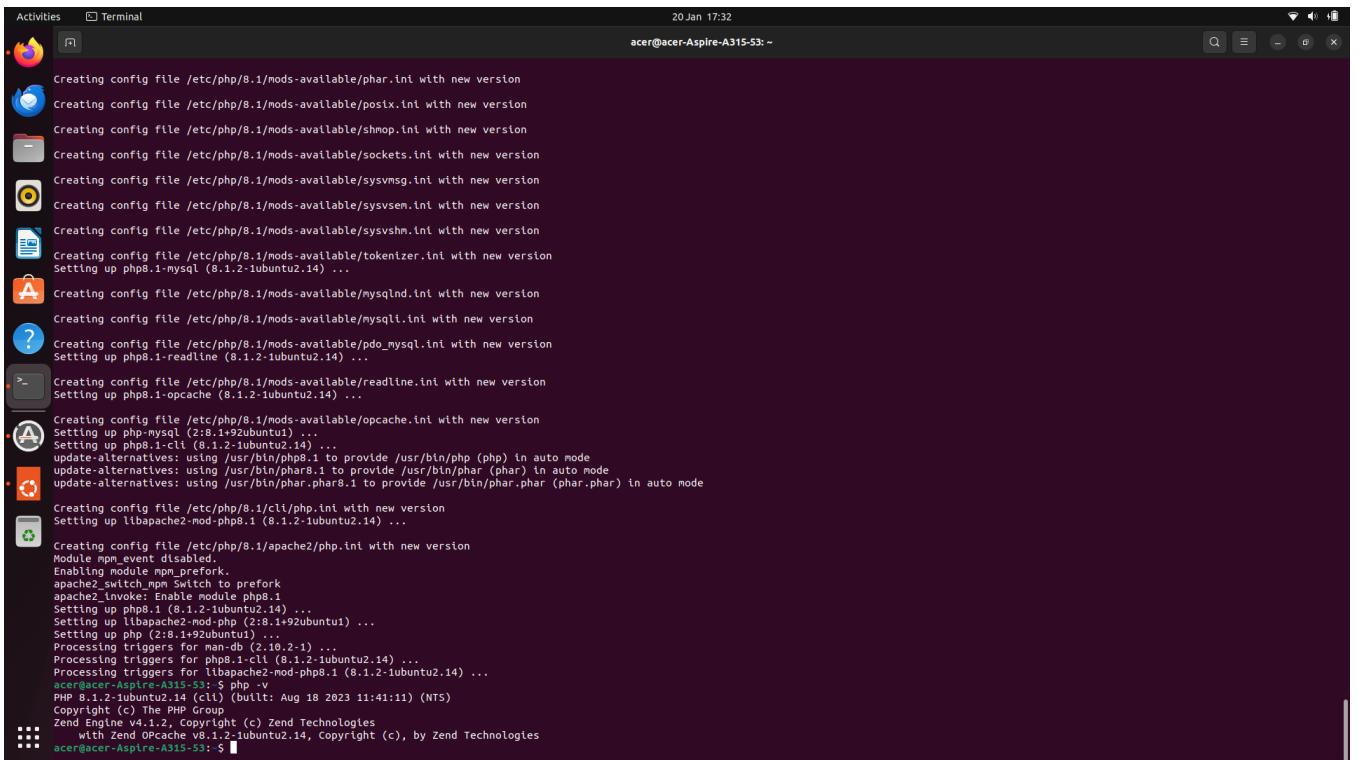
Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> exit
Bye
acer@acer-Aspire-A315-53: $ sudo apt install php libapache2-mod-php php-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php8.1 php-common php8.1-cli php8.1-common php8.1-mysql php8.1-opcache php8.1-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php libapache2-mod-php8.1 php php-common php-mysql php8.1 php8.1-cli php8.1-common php8.1-mysql php8.1-opcache php8.1-readline
0 to upgrade, 0 to newly install, 0 to remove and 4 not to upgrade.
Need to get 5,245 kB of archives.
After this operation, 21.8 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

To confirm PHP version I run the command: `php -v`



```
Activities Terminal 20 Jan 17:32 acer@acer-Aspire-A315-53: ~
Creating config file /etc/php/8.1/mods-available/phar.ini with new version
Creating config file /etc/php/8.1/mods-available/posix.ini with new version
Creating config file /etc/php/8.1/mods-available/shmop.ini with new version
Creating config file /etc/php/8.1/mods-available/sockets.ini with new version
Creating config file /etc/php/8.1/mods-available/sysvmsg.ini with new version
Creating config file /etc/php/8.1/mods-available/sysvsem.ini with new version
Creating config file /etc/php/8.1/mods-available/sysvshm.ini with new version
Creating config file /etc/php/8.1/mods-available/tokenizer.ini with new version
Setting up php8.1-mysql (8.1.2-1ubuntu2.14) ...
Creating config file /etc/php/8.1/mods-available/mysqlnd.ini with new version
Creating config file /etc/php/8.1/mods-available/mysqli.ini with new version
Creating config file /etc/php/8.1/mods-available/pdo_mysql.ini with new version
Setting up php8.1-readline (8.1.2-1ubuntu2.14) ...
Creating config file /etc/php/8.1/mods-available/readline.ini with new version
Setting up php8.1-opcache (8.1.2-1ubuntu2.14) ...
Creating config file /etc/php/8.1/mods-available/opcache.ini with new version
Setting up php8.1-mysql (2:8.1+92ubuntu1) ...
Setting up php8.1-cli (8.1.2-1ubuntu2.14) ...
update-alternatives: using /usr/bin/php8.1 to provide /usr/bin/php (php) in auto mode
update-alternatives: using /usr/bin/phar8.1 to provide /usr/bin/phar (phar) in auto mode
update-alternatives: using /usr/bin/phar.phar8.1 to provide /usr/bin/phar.phar (phar.phar) in auto mode
Creating config file /etc/php/8.1/cli/php.ini with new version
Setting up libapache2-mod-php8.1 (8.1.2-1ubuntu2.14) ...
Creating config file /etc/php/8.1/apache2/php.ini with new version
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2: switch_mpm Switch to prefork
apache2_invoke: Enable module php8.1
Setting up php8.1 (8.1.2-1ubuntu2.14) ...
Setting up libapache2-mod-php (2:8.1+92ubuntu1) ...
Setting up php (2:8.1+92ubuntu1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for phar (1.0.1-1) ...
Processing triggers for libapache2-mod-php8.1 (8.1.2-1ubuntu2.14) ...
acer@acer-Aspire-A315-53: $ php -v
PHP 8.1.2-1ubuntu2.14 (cli) (built: Aug 18 2023 11:41:11) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.1.2, Copyright (c) Zend Technologies
    with Zend OPcache v8.1.2-1ubuntu2.14, Copyright (c), by Zend Technologies
acer@acer-Aspire-A315-53: $
```

## Step 4 — Creating a Virtual Host for your Website

I created *virtual hosts* to encapsulate configuration details and host more than one domain from a single server. I set up a domain called `my_domain`.

Apache on Ubuntu 22.04 has one virtual host enabled by default that is configured to serve documents from the `/var/www/html` directory. I created a directory structure within `/var/www` for the `my_domain` site, leaving `/var/www/html` in place as the default directory to be served if a client request doesn't match any other sites.

I created the directory for `my_domain` :

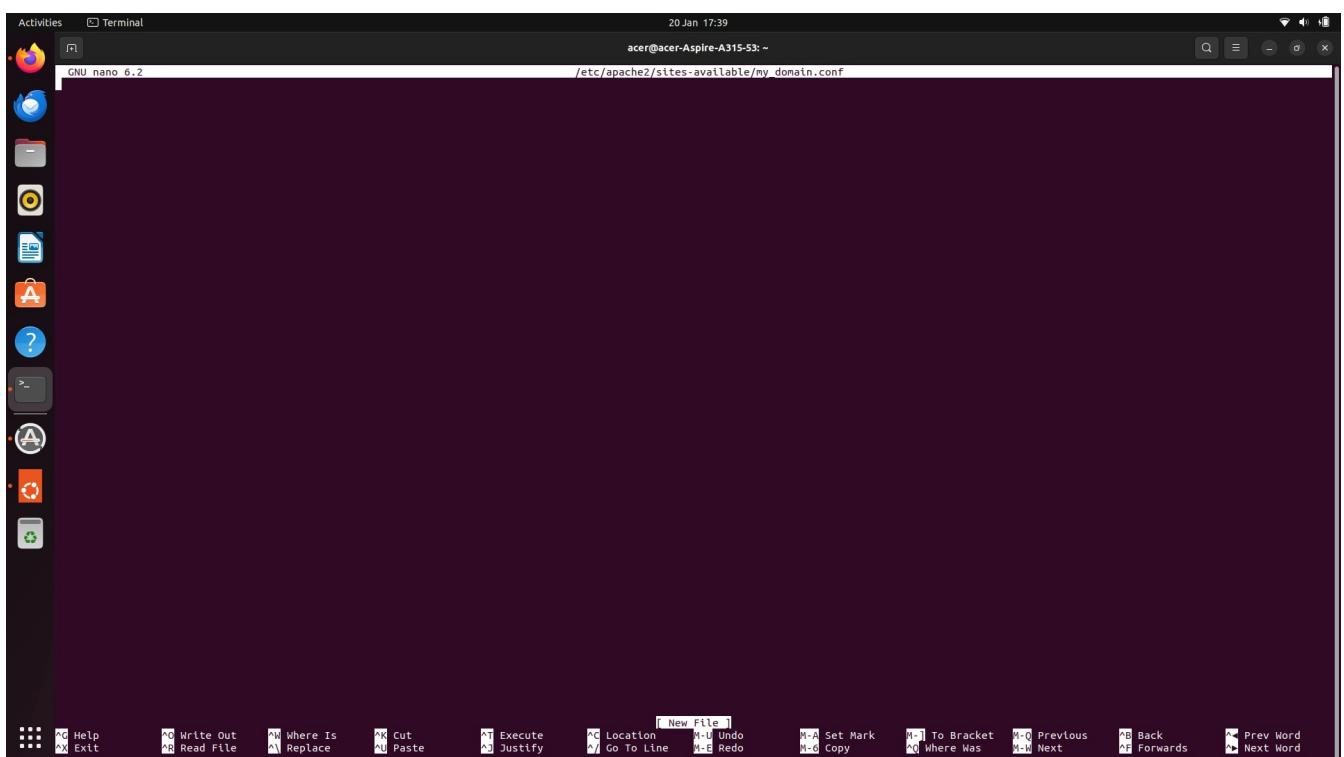
```
sudo mkdir /var/www/my_domain
```

Next, I assigned ownership of the directory with the `$USER` environment variable, which will reference my current system user:

```
sudo chown -R $USER:$USER /var/www/my_domain
```

Then, I opened a new configuration file in Apache's `sites-available` directory using your preferred command-line editor. Here, I used `nano`:

```
sudo nano /etc/apache2/sites-available/your_domain.conf
```



I add in the following bare-bones configuration with my domain name:

```
/etc/apache2/sites-available/your_domain.conf
```

```
<VirtualHost *:80>
    ServerName my_domain
```

```
ServerAlias www.my_domain
ServerAdmin webmaster@localhost
DocumentRoot /var/www/my_domain
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

With this `VirtualHost` configuration, I'm telling Apache to serve using `/var/www/` as the web root directory. I, use `a2ensite` to enable the new virtual host:

```
sudo a2ensite your_domain
```

I disabled Apache's default website

```
sudo a2dissite 000-default
```

To make sure my configuration file doesn't contain syntax errors, I run the command:

```
sudo apache2ctl configtest
sudo systemctl reload apache2
```

Then I created an `index.html` file in that location to test that the virtual host works as expected:

```
nano /var/www/my_domain/index.html
var/www/your_domain/index.html
```

```
<html>
  <head>
    <title>your_domain website</title>
  </head>
  <body>
    <h1>Hello World!</h1>

    <p>This is the landing page of <strong>your_domain</strong>.</p>
  </body>
</html>
```

A screenshot of a web browser window. The address bar shows "127.0.0.1". The page content is "Hello World!". Below the content, a status bar displays "This is the landing page of my\_domain.".

**Hello World!**

This is the landing page of **my\_domain**.

```

acer@acer-Aspire-A315-53:~$ sudo ufw status
Status: inactive
acer@acer-Aspire-A315-53:~$ sudo ufw allow from 94.197.150.147
Rules updated
acer@acer-Aspire-A315-53:~$ ip addr show ens3 | grep inet | awk '{ print $2; }' | sed 's/\.\.*$//'
Device "ens3" does not exist.
acer@acer-Aspire-A315-53:~$ sudo a2ensite my_domain
Enabling site my_domain.
To activate the new configuration, you need to run:
  systemctl reload apache2
acer@acer-Aspire-A315-53:~$ sudo a2dissite 000-default
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
acer@acer-Aspire-A315-53:~$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
acer@acer-Aspire-A315-53:~$ sudo systemctl reload apache2
acer@acer-Aspire-A315-53:~$ nano /var/www/my_domain/index.html
acer@acer-Aspire-A315-53:~$ sudo apt update
[sudo] password for acer:
Hit:1 http://gb.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:4 https://dl.google.com/linux/chrome/deb stable InRelease [1,825 B]
Get:5 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,082 B]
Hit:6 http://gb.archive.ubuntu.com/ubuntu jammy-backports InRelease
Fetched 232 kB in 2s (124 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
4 packages can be upgraded. Run 'apt list --upgradable' to see them.
acer@acer-Aspire-A315-53:~$ sudo apt install apache2

```

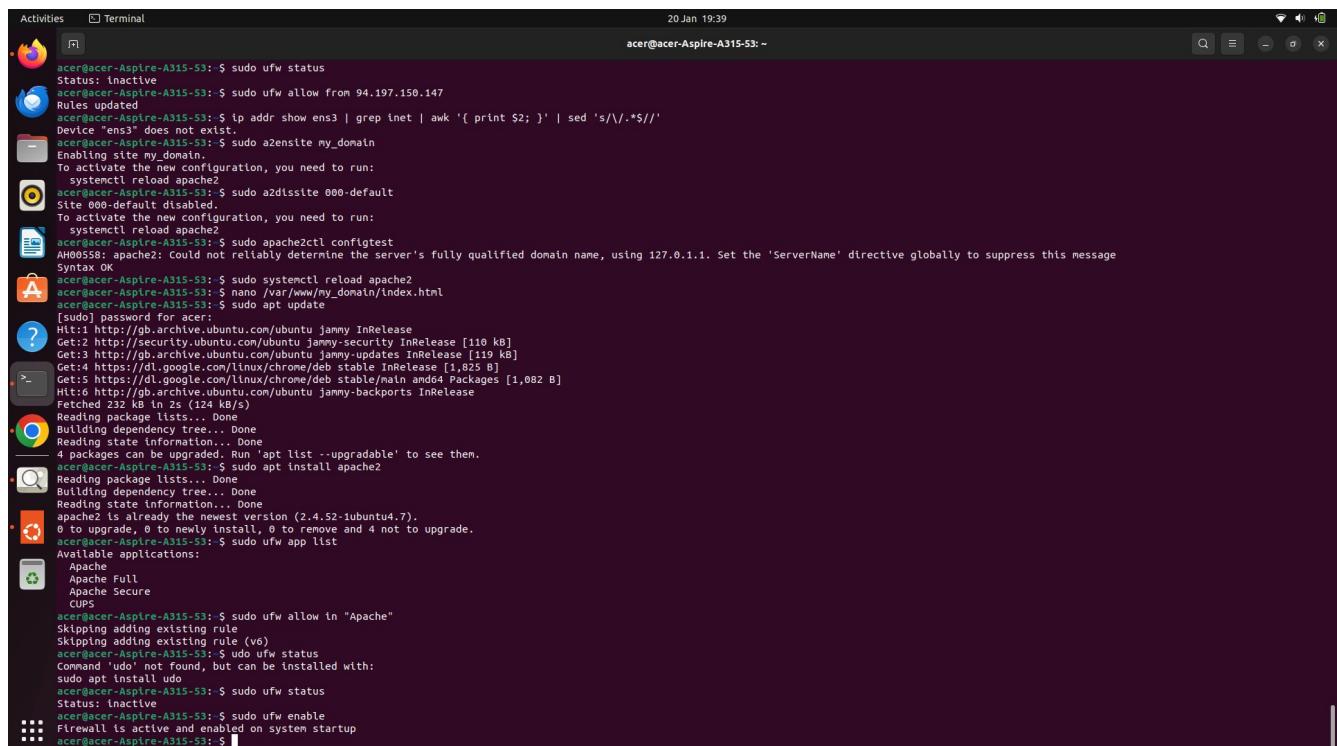
Then I edited the **/etc/apache2/mods-enabled/dir.conf** file and modify the order in which the `index.php` file is listed within the `DirectoryIndex` directive:

**sudo nano /etc/apache2/mods-enabled/dir.conf**  
**/etc/apache2/mods-enabled/dir.conf**

```

<IfModule mod_dir.c>
    DirectoryIndex index.php index.html index.cgi index.pl index.xhtml
    index.htm
</IfModule>

```



```

Activities Terminal 20 Jan 19:39
acer@acer-Aspire-A315-53:~$ sudo ufw status
Status: inactive
acer@acer-Aspire-A315-53:~$ sudo ufw allow from 94.197.150.147
Rules updated
acer@acer-Aspire-A315-53:~$ ip addr show ens3 | grep inet | awk '{ print $2; }' | sed 's/\.\.*$//'
Device "ens3" does not exist.
acer@acer-Aspire-A315-53:~$ sudo a2ensite my_domain
Enabling site my_domain.
To activate the new configuration, you need to run:
  systemctl reload apache2
acer@acer-Aspire-A315-53:~$ sudo a2dissite 000-default
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
acer@acer-Aspire-A315-53:~$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
acer@acer-Aspire-A315-53:~$ sudo systemctl reload apache2
acer@acer-Aspire-A315-53:~$ nano /var/www/my_domain/index.html
acer@acer-Aspire-A315-53:~$ sudo apt update
[sudo] password for acer:
Hit:1 http://gb.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:4 https://dl.google.com/linux/chrome/deb stable InRelease [1,825 B]
Get:5 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,082 B]
Hit:6 http://gb.archive.ubuntu.com/ubuntu jammy-backports InRelease
Fetched 232 kB in 2s (124 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
4 packages can be upgraded. Run 'apt list --upgradable' to see them.
acer@acer-Aspire-A315-53:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.52-1ubuntu4.7).
0 to upgrade, 0 to newly install, 0 to remove and 4 not to upgrade.
acer@acer-Aspire-A315-53:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
acer@acer-Aspire-A315-53:~$ sudo ufw allow in "Apache"
Skipping adding existing rule
Skipping adding existing rule (v6)
acer@acer-Aspire-A315-53:~$ sudo ufw status
Command 'udo' not found, but can be installed with:
  sudo apt install udo
acer@acer-Aspire-A315-53:~$ sudo ufw status
Status: inactive
acer@acer-Aspire-A315-53:~$ sudo ufw enable
Firewall is active and enabled on system startup
acer@acer-Aspire-A315-53:~$ 

```

```

b: New profiles: skip
To           Action    From
--           -----    ---
80/tcp (Apache)      ALLOW IN  Anywhere
Anywhere          ALLOW IN  94.197.150.147
22/tcp            ALLOW IN  Anywhere
80/tcp (Apache (v6)) ALLOW IN  Anywhere (v6)
22/tcp (v6)        ALLOW IN  Anywhere (v6)

acer@acer-Aspire-A315-53:~$ sudo ufw allow OpenSSH
ERROR: Could not find a profile matching 'OpenSSH'
acer@acer-Aspire-A315-53:~$ ip addr show ens3 | grep inet | awk '{ print $2; }' | sed 's/\.*$//'
Device "ens3" does not exist.
acer@acer-Aspire-A315-53:~$ ip addr show grep inet | awk '{ print $2; }' | sed 's/\.*$//'
Error: either "dev" is duplicate, or "inet" is a garbage.
acer@acer-Aspire-A315-53:~$ curl http://icanhazip.com
94.197.150.147
acer@acer-Aspire-A315-53:~$ php -v
PHP 8.1.2-1ubuntu2.14 (cli) (built: Aug 18 2023 11:41:11) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.1.2, Copyright (c) Zend Technologies
    with Zend OPcache v8.1.2-1ubuntu2.14, Copyright (c), by Zend Technologies
acer@acer-Aspire-A315-53:~$ sudo nano /etc/apache2/mods-enabled/dir.conf
> acer@acer-Aspire-A315-53:~$ sudo systemctl reload apache2
acer@acer-Aspire-A315-53:~$ nano /var/www/my_domain/info.php
acer@acer-Aspire-A315-53:~$ nano /var/www/my_domain/index.html
acer@acer-Aspire-A315-53:~$ sudo mysql
[sudo] password for acer:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
acer@acer-Aspire-A315-53:~$ sudo mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
acer@acer-Aspire-A315-53:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 16
Server version: 8.0.35-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE example_database;
Now give this user permission over the example_database database:

```

---

**sudo systemctl reload apache2**

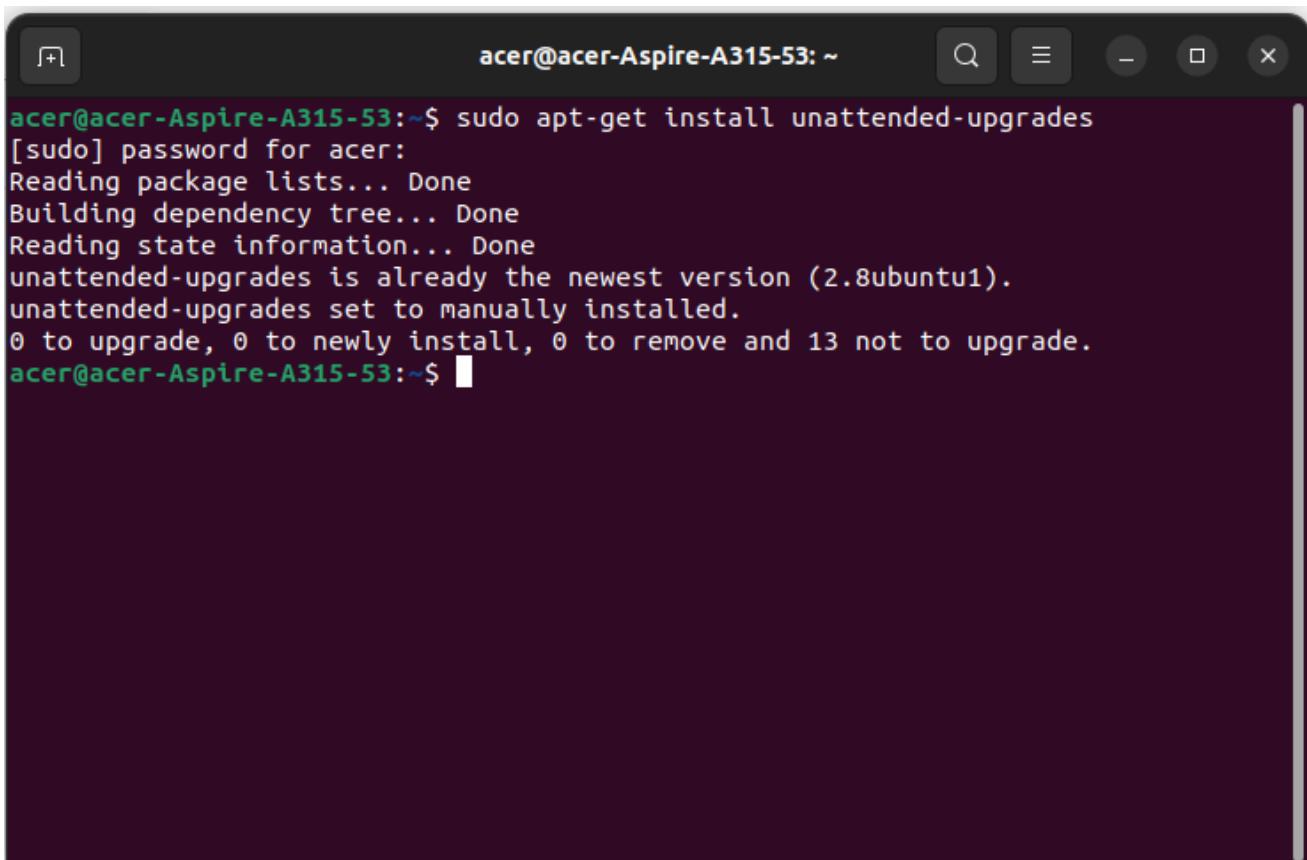
### 3.6 Recommend final adjustments before going live

#### Securing LAMP server:

##### 1. Enable automatic updates

In case this feature is not enabled on server and are not installing the latest upgrades and patches manually, server is at risk of being exploited. To enable automatic unattended upgrades you I installed the *unattended-upgrades* package.

**sudo apt-get install unattended-upgrades**



```
acer@acer-Aspire-A315-53:~$ sudo apt-get install unattended-upgrades
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unattended-upgrades is already the newest version (2.8ubuntu1).
unattended-upgrades set to manually installed.
0 to upgrade, 0 to newly install, 0 to remove and 13 not to upgrade.
acer@acer-Aspire-A315-53:~$
```

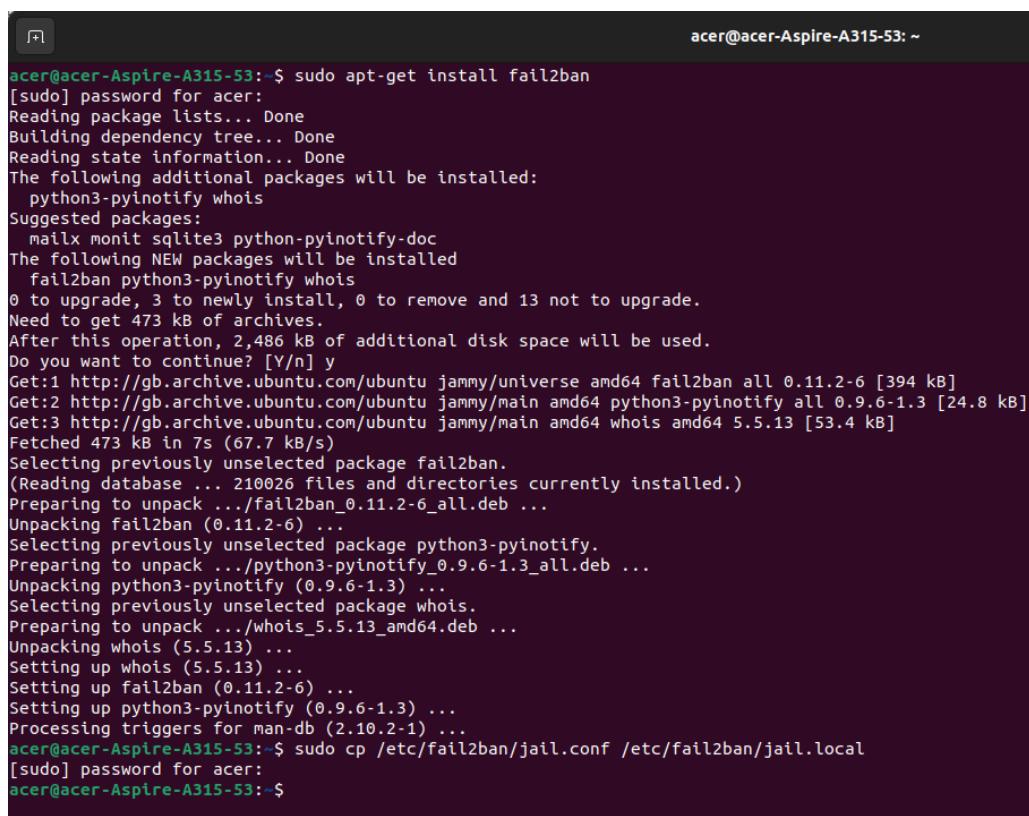
## 2. Install Fail2ban

Fail2ban is a service which scans the log files for too many login failures and blocks the IP address which is showing malicious signs. I installed [Fail2ban](#) by command:

**sudo apt-get install fail2ban**

Then I created a copy of the default configuration file so I can safely make changes without them being overwritten by system upgrades:

**sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local**



```
acer@acer-Aspire-A315-53:~$ sudo apt-get install fail2ban
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 to upgrade, 3 to newly install, 0 to remove and 13 not to upgrade.
Need to get 473 kB of archives.
After this operation, 2,486 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 fail2ban all 0.11.2-6 [394 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 python3-pyinotify all 0.9.6-1.3 [24.8 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 whois amd64 5.5.13 [53.4 kB]
Fetched 473 kB in 7s (67.7 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 210026 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.11.2-6_all.deb ...
Unpacking fail2ban (0.11.2-6) ...
Selecting previously unselected package python3-pyinotify.
Preparing to unpack .../python3-pyinotify_0.9.6-1.3_all.deb ...
Unpacking python3-pyinotify (0.9.6-1.3) ...
Selecting previously unselected package whois.
Preparing to unpack .../whois_5.5.13_amd64.deb ...
Unpacking whois (5.5.13) ...
Setting up whois (5.5.13) ...
Setting up fail2ban (0.11.2-6) ...
Setting up python3-pyinotify (0.9.6-1.3) ...
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
[sudo] password for acer:
acer@acer-Aspire-A315-53:~$
```

```
sudo nano /etc/fail2ban/jail.local
```

The [sshd] block was changed :

```
[sshd]
```

```
# Provide customizations in a jail.local file or a jail.d/customisation
# For example to change the default bantime for all jails and to enable
# ssh-iptables jail the following (uncommented) would appear in the .1
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
# enabled = true
# port      = ssh
# filter    = sshd
# logpath   = /var/log/auth.log
# maxretry  = 5

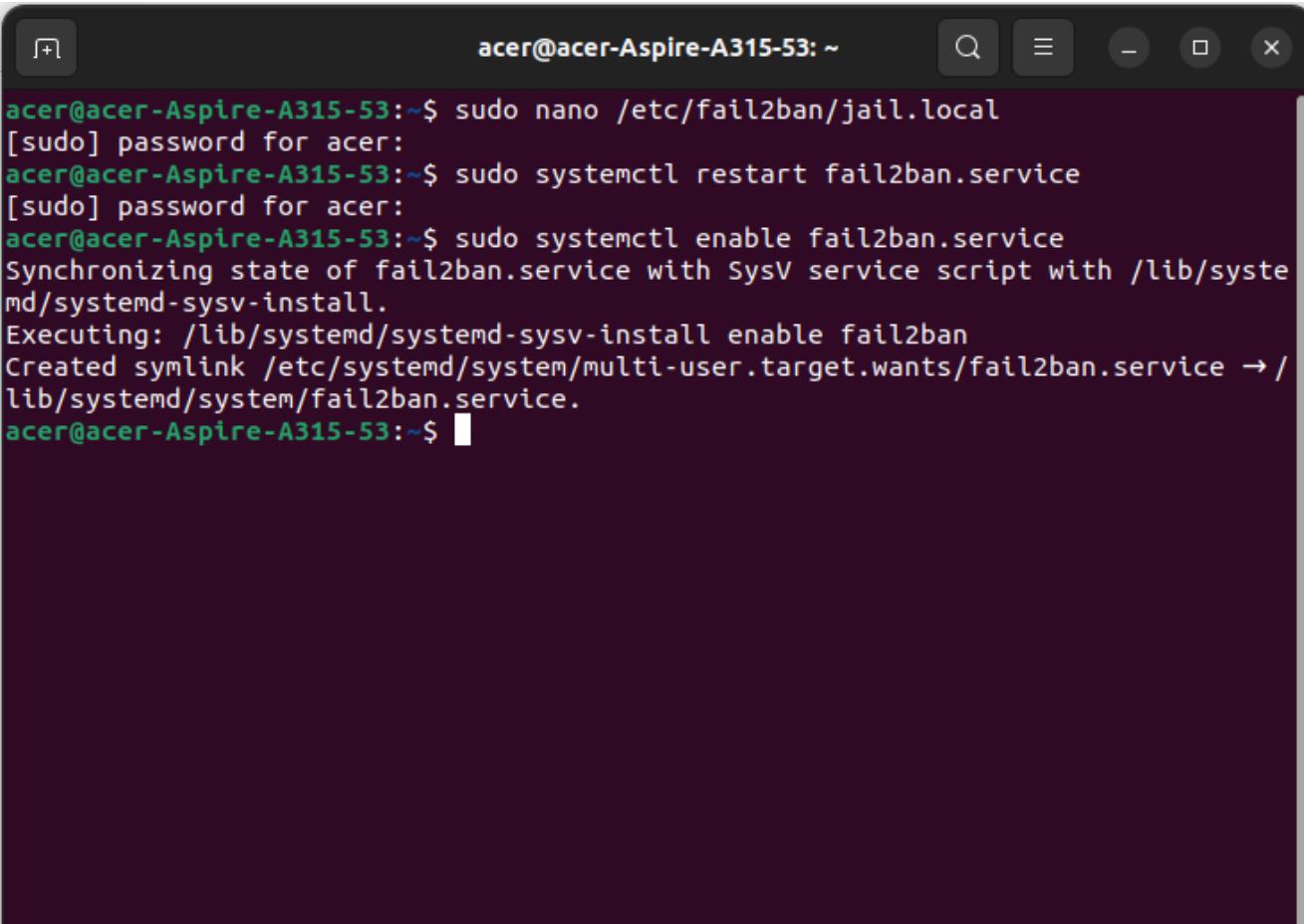
# bantime = 600
# See jail.conf(5) man page for more information
```

I saved the file and restart Fail2ban for the changes to take effect:

```
sudo systemctl restart fail2ban.service
```

And then enabled Fail2ban on system boot:

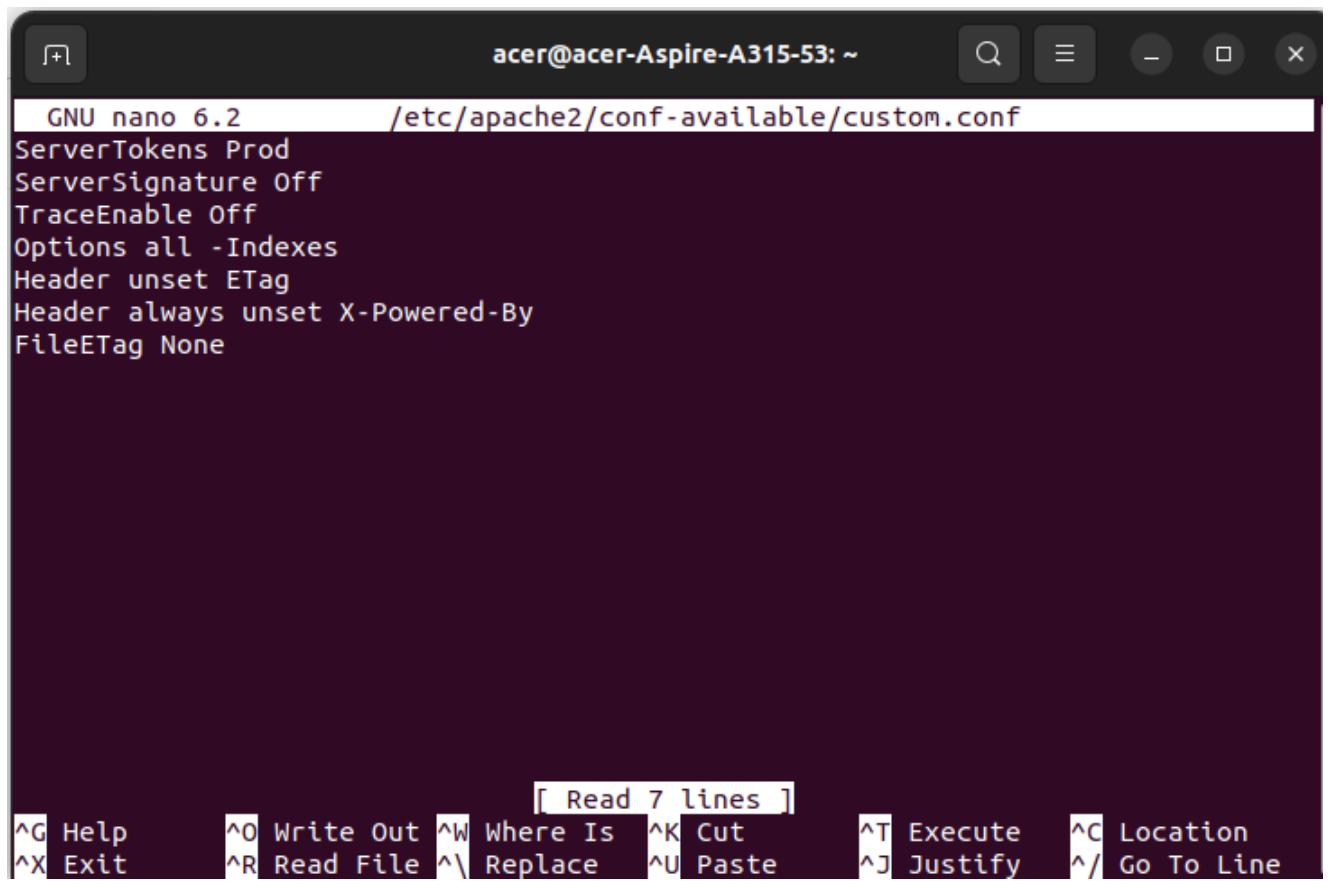
```
sudo systemctl enable fail2ban.service
```



```
acer@acer-Aspire-A315-53:~$ sudo nano /etc/fail2ban/jail.local
[sudo] password for acer:
acer@acer-Aspire-A315-53:~$ sudo systemctl restart fail2ban.service
[sudo] password for acer:
acer@acer-Aspire-A315-53:~$ sudo systemctl enable fail2ban.service
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/system/fail2ban.service.
acer@acer-Aspire-A315-53:~$
```

### 3. Hide Apache sensitive information

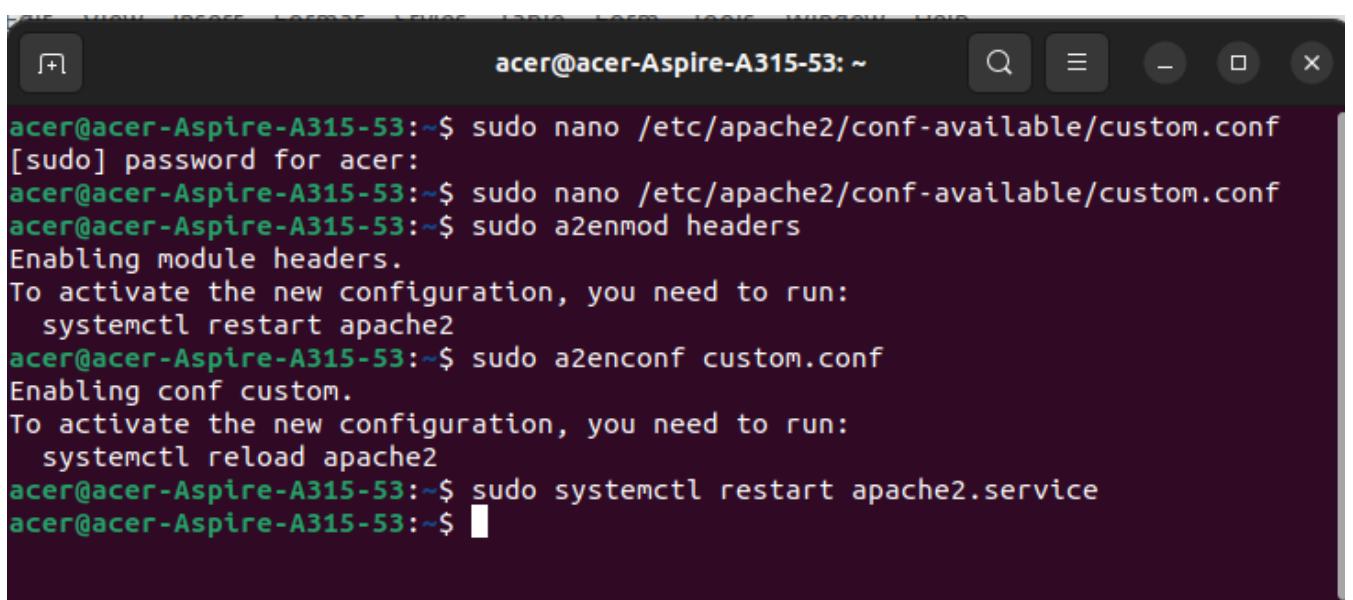
The default Apache configuration provides much sensitive information which can be used against the service. I made this information hidden and created a configuration file for new settings:



```
GNU nano 6.2          /etc/apache2/conf-available/custom.conf
ServerTokens Prod
ServerSignature Off
TraceEnable Off
Options all -Indexes
Header unset ETag
Header always unset X-Powered-By
FileETag None
```

[ Read 7 lines ]

**^G Help** **^O Write Out** **^W Where Is** **^K Cut** **^T Execute** **^C Location**  
**^X Exit** **^R Read File** **^V Replace** **^U Paste** **^J Justify** **^/ Go To Line**

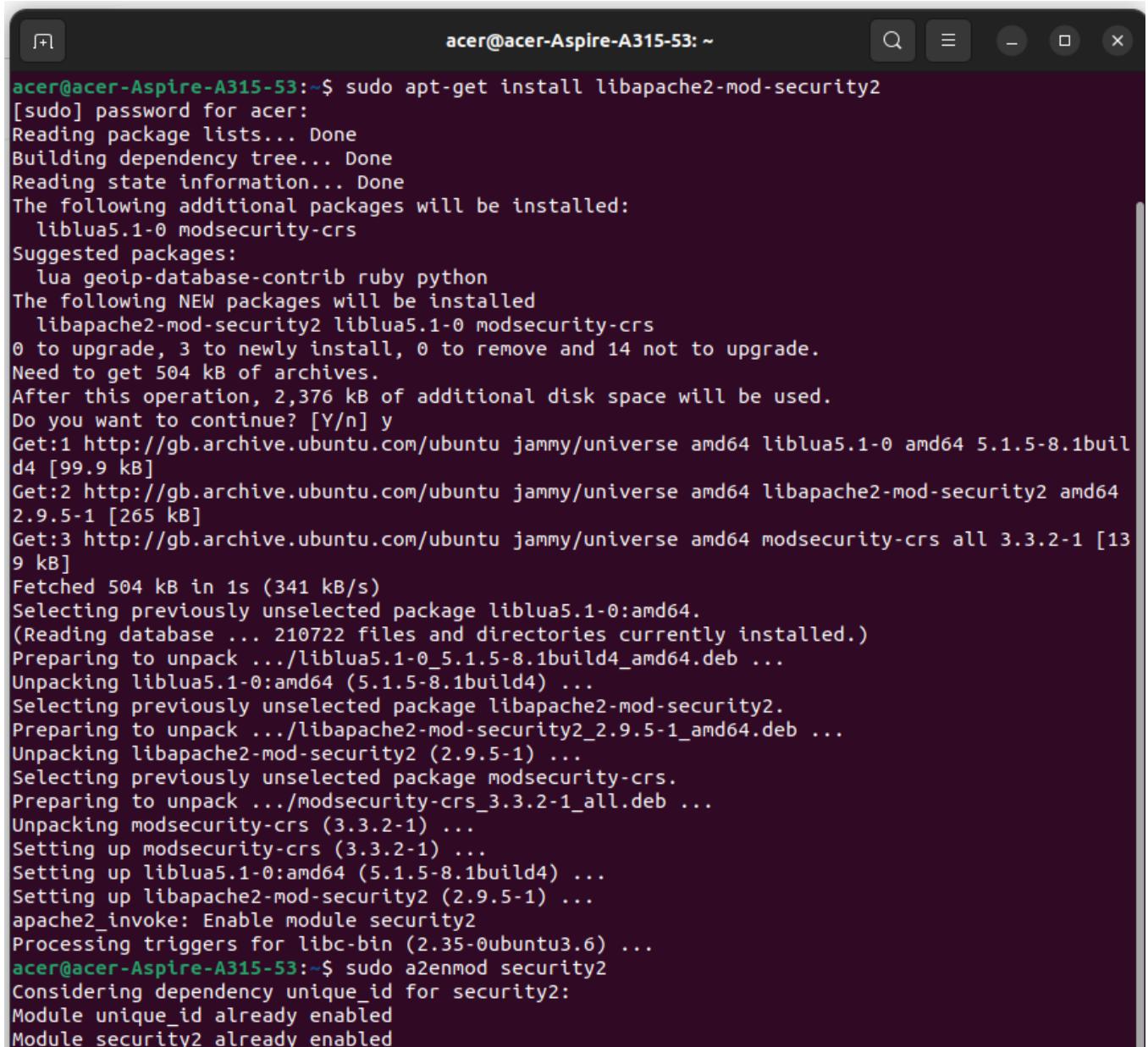


```
acer@acer-Aspire-A315-53:~$ sudo nano /etc/apache2/conf-available/custom.conf
[sudo] password for acer:
acer@acer-Aspire-A315-53:~$ sudo nano /etc/apache2/conf-available/custom.conf
acer@acer-Aspire-A315-53:~$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  systemctl restart apache2
acer@acer-Aspire-A315-53:~$ sudo a2enconf custom.conf
Enabling conf custom.
To activate the new configuration, you need to run:
  systemctl reload apache2
acer@acer-Aspire-A315-53:~$ sudo systemctl restart apache2.service
acer@acer-Aspire-A315-53:~$
```

#### 4. Install and enable mod\_security

I installed and enabled mod\_security :

```
sudo apt-get install libapache2-modsecurity2  
sudo a2enmod security2
```



The screenshot shows a terminal window titled "acer@acer-Aspire-A315-53: ~". The terminal output is as follows:

```
acer@acer-Aspire-A315-53:~$ sudo apt-get install libapache2-mod-security2  
[sudo] password for acer:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  liblua5.1-0 modsecurity-crs  
Suggested packages:  
  lua geoip-database-contrib ruby python  
The following NEW packages will be installed  
  libapache2-mod-security2 liblua5.1-0 modsecurity-crs  
0 to upgrade, 3 to newly install, 0 to remove and 14 not to upgrade.  
Need to get 504 kB of archives.  
After this operation, 2,376 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 liblua5.1-0 amd64 5.1.5-8.1build4 [99.9 kB]  
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 libapache2-mod-security2 amd64 2.9.5-1 [265 kB]  
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 modsecurity-crs all 3.3.2-1 [139 kB]  
Fetched 504 kB in 1s (341 kB/s)  
Selecting previously unselected package liblua5.1-0:amd64.  
(Reading database ... 210722 files and directories currently installed.)  
Preparing to unpack .../liblua5.1-0_5.1.5-8.1build4_amd64.deb ...  
Unpacking liblua5.1-0:amd64 (5.1.5-8.1build4) ...  
Selecting previously unselected package libapache2-mod-security2.  
Preparing to unpack .../libapache2-mod-security2_2.9.5-1_amd64.deb ...  
Unpacking libapache2-mod-security2 (2.9.5-1) ...  
Selecting previously unselected package modsecurity-crs.  
Preparing to unpack .../modsecurity-crs_3.3.2-1_all.deb ...  
Unpacking modsecurity-crs (3.3.2-1) ...  
Setting up modsecurity-crs (3.3.2-1) ...  
Setting up liblua5.1-0:amd64 (5.1.5-8.1build4) ...  
Setting up libapache2-mod-security2 (2.9.5-1) ...  
apache2_invoke: Enable module security2  
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...  
acer@acer-Aspire-A315-53:~$ sudo a2enmod security2  
Considering dependency unique_id for security2:  
Module unique_id already enabled  
Module security2 already enabled
```

Then I configured the module and enabled the OWASP ModSecurity Core Rule Set (CRS).

```
sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

Then, I opened the */etc/modsecurity/modsecurity.conf* file and edited

```
acer@acer-Aspire-A315-53: ~
GNU nano 6.2          /etc/modsecurity/modsecurity.conf *
# -- Rule engine initialization -----
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On
SecResponseBodyAccess Off
SecRequestBodyLimit 8388608
SecRequestBodyNoFilesLimit 131072
SecRequestBodyInMemoryLimit 262144

# -- Request body handling -----
# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute   ^C Location
^X Exit      ^R Read File ^L Replace   ^U Paste     ^J Justify    ^/ Go To Line
```

Then I removed the current CRS and download the OWASP CRS and edited `/etc/apache2/mods-enabled/security2.conf` file

```
acer@acer-Aspire-A315-53: ~
GNU nano 6.2          /etc/apache2/mods-enabled/security2.conf *
<IfModule security2_module>
    # Default Debian dir for modsecurity's persistent data
    SecDataDir /var/cache/modsecurity

    # Include all the *.conf files in /etc/modsecurity.
    # Keeping your local configuration in that directory
    # will allow for an easy upgrade of THIS file and
    # make your life easier
    IncludeOptional /etc/modsecurity/*.conf

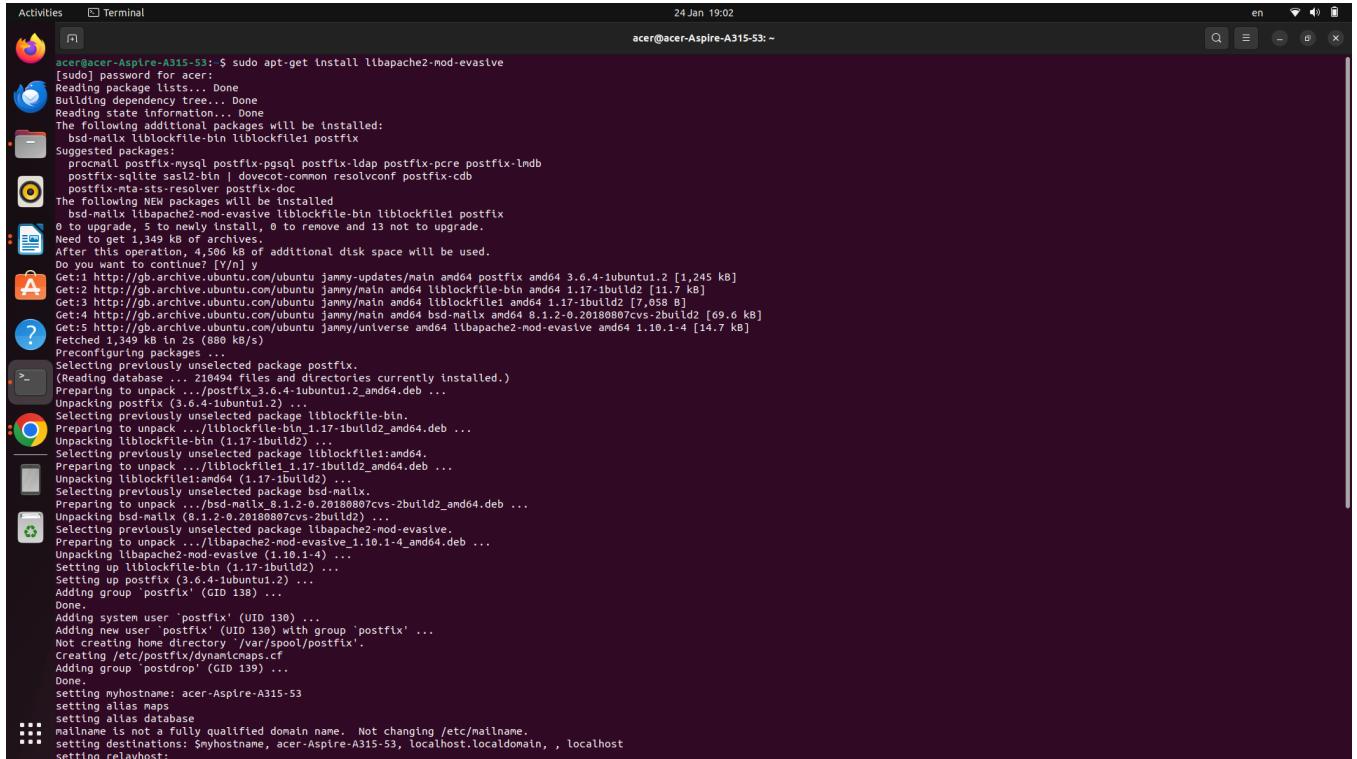
    # Include OWASP ModSecurity CRS rules if installed
    IncludeOptional /usr/share/modsecurity-crs/*.conf
    IncludeOptional /usr/share/modsecurity-crs/rules/*.conf
</IfModule>

^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute   ^C Location
^X Exit      ^R Read File ^L Replace   ^U Paste     ^J Justify    ^/ Go To Line
```

## 5. Install and enable mod\_evasive

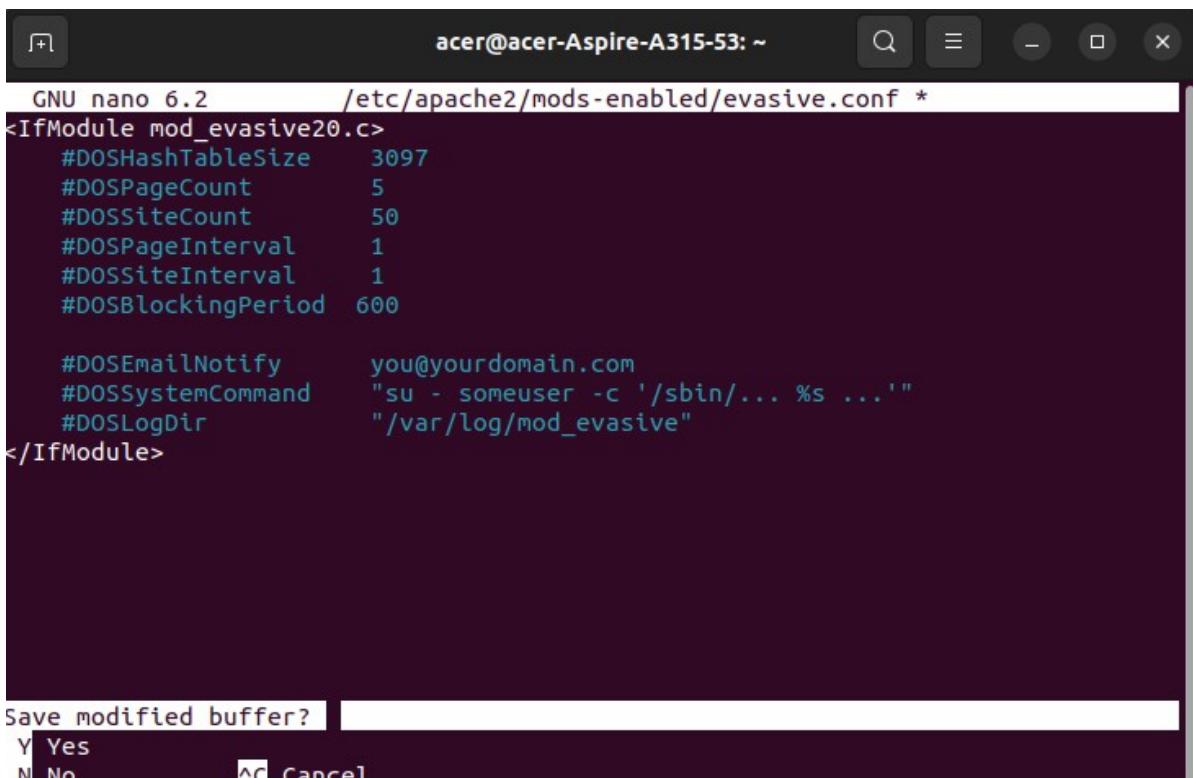
Mod\_evasive is an Apache module which can be used to protect the web server from DoS (Denial of Service), DDoS (Distributed Denial of Service) and brute-force attacks. To install mod\_evasive on server, I run :

```
sudo apt-get install libapache2-mod-evasive
```



```
acer@acer-Aspire-A315-53:~$ sudo apt-get install libapache2-mod-evasive
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading status information... Done
The following additional packages will be installed:
bsd-mailx libblockfile-bin libblockfile1 postfix
Suggested packages:
procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb
postfix-sqlite sa12-bin | dovecot-common resolvconf postfix-cdb
postfix-nta-sts-resolver postfix-dove
The following NEW packages will be installed:
bsd-mailx libapache2-mod-evasive libblockfile-bin libblockfile1 postfix
0 to upgrade, 5 newly installed, 0 to remove and 13 not to upgrade.
Need to get 4.549 kB of archives.
After this operation, 4,566 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 postfix amd64 3.6.4-1ubuntu1.2 [1,245 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 libblockfile-bin amd64 1.17-1build2 [11.7 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 libblockfile1 amd64 1.17-1build2 [7,058 B]
Get:4 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 bsd-mailx amd64 8.1.2-0.20180807cvs-2build2 [69.6 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 libapache2-mod-evasive amd64 1.10.1-4 [14.7 kB]
Fetched 1,349 kB in 2s (880 kB/s)
Preconfiguring packages...
Selecting previously unselected package postfix.
(Reading database ... 210494 files and directories currently installed.)
Preparing to unpack .../postfix_3.6.4-1ubuntu1.2_amd64.deb ...
Unpacking postfix (3.6.4-1ubuntu1.2) ...
Selecting previously unselected package libblockfile-bin.
Preparing to unpack .../libblockfile-bin_1.17-1build2_amd64.deb ...
Unpacking libblockfile-bin (1.17-1build2) ...
Selecting previously unselected package libblockfile1:amd64.
Preparing to unpack .../libblockfile1_1.17-1build2_amd64.deb ...
Unpacking libblockfile1:amd64 (1.17-1build2) ...
Selecting previously unselected package bsd-mailx.
Preparing to unpack .../bsd-mailx_8.1.2-0.20180807cvs-2build2_amd64.deb ...
Unpacking bsd-mailx (8.1.2-0.20180807cvs-2build2) ...
Selecting previously unselected package libapache2-mod-evasive.
Preparing to unpack .../libapache2-mod-evasive_1.10.1-4_amd64.deb ...
Unpacking libapache2-mod-evasive (1.10.1-4) ...
Setting up libblockfile-bin (3.6.4-1ubuntu1.2) ...
Setting up postfix (3.6.4-1ubuntu1.2) ...
Adding group 'postfix' (GID 138) ...
Done.
Adding system user 'postfix' (UID 138) ...
Adding new user 'postfix' (UID 138) with group 'postfix'.
Not creating home directory '/var/spool/postfix'.
Creating '/etc/postfix/dynamicmaps.cf'.
Adding group 'postdrop' (GID 139) ...
Done.
setting myhostname: acer-Aspire-A315-53
setting alias maps
setting alias database
mailname is not a fully qualified domain name. Not changing /etc/mailname.
setting destinations: $myhostname, acer-Aspire-A315-53, localhost.localdomain, localhost
setting relayhost:
```

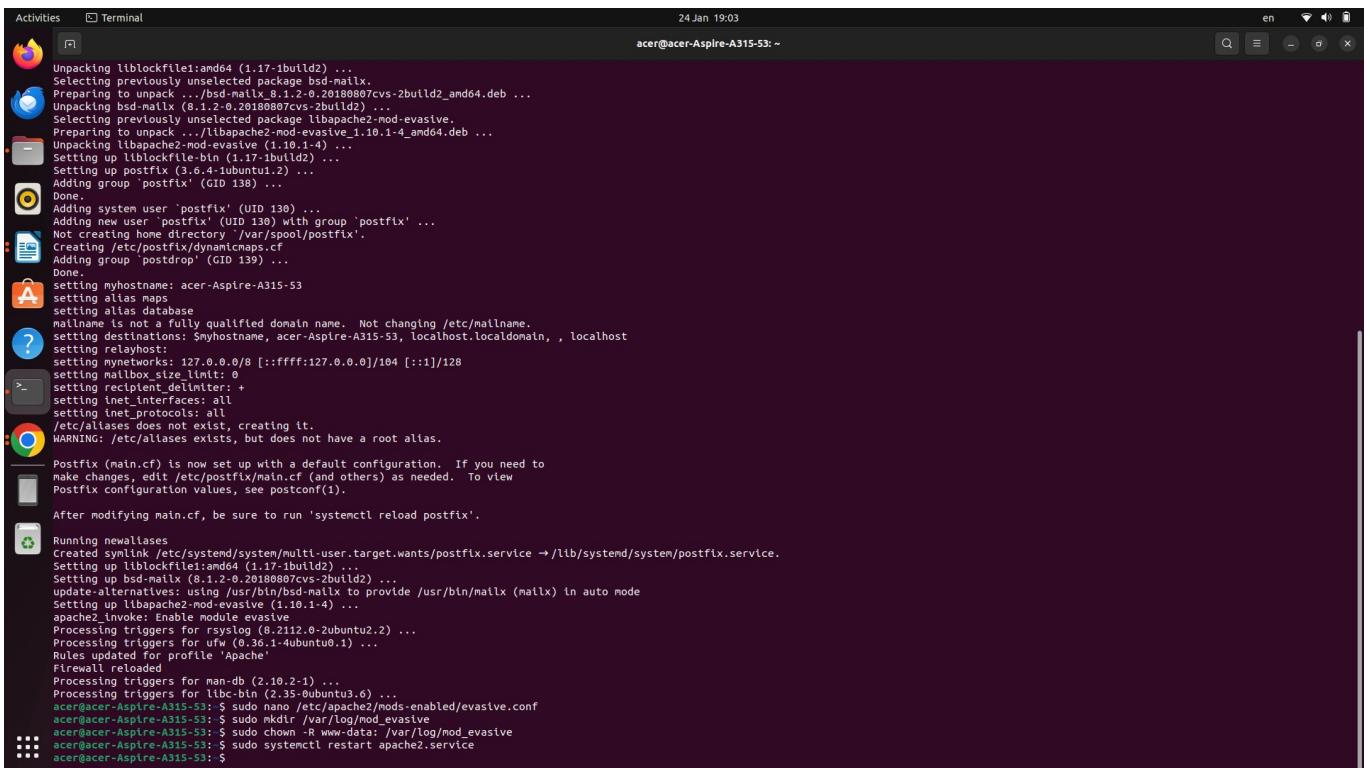
I edited the default configuration file `/etc/apache2/mods-enabled/evasive.conf`



```
GNU nano 6.2          /etc/apache2/mods-enabled/evasive.conf *
<IfModule mod_evasive20.c>
    #DOSHashTableSize      3097
    #DOSSiteCount          5
    #DOSSiteInterval        1
    #DOSSiteInterval        1
    #DOSBlockingPeriod     600

    #DOSEmailNotify        you@yourdomain.com
    #DOSSystemCommand      "su - someuser -c '/sbin/... %s ...'"
    #DOSLogDir              "/var/log/mod_evasive"
</IfModule>
```

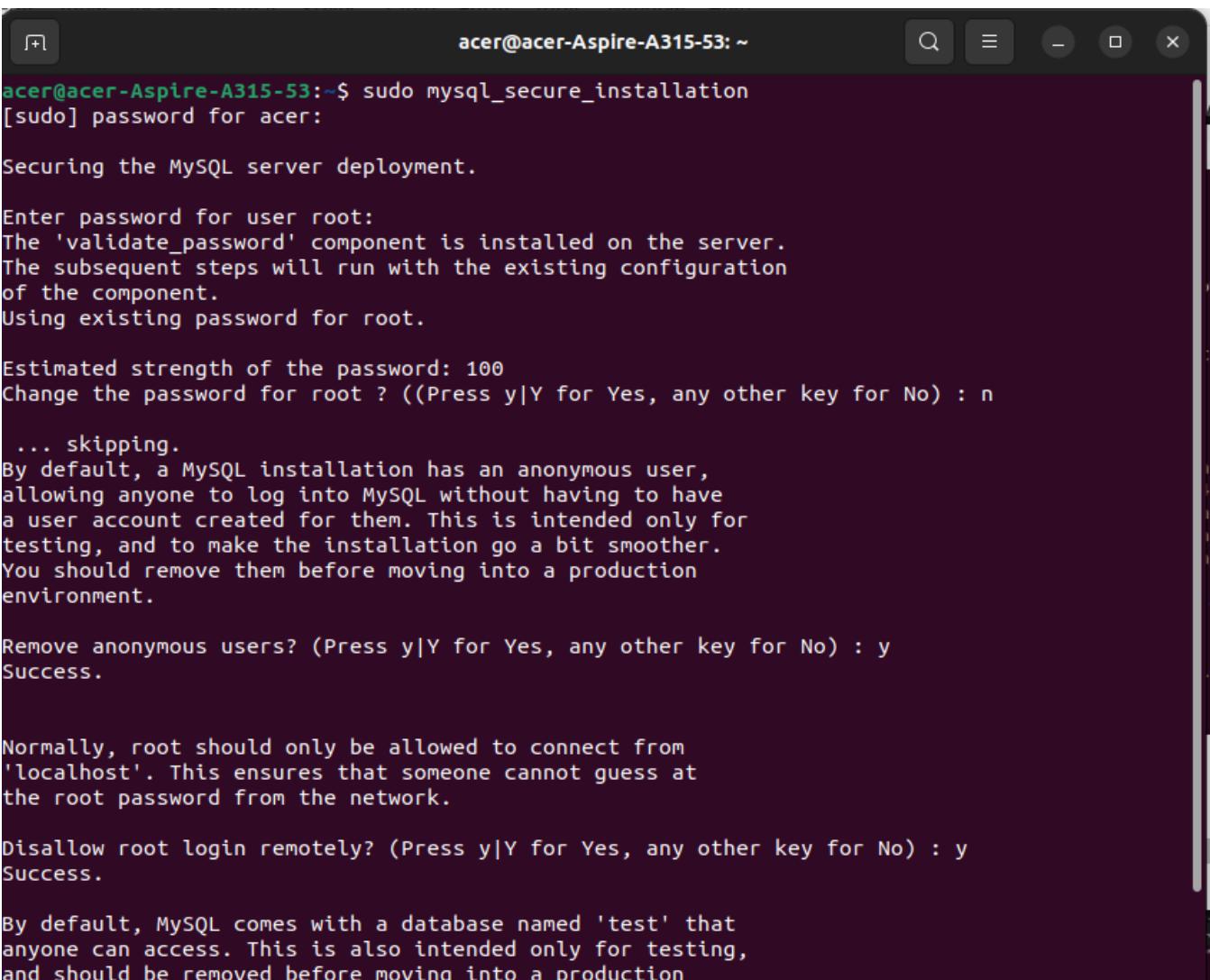
Save modified buffer? [Y/N]  Yes  No  Cancel



```
Activities Terminal 24 Jan 19:03 acer@acer-Aspire-A315-53: ~
Unpacking libblockfile1:amd64 (1.17-1build2) ...
Selecting previously unselected package bsd-mailx.
Preparing to unpack .../bsd-mailx_8.1.2-6.20180807cvs-2build2_amd64.deb ...
Unpacking bsd-mailx (8.1.2-6.20180807cvs-2build2_amd64.deb) ...
Selecting previously unselected package libapache2-mod-evasive.
Preparing to unpack .../libapache2-mod-evasive_1.10.1-4_amd64.deb ...
Unpacking libapache2-mod-evasive (1.10.1-4) ...
Setting up libblockfile1:amd64 (1.17-1build2) ...
Setting up postfix (3.6.4-1ubuntu1.2) ...
Adding group 'postfix' (GID 139) ...
Done.
setting myhostname: acer-Aspire-A315-53
setting alias maps
setting alias database
myhostname is not a fully qualified domain name. Not changing /etc/mailname.
Setting myhostname: acer-Aspire-A315-53, localhost.localdomain, localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [:ffff:127.0.0.0]/104 [:1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
/etc/aliases does not exist, creating it.
WARNING: /etc/aliases exists, but does not have a root alias.
Postfix (main.cf) is now set up with a default configuration. If you need to
make changes, edit /etc/postfix/main.cf (and others) as needed. To view
Postfix configuration values, see postconf(1).
After modifying main.cf, be sure to run 'systemctl reload postfix'.
Running newaliases
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /lib/systemd/system/postfix.service.
Setting up libblockfile1:amd64 (1.17-1build2) ...
Setting up bsd-mailx (8.1.2-6.20180807cvs-2build2) ...
update-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode
Setting up libapache2-mod-evasive (1.10.1-4) ...
apache2: command-line module evasive
Processing triggers for syslog (0.2112.0-2ubuntu2.2) ...
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Rules updated for profile 'Apache'
Firewall reloaded
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for liblc-bin (2.35-0ubuntu3.6) ...
acer@acer-Aspire-A315-53: $ sudo nano /etc/apache2/mods-enabled/evasive.conf
acer@acer-Aspire-A315-53: $ sudo mkdir /var/log/mod_evasive
acer@acer-Aspire-A315-53: $ sudo chown -R www-data: /var/log/mod_evasive
acer@acer-Aspire-A315-53: $ sudo systemctl restart apache2.service
acer@acer-Aspire-A315-53: $
```

## 6 Secure the MySQL server deployment

To secure the MySQL service I run the *mysql\_secure\_installation* script.



```
acer@acer-Aspire-A315-53:~$ sudo mysql_secure_installation
[sudo] password for acer:

Securing the MySQL server deployment.

Enter password for user root:
The 'validate_password' component is installed on the server.
The subsequent steps will run with the existing configuration
of the component.
Using existing password for root.

Estimated strength of the password: 100
Change the password for root ? ((Press y|Y for Yes, any other key for No) : n

... skipping.
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.

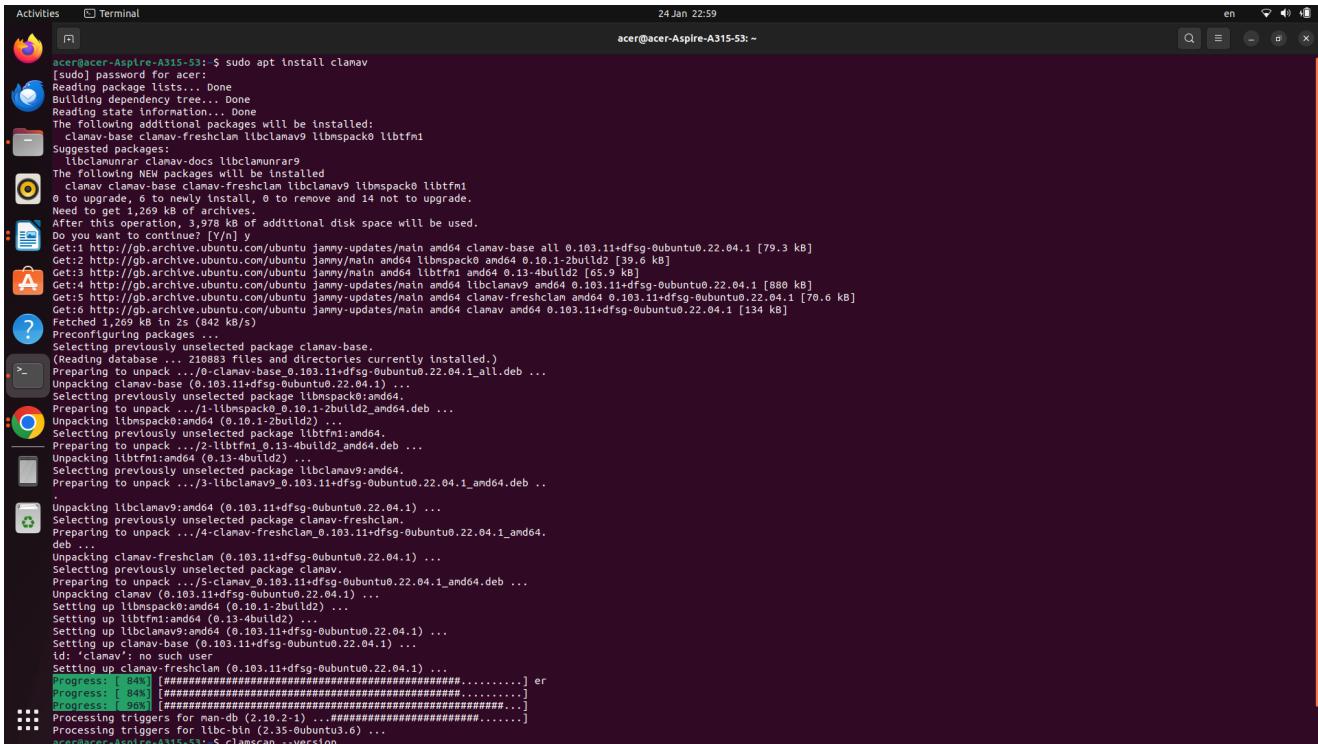
Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
```

## 7. Installing ClamAV (Anti-Virus Protection)

I Installed the clamav package by running the following command: **sudo apt install clamav**



```
acer@acer-Aspire-A315-53: ~$ sudo apt install clamav
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  clamav-base clamav-freshclam libclamav9 libmspack0 libtfrm1
  libclamunrar clamav-docs libclamunrar9
The following NEW packages will be installed:
  clamav clamav-base clamav-freshclam libclamav9 libmspack0 libtfrm1
0 to upgrade, 6 to newly install, 0 to remove and 14 not to upgrade.
Need to get 1,267 kB of archives.
After this operation, 5,290 kB additional disk space will be used.

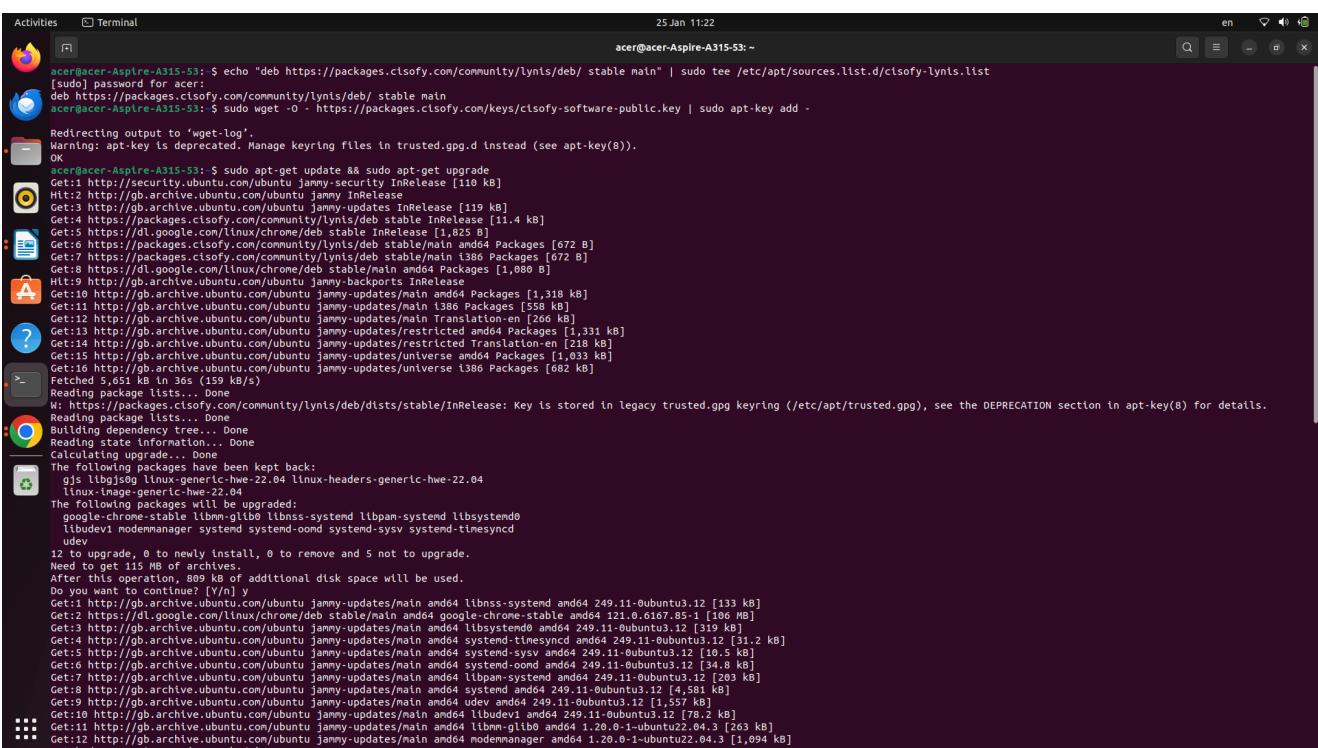
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 clamav-base all 0.103.11+dfsg-0ubuntu0.22.04.1 [79.3 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 libmspack0 amd64 0.10.1-2build2 [39.6 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 libtfrm1 amd64 0.13-4build2 [65.9 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libclamav9 amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [880 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav-freshclam amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [76.6 kB]
Get:6 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [134 kB]
Fetched 5,290 kB in 2s (242 kB/s)
Preconfiguring packages...
Selecting previously unselected package clamav-base.
(Reading database ... 210883 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.103.11+dfsg-0ubuntu0.22.04.1_all.deb ...
Unpacking clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package libmspack0:amd64.
Preparing to unpack .../1-libmspack0_0.10.1-2build2_amd64.deb ...
Unpacking libmspack0:amd64 (0.10.1-2build2) ...
Selecting previously unselected package libtfrm1:amd64.
Preparing to unpack .../2-libtfrm1_0.13-4build2_amd64.deb ...
Unpacking libtfrm1:amd64 (0.13-4build2) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../3-libclamav9_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../4-clamav-freshclam_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../5-clamav_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up libmspack0:amd64 (0.10.1-2build2) ...
Setting up libtfrm1:amd64 (0.13-4build2) ...
Setting up libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
id: 'Clamav': no such user
Setting up clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Progress: [ 94%] [########################################.....] er
Progress: [ 94%] [########################################.....] er
Progress: [ 96%] [########################################.....]
Processing triggers for man-db (2.18.2-1) ...
Processing triggers for lsb-bin (2.35-0ubuntu3.6) ...
acer@acer-Aspire-A315-53: ~$ clamscan --version
```

## 8. Installing Lynis

I add the CISOfy repository to list of repos:**echo "deb**

**https://packages.cisofy.com/community/lynis/deb/ stable main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list**

Then, import a public GPG key for a secure Lynis installation:**sudo wget -O - https://packages.cisofy.com/keys/cisofy-software-public.key | sudo apt-key add -**



```
acer@acer-Aspire-A315-53: ~$ echo "deb https://packages.cisofy.com/community/lynis/deb/ stable main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list
[sudo] password for acer:
deb https://packages.cisofy.com/community/lynis/deb/ stable main
acer@acer-Aspire-A315-53: ~$ sudo wget -O - https://packages.cisofy.com/keys/cisofy-software-public.key | sudo apt-key add -
Redirecting output to 'wget.log'.
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
acer@acer-Aspire-A315-53: ~$ sudo apt-get update && sudo apt-get upgrade
OK
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:2 http://gb.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:4 https://packages.cisofy.com/community/lynis/deb/stable InRelease [11.4 kB]
Get:5 https://dl.google.com/linux/chrome/deb/stable InRelease [1,025 B]
Get:6 https://dl.google.com/linux/chrome/deb/stable/main i386 Packages [672 B]
Get:7 https://packages.cisofy.com/community/lynis/deb/stable/main i386 Packages [672 B]
Get:8 https://dl.google.com/linux/chrome/deb/stable/main amd64 Packages [1,080 B]
Hit:9 http://gb.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:10 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1,318 kB]
Get:11 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [558 kB]
Get:12 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [266 kB]
Get:13 http://gb.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [1,331 kB]
Get:14 http://gb.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [228 kB]
Get:15 http://gb.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,022 kB]
Get:16 http://gb.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [682 kB]
Fetched 5,651 kB in 30s (159 kB/s)
Reading package lists... Done
W: https://packages.cisofy.com/community/lynis/deb/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  gis/libgis9g linux-generic-hwe-22.04 linux-headers-generic-hwe-22.04
  linux-image-generic-hwe-22.04
The following packages will be upgraded:
  google-chrome-stable libgnutls-openssl libnss-syst� libpam-syst� libsystemd
  libubidev1 modemmanager syst�d-oond syst�d-sysv syst�d-timesyncd
  udev
12 to upgrade, 0 to newly install, 0 to remove and 5 not to upgrade.
Need to get 115 MB of archives.
After this operation, 899 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnss-syst� and64 249.11-0ubuntu3.12 [133 kB]
Get:2 https://dl.google.com/linux/chrome/deb/stable/main amd64 google-chrome-stable and64 121.0.6167.85-1 [106 MB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 syst�d and64 249.11-0ubuntu3.12 [319 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 syst�d-timesyncd and64 249.11-0ubuntu3.12 [31.2 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 syst�d-timesyncd and64 249.11-0ubuntu3.12 [15.5 kB]
Get:6 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpam-syst� and64 249.11-0ubuntu3.12 [34.8 kB]
Get:7 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpam-syst� and64 249.11-0ubuntu3.12 [4,581 kB]
Get:8 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 and6d and64 249.11-0ubuntu3.12 [4,581 kB]
Get:9 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 udev and64 249.11-0ubuntu3.12 [1,557 kB]
Get:10 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libudev1 and64 249.11-0ubuntu3.12 [78.2 kB]
Get:11 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libgnutls-openssl and64 1.20.0-1-ubuntu22.04.3 [263 kB]
Get:12 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 modemmanager and64 1.20.0-1-ubuntu22.04.3 [1,094 kB]
Fetched 115 MB in 38s (3,815 kB/s)
```

Then install Linus by running the following command:

```
sudo apt install lynis
```

```
acer@acer-Aspire-A315-53:~$ sudo apt install lynis
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed
  lynis
0 to upgrade, 1 to newly install, 0 to remove and 5 not to upgrade.
Need to get 265 kB of archives.
After this operation, 1,695 kB of additional disk space will be used.
Get:1 https://packages.cisofy.com/community/lynis/deb stable/main amd64 lynis all 3.0.9-100 [265 kB]
Fetched 265 kB in 0s (770 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 210964 files and directories currently installed.)
Preparing to unpack .../lynis_3.0.9-100_all.deb ...
Unpacking lynis (3.0.9-100) ...
Setting up lynis (3.0.9-100) ...
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53:~$ lynis show options
--auditor
--cronjob (--cron)
--debug
--developer
--devops
--forensics
--help (-h)
--log-file
--manpage (--man)
--no-colors
--no-log
--no-plugins
--pentest
--profile
--plugin-dir
--quick (-Q)
--quiet (-q)
--report-file
--reverse-colors
--tests
--tests-from-category
--tests-from-group
--usecwd
--upload
--verbose
--version (-V)
--wait
--warnings-only
```

Before scanning, I ensured that Lynis is up to date.

```
acer@acer-Aspire-A315-53:~$ sudo lynis update info
== Lynis ==
Version      : 3.0.9
Status       : Up-to-date
Release date : 2023-08-03
Project page : https://cisofy.com/lynis/
Source code   : https://github.com/CISOfy/lynis
Latest package : https://packages.cisofy.com/
```

## 9. Using a MySAT

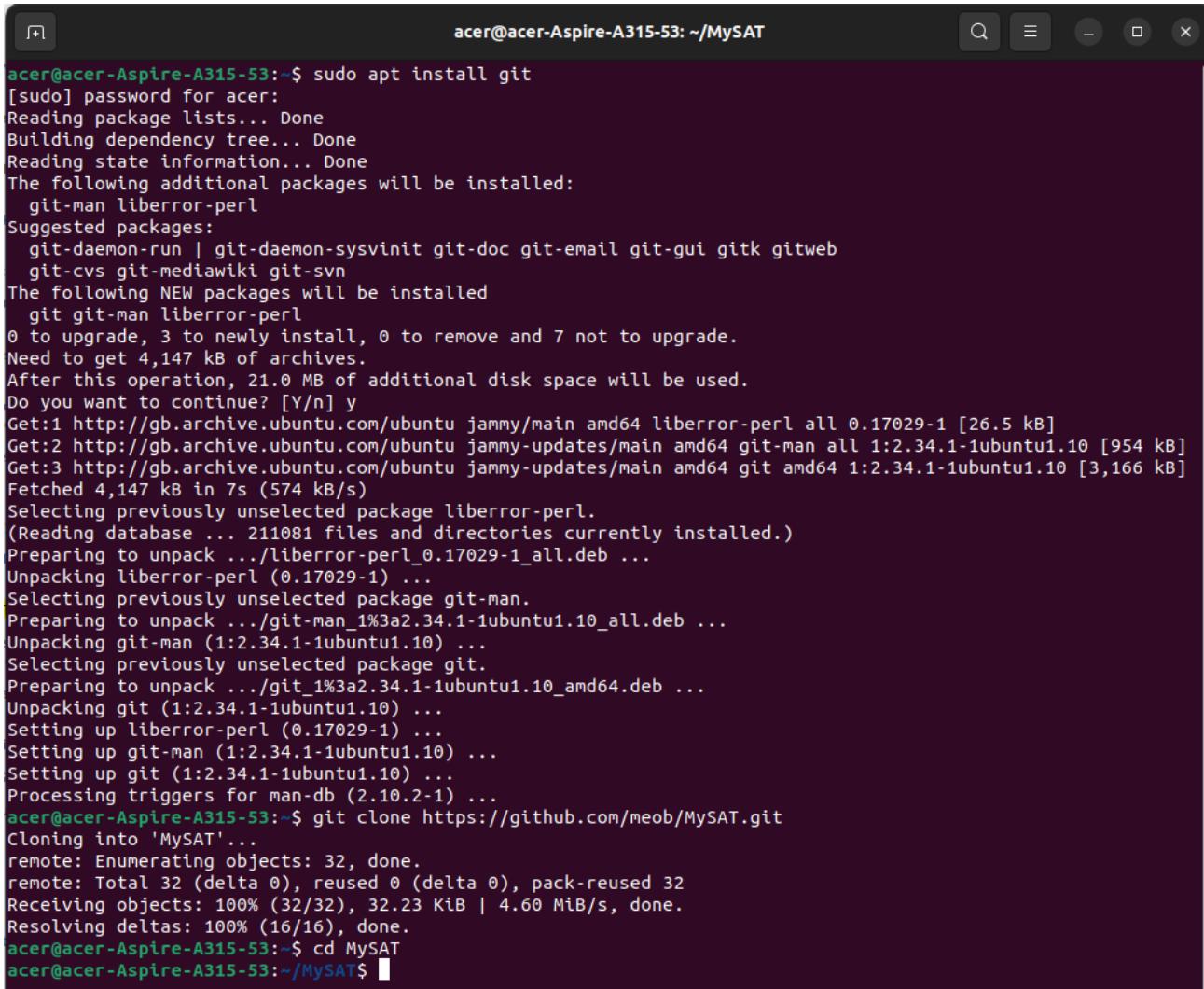
I audit the security of MySQL server by using a tool MySAT. MySAT performs several test to analyze database configurations and security policies. MySAT help to assess and therefore increase MySQL database security. MySAT results are output in HTML format.

I cloned the MySAT Github repository by running the following command:

```
git clone https://github.com/meob/MySAT.git
```

and navigated into the MySAT directory, which contains the `mysat.sql` file and used in conjunction with the MySQL server to output the results into a `MySAT.htm` file.

```
cd MySAT
```



The screenshot shows a terminal window titled "acer@acer-Aspire-A315-53: ~/MySAT". The terminal displays the following command and its execution:

```
acer@acer-Aspire-A315-53:~$ sudo apt install git
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb
  git-cvs git-mediawiki git-svn
The following NEW packages will be installed
  git git-man liberror-perl
0 to upgrade, 3 to newly install, 0 to remove and 7 not to upgrade.
Need to get 4,147 kB of archives.
After this operation, 21.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 liberror-perl all 0.17029-1 [26.5 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git-man all 1:2.34.1-1ubuntu1.10 [954 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git amd64 1:2.34.1-1ubuntu1.10 [3,166 kB]
Fetched 4,147 kB in 7s (574 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 211081 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17029-1_all.deb ...
Unpacking liberror-perl (0.17029-1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a2.34.1-1ubuntu1.10_all.deb ...
Unpacking git-man (1:2.34.1-1ubuntu1.10) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.34.1-1ubuntu1.10_amd64.deb ...
Unpacking git (1:2.34.1-1ubuntu1.10) ...
Setting up liberror-perl (0.17029-1) ...
Setting up git-man (1:2.34.1-1ubuntu1.10) ...
Setting up git (1:2.34.1-1ubuntu1.10) ...
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53:~$ git clone https://github.com/meob/MySAT.git
Cloning into 'MySAT'...
remote: Enumerating objects: 32, done.
remote: Total 32 (delta 0), reused 0 (delta 0), pack-reused 32
Receiving objects: 100% (32/32), 32.23 KiB | 4.60 MiB/s, done.
Resolving deltas: 100% (16/16), done.
acer@acer-Aspire-A315-53:~$ cd MySAT
acer@acer-Aspire-A315-53:~/MySAT$
```

## 10. Install Chkrootkit – A Linux Rootkit Scanner

The chkrootkit tool I installed using the following command:

```
sudo apt install chkrootkit
```

```

Activities Terminal 3 Feb 17:19
acer@acer-Aspire-A315-53: $ sudo apt install chkrootkit
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu libbinutils liblctf-nobfd0
liblctf0
Suggested packages:
binutils
The following NEW packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu chkrootkit libbinutils
liblctf-nobfd0 liblctf0
0 to upgrade, 7 to newly install, 0 to remove and 8 not to upgrade.
Need to get 3,776 kB of archives.
After this operation, 15.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 binutils-common amd64 2.38-4ubuntu2.5 [222 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libbinutils amd64 2.38-4ubuntu2.5 [662 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 liblctf-nobfd0 amd64 2.38-4ubuntu2.5 [108 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 liblctf0 amd64 2.38-4ubuntu2.5 [103 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 binutils-x86_64-linux-gnu amd64 2.38-4ubuntu2.5 [2,326 kB]
Get:6 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 binutils amd64 2.38-4ubuntu2.5 [3,202 kB]
Get:7 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 chkrootkit amd64 0.55-4 [352 kB]
Fetched 3,776 kB in 9s (400 kB/s)
Selecting previously unselected package binutils-common:amd64.
(Reading database ... 212570 files and directories currently installed.)
Preparing to unpack .../0-binutils-common:amd64 (2.38-4ubuntu2.5_amd64.deb ...
Unpacking binutils-common:amd64 (2.38-4ubuntu2.5) ...
Selecting previously unselected package libbinutils:amd64.
Preparing to unpack .../1-libbinutils:amd64 (2.38-4ubuntu2.5_amd64.deb ...
Unpacking libbinutils:amd64 (2.38-4ubuntu2.5) ...
Selecting previously unselected package liblctf-nobfd0:amd64.
Preparing to unpack .../2-liblctf-nobfd0_2.38-4ubuntu2.5_amd64.deb ...
Unpacking liblctf-nobfd0:amd64 (2.38-4ubuntu2.5) ...
Selecting previously unselected package liblctf0:amd64.
Preparing to unpack .../3-liblctf0_2.38-4ubuntu2.5_amd64.deb ...
Unpacking liblctf0:amd64 (2.38-4ubuntu2.5) ...
Selecting previously unselected package binutils-x86_64-linux-gnu.
Preparing to unpack .../4-binutils-x86_64-linux-gnu:2.38-4ubuntu2.5_amd64.deb ...
Unpacking binutils-x86_64-linux-gnu (2.38-4ubuntu2.5) ...
Selecting previously unselected package binutils.
Preparing to unpack .../5-binutils_2.38-4ubuntu2.5_amd64.deb ...
Unpacking binutils (2.38-4ubuntu2.5) ...
Selecting previously unselected package chkrootkit.
Preparing to unpack .../6-chkrootkit_0.55-4_amd64.deb ...
Unpacking chkrootkit (0.55-4) ...
Selecting previously unselected package binutils-common:amd64 (2.38-4ubuntu2.5) ...
Setting up liblctf-nobfd0:amd64 (2.38-4ubuntu2.5) ...
Setting up chkrootkit (0.55-4) ...
Setting up libbinutils:amd64 (2.38-4ubuntu2.5) ...
Setting up liblctf0:amd64 (2.38-4ubuntu2.5) ...
Setting up binutils-x86_64-linux-gnu (2.38-4ubuntu2.5) ...
Setting up binutils (2.38-4ubuntu2.5) ...
Processing triggers for libhr-hlo (2.35-6ubuntu3.6) ...

```

## 11. The rkhunter tool was installed using the following command on Ubuntu and RHEL-based systems:

`sudo apt install rkhunter`

```

Activities Terminal 3 Feb 17:31
acer@acer-Aspire-A315-53: $ sudo apt install rkhunter
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
fonts-lato javascript-common libjs-jquery libruby3.0 net-tools rake ruby
ruby-net-telnet ruby-rubygems ruby-webrick ruby-xmlext ruby3.0
rubygems-integration unihde unihde.rb
0 upgraded, 0 newly installed, 0 to remove and 8 not to upgrade.
Need to get 9,656 kB of archives.
After this operation, 39.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 fonts-lato all 2.0.2-1 [2,696 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.0.0+git20181003.0.eebcebe-1ubuntu5 [204 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 rkhunter all 1.4.6-10 [226 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 javascript-common all 3.1+nmu1 [5,936 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 ruby-rubygems all 3.0.2-1+nmu1 [321 kB]
Get:6 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 ruby-rubygems-integration all 1.1.18 [5,336 kB]
Get:7 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ruby3.0 amd64 3.0.2-2~ubuntu2.4 [50.1 kB]
Get:8 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 ruby-rubygems all 3.3.5-2 [228 kB]
Get:9 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 rake all 1.3.0-6-2 [61.7 kB]
Get:10 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 ruby-webrick all 1.7.0-1 [12.6 kB]
Get:11 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 ruby-webrick all 1.7.0-3 [51.8 kB]
Get:12 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ruby-xmlext all 0.3.2-2~ubuntu0.1 [24.9 kB]
Get:13 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libruby3.0 amd64 3.0.2-2~ubuntu2.4 [5,113 kB]
Get:14 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 unihde.ruby.all deb all 22-6 [8,942 B]
Fetched 9,656 kB in 19s (479 kB/s)
Selecting previously unselected package fonts-lato.
(Reading database ... 212867 files and directories currently installed.)
Preparing to unpack .../0-fonts-lato_2.0-2.1_all.deb ...
Unpacking fonts-lato (2.0-2.1) ...
Selecting previously unselected package net-tools.
Preparing to unpack .../01-net-tools_1.00+git20181003.0.eebcebe-1ubuntu5_amd64.deb ...
Unpacking net-tools (1.00+git20181003.0.eebcebe-1ubuntu5) ...
Selecting previously unselected package rkhunter.
Preparing to unpack .../02-rkhunter_1.4.6-10_all.deb ...
Unpacking rkhunter (1.4.6-10) ...
Selecting previously unselected package javascript-common.
Preparing to unpack .../03-javascript-common_11+nmu1_all.deb ...
Unpacking javascript-common (11+nmu1) ...
Selecting previously unselected package libjs-jquery.
Preparing to unpack .../04-libjs-jquery_3.6.0+dfsg+3.5.13-1_all.deb ...
Unpacking libjs-jquery (3.6.0+dfsg+3.5.13-1) ...
Selecting previously unselected package rubygems-integration.
Preparing to unpack .../05-rubygems-integration_1.18_all.deb ...

```

## 12.I installed Nmap on Ubuntu 22.04:

`sudo apt install nmap`

Activities Terminal 3 Feb 22:26 acer@acer-Aspire-A315-53: ~

```
acer@acer-Aspire-A315-53: ~$ sudo apt install nmap
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libllinear4 libllinear4-dev ncat nifff zenmap
libblas3 libllinear4 libllinear4-dev nmap-common
0 to upgrade, 5 to newly install, 0 to remove and 8 not to upgrade.
Need to get 5,973 kB of archives.
After this operation, 11.3 MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get: http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 libblas3 amd64 3.10.0-2ubuntu1 [228 kB]
Get: http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 libllinear4 amd64 2.3.0+dfsg-5 [41.4 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 libllinear4 libllinear4-dev 1.6.2-2.1 [31.4 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap-common all 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [3,940 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap amd64 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [1,731 kB]
Fetched 5,973 kB in 4s (1,562 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 216011 files and directories currently installed.)
Preparing to unpack .../libblas3_3.10.0-2ubuntu1_amd64.deb ...
Unpacking libblas3:amd64 (3.10.0-2ubuntu1) ...
Selecting previously unselected package libllinear4:amd64.
Preparing to unpack .../libllinear4_2.3.0+dfsg-5_amd64.deb ...
Unpacking libllinear4:amd64 (2.3.0+dfsg-5) ...
Selecting previously unselected package libllinear4 libllinear4-dev:amd64.
Preparing to unpack .../libllinear4_1.6.2-2.1_amd64.deb ...
Unpacking libllinear4 libllinear4-dev:amd64 (1.6.2-2.1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_all.deb ...
Unpacking nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_amd64.deb ...
Unpacking nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up libblas3:amd64 (3.10.0-2ubuntu1) ...
Setting up alternatives: using /usr/lib/x86_64-linux-gnu/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode
Setting up nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up libllinear4:amd64 (2.3.0+dfsg-5) ...
Setting up libllinear4 libllinear4-dev:amd64 (2.3.0+dfsg-5) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
acer@acer-Aspire-A315-53: ~
```

## **4. Test the system against common threats**

### **4.1 I can develop a basic test regime**

Developing a basic test regime for ensuring the security of a system involves a systematic approach that covers various aspects of the site and different levels of protection. Considering the different methods of threats generation, including push and pull methods, the test regime should encompass measures to mitigate each type of threat. Here's a basic outline for such a test regime:

- Threat Assessment and Analysis:
  - Conduct a thorough assessment of potential threats, including push and pull methods mentioned (SPAM, phishing, spoofs, malware, injections, pharmings, spear phishing, drive-bys).
  - Analyze the potential impact of each threat on the system, considering the sensitivity and value of the data involved.
- Vulnerability Scanning:
  - Utilize automated tools to scan the system for known vulnerabilities.
  - Regularly update the scanning tools to ensure coverage of the latest threats and vulnerabilities.
  - Address identified vulnerabilities promptly through patches, updates, or configuration changes.
- Penetration Testing:
  - Conduct penetration testing to simulate real-world attacks and identify potential weaknesses in the system.
  - Test both push and pull methods to evaluate the system's resilience against various types of attacks.
  - Engage skilled professionals or ethical hackers to perform penetration testing and provide detailed reports on vulnerabilities and recommendations for mitigation.
- Security Controls Testing:
  - Verify the effectiveness of security controls implemented in the system, such as firewalls, intrusion detection/prevention systems, access controls, encryption mechanisms, etc.
  - Ensure that security controls are properly configured and functioning as intended.
- Authentication and Authorization Testing:
  - Test the strength of authentication mechanisms (e.g., passwords, multi-factor authentication) to prevent unauthorized access.
  - Verify proper enforcement of access control policies to restrict access to sensitive data based on user roles and permissions.
- Data Protection Testing:
  - Validate data protection measures, including encryption of sensitive data both at rest and in transit.
  - Test for potential data leakage or exposure through various channels, such as APIs, databases, and file systems.
- Social Engineering Testing:
  - Conduct simulated social engineering attacks, such as phishing and spear phishing campaigns, to assess the susceptibility of users to manipulation.
  - Provide training and awareness programs to educate users on identifying and avoiding social engineering attacks.
- Incident Response Testing:
  - Develop and test incident response plans to ensure a timely and effective response to security incidents.

- Conduct tabletop exercises or simulated incident scenarios to validate the readiness of the incident response team and the effectiveness of response procedures.
- Continuous Monitoring and Improvement:
  - Implement continuous monitoring mechanisms to detect and respond to security threats in real-time.
  - Regularly review and update the test regime based on evolving threats, changes in the system architecture, and lessons learned from previous security incidents.
- Documentation and Reporting:
  - Document test procedures, findings, and remediation actions taken.
  - Provide comprehensive reports to stakeholders, including management, IT teams, and regulatory bodies, to demonstrate compliance with security requirements and ongoing efforts to protect the system.

By following this test regime, organizations can systematically identify and mitigate security risks, strengthen their defences against various types of threats, and enhance the overall security posture of their systems.

#### **4.2 I can explain the purpose of the main test procedures**

The purpose of the main test procedures:

- Assess whether common security best practices are implemented.
- Evaluate the server's susceptibility to known attack vectors.
- Deter automated attacks and slow down potential attackers by introducing obstacles.
- Prevent unauthorized access to critical system resources, such as the root account.

#### **4.3 I can explain the expected results from the test**

When conducting a test for a LAMP (Linux, Apache, MySQL, PHP) server, the expected results depend on the specific test being performed. Overall, the expected results from the test for a LAMP server involve confirming that all components (Apache, MySQL, PHP) are functioning correctly, the website is accessible, and appropriate security measures are in place. Any anomalies discovered during the test should be investigated and addressed promptly to ensure the server's reliability, performance, and security.

#### **Test Plan**

| <b>Test</b>            | <b>Description</b>                                  | <b>Test step</b>   | <b>Expected result</b>  | <b>Status</b> |
|------------------------|---|--|---|---------------|
| Checking Apache server | The Apache service should be running and accessible | test that the virtual host works as expected:<br><br>nano /var/www/my_do | The test should confirm that Apache is running without errors and | Pass          |

|                                |  |   |  |      |
|--------------------------------|--|---|--|------|
|                                |  | main/index.html<br>var/www/<br>your_domain/<br>index.html   | that the server<br>responds to HTTP<br>requests  |      |
| Testing MySQL Service          | The MySQL service should be running and accessible   | Test by command<br>sudo mysql   | The test should confirm that MySQL is running without errors and that it's possible to connect to the MySQL server.                      | Pass |
| Verifying PHP Interpreter      | PHP should be installed and configured correctly   | create a new file named info.php<br>nano /var/www/my_domain/main/info.php<br>/var/www/my_domain/info.php  | The test should confirm that PHP scripts can be executed by the server without errors.   | Pass |
| Checking Database Connectivity | The PHP application should be able to connect to the MySQL database                              | create database CREATE DATABASE example_database<br>create the PHP script that connected to MySQL and query for content.<br>nano /var/www/my_domain/todo_list.php | The test should confirm that the PHP application can establish a connection to the MySQL database and perform basic database operations. | Pass |
| Monitoring With Fail2Ban       | The Fail2Ban monitor all the failed authentication attempts and the various blocked IP addresses | check the status of Fail2Ban and the active jails:<br>sudo fail2ban-client status   | The test should show all of failed and banned IP addresses.  | Pass |
| Scanning with ClamAV           | To scan the /etc directory for infected files  | run the command:<br>sudo clamscan -i -r --remove  | After the scan is completed, a summary of all infected files   | Pass |

|                              |   |  |  |   |
|------------------------------|---|--|--|---|
|                              |   | /etc   | found should be displayed.   |   |
| Security Auditing with Lynis | The summary of the system audit reveals important information about system's security posture and various security misconfigurations and vulnerabilities. | Run Lynis:<br>sudo lynis audit system  | The server is effectively protected from unauthorized access.  | In the report, Linus displays any potential warnings that indicate a severe security vulnerability or misconfiguration that needs to be fixed or patched. |
| Auditing MySQL Security      | In the MySAT.htm file should be the detailed analysis results generated by MySAT, highlighting potential vulnerabilities and areas for improvement.       | Run:<br>the mysat.sql file with root permission and output to the MySAT.htm file | The failed configuration check is color coded in orange and a passed check is color coded in green.  | MySAT provided recommendations for improving the security of the MySQL database.  |
| Check server with Chkrootkit | Scan if the system is infected with a 'rootkit'.  | Run :<br>sudo chkrootkit   | The server is effectively protected from unauthorized access. This test show that chkrootkit not found signs that the system is infected with a 'rootkit'. | Pass  |
| Check server with rkhunter   | Scan if the system is infected with a 'rootkit'.  | Run command:<br>sudo rkhunter -c   | The server is effectively protected from unauthorized access.This test shown the files not infected. Rootkits not found.                                   | Pass  |

|                |   |   |  |      |
|----------------|---|---|--|------|
| Scan with Nmap | Use Nmap scan the IP address, scan the host, find a live host | Scan the "192.168.214.138" for open ports:<br>nmap -F 192.168.214.138 | Test should show the list of all live hosts, check the open ports on the network, real-time information about the network. | Pass |
|----------------|---|---|--|------|

- Checking Apache Service:
  - Expected Outcome: The Apache service should be running and accessible.
  - Result: The test should confirm that Apache is running without errors and that the server responds to HTTP requests.
- Testing MySQL Service:
  - Expected Outcome: The MySQL service should be running and accessible.
  - Result: The test should confirm that MySQL is running without errors and that it's possible to connect to the MySQL server.
- Verifying PHP Interpreter:
  - Expected Outcome: PHP should be installed and configured correctly.
  - Result: The test should confirm that PHP scripts can be executed by the server without errors.
- Testing Website Availability:
  - Expected Outcome: The website hosted on the LAMP server should be accessible.
  - Result: The test should confirm that the website is reachable through its domain or IP address, and web pages load correctly without errors.
- Checking Database Connectivity:
  - Expected Outcome: The PHP application should be able to connect to the MySQL database.
  - Result: The test should confirm that the PHP application can establish a connection to the MySQL database and perform basic database operations.
- Testing Security Measures:
  - Expected Outcome: Security configurations, such as file permissions and firewall rules, should be properly set up.
  - Result: The test should confirm that sensitive files are not accessible to unauthorized users and that firewall rules are effectively protecting the server from unauthorized access.

## 4.4 I can describe the test results and what they mean

### Checking apache server

Then I created an `index.html` file in that location to test that the virtual host works as expected:

```
nano /var/www/my_domain/index.html  
var/www/your_domain/index.html
```

```
<html>  
  <head>  
    <title>your_domain website</title>  
  </head>  
  <body>  
    <h1>Hello World!</h1>  
  
    <p>This is the landing page of <strong>your_domain</strong>.</p>  
  </body>  
</html>
```

← → ⌂ 127.0.0.1

### Hello World!

This is the landing page of **my\_domain**.

### Testing to log in to the MySQL :

```
sudo mysql
```

This connected to the MySQL server as the administrative database user root, which is inferred by the use of `sudo` when running this command.

I need to provide a password to connect as the root user.

```
success!
```

```
All done!
acer@acer-Aspire-A315-53:~$ sudo mysql
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO
acer@acer-Aspire-A315-53:~$ ^C
acer@acer-Aspire-A315-53:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.35-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> exit
Bye
acer@acer-Aspire-A315-53:~$
```

This test confirmed that MySQL is running without errors and that it's possible to connect to the MySQL server.

### Testing PHP Processing on my Web Server

I created a PHP test script to confirm that Apache is able to handle and process requests for PHP files. I created a new file named `info.php` inside my custom web root folder:

```
nano /var/www/my_domain/info.php
/var/www/my_domain/info.php
```

```
<?php
phpinfo();
```

Activities Firefox Web Browser 20 Jan 20:53

How To Install | PHP 8.1.2-1ubuntu2.14 | OpenSSH ALLO | How to open s | How to limit ss | How To Ubuntu | New Tab | Anywhere ALLO | OpenSSH ALLO | UFW Essential | + | - | x

127.0.0.1/info.php

**PHP Version 8.1.2-1ubuntu2.14**

**System**

|   |   |
|---|---|
| Build Date                              | Aug 18 2023 11:41:11  |
| Build System                            | Linux   |
| Server API                              | Apache 2.0 Handler  |
| Virtual Directory Support               | disabled  |
| Configuration File (php.ini) Path       | /etc/php/8.1/apache2  |
| Loaded Configuration File               | /etc/php/8.1/apache2/php.ini  |
| Scan this dir for additional .ini files |   |
| Additional .ini files parsed            | /etc/php/8.1/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.1/apache2/conf.d/20-opcache.ini, /etc/php/8.1/apache2/conf.d/10-pdo.ini, /etc/php/8.1/apache2/conf.d/20-calendar.ini, /etc/php/8.1/apache2/conf.d/20-ctype.ini, /etc/php/8.1/apache2/conf.d/20-exif.ini, /etc/php/8.1/apache2/conf.d/20-ffi.ini, /etc/php/8.1/apache2/conf.d/20-fileinfo.ini, /etc/php/8.1/apache2/conf.d/20-ftp.ini, /etc/php/8.1/apache2/conf.d/20-gettext.ini, /etc/php/8.1/apache2/conf.d/20-iconv.ini, /etc/php/8.1/apache2/conf.d/20-phar.ini, /etc/php/8.1/apache2/conf.d/20-posix.ini, /etc/php/8.1/apache2/conf.d/20-readline.ini, /etc/php/8.1/apache2/conf.d/20-shmop.ini, /etc/php/8.1/apache2/conf.d/20-sockets.ini, /etc/php/8.1/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.1/apache2/conf.d/20-sysvshm.ini, /etc/php/8.1/apache2/conf.d/20-tokenizer.ini |

**PHP API** 20210902

**PHP Extension** 20210902

**Zend Extension** 420210902

**Zend Extension Build** API20210902.0NTS

**PHP Extension Build** API20210902.0NTS

**Debug Build** no

**Thread Safety** disabled

**Zend Signal Handling** enabled

**Zend Memory Manager** enabled

**Zend MultiByte Support** disabled

**IPv6 Support** enabled

**DTrace Support** available, disabled

**Registered PHP Streams** https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar

**Registered Stream Socket Transports** tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3

**Registered Stream Filters** zlib.\*, string.rot13, string.toupper, string.tolower, convert.\*, consumed, dechunk, convert.iconv.\*

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v4.1.2, Copyright (c) Zend Technologies  
with Zend OPcache v8.1.2-1ubuntu2.14, Copyright (c), by Zend Technologies

**zendengine**

## Configuration

Activities Firefox Web Browser 20 Jan 20:53

How To Install | PHP 8.1.2-1ubuntu2.14 | OpenSSH ALLO | How to open s | How to limit ss | How To Ubuntu | New Tab | Anywhere ALLO | OpenSSH ALLO | UFW Essential | + | - | x

127.0.0.1/info.php

**Configuration**

**apache2handler**

|                      |  |
|----------------------|--|
| Apache Version       | Apache/2.4.52 (Ubuntu)   |
| Apache API Version   | 20120211   |
| Server Administrator | webmaster@localhost  |
| Hostname:Port        | my_domain:0  |
| User/Group           | www-data(33)/33  |
| Max Requests         | Per Child: 0 - Keep Alive: on - Max Per Connection: 100  |
| Timeouts             | Connection: 300 - Keep-Alive: 5  |
| Virtual Server       | Yes  |
| Server Root          | /etc/apache2   |
| Loaded Modules       | core mod_so mod_watchdog http_core mod_log_config mod_logio mod_version mod_mod_imod mod_access_compat mod_alias mod_authn_core mod_authn_file mod_authz_core mod_authz_host mod_authz_user mod_autoindex mod_deflate mod_dir mod_env mod_filter mod_mime prefork mod_negotiation mod_php mod_reqtimeout mod_setenvif mod_status |

| Directive     | Local Value | Master Value |
|---------------|-------------|--------------|
| engine        | On          | On           |
| last_modified | Off         | Off          |
| xbitHack      | Off         | Off          |

**Apache Environment**

|                                |   |
|--------------------------------|---|
| Variable                       | Value   |
| HTTP_HOST                      | 127.0.0.1   |
| HTTP_USER_AGENT                | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0      |
| HTTP_ACCEPT                    | text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*;q=0.8 |
| HTTP_ACCEPT_LANGUAGE           | en-GB,en;q=0.5  |
| HTTP_ACCEPT_ENCODING           | gzip, deflate, br   |
| HTTP_CONNECTION                | keep-alive  |
| HTTP_UPGRADE_INSECURE_REQUESTS | 1   |
| HTTP_SEC_FETCH_DEST            | document  |
| HTTP_SEC_FETCH_MODE            | navigate  |
| HTTP_SEC_FETCH_SITE            | none  |
| HTTP_SEC_FETCH_USER            | ?1  |
| PATH                           | /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin              |
| SERVER_SIGNATURE               | <address>Apache/2.4.52 (Ubuntu) Server at 127.0.0.1 Port 80</address>               |
| SERVER_SOFTWARE                | Apache/2.4.52 (Ubuntu)  |
| SERVER_NAME                    | 127.0.0.1   |
| SERVER_ADDR                    | 127.0.0.1   |

This page provides information about my server from the perspective of PHP. I got this page in my browser as proof that the PHP installation is working properly.

## Testing Database Connection from PHP

I created a new database

```
CREATE DATABASE example_database;
```

Then created a new user that authenticates with the `caching_sha2_password` method and grant them full privileges on the `example_database`.

```
CREATE USER 'example_user'@'%' IDENTIFIED BY 'password';
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY
'password';
GRANT ALL ON example_database.* TO 'example_user'@'%';
exit
```

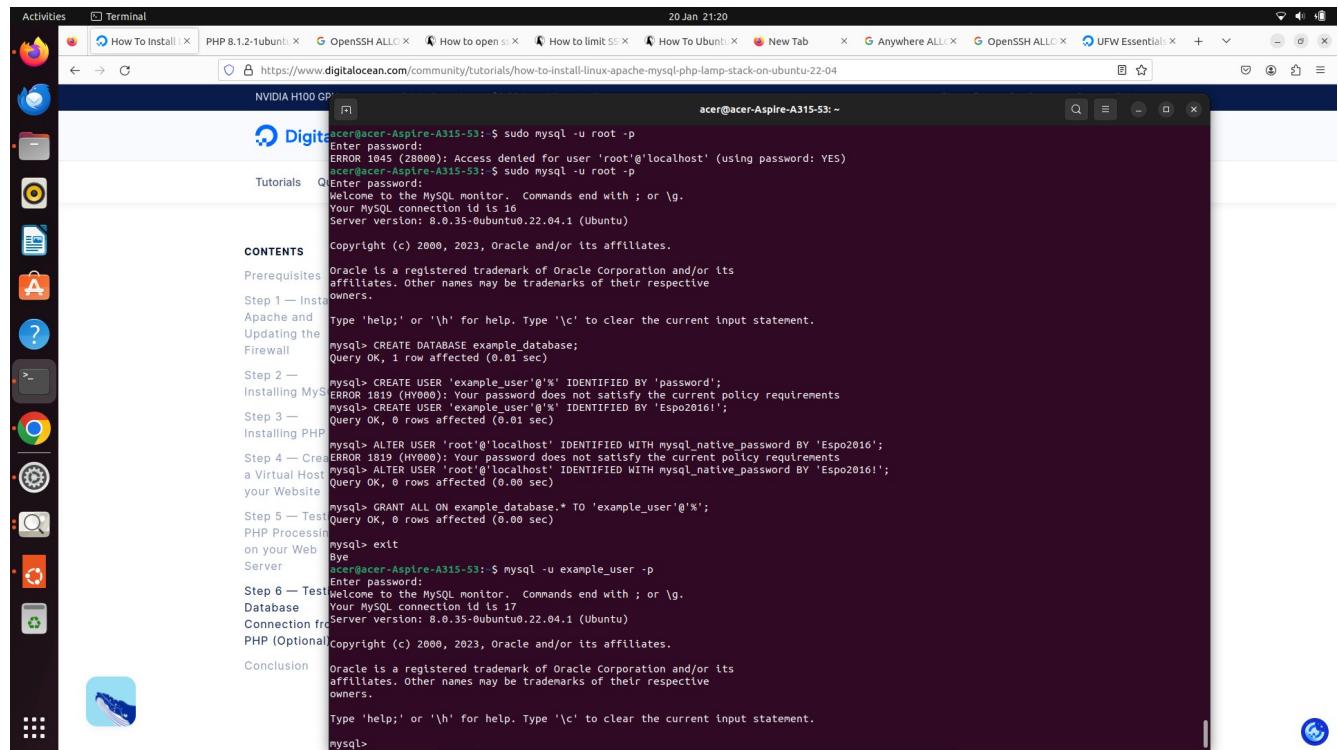
I tested if the new user has the proper permissions by logging in to the MySQL console , using the custom user credentials.

After logging in to the MySQL console, I tested that I have access to the `example_database` database:

```
SHOW DATABASES;
```

Next, I created a test table named `todo_list` and Inserted a few rows of content in the test table To confirm that the data was successfully saved to your table, I run:

```
SELECT * FROM example_database.todo_list;
```



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and it displays a MySQL session. The session starts with a root password entry, followed by creating a new database named "example\_database". Then, it attempts to create a user "example\_user" with a password, but fails due to policy requirements. It then creates a user "root" with the native password method. Finally, it grants all privileges on the "example\_database" to the "example\_user". The terminal window is part of a desktop interface with a sidebar containing links like "Activities", "Terminal", "How To Install", "OpenSSH ALLO", "How to open", "How to limit", "How To Bunt", "New Tab", "Anywhere ALLO", "OpenSSH ALLO", and "UFW Essentials". The desktop background is visible, showing icons for various applications like a browser, file manager, and system tools.

```
acer@acer-Aspire-A315-53:~$ sudo mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
acer@acer-Aspire-A315-53:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 16
Server version: 8.0.35-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE example_database;
Query OK, 1 row affected (0.01 sec)

Step 2 — Installing MySQL
mysql> CREATE USER 'example_user'@'%' IDENTIFIED BY 'password';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql> CREATE USER 'example_user'@'%' IDENTIFIED BY 'Esp02016!';
Query OK, 0 rows affected (0.01 sec)

mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'Esp02016';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'Esp02016!';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL ON example_database.* TO 'example_user'@'%';
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
acer@acer-Aspire-A315-53:~$ mysql -u example_user -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 8.0.35-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

```

b@acer-Aspire-A315-53: ~
Copyright (c) 2000, 2023, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| example_database |
| information_schema |
| performance_schema |
+-----+
3 rows in set (0.01 sec)

mysql> CREATE TABLE example_database.todo_list (
    -> item_id INT AUTO_INCREMENT,
    -> content VARCHAR(255),
    -> PRIMARY KEY(item_id)
    -> );
Query OK, 0 rows affected (0.02 sec)

mysql> INSERT INTO example_database.todo_list (content) VALUES ("My first important item");
Query OK, 1 row affected (0.01 sec)

mysql> SELECT * FROM example_database.todo_list;
+-----+
| item_id | content |
+-----+
|       1 | My first important item |
+-----+
1 row in set (0.00 sec)

mysql> INSERT INTO example_database.todo_list (content) VALUES ("My second important item");
Query OK, 1 row affected (0.00 sec)

mysql> SELECT * FROM example_database.todo_list;
+-----+
| item_id | content |
+-----+
|       1 | My first important item |
|       2 | My second important item |
+-----+
2 rows in set (0.00 sec)

mysql>

```

Then I can created the PHP script that connected to MySQL and query for content.

**nano /var/www/my\_domain/todo\_list.php**

```

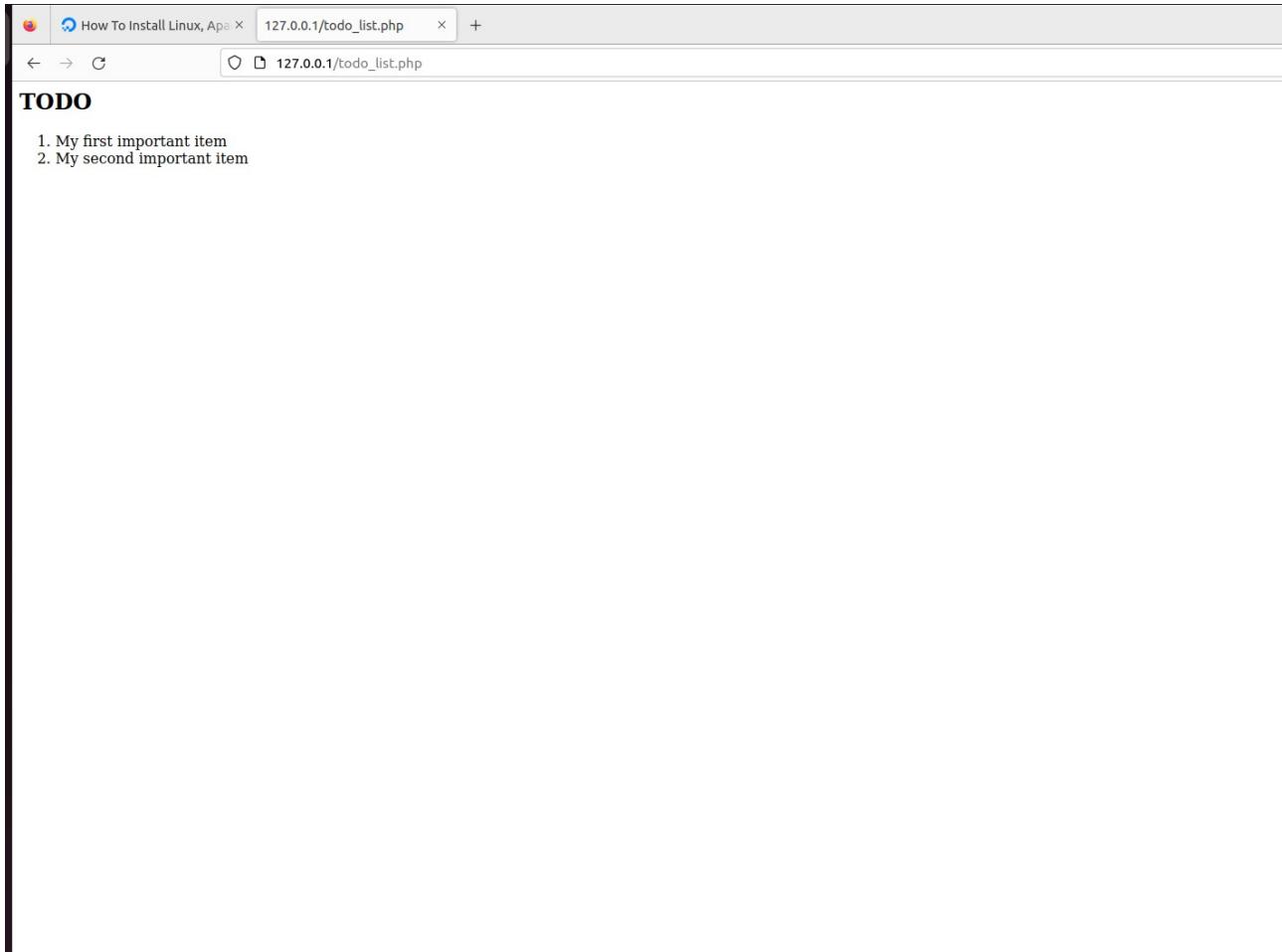
GNU nano 6.2          /var/www/my_domain/todo_list.php
<?php
$user = "example_user";
$password = "Espo2016!";
$database = "example_database";
$table = "todo_list";

try {
    $db = new PDO("mysql:host=localhost;dbname=$database", $user, $password);
    echo "<h2>TODO</h2><ol>";
    foreach($db->query("SELECT content FROM $table") as $row) {
        echo "<li>" . $row['content'] . "</li>";
    }
    echo "</ol>";
} catch (PDOException $e) {
    print "Error!: " . $e->getMessage() . "<br/>";
    die();
}

^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste      ^J Justify  ^/ Go To Line

```

I accessed this page in my web browser by visiting public IP address configured for my website, followed by /todo\_list.php:



This test confirmed that :

- PHP scripts can be executed by the server without errors,
- the website hosted on the LAMP server should be accessible, the website is reachable through its domain or IP address, and web pages load correctly without errors.

## Monitoring With Fail2Ban

One of the greatest advantages of using Fail2Ban the ability to monitor all the failed authentication attempts and the various blocked IP addresses.

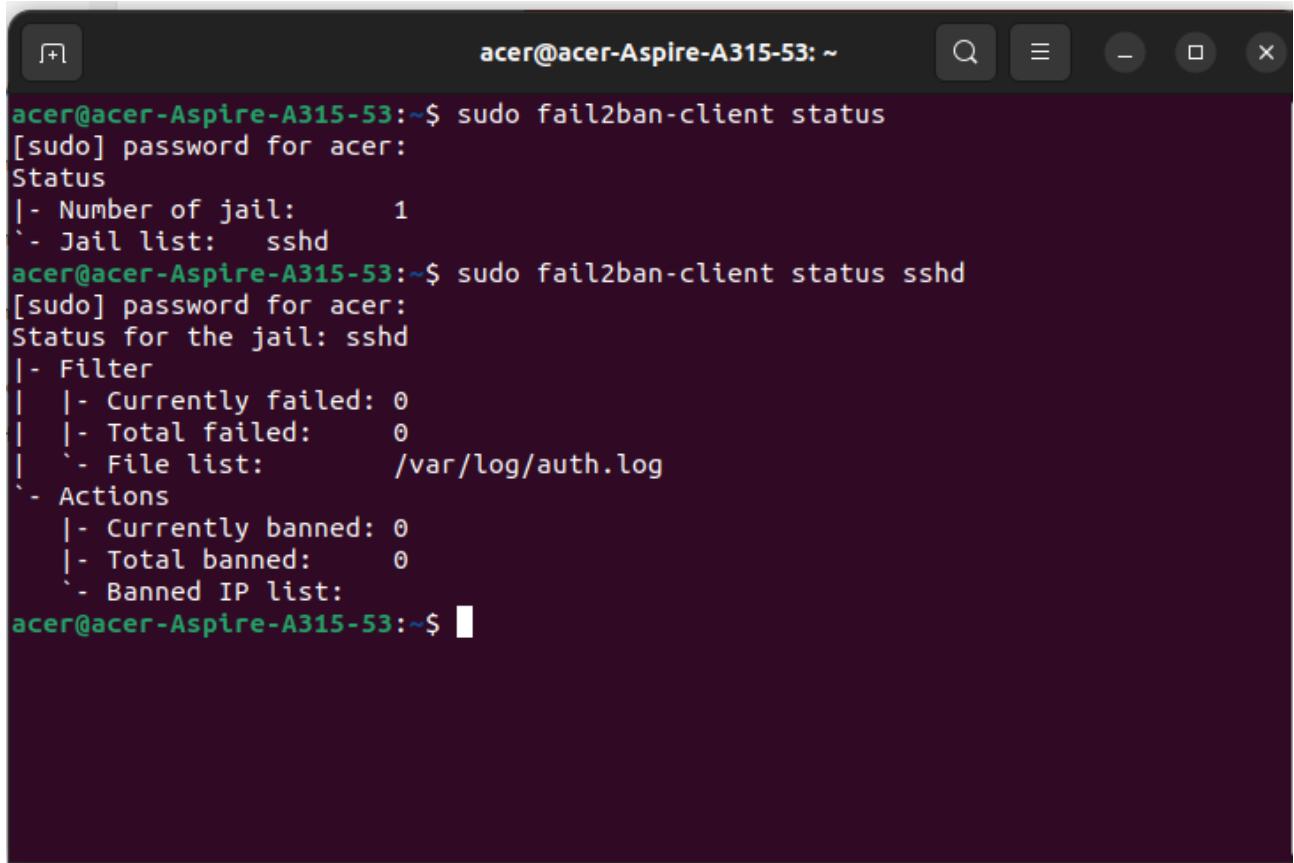
I used the Fail2Ban-client tool to check the status of Fail2Ban and the active jails:

**sudo fail2ban-client status**

In my case, the sshd jail is active.

To view the status and information regarding a particular jail like sshd, I used the following command:

**sudo fail2ban-client status sshd**



```
acer@acer-Aspire-A315-53:~$ sudo fail2ban-client status
[sudo] password for acer:
Status
|- Number of jail:      1
`- Jail list:    sshd
acer@acer-Aspire-A315-53:~$ sudo fail2ban-client status sshd
[sudo] password for acer:
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:      0
| `- File list:          /var/log/auth.log
`- Actions
  |- Currently banned: 0
  |- Total banned:      0
  `- Banned IP list:
acer@acer-Aspire-A315-53:~$
```

This test shows 0 of failed and banned IP addresses.

### Scanning with ClamAV

To scan the /etc directory for infected files, I run the following command:

**sudo clamscan -i -r --remove /etc**

After the scan is completed, a summary of all infected files found is displayed.

```
acer@acer-Aspire-A315-53:~$ sudo clamscan -i -r --remove /
[sudo] password for acer:

LibClamAV Warning: cli_scanxz: decompress file size exceeds limits - only scanning 27262976 bytes

^C
acer@acer-Aspire-A315-53:~$ sudo clamscan -i -r --remove /etc
[sudo] password for acer:

----- SCAN SUMMARY -----
Known viruses: 8683239
Engine version: 0.103.11
Scanned directories: 401
Scanned files: 1973
Infected files: 0
Data scanned: 21.60 MB
Data read: 11.21 MB (ratio 1.93:1)
Time: 46.868 sec (0 m 46 s)
Start Date: 2024:01:24 23:31:53
End Date: 2024:01:24 23:32:40
acer@acer-Aspire-A315-53:~$
```

This test shows 0 infected files found.

## Security Auditing with Lynis

Lynis outputs a lot of information that it stores under the `/var/log/lynis.log` file for easier access. The summary of the system audit reveals important information about system's security posture and various security misconfigurations and vulnerabilities.

### **sudo lynis audit system**

[ Lynis 3.0.9 ]

```
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
```

```
2007-2021, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####
```

[+] Initializing program

```
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
```

```
-----
Program version: 3.0.9
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 22.04
```

Kernel version: 6.5.0  
Hardware platform: x86\_64  
Hostname: acer-Aspire-A315-53  
-----  
Profiles: /etc/lynis/default.prf  
Log file: /var/log/lynis.log  
Report file: /var/log/lynis-report.dat  
Report version: 1.0  
Plugin directory: /usr/share/lynis/plugins  
-----

Auditor: [Not Specified]  
Language: en  
Test category: all  
Test group: all  
-----

- Program update status... [ NO UPDATE ]

[+] System tools

- Scanning available tools...  
- Checking system binaries...

[+] Plugins (phase 1)

Note: plugins have more extensive tests and may take several minutes to complete

- Plugins enabled [ NONE ]

[+] Boot and services

- Service Manager [ systemd ]  
- Checking UEFI boot [ ENABLED ]  
- Checking Secure Boot [ ENABLED ]  
- Checking presence GRUB2 [ FOUND ]  
- Checking for password protection [ NONE ]  
- Check running services (systemctl) [ DONE ]  
Result: found 40 running services  
- Check enabled services at boot (systemctl) [ DONE ]  
Result: found 53 enabled services  
- Check startup files (permissions) [ OK ]  
- Running 'systemd-analyze security'  
- ModemManager.service: [ MEDIUM ]  
- NetworkManager.service: [ EXPOSED ]  
- accounts-daemon.service: [ MEDIUM ]  
- acpid.service: [ UNSAFE ]  
- alsa-state.service: [ UNSAFE ]  
- anacron.service: [ UNSAFE ]  
- apache2.service: [ UNSAFE ]  
- apport.service: [ UNSAFE ]  
- avahi-daemon.service: [ UNSAFE ]  
- bluetooth.service: [ MEDIUM ]  
- clamav-freshclam.service: [ UNSAFE ]  
- colord.service: [ EXPOSED ]  
- cron.service: [ UNSAFE ]  
- cups-browsed.service: [ UNSAFE ]  
- cups.service: [ UNSAFE ]  
- dbus.service: [ UNSAFE ]  
- dmesg.service: [ UNSAFE ]  
- emergency.service: [ UNSAFE ]  
- fail2ban.service: [ UNSAFE ]  
- fwupd.service: [ EXPOSED ]  
- gdm.service: [ UNSAFE ]  
- getty@tty1.service: [ UNSAFE ]  
- irqbalance.service: [ MEDIUM ]  
- kerneloops.service: [ UNSAFE ]  
- mysql.service: [ UNSAFE ]  
- networkd-dispatcher.service: [ UNSAFE ]  
- packagekit.service: [ UNSAFE ]  
- plymouth-start.service: [ UNSAFE ]

|  |               |
|--|---------------|
| - polkit.service:                        | [ UNSAFE ]    |
| - postfix@-.service:                     | [ UNSAFE ]    |
| - power-profiles-daemon.service:         | [ EXPOSED ]   |
| - rc-local.service:                      | [ UNSAFE ]    |
| - rescue.service:                        | [ UNSAFE ]    |
| - rsyslog.service:                       | [ UNSAFE ]    |
| - rtkit-daemon.service:                  | [ MEDIUM ]    |
| - snapd_aa-prompt-listener.service:      | [ UNSAFE ]    |
| - snapd.service:                         | [ UNSAFE ]    |
| - switcheroo-control.service:            | [ EXPOSED ]   |
| - systemd-ask-password-console.service:  | [ UNSAFE ]    |
| - systemd-ask-password-plymouth.service: | [ UNSAFE ]    |
| - systemd-ask-password-wall.service:     | [ UNSAFE ]    |
| - systemd-fsckd.service:                 | [ UNSAFE ]    |
| - systemd-initctl.service:               | [ UNSAFE ]    |
| - systemd-journald.service:              | [ PROTECTED ] |
| - systemd-logind.service:                | [ PROTECTED ] |
| - systemd-networkd.service:              | [ PROTECTED ] |
| - systemd-oomd.service:                  | [ PROTECTED ] |
| - systemd-resolved.service:              | [ PROTECTED ] |
| - systemd-rfkill.service:                | [ UNSAFE ]    |
| - systemd-timesyncd.service:             | [ PROTECTED ] |
| - systemd-udevd.service:                 | [ MEDIUM ]    |
| - thermald.service:                      | [ UNSAFE ]    |
| - ubuntu-advantage.service:              | [ UNSAFE ]    |
| - udisks2.service:                       | [ UNSAFE ]    |
| - unattended-upgrades.service:           | [ UNSAFE ]    |
| - upower.service:                        | [ PROTECTED ] |
| - user@1000.service:                     | [ UNSAFE ]    |
| - uidd.service:                          | [ PROTECTED ] |
| - whoopsie.service:                      | [ UNSAFE ]    |
| - wpa_supplicant.service:                | [ UNSAFE ]    |

#### [+] Kernel

|   |                |
|---|----------------|
| - Checking default run level                        | [ RUNLEVEL 5 ] |
| - Checking CPU support (NX/PAE)                     |                |
| CPU support: PAE and/or NoeXecute supported         | [ FOUND ]      |
| - Checking kernel version and release               | [ DONE ]       |
| - Checking kernel type                              | [ DONE ]       |
| - Checking loaded kernel modules                    | [ DONE ]       |
| Found 173 active modules                            |                |
| - Checking Linux kernel configuration file          | [ FOUND ]      |
| - Checking default I/O kernel scheduler             | [ NOT FOUND ]  |
| - Checking for available kernel update              | [ OK ]         |
| - Checking core dumps configuration                 |                |
| - configuration in systemd conf files               | [ DEFAULT ]    |
| - configuration in /etc/profile                     | [ DEFAULT ]    |
| - 'hard' configuration in /etc/security/limits.conf | [ DEFAULT ]    |
| - 'soft' configuration in /etc/security/limits.conf | [ DEFAULT ]    |
| - Checking setuid core dumps configuration          | [ PROTECTED ]  |
| - Check if reboot is needed                         | [ NO ]         |

#### [+] Memory and Processes

|                                       |               |
|---------------------------------------|---------------|
| - Checking /proc/meminfo              | [ FOUND ]     |
| - Searching for dead/zombie processes | [ NOT FOUND ] |
| - Searching for IO waiting processes  | [ NOT FOUND ] |
| - Search prelink tooling              | [ NOT FOUND ] |

#### [+] Users, Groups and Authentication

|                                      |        |
|--------------------------------------|--------|
| - Administrator accounts             | [ OK ] |
| - Unique UIDs                        | [ OK ] |
| - Consistency of group files (grpck) | [ OK ] |
| - Unique group IDs                   | [ OK ] |
| - Unique group names                 | [ OK ] |
| - Password file consistency          | [ OK ] |
| - Password hashing methods           | [ OK ] |

- Checking password hashing rounds [ DISABLED ]
- Query system users (non daemons) [ DONE ]
- NIS+ authentication support [ NOT ENABLED ]
- NIS authentication support [ NOT ENABLED ]
- Sudoers file(s) [ FOUND ]
  - Permissions for directory: /etc/sudoers.d [ WARNING ]
  - Permissions for: /etc/sudoers [ OK ]
  - Permissions for: /etc/sudoers.d/README [ OK ]
- PAM password strength tools [ OK ]
- PAM configuration files (pam.conf) [ FOUND ]
- PAM configuration files (pam.d) [ FOUND ]
- PAM modules [ FOUND ]
- LDAP module in PAM [ NOT FOUND ]
- Accounts without expire date [ SUGGESTION ]
- Accounts without password [ OK ]
- Locked accounts [ OK ]
- Checking user password aging (minimum) [ DISABLED ]
- User password aging (maximum) [ DISABLED ]
- Checking expired passwords [ OK ]
- Checking Linux single user mode authentication [ OK ]
- Determining default umask
  - umask (/etc/profile) [ NOT FOUND ]
  - umask (/etc/login.defs) [ SUGGESTION ]
- LDAP authentication support [ NOT ENABLED ]
- Logging failed login attempts [ ENABLED ]

#### [+] Shells

- Checking shells from /etc/shells

Result: found 8 shells (valid shells: 8).

- Session timeout settings/tools [ NONE ]
- Checking default umask values
  - Checking default umask in /etc/bash.bashrc [ NONE ]
  - Checking default umask in /etc/profile [ NONE ]

#### [+] File systems

- Checking mount points
  - Checking /home mount point [ SUGGESTION ]
  - Checking /tmp mount point [ SUGGESTION ]
  - Checking /var mount point [ SUGGESTION ]
- Query swap partitions (fstab) [ OK ]
- Testing swap partitions [ OK ]
- Testing /proc mount (hidepid) [ SUGGESTION ]
- Checking for old files in /tmp [ OK ]
- Checking /tmp sticky bit [ OK ]
- Checking /var/tmp sticky bit [ OK ]
- ACL support root file system [ ENABLED ]
- Mount options of / [ NON DEFAULT ]
- Mount options of /dev [ PARTIALLY HARDEDNED ]
- Mount options of /dev/shm [ PARTIALLY HARDEDNED ]
- Mount options of /run [ HARDEDNED ]
- Total without nodev:9 noexec:26 nosuid:22 ro or noexec (W^X): 11 of total 45
- Disable kernel support of some filesystems

#### [+] USB Devices

- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]
- Checking USB devices authorization [ ENABLED ]
- Checking USBGuard [ NOT FOUND ]

#### [+] Storage

- Checking firewire ohci driver (modprobe config) [ DISABLED ]

#### [+] NFS

- Check running NFS daemon [ NOT FOUND ]

## [+] Name services

- 
- Checking search domains [ FOUND ]
  - Checking /etc/resolv.conf options [ FOUND ]
  - Searching DNS domain name [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file [ NONE ]
    - Presence of configured hostname in /etc/hosts [ FOUND ]
    - Hostname mapped to localhost [ NOT FOUND ]
    - Localhost mapping to IP address [ OK ]

## [+] Ports and packages

- 
- Searching package managers
    - Searching dpkg package manager [ FOUND ]
    - Querying package manager
    - Query unpurged packages [ NONE ]
  - Checking security repository in sources.list file [ OK ]
  - Checking APT package database [ OK ]
- W: <https://packages.cisofy.com/community/lynis/deb/dists/stable/InRelease>: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
- Checking vulnerable packages [ OK ]

[WARNING]: Test PKGS-7392 had a long execution: 10.291355 seconds

- Checking upgradeable packages [ SKIPPED ]
- Checking package audit tool [ INSTALLED ]  
Found: apt-check
- Toolkit for automatic upgrades (unattended-upgrade) [ FOUND ]

## [+] Networking

- 
- Checking IPv6 configuration [ ENABLED ]
    - Configuration method [ AUTO ]
    - IPv6 only [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      - Nameserver: 127.0.0.53 [ OK ]
      - DNSSEC supported (systemd-resolved) [ NO ]
    - Getting listening ports (TCP/UDP) [ DONE ]
    - Checking promiscuous interfaces [ OK ]
    - Checking status DHCP client
    - Checking for ARP monitoring software [ NOT FOUND ]
    - Uncommon network protocols [ 0 ]

## [+] Printers and Spools

- 
- Checking cups daemon [ RUNNING ]
  - Checking CUPS configuration file [ OK ]
  - File permissions [ WARNING ]
  - Checking CUPS addresses/sockets [ FOUND ]
  - Checking lp daemon [ NOT RUNNING ]

## [+] Software: e-mail and messaging

- 
- Postfix status [ RUNNING ]
  - Postfix configuration [ FOUND ]
  - Postfix banner [ WARNING ]

## [+] Software: firewalls

- 
- Checking iptables kernel module [ FOUND ]
  - Checking iptables policies of chains [ FOUND ]
  - Checking for empty ruleset [ OK ]
  - Checking for unused rules [ FOUND ]
  - Checking host based firewall [ ACTIVE ]

## [+] Software: webserver

-

```
- Checking Apache (binary /usr/sbin/apache2) [ FOUND ]
  Info: Configuration file found (/etc/apache2/apache2.conf)
  Info: Found 4 virtual hosts
* Loadable modules [ FOUND (120) ]
- Found 120 loadable modules
  mod_evasive: anti-DoS/brute force [ FOUND ]
  mod_reqtimeout/mod_qos [ FOUND ]
  ModSecurity: web application firewall [ FOUND ]
- Checking nginx [ NOT FOUND ]
```

```
[+] SSH Support
-----
- Checking running SSH daemon [ NOT FOUND ]
```

```
[+] SNMP Support
-----
- Checking running SNMP daemon [ NOT FOUND ]
```

```
[+] Databases
-----
- MySQL process status [ FOUND ]
```

```
[+] LDAP Services
-----
- Checking OpenLDAP instance [ NOT FOUND ]
```

```
[+] PHP
-----
- Checking PHP [ NOT FOUND ]
```

```
[+] Squid Support
-----
- Checking running Squid daemon [ NOT FOUND ]
```

```
[+] Logging and files
-----
- Checking for a running log daemon [ OK ]
- Checking Syslog-NG status [ NOT FOUND ]
- Checking systemd journal status [ FOUND ]
- Checking Metalog status [ NOT FOUND ]
- Checking RSyslog status [ FOUND ]
- Checking RFC 3195 daemon status [ NOT FOUND ]
- Checking minilogd instances [ NOT FOUND ]
- Checking logrotate presence [ OK ]
- Checking remote logging [ NOT ENABLED ]
- Checking log directories (static list) [ DONE ]
- Checking open log files [ DONE ]
- Checking deleted files in use [ FILES FOUND ]
```

```
[+] Insecure services
-----
- Installed inetd package [ NOT FOUND ]
- Installed xinetd package [ OK ]
- xinetd status
- Installed rsh client package [ OK ]
- Installed rsh server package [ OK ]
- Installed telnet client package [ OK ]
- Installed telnet server package [ NOT FOUND ]
- Checking NIS client installation [ OK ]
- Checking NIS server installation [ OK ]
- Checking TFTP client installation [ OK ]
- Checking TFTP server installation [ OK ]
```

```
[+] Banners and identification
-----
- /etc/issue [ FOUND ]
- /etc/issue contents [ WEAK ]
- /etc/issue.net [ FOUND ]
- /etc/issue.net contents [ WEAK ]
```

## [+] Scheduled tasks

- Checking crontab and cronjob files [ DONE ]

## [+] Accounting

- Checking accounting information [ NOT FOUND ]  
- Checking sysstat accounting data [ NOT FOUND ]  
- Checking auditd [ NOT FOUND ]

## [+] Time and Synchronization

- NTP daemon found: systemd (timesyncd) [ FOUND ]  
- Checking for a running NTP daemon or client [ OK ]  
- Last time synchronization [ 58s ]

## [+] Cryptography

- Checking for expired SSL certificates [0/142] [ NONE ]

[WARNING]: Test CRYP-7902 had a long execution: 26.469912 seconds

- Kernel entropy is sufficient [ YES ]  
- HW RNG & rngd [ NO ]  
- SW prng [ NO ]  
MOR-bit set [ YES ]

## [+] Virtualization

## [+] Containers

## [+] Security frameworks

- Checking presence AppArmor [ FOUND ]  
- Checking AppArmor status [ ENABLED ]  
  Found 199 unconfined processes  
- Checking presence SELinux [ NOT FOUND ]  
- Checking presence TOMOYO Linux [ NOT FOUND ]  
- Checking presence grsecurity [ NOT FOUND ]  
- Checking for implemented MAC framework [ OK ]

## [+] Software: file integrity

- Checking file integrity tools  
- Checking presence integrity tool [ NOT FOUND ]

## [+] Software: System tooling

- Checking automation tooling  
- Automation tooling [ NOT FOUND ]  
- Checking presence of Fail2ban [ FOUND ]  
  - Checking Fail2ban jails [ ENABLED ]  
- Checking for IDS/IPS tooling [ FOUND ]

## [+] Software: Malware

- Checking ClamAV scanner [ FOUND ]  
- Malware software components [ FOUND ]  
  - Active agent [ NOT FOUND ]  
  - Rootkit scanner [ NOT FOUND ]

## [+] File Permissions

- Starting file permissions check  
File: /boot/grub/grub.cfg [ SUGGESTION ]  
File: /etc/crontab [ SUGGESTION ]

|                              |                |
|------------------------------|----------------|
| File: /etc/group             | [ OK ]         |
| File: /etc/group-            | [ OK ]         |
| File: /etc/hosts.allow       | [ OK ]         |
| File: /etc/hosts.deny        | [ OK ]         |
| File: /etc/issue             | [ OK ]         |
| File: /etc/issue.net         | [ OK ]         |
| File: /etc/passwd            | [ OK ]         |
| File: /etc/passwd-           | [ OK ]         |
| Directory: /etc/cron.d       | [ SUGGESTION ] |
| Directory: /etc/cron.daily   | [ SUGGESTION ] |
| Directory: /etc/cron.hourly  | [ SUGGESTION ] |
| Directory: /etc/cron.weekly  | [ SUGGESTION ] |
| Directory: /etc/cron.monthly | [ SUGGESTION ] |

#### [+] Home directories

---

|                                   |        |
|-----------------------------------|--------|
| - Permissions of home directories | [ OK ] |
| - Ownership of home directories   | [ OK ] |
| - Checking shell history files    | [ OK ] |

#### [+] Kernel Hardening

---

|   |               |
|---|---------------|
| - Comparing sysctl key pairs with scan profile        |               |
| - dev.tty.ldisc_autoload (exp: 0)                     | [ DIFFERENT ] |
| - fs.protected_fifos (exp: 2)                         | [ DIFFERENT ] |
| - fs.protected_hardlinks (exp: 1)                     | [ OK ]        |
| - fs.protected_regular (exp: 2)                       | [ OK ]        |
| - fs.protected_symlinks (exp: 1)                      | [ OK ]        |
| - fs.suid_dumpable (exp: 0)                           | [ DIFFERENT ] |
| - kernel.core_uses_pid (exp: 1)                       | [ OK ]        |
| - kernel.ctrl-alt-del (exp: 0)                        | [ OK ]        |
| - kernel.dmesg_restrict (exp: 1)                      | [ OK ]        |
| - kernel.kptr_restrict (exp: 2)                       | [ DIFFERENT ] |
| - kernel.modules_disabled (exp: 1)                    | [ DIFFERENT ] |
| - kernel.perf_event_paranoid (exp: 3)                 | [ DIFFERENT ] |
| - kernel.randomize_va_space (exp: 2)                  | [ OK ]        |
| - kernel.sysrq (exp: 0)                               | [ DIFFERENT ] |
| - kernel.unprivileged_bpf_disabled (exp: 1)           | [ DIFFERENT ] |
| - kernel.yama.ptrace_scope (exp: 1 2 3)               | [ OK ]        |
| - net.core.bpf_jit_harden (exp: 2)                    | [ DIFFERENT ] |
| - net.ipv4.conf.all.accept_redirects (exp: 0)         | [ OK ]        |
| - net.ipv4.conf.all.accept_source_route (exp: 0)      | [ OK ]        |
| - net.ipv4.conf.all.bootp_relay (exp: 0)              | [ OK ]        |
| - net.ipv4.conf.all.forwarding (exp: 0)               | [ OK ]        |
| - net.ipv4.conf.all.log_martians (exp: 1)             | [ DIFFERENT ] |
| - net.ipv4.conf.all.mc_forwarding (exp: 0)            | [ OK ]        |
| - net.ipv4.conf.all.proxy_arp (exp: 0)                | [ OK ]        |
| - net.ipv4.conf.all.rp_filter (exp: 1)                | [ DIFFERENT ] |
| - net.ipv4.conf.all.send_redirects (exp: 0)           | [ DIFFERENT ] |
| - net.ipv4.conf.default.accept_redirects (exp: 0)     | [ OK ]        |
| - net.ipv4.conf.default.accept_source_route (exp: 0)  | [ OK ]        |
| - net.ipv4.conf.default.log_martians (exp: 1)         | [ DIFFERENT ] |
| - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)       | [ OK ]        |
| - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) | [ OK ]        |
| - net.ipv4.tcp_syncookies (exp: 1)                    | [ OK ]        |
| - net.ipv4.tcp_timestamps (exp: 0 1)                  | [ OK ]        |
| - net.ipv6.conf.all.accept_redirects (exp: 0)         | [ OK ]        |
| - net.ipv6.conf.all.accept_source_route (exp: 0)      | [ OK ]        |
| - net.ipv6.conf.default.accept_redirects (exp: 0)     | [ OK ]        |
| - net.ipv6.conf.default.accept_source_route (exp: 0)  | [ OK ]        |

#### [+] Hardening

---

|                             |               |
|-----------------------------|---------------|
| - Installed compiler(s)     | [ NOT FOUND ] |
| - Installed malware scanner | [ FOUND ]     |
| - Non-native binary formats | [ FOUND ]     |

#### [+] Custom tests

---

- Running custom tests... [ NONE ]

[+] Plugins (phase 2)

Lynis also generates output on how these vulnerabilities and misconfigurations can be fixed or tweaked.

```
=====
Lynis security scan details:

Hardening index : 73 [#####
Tests performed : 255
Plugins enabled : 0

Components:
- Firewall      [V]
- Malware scanner [V]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status      [?]
- Security audit          [V]
- Vulnerability scan      [V]

Files:
- Test and debug information   : /var/log/lynis.log
- Report data                 : /var/log/lynis-report.dat
=====

Lynis 3.0.9

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2021, CISOfy - https://cisofty.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
```

The output also contains a hardening index score that is rated out of 100, this is used to give you a trackable tangible score of system's current security posture.

Also found in the report, Linus displays any potential warnings that indicate a severe security vulnerability or misconfiguration that needs to be fixed or patched.

Warnings (1):

! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]  
<https://cisofty.com/lynis/controls/MAIL-8818/>

To increase our hardening index score, Lynis provides us with helpful suggestions that detail the various security configurations to be made.

Suggestions (35):

\* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]  
<https://cisofty.com/lynis/controls/LYNIS/>

\* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]  
<https://cisofty.com/lynis/controls/BOOT-5122/>

\* Consider hardening system services [BOOT-5264]

- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service  
<https://cisofy.com/lynis/controls/BOOT-5264/>
- \* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNLL-5820]  
<https://cisofy.com/lynis/controls/KRNLL-5820/>
- \* Configure password hashing rounds in /etc/login.defs [AUTH-9230]  
<https://cisofy.com/lynis/controls/AUTH-9230/>
- \* When possible set expire dates for all password protected accounts [AUTH-9282]  
<https://cisofy.com/lynis/controls/AUTH-9282/>
- \* Configure minimum password age in /etc/login.defs [AUTH-9286]  
<https://cisofy.com/lynis/controls/AUTH-9286/>
- \* Configure maximum password age in /etc/login.defs [AUTH-9286]  
<https://cisofy.com/lynis/controls/AUTH-9286/>
- \* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]  
<https://cisofy.com/lynis/controls/AUTH-9328/>
- \* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]  
[https://cisofy.com/lynis/controls\(FILE-6310/](https://cisofy.com/lynis/controls(FILE-6310)
- \* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]  
[https://cisofy.com/lynis/controls\(FILE-6310/](https://cisofy.com/lynis/controls(FILE-6310)
- \* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]  
[https://cisofy.com/lynis/controls\(FILE-6310/](https://cisofy.com/lynis/controls(FILE-6310)
- \* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]  
<https://cisofy.com/lynis/controls/USB-1000/>
- \* Check DNS configuration for the dns domain name [NAME-4028]  
<https://cisofy.com/lynis/controls/NAME-4028/>
- \* Install debsums utility for the verification of packages with known good database. [PKGS-7370]  
<https://cisofy.com/lynis/controls/PKGS-7370/>
- \* Install package apt-show-versions for patch management purposes [PKGS-7394]  
<https://cisofy.com/lynis/controls/PKGS-7394/>
- \* Determine if protocol 'dccp' is really needed on this system [NETW-3200]  
<https://cisofy.com/lynis/controls/NETW-3200/>
- \* Determine if protocol 'sctp' is really needed on this system [NETW-3200]  
<https://cisofy.com/lynis/controls/NETW-3200/>
- \* Determine if protocol 'rds' is really needed on this system [NETW-3200]  
<https://cisofy.com/lynis/controls/NETW-3200/>
- \* Determine if protocol 'tipc' is really needed on this system [NETW-3200]  
<https://cisofy.com/lynis/controls/NETW-3200/>
- \* Access to CUPS configuration could be more strict. [PRNT-2307]  
<https://cisofy.com/lynis/controls/PRNT-2307/>
- \* You are advised to hide the mail\_name (option: smtpd\_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818]  
<https://cisofy.com/lynis/controls/MAIL-8818/>

\* Disable the 'VRFY' command [MAIL-8820:disable\_vrfy\_command]  
- Details : disable\_vrfy\_command=no  
- Solution : run postconf -e disable\_vrfy\_command=yes to change the value  
<https://cisofy.com/lynis/controls/MAIL-8820/>

\* Check iptables rules to see which rules are currently not used [FIRE-4513]  
<https://cisofy.com/lynis/controls/FIRE-4513/>

\* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]  
<https://cisofy.com/lynis/controls/LOGG-2154/>

\* Check what deleted files are still in use and why. [LOGG-2190]  
<https://cisofy.com/lynis/controls/LOGG-2190/>

\* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]  
<https://cisofy.com/lynis/controls/BANN-7126/>

\* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]  
<https://cisofy.com/lynis/controls/BANN-7130/>

\* Enable process accounting [ACCT-9622]  
<https://cisofy.com/lynis/controls/ACCT-9622/>

\* Enable sysstat to collect accounting (no results) [ACCT-9626]  
<https://cisofy.com/lynis/controls/ACCT-9626/>

\* Enable auditd to collect audit information [ACCT-9628]  
<https://cisofy.com/lynis/controls/ACCT-9628/>

\* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]  
<https://cisofy.com/lynis/controls/FINT-4350/>

\* Determine if automation tools are present for system management [TOOL-5002]  
<https://cisofy.com/lynis/controls/TOOL-5002/>

\* Consider restricting file permissions [FILE-7524]  
- Details : See screen output or log file  
- Solution : Use chmod to change file permissions  
[https://cisofy.com/lynis/controls\(FILE-7524/\)](https://cisofy.com/lynis/controls(FILE-7524)/)

\* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]  
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)  
<https://cisofy.com/lynis/controls/KRNL-6000/>

After following the suggestions and making the necessary changes, I will run the system audit with Lynis again.

Once all the changes will be made, I expect to see a significant improvement in the hardening index score that confirms the changes and configurations applied are effective.

Lynis simulated a privileged/internal pentest on the system, this was invoked :

**sudo lynis --pentest**

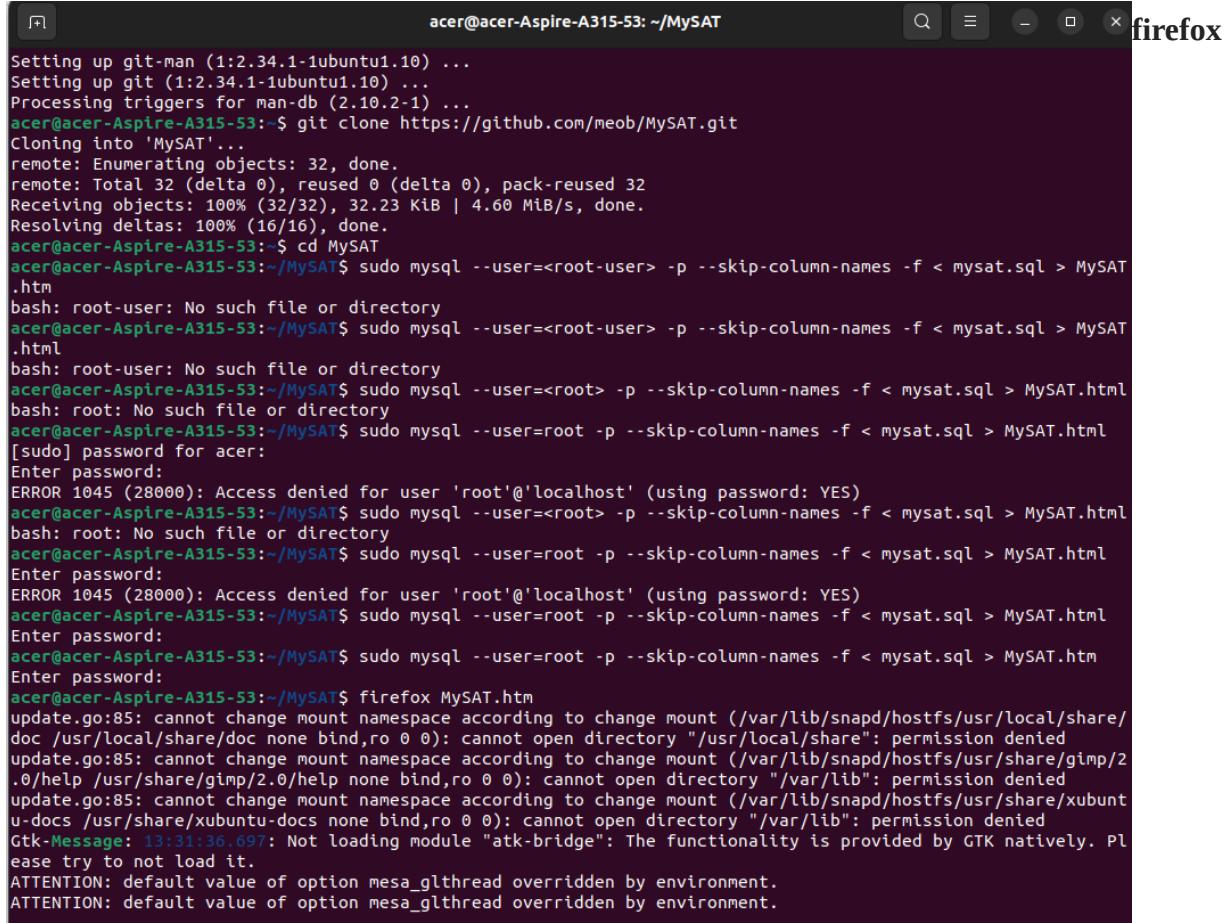
This performs a pentest on the system and outputs a hardening index score that reflects the overall security posture of the system. It also outputted similar recommendations and patches that can be implied to improve the score.

## Auditing MySQL Security

I run the mysat.sql file with root permission and output to the MySAT.htm file:

```
sudo mysql --user=root -p --skip-column-names -f < mysat.sql > MySAT.htm
```

I opened the MySAT.htm file by typing the following command to open it in Firefox:



The terminal window shows the following command and its output:

```
acer@acer-Aspire-A315-53: ~/MySAT
Setting up git-man (1:2.34.1-1ubuntu1.10) ...
Setting up git (1:2.34.1-1ubuntu1.10) ...
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53:~$ git clone https://github.com/meob/MySAT.git
Cloning into 'MySAT'...
remote: Enumerating objects: 32, done.
remote: Total 32 (delta 0), reused 0 (delta 0), pack-reused 32
Receiving objects: 100% (32/32), 32.23 KiB | 4.60 MiB/s, done.
Resolving deltas: 100% (16/16), done.
acer@acer-Aspire-A315-53:~$ cd MySAT
acer@acer-Aspire-A315-53:~/MySAT$ sudo mysql --user=<root-user> -p --skip-column-names -f < mysat.sql > MySAT.htm
bash: root-user: No such file or directory
acer@acer-Aspire-A315-53:~/MySAT$ sudo mysql --user=<root-user> -p --skip-column-names -f < mysat.sql > MySAT.htm
bash: root-user: No such file or directory
acer@acer-Aspire-A315-53:~/MySAT$ sudo mysql --user=<root> -p --skip-column-names -f < mysat.sql > MySAT.html
bash: root: No such file or directory
acer@acer-Aspire-A315-53:~/MySAT$ sudo mysql --user=root -p --skip-column-names -f < mysat.sql > MySAT.html
[sudo] password for acer:
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
acer@acer-Aspire-A315-53:~/MySAT$ sudo mysql --user=<root> -p --skip-column-names -f < mysat.sql > MySAT.html
bash: root: No such file or directory
acer@acer-Aspire-A315-53:~/MySAT$ sudo mysql --user=root -p --skip-column-names -f < mysat.sql > MySAT.html
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
acer@acer-Aspire-A315-53:~/MySAT$ sudo mysql --user=root -p --skip-column-names -f < mysat.sql > MySAT.html
Enter password:
acer@acer-Aspire-A315-53:~/MySAT$ sudo mysql --user=root -p --skip-column-names -f < mysat.sql > MySAT.htm
Enter password:
acer@acer-Aspire-A315-53:~/MySAT$ firefox MySAT.htm
update.go:85: cannot change mount namespace according to change mount (/var/lib/snapd/hostfs/usr/local/share/doc /usr/local/share/doc none bind,ro 0 0): cannot open directory "/usr/local/share": permission denied
update.go:85: cannot change mount namespace according to change mount (/var/lib/snapd/hostfs/usr/share/gimp/2.0/help /usr/share/gimp/2.0/help none bind,ro 0 0): cannot open directory "/var/lib": permission denied
update.go:85: cannot change mount namespace according to change mount (/var/lib/snapd/hostfs/usr/share/xubuntu-docs /usr/share/xubuntu-docs none bind,ro 0 0): cannot open directory "/var/lib": permission denied
Gtk-Message: 13:31:36.697: Not loading module "atk-bridge": The functionality is provided by GTK natively. Please try to not load it.
ATTENTION: default value of option mesa_glthread overridden by environment.
ATTENTION: default value of option mesa_glthread overridden by environment.
```

## MySAT.htm

The results are formatted in a simple to read and understand format. Configurations are checked and results are color coded based on their current configuration security impact. For example, a failed configuration check is color coded in orange and a passed check is color coded in green.

In the MySAT.htm file I review the detailed analysis results generated by MySAT, highlighting potential vulnerabilities and areas for improvement. Also MySAT provided recommendations for improving the security of the MySQL database.

| Database Hardening      |          |                                   |                            |
|-------------------------|----------|-----------------------------------|----------------------------|
| Anonymous user          | Pass     | Users can connect from everywhere | example_user               |
| Any host access         | Fail     |                                   |                            |
| Many host access        | Pass     |                                   |                            |
| DB Password check       | Pass     |                                   |                            |
| Backdoor users          | Pass     |                                   |                            |
| Test schema             | Pass     |                                   |                            |
| Admin users <>root      | Evaluate |                                   | debian-sys-maint@localhost |
| Oper users <>root       | Evaluate |                                   | mysql.infoschema@localhost |
| IDS                     | External | Configure IDS to monitor honeypot |                            |
| Spammable tables        | Pass     |                                   |                            |
| Dedicated datadir       | Fall     | Not dedicated datadir             |                            |
| Memcache plugin         | Pass     |                                   |                            |
| secure_file_priv        | Pass     |                                   |                            |
| Master Info             | Pass     |                                   |                            |
| Automatic User Creation | Fall     | Not disabled                      |                            |
| Password lenght         | Fall     | Too short                         | NULL                       |
| Password policy         | Fall     | Not secure                        |                            |
| Performance statistics  | Fall     | my2 collector not found           |                            |
| local_infile            | Pass     |                                   |                            |
| Symbolic Links          | Pass     |                                   |                            |
| Skip grant              | Evaluate | Do not enable skip_grant_tables   |                            |
| <b>Patching</b>         |          |                                   |                            |
| MySQL update            | Fall     | 8.0.35-Ubuntu0.22.04.1            |                            |
| MySAT update            | Fall     | 1.0.2                             |                            |
| <b>GDPR Countdown</b>   |          |                                   |                            |
| Days since promulgation | Pass     | 2829                              |                            |
| Days since application  | Pass     | 2071                              |                            |

## DB Configuration

| <b>Database Summary</b>  |                         |
|--------------------------|-------------------------|
| <b>Item</b>              | <b>Value</b>            |
| Version :                | 8.0.35-0ubuntu0.22.04.1 |
| Created :                | 2024-01-20 16:57:42     |
| Started :                | 2024-01-22 15:38:17     |
| Database Size (MB):      | 3                       |
| Buffers Size (MB):       | 179                     |
| Defined Users :          | 6                       |
| Defined Schemata :       | 4                       |
| Defined Tables :         | 329                     |
| Sessions :               | 2                       |
| Sessions (active) :      | 2                       |
| Questions (#/sec.) :     | 0.00251                 |
| Connections (#/sec.) :   | 0.00009                 |
| BinLog Writes Day (MB) : | 0                       |
| Hostname :               | acer-Aspire-A315-53     |
| Port :                   | 3306                    |

| Database Summary         |                        |
|--------------------------|------------------------|
| Item                     | Value                  |
| Version :                | 8.0.35-Ubuntu0.22.04.1 |
| Created :                | 2024-01-20 16:57:42    |
| Started :                | 2024-01-22 15:38:17    |
| Database Size (MB):      | 3                      |
| Buffers Size (MB):       | 179                    |
| Defined Users :          | 6                      |
| Defined Schemata :       | 4                      |
| Defined Tables :         | 329                    |
| Sessions :               | 2                      |
| Sessions (active) :      | 2                      |
| Questions (#/sec.) :     | 0.00251                |
| Connections (#/sec.) :   | 0.00009                |
| BinLog Writes Day (MB) : | 0                      |
| Hostname :               | acer-Aspire-A315-53    |
| Port :                   | 3306                   |

| Users            |           |    |     |        |     |     |    |        |
|------------------|-----------|----|-----|--------|-----|-----|----|--------|
| User             | Host      | SL | IUD | CDGRIA | CCS | CAE | RR | SPPFSR |
|                  |           | Y  | Y   | Y      | Y   | Y   | Y  | Y      |
| debian-sys-maint | localhost | N  | N   | N      | N   | N   | N  | N      |
| example_user     | %         | N  | N   | N      | N   | N   | N  | N      |
| mysql.infoschema | localhost | N  | N   | N      | N   | N   | N  | N      |
| mysql.session    | localhost | N  | N   | N      | N   | N   | N  | N      |
| mysql.sys        | localhost | N  | N   | N      | N   | N   | N  | N      |
| root             | localhost | Y  | Y   | Y      | Y   | Y   | Y  | Y      |

| Schema/Object Matrix |        |         |          |          |       |              |
|----------------------|--------|---------|----------|----------|-------|--------------|
| Database             | Tables | Indexes | Routines | Triggers | Views | Primary Keys |
| example_database     | 1      | 1       | 0        | 0        | 0     | 1            |
| information_schema   | 79     | 0       | 0        | 0        | 0     | 0            |
| mysql                | 37     | 38      | 0        | 0        | 0     | 35           |
| performance_schema   | 111    | 93      | 0        | 0        | 0     | 59           |
| sys                  | 101    | 1       | 48       | 2        | 100   | 1            |
| NULL                 | 329    | 133     | 48       | 2        | 100   | 96           |

| Space Usage        |           |           |            |            |        |           |
|--------------------|-----------|-----------|------------|------------|--------|-----------|
| Database           | Row#      | Data size | Index size | Total size | MyISAM | InnoDB    |
| example_database   | 2         | 16,384    | 0          | 16,384     | 0      | 16,384    |
| information_schema | 0         | 0         | 0          | 0          | 0      | 0         |
| mysql              | 4,329     | 2,408,448 | 344,064    | 2,752,512  | 0      | 2,752,512 |
| performance_schema | 2,959,379 | 0         | 0          | 0          | 0      | 0         |
| sys                | 6         | 16,384    | 0          | 16,384     | 0      | 16,384    |
| NULL               | 2,963,716 | 2,441,216 | 344,064    | 2,785,280  | 0      | 2,785,280 |

| Biggest Objects |                                  |      |        |           |           |  |
|-----------------|----------------------------------|------|--------|-----------|-----------|--|
| Database        | Object                           | Type | Engine | Bytes     | Est. rows |  |
| mysql           | help_topic                       | T    | InnoDB | 1,687,552 | 953       |  |
| mysql           | help_keyword                     | T    | InnoDB | 262,144   | 1,016     |  |
| mysql           | help_relation                    | T    | InnoDB | 98,304    | 2,186     |  |
| mysql           | global_grants                    | T    | InnoDB | 81,920    | 81        |  |
| mysql           | procs_priv                       | T    | InnoDB | 32,768    | 0         |  |
| mysql           | help_category                    | T    | InnoDB | 32,768    | 53        |  |
| mysql           | replication_group_member_actions | T    | InnoDB | 32,768    | 2         |  |
| mysql           | db                               | T    | InnoDB | 32,768    | 3         |  |
|                 | innodb_index_size                |      | InnoDB | 22,760    | n         |  |

|       |  |   |        |        |       |
|-------|--|---|--------|--------|-------|
| mysql | neip_relation                                | I | InnoDB | 98,304 | 4,180 |
| mysql | global_grants                                | T | InnoDB | 81,920 | 81    |
| mysql | procs_priv                                   | T | InnoDB | 32,768 | 0     |
| mysql | help_category                                | T | InnoDB | 32,768 | 53    |
| mysql | replication_group_member_actions             | T | InnoDB | 32,768 | 2     |
| mysql | db   | T | InnoDB | 32,768 | 3     |
| mysql | replication_asynchronous_connection_failover | T | InnoDB | 32,768 | 0     |
| mysql | proxies_priv                                 | T | InnoDB | 32,768 | 1     |

| Processes |                 |           |                    |         |           |
|-----------|-----------------|-----------|--------------------|---------|-----------|
| ID        | User            | Host      | DB                 | Command | Time      |
| 5         | event_scheduler | localhost | NULL               | Daemon  | 251571    |
| 22        | root            | localhost | information_schema | Query   | 0         |
|           |                 |           |                    |         | executing |

| Tuning Parameters (most used ones) |             |                    |
|------------------------------------|-------------|--------------------|
| Parameter                          | Value       | Type               |
| binlog_cache_size                  | 32,768      | Client Cache       |
| binlog_stmt_cache_size             | 32,768      | Client Cache       |
| innodb_buffer_pool_size            | 134,217,728 | Cache              |
| innodb_flush_log_at_timeout        | 1           | Tuning and timeout |
| innodb_flush_log_at_trx_commit     | 1           | Tuning and timeout |
| innodb_lock_wait_timeout           | 50          | Tuning and timeout |
| innodb_log_buffer_size             | 16,777,216  | Cache              |
| innodb_log_file_size               | 50,331,648  | Cache              |
| innodb_log_files_in_group          | 2           | Tuning and timeout |
| innodb_thread_concurrency          | 0           | Tuning and timeout |
| join_buffer_size                   | 262,144     | Client Cache       |
| key_buffer_size                    | 16,777,216  | Cache              |
| log_bin                            | ON          | Flag               |
| long_query_time                    | 10          | Tuning and timeout |
| max_connections                    | 151         | Client Cache       |
| max_heap_table_size                | 16,777,216  | Cache              |
| read_buffer_size                   | 131,072     | Client Cache       |
| read_rnd_buffer_size               | 262,144     | Client Cache       |
| slow_query_log                     | OFF         | Flag               |
| sort_buffer_size                   | 262,144     | Client Cache       |
| sync_binlog                        | 1           | Tuning and timeout |
| table_open_cache                   | 4,000       | Cache              |
| thread_stack                       | 1,048,576   | Client Cache       |
| tmp_table_size                     | 16,777,216  | Cache              |
| wait_timeout                       | 28,800      | Tuning and timeout |

| Performance Statistics Summary       |           |                  |                                 |
|--------------------------------------|-----------|------------------|---------------------------------|
| Statistic                            | Value     | Suggested value  | Potential Action                |
| Uptime (days)                        | 2.9       |                  |                                 |
| Buffer Cache: MyISAM Read Hit Ratio  | NULL >95  |                  | Increase KEY_BUFFER_SIZE        |
| Buffer Cache: InnoDB Read Hit Ratio  | 98.82 >95 |                  | Increase INNODB_BUFFER_SIZE     |
| Buffer Cache: MyISAM Write Hit Ratio | NULL >95  |                  | Increase KEY_BUFFER_SIZE        |
| Log Cache: InnoDB Log Write Ratio    | 89.18 >95 |                  | Increase INNODB_LOG_BUFFER_SIZE |
| Threads_connected                    | 1 /151    | Far from maximum | Increase MAX_CONNECTIONS        |
| Threads_running                      | 2 LOW     |                  | Check user load                 |
| Slow_queries                         | 0 LOW     |                  | Check application               |
| DBcpu (SUM_TIMER_WAIT)               | 0.00001   |                  |                                 |
| Connections #/sec.                   | 0.00009   |                  |                                 |
| Questions #/sec.                     | 0.00266   |                  |                                 |
| SELECT #/sec.                        | 0.00259   |                  |                                 |

| Performance Statistics Summary       |           |                  |                                 |
|--------------------------------------|-----------|------------------|---------------------------------|
| Statistic                            | Value     | Suggested value  | Potential Action                |
| Uptime (days)                        | 2.9       |                  |                                 |
| Buffer Cache: MyISAM Read Hit Ratio  | NULL >95  |                  | Increase KEY_BUFFER_SIZE        |
| Buffer Cache: InnoDB Read Hit Ratio  | 98.82 >95 |                  | Increase INNODB_BUFFER_SIZE     |
| Buffer Cache: MyISAM Write Hit Ratio | NULL >95  |                  | Increase KEY_BUFFER_SIZE        |
| Log Cache: InnoDB Log Write Ratio    | 89.18 >95 |                  | Increase INNODB_LOG_BUFFER_SIZE |
| Threads_connected                    | 1 /151    | Far from maximum | Increase MAX_CONNECTIONS        |
| Threads_running                      | 2 LOW     |                  | Check user load                 |
| Slow_queries                         | 0 LOW     |                  | Check application               |
| DBcpu (SUM_TIMER_WAIT)               | 0.00001   |                  |                                 |
| Connections #/sec.                   | 0.00009   |                  |                                 |
| Questions #/sec.                     | 0.00266   |                  |                                 |
| SELECT #/sec.                        | 0.00259   |                  |                                 |
| COMMIT #/sec. (TPS)                  | 0.00000   |                  |                                 |
| COM DML #/sec.                       | 0.00259   |                  |                                 |
| Bytes_sent Mb/sec.                   | 0.00001   |                  |                                 |
| Bytes_received Mb/sec.               | 0.00000   |                  |                                 |

| SQL Statements     | Text   | Representativeness: 100.00 % |
|--------------------|--|------------------------------|
| information_schema | SELECT IF ( COUNT( * ) = ? , ... ) FROM `performance_schema` . `events_statements_summary_by_digest` WHERE `DIGEST_TEXT` LIKE ? OR ...           | Count Sum Timer              |
| information_schema | SELECT ?, ... , `version` ( ? ) UNION SELECT ?, ..., MIN ( `create_time` ) FROM TABLES UNION SELECT ?,..., `date_format` ( `DATE_SUB` ...        | 262866817800                 |
| information_schema | SELECT ?, `sk` , ?, SUM ( IF ( `otype` = ? , ... ) , ? , SUM ( IF ( `otype` = ? , ... ) , ? , SUM ( IF ( `otype` = ? , ... ) , ? , ... ) ) , ... | 238867381900                 |
| information_schema | SELECT IF ( COUNT( * ) > ? , ... ) FROM `INFORMATION_SCHEMA` . `TABLES` WHERE `CREATE_OPTIONS` LIKE ? ...  | 212445580300                 |
| information_schema | SELECT IF ( `variable_value` != ? , ... ) FROM `performance_schema` . `global_variables` WHERE `variable_name` = ? ...                           | 2 6153273100                 |
|                    |  | 4 4197674400                 |

| Host Cache | Host | IP | Validated | SUM Errors | First Seen | Last Seen | Last Error Seen | # Handshake Err. | # Authentication Err. | # ACL Err. |
|------------|------|----|-----------|------------|------------|-----------|-----------------|------------------|-----------------------|------------|
|------------|------|----|-----------|------------|------------|-----------|-----------------|------------------|-----------------------|------------|

| MySQL Parameters            |                  |
|-----------------------------|------------------|
| Parameter                   | Value            |
| activate_all_roles_on_login | OFF              |
| admin_address               |                  |
| admin_port                  | 33062            |
| admin_ssl_ca                |                  |
| admin_ssl_capath            |                  |
| admin_ssl_cert              |                  |
| admin_ssl_cipher            |                  |
| admin_ssl_crl               |                  |
| admin_ssl_crlpath           |                  |
| admin_ssl_key               |                  |
| admin_tls_ciphersuites      |                  |
| admin_tls_version           | TLSv1.2, TLSv1.3 |
| authentication_policy       | PERMISSIVE       |
| auto_generate_certs         | ON               |
| auto_increment_increment    | 1                |
| auto_increment_offset       | 1                |
| autocommit                  | ON               |
| automatic_sp_privileges     | ON               |
| avoid_temporal_upgrade      | OFF              |
| back_log                    | 151              |
| basedir                     | /usr/            |
| big_tables                  | OFF              |
| bind_address                | 127.0.0.1        |
| binlog_error_recovery       | 19768            |

# I checked my server with Chkrootkit

I run sudo chkrootkit

```
Activities Terminal 3 Feb 17:20
acer@acer-Aspire-A315-53: ~
acer@acer-Aspire-A315-53: $ sudo chkrootkit
ROOTDIR is '/'
Checking `and'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `crontab'... not found
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not found
Checking `inetdconf'... not tested
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldroppreload'... not infected
Checking `login'... not found
Checking `lsof'... not infected
Checking `mail'... not infected
Checking `minetty'... not found
Checking `netstat'... not found
not found
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not found
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not found
Checking `rlogind'... not found
Checking `rshd'... not found
Checking `slogin'... not infected
Checking `sendmail'... not infected
Checking `sshd'... not infected
Checking `syslogd'... not tested
Checking `tcpdump'... not infected
Checking `tcpd'... not found
Checking `tcpdump'... not infected
Checking `top'... not infected
Checking `telnetd'... not found
Checking `timed'... not found
Checking `tzselect'... not found
```

```
Activities Terminal 3 Feb 17:20
acer@acer-Aspire-A315-53: ~
acer@acer-Aspire-A315-53: ~
Checking `timed'... not found
Checking `traceroute'... not found
Checking `vdri'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `altens'... no suspect files
Searching for suspicious logs, it may take a while...
Searching for rootkit Hidra's default files... nothing found
Searching for rootkit torn's default files... nothing found
Searching for torn's v8 defaults nothing found
Searching for rootkit Lion's default files... nothing found
Searching for rootkit RSWA's default files... nothing found
Searching for rootkit RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while... The following suspicious files and directories were found:
/usr/lib/modules/6.5.0-15-generic/vdso/.build_id
/usr/lib/modules/6.5.0-15-generic/.build_id
/usr/lib/python3/dist-packages/fail2ban/test/files/config/apache-auth/noentry/.htaccess
/usr/lib/python3/dist-packages/fail2ban/test/files/config/apache-auth/digest_anon/.htpasswd
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_anon/.htaccess
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_wrongrealm/.htpasswd
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_wrongrealm/.htaccess
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_time/.htpasswd
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_time/.htaccess
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest/.htpasswd
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest/.htaccess
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/basic/auth_owner/.htpasswd
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/basic/auth_owner/.htaccess
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/basic/file/.htpasswd
/usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/basic/file/.htaccess
/usr/lib/libreoffice/share/.registry
/usr/lib/debug/.build_id
Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RKit files and dirs... nothing found
Searching for Monero rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for Shitc Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKlt... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for QBot.vi... nothing found
Searching for Loc rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for HKRK rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Goldz rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoving rootkit default files and dirs... nothing found
```

```

Activities Terminal 3 Feb 17:21 acer@acer-Aspire-A315-53: ~
[1] 1000 1000
Searching for LUC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for HKRK rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Annoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for SHKL rootkit default files and dirs... nothing found
Searching for Ajakit rootkit default files and dirs... nothing found
Searching for Zabbix rootkit default files and dirs... nothing found
Searching for Zabbix rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootedoor... nothing found
Searching for ENYELIK rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for Linux/Ebury - Operation Windigo ssh... nothing found
Searching for 64-bit Linux Rootkit ... nothing found
Searching for 64-bit Linux Rootkit modules... nothing found
Searching for Mumblehard Linux ... nothing found
Searching for Backdoor-Linux.Mokes.a ... nothing found
Searching for Malicious.TinyONS ... nothing found
Searching for Linux.Xor.DDoS ... nothing found
Searching for Linux.Xor.TrojanProxy.1.0 ... nothing found
Searching for CrossRAT ... nothing found
Searching for Hidden Cobra ... nothing found
Searching for Rocke Miner ... nothing found
Searching for PWNLNX4 lkm... nothing found
Searching for PWNLNX6 lkm... nothing found
Searching for Umbreon.lrk... nothing found
Searching for Kinsing.a.backdoor... nothing found
Searching for RotaJakiro backdoor... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... not infected
Checking 'asp'... not infected
Checking 'blsshell'... chkproc: nothing detected
Checking 'lkey'... not found
chkrootkit: nothing detected
Checking 'rexeds'... not found
Checking 'sniffer'... Output from ifpromisc:
lo: no promisc and no packet sniffer sockets
wlp2s0: PACKET SNIFFER[/usr/sbin/NetworkManager[586], /usr/sbin/WirelessManager[586], /usr/sbin/wpa_supplicant[575])
Checking 'ws5808'... not infected
Checking 'wted'... chkwtmp: nothing deleted
Checking 'scalper'... not infected
Checking 'slapper'... not infected
Checking 'zz'... user acer deleted or never logged from lastlog!
Checking 'chkutmp'... The tty of the following process(es) was not found in /var/run/utmp:
! RUID ! EUID ! TTY CMD
! acer ! 34681 ! pts/0 bash
! acer ! 34683 ! pts/0 sudo chkrootkit
chkutmp: nothing deleted
Checking 'OSX_RSPLUG'... not tested
acer@acer-Aspire-A315-53: ~

```

This test show that chkrootkit not found signs that the system is infected with a ‘rootkit’.

I checked my server with rkhunter run the following command:

`sudo rkhunter -c`

```

Activities Terminal 3 Feb 17:33 acer@acer-Aspire-A315-53: ~
[1] 1000 1000
acer@acer-Aspire-A315-53: $ sudo rkhunter -c
[ Rootkit Hunter version 1.4.6 ]
Checking system commands...
Performing 'strings' command checks [ OK ]
Checking 'strings' command [ OK ]
Performing 'shared libraries' checks [ None found ]
Checking for preloaded variables [ None found ]
Checking for preloaded libraries [ Not found ]
Checking LD_LIBRARY_PATH variable
Performing file properties checks
Checking for prerequisites
/usr/sbin/adduser [ OK ]
/usr/sbin/chroot [ OK ]
/usr/sbin/cryptsetup [ OK ]
/usr/sbin/demod [ OK ]
/usr/sbin/fscck [ OK ]
/usr/sbin/groupdel [ OK ]
/usr/sbin/groupmod [ OK ]
/usr/sbin/grpcck [ OK ]
/usr/sbin/ifconfig [ OK ]
/usr/sbin/init [ OK ]
/usr/sbin/modinfo [ OK ]
/usr/sbin/lsmod [ OK ]
/usr/sbin/mindinfo [ OK ]
/usr/sbin/modprobe [ OK ]
/usr/sbin/nologin [ OK ]
/usr/sbin/pwck [ OK ]
/usr/sbin/rmmod [ OK ]
/usr/sbin/route [ OK ]
/usr/sbin/syslogd [ OK ]
/usr/sbin/unhide [ OK ]
/usr/sbin/unhide-linux [ OK ]
/usr/sbin/unhide-postx [ OK ]
/usr/sbin/unhide-tcp [ OK ]
/usr/bin/awk [ OK ]
/usr/bin/basename [ OK ]
/usr/bin/bash [ OK ]
/usr/bin/cat [ OK ]
/usr/bin/chattr [ OK ]
/usr/bin/chmod [ OK ]
/usr/bin/chown [ OK ]
/usr/bin/cp [ OK ]
/usr/bin/cut [ OK ]

```

```
Activities Terminal 3 Feb 17:33 acer@acer-Aspire-A315-53: ~
[OK] /usr/bin/cp
[OK] /usr/bin/cut
[OK] /usr/bin/date
[OK] /usr/bin/dcd
[OK] /usr/bin/diff
[OK] /usr/bin dirname
[OK] /usr/bin/dmesg
[OK] /usr/bin/dpkg
[OK] /usr/bin/dpkg-query
[OK] /usr/bin/du
[OK] /usr/bin/echo
[OK] /usr/bin/ed
[OK] /usr/bin/egrep
[OK] /usr/bin/env
[OK] /usr/bin/fgrep
[OK] /usr/bin/file
[OK] /usr/bin/ffind
[OK] /usr/bin/fuser
[OK] /usr/bin/GET
[OK] /usr/bin/grep
[OK] /usr/bin/groups
[OK] /usr/bin/head
[OK] /usr/bin/ld
[OK] /usr/bin/ip
[OK] /usr/bin/ips
[OK] /usr/bin/kill
[OK] /usr/bin/killall
[OK] /usr/bin/last
[OK] /usr/bin/lastlog
[OK] /usr/bin/ldd
[OK] /usr/bin/less
[OK] /usr/bin/logger
[OK] /usr/bin/login
[OK] /usr/bin/ls
[OK] /usr/bin/lsattr
[OK] /usr/bin/lsmod
[OK] /usr/bin/lsof
[OK] /usr/bin/mail
[OK] /usr/bin/md5sum
[OK] /usr/bin/mktemp
[OK] /usr/bin/more
[OK] /usr/bin/mount
[OK] /usr/bin/mv
[OK] /usr/bin/netstat
[OK] /usr/bin/newgrp
[OK] /usr/bin/passwd
[OK] /usr/bin/perl
[OK] /usr/bin/pgrep
[OK] /usr/bin/ping
[OK] /usr/bin/pkill
[OK] /usr/bin/pstree
[OK] /usr/bin/pwd
[OK] /usr/bin/readlink
[OK] /usr/bin/rkhunter
[OK] /usr/bin/runcon
```

```
Activities Terminal 3 Feb 17:34 acer@acer-Aspire-A315-53: ~
[Press <ENTER> to continue]
[OK] Checking for rootkits...
Performing check of known rootkit files and directories
55900 Trojan - Variant A [ Not found ]
ADM Worm [ Not found ]
AjakIT Rootkit [ Not found ]
Adore Rootkit [ Not found ]
aPa Kit [ Not found ]
Apache Worm [ Not found ]
Ambient (ark) Rootkit [ Not found ]
Balaur Rootkit [ Not found ]
BeastKit Rootkit [ Not found ]
bex Rootkit [ Not found ]
BopKit Rootkit [ Not found ]
Cb Rootkit [ Not found ]
CINIK Worm (Slapper.B variant) [ Not found ]
Danny-Boy's Abuse Kit [ Not found ]
Devil Rootkit [ Not found ]
Dlamorphine LKM [ Not found ]
Dica-Kit Rootkit [ Not found ]
Dreams Rootkit [ Not found ]
Duarawkz Rootkit [ Not found ]
Ebury Backdoor [ Not found ]
Evile LKM [ Not found ]
Flea Linux Rootkit [ Not found ]
Fu Rootkit [ Not found ]
Fuck_it Rootkit [ Not found ]
GasKit Rootkit [ Not found ]
HeronL LKM [ Not found ]
Hjt Kit [ Not found ]
ignokit Rootkit [ Not found ]
Intoxikits Rootkit [ Not found ]
J2 Rootkit [ Not found ]
Jinx Rootkit [ Not found ]
Jynx Rootkit [ Not found ]
KBeast Rootkit [ Not found ]
Kitko Rootkit [ Not found ]
Knark Rootkit [ Not found ]
ld-linuxv.so Rootkit [ Not found ]
Lion Worm [ Not found ]
Lockit_LjK2 Rootkit [ Not found ]
Mole Backdoor [ Not found ]
Mood-NT Rootkit [ Not found ]
Nbv Rootkit [ Not found ]
Nt6 Rootkit [ Not found ]
Ohhara Rootkit [ Not found ]
Optic Kit (Tux) Worm [ Not found ]
Oz Rootkit [ Not found ]
Phalanx Rootkit [ Not found ]
Phalanx2 Rootkit [ Not found ]
Phalanx2 Rootkit (extended tests) [ Not found ]
```

```
Activities Terminal 3 Feb 17:34
acer@acer-Aspire-A315-53: ~

GasKit Rootkit [ Not found ]
Heroin LKM [ Not found ]
Hjc KIt [ Not found ]
Ignokit Rootkit [ Not found ]
IntoXona-NG Rootkit [ Not found ]
Irix Rootkit [ Not found ]
Jynx Rootkit [ Not found ]
Jynx2 Rootkit [ Not found ]
K3RnT Rootkit [ Not found ]
K3RnT Rootkit [ Not found ]
Knark Rootkit [ Not found ]
ld-linux.so Rootkit [ Not found ]
Lion Worm [ Not found ]
Lockit / LK2 Rootkit [ Not found ]
Mokes backdoor [ Not found ]
Mood-NT Rootkit [ Not found ]
MRK Rootkit [ Not found ]
Nt0 Rootkit [ Not found ]
Ohara Rootkit [ Not found ]
Optic Kit (Tx) Worm [ Not found ]
OZ Rootkit [ Not found ]
Phalanx Rootkit [ Not found ]
Phalanx2 Rootkit [ Not found ]
Phalanx2 Rootkit (extended tests) [ Not found ]
Portacelo Rootkit [ Not found ]
R3dstorm Toolkit [ Not found ]
RH-Sharpe's Rootkit [ Not found ]
RSHA's Rootkit [ Not found ]
Scalper Worm [ Not found ]
Sebek LKM [ Not found ]
Shutdown Rootkit [ Not found ]
SHV4 Rootkit [ Not found ]
SHVS Rootkit [ Not found ]
Slapper Worm [ Not found ]
Sneakin Rootkit [ Not found ]
'Spanish' Rootkit [ Not found ]
Suckit Rootkit [ Not found ]
Superkit Rootkit [ Not found ]
TBD (Telnet BackDoor) [ Not found ]
TeleKit Rootkit [ Not found ]
T0rn Rootkit [ Not found ]
trnkit Rootkit [ Not found ]
Trojanit KIt [ Not found ]
Tuxtendo Rootkit [ Not found ]
URK Rootkit [ Not found ]
Vampire Rootkit [ Not found ]
Vckit Rootkit [ Not found ]
Volc Rootkit [ Not found ]
Xzibit Rootkit [ Not found ]
zaRW!K! Rootkit [ Not found ]
ZK Rootkit [ Not found ]

[Press <ENTER> to continue]
```

```
Activities Terminal 3 Feb 17:35
acer@acer-Aspire-A315-53: ~

Oz Rootkit [ Not found ]
Phalanx Rootkit [ Not found ]
Phalanx2 Rootkit [ Not found ]
Phalanx2 Rootkit (extended tests) [ Not found ]
Portacelo Rootkit [ Not found ]
R3dstorm Toolkit [ Not found ]
RH-Sharpe's Rootkit [ Not found ]
RSHA's Rootkit [ Not found ]
Scalper Worm [ Not found ]
Sebek LKM [ Not found ]
Shutdown Rootkit [ Not found ]
SHV4 Rootkit [ Not found ]
SHVS Rootkit [ Not found ]
Slapper Worm [ Not found ]
Sneakin Rootkit [ Not found ]
'Spanish' Rootkit [ Not found ]
Suckit Rootkit [ Not found ]
Superkit Rootkit [ Not found ]
TBD (Telnet BackDoor) [ Not found ]
TeleKit Rootkit [ Not found ]
T0rn Rootkit [ Not found ]
trnkit Rootkit [ Not found ]
Trojanit KIt [ Not found ]
Tuxtendo Rootkit [ Not found ]
URK Rootkit [ Not found ]
Vampire Rootkit [ Not found ]
Vckit Rootkit [ Not found ]
Volc Rootkit [ Not found ]
Xzibit Rootkit [ Not found ]
zaRW!K! Rootkit [ Not found ]
ZK Rootkit [ Not found ]

[Press <ENTER> to continue]

Performing additional rootkit checks
  Suckit Rootkit additional checks [ OK ]
  Checking for possible rootkit files and directories [ None Found ]
  Checking for possible rootkit strings [ None Found ]

Performing malware checks
  Checking for suspicious processes for suspicious files [ None Found ]
  Checking for login backdoors [ None Found ]
  Checking for sniffer log files [ None Found ]
  Checking for suspicious directories [ None Found ]
  Checking for suspicious (large) shared memory segments [ Warning ]
  Checking for Apache backdoor [ Not found ]

Performing Linux specific checks
  Checking loaded kernel modules [ OK ]
  Checking kernel module names [ OK ]

[Press <ENTER> to continue]
```

```

Activities Terminal 3 Feb 17:34
acer@acer-Aspire-A315-53: ~
[OK ] /usr/bin/readlink
[OK ] /usr/bin/rkHunter
[OK ] /usr/bin/rkUnroot
[OK ] /usr/bin/sed
[OK ] /usr/bin/sh
[OK ] /usr/bin/sha1sum
[OK ] /usr/bin/sha24sum
[OK ] /usr/bin/sha256sum
[OK ] /usr/bin/sha384sum
[OK ] /usr/bin/sha512sum
[OK ] /usr/bin/stty
[OK ] /usr/bin/sort
[OK ] /usr/bin/ssh
[OK ] /usr/bin/stat
[OK ] /usr/bin/trace
[OK ] /usr/bin/strings
[OK ] /usr/bin/tar
[OK ] /usr/bin/sudo
[OK ] /usr/bin/tail
[OK ] /usr/bin/telnet
[OK ] /usr/bin/test
[OK ] /usr/bin/top
[OK ] /usr/bin/touch
[OK ] /usr/bin/tr
[OK ] /usr/bin/truncate
[OK ] /usr/bin/unlq
[OK ] /usr/bin/users
[OK ] /usr/bin/vmstat
[OK ] /usr/bin/w
[OK ] /usr/bin/watch
[OK ] /usr/bin/wc
[OK ] /usr/bin/wget
[OK ] /usr/bin/whatis
[OK ] /usr/bin/whereis
[OK ] /usr/bin/which
[OK ] /usr/bin/whoami
[OK ] /usr/bin/nufmt
[OK ] /usr/bin/kmod
[OK ] /usr/bin/systemd
[OK ] /usr/bin/systemctl
[OK ] /usr/bin/mawk
[Warning ] /usr/bin/lwp-request
[OK ] /usr/bin/bsd-mailx
[OK ] /usr/bin/dash
[OK ] /usr/bin/x86_64-linux-gnu-size
[OK ] /usr/bin/x86_64-linux-gnu-strings
[OK ] /usr/bin/telnet.netkit
[OK ] /usr/bin/which.debianutils
[Warning ] /usr/bin/snap
[Warning ] /snap/bin/curl
[OK ] /usr/lib/systemd/systemd

[Press <ENTER> to continue]

```

This test shown the files not infected. Rootkits not found:

```

Performing check of known rootkit files and directories
55888 Trojan - Variant A [ Not Found ]
ADM Rootkit [ Not Found ]
AAPT Rootkit [ Not Found ]
Adore Rootkit [ Not Found ]
afe Rootkit [ Not Found ]
Aggressive Worm [ Not Found ]
Ambient (ark) Rootkit [ Not Found ]
Balaur Rootkit [ Not Found ]
Bassi Rootkit [ Not Found ]
beX2 Rootkit [ Not Found ]
BOBKIT Rootkit [ Not Found ]
C2 Rootkit [ Not Found ]
CINIK Worm (Slapper.B variant) [ Not Found ]
Danny Boy's Abuse Kit [ Not Found ]
DDE Rootkit [ Not Found ]
Dianorphine LKM [ Not Found ]
DiCa-Kit Rootkit [ Not Found ]
Dionysus Rootkit [ Not Found ]
Duarawz Rootkit [ Not Found ]
Ebony backdoor [ Not Found ]
EFS Rootkit [ Not Found ]
Flea Linux Rootkit [ Not Found ]
Fu Rootkit [ Not Found ]
Fuz Rootkit [ Not Found ]
Gaskit Rootkit [ Not Found ]
Heroin LKM [ Not Found ]
HIV Rootkit [ Not Found ]
Ignokit Rootkit [ Not Found ]
Int0Kon1-M Rootkit [ Not Found ]
IJK Rootkit [ Not Found ]
Jynx Rootkit [ Not Found ]
Jynx2 Rootkit [ Not Found ]
KeezeRoot Rootkit [ Not Found ]
Kite Rootkit [ Not Found ]
Knark Rootkit [ Not Found ]
L01Thruve.s0 Rootkit [ Not Found ]
L1K Rootkit [ Not Found ]
Lockit / LK2 Rootkit [ Not Found ]
Mokes Rootkit [ Not Found ]
Monera NT Rootkit [ Not Found ]
MRB Rootkit [ Not Found ]
NBB Rootkit [ Not Found ]
Obamara Rootkit [ Not Found ]
Optic Kit (Tux) Worm [ Not Found ]
OZ Rootkit [ Not Found ]
Panda Rootkit [ Not Found ]
Phalanz Rootkit [ Not Found ]
Phalanz2 Rootkit (extended tests) [ Not Found ]
Piranha Rootkit [ Not Found ]
R3dstorm Toolkit [ Not Found ]
RH-Sharp 5 Rootkit [ Not Found ]
RSH Rootkit [ Not Found ]
Scalper Worm [ Not Found ]
Sehgal LKM [ Not Found ]
Shutter Rootkit [ Not Found ]
SH4 Rootkit [ Not Found ]
SHVS Rootkit [ Not Found ]
SIS Rootkit [ Not Found ]
Slapper Worm [ Not Found ]
Sneakin Rootkit [ Not Found ]
Sploit Rootkit [ Not Found ]
Suckit Rootkit [ Not Found ]
Superkit Rootkit [ Not Found ]
T3LLY (Linux Backdoor) [ Not Found ]
Telekit Rootkit [ Not Found ]
Torn Rootkit [ Not Found ]
TNT Rootkit [ Not Found ]
TrojanKit Rootkit [ Not Found ]
Tuxedo Rootkit [ Not Found ]
U3 Rootkit [ Not Found ]
Vampire Rootkit [ Not Found ]
Vckit Rootkit [ Not Found ]
Virus Rootkit [ Not Found ]
Xzibit Rootkit [ Not Found ]
zad0W.KIT Rootkit [ Not Found ]

```

## I used Nmap on Ubuntu 22.04

Nmap is the favorite utility of network administrators as they can use Nmap to scan the IP address, scan the host, find a live host, and much more like that. The Nmap command can be used to scan through the open ports of the host. For instance, I scanned the “192.168.214.138” for open ports:

```
nmap -F 192.168.214.138
```

```
acer@acer-Aspire-A315-53:~$ nmap -F 192.168.214.138
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-03 22:39 GMT
Nmap scan report for 192.168.214.138
Host is up (0.23s latency).
Not shown: 96 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds
acer@acer-Aspire-A315-53:~$ █
```

Nmap command has an extensive list of options to deal with security auditing and network exploration. Nmap command will be used to scan the ports or hosts, list down the services on the network, get the list of all live hosts, check the open ports on the network, real-time information about the network.

#### 4.5 We can adjust the system in light of test results

Based on the test results for the LAMP server, adjustments may be needed to ensure optimal functionality while maintaining security. Here are some steps to adjust the system in light of the test results:

- Email Spam Filtering:
  - Review the spam detection thresholds: If the system is too aggressive in labelling emails as spam, the thresholds for spam detection scores may need to be adjusted. This adjustment should balance between effectively filtering out spam and avoiding false positives.
  - Fine-tune email actions: Ensure that emails labelled as spam are handled appropriately based on the configured actions, such as moving them to a spam folder or deleting them. Adjustments may be necessary to ensure the desired behaviour.
- Web Server Security and Error Handling:
  - Review file permissions: If the web server requires write access to certain directories for functionality (such as creating temporary files for portfolio pages), ensure that

the necessary file permissions are set correctly. Adjust permissions if needed to allow the web server to write to the required directories while maintaining security.

- **Modify error messages:** If errors occur due to permissions issues or other reasons, review and modify the error messages to provide clear and informative feedback to users. Generic error messages can be updated to provide specific guidance on resolving the issue, such as checking directory permissions or contacting the administrator for assistance.
- **Monitor web server logs:** Check the web server logs for corresponding error messages related to file write permissions or any other issues encountered. Use these logs to diagnose and address any configuration or permissions problems affecting the functionality of the web server.

By making these adjustments and fine-tuning the system based on the test results, you can ensure that the LAMP server operates securely while effectively supporting the intended functionality of email services and web applications. Regular monitoring and maintenance are essential to address any issues that arise and maintain the security and functionality of the server over time.

#### **4.6 We can document the test results for third party support people**

To effectively document the test results for third-party support people, a comprehensive and organized document can be created. Below is an example template for documenting system tests:

---

##### System Test Results Documentation

*Date of Testing:* [Insert Date]

*Tested By:* [Insert Name]

*Tested Component:* LAMP Server

##### 1. Email Spam Filtering Test Results:

- **Spam Detection Scores:**
  - Average Spam Score: [Insert Average Score]
  - Highest Score Observed: [Insert Highest Score]
  - Lowest Score Observed: [Insert Lowest Score]
- **Email Actions:**
  - Configuration: [Describe Configured Actions]
  - Effectiveness: [Describe Effectiveness Based on Test Results]

## 2. Web Server Functionality and Security Test Results:

- File Write Permissions:
  - Directory: [Insert Directory Path]
  - Permissions: [Describe Permissions Set]
  - Functionality Impact: [Describe Impact on Server Functionality]
- Error Handling and Messages:
  - Generic Error Message: [Insert Message]
  - Modification: [Describe Modified Error Message]
- Web Server Logs:
  - Reviewed Logs: [Specify Logs Reviewed]
  - Errors Identified: [List Identified Errors]
  - Actions Taken: [Describe Actions Taken to Address Errors]

## **5. Evaluate the effectiveness of the system**

### **5.1 I can analyse the results in terms of the objectives**

The output obtained a Lynis report, contains a hardening index score that is rated out of 100, this is used to give a trackable tangible score of system's current security posture. In previous executions, Lynis showed a 73 hardening index level.

To increase hardening index score, Lynis provided helpful suggestions that detail the various security configurations to be made.

### **5.2 I can evaluate some of the features of the system and their purpose**

Program version: 3.0.9

Operating system: Linux

Operating system name: Ubuntu

Operating system version: 22.04

Kernel version: 6.5.0

Hardware platform: x86\_64

Hostname: acer-Aspire-A315-53

Boot and services

---

- Service Manager [ systemd ]
- Checking UEFI boot [ ENABLED ]
- Checking Secure Boot [ ENABLED ]
- Checking presence GRUB2 [ FOUND ]

Users, Groups and Authentication

---

- Administrator accounts [ OK ]
- Unique UIDs [ OK ]
- Consistency of group files (grpck) [ OK ]
- Unique group IDs [ OK ]
- Unique group names [ OK ]
- Password file consistency [ OK ]
- Password hashing methods [ OK ]

Networking

---

- Checking IPv6 configuration [ ENABLED ]
- Configuration method [ AUTO ]
- IPv6 only [ NO ]

## Software: firewalls

---

- Checking iptables kernel module [ FOUND ]
- Checking iptables policies of chains [ FOUND ]
- Checking for empty ruleset [ OK ]
- Checking for unused rules [ FOUND ]
- Checking host based firewall [ ACTIVE ]

## [+] Software: webserver

---

- Checking Apache (binary /usr/sbin/apache2) [ FOUND ]
- Info: Configuration file found (/etc/apache2/apache2.conf)
- Info: Found 4 virtual hosts
- \* Loadable modules [ FOUND (120) ]

## Databases

---

- MySQL process status [ FOUND ]

## Software: file integrity

---

- Checking file integrity tools
- AIDE [ FOUND ]
- AIDE config file [ FOUND ]
- AIDE database [ NOT FOUND ]
- AIDE config (Checksum) [ OK ]
- Checking presence integrity tool [ FOUND ]

## [+] Software: System tooling

---

- Checking automation tooling
- Automation tooling [ NOT FOUND ]
- Checking presence of Fail2ban [ FOUND ]
- Checking Fail2ban jails [ ENABLED ]
- Checking for IDS/IPS tooling [ FOUND ]

## [+] Software: Malware

---

- Checking chkrootkit [ FOUND ]
- Checking Rootkit Hunter [ FOUND ]

- Checking ClamAV scanner [ FOUND ]
- Malware software components [ FOUND ]
- Active agent [ NOT FOUND ]
- Rootkit scanner [ FOUND ]

### 5.3 I can justify some design decisions in terms of objectives

In the Linus report was displayed potential warning :

Warnings (1):

-----  
! Found some information disclosure in SMTP banner (OS or software name)  
[MAIL-8818]

<https://cisofy.com/lynis/controls/MAIL-8818/>

I fixed it by editing the file /etc/postfix/main.cf and removing everything after the ESMTP on the following line:

smtpd\_banner = \$myhostname ESMTP \$mail\_name

```
acer@acer-Aspire-A315-53:~$ sudo nano /etc/postfix/main.cf
[sudo] password for acer:
sudo: nano/etc/postfix/main.cf: command not found
acer@acer-Aspire-A315-53:~$ sudo nano /etc/postfix/main.cf
acer@acer-Aspire-A315-53:~$ sudo lynis audit system
```

```
Activities Terminal 4 Feb 12:03
acer@acer-Aspire-A315-53:~$ sudo nano /etc/postfix/main.cf
[sudo] password for acer:
GNU nano 6.2
See /usr/share/postfix/main.cf.dist for a commented, more complete version
acer@acer-Aspire-A315-53:~$ /etc/postfix/main.cf
acer@acer-Aspire-A315-53:~$ sudo lynis audit system

# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_Capath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = acer-Aspire-A315-53
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, acer-Aspire-A315-53, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [:ffff:127.0.0.0]/104 [:1]:128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

```

Activities Terminal 4 Feb 12:04
acer@acer-Aspire-A315-53: ~
GNU nano 6.2
See /usr/share/postfix/main.cf.dist for a commented, more complete version
/etc/postfix/main.cf *

# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_Capath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = acer-Aspire-A315-53
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, acer-Aspire-A315-53, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [:ffff:127.0.0.0]/104 [:1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

```

Help Exit Write Out Read File Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark To Bracket Where Was Previous Back Forwards Next Word

And restarted postfix: sudo /etc/init.d/postfix restart

After made this configuration, I done system audit again.

sudo lynis audit system

The summary of the system audit didn't contain previous warning.

## 5.4 I can analyse possible improvements to the system based on usage

1. In the Linus report was displayed potential warnings :

\* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]

<https://cisofy.com/lynis/controls/LYNIS/>

I fixed it by update Lynis

```

acer@acer-Aspire-A315-53: ~$ sudo apt update
[sudo] password for acer:
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://gb.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://gb.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 https://packages.cisofy.com/community/lynis/deb stable InRelease
Hit:5 http://gb.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:6 https://dl.google.com/linux/chrome/deb stable InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://packages.cisofy.com/community/lynis/deb/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
acer@acer-Aspire-A315-53: ~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
Get another security update through Ubuntu Pro with 'esm-apps' enabled:
 libapache2-mod-security2
Learn more about Ubuntu Pro at https://ubuntu.com/pro
The following packages have been kept back:
 gjs libgjs0g
0 to upgrade, 0 to newly install, 0 to remove and 2 not to upgrade.
acer@acer-Aspire-A315-53: ~$ lynis show version
3.0.9

```

2. In the Linus report was displayed potential warning :

\* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]

<https://cisofy.com/lynis/controls/KRNL-5820/>

I add the following line to /etc/security/limits.conf file:

\* hard core 0

Set the following parameter in /etc/sysctl.d/\* file:

fs.suid\_dumpable = 0

Run the following command to set the active kernel parameter:

# sysctl -w fs.suid\_dumpable=0

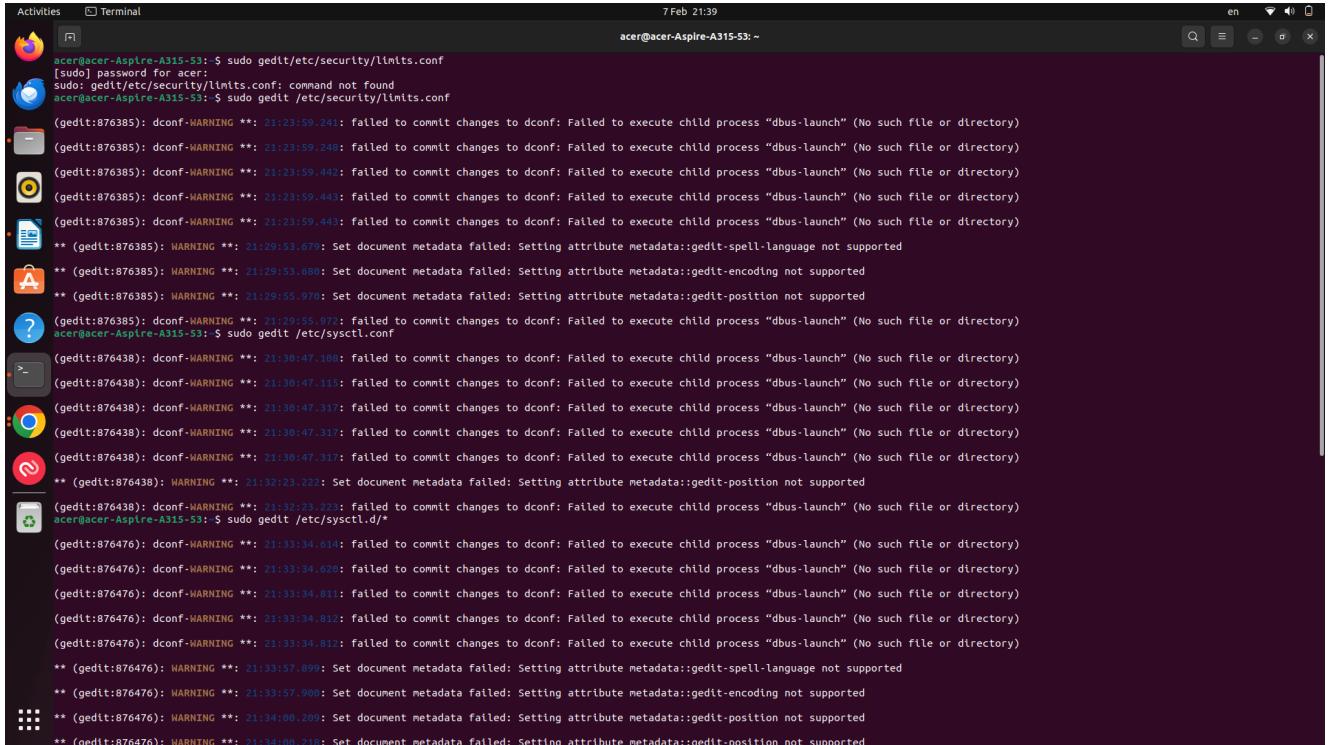
Then edited /etc/systemd/coredump.conf :

Storage=none

ProcessSizeMax=0

And run the command:

systemctl daemon-reload



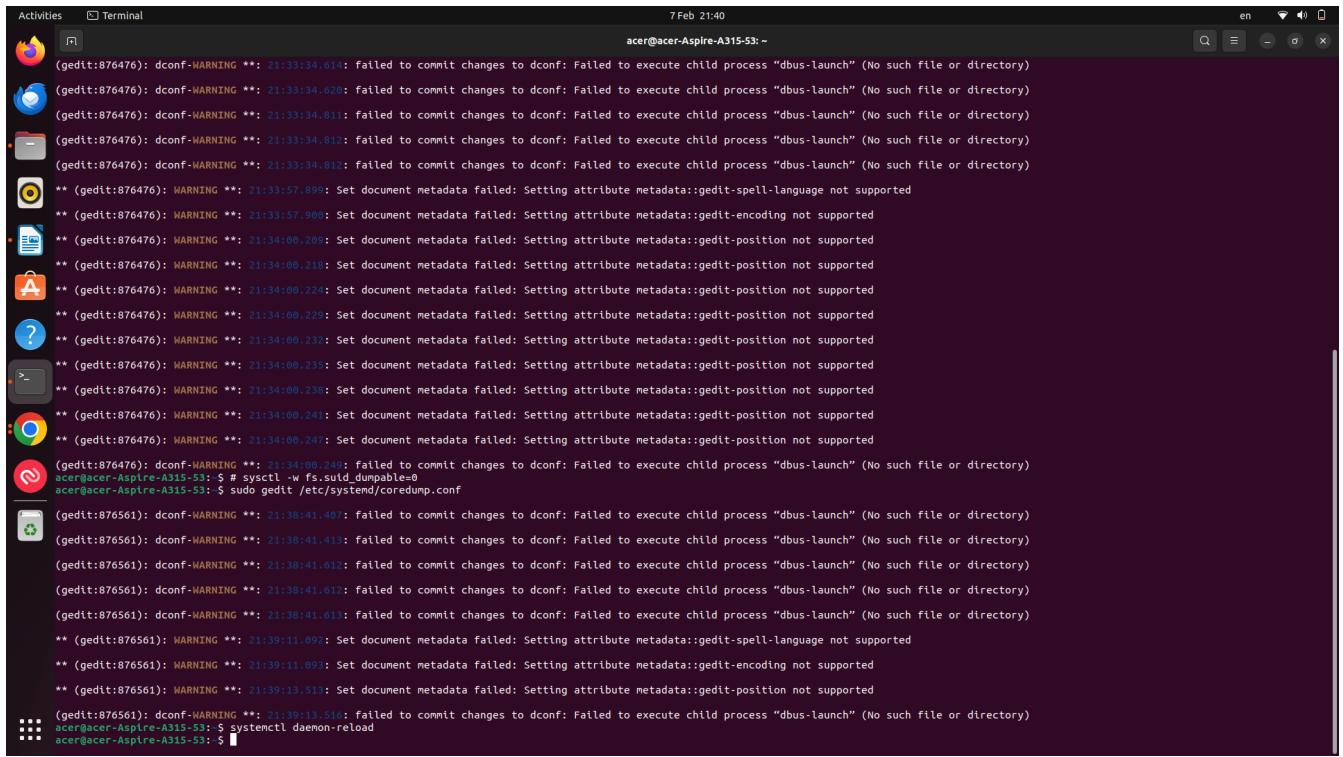
```
Activities Terminal 7 Feb 21:39
acer@acer-Aspire-A315-53:~$ sudo gedit/etc/security/limits.conf
[sudo] password for acer:
sudo: gedit/etc/security/limits.conf: command not found
acer@acer-Aspire-A315-53:~$ sudo gedit /etc/security/limits.conf

(gedit:876385): dconf-WARNING **: 21:23:59.241: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876385): dconf-WARNING **: 21:23:59.248: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876385): dconf-WARNING **: 21:23:59.442: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876385): dconf-WARNING **: 21:23:59.443: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876385): dconf-WARNING **: 21:23:59.443: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

** (gedit:876385): WARNING **: 21:29:53.070: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:876385): WARNING **: 21:29:53.680: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:876385): WARNING **: 21:29:55.970: Set document metadata failed: setting attribute metadata::gedit-position not supported
(gedit:876438): dconf-WARNING **: 21:30:59.972: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
acer@acer-Aspire-A315-53:~$ sudo gedit /etc/sysctl.conf

(gedit:876438): dconf-WARNING **: 21:30:47.108: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876438): dconf-WARNING **: 21:30:47.115: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876438): dconf-WARNING **: 21:30:47.317: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876438): dconf-WARNING **: 21:30:47.317: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876438): dconf-WARNING **: 21:30:47.317: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:876438): WARNING **: 21:32:23.222: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:876438): dconf-WARNING **: 21:32:23.223: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
acer@acer-Aspire-A315-53:~$ sudo gedit /etc/sysctl.d/*
(gedit:876476): dconf-WARNING **: 21:33:34.614: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876476): dconf-WARNING **: 21:33:34.626: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876476): dconf-WARNING **: 21:33:34.811: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876476): dconf-WARNING **: 21:33:34.812: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:876476): dconf-WARNING **: 21:33:34.812: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

** (gedit:876476): WARNING **: 21:33:57.890: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:876476): WARNING **: 21:33:57.900: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:876476): WARNING **: 21:34:00.269: Set document metadata failed: Setting attribute metadata::gedit-position not supported
** (gedit:876476): WARNING **: 21:34:00.270: Set document metadata failed: Setting attribute metadata::gedit-position not supported
```



```
Activities Terminal 7 Feb 21:40 acer@acer-Aspire-A315-53:~  
gedit(876476): dconf-WARNING **: 21:33:34.614: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
gedit(876476): dconf-WARNING **: 21:33:34.620: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
gedit(876476): dconf-WARNING **: 21:33:34.811: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
gedit(876476): dconf-WARNING **: 21:33:34.812: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
gedit(876476): dconf-WARNING **: 21:33:34.812: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
** (gedit:876476): WARNING **: 21:33:57.897: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported  
** (gedit:876476): WARNING **: 21:33:57.900: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported  
** (gedit:876476): WARNING **: 21:34:00.207: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.211: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.222: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.227: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.231: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.231: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.231: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.231: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.241: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.241: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
** (gedit:876476): WARNING **: 21:34:00.241: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
(gedit:876476): dconf-WARNING **: 21:34:00.249: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
acer@acer-Aspire-A315-53:~$ # systemctl -w fs.suid_dumpable=0  
acer@acer-Aspire-A315-53:~$ sudo gedit /etc/systemd/coredump.conf  
(gedit:876561): dconf-WARNING **: 21:38:41.407: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
(gedit:876561): dconf-WARNING **: 21:38:41.411: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
(gedit:876561): dconf-WARNING **: 21:38:41.612: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
(gedit:876561): dconf-WARNING **: 21:38:41.612: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
(gedit:876561): dconf-WARNING **: 21:38:41.613: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
** (gedit:876561): WARNING **: 21:39:11.097: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported  
** (gedit:876561): WARNING **: 21:39:11.099: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported  
** (gedit:876561): WARNING **: 21:39:13.511: Set document metadata failed: Setting attribute metadata::gedit-position not supported  
(gedit:876561): dconf-WARNING **: 21:39:13.516: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)  
acer@acer-Aspire-A315-53:~$ systemctl daemon-reload  
acer@acer-Aspire-A315-53:~$
```

### 3. In the Linus report was displayed potential warnings :

- \* Configure password hashing rounds in /etc/login.defs [AUTH-9230]  
<https://cisofy.com/lynis/controls/AUTH-9230/>
- \* When possible set expire dates for all password protected accounts [AUTH-9282]  
<https://cisofy.com/lynis/controls/AUTH-9282/>
- \* Configure minimum password age in /etc/login.defs [AUTH-9286]  
<https://cisofy.com/lynis/controls/AUTH-9286/>
- \* Configure maximum password age in /etc/login.defs [AUTH-9286]  
<https://cisofy.com/lynis/controls/AUTH-9286/>

I fixed it by edit /etc/login.defs

Activities Terminal

11 Feb 10:25 acer@acer-Aspire-A315-53: ~ /etc/login.defs \*

```
GNU nano 6.2
#ENCRYPT_METHOD SHA512

#
# Only used if ENCRYPT_METHOD is set to SHA256 or SHA512.
#
# Define the number of SHA rounds.
# With a lot of rounds, it is more difficult to brute force the password.
# But note also that it more CPU resources will be needed to authenticate
# users.
#
# If not specified, the libp will choose the default number of rounds (5000).
# The values must be inside the 1000-99999999 range.
# If only one of the MIN or MAX values is set, then this value will be used.
# If MIN > MAX, the highest value will be used.
#
# SHA_CRYPT_MIN_ROUNDS 5000
#SHA_CRYPT_MAX_ROUNDS 5000
#####
##### OBSOLETE BY PAM #####
# These options are now handled by PAM. Please #
# edit the appropriate file in /etc/pam.d/ to #
# enable the equivalents of them.
#
#####

#NOTFILE
#LASTLOG_ENAB
#MAIL_CHECK_ENAB
#OBSCURE_CHECKS_ENAB
#PORTTIME_CHECKS_ENAB
#SU_WHEEL_ONLY
#CRACKLIB_DICTPATH
#PASS_MAX_TRIES
#PASS_DAYS_MARN
#ENVIRON_FILE
#NOLOGINS_FILE
#ISSUE_FILE
#PASS_MIN_LEN
#PASS_MAX_LEN
#ULIMIT
#ENV_HZ
#CHFN_AUTH
#CHGD_AUTH
#FAIL_DELAY

#####
##### OBSOLETE #####
# These options are no more handled by shadow. #
#
#####

^G Help ^C Write Out ^W Where Is ^K Cut ^T Execute ^L Location ^U Undo ^A Set Mark ^H To Bracket ^Q Previous ^B Copy ^Q Where Was ^N Next ^B Back ^F Forwards ^P Prev Word ^N Next Word
```

Activities Terminal

11 Feb 11:48 acer@acer-Aspire-A315-53: ~ /etc/login.defs \*

```
GNU nano 6.2
# Users can still allow other people to write them by issuing
# the "mesg y" command.

TTYGROUP      tty
TTYPERM       0600

#
# Login configuration initializations:
#
# ERASECHAR   Terminal ERASE character ('\010' = backspace).
# KILLCHAR    Terminal KILL character ('\025' = CTRL/U).
# UMASK        Default "umask" value.

# The ERASECHAR and KILLCHAR are used only on System V machines.

# UMASK is the default umask value for pam_umask and is used by
# useradd and newusers to set the mode of the new home directories.
# 022 is the "historical" value in Debian for UMASK
# 027, or even 077, could be considered better for privacy
# There is no One True Answer here : each sysadmin must make up his/her
# mind.

# If USERGROUPS_ENAB is set to "yes", that will modify this UMASK default value
# for private user groups, i. e., the uid is the same as gid, and username is
# the same as the primary group name: for these, the user permissions will be
# used as group permissions, e. g. 022 will become 002.
#
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.

# ERASECHAR     0177
# KILLCHAR      025
# UMASK         027

# HOME_MODE is used by useradd(8) and newusers(8) to set the mode for new
# home directories.
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
# HOME_MODE     0750

#
# Password aging controls:
#
# PASS_MAX_DAYS Maximum number of days a password may be used.
# PASS_MIN_DAYS Minimum number of days allowed between password changes.
# PASS_WARN_AGE Number of days warning given before a password expires.

PASS_MAX_DAYS  99
PASS_MIN_DAYS 0
PASS_WARN_AGE  7

#
# Min/max values for automatic uid selection in useradd
```

#### 4. In the Linus report was displayed potential warning :

- \* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]  
<https://cisofy.com/lynis/controls/AUTH-9328/>

You will fix it by editing the file /etc/login.defs and changing the following line from 022 to 027:

```

# This file contains system-wide login configuration
# parameters.  It is read by /bin/login and /bin/getpwnam.
# Users can still allow other people to write them by issuing
# the "msg y" command.

# TTYGROUP      tty
# TTYPERM      6660
# Login configuration initializations:
#   # ERASECHAR      Terminal ERASE character ('\010' = backspace).
#   # KILLCHAR       Terminal KILL character ('\025' = CTRL/U).
#   # UNASK         Default "umask" value.
#   # The ERASECHAR and KILLCHAR are used only on System V machines.
#   # UMASK is the default umask value for pam_umask and is used by
#   # useradd and newusers to set the mode of the new home directories.
#   # 022 is the "historical" value in Debian for UMASK
#   # 027, or even 077, could be considered better for privacy
#   # There is no One True Answer here : each sysadmin must make up his/her
#   # mind.
#   #
# If USERGROUPS_ENAB is set to "yes", that will modify this UMASK default value
# for private user groups, i.e. the uid is the same as gid, and username is
# the same as the primary group name; for these, the user permissions will be
# used as group permissions, e.g. 022 will become 002.
#
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.
#
# ERASECHAR      0177
# KILLCHAR       025
# UMASK          027
#
# HOME_MODE is used by useradd(8) and newusers(8) to set the mode for new
# home directories.
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
HOME_MODE        0750
#
# Password aging controls:
#
#   PASS_MAX_DAYS    Maximum number of days a password may be used.
#   PASS_MIN_DAYS    Minimum number of days allowed between password changes.
#   PASS_WARN_AGE    Number of days warning given before a password expires.
#
PASS_MAX_DAYS   999999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
#

```

Key bindings at the bottom:

- Ctrl-G Help
- Ctrl-W Write Out
- Ctrl-H Where Is
- Ctrl-K Cut
- Ctrl-C Paste
- Ctrl-T Execute
- Ctrl-J Justify
- Ctrl-L Location
- Ctrl-U Undo
- Ctrl-A Set Mark
- Ctrl-B To Bracket
- Ctrl-Q Where Was
- Ctrl-P Previous
- Ctrl-N Next
- Ctrl-F Backwards
- Ctrl-B Prev Word

## 5. In the Linus report was displayed potential warning :

Check DNS configuration for the dns domain name [NAME-4028]

<https://cisofy.com/lynis/controls/NAME-4028/>

```

acer@acer-Aspire-A315-53:~$ dig domain.com

; <>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>> domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 11813
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;domain.com.           IN      A

;; ANSWER SECTION:
domain.com.            300     IN      A      172.64.145.59
domain.com.            300     IN      A      104.18.42.197

;; Query time: 60 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Feb 11 13:09:34 GMT 2024
;; MSG SIZE  rcvd: 71

acer@acer-Aspire-A315-53:~$
```

6. In the Linus report was displayed potential warning :

\* Install debsums utility for the verification of packages with known good database.  
[PKGS-7370]  
<https://cisofy.com/lynis/controls/PKGS-7370/>

I installed debsums: **sudo apt install debsums**

```
acer@acer-Aspire-A315-53:~$ sudo apt install debsums
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdpkg-perl libfile-fcntllock-perl libfile-fnmatch-perl
Suggested packages:
  debian-keyring gcc | c-compiler bzr
The following NEW packages will be installed
  debsums libdpkg-perl libfile-fcntllock-perl libfile-fnmatch-perl
0 to upgrade, 4 to newly install, 0 to remove and 2 not to upgrade.
Need to get 317 kB of archives.
After this operation, 2,687 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libdpkg-perl all 1.21.1ubuntu2.2 [237 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 libfile-fnmatch-perl amd64 0.02-2build8 [10.5 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 debsums all 3.0.2 [36.3 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 libfile-fcntllock-perl amd64 0.22-3build7 [33.9 kB]
Fetched 317 kB in 3s (107 kB/s)
Selecting previously unselected package libdpkg-perl.
(Reading database ... 217042 files and directories currently installed.)
Preparing to unpack .../libdpkg-perl_1.21.1ubuntu2.2_all.deb ...
Unpacking libdpkg-perl (1.21.1ubuntu2.2) ...
Selecting previously unselected package libfile-fnmatch-perl.
Preparing to unpack .../libfile-fnmatch-perl_0.02-2build8_amd64.deb ...
Unpacking libfile-fnmatch-perl (0.02-2build8) ...
Selecting previously unselected package debsums.
Preparing to unpack .../archives/debsums_3.0.2_all.deb ...
Unpacking debsums (3.0.2) ...
Selecting previously unselected package libfile-fcntllock-perl.
Preparing to unpack .../libfile-fcntllock-perl_0.22-3build7_amd64.deb ...
Unpacking libfile-fcntllock-perl (0.22-3build7) ...
Setting up libdpkg-perl (1.21.1ubuntu2.2) ...
Setting up libfile-fnmatch-perl (0.02-2build8) ...
Setting up debsums (3.0.2) ...
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53:~$
```

7. In the Linus report was displayed potential warning :

\* Install package apt-show-versions for patch management purposes [PKGS-7394]

<https://cisofy.com/lynis/controls/PKGS-7394/>

I installed apt-show-versions package:

**sudo apt -y install apt-show-versions**

```
acer@acer-Aspire-A315-53:~$ sudo apt -y install apt-show-versions
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapt-pkg-perl
The following NEW packages will be installed
  apt-show-versions libapt-pkg-perl
0 to upgrade, 2 to newly install, 0 to remove and 2 not to upgrade.
Need to get 103 kB of archives.
After this operation, 333 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 libapt-pkg-perl amd64 0.1.40build2 [72.5 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 apt-show-versions all 0.22.13 [30.5 kB]
Fetched 103 kB in 26s (3,977 B/s)
Selecting previously unselected package libapt-pkg-perl.
(Reading database ... 217238 files and directories currently installed.)
Preparing to unpack .../libapt-pkg-perl_0.1.40build2_amd64.deb ...
Unpacking libapt-pkg-perl (0.1.40build2) ...
Selecting previously unselected package apt-show-versions.
Preparing to unpack .../apt-show-versions_0.22.13_all.deb ...
Unpacking apt-show-versions (0.22.13) ...
Setting up libapt-pkg-perl (0.1.40build2) ...
Setting up apt-show-versions (0.22.13) ...
** initializing cache. This may take a while **
Created symlink /etc/systemd/system/timers.target.wants/apt-show-versions.timer → /lib/systemd/system/apt-show-versions.timer.
apt-show-versions.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53:~$
```

8. In the Linus report was displayed potential warning :

\* You are advised to hide the mail\_name (option: smtpd\_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818]

<https://cisofy.com/lynis/controls/MAIL-8818/>

I modified the postfix main.cf file and set the smtpd\_banner setting, uncommented and removed \$mail\_name.

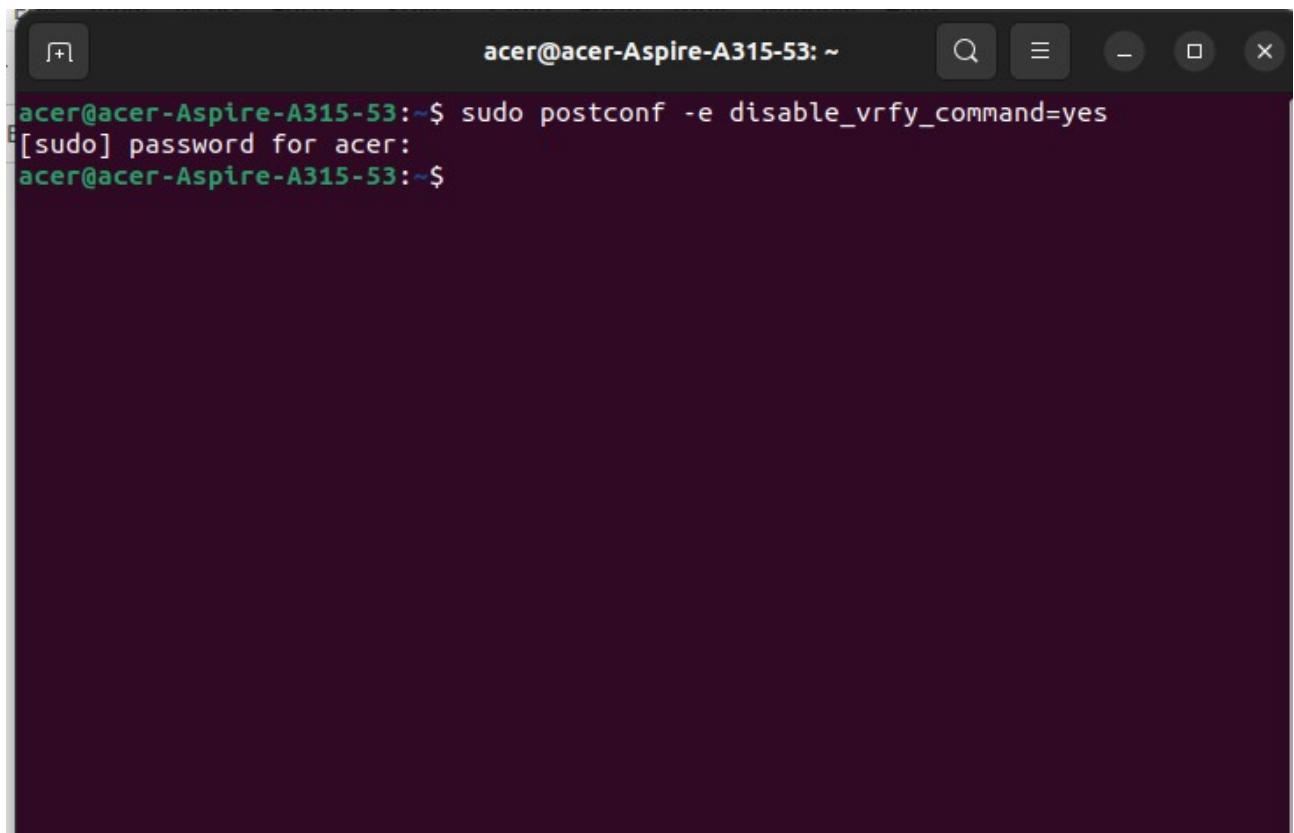
In the Linus report was displayed potential warning :

\* Disable the 'VRFY' command [MAIL-8820:disable\_vrfy\_command]

- Details : disable\_vrfy\_command=no

- Solution : run postconf -e disable\_vrfy\_command=yes to change the value

<https://cisofy.com/lynis/controls/MAIL-8820/>



```
acer@acer-Aspire-A315-53:~$ sudo postconf -e disable_vrfy_command=yes
[sudo] password for acer:
acer@acer-Aspire-A315-53:~$
```

8. In the Linus report was displayed potential warning :

\* Check iptables rules to see which rules are currently not used [FIRE-4513]

<https://cisofy.com/lynis/controls/FIRE-4513/>

I used **iptables --list --numeric --verbose** to display all rules.

```

acer@acer-Aspire-A315-53:~$ sudo iptables -list --numeric --verbose
Chain INPUT (policy DROP 233 packets, 87136 bytes)
pkts bytes target prot opt in  out  source           destination
  56K  52G ufw-before-input all -- *   *      0.0.0.0/0     0.0.0.0/0
  56K  52G ufw-before-input all -- *   *      0.0.0.0/0     0.0.0.0/0
 44973 19M ufw-after-input all -- *   *      0.0.0.0/0     0.0.0.0/0
44996 18M ufw-after-logging-input all -- *   *      0.0.0.0/0     0.0.0.0/0
43590 18M ufw-reject-input all -- *   *      0.0.0.0/0     0.0.0.0/0
43590 18M ufw-track-input all -- *   *      0.0.0.0/0     0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in  out  source           destination
  0   0 ufw-before-logging-forward all -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-forward-forward all -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-after-forward all -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-before-logging-forward all -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-reject-forward all -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-track-forward all -- *   *      0.0.0.0/0     0.0.0.0/0

Chain OUTPUT (policy ACCEPT 842 packets, 48034 bytes)
pkts bytes target prot opt in  out  source           destination
  18W 4057M ufw-before-output all -- *   *      0.0.0.0/0     0.0.0.0/0
  18W 4057M ufw-before-logging-output all -- *   *      0.0.0.0/0     0.0.0.0/0
  985K 341M ufw-after-output all -- *   *      0.0.0.0/0     0.0.0.0/0
  985K 341M ufw-after-logging-output all -- *   *      0.0.0.0/0     0.0.0.0/0
  985K 341M ufw-reject-output all -- *   *      0.0.0.0/0     0.0.0.0/0
  985K 341M ufw-track-output all -- *   *      0.0.0.0/0     0.0.0.0/0

Chain ufw-after-forward (1 references)
pkts bytes target prot opt in  out  source           destination
Chain ufw-after-input (1 references)
pkts bytes target prot opt in  out  source           destination
  844 8050K ufw-skip-to-policy-input udp -- *   *      0.0.0.0/0     0.0.0.0/0
 155 37416 ufw-skip-to-policy-input udp -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-before-forward all -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-skip-to-policy-input tcp -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-skip-to-policy-input udp -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-skip-to-policy-input udp -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ufw-skip-to-policy-input udp -- *   *      0.0.0.0/0     0.0.0.0/0
  1   43 ufw-skip-to-policy-input all -- *   *      0.0.0.0/0     0.0.0.0/0
                                         ADDRTYPE match dst-type BROADCAST

Chain ufw-after-logging-forward (1 references)
pkts bytes target prot opt in  out  source           destination
  0   0 LOG    all -- *   *      0.0.0.0/0     0.0.0.0/0
                                         limit: avg 3/min burst 10 LOG Flags 0 level 4 prefix "[UFW BLOCK]"

Chain ufw-after-logging-input (1 references)
pkts bytes target prot opt in  out  source           destination
  26 27773 LOG   all -- *   *      0.0.0.0/0     0.0.0.0/0
                                         limit: avg 3/min burst 10 LOG Flags 0 level 4 prefix "[UFW BLOCK]"

Chain ufw-after-logging-output (1 references)
pkts bytes target prot opt in  out  source           destination

Chain ufw-after-output (1 references)
pkts bytes target prot opt in  out  source           destination

Chain ufw-before-forward (1 references)
pkts bytes target prot opt in  out  source           destination

```

```

Chain ufw-skip-to-policy-forward (0 references)
pkts bytes target prot opt in  out  source           destination
  0   0 DROP   all -- *   *      0.0.0.0/0     0.0.0.0/0

Chain ufw-skip-to-policy-input (7 references)
pkts bytes target prot opt in  out  source           destination
 1364 239K DROP   all -- *   *      0.0.0.0/0     0.0.0.0/0

Chain ufw-skip-to-policy-output (0 references)
pkts bytes target prot opt in  out  source           destination
  0   0 ACCEPT  all -- *   *      0.0.0.0/0     0.0.0.0/0

Chain ufw-track-forward (1 references)
pkts bytes target prot opt in  out  source           destination
Chain ufw-track-input (1 references)
pkts bytes target prot opt in  out  source           destination
Chain ufw-track-output (1 references)
pkts bytes target prot opt in  out  source           destination
 208K 12M ACCEPT  tcp -- *   *      0.0.0.0/0     0.0.0.0/0
 740K 32M ACCEPT  udp -- *   *      0.0.0.0/0     0.0.0.0/0
                                         ctstate NEW
Chain ufw-user-forward (1 references)
pkts bytes target prot opt in  out  source           destination
Chain ufw-user-input (1 references)
pkts bytes target prot opt in  out  source           destination
  0   0 ACCEPT  tcp -- *   *      0.0.0.0/0     0.0.0.0/0
  0   0 ACCEPT  tcp -- *   *      0.0.0.0/0     0.0.0.0/0
                                         tcp dpt:80 /* 'dapp_Apache' */
  0   0 ACCEPT  tcp -- *   *      0.0.0.0/0     0.0.0.0/0
                                         tcp dpt:22
Chain ufw-user-limit (0 references)
pkts bytes target prot opt in  out  source           destination
  0   0 LOG    all -- *   *      0.0.0.0/0     0.0.0.0/0
                                         limit: avg 3/min burst 5 LOG Flags 0 level 4 prefix "[UFW LIMIT BLOCK]"
  0   0 REJECT all -- *   *      0.0.0.0/0     0.0.0.0/0
                                         reject-with icmp-port-unreachable
Chain ufw-user-limit-accept (0 references)
pkts bytes target prot opt in  out  source           destination
  0   0 ACCEPT  all -- *   *      0.0.0.0/0     0.0.0.0/0

Chain ufw-user-logging-forward (0 references)
pkts bytes target prot opt in  out  source           destination
Chain ufw-user-logging-input (0 references)
pkts bytes target prot opt in  out  source           destination
Chain ufw-user-logging-output (0 references)
pkts bytes target prot opt in  out  source           destination
Chain ufw-user-output (1 references)
pkts bytes target prot opt in  out  source           destination
acer@acer-Aspire-A315-53:~$
```

## 9. In the Linus report was displayed potential warning :

\* Check what deleted files are still in use and why. [LOGG-2190]

<https://cisofy.com/lynis/controls/LOGG-2190/>

I have checked that deleted files by the command

```
sudo find /proc/*/fd -ls | grep '(deleted)'
```

| Activities | Terminal                | 11 Feb 14:15   |
|------------|-------------------------|--|
|            |                         | acer@acer-Aspire-A315-53: ~  |
|            |                         |  |
| 6729754    | 0 lrwx----- 1 acer acer | 64 Feb 11 10:43 /proc/934463/fd/61 -> /dev/shm/.com.google.Chrome_SDnLTl_ (deleted)                      |
| 6729764    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934473/fd/6 -> /opt/google/chrome/icudtl.dat_ (deleted)                            |
| 6729765    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934473/fd/6 -> /opt/google/chrome/v8_context_snapshot.bin_ (deleted)               |
| 6729766    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934473/fd/7 -> /opt/google/chrome/chrome_100_percent.pak_ (deleted)                |
| 6729767    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934473/fd/8 -> /opt/google/chrome/chrome_200_percent.pak_ (deleted)                |
| 6729768    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934473/fd/9 -> /opt/google/chrome/locales/en-GB.pak_ (deleted)                     |
| 6729769    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934473/fd/10 -> /opt/google/chrome/resources.pak_ (deleted)                        |
| 6729770    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934473/fd/11 -> /opt/google/chrome/v8_context_snapshot.bin_ (deleted)              |
| 6729792    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934541/fd/6 -> /opt/google/chrome/icudtl.dat_ (deleted)                            |
| 6729795    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934541/fd/7 -> /opt/google/chrome/chrome_100_percent.pak_ (deleted)                |
| 6729796    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934541/fd/8 -> /opt/google/chrome/chrome_200_percent.pak_ (deleted)                |
| 6729797    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934541/fd/9 -> /opt/google/chrome/locales/en-GB.pak_ (deleted)                     |
| 6729798    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/934541/fd/10 -> /opt/google/chrome/resources.pak_ (deleted)                        |
| 6729800    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/935667/fd/6 -> /opt/google/chrome/v8_context_snapshot.bin_ (deleted)               |
| 6729805    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/935667/fd/7 -> /opt/google/chrome/icudtl.dat_ (deleted)                            |
| 6729852    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/935667/fd/7 -> /opt/google/chrome/chrome_100_percent.pak_ (deleted)                |
| 6729853    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/935667/fd/8 -> /opt/google/chrome/chrome_200_percent.pak_ (deleted)                |
| 6729854    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/935667/fd/9 -> /opt/google/chrome/locales/en-GB.pak_ (deleted)                     |
| 6729855    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/935667/fd/10 -> /opt/google/chrome/resources.pak_ (deleted)                        |
| 6729861    | 0 lr-x----- 1 acer acer | 64 Feb 11 10:43 /proc/935667/fd/11 -> /opt/google/chrome/v8_context_snapshot.bin_ (deleted)              |
| 6598855    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:49 /proc/935667/fd/12 -> /dev/shm/.com.google.Chrome_wNzqB1_ (deleted)                      |
| 6599414    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935667/fd/37 -> /dev/shm/.com.google.Chrome_67N11F_ (deleted)                      |
| 6599415    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935667/fd/38 -> /dev/shm/.com.google.Chrome_vC4vEf_ (deleted)                      |
| 7245071    | 0 lrwx----- 1 acer acer | 64 Feb 11 13:19 /proc/935667/fd/44 -> /dev/shm/.com.google.Chrome_A6TuBz1_ (deleted)                     |
| 6599416    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935667/fd/44 -> /dev/shm/.com.google.Chrome_ngwRtI_ (deleted)                      |
| 6599506    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:49 /proc/935667/fd/42 -> /dev/shm/.com.google.Chrome_BWfxE4_ (deleted)                      |
| 6599507    | 0 lrwx----- 1 acer acer | 64 Feb 11 08:59 /proc/935667/fd/43 -> /dev/shm/.com.google.Chrome_16529D_ (deleted)                      |
| 6598287    | 0 lr-x----- 1 acer acer | 64 Feb 11 08:59 /proc/935820/fd/6 -> /opt/google/chrome/v8_context_snapshot.bin_ (deleted)               |
| 6598288    | 0 lr-x----- 1 acer acer | 64 Feb 11 08:59 /proc/935820/fd/7 -> /opt/google/chrome/chrome_100_percent.pak_ (deleted)                |
| 6598289    | 0 lr-x----- 1 acer acer | 64 Feb 11 08:59 /proc/935820/fd/8 -> /opt/google/chrome/chrome_200_percent.pak_ (deleted)                |
| 6598210    | 0 lr-x----- 1 acer acer | 64 Feb 11 08:59 /proc/935820/fd/9 -> /opt/google/chrome/locales/en-GB.pak_ (deleted)                     |
| 6598211    | 0 lr-x----- 1 acer acer | 64 Feb 11 08:59 /proc/935820/fd/10 -> /opt/google/chrome/resources.pak_ (deleted)                        |
| 6598217    | 0 lr-x----- 1 acer acer | 64 Feb 11 08:59 /proc/935820/fd/18 -> /opt/google/chrome/v8_context_snapshot.bin_ (deleted)              |
| 6599487    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/23 -> /tmp/.com.google.Chrome_GfUEBV_ (deleted)                          |
| 6599488    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/33 -> /dev/shm/.com.google.Chrome_32Zx33_ (deleted)                      |
| 6599489    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/37 -> /dev/shm/.com.google.Chrome_bkUkEW_ (deleted)                      |
| 6599490    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/39 -> /dev/shm/.com.google.Chrome_lDb3DE_ (deleted)                      |
| 6599494    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/44 -> /dev/shm/.com.google.Chrome_oVRRAx_ (deleted)                      |
| 6599495    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/44 -> /dev/shm/.com.google.Chrome_X8CN5J_ (deleted)                      |
| 6599496    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/42 -> /dev/shm/.com.google.Chrome_wNsJN_ (deleted)                       |
| 6599497    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/46 -> /dev/shm/.com.google.Chrome_pQvV_ (deleted)                        |
| 6599499    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/46 -> /dev/shm/.com.google.Chrome_IwPjD_ (deleted)                       |
| 6599493    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/47 -> /dev/shm/.com.google.Chrome_HWv3D_ (deleted)                       |
| 7314746    | 0 lrwx----- 1 acer acer | 64 Feb 11 14:13 /proc/935820/fd/49 -> /dev/shm/.com.google.Chrome_beUKew_ (deleted)                      |
| 6599498    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/54 -> /dev/shm/.com.google.Chrome_8ldBgB_ (deleted)                      |
| 6599502    | 0 lr-x----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/6 -> /dev/shm/.com.google.Chrome_vvWEgA_ (deleted)                       |
| 6599509    | 0 lr-x----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/98 -> /dev/shm/.com.google.Chrome_INXzB1_ (deleted)                      |
| 6599510    | 0 lrwx----- 1 acer acer | 64 Feb 11 09:19 /proc/935820/fd/100 -> /dev/shm/.com.google.Chrome_142d87e4.log_ (deleted)               |
| 6634654    | 0 lr-x----- 1 acer acer | 64 Feb 11 09:22 /proc/936806/fd/14 -> /home/acer/.local/share/gvfs-metadata/home_ (deleted)              |
| 6634655    | 0 lr-x----- 1 acer acer | 64 Feb 11 09:22 /proc/936806/fd/15 -> /home/acer/.local/share/gvfs-metadata/home-142d87e4.log_ (deleted) |
| 5189308    | 0 lrwx----- 1 acer acer | 64 Feb 11 16:08 /proc/9886/fd/8 -> /memfd/wayland-cursor_ (deleted)                                      |

10. In the Linus report was displayed potential warning:

\* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

<https://cisofy.com/lynis/controls/BANN-7126/>

\* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

<https://cisofy.com/lynis/controls/BANN-7130/>

One of the easiest way to protect and secure SSH logins by displaying warming message to UN-authorized users or display welcome or informational messages to authorized users.

A legal banner contains some security warning information or general information, that alerts the user. It can be used for security, legal info, company policy, etc.

One way to display messages is using issue.net file. issue.net : Display a banner message before the password login prompt.

To display Welcome or Warning message for SSH users before login. I use issue.net file to display a banner massages. I opened the following file with the editor.

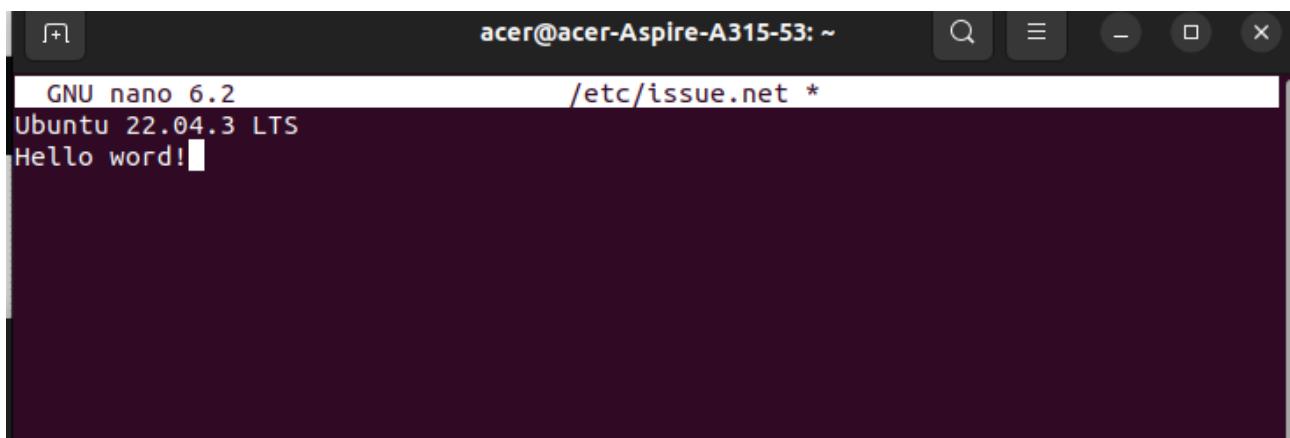
vi /etc/issue.net

Add the banner message “Hello word” and save the file. Next I opened the master ssh configuration file and enable banners.

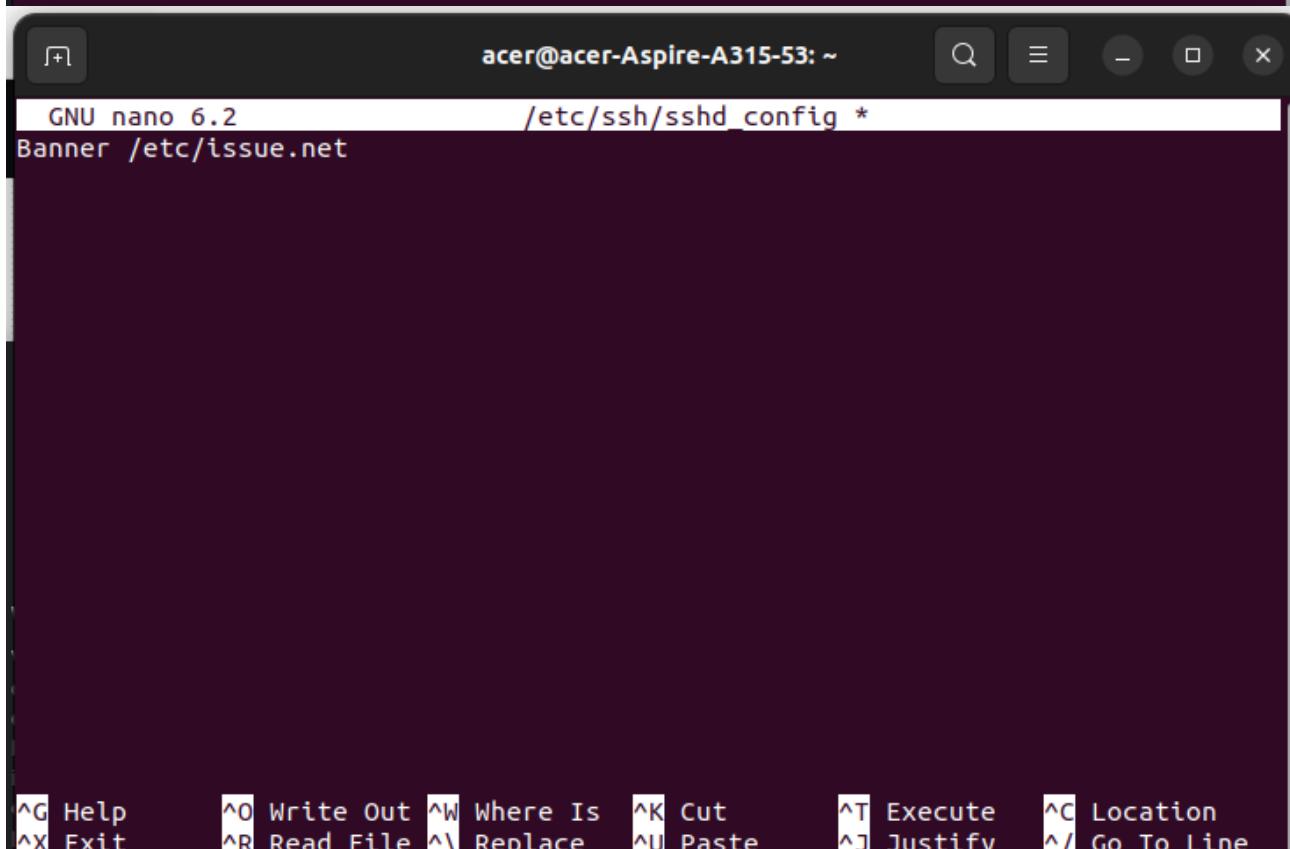
vi /etc/ssh/sshd\_config

After that I find the word “Banner” and uncomment out the line and save the file.

Banner /etc/issue.net



The screenshot shows a terminal window titled "acer@acer-Aspire-A315-53: ~". The command "nano /etc/issue.net" was run. The file contains the text "Hello word!". The terminal has a dark theme with light-colored text.



The screenshot shows a terminal window titled "acer@acer-Aspire-A315-53: ~". The command "nano /etc/ssh/sshd\_config" was run. The file contains the line "Banner /etc/issue.net". The terminal has a dark theme with light-colored text.

of the commands and resources currently being used in the system. The “acct” utility runs in the system background; therefore, the system’s performance is unaffected.

```
acer@acer-Aspire-A315-53:~$ sudo apt-get install acct
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed
  acct
0 to upgrade, 1 to newly install, 0 to remove and 2 not to upgrade.
Need to get 88.4 kB of archives.
After this operation, 312 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 acct amd64 6.6.4-4build2 [88.4 kB]
Fetched 88.4 kB in 2s (43.3 kB/s)
Selecting previously unselected package acct.
(Reading database ... 219226 files and directories currently installed.)
Preparing to unpack .../acct_6.6.4-4build2_amd64.deb ...
Unpacking acct (6.6.4-4build2) ...
Setting up acct (6.6.4-4build2) ...
update-rc.d: warning: start and stop actions are no longer supported; falling back to defaults
update-rc.d: warning: stop runlevel arguments (1) do not match acct Default-Stop values (0 1 6)
Created symlink /etc/systemd/system/multi-user.target.wants/acct.service → /lib/systemd/system/acct.service.
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53:~$
```

The error-free output declares that “**acct**” is successfully installed on my system. I enabled the process accounting by utilizing the below-given command:

**sudo /usr/sbin/accton on**

I executed the “ac” command to get the connection time statistics of the user.

The “-d” option is added in the “ac” command to view the daily log in hour-based time.

To know about connect time of all system users, utilize the “-p” option in “ac” command.

The “sa” command summarizes the contents of the file containing the raw accounting data.

```

acer@acer-Aspire-A315-53:~$ ac
      total      526.68
acer@acer-Aspire-A315-53:~$ ac -d
Jan 20  total      7.67
Jan 21  total     24.00
Jan 22  total     23.96
Today   total    471.07
acer@acer-Aspire-A315-53:~$ ac -p
      acer          526.71
acer@acer-Aspire-A315-53:~$ sudo sa
 273    164.87re    2.01cp    0avio  99324877k  AuctionV8Helper*
   39     1.71re    0.90cp    0avio 293928960k  ThreadPoolForeg*
   59     4.23re    0.81cp    0avio 197879843k
   3     0.08re    0.08cp    0avio  11971k   apt-check
   27    11.63re    0.07cp    0avio 10992689k  ***other*
   4     5.94re    0.06cp    0avio 296550400k  Chrome_ChildIOT*
   13    5.64re    0.05cp    0avio 163557691k  chrome*
   4     0.03re    0.02cp    0avio  2824k   fuser
   6    134.30re    0.02cp    0avio      0k   kworker/dying*
   8     0.77re    0.01cp    0avio 46002176k  HangWatcher*
   2     0.28re    0.00cp    0avio  3557k   sudo
   17    0.04re    0.00cp    0avio  3736k   dpkg
   22    0.00re    0.00cp    0avio  912k   gzip
   5     0.00re    0.00cp    0avio  5216k   apt-config
   25    0.04re    0.00cp    0avio  723k   sh
   22    0.00re    0.00cp    0avio 2903k   install-info
   3     0.00re    0.00cp    0avio  463k   accton
   3     0.00re    0.00cp    0avio 2812k   rm
   3     0.00re    0.00cp    0avio  698k   ac
   2     0.18re    0.00cp    0avio 4323k   sudo*
   2     0.00re    0.00cp    0avio  3060k   find
   2     0.00re    0.00cp    0avio 2808k   test
   2     0.00re    0.00cp    0avio  661k   ischroot

```

12. In the Linus report was displayed potential warning :

\* Enable sysstat to collect accounting (no results) [ACCT-9626]

<https://cisofy.com/lynis/controls/ACCT-9626/>

The package is available from the default repositories, so I used

**sudo apt install sysstat -y**

By default Sysstat monitoring is disabled. To enable the sysstat monitoring, I edited the configuration file in a text editor:

```

Activities Terminal 11 Feb 15:20
acer@acer-Aspire-A315-53: ~ /etc/default/sysstat

# Default settings for /etc/init.d/sysstat, /etc/cron.d/sysstat
# and /etc/cron.daily/sysstat files
#
# Should sdac collect system activity informations? Valid values
# are "true" and "false". Please do not put other values, they
# will be overwritten by debconf!
ENABLED="true"

```

After enabling the monitoring, enable the sysstat service and start it by executing:

```
sudo systemctl enable sysstat
sudo systemctl start sysstat
```

```

Activities Terminal 11 Feb 15:27
acer@acer-Aspire-A315-53: ~ /etc/default/sysstat

Error: There are no enabled repositories in "/etc/yum.repos.d", "/etc/yum/repos.d", "/etc/distro.repos.d".
acer@acer-Aspire-A315-53: $ sudo apt install sysstat -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  isag
The following NEW packages will be installed:
  sysstat
0 upgraded, 0 newly installed, 0 to remove and 2 not to upgrade.
Need to get 487 kB of archives.
After this operation, 1,507 kB of additional disk space will be used.
Get: http://gb.archive.ubuntu.com/ubuntu jammy-updates/main amd64 sysstat amd64 12.5.2-2ubuntu0.2 [487 kB]
Fetched 487 kB in 11s (42.9 kB/s)
Preconfiguring packages...
Selecting previously unselected package sysstat.
(Reading database ... 22000 packages available, reading the index...
Preparing to unpack .../sysstat_12.5.2-2ubuntu0.2_amd64.deb ...
Unpacking sysstat (12.5.2-2ubuntu0.2) ...
Setting up sysstat (12.5.2-2ubuntu0.2) ...

Creating config file /etc/default/sysstat with new version
update-alternatives: using /usr/bin/sar.sysstat to provide /usr/bin/sar (sar) in auto mode
Created symlink /etc/systemd/system/sysstat.service.wants/sysstat-collect.timer → /lib/systemd/system/sysstat-collect.timer.
Created symlink /etc/systemd/system/sysstat.service.wants/sysstat-summary.timer → /lib/systemd/system/sysstat-summary.timer.
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53: $ sudo nano /etc/default/sysstat
acer@acer-Aspire-A315-53: $ rc
acer@acer-Aspire-A315-53: $ sudo nano /etc/default/sysstat
acer@acer-Aspire-A315-53: $ sudo systemctl enable sysstat
Synchronizing state of sysstat.service with sysv-installable script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable sysstat
Created symlink /etc/systemd/system/multi-user.target.wants/sysstat.service → /lib/systemd/system/sysstat.service.
Created symlink /etc/systemd/system/sysstat.service.wants/sysstat-collect.timer → /lib/systemd/system/sysstat-collect.timer.
Created symlink /etc/systemd/system/sysstat.service.wants/sysstat-summary.timer → /lib/systemd/system/sysstat-summary.timer.
acer@acer-Aspire-A315-53: $ sar -u
Cannot open '/var/log/sysstat/sar1': No such file or directory
Please check if the daemons are enabled
acer@acer-Aspire-A315-53: $ sudo systemctl start sysstat
acer@acer-Aspire-A315-53: $ sar -u
Linux 6.5.0-14-generic (acer-Aspire-A315-53) 11/02/24      _x86_64_      (4 CPU)

15:25:56   LINUX RESTART      (4 CPU)
acer@acer-Aspire-A315-53: $ sar -u 1 5
Linux 6.5.0-14-generic (acer-Aspire-A315-53) 11/02/24      _x86_64_      (4 CPU)

15:26:24    CPU   kUser   kNice   kSystem   kIowait   kSteal   kIdle
15:26:25    all    6.41    0.00    3.33    0.00    0.00    90.26
15:26:26    all   17.47    0.00   10.13    0.00    0.00    72.41
15:26:27    all   14.55    0.00    8.05    0.00    0.00    77.40
15:26:28    all   13.33    0.00    4.62    0.00    0.00    82.05
15:26:29    all   19.05    0.00    7.27    0.00    0.00    73.68
Average:    all   14.10    0.00    6.69    0.00    0.00    79.12
acer@acer-Aspire-A315-53: $

```

I Use -u with the sar command to view real-time cpu statics

```
sar -u
```

I also view the real-time CPU uses by specifying the time interval and the number of times to show data. For example, to view real-time CPU uses for 5 times with a difference of 1 second.

```
sar -u 1 5
```

I view the CPU utilization data in more depth. Nowadays most the CPUs are multi-core. To view the utilization details of each core individually use the -P ALL command.

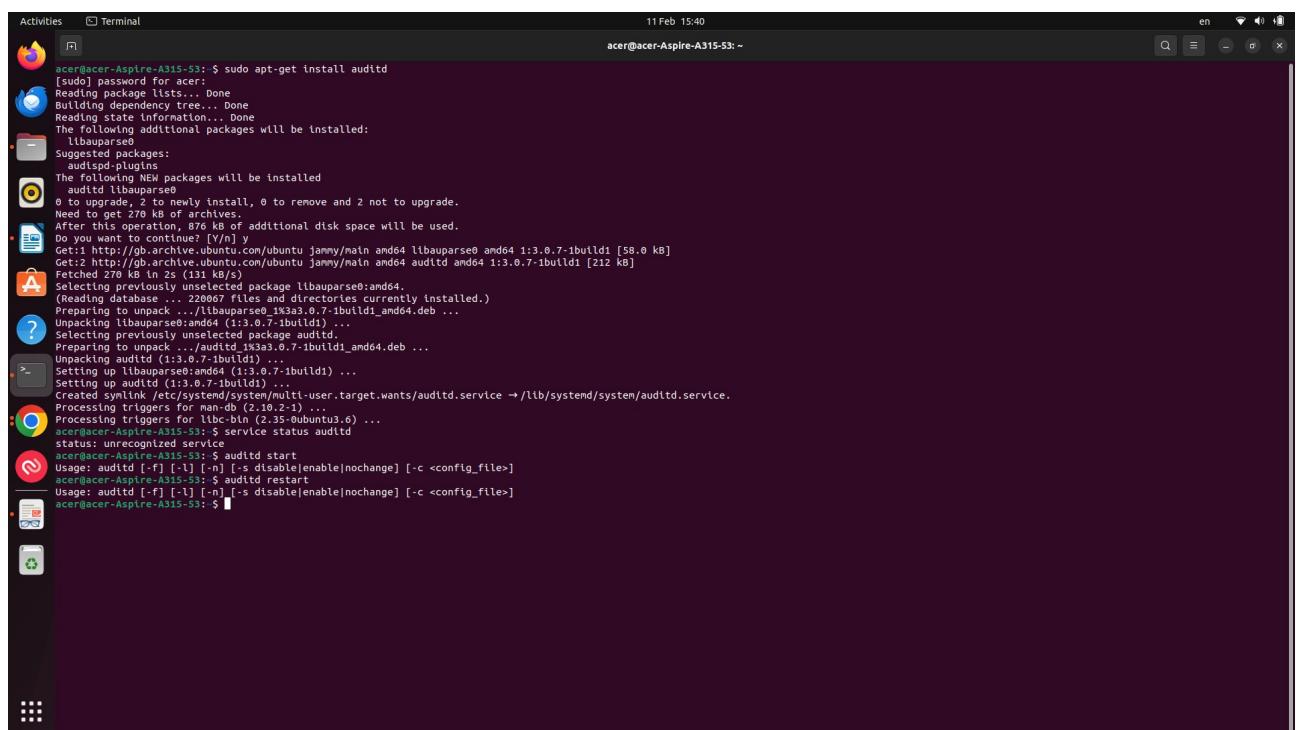
```
sar -P ALL 1 3
```

View Device Usage – I use the iostat command to find disk statics. It shows the current data transfer per second, the total number of blocks read and written to disk and an average block per second.

```
iostat -d 1 5
```

Sysstat also stores monitoring data in files. I see the historical data with the sar command.

```
acer@acer-Aspire-A315-53:~$ sar -u -f /var/log/sysstat/sa28
Cannot open /var/log/sysstat/sa28: No such file or directory
acer@acer-Aspire-A315-53:~$ sar -u -f /var/log/sysstat
Linux 6.5.0-14-generic (acer-Aspire-A315-53)   11/02/24      _x86_64_          (4 CPU)
15:25:56    LINUX RESTART      (4 CPU)
```



A screenshot of a Linux desktop environment. At the top, there's a dark header bar with icons for battery, signal, and volume. Below it is a dock with various application icons. A terminal window is open in the center, showing a command-line session. The session starts with a user trying to open a non-existent file 'sa28' in the sysstat directory. Then, the user runs 'sar -u -f /var/log/sysstat' to check historical CPU usage data. The terminal shows the system configuration (Linux 6.5.0-14-generic), the date (11/02/24), and the processor type (\_x86\_64\_ (4 CPU)). The user then performs a 'LINUX RESTART'. The terminal window has a dark background and light-colored text. The overall interface is clean and modern.

```
Activities Terminal acer@acer-Aspire-A315-53:~$ sudo apt-get install audited
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  audited-plugins
Suggested packages:
  libaudit-dev
The following NEW packages will be installed:
  audited libaudit0
0 to upgrade, 2 to newly install, 0 to remove and 2 not to upgrade.
Need to get 270 kB of additional disk space.
After this operation, 876 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 libaudit0 amd64 1:3.0.7-1build1 [58.0 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 audited amd64 1:3.0.7-1build1 [212 kB]
Fetched 270 kB in 2s (131 kB/s)
Selecting previously unselected package libaudit0:amd64.
(Reading database ... 22999 files and directories currently installed.)
Preparing to unpack .../libaudit0_1:3.0.7-1build1_amd64.deb ...
Unpacking libaudit0:amd64 (1:3.0.7-1build1) ...
Selecting previously unselected package audited.
Preparing to unpack .../audited_1:3.0.7-1build1_amd64.deb ...
Unpacking audited (1:3.0.7-1build1) ...
Setting up libaudit0:amd64 (1:3.0.7-1build1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/audited.service → /lib/systemd/system/audited.service.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.0) ...
acer@acer-Aspire-A315-53:~$ service status audited
status: unrecognized service
acer@acer-Aspire-A315-53:~$ audited start
Usage: audited [-f] [-l] [-n] [-s disable|enable|nochange] [-c <config_file>]
               [-r] [-t] [-v] [-z] audited restart
Usage: audited [-f] [-l] [-n] [-s disable|enable|nochange] [-c <config_file>]
acer@acer-Aspire-A315-53:~$
```

13. In the Linus report was displayed potential warning :

\* Enable audited to collect audit information [ACCT-9628]

<https://cisofy.com/lynis/controls/ACCT-9628/>

```

Activities Terminal 11 Feb 15:40 acer@acer-Aspire-A315-53:~ 
acer@acer-Aspire-A315-53:~ $ sudo apt-get install auditd
[sudo] password for acer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
 liblbauparse0
Suggested packages:
 audispd-plugins
The following NEW packages will be installed:
 auditd
0 to upgrade, 2 to newly install, 0 to remove and 2 not to upgrade.
Need to get 270 kB of archives.
After this operation, 876 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 liblbauparse0 amd64 1:3.0.7-1build1 [58.0 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 auditd amd64 1:3.0.7-1build1 [212 kB]
Fetched 270 kB in 2s (111 kB/s)
Selecting previously unselected package liblbauparse0:amd64.
(Reading database ... 220067 files and directories currently installed.)
Preparing to unpack .../liblbauparse0:amd64_1:3.0.7-1build1_amd64.deb ...
Unpacking liblbauparse0:amd64 (1:3.0.7-1build1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1:3.0.7-1build1_amd64.deb ...
Unpacking auditd (1:3.0.7-1build1) ...
Setting up liblbauparse0:amd64 (1:3.0.7-1build1) ...
Setting up auditd (1:3.0.7-1build1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service → /lib/systemd/system/auditd.service.
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
acer@acer-Aspire-A315-53:~ $ service status auditd
status: started
acer@acer-Aspire-A315-53:~ $ auditd start
Usage: auditd [-f] [-l] [-n] [-s disable|enable|nochange] [-c <config_file>]
acer@acer-Aspire-A315-53:~ $ auditd restart
Usage: auditd [-f] [-l] [-n] [-s disable|enable|nochange] [-c <config_file>]
acer@acer-Aspire-A315-53:~ $

```

#### 14. In the Linus report was displayed potential warning :

\* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]

<https://cisofy.com/lynis/controls/FINT-4350/>

To install AIDE on your system, I used the following command:

`sudo apt-get install aide -y`

```

Activities Terminal 11 Feb 16:00 acer@acer-Aspire-A315-53:~ 
acer@acer-Aspire-A315-53:~ $ sudo apt-get install aide -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
 aide-common
Suggested packages:
 figlet
The following NEW packages will be installed:
 aide aide-common
0 to upgrade, 2 to newly install, 0 to remove and 2 not to upgrade.
Need to get 164 kB of archives.
After this operation, 655 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 aide amd64 0.17.4-1 [91.5 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/main amd64 aide-common all 0.17.4-1 [72.1 kB]
Fetched 164 kB in 2s (66.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package aide.
(Reading database ... 220067 files and directories currently installed.)
Preparing to unpack .../aide_0.17.4-1_amd64.deb ...
Unpacking aide (0.17.4-1) ...
Selecting previously unselected package aide-common.
Preparing to unpack .../aide-common_0.17.4-1_all.deb ...
Unpacking aide-common (0.17.4-1) ...
Setting up aide (0.17.4-1) ...
Setting up aide-common (0.17.4-1) ...
Creating config file /etc/cron.daily/aide with new version
Creating config file /etc/aide/aide.conf with new version
Creating config file /etc/aide/aide.settings.d/31_aide_apt_settings with new version
Creating config file /etc/aide/aide.settings.d/31_aide_trac_settings with new version
Creating config file /etc/aide/aide.settings.d/31_aide_torrius_settings with new version
Creating config file /etc/aide/aide.settings.d/31_aide_svn-server_settings with new version
Creating config file /etc/aide/aide.settings.d/10_aide_sourceslist with new version
Creating config file /etc/aide/aide.conf.d/70_aide_var with new version
Creating config file /etc/aide/aide.conf.d/31_aide_logrotate with new version
Creating config file /etc/aide/aide.conf.d/31_aide_chrony with new version
Creating config file /etc/aide/aide.conf.d/31_aide_xdm with new version
Creating config file /etc/aide/aide.conf.d/31_aide_openvpn-server with new version
Creating config file /etc/aide/aide.conf.d/31_aide_amanda-client with new version
Creating config file /etc/aide/aide.conf.d/31_aide_mailman with new version
Creating config file /etc/aide/aide.conf.d/31_aide_iclinaq2 with new version

```

```

Activities Terminal 11 Feb 16:02 acer@acer-Aspire-A315-53: ~
Creating config file /etc/aide/aide.conf.d/31_aide_opie-server with new version
Creating config file /etc/aide/aide.conf.d/31_aide_botinc-client with new version
Creating config file /etc/aide/aide.conf.d/31_aide_xinetd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_debspawn with new version
Creating config file /etc/aide/aide.conf.d/31_aide_sudo with new version
Creating config file /etc/default/aide with new version
Processing triggers for man-db (2.10.2-1) ...
acer@acer-Aspire-A315-53: ~ aide -v
Aide 0.17.4
Compiled with the following options:
WITH_MMAP
WITH_PCRE
WITH_POSIX_ACL
WITH_SELINUX
WITH_XATTR
WITH_CAPABILITIES
WITH_OPENATRCS
WITH_ZLIB
WITH_MHASH
WITH_AUDIT
Default config values:
config_file: <none>
database_in: <none>
database_out: <none>
Available hashsum groups:
md5: yes
sha1: yes
sha256: yes
sha512: yes
rnd100: yes
tiger: yes
tigerv: yes
crc32: yes
crc32b: yes
haval: yes
whirlpool: yes
gost: yes
stribog256: no
stribog512: no
Default compound groups:
R: l+p+u+g+i+n+acl+selinux+xattr+ftype+e?fsattr+caps
L: l+p+u+g+i+n+acl+selinux+xattr+ftype+e?fsattr+caps
>: l+p+u+g+i+n+acl+S+selinux+xattr+ftype+e?fsattr+caps
H: md5+sha1+md100+tiger+crc32+haval+gost+crc32b+sha256+sha512+whirlpool
X: acl+selinux+xattr+e?fsattr+caps
acer@acer-Aspire-A315-53: ~

```

## 15. In the Linus report was displayed potential warning :

\* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]

- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)

<https://cisofy.com/lynis/controls/KRNL-6000/>

First get a backup of the default settings just in case:

sudo sysctl -a > /tmp/sysctl-defaults.conf

Then create the config file:

```

GNU nano 6.2          /etc/sysctl.d/80-lynis.conf *
kernel.kptr_restrict = 2
kernel.sysrq = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.log_martians = 1
#net.ipv4.tcp_timestamps = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste    ^J Justify  ^/ Go To Line

```

And then applied the settings:

```
acer@acer-Aspire-A315-53:~$ sudo nano /etc/sysctl.d/80-lyntis.conf
acer@acer-Aspire-A315-53:~$ sudo sysctl -p
kernel.printk = 4 4 1 7
fs.suid_dumpable = 0
* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
* Applying /etc/sysctl.d/10-kernel-hardening.conf ...
kernel.core_uses_pid = 1
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
kernel.sysrq = 176
* Applying /etc/sysctl.d/10-network-security.conf ...
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.all.rp_filter = 2
* Applying /etc/sysctl.d/10-prtrace.conf ...
kernel.prctl_seccomp = 0
* Applying /etc/sysctl.d/10-zero-page.conf ...
vm.mmap_min_addr = 65536
* Applying /usr/lib/sysctl.d/30-tracker.conf ...
fs.inotify.max_user_watches = 65536
* Applying /usr/lib/sysctl.d/50-bubblewrap.conf ...
kernel.unprivileged_userns_clone = 1
* Applying /usr/lib/sysctl.d/50-default.conf ...
kernel.core_uses_pid = 1
kernel.core_dump_in_coredump = 1
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.default.accept_source_route = 0
sysctl: setting key "net.ipv4.conf.all.accept_source_route": Invalid argument
net.ipv4.conf.default.promote_secondaries = 1
sysctl: setting key "net.ipv4.conf.all.promote_secondaries": Invalid argument
net.ipv4.ip_local_port_range = 32768 65535
net.core.default_qdisc = fq_codel
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
fs.protected_regular = 1
fs.protected_fifos = 1
* Applying /usr/lib/sysctl.d/50-pid-max.conf ...
kernel.pid_max = 4194304
* Applying /etc/sysctl.d/80-lyntis.conf ...
kernel.kptr_restrict = 2
kernel.sysrq = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.local_martians = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.local_martians = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
* Applying /usr/lib/sysctl.d/99-protect-links.conf ...
fs.protected_fifos = 1
fs.protected_hardlinks = 1
fs.protected_regular = 2
fs.protected_symlinks = 1
* Applying /etc/sysctl.d/99-protect-links.conf ...
* Applying /etc/sysctl.conf ...
```

## 5.5 I can analyse the effectiveness of the system by viewing the different log files

Finally, these actions done on the system in the hardening index which currently has been increased to 78:

Hardening a system means optimizing its configuration for secure operations and data protection.

```
https://cisoxy.com/lynis/controls/FILE-7524/
* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
  https://cisoxy.com/lynis/controls/KRNL-6000/
* Harden compilers like restricting access to root user only [HRDN-7222]
  https://cisoxy.com/lynis/controls/HRDN-7222/
Follow-up:
-----
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisoxy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

=====
Lynis security scan details:
Hardening index : 78 [#####
Tests performed : 269
Plugins enabled : 0

Components:
- Firewall [V]
- Malware scanner [V]

Scan mode:
Normal [ ] Forensics [ ] Integration [ ] Pentest [V] (running privileged)

Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

=====
Lynis 3.0.9
Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2021, CISofy - https://cisoxy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====
[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
```

The hardening index is not an accurate assessment of how secure a server is, but merely a measure of how well the server is securely configured (or hardened) based on the tests performed by Lynis. And the higher the index, the better. The objective of a Lynis security audit is not just to get a high hardening index, but to fix the warnings and suggestions it generates.

## 5.6 I can recommend improvements to the system for future-proofing

Lynis is a security auditing tool for UNIX-based systems like Linux and macOS. Lynis performs security scans, checks for system hardening, vulnerabilities, and provides suggestions for improvements based on best practices and security standards. It assesses the system's security posture and offers recommendations for improving it.

In the Linus report was displayed potential warning :

- \* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

<https://ciscofy.com/lynis/controls/BOOT-5122/>

<https://linuxconfig.org/set-boot-password-with-grub>

It can be fixed it by GRUB set password boot protection by comand

\$ grub-mkpasswd-pbkdf2

Next, needs some edits to the /etc/grub.d/00\_header GRUB configuration file.

I also recommend improvements concerning the Linus report potential warnings :

- \* Consider hardening system services [BOOT-5264]

- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service

<https://ciscofy.com/lynis/controls/BOOT-5264/>

- \* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]

[https://ciscofy.com/lynis/controls\(FILE-6310\)](https://ciscofy.com/lynis/controls(FILE-6310))

- \* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]

[https://ciscofy.com/lynis/controls\(FILE-6310\)](https://ciscofy.com/lynis/controls(FILE-6310))

- \* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]

[https://ciscofy.com/lynis/controls\(FILE-6310\)](https://ciscofy.com/lynis/controls(FILE-6310))

- \* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]

[https://ciscofy.com/lynis/controls\(USB-1000\)](https://ciscofy.com/lynis/controls(USB-1000))

- \* Determine if protocol 'dccp' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- \* Determine if protocol 'sctp' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- \* Determine if protocol 'rds' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- \* Determine if protocol 'tipc' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- \* Access to CUPS configuration could be more strict. [PRNT-2307]

<https://cisofy.com/lynis/controls/PRNT-2307/>

- \* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]

<https://cisofy.com/lynis/controls/LOGG-2154/>

- \* Determine if automation tools are present for system management [TOOL-5002]

<https://cisofy.com/lynis/controls/TOOL-5002/>

- \* Consider restricting file permissions [FILE-7524]

- Details : See screen output or log file

- Solution : Use chmod to change file permissions

[https://cisofy.com/lynis/controls\(FILE-7524/](https://cisofy.com/lynis/controls(FILE-7524)

## **References:**

1. Amazon Web Services, Inc. (n.d.). *What is LAMP Stack? - LAMP Stack - AWS*. [online] Available at: <https://aws.amazon.com/what-is/lamp-stack/>.
2. DigitalOcean. (n.d.). *Tutorials*. [online] Available at: <https://www.digitalocean.com/community/tutorials/>.
3. Linode Guides & Tutorials. (n.d.). *How to Secure Your LAMP Stack*. [online] Available at: <https://www.linode.com/docs/guides/securing-your-lamp-stack/>.
4. <https://www.facebook.com/RoseHosting> (2018). *How to secure LAMP server*. [online] RoseHosting.com Blog. Available at: <https://www.rosehosting.com/blog/how-to-secure-your-lamp-server/>.
5. Tecmint.com. (2018). *5 Tools to Scan a Linux Server for Malware and Rootkits*. [online] Available at: <https://www.tecmint.com/scan-linux-for-malware-and-rootkits/>.
6. Brereton, R. (2022). *How to Secure a LAMP Server*. [online] Ricmedia. Available at: <https://www.ricmedia.com/tutorials/how-to-secure-a-lamp-server> [Accessed 3 Mar. 2024].





