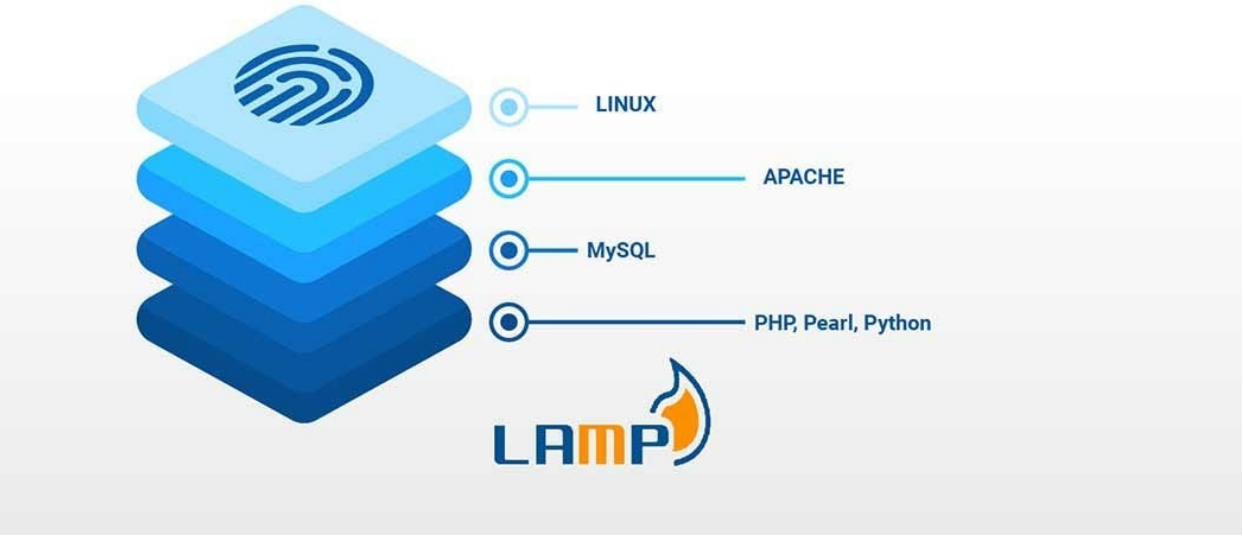
Coursework Project:

“Defending an Online System”

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.

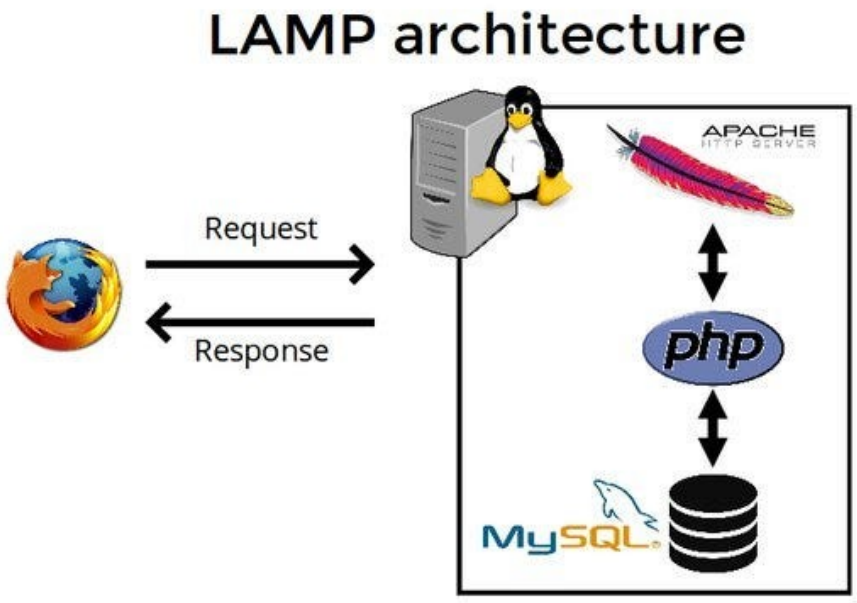
2. Apache is a web server. It processes all requests to site pages and issues appropriate responses. Apache HTTP Server is a free web server software package made available under an open-source license and offers a secure and extendable Web server that's in sync with current HTTP standards. Web servers 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.



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.

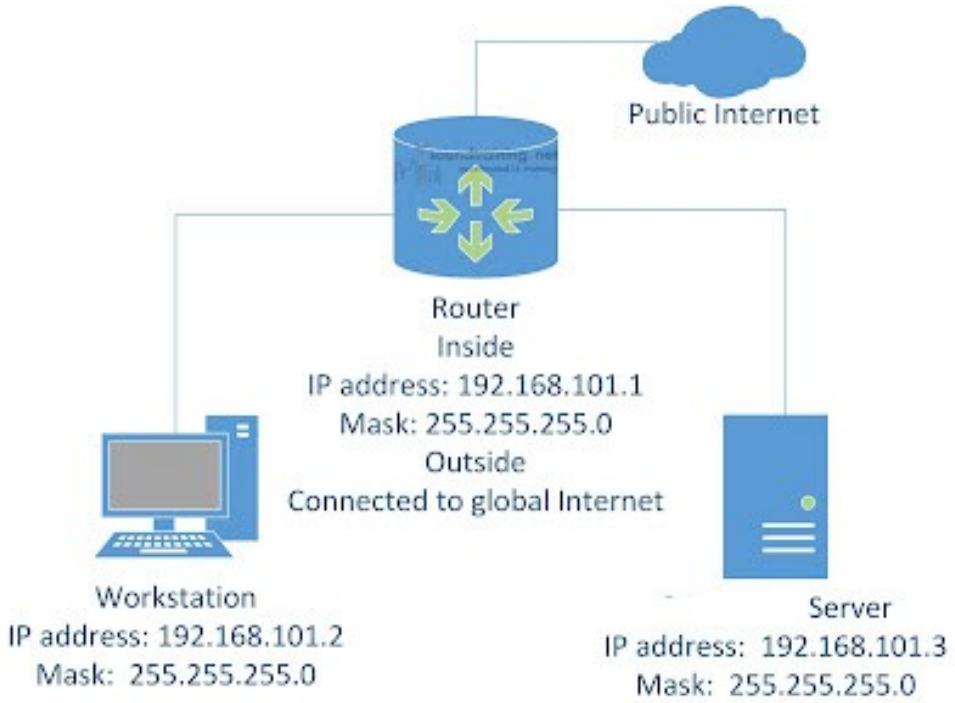
2. Plan to build a Cyber safe website or server

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

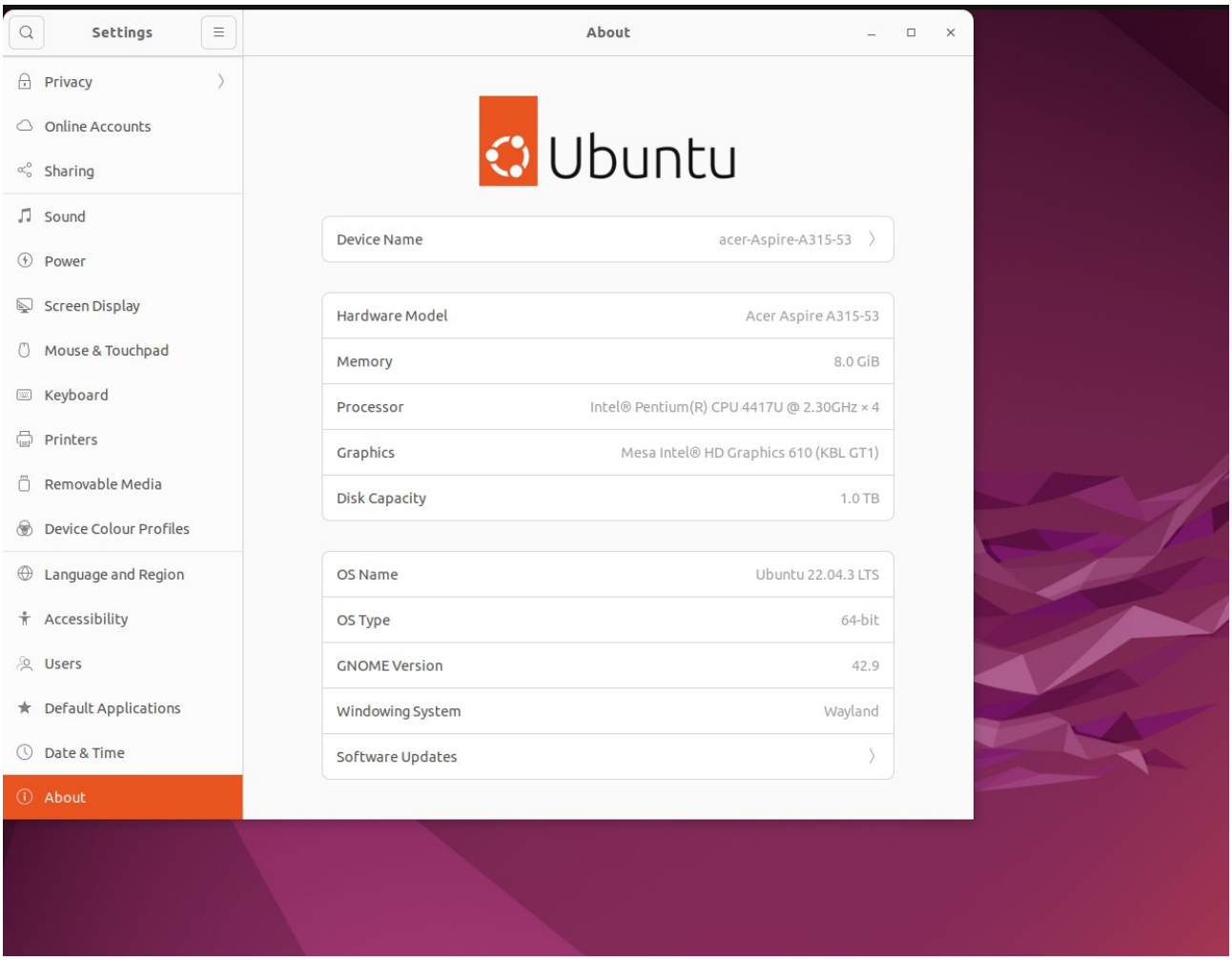
Time plan for building my LAMP server:

Name of Task	Week 1	Week 2	Week 3	Week 4	Week 5
Researching	Week 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.

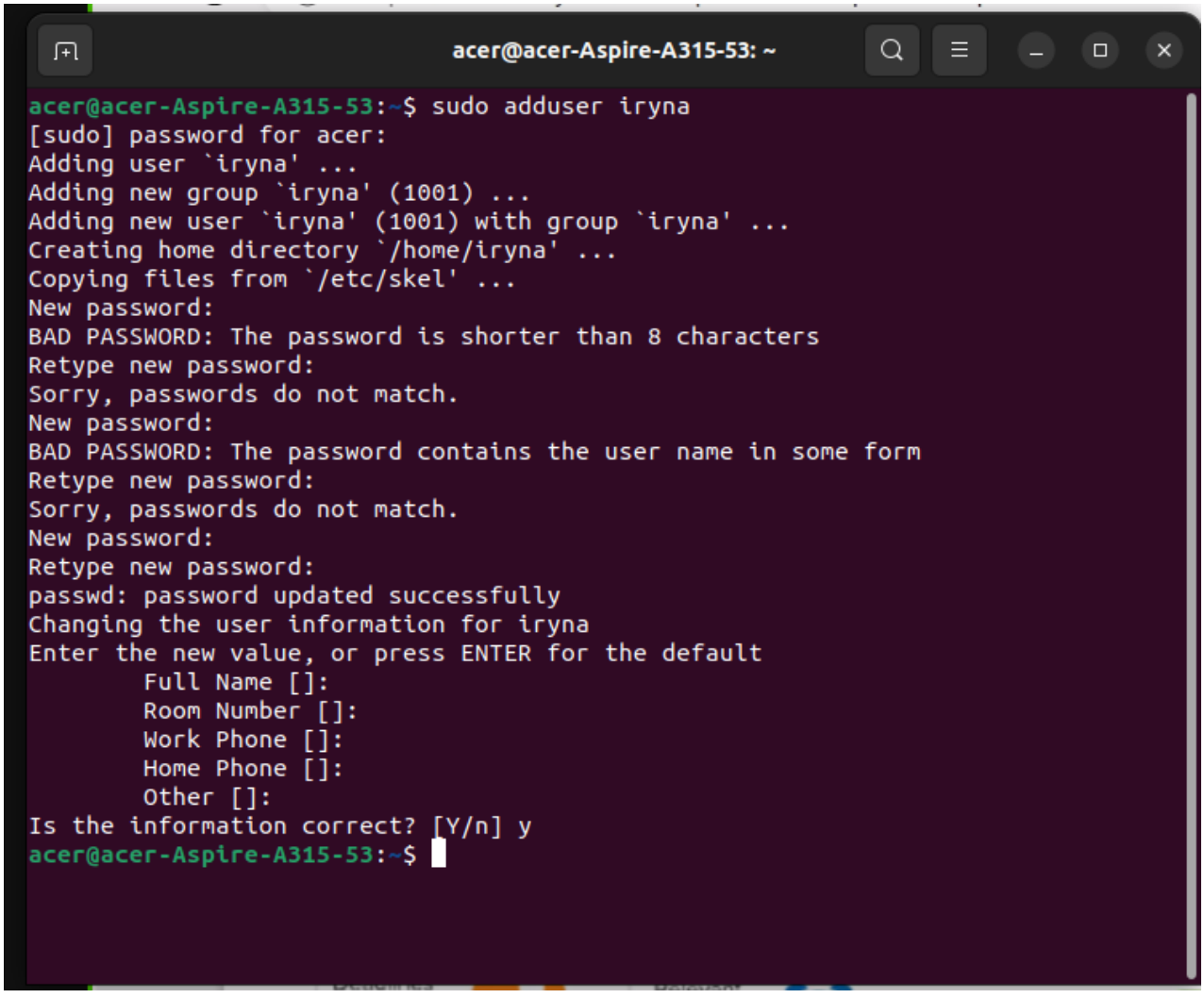
10. Nmap (an acronym of Network Mapper) is an open-source command-line utility to securely manage the network. Nmap command has an extensive list of options to deal with security auditing and network exploration.

3.5 Describe the configuration settings for a working system

Initial Server Setup with Ubuntu 22.04

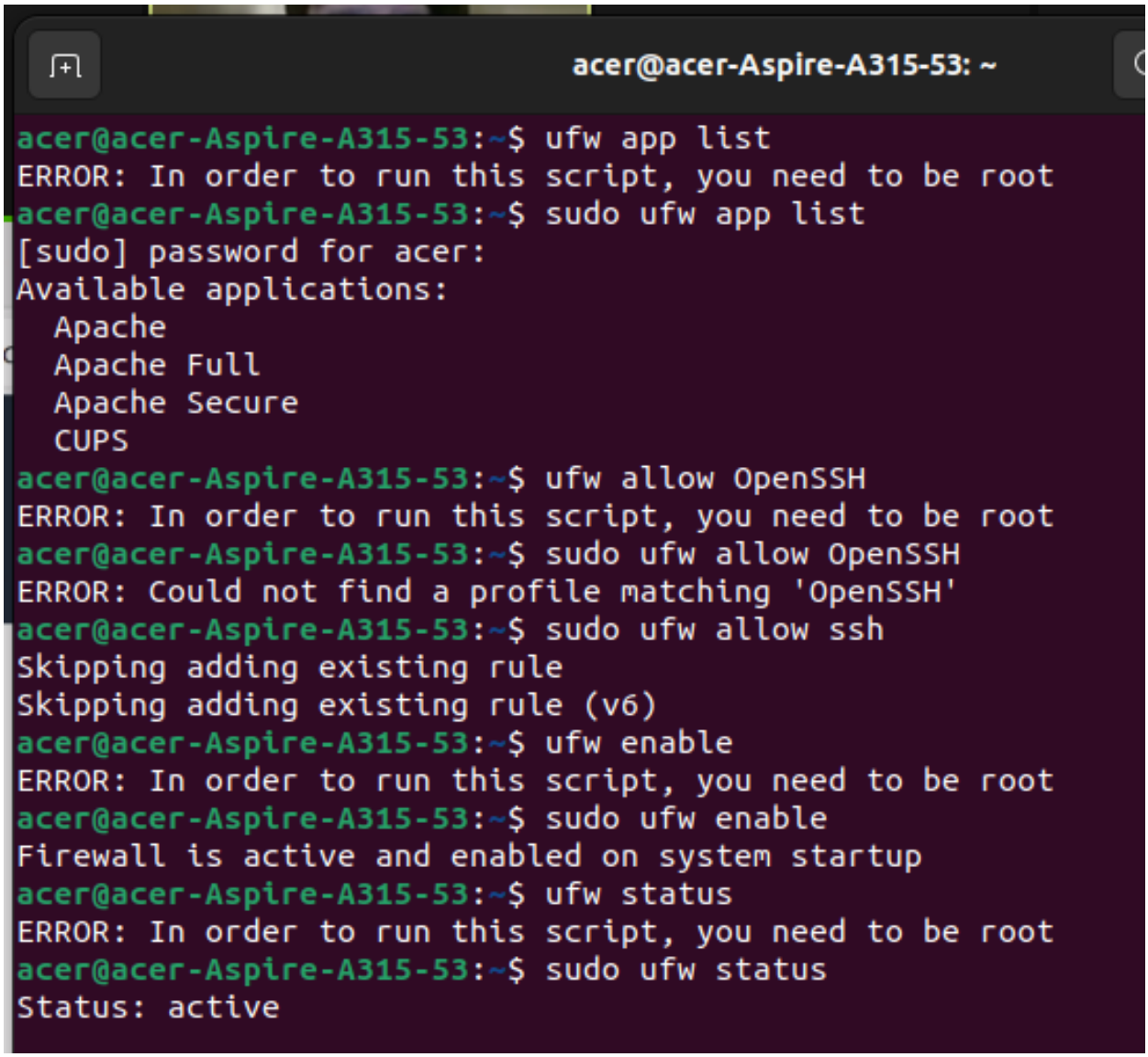
These steps will increase the security and usability of server:

Step 1 — Creating a New User



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.

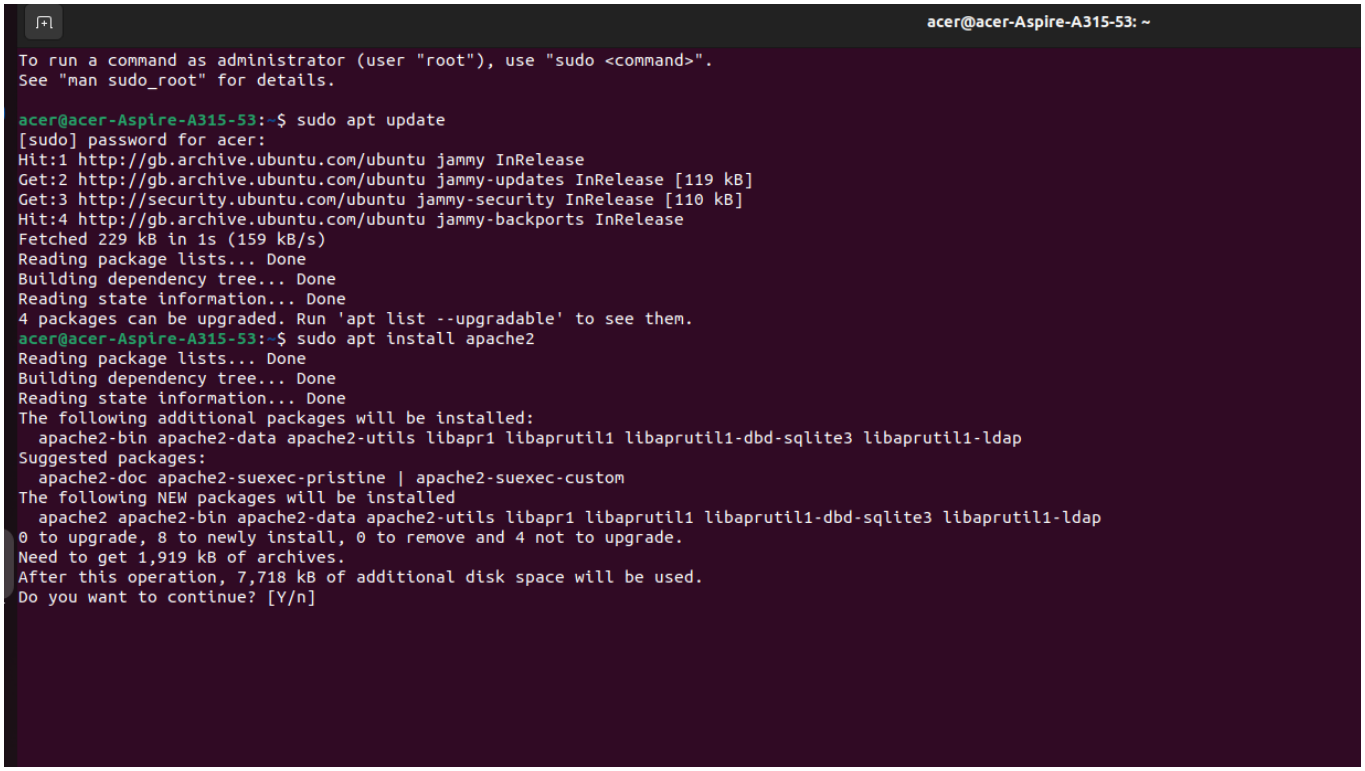


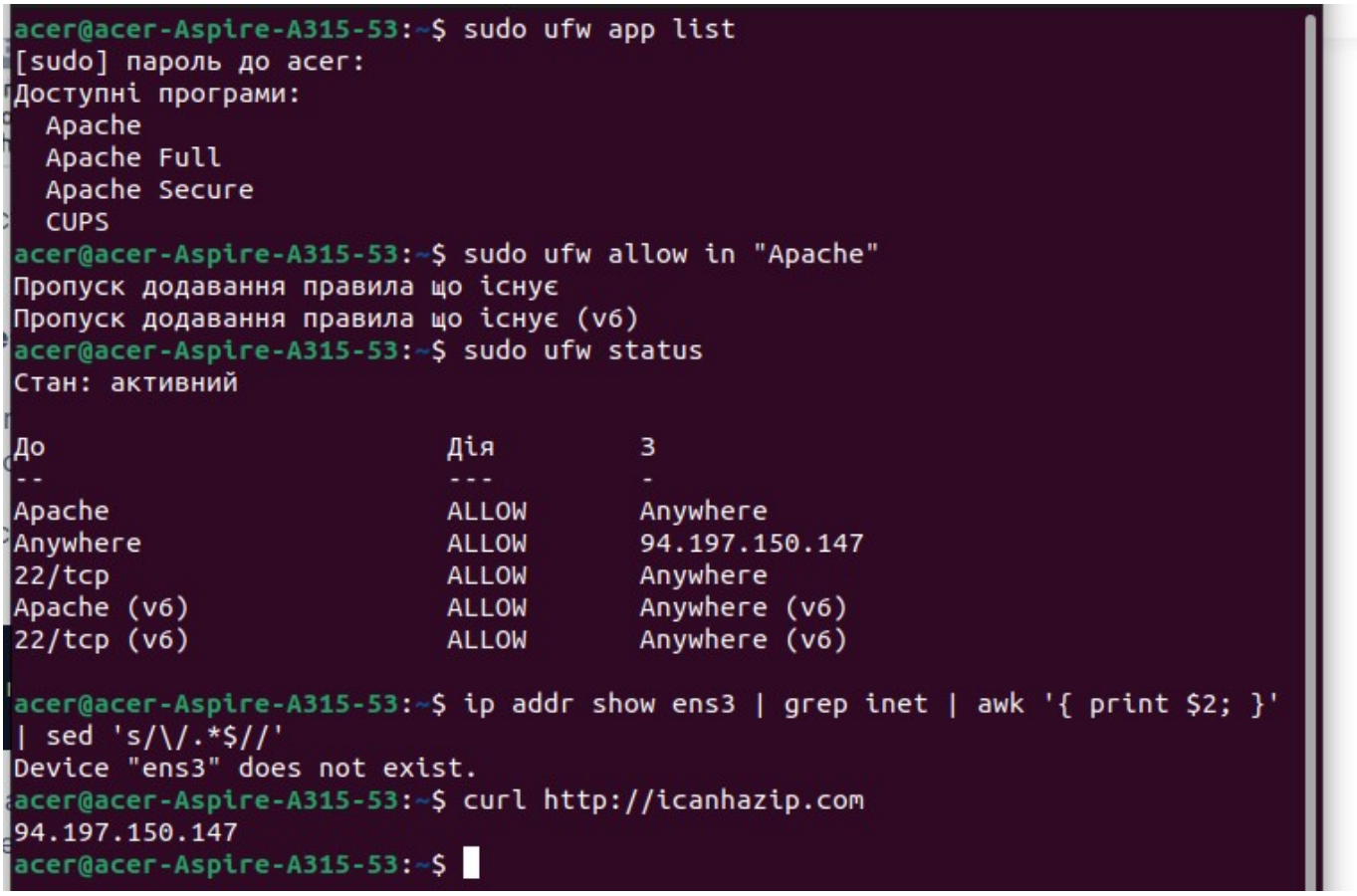
Install Linux, Apache, MySQL, PHP (LAMP) Stack on Ubuntu 22.04

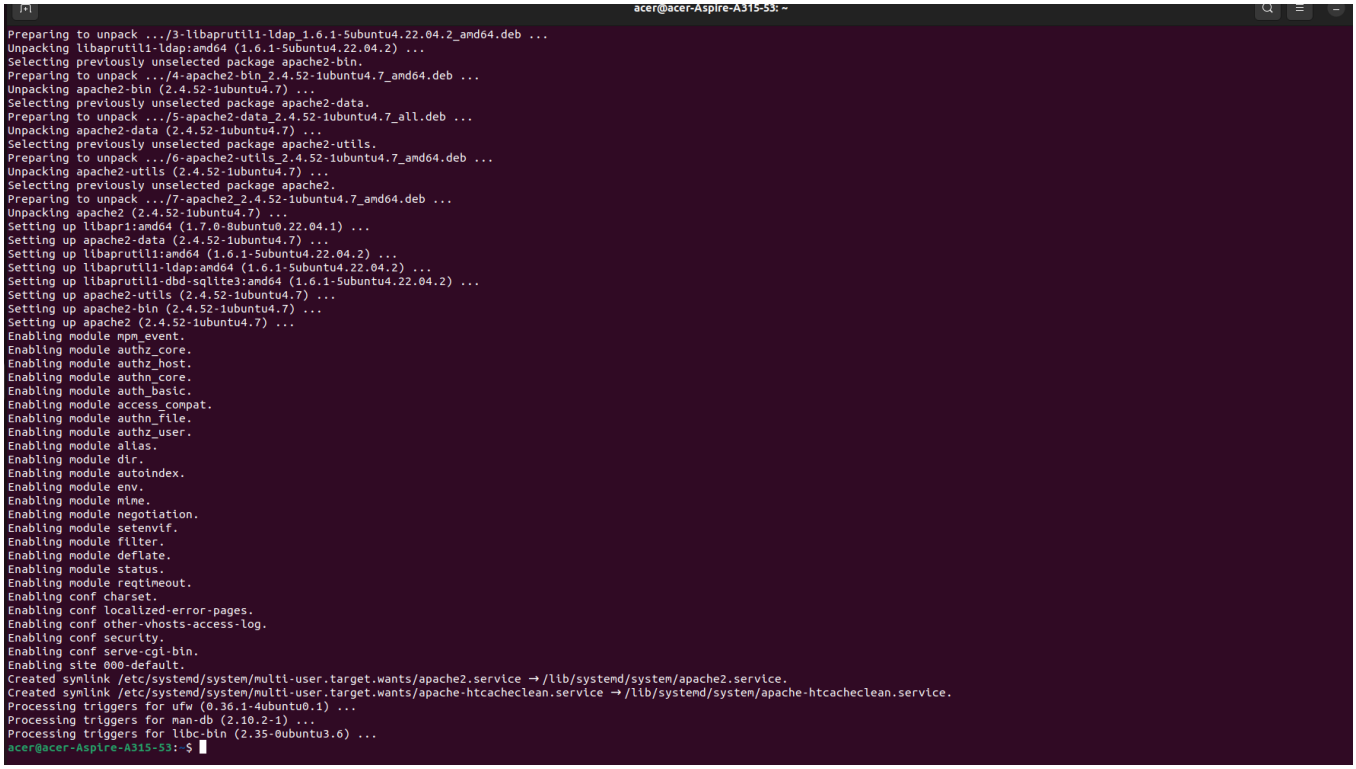
Step 1 — Installing Apache and Updating the Firewall:

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.

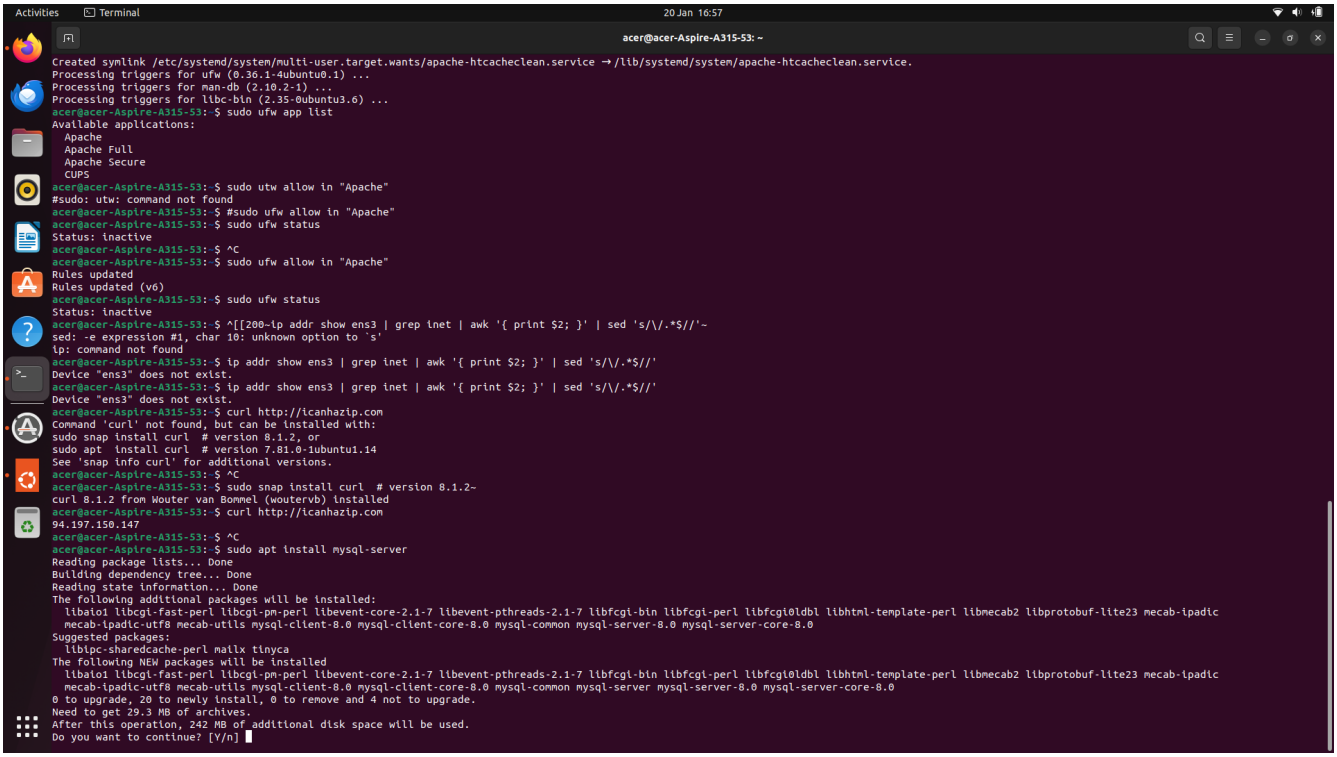

acer@acer-Aspire-A315-53: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
acer@acer-Aspire-A315-53:~$ sudo apt update
[sudo] password for acer:
Hit:1 http://gb.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://gb.archive.ubuntu.com/ubuntu 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:~$



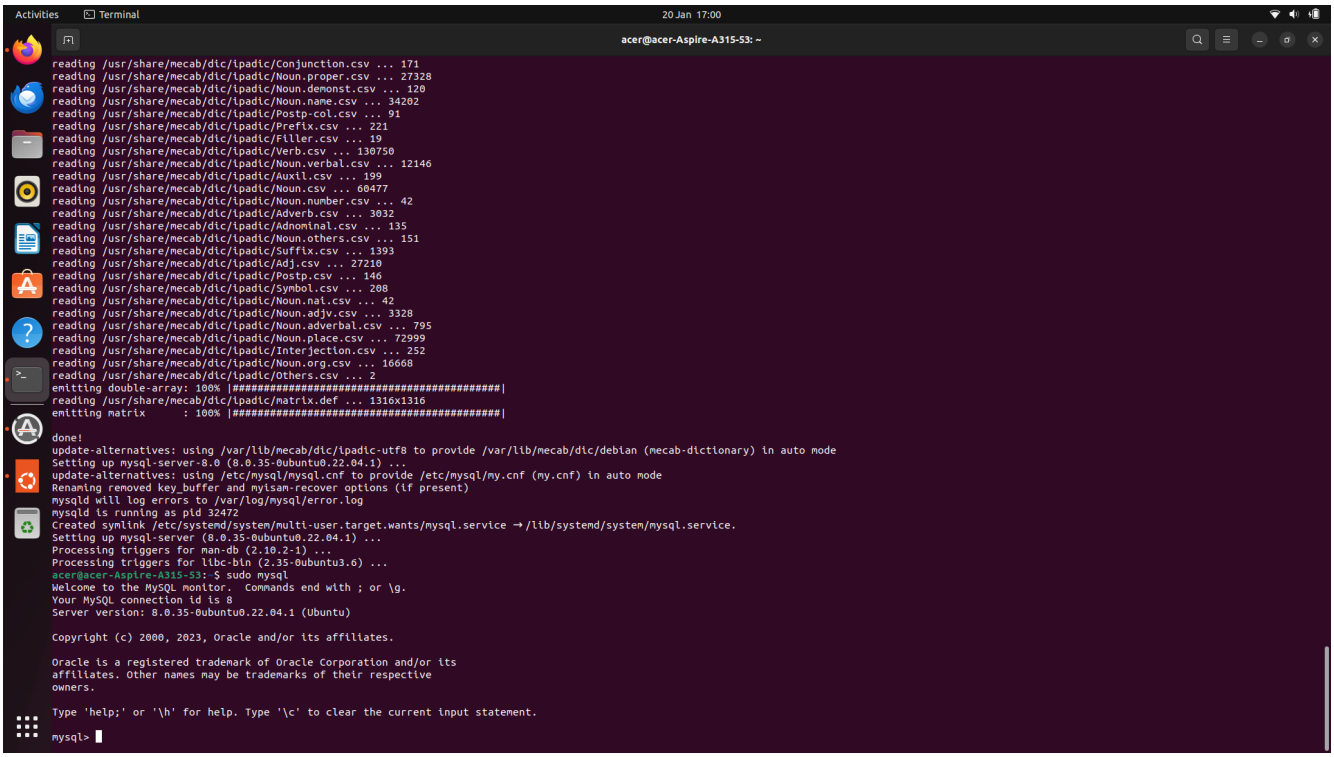
Step 2 — Installing MySQL

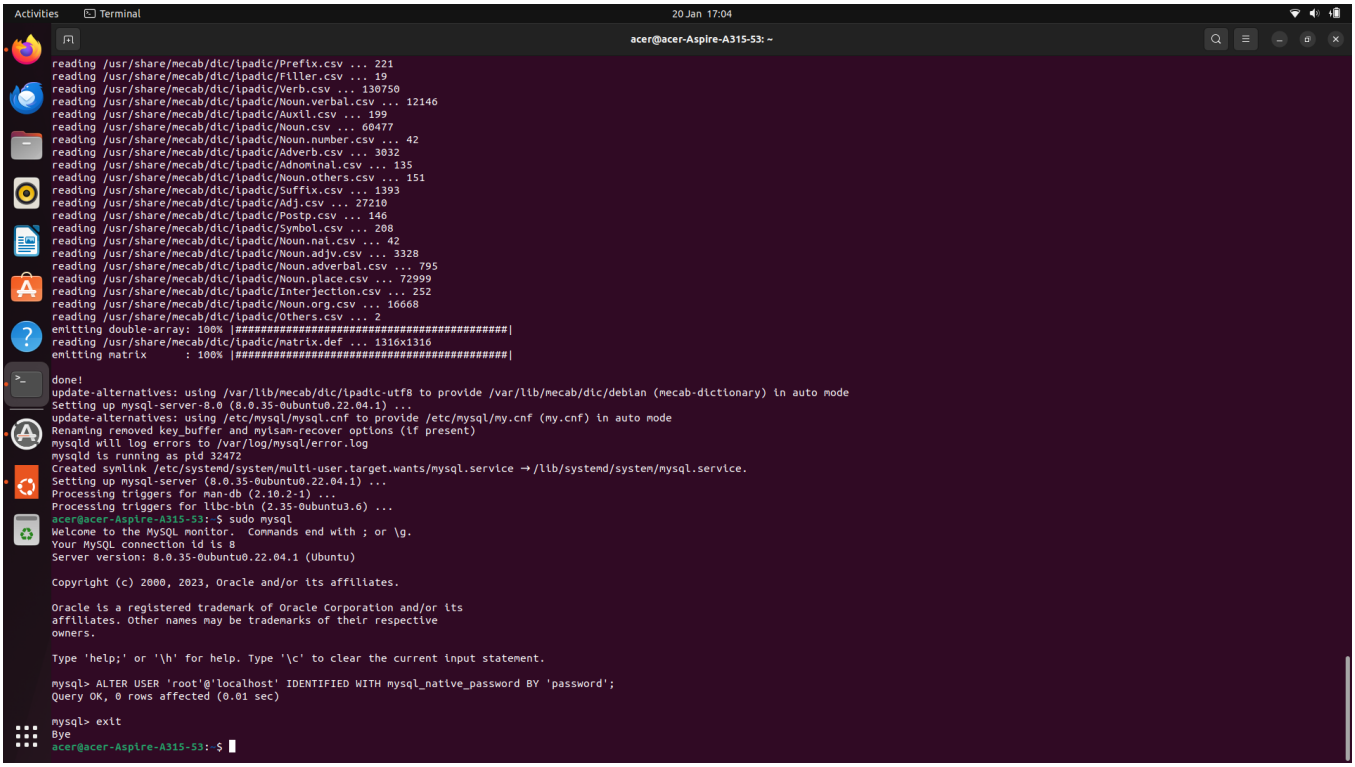
Now that I had a web server up and running, I used `apt` to acquire and install MySQL:



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.

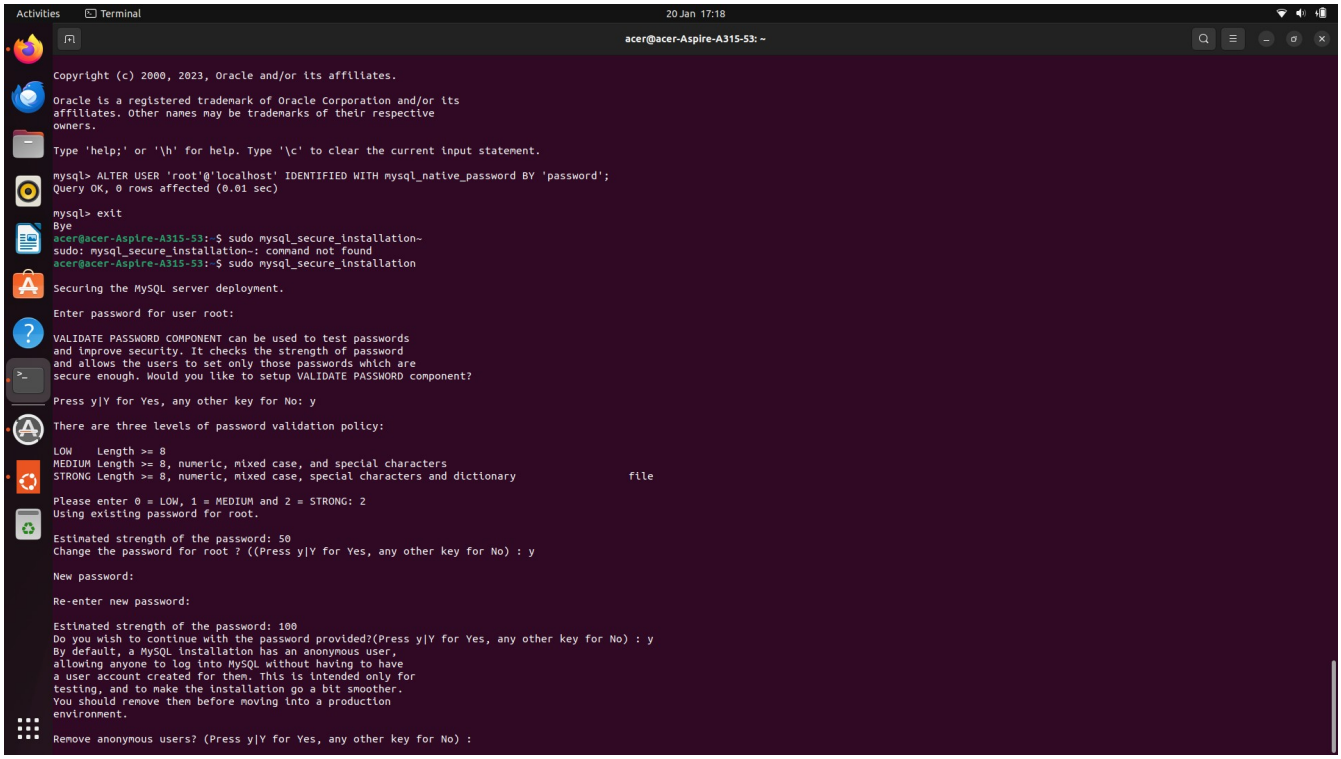
I run the following ALTER USER command to change the root user's authentication method to one that uses a password.

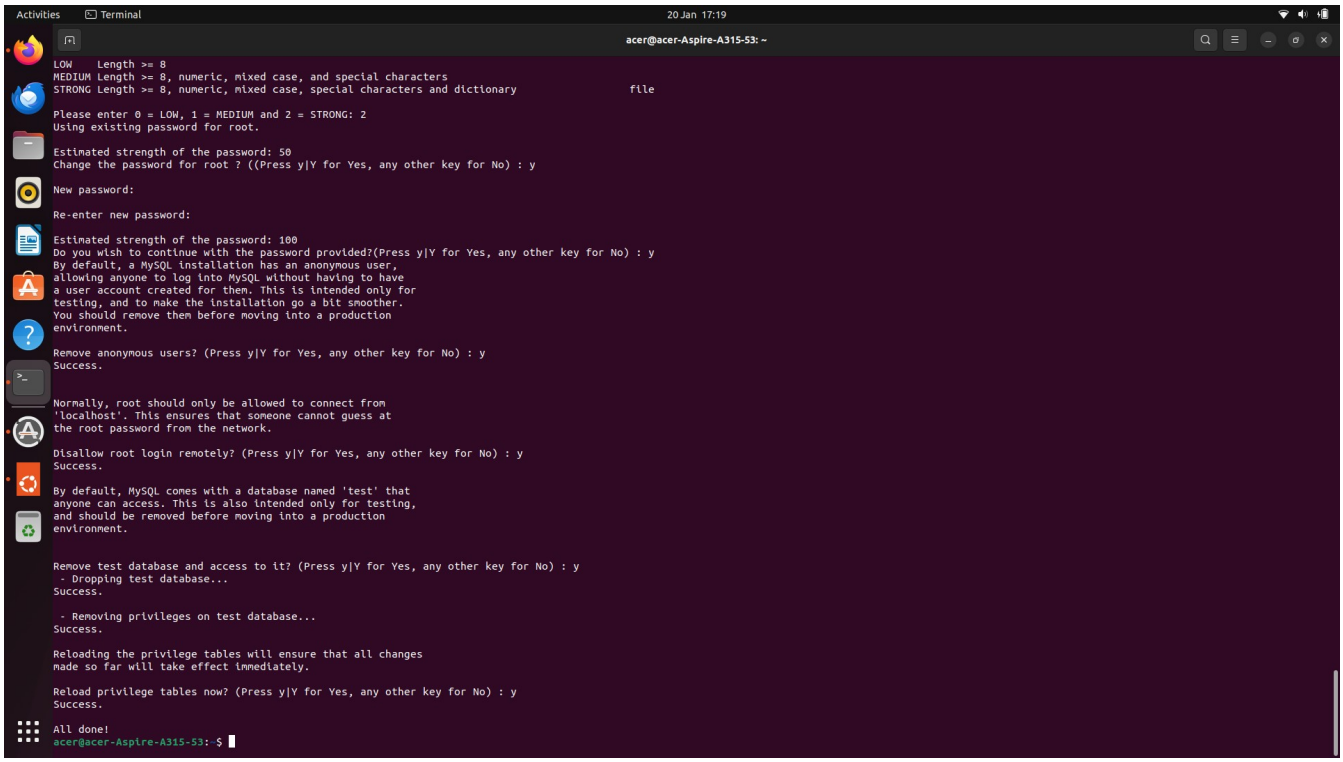




I started the interactive script by running:
sudo mysql_secure_installation
This asked to configure the VALIDATE PASSWORD PLUGIN.

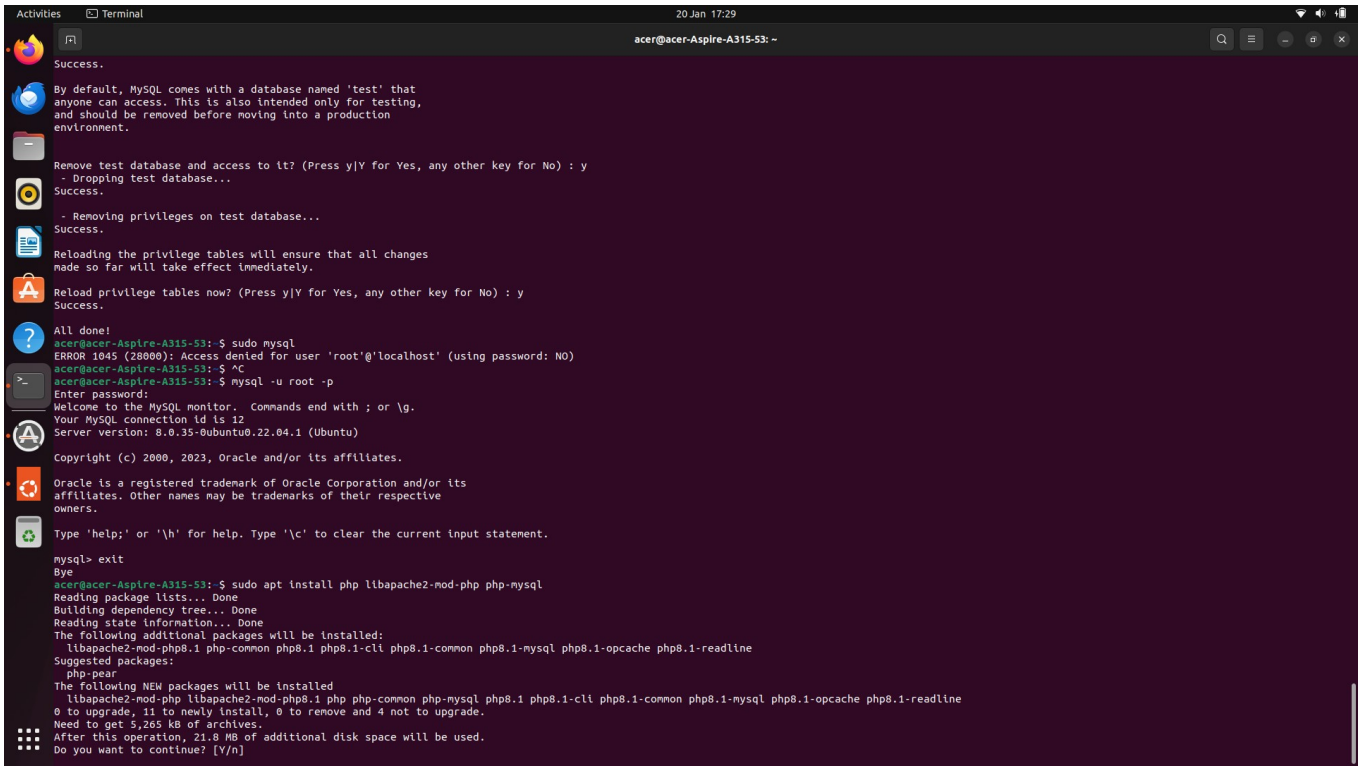
I answered “yes”, and be asked to select a level of password validation. I entered `2` for the strongest level. In this case I will receive errors when attempting to set any password which does not contain numbers, upper and lowercase letters, and special characters.
I enabled password validation, and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



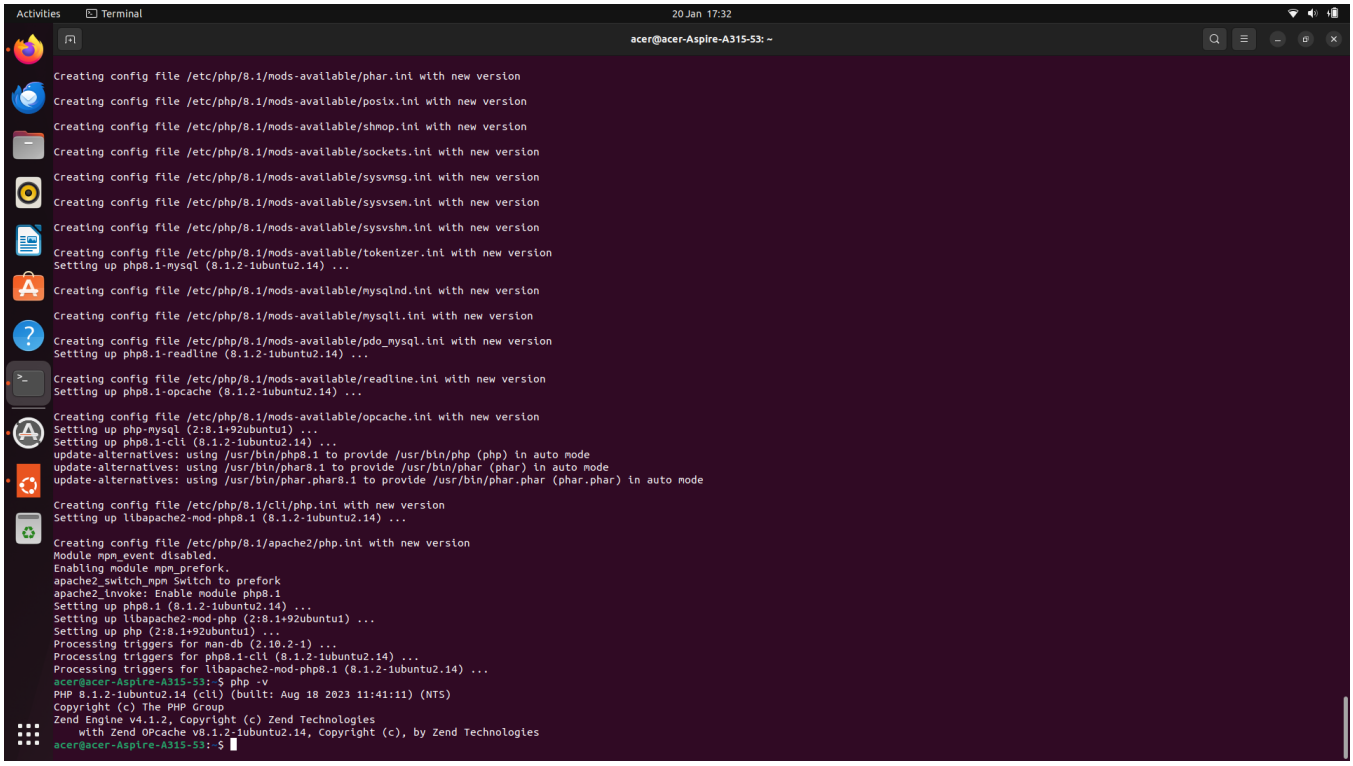


Step 3 — Installing PHP

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.



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



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** :

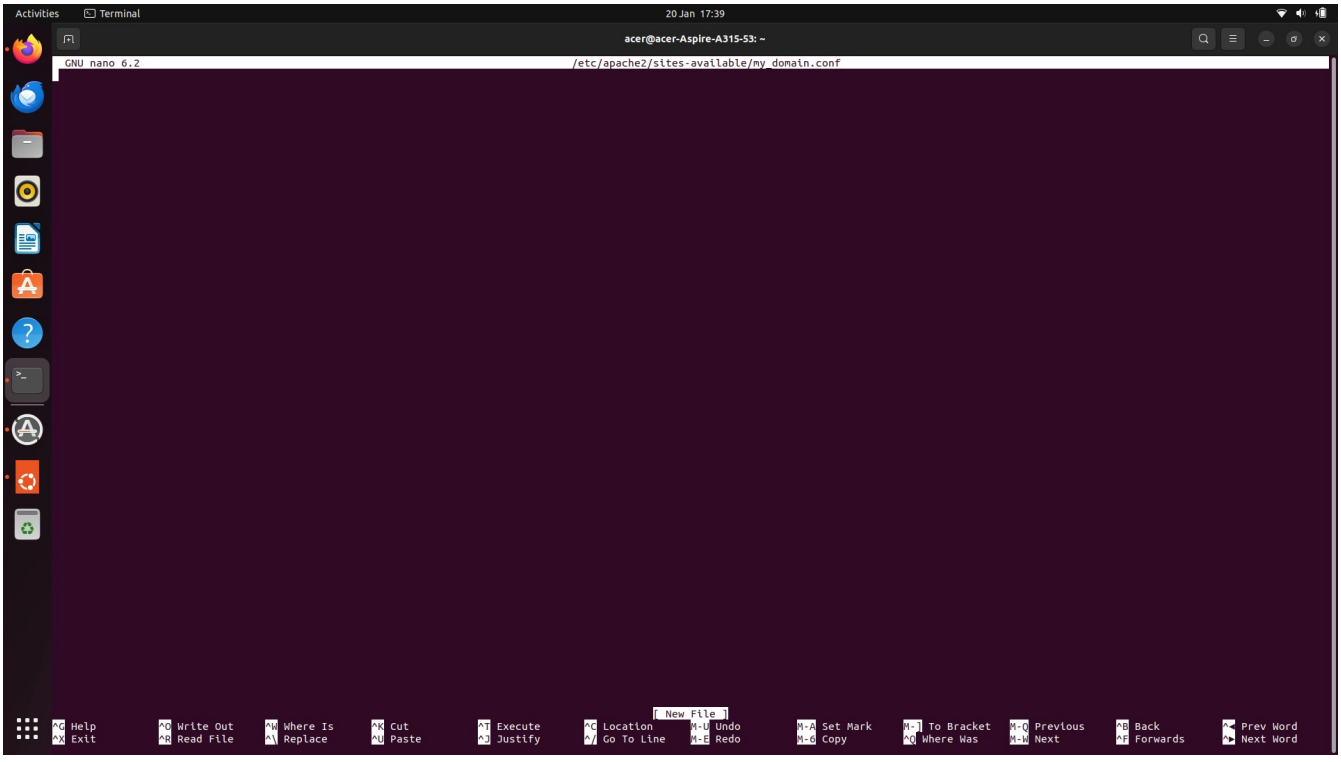
sudo mkdir /var/www/my_domain

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'am 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

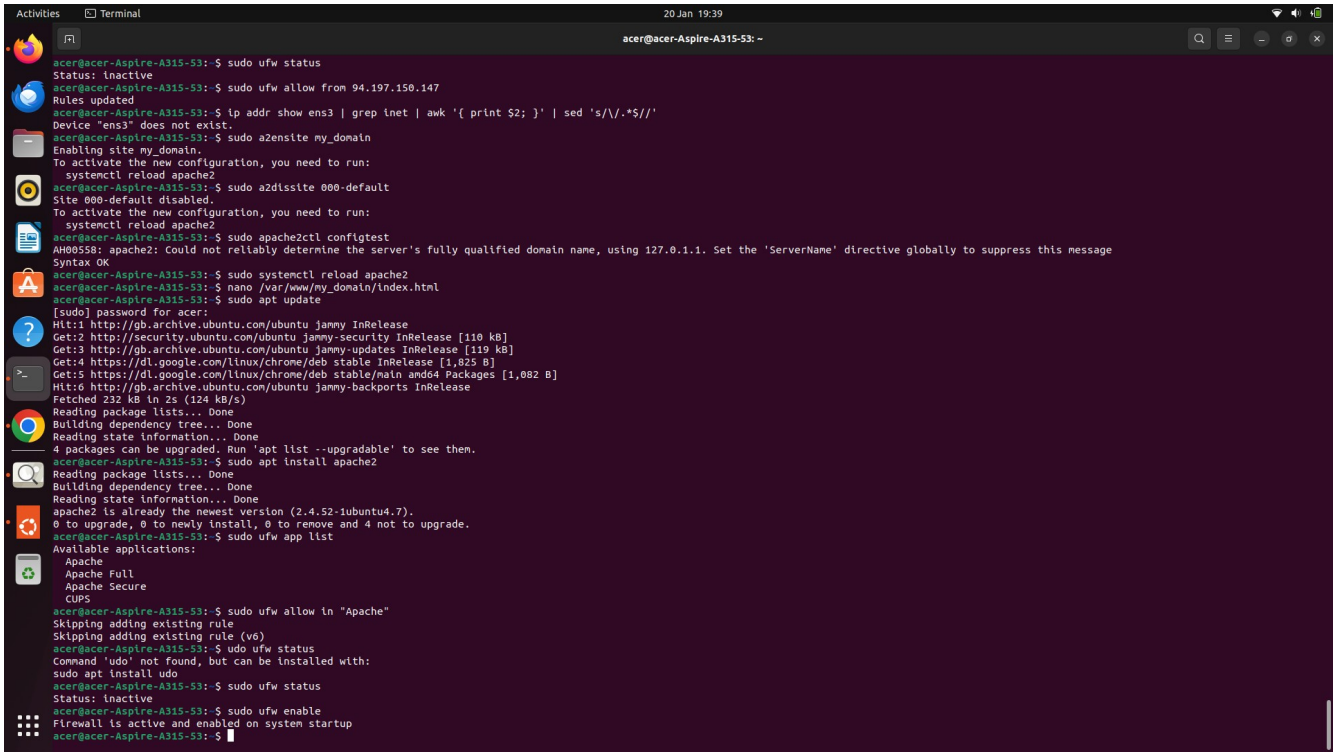
```
<html>
  <head>
    <title>your_domain website</title>
  </head>
  <body>
    <h1>Hello World!</h1>

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

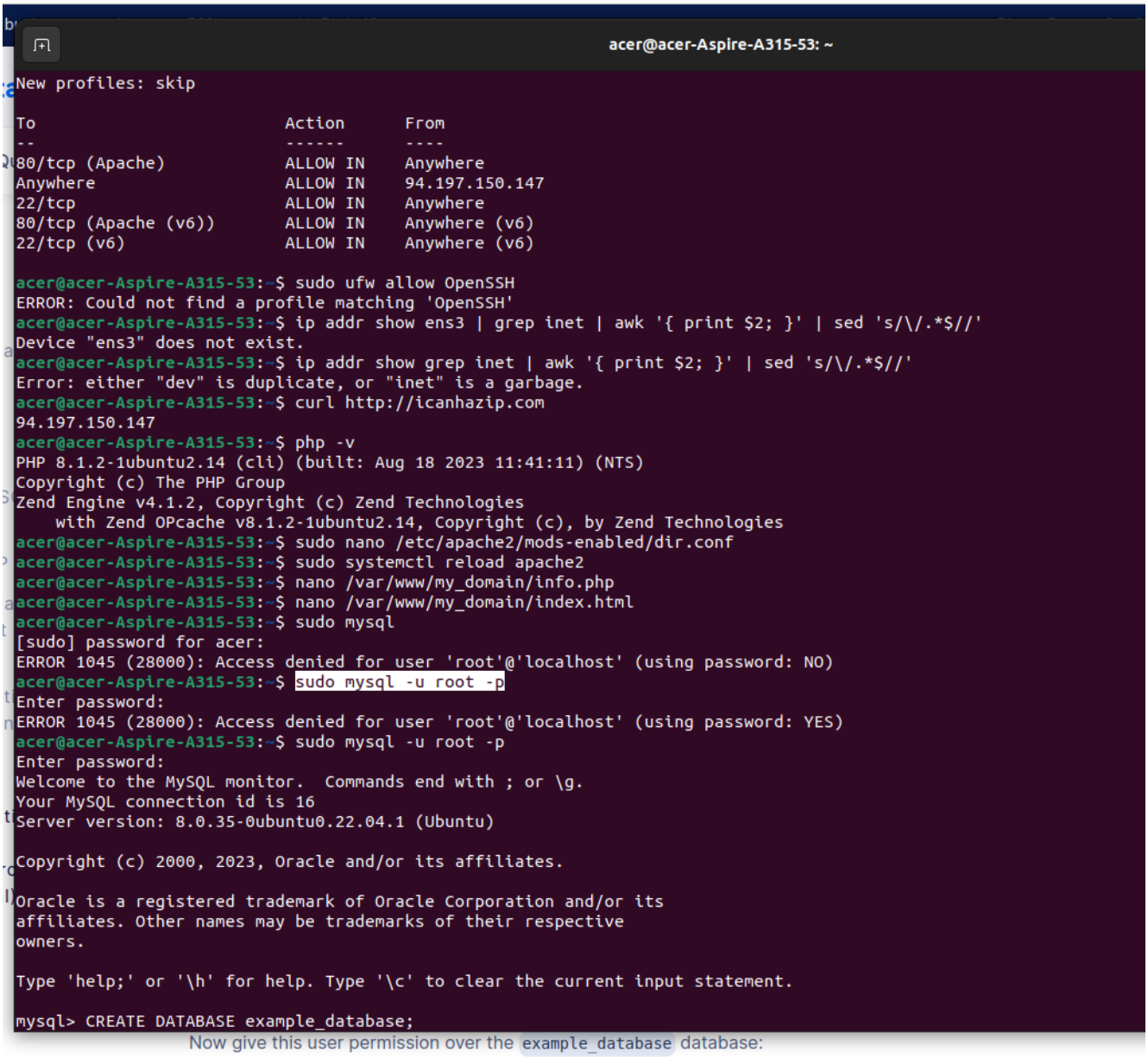
```
acer@acer-Aspire-A315-53:~$ sudo ufw status
Status: inactive
acer@acer-Aspire-A315-53:~$ sudo ufw allow from 94.197.150.147
Rules updated
acer@acer-Aspire-A315-53:~$ ip addr show ens3 | grep inet | awk '{ print $2; }' | sed 's/\/.*$//'
Device "ens3" does not exist.
acer@acer-Aspire-A315-53:~$ sudo 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 '
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.
```

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>
```





sudo systemctl reload apache2

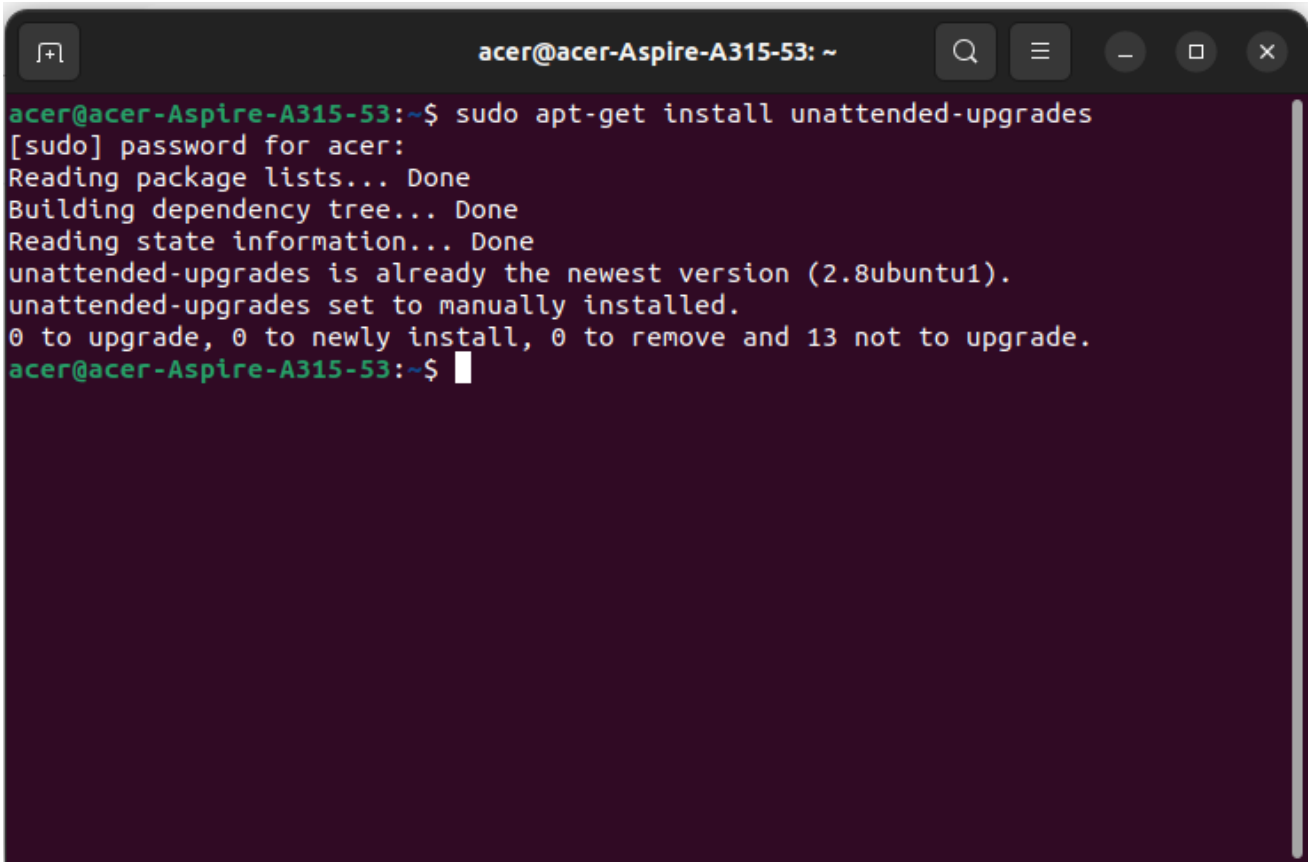
3.6 Recommend final adjustments before going live

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

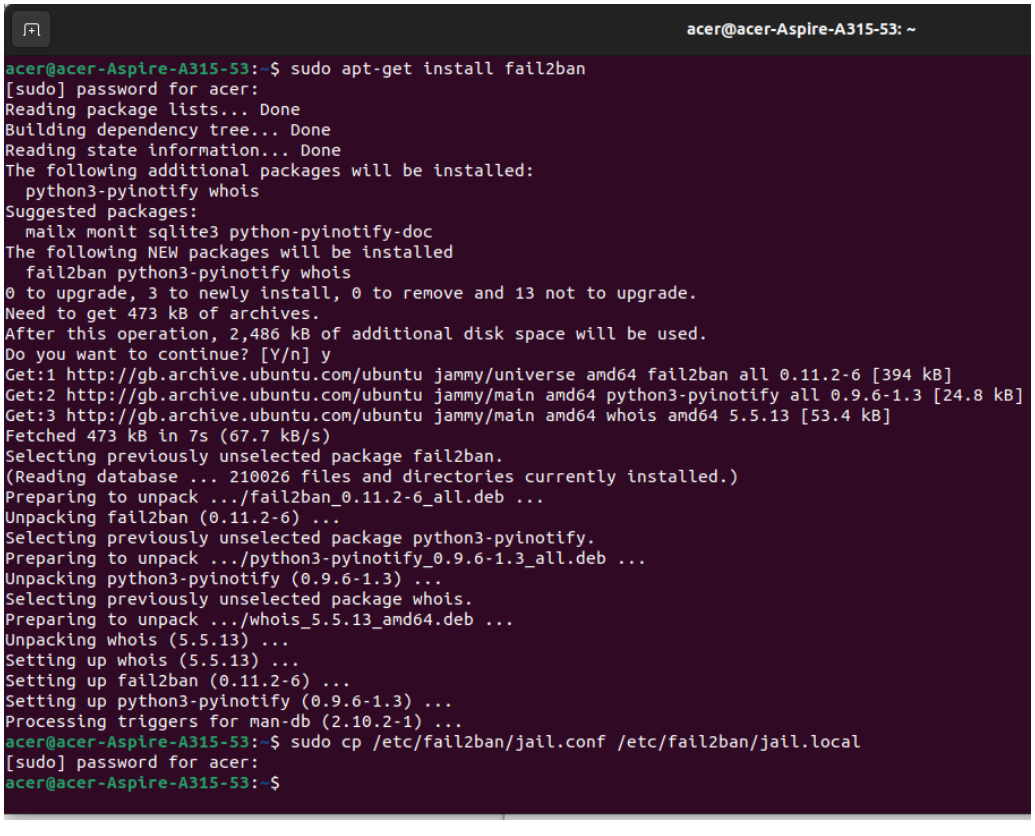


2. Install Fail2ban

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

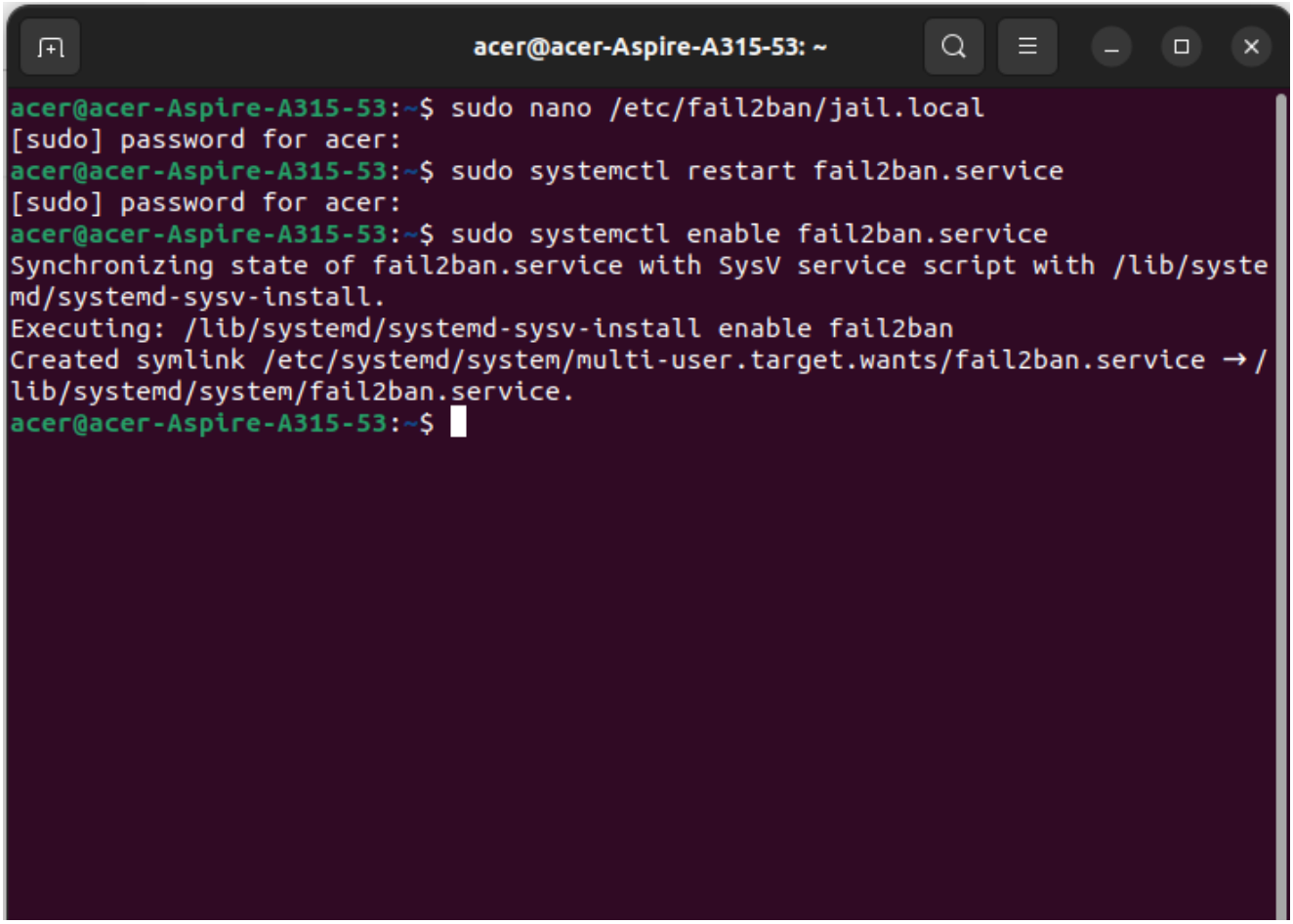


sudo nano /etc/fail2ban/jail.local

The [sshd] block was changed :
[sshd]

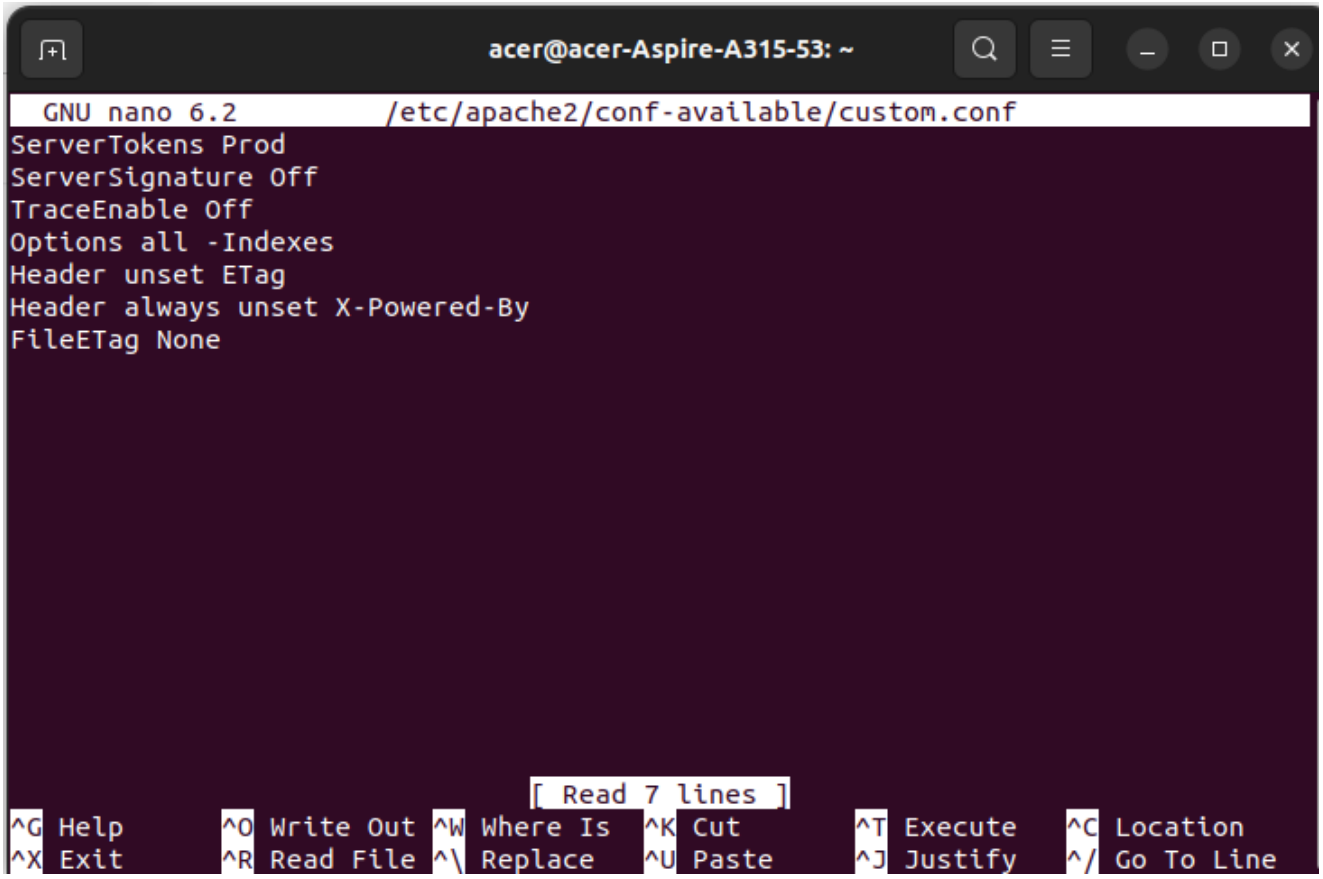
```
# Provide customizations in a jail.local file or a jail.d/customisatio
# For example to change the default bantime for all jails and to enabl
# ssh-iptables jail the following (uncommented) would appear in the .l
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
# enabled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

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

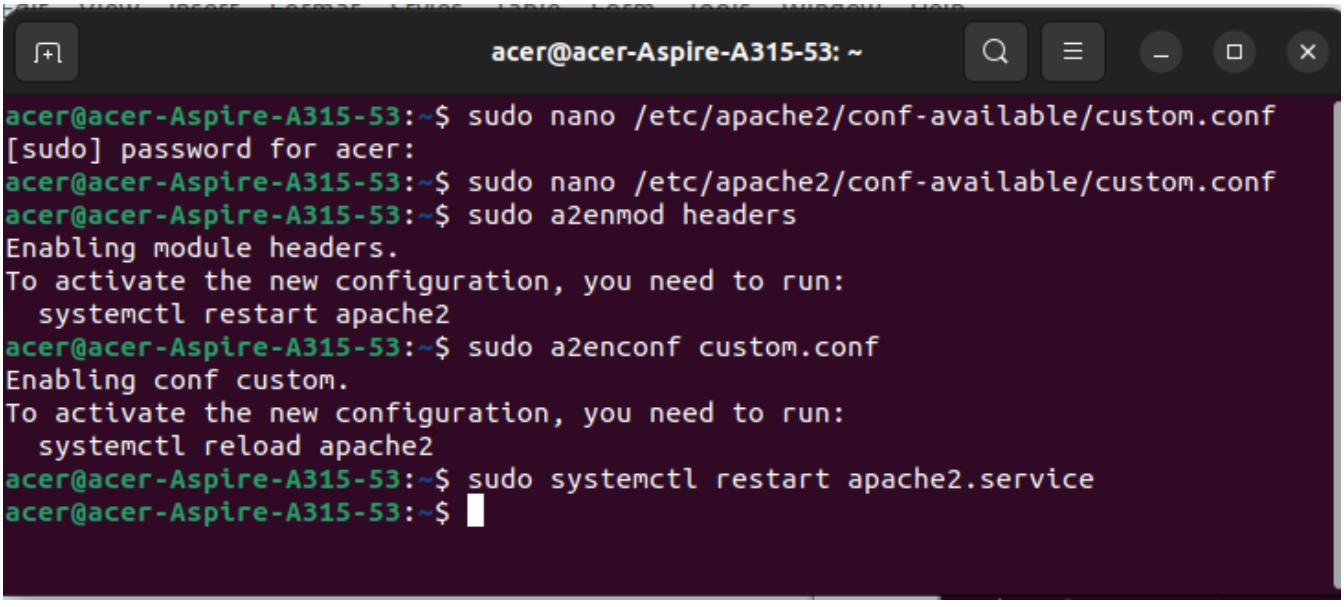
I saved the file and restart Fail2ban for the changes to take effect:
sudo systemctl restart fail2ban.service
And then enabled Fail2ban on system boot:
sudo systemctl enable fail2ban.service



3. Hide Apache sensitive information

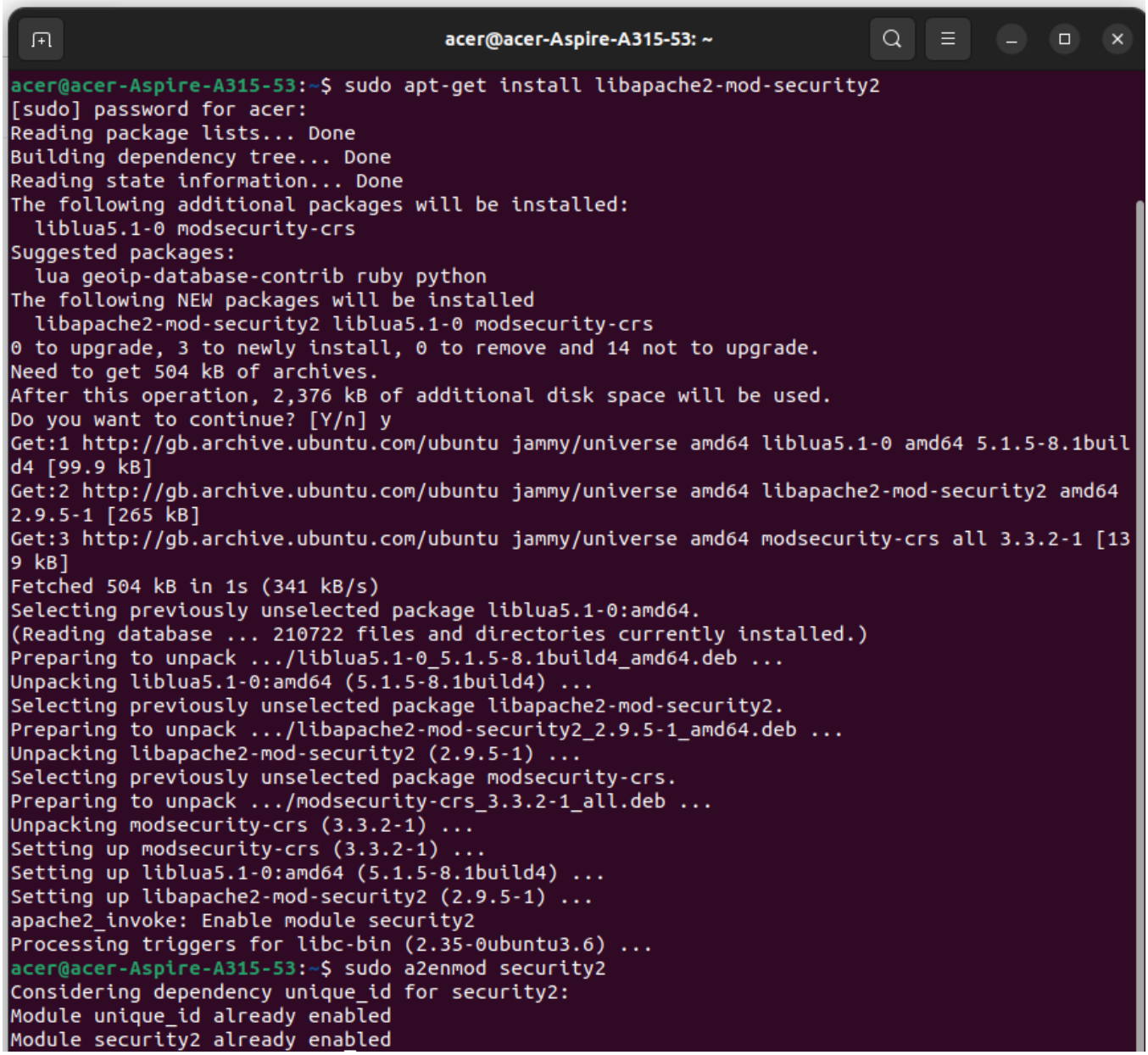
The default Apache configuration provides much sensitive information which can be used against the service. I Maked this information hidden and created a configuration file for new settings:





4. Install and enable mod_security

I installed and enabled mod_security :
sudo apt-get install libapache2-modsecurity2
sudo a2enmod security2

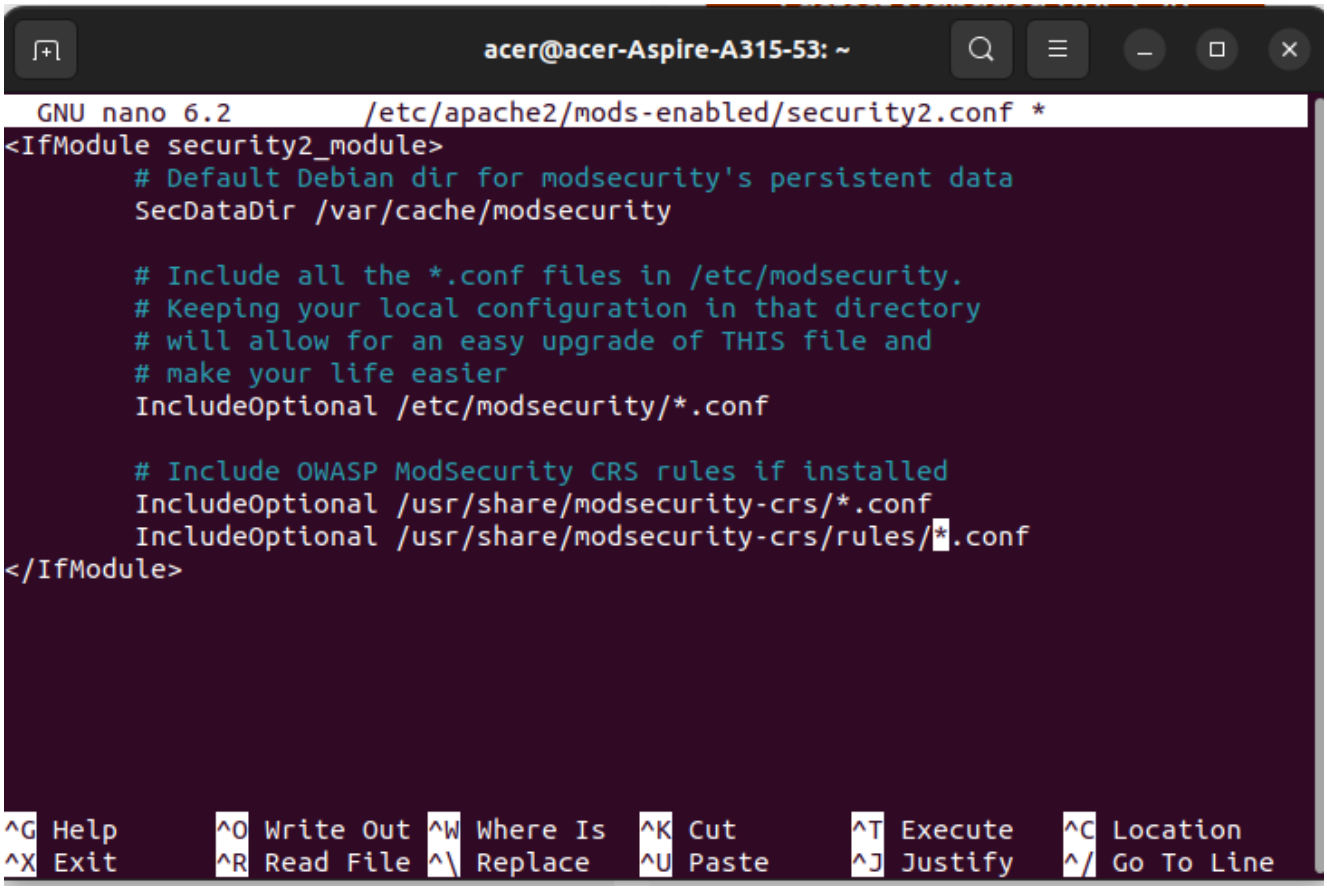


Then Iconfigured the module and enabled the OWASP ModSecurity Core Rule Set (CRS).

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

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

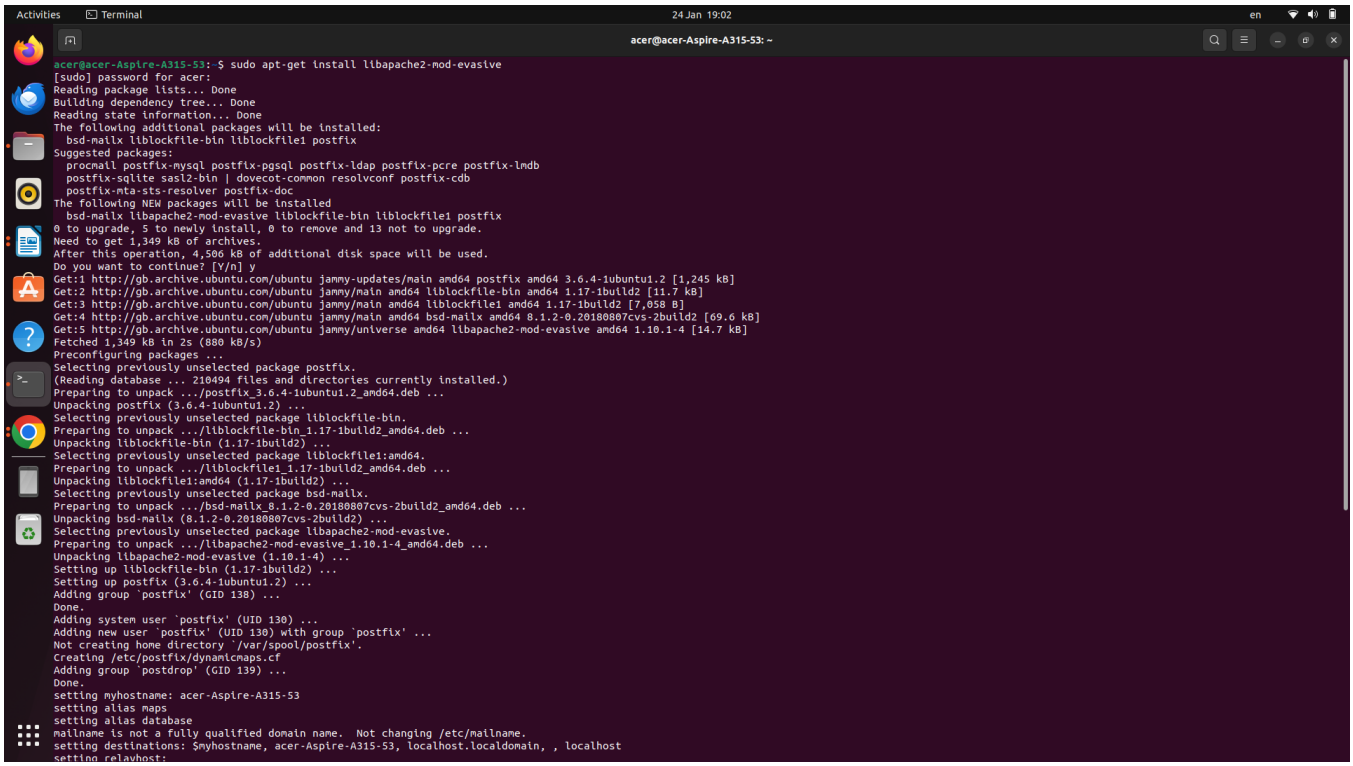
Then I removed the current CRS and download the OWASP CRS and edited ***/etc/apache2/mods-enabled/security2.conf*** **file**



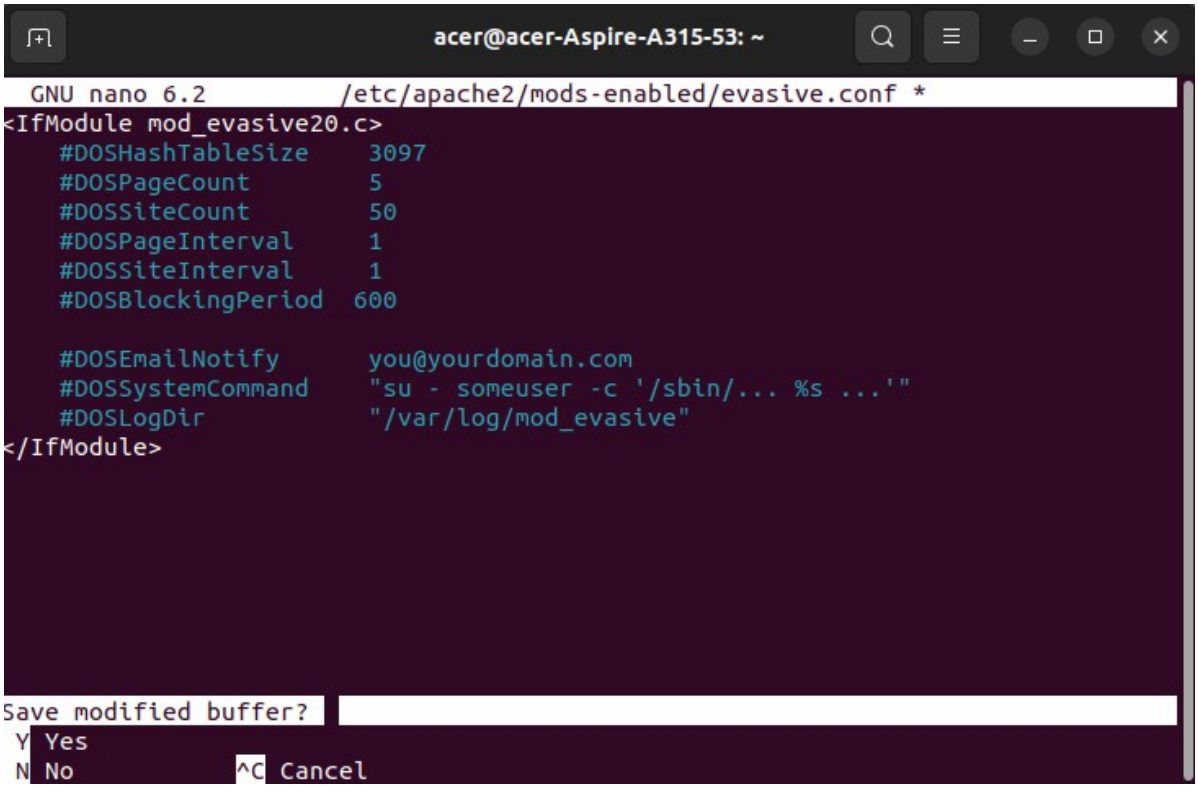
5. Install and enable mod_evasive

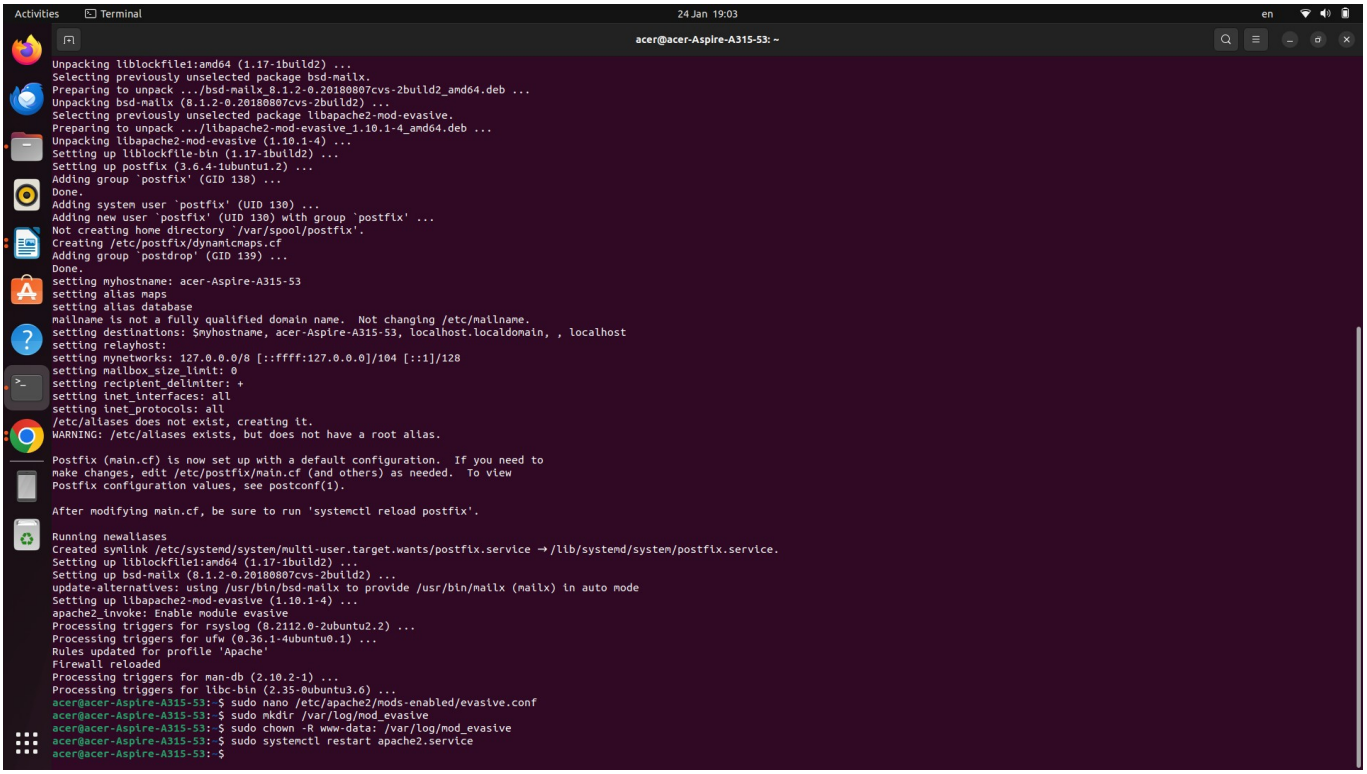
Mod_evasive is an Apache module which can be used to protect the web server from DoS (Denial of Service), DDoS (Distributed Denial of Service) and brute-force attacks. To install mod_evasive on server, I run :

sudo apt-get install libapache2-mod-evasive



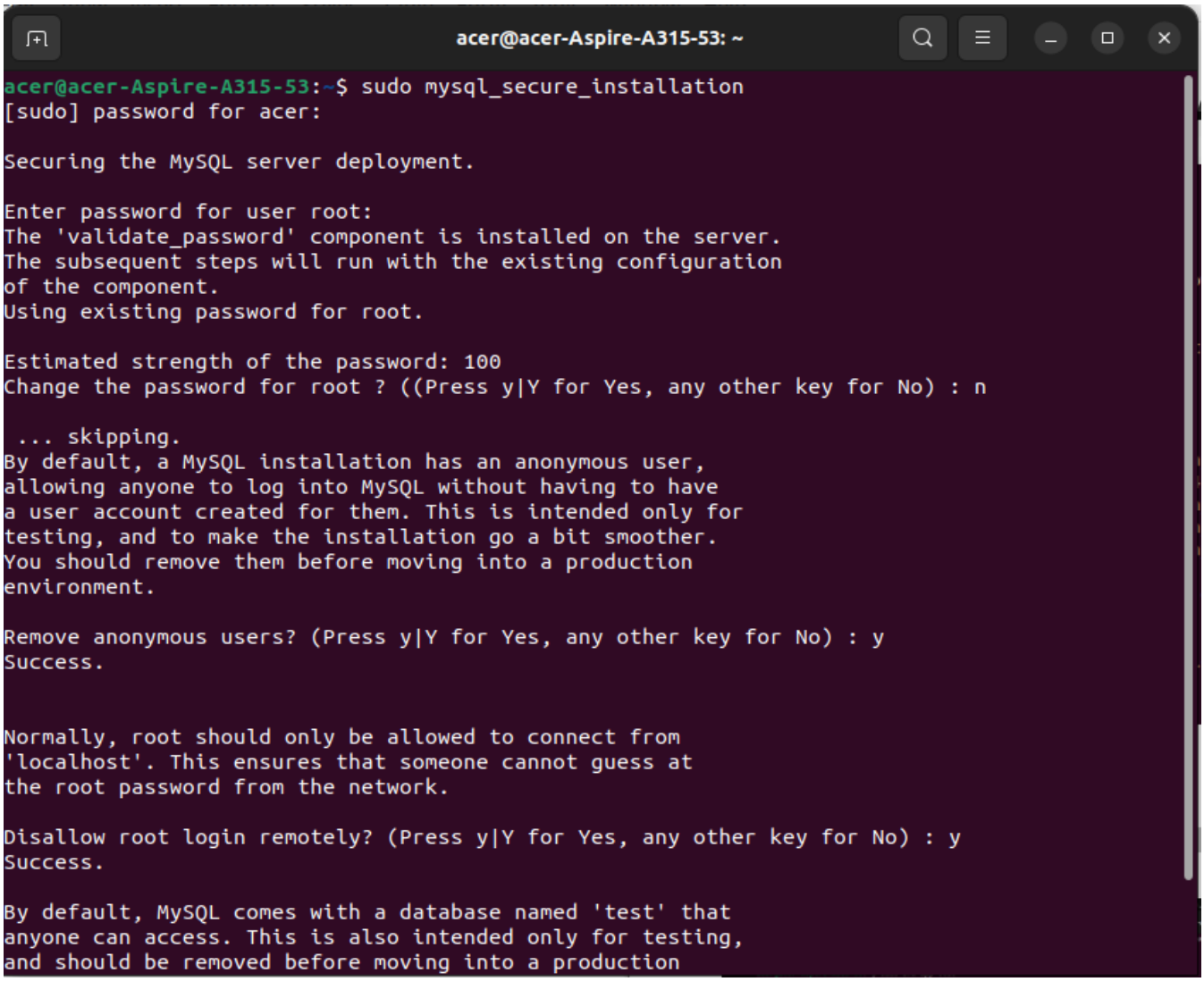
I edited the default configuration file */etc/apache2/mods-enabled/evasive.conf*





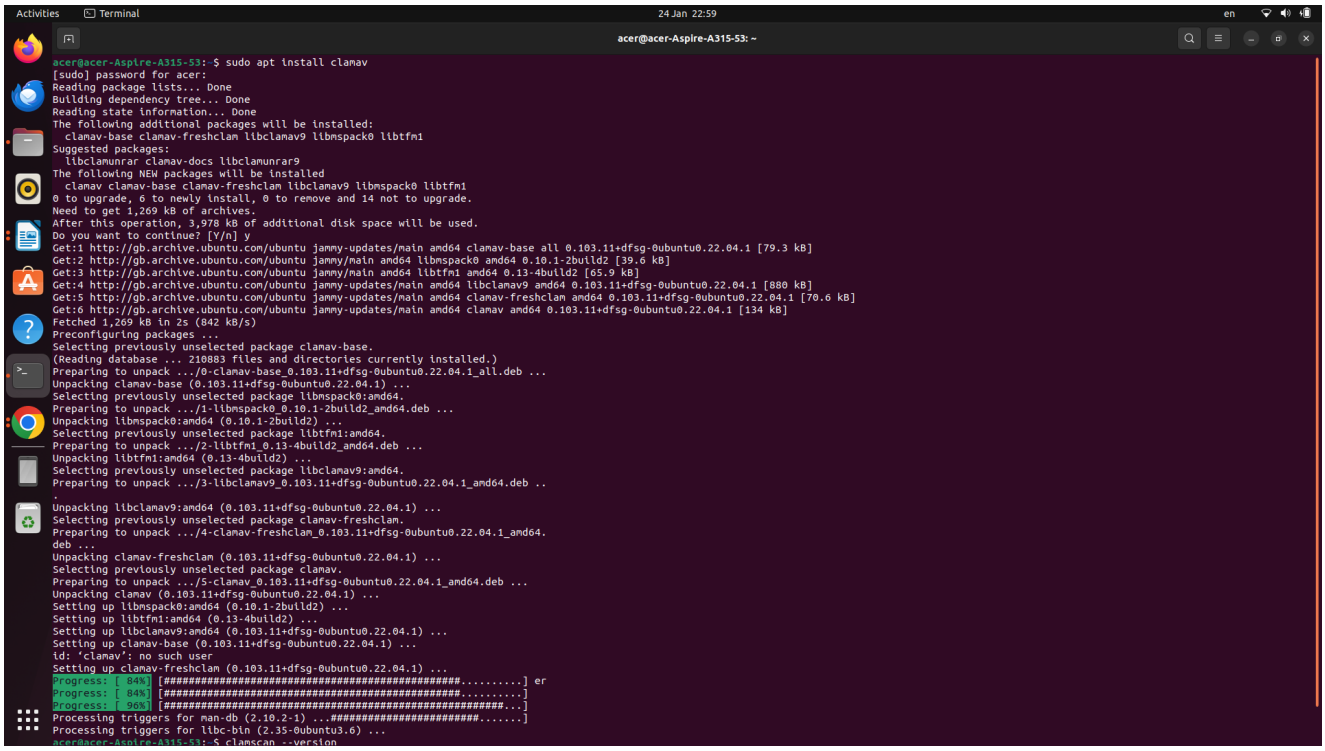
6 Secure the MySQL server deployment

To secure the MySQL service I run the *mysql_secure_installation* script.



7. Installing ClamAV (Anti-Virus Protection)

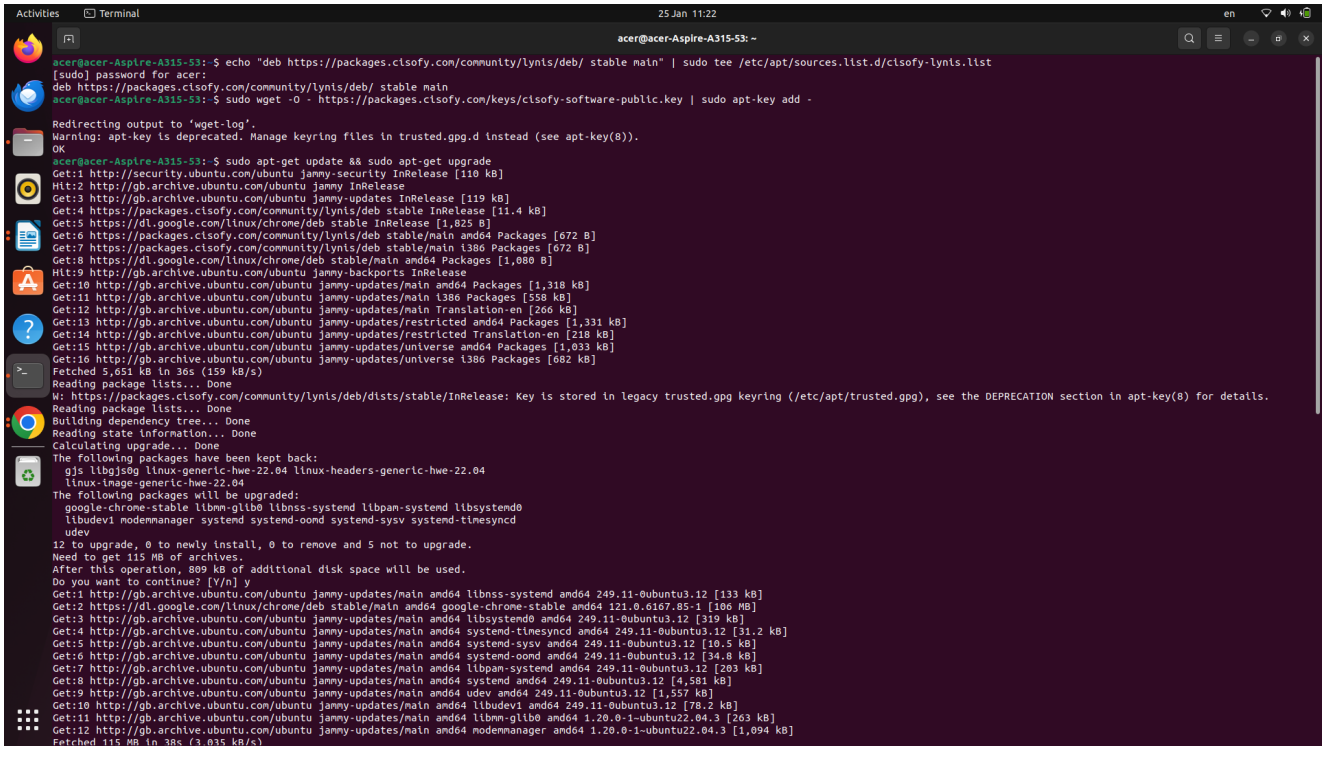
I Installed the clamav package by running the following command: **sudo apt install clamav**



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 -**



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/


2007-2021, CISOfy - https://cisofy.com/lynis/
```

9. Using a MySAT

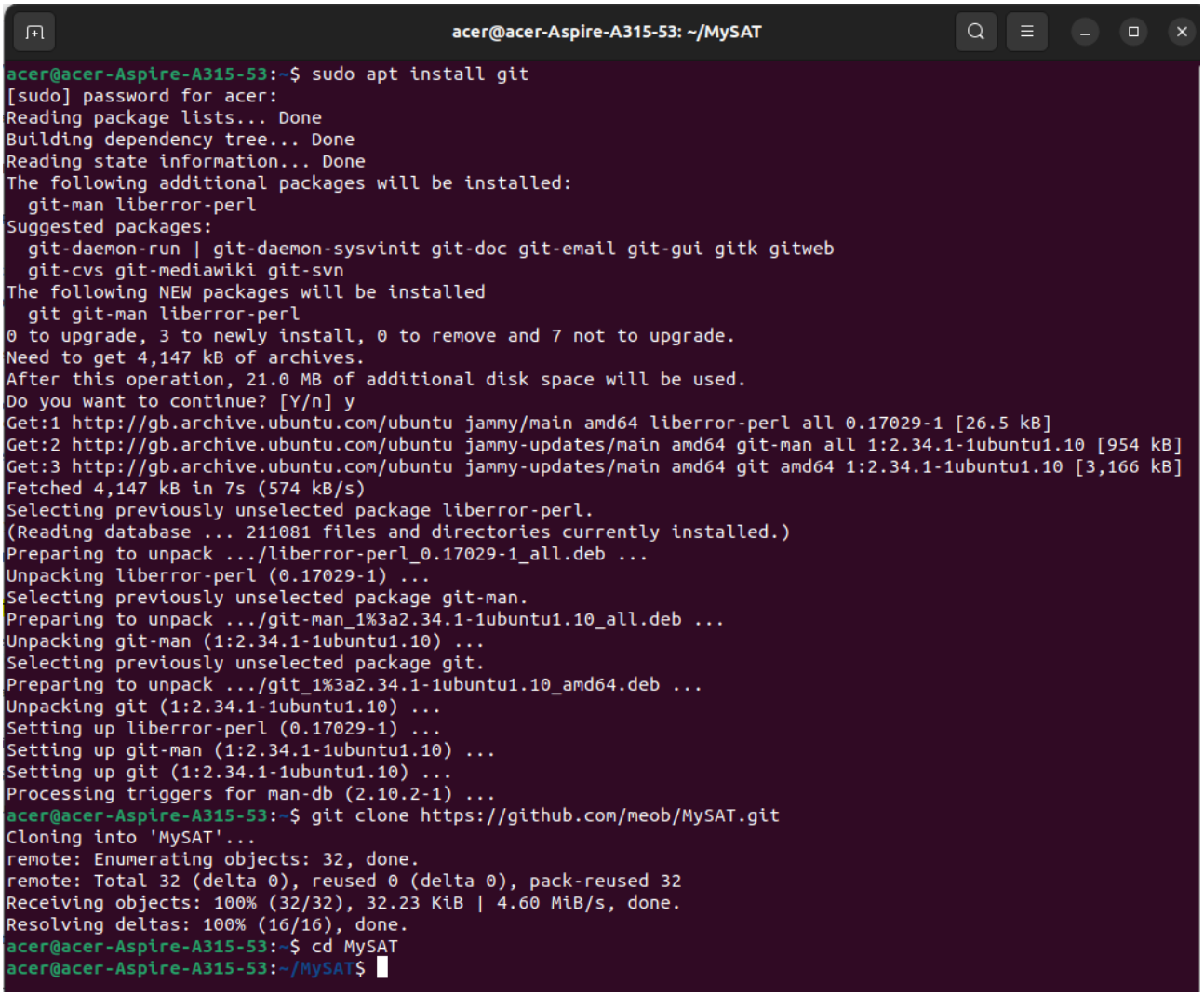
I audit the security of MySQL server by using a tool MySAT. MySAT performs several test to analyze database configurations and security policies. MySAT help to assess and therefore increase MySQL database security. MySAT results are output in HTML format.

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.

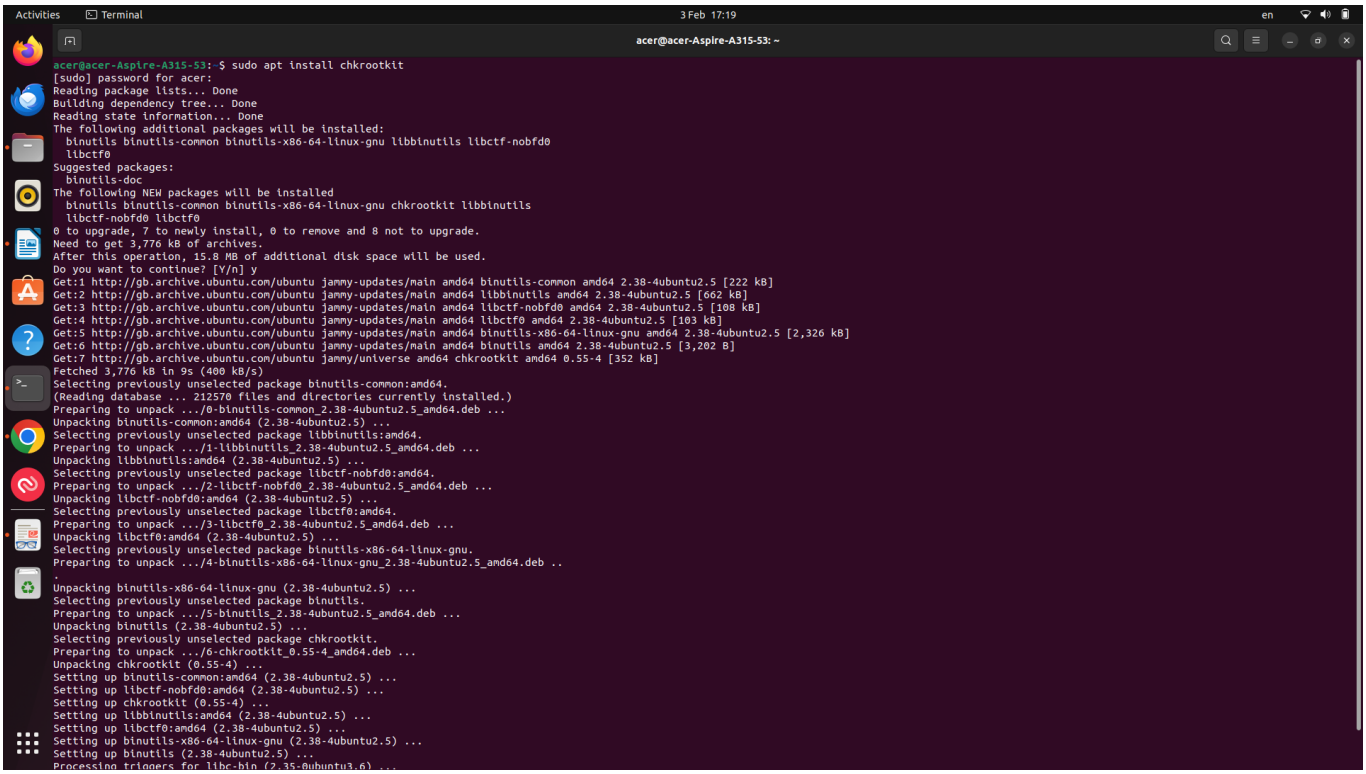
cd MySA



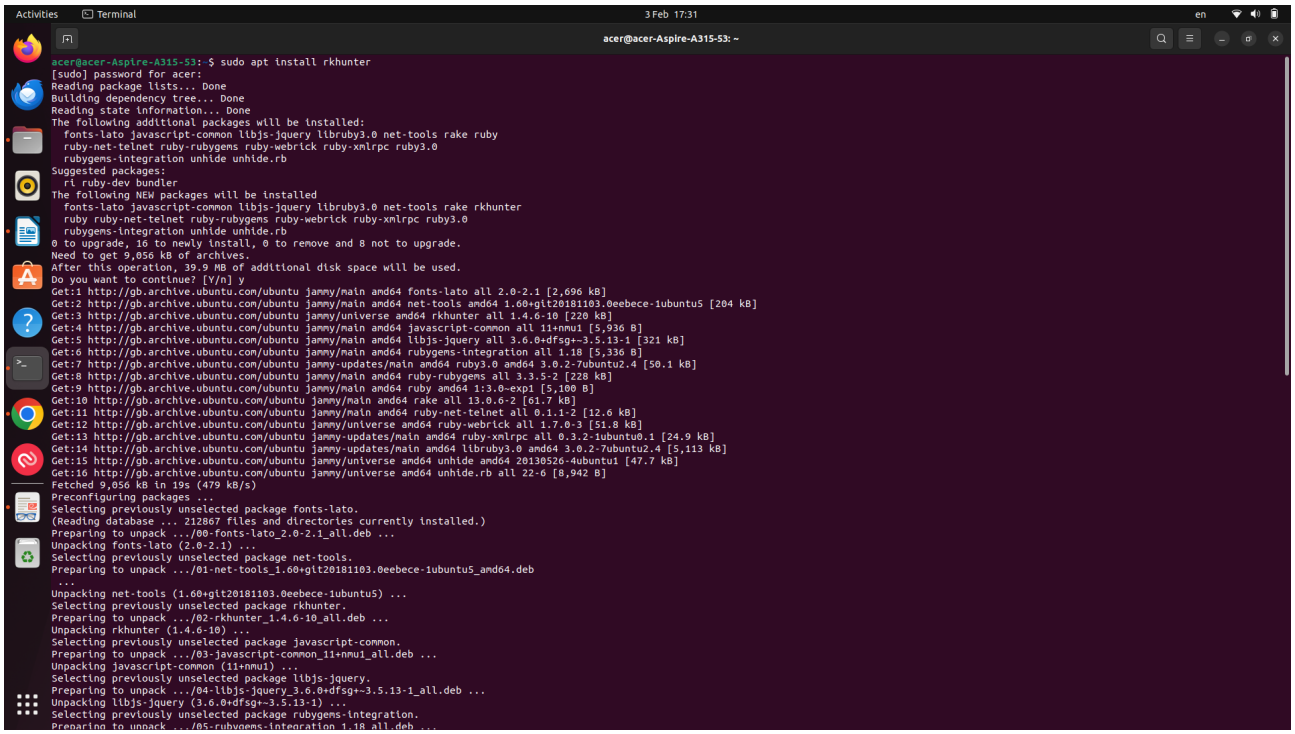
10. Install Chkrootkit – A Linux Rootkit Scanner

The chkrootkit tool I installed using the following command:

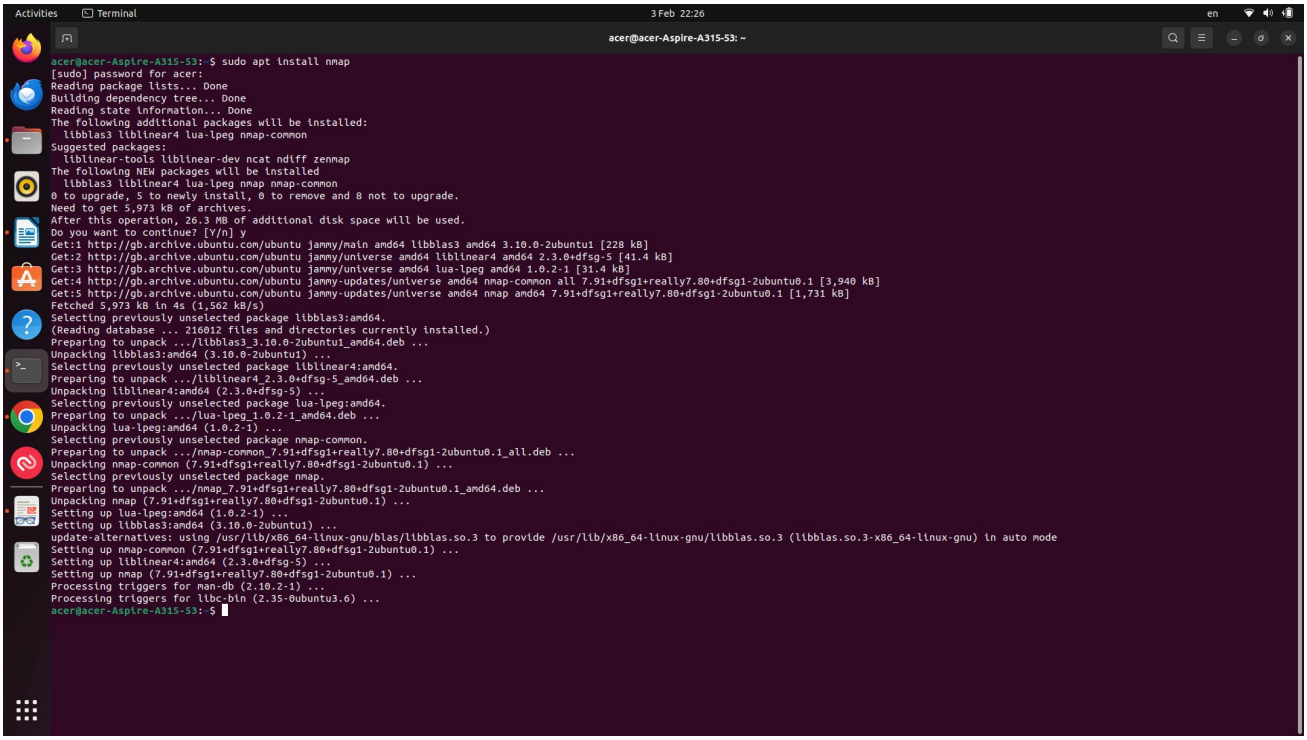
sudo apt install chkrootkit



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



12.I installed Nmap on Ubuntu 22.04:
sudo apt install nmap


Activities
Terminal
3 Feb 22:26
en
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:
libblas3 liblinear4 lua-lpeg nmap-common
Suggested packages:
liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed
libblas3 liblinear4 lua-lpeg nmap 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, 26.3 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 libblas3 amd64 3.10.0-2ubuntu1 [228 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 liblinear4 amd64 2.3.0+dfsg-5 [41.4 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 lua-lpeg amd64 1.0.2-1 [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 ... 216012 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 liblinear4:amd64.
Preparing to unpack .../liblinear4_2.3.0+dfsg-5_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-5) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
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 lua-lpeg:amd64 (1.0.2-1) ...
Setting up libblas3:amd64 (3.10.0-2ubuntu1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/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 liblinear4:amd64 (2.3.0+dfsg-5) ...
Setting up nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
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

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

		main/index.html var/www/ your_domain/ index.html	that the server responds to HTTP requests	
Testing MySQL Service	The MySQL service should be running and accessible	Test by command 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 nano /var/www/my_domain/info.php /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 create the PHP script that connected to MySQL and query for content. 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: 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: 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: 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: the mysat.sql file with root permission and output to the MySAT.htm fi le	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 : 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: `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: 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>
```

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.

```
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:~$
```

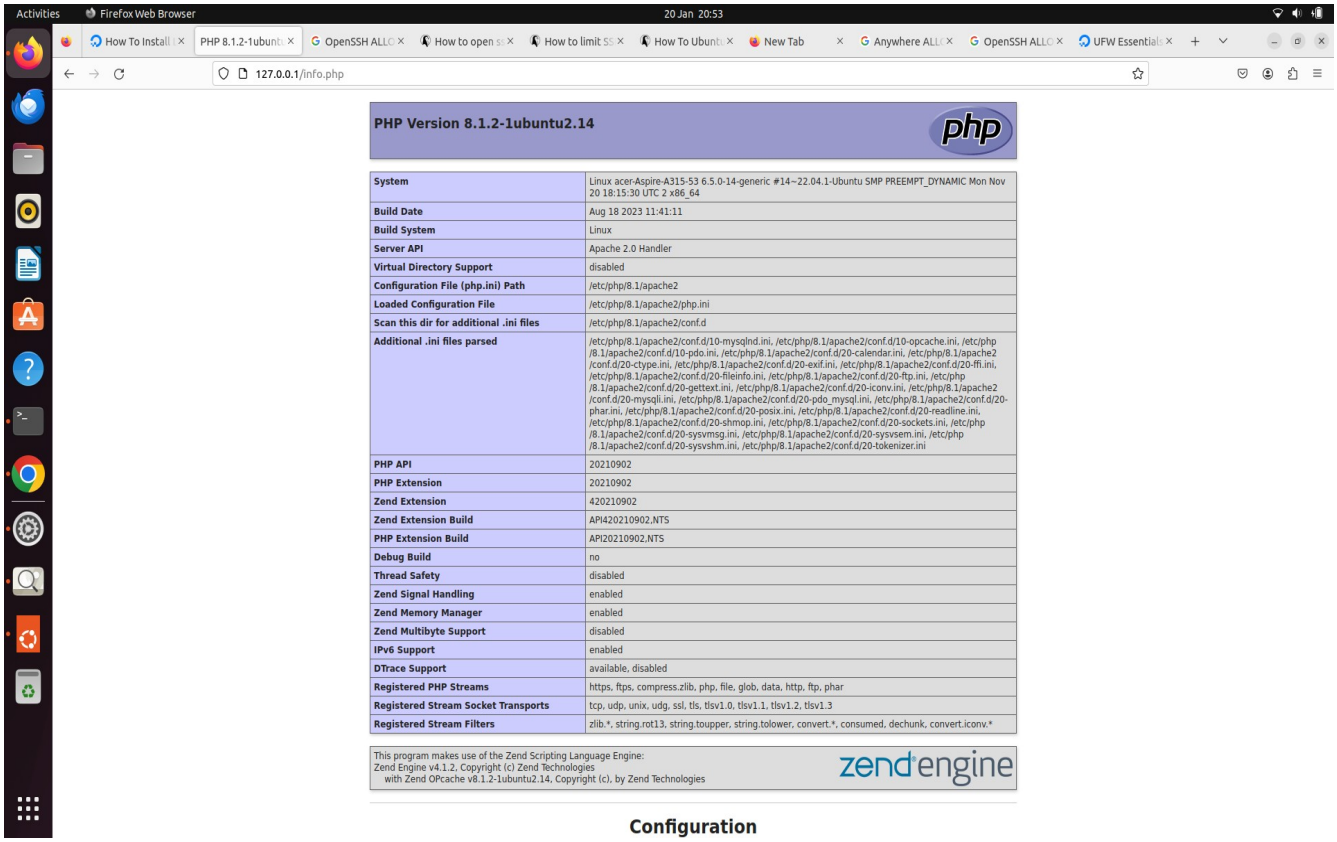
This test confirmed that MySQL is running without errors and that it's possible to connect to the MySQL server.

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
<?php
phpinfo();
```

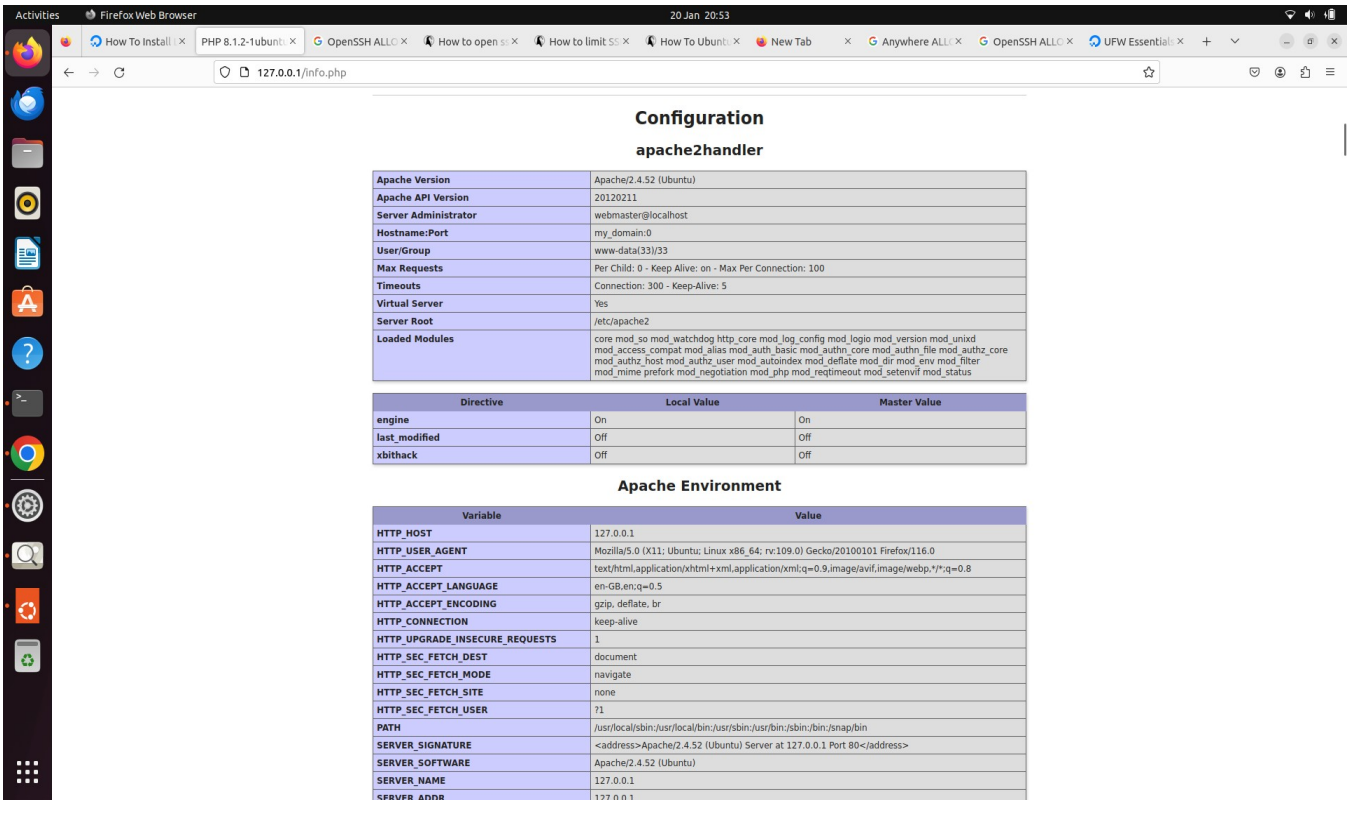


PHP Version 8.1.2-1ubuntu2.14

System	Linux acer-Aspire-A315-53 6.5.0-14-generic #14~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Mon Nov 20 18:15:30 UTC 2 x86_64
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	/etc/php/8.1/apache2/conf.d
Additional .ini files parsed	/etc/php/8.1/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.1/apache2/conf.d/10-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-mysqli.ini, /etc/php/8.1/apache2/conf.d/20-pdo_mysql.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-sysvsem.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	API420210902,NTS
PHP Extension Build	API20210902,NTS
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

Configuration



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_unixd mod_access_compat mod_alias mod_auth_basic 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.

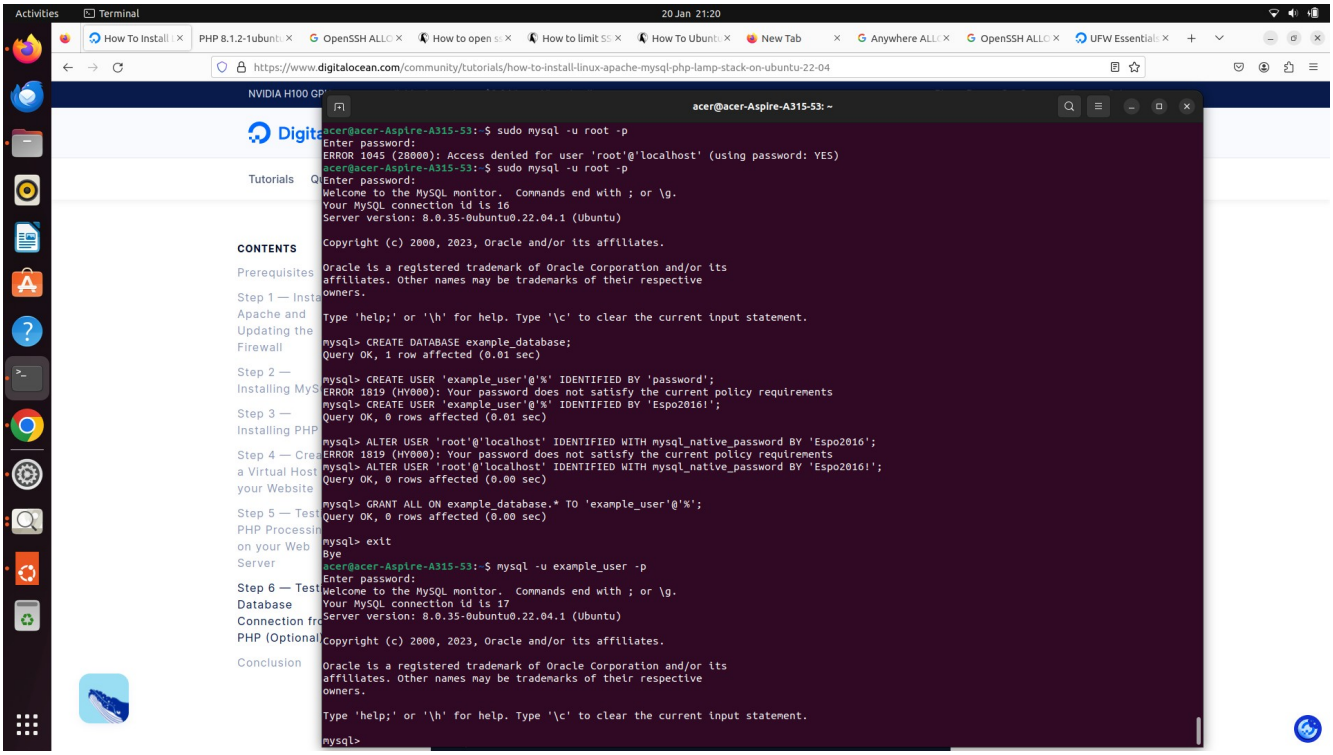
CREATE USER 'example_user'@'%' IDENTIFIED BY 'password';
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';
GRANT ALL ON example_database.* TO 'example_user'@'%';
exit
I tested if the new user has the proper permissions by logging in to the MySQL console , using the custom user credentials.

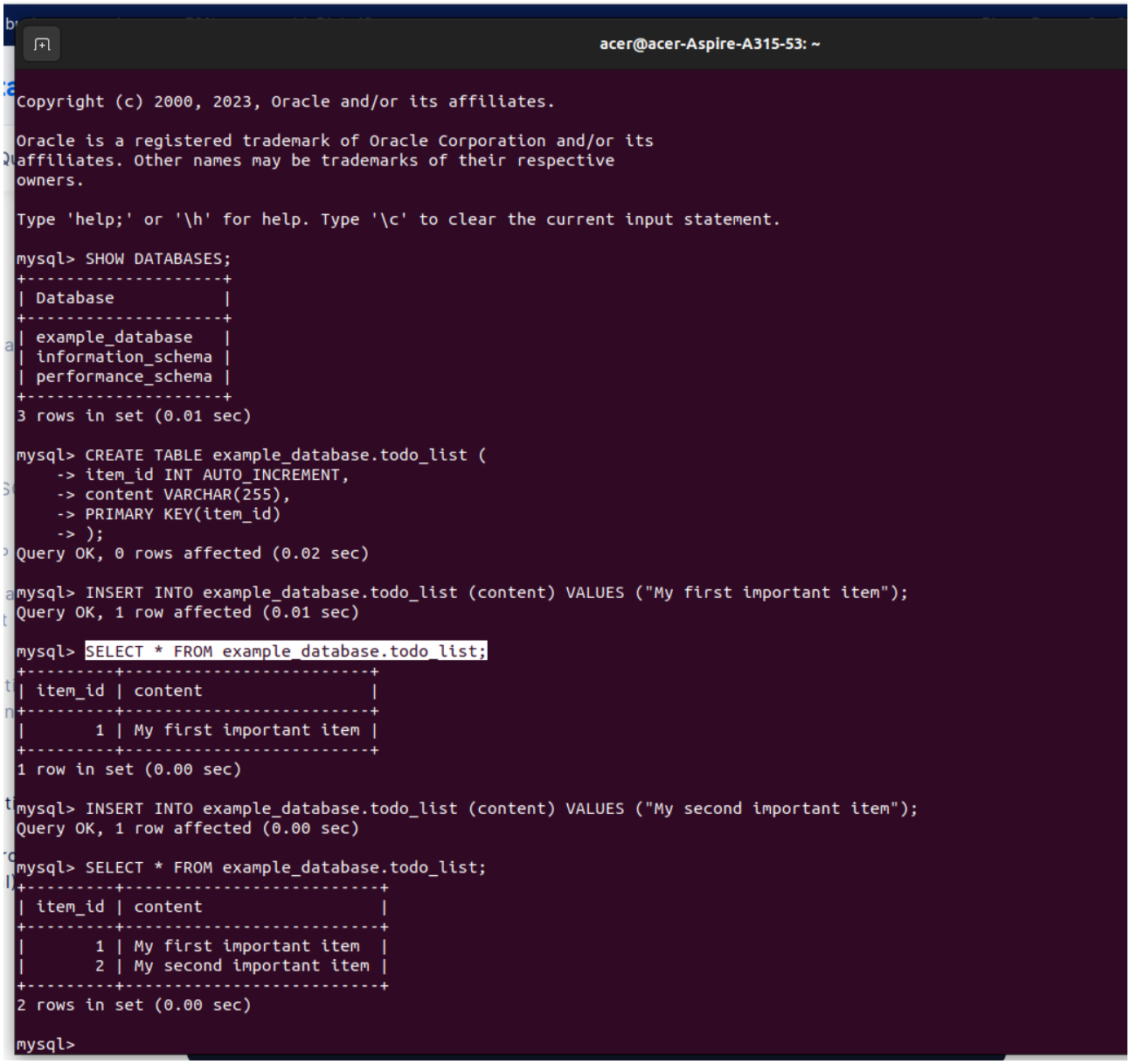
After logging in to the MySQL console, I tested that I have access to the example_database database:

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:

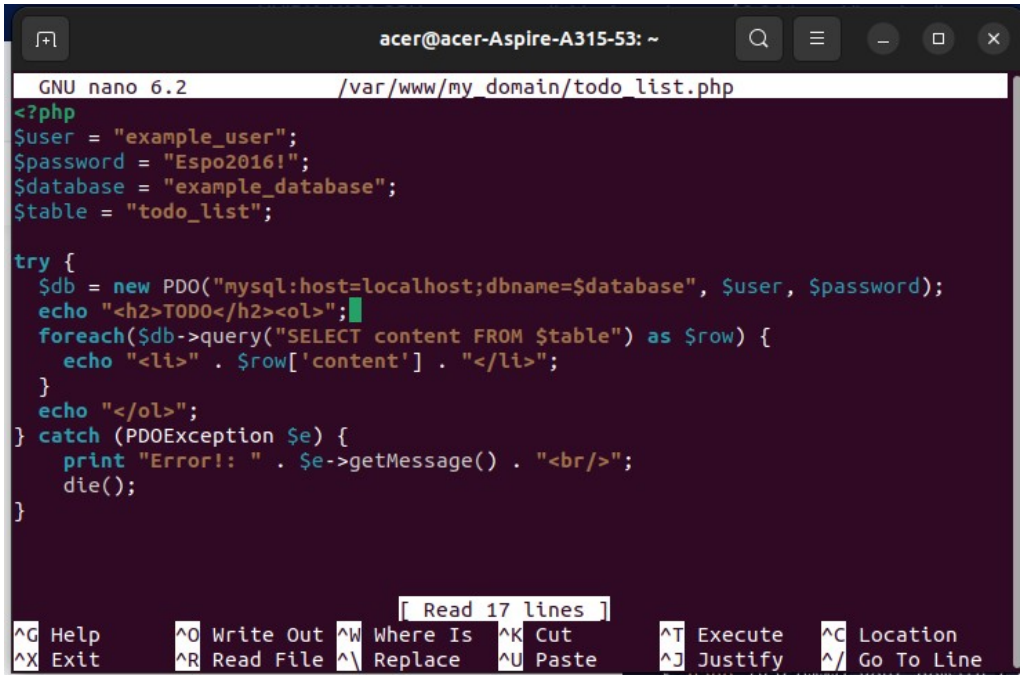
SELECT * FROM example_database.todo_list;



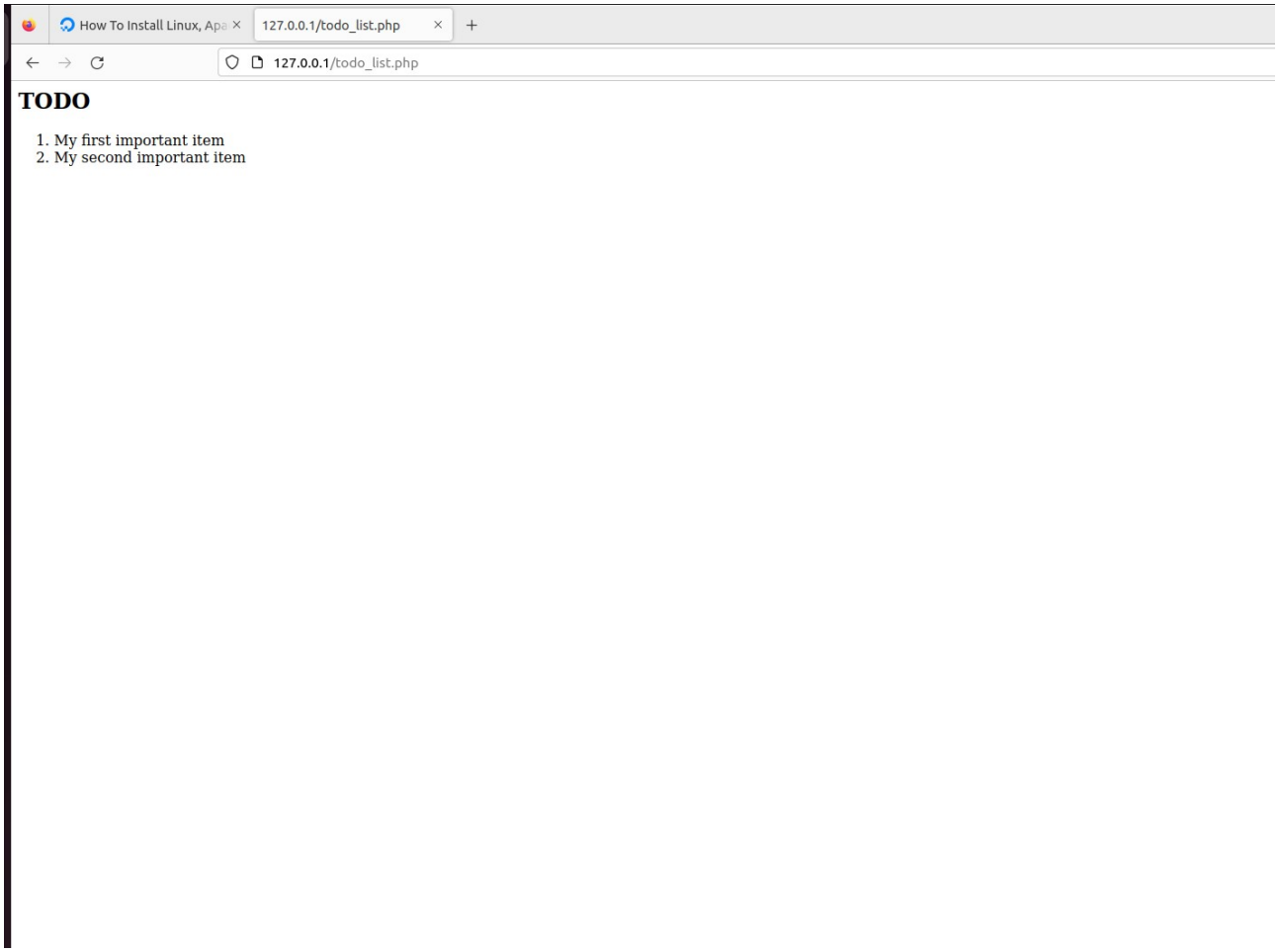


Then I can created the PHP script that connected to MySQL and query for content.

nano /var/www/my_domain/todo_list.php



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

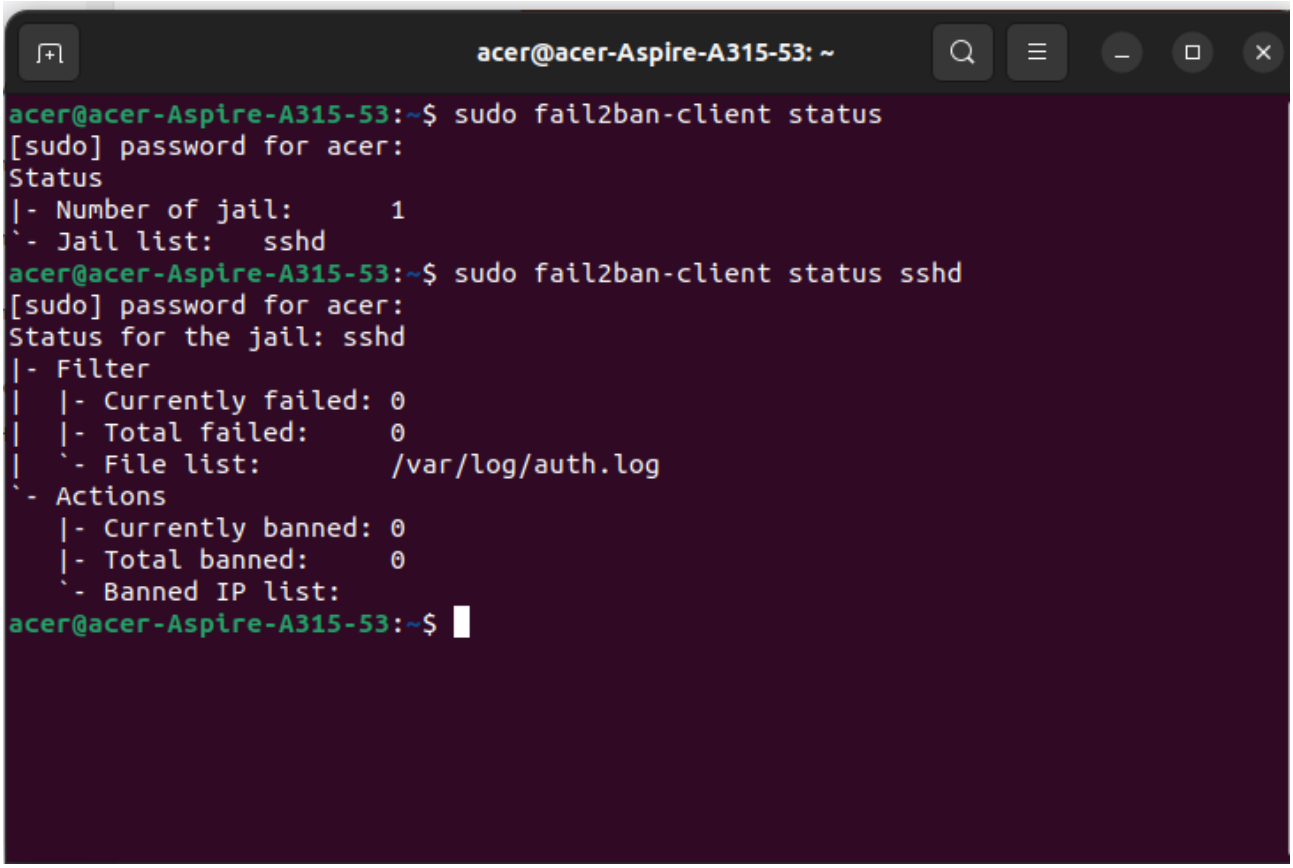
One of the greatest advantages of using Fail2Ban the ability to monitor all the failed authentication attempts and the various blocked IP addresses.

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



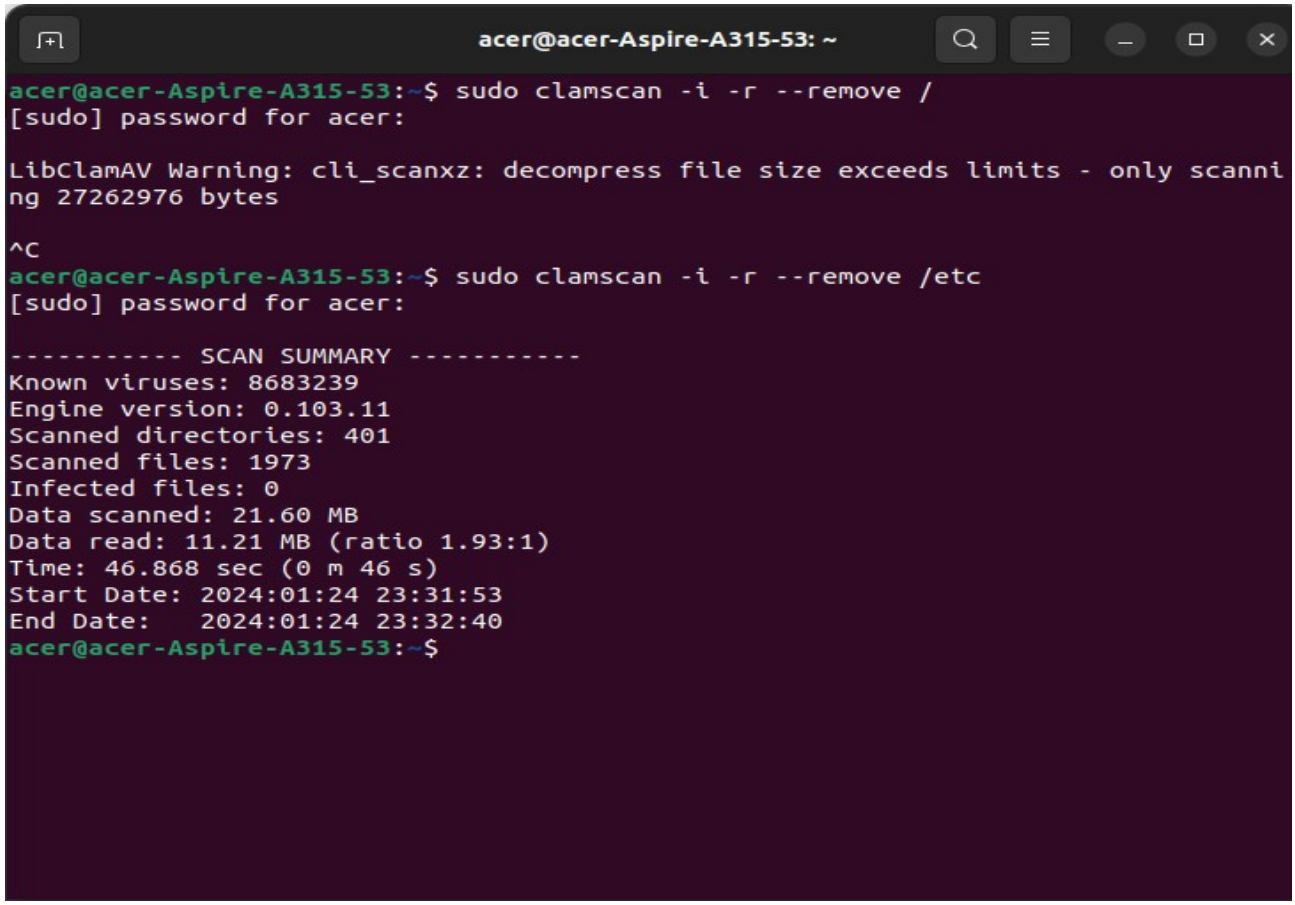
This test show 0 of failed and banned IP addresses.

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.



This test show 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 ]
      - uuidd.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 HARDENED]
- Mount options of /dev/shm [PARTIALLY HARDENED]
- Mount options of /run [HARDENED]
- 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]

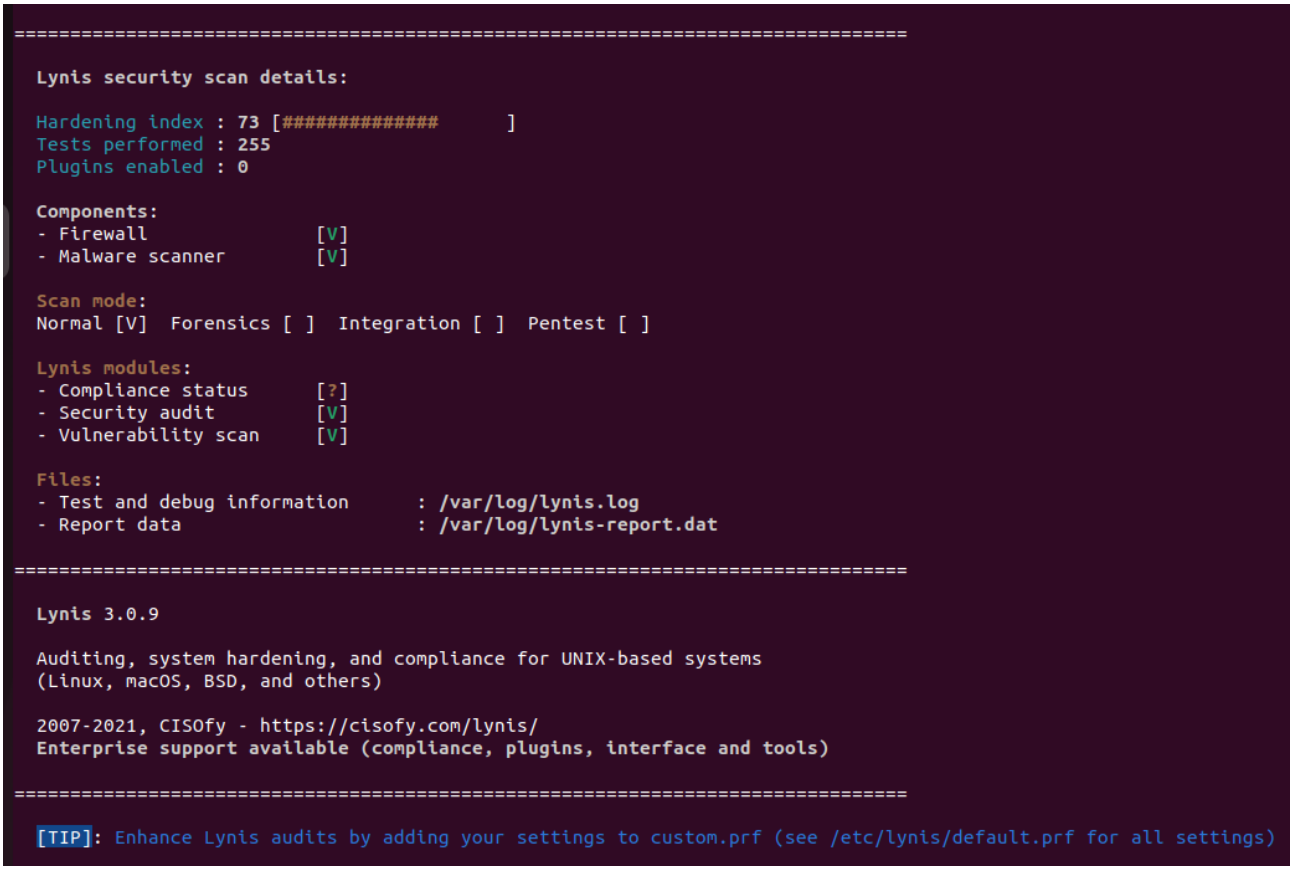
[+] File Permissions

- 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.



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://cisofy.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://cisofy.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://cisofy.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 [KRNL-5820]
https://cisofy.com/lynis/controls/KRNL-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/

* 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/

* 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/

* 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/

 * 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

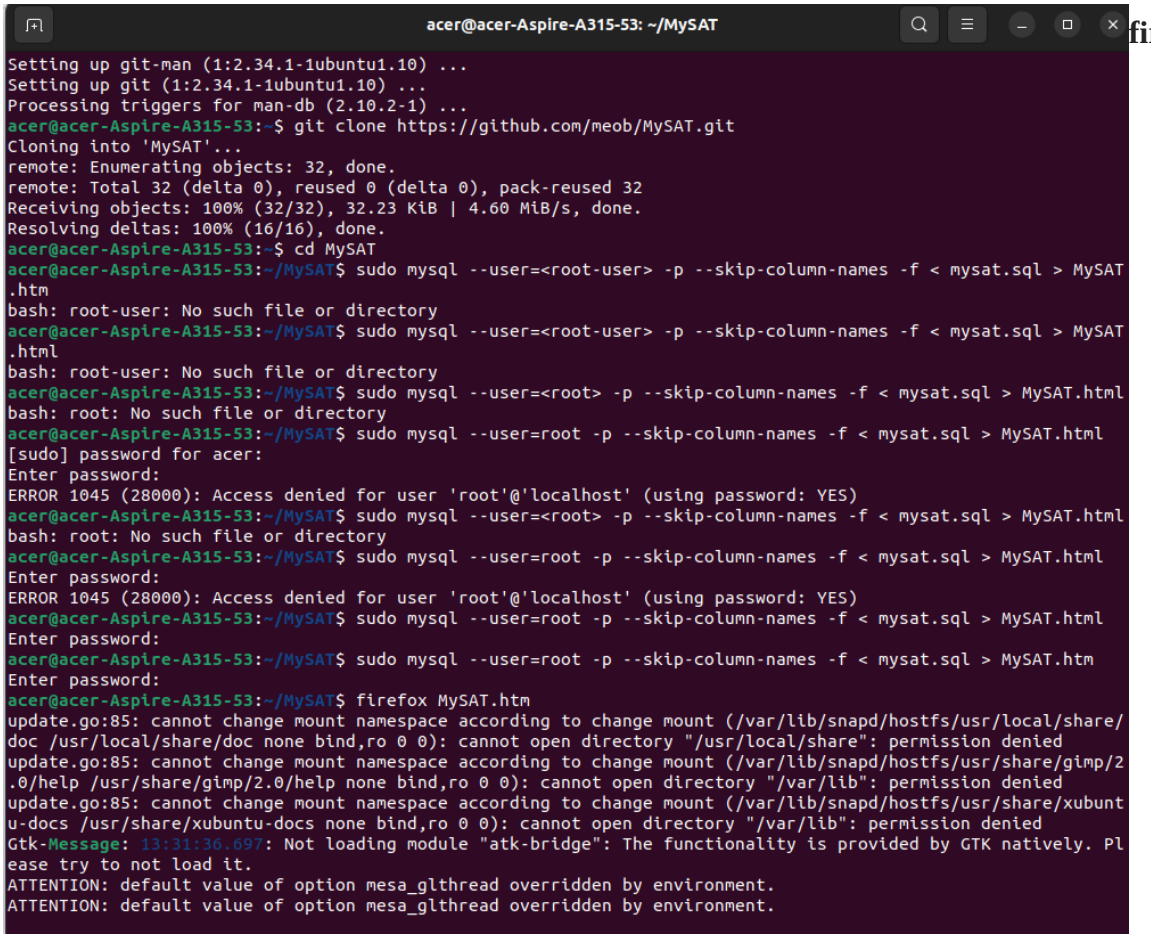
This performs a pentest on the system and outputs a hardening index score that reflects the overall security posture of the system. It also outputted similar recommendations and patches that can be implied to improve the score.

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:



firefox 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		
Any host access	Fail	Users can connect from everywhere	example_user
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	Fail	Not dedicated datadir	
Memcache plugin	Pass		
secure_file_priv	Pass		
Master Info	Pass		
Automatic User Creation	Fail	Not disabled	
Password lenght	Fail	Too short	NULL
Password policy	Fail	Not secure	
Performance statistics	Fail	my2 collector not found	
local_infile	Pass		
Symbolic Links	Pass		
Skip grant	Evaluate	Do not enable skip_grant_tables	
Patching			
MySQL update	Fail	8.0.35-0ubuntu0.22.04.1	
MySAT update	Fail	1.0.2	
GDPR Countdown			
Days since promulgation	Pass	2829	
Days since application	Pass	2071	

DB Configuration

Database Summary	
Item	**Value**
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

Users								
User	**Host**	SL IUD CDGRIA CCS CAE RR SSPFSR	**Select**	**Execute**	**Grant**	**Expired**	**Password lifetime**	**Locked**

Data Masking		
miXen package	Fail	miXen data masking package not found
Secure configuration		
Version Check		
MySQL version	Fail	8.0

Database Summary	
Item	**Value**
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

Users									
User	**Host**	**SL IUD CDGRIA CCS CAE RR SSPFSR**	**Select**	**Execute**	**Grant**	**Expired**	**Password lifetime**	**Locked**
debian-sys-maint	localhost	YY YYY YYYYYY YYY YYY YY YYYYYY	Y	Y	Y	N	NULL	N
example_user	%	NN NNN NNNNNN NNN NNN NN NNNNNN	N	N	N	N	NULL	N
mysql.infoschema	localhost	YN NNN NNNNNN NNN NNN NN NNNNNN	Y	N	N	N	NULL	Y
mysql.session	localhost	NN NNN NNNNNN NNN NNN NN YYNNNN	N	N	N	N	NULL	Y
mysql.sys	localhost	NN NNN NNNNNN NNN NNN NN NNNNNN	N	N	N	N	NULL	Y
root	localhost	YY YYY YYYYYY YYY YYY YY YYYYYY	Y	Y	Y	N	NULL	N

Schema/Object Matrix								
Database	**Tables**	**Indexes**	**Routines**	**Triggers**	**Views**	**Primary Keys**	**Foreign Keys**	**All**
example_database	1	1	0	0	0	1	0	3
information_schema	79	0	0	0	0	0	0	79
mysql	37	38	0	0	0	35	0	110
performance_schema	111	93	0	0	0	59	0	263
sys	101	1	48	2	100	1	0	253
NULL	329	133	48	2	100	96	0	708

Space Usage							
Database	**Row#**	**Data size**	**Index size**	**Total size**	**MyISAM**	**InnoDB**	**Created**
example_database	2	16,384	0	16,384	0	16,384	2024-01-20
information_schema	0	0	0	0	0	0	2024-01-20
mysql	4,329	2,408,448	344,064	2,752,512	0	2,752,512	2024-01-20
performance_schema	2,959,379	0	0	0	0	0	2024-01-20
sys	6	16,384	0	16,384	0	16,384	2024-01-20
NULL	2,963,716	2,441,216	344,064	2,785,280	0	2,785,280	2024-01-20

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
mysql	replication_asynchronous_connection_failover	T	InnoDB	32,768	0

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
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	State
5	event_scheduler	localhost	NULL	Daemon	251571	Waiting on empty queue
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 Representativeness: 100.00 %

Schema	Text	Count	Sum Timer
information_schema	SELECT IF (COUNT (*) = ?, ...) FROM `performance_schema` . `events_statements_summary_by_digest` WHERE `DIGEST_TEXT` LIKE ? OR ` ...	2	62866817800
information_schema	SELECT ?, ... , `version` ( ) UNION SELECT ?, ... , MIN (`create_time`) FROM TABLES UNION SELECT ?, ... , `date_format` (DATE_SUB ...	2	38867381900
information_schema	SELECT ? , `sk` , ? , SUM (IF (`otype` = ?, ...)) , ? , SUM (IF (`otype` = ?, ...)) , ? , SUM (IF (`otype` = ?, ...)) , ...	2	12445580300
information_schema	SELECT IF (COUNT (*) > ?, ...) FROM `INFORMATION_SCHEMA` . `TABLES` WHERE `CREATE_OPTIONS` LIKE ? ...	2	6153273100
information_schema	SELECT IF (`variable_value` != ?, ...) FROM `performance_schema` . `global_variables` WHERE `variable_name` = ? ...	4	4197674400

Host Cache

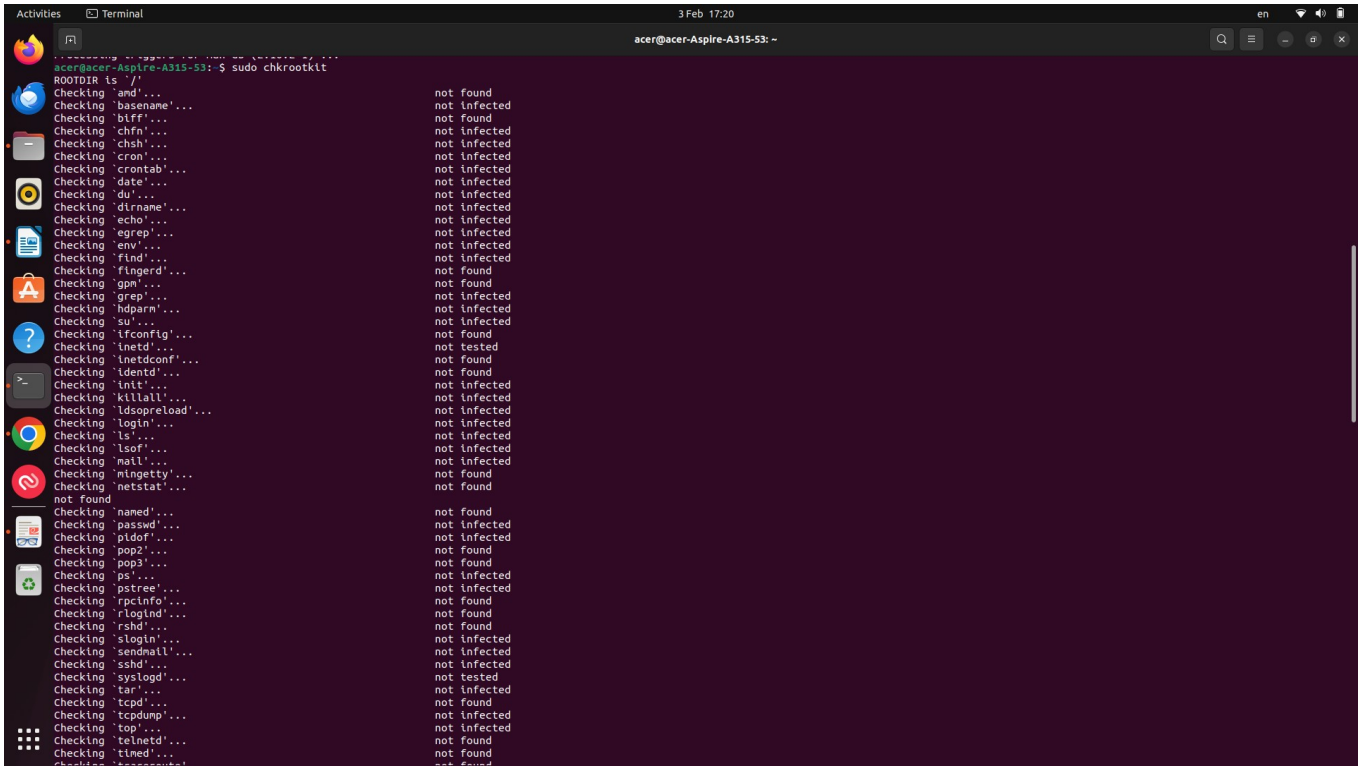
Host	IP	Validated	SUM Errors	First Seen	Last Seen	Last Error Seen	# Handshake Err.	# Authentication Err.	# ACL Err.

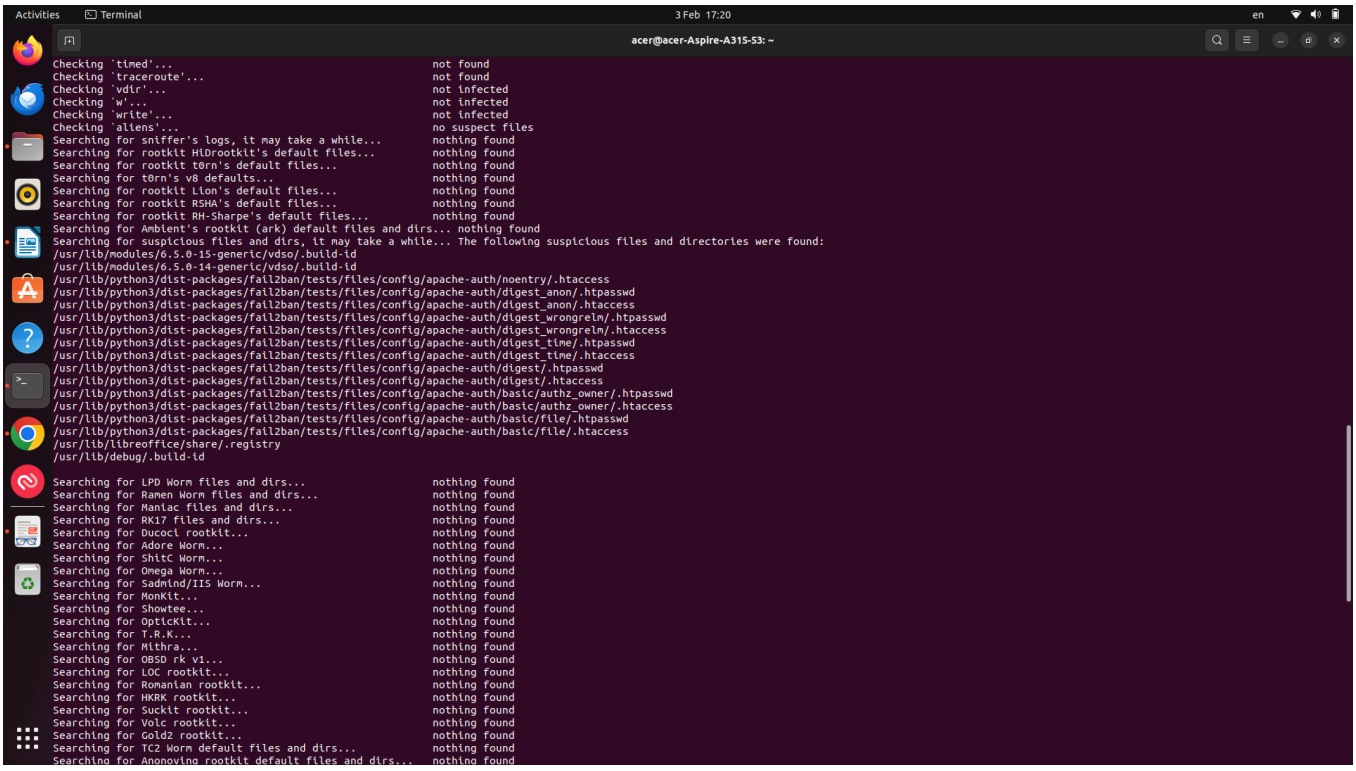
MySQL Parameters

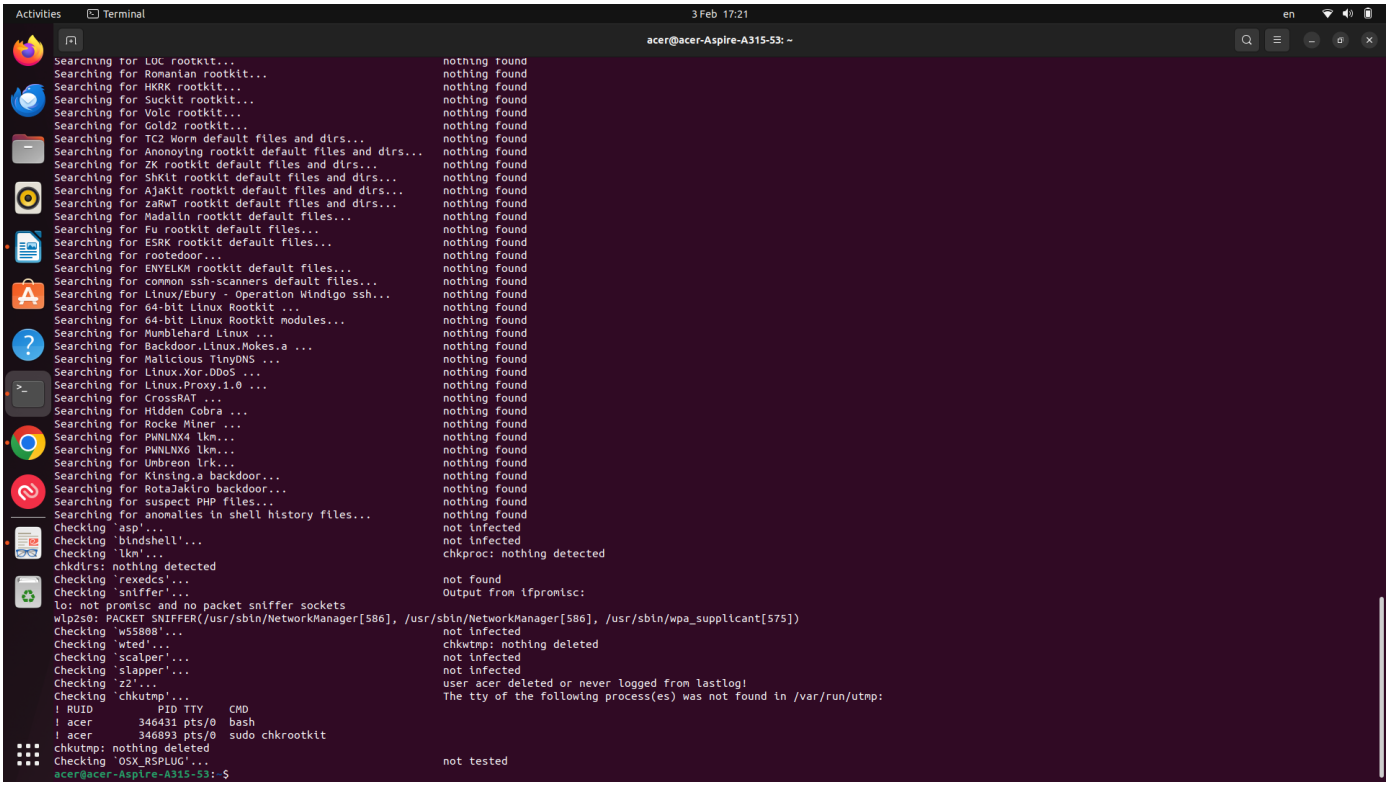
Parameter	Value
activate_all_roles_on_login	OFF
admin_address	
admin_port	33062
admin_ssl_ca	
admin_ssl_capath	
admin_ssl_cert	
admin_ssl_cipher	
admin_ssl_crl	
admin_ssl_crlpath	
admin_ssl_key	
admin_tls_ciphersuites	
admin_tls_version	TLSv1.2, TLSv1.3
authentication_policy	*, ,
auto_generate_certs	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_cache_size	32768

I checked my server with Chkrootkit

I run sudo chkrootkit



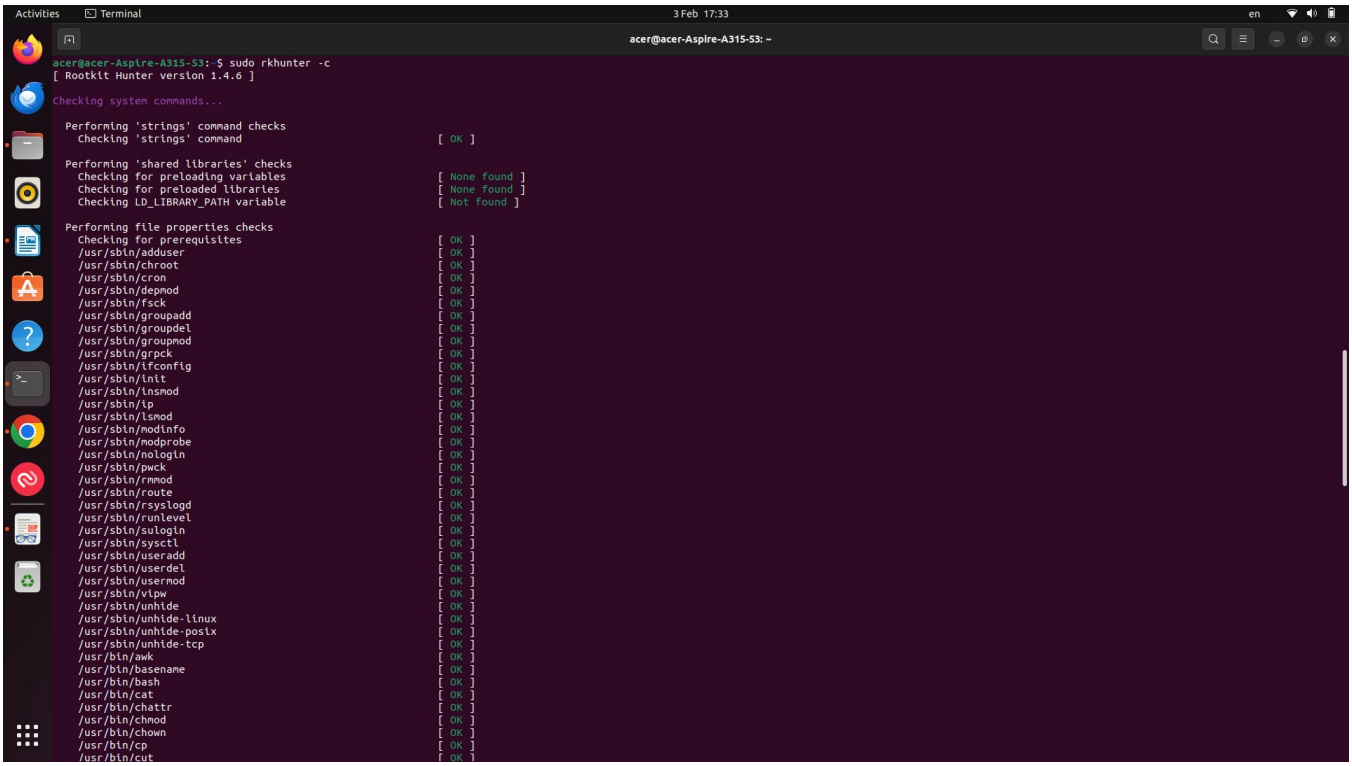


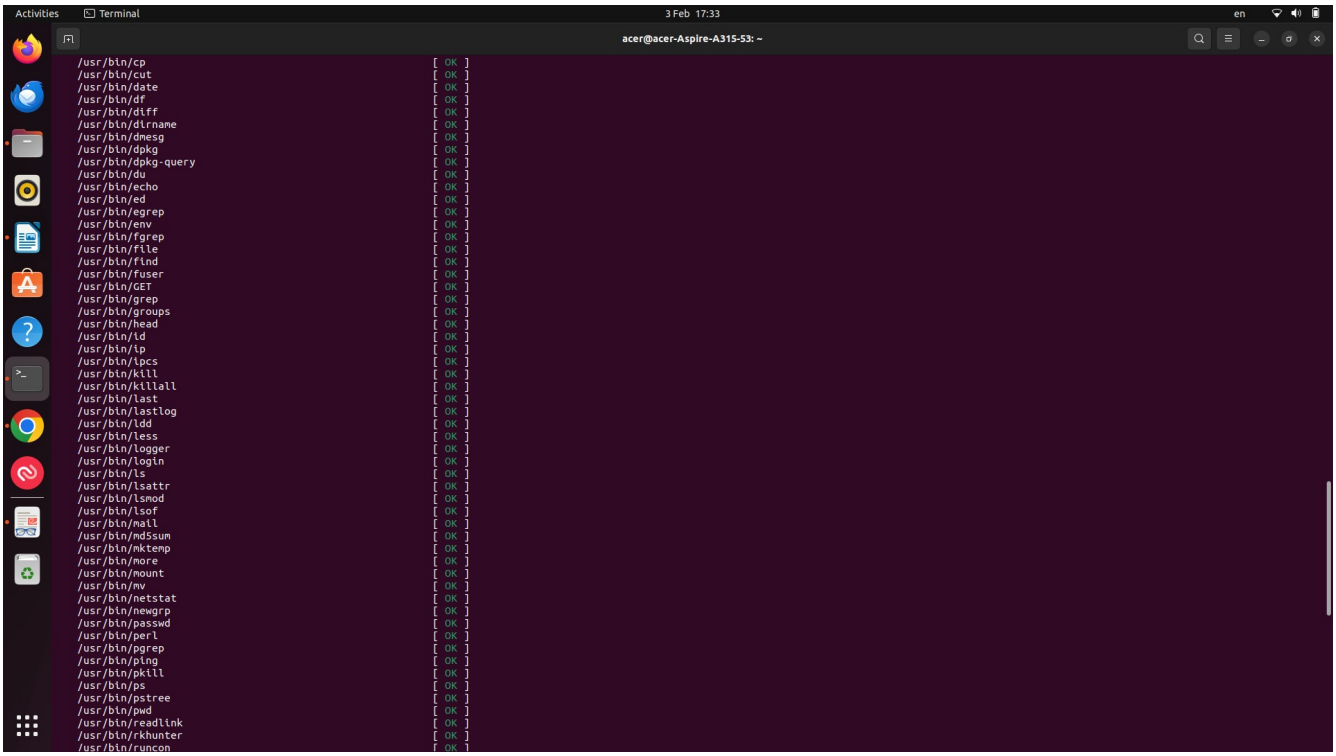


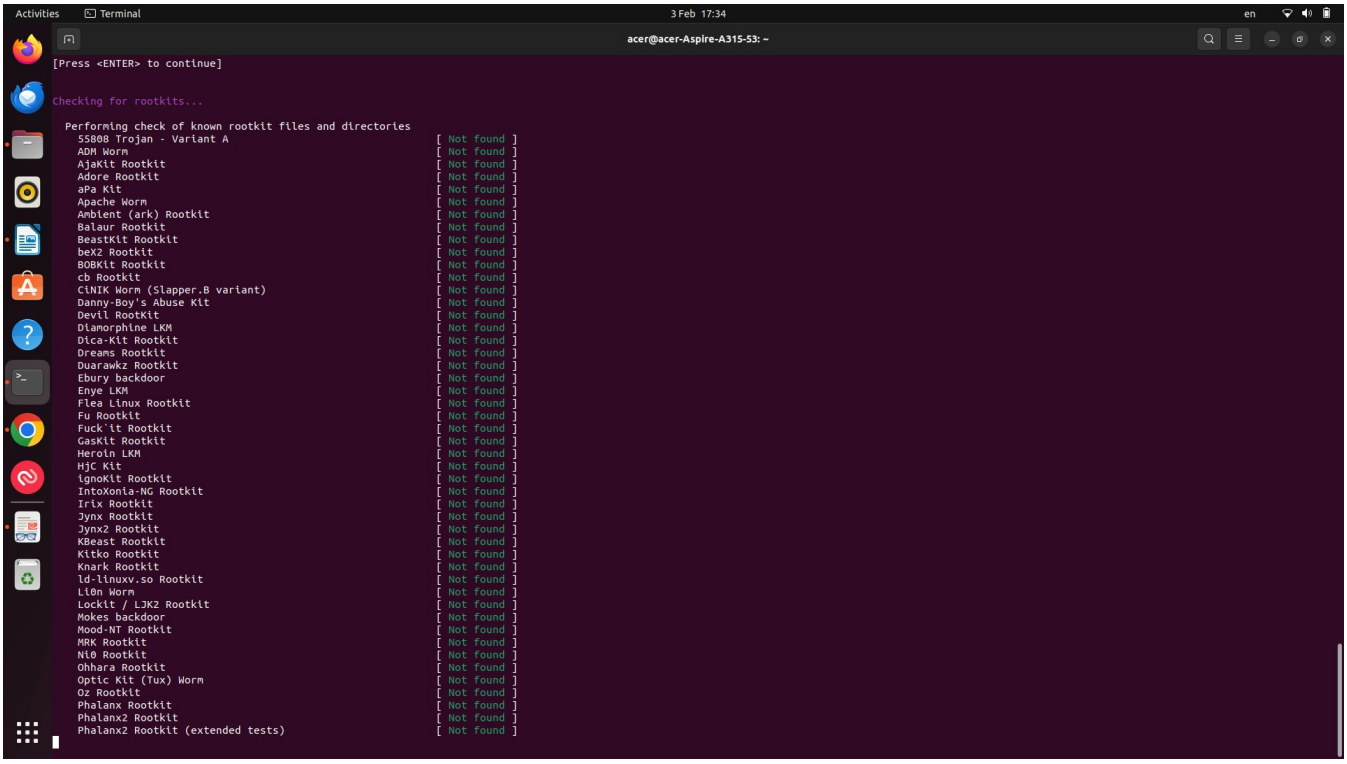
This test show that chkrootkit not found signs that the system is infected with a ‘rootkit’.

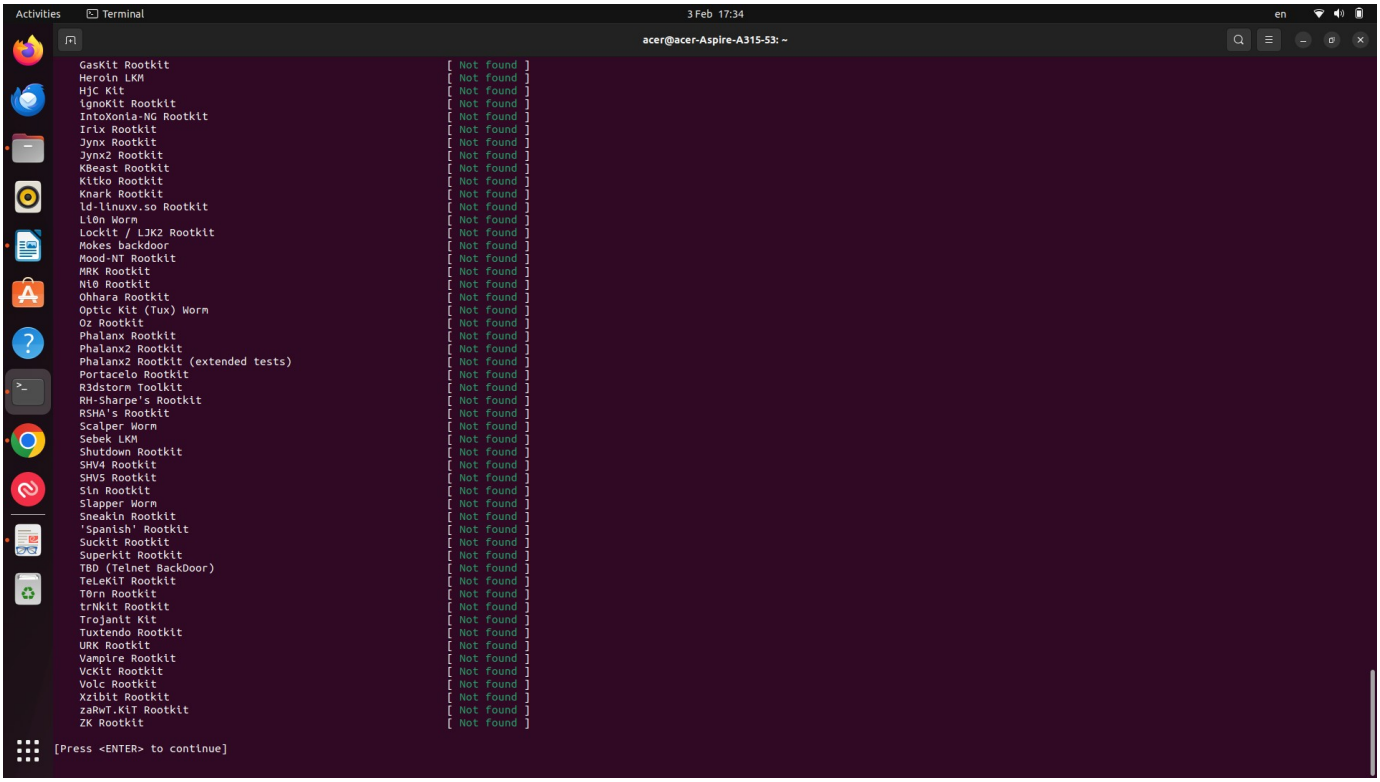
I **checked my server with rkhunter** run the following command:

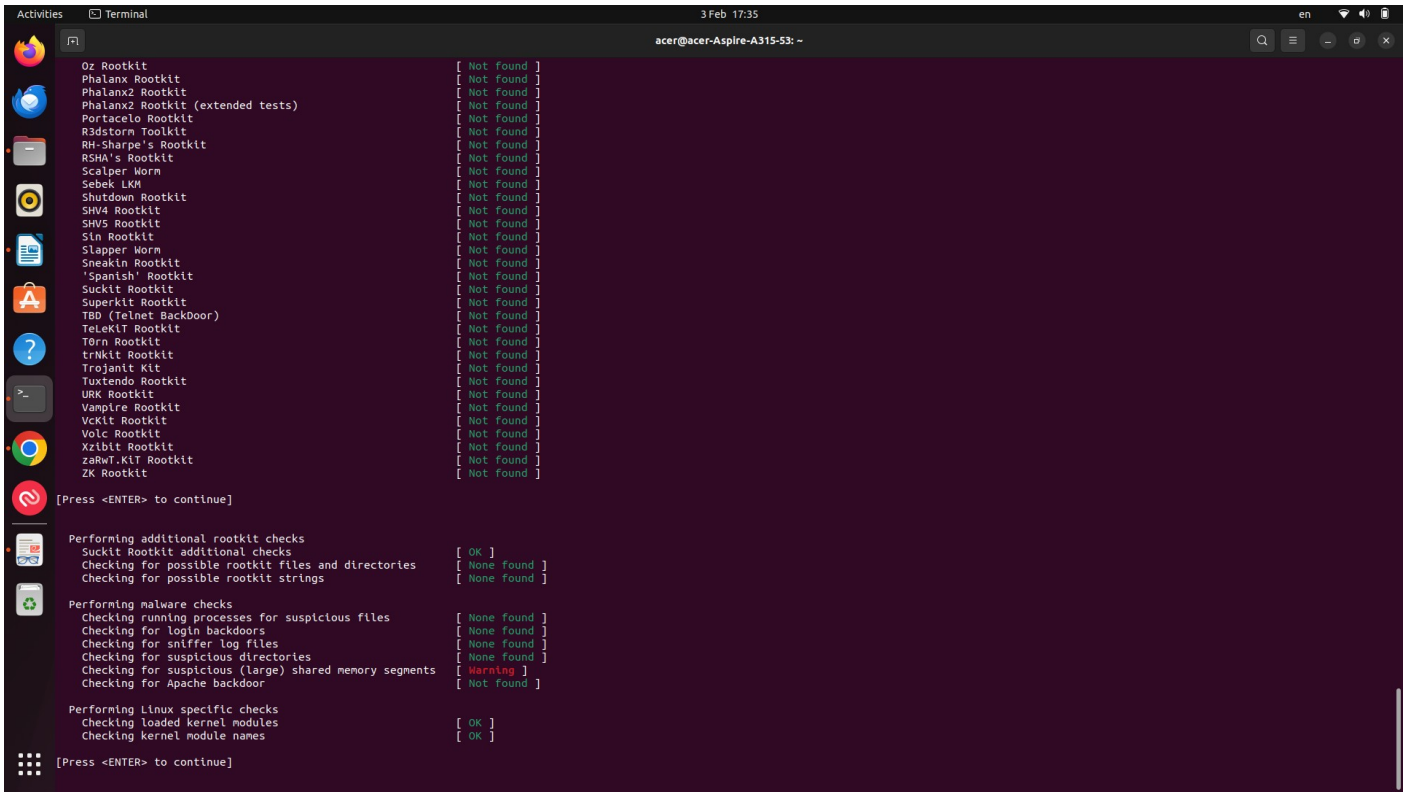
sudo rkhunter -c

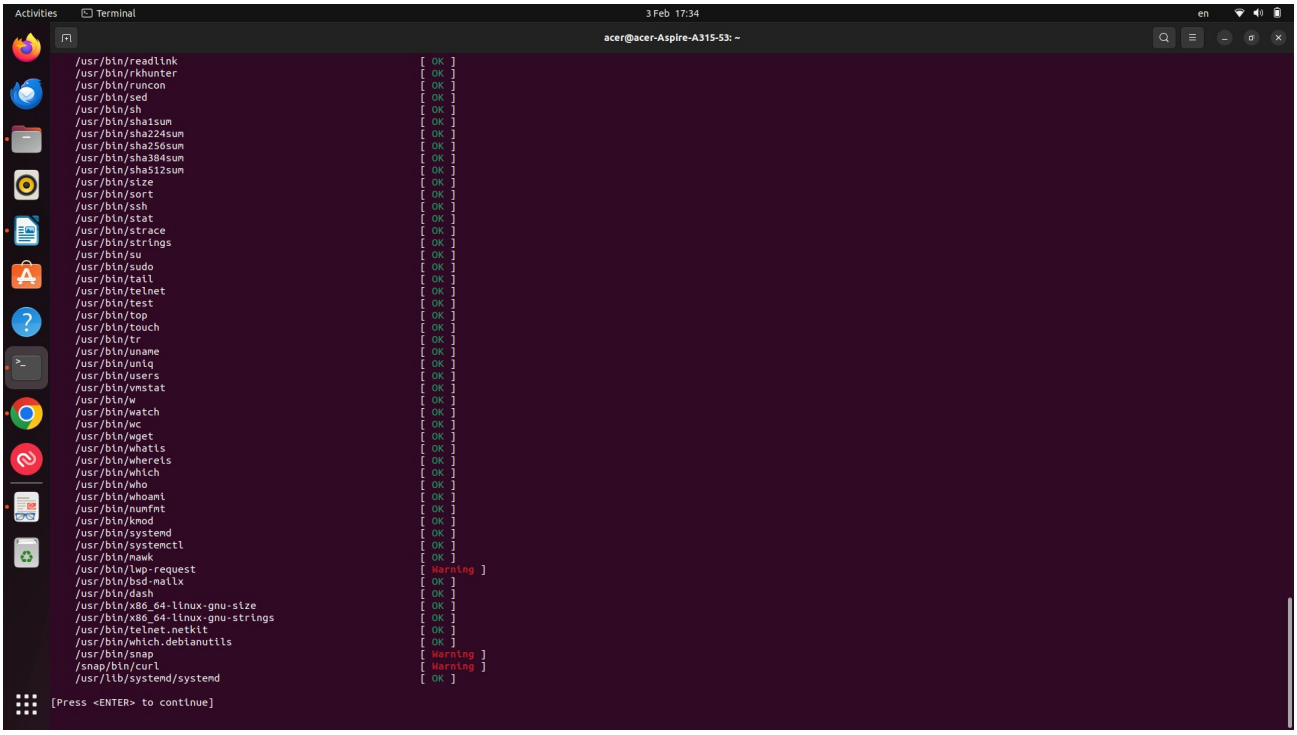



Activities
Terminal
3 Feb 17:33
en
acer@acer-Aspire-A315-53: ~
/usr/bin/cp [OK]
/usr/bin/cut [OK]
/usr/bin/date [OK]
/usr/bin/df [OK]
/usr/bin/diff [OK]
/usr/bin/dirname [OK]
/usr/bin/dmesg [OK]
/usr/bin/dpkg [OK]
/usr/bin/dpkg-query [OK]
/usr/bin/du [OK]
/usr/bin/echo [OK]
/usr/bin/ed [OK]
/usr/bin/egrep [OK]
/usr/bin/env [OK]
/usr/bin/fgrep [OK]
/usr/bin/file [OK]
/usr/bin/find [OK]
/usr/bin/fuser [OK]
/usr/bin/GET [OK]
/usr/bin/grep [OK]
/usr/bin/groups [OK]
/usr/bin/head [OK]
/usr/bin/id [OK]
/usr/bin/ip [OK]
/usr/bin/ipcs [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/ps [OK]
/usr/bin/pstree [OK]
/usr/bin/pwd [OK]
/usr/bin/readlink [OK]
/usr/bin/rkhunter [OK]
/usr/bin/runcon [OK]

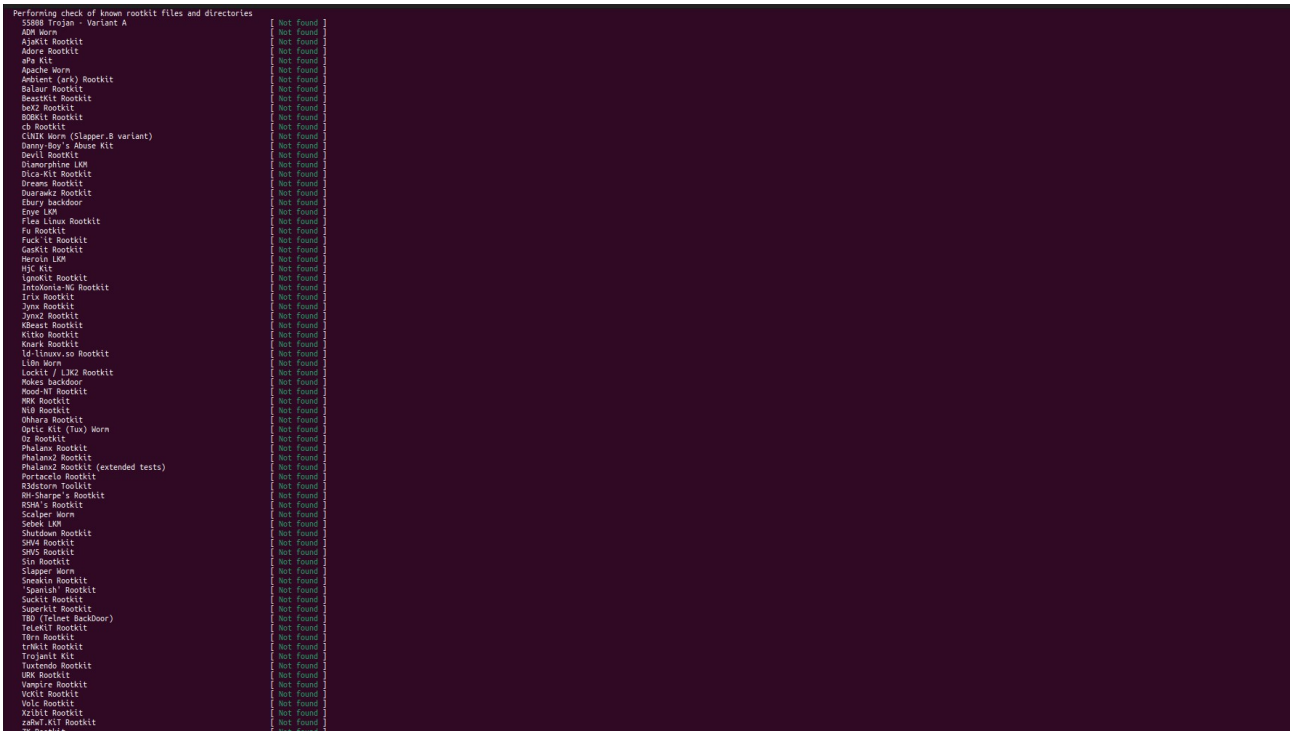

Activities
Terminal
3 Feb 17:34
en
acer@acer-Aspire-A315-53: ~
[Press <ENTER> to continue]
Checking for rootkits...
Performing check of known rootkit files and directories
55808 Trojan - Variant A [Not found]
ADM Worm [Not found]
AjaKit Rootkit [Not found]
Adore Rootkit [Not found]
aPa Kit [Not found]
Apache Worm [Not found]
Ambient (ark) Rootkit [Not found]
Balaur Rootkit [Not found]
BeastKit Rootkit [Not found]
beX2 Rootkit [Not found]
BOBKit 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]
Diamorphine LKM [Not found]
Dica-Kit Rootkit [Not found]
Dreams Rootkit [Not found]
Duarawkz Rootkit [Not found]
Ebury backdoor [Not found]
Enye LKM [Not found]
Flea Linux Rootkit [Not found]
Fu Rootkit [Not found]
Fuck'it Rootkit [Not found]
GasKit Rootkit [Not found]
Heroin LKM [Not found]
HjC Kit [Not found]
ignoKit Rootkit [Not found]
IntoXonia-NG Rootkit [Not found]
Irix Rootkit [Not found]
Jynx Rootkit [Not found]
Jynx2 Rootkit [Not found]
KBeast Rootkit [Not found]
Kitko Rootkit [Not found]
Knark Rootkit [Not found]
ld-linuxv.so Rootkit [Not found]
Li0n Worm [Not found]
Lockit / LJK2 Rootkit [Not found]
Mokes backdoor [Not found]
Mood-NT Rootkit [Not found]
MRK Rootkit [Not found]
Ni0 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
en
acer@acer-Aspire-A315-53: ~
GasKit Rootkit [Not found]
Heroin LKM [Not found]
HjC Kit [Not found]
IgnoKit Rootkit [Not found]
IntoXonia-NG Rootkit [Not found]
Irix Rootkit [Not found]
Jynx Rootkit [Not found]
Jynx2 Rootkit [Not found]
KBeast Rootkit [Not found]
Kitko Rootkit [Not found]
Knark Rootkit [Not found]
ld-linuxv.so Rootkit [Not found]
Li0n Worm [Not found]
Lockit / LJK2 Rootkit [Not found]
Mokes backdoor [Not found]
Mood-NT Rootkit [Not found]
MRK Rootkit [Not found]
Ni0 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]
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]
SHV5 Rootkit [Not found]
Sin 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]
zaRwT.KiT Rootkit [Not found]
ZK Rootkit [Not found]
[Press <ENTER> to continue]


Activities
Terminal
3 Feb 17:35
en
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]
SHV5 Rootkit [Not found]
Sin 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]
zaRwT.KiT 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 running 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]



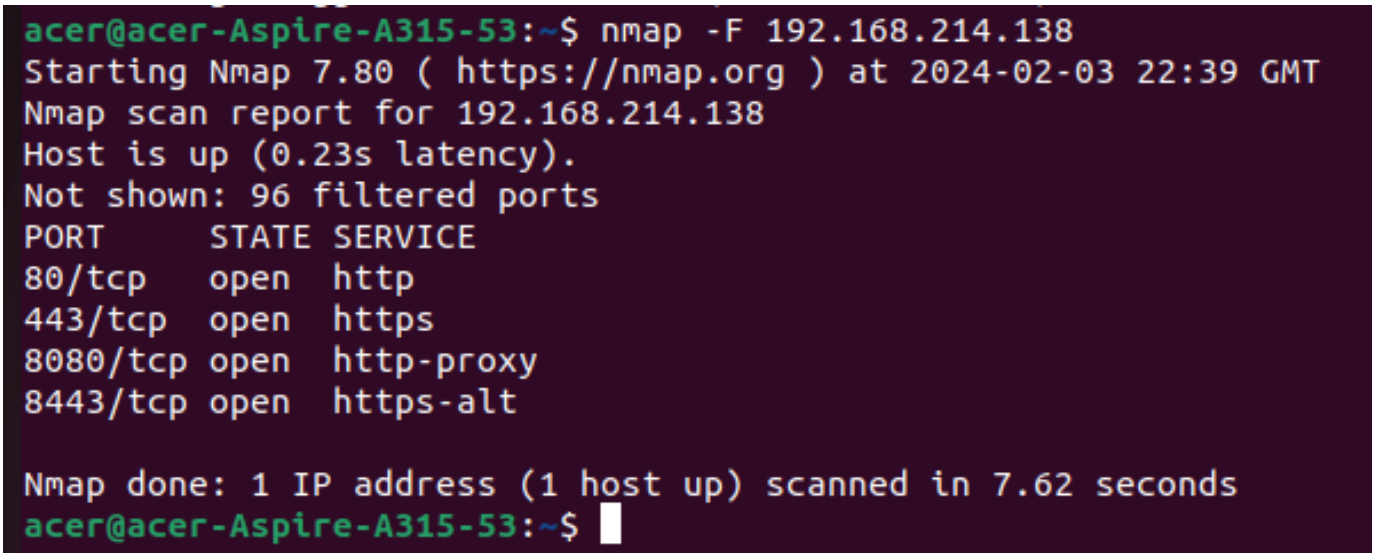
This test shown the files not infected. Rootkits not found:



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 scaned the “192.168.214.138**”** for open ports:

nmap -F 192.168.214.138



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):

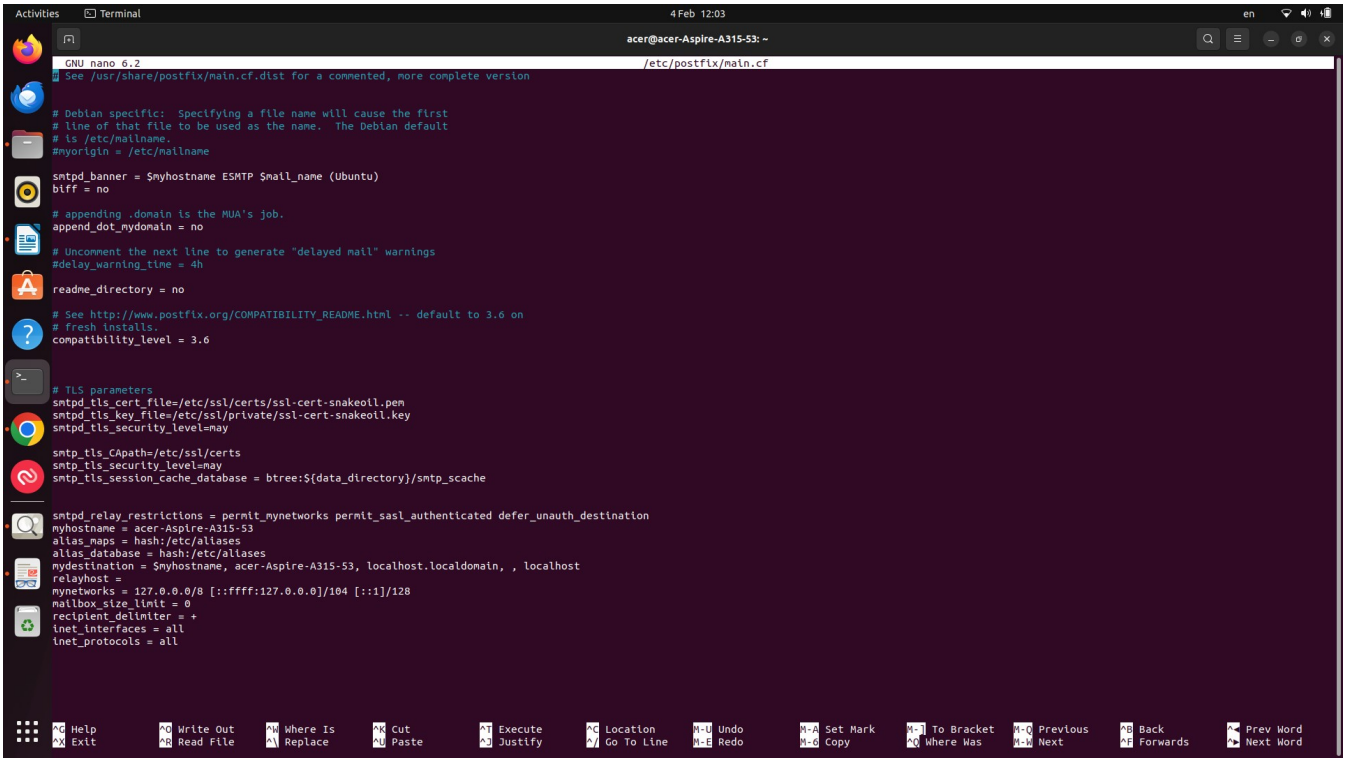
! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]

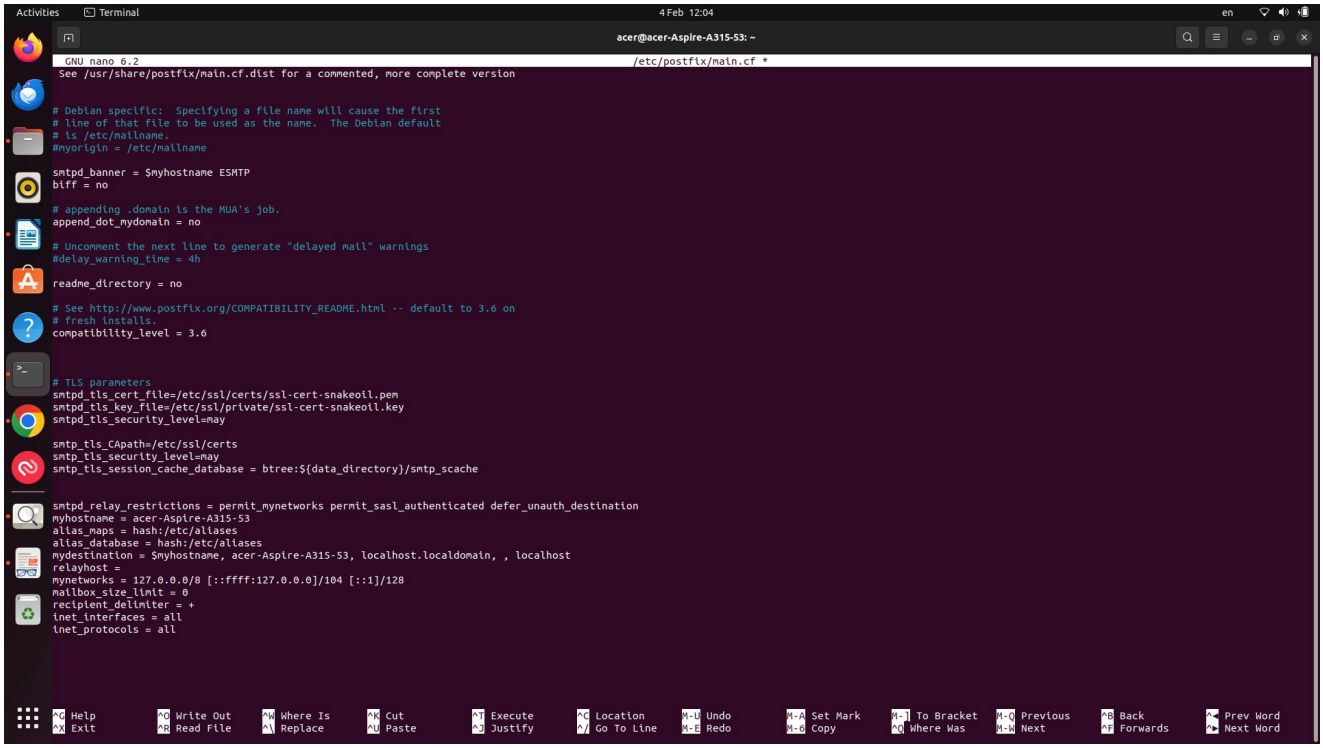
https://cisofy.com/lynis/controls/MAIL-8818/

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
```





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

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:

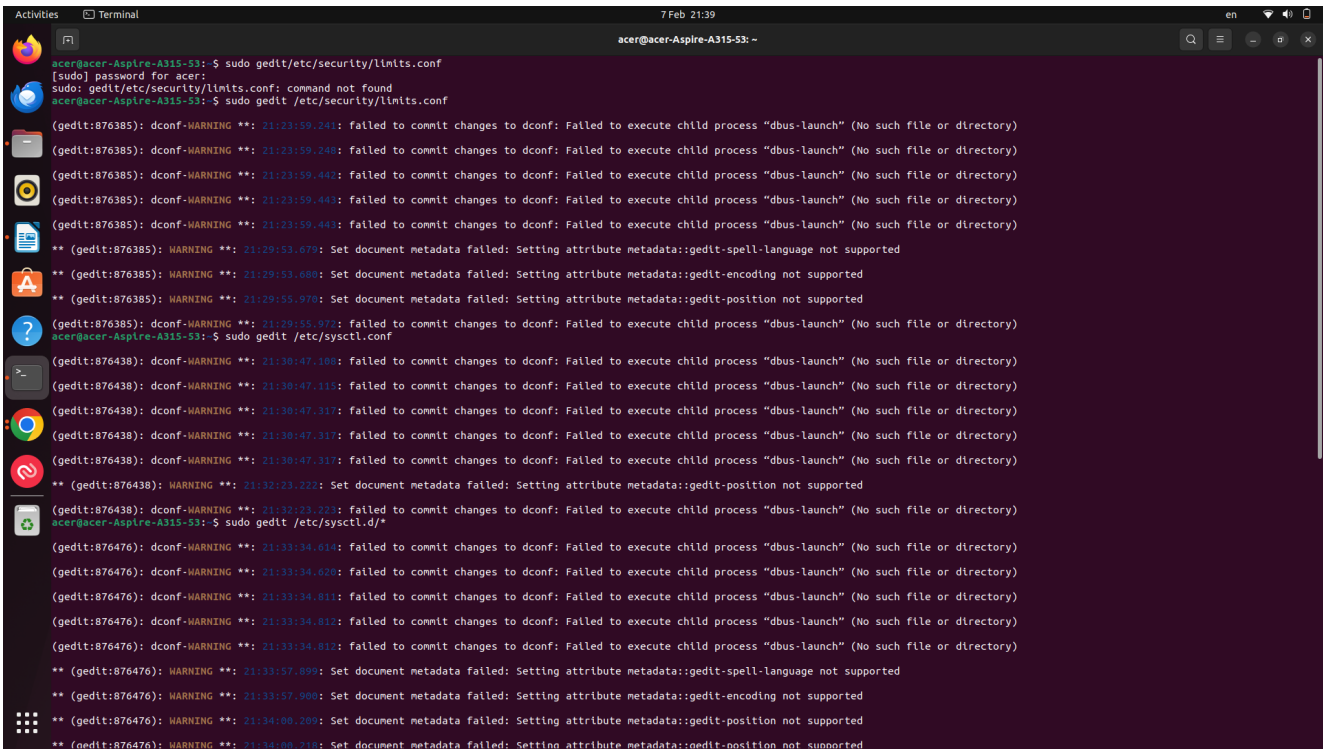
sysctl -w fs.suid_dumpable=0

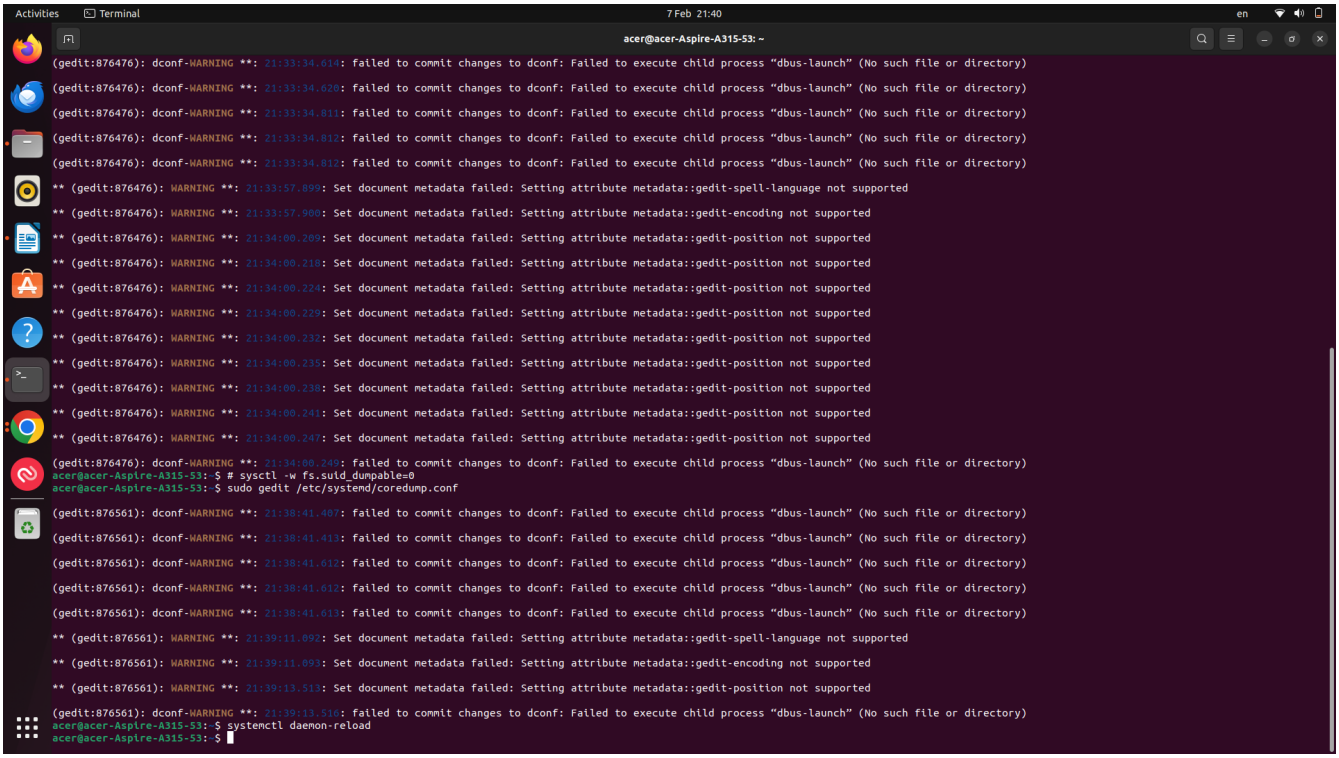
Then edited /etc/systemd/coredump.conf :

Storage=none
ProcessSizeMax=0

And run the command:

systemctl daemon-reload





3. In the Linus report was displaed potential warnings :

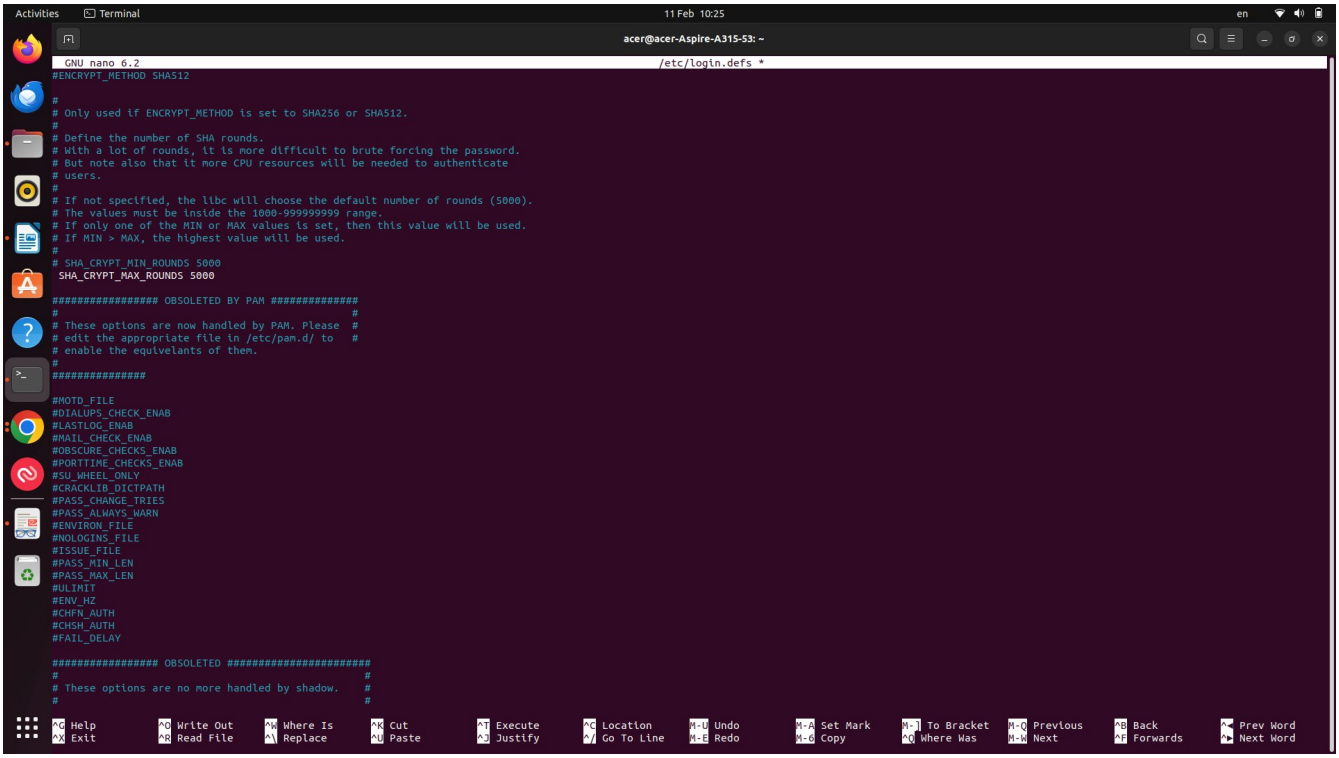
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
https://cisofy.com/lynis/controls/AUTH-9230/

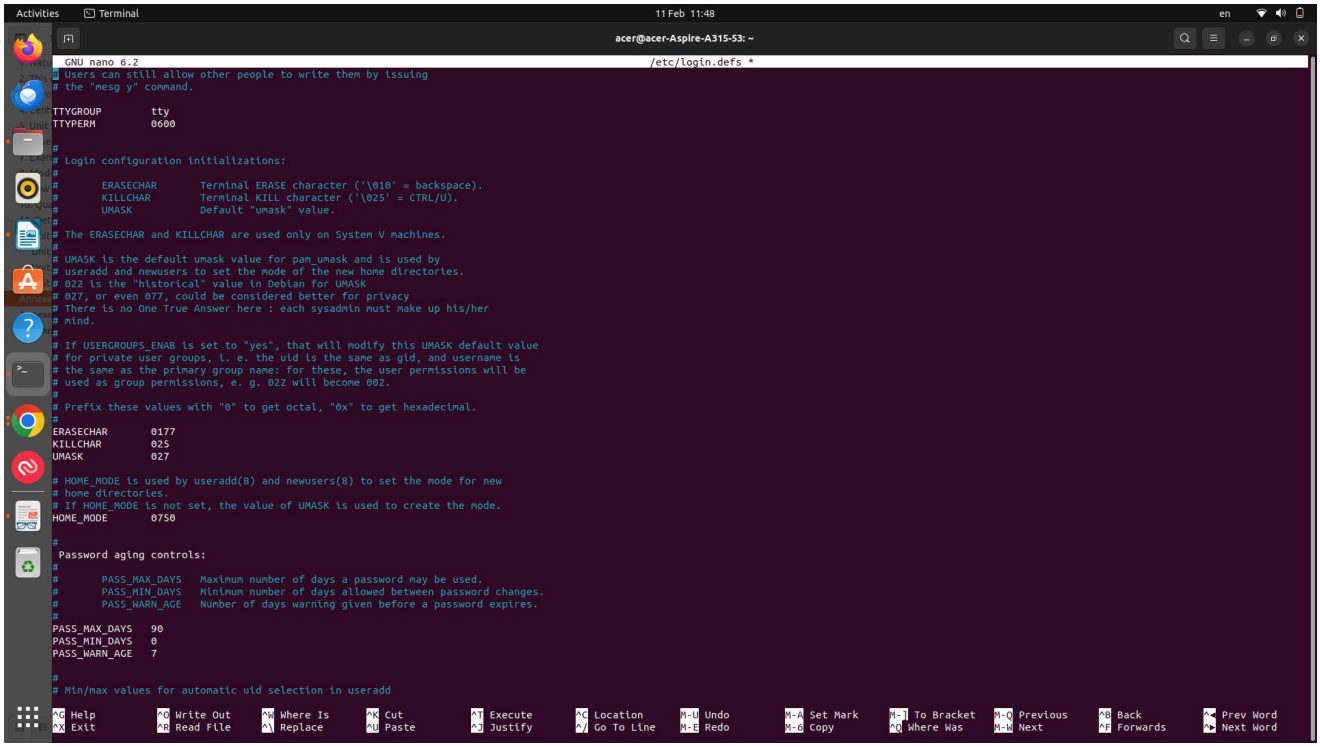
* When possible set expire dates for all password protected accounts [AUTH-9282]
https://cisofy.com/lynis/controls/AUTH-9282/

* 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

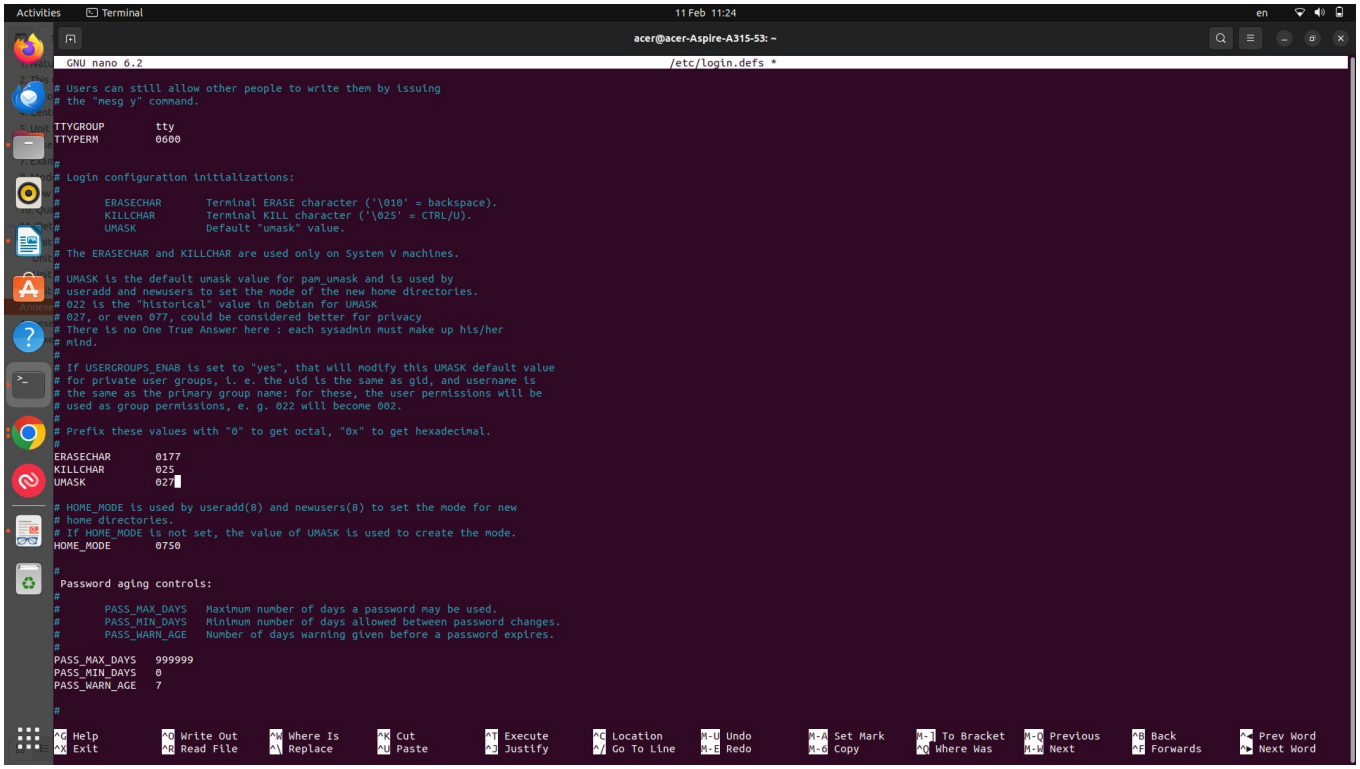




4. In the Linus report was displaed potential warning :

* 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:



5. In the Linus report was displaed 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 displaed 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 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 displaed 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.

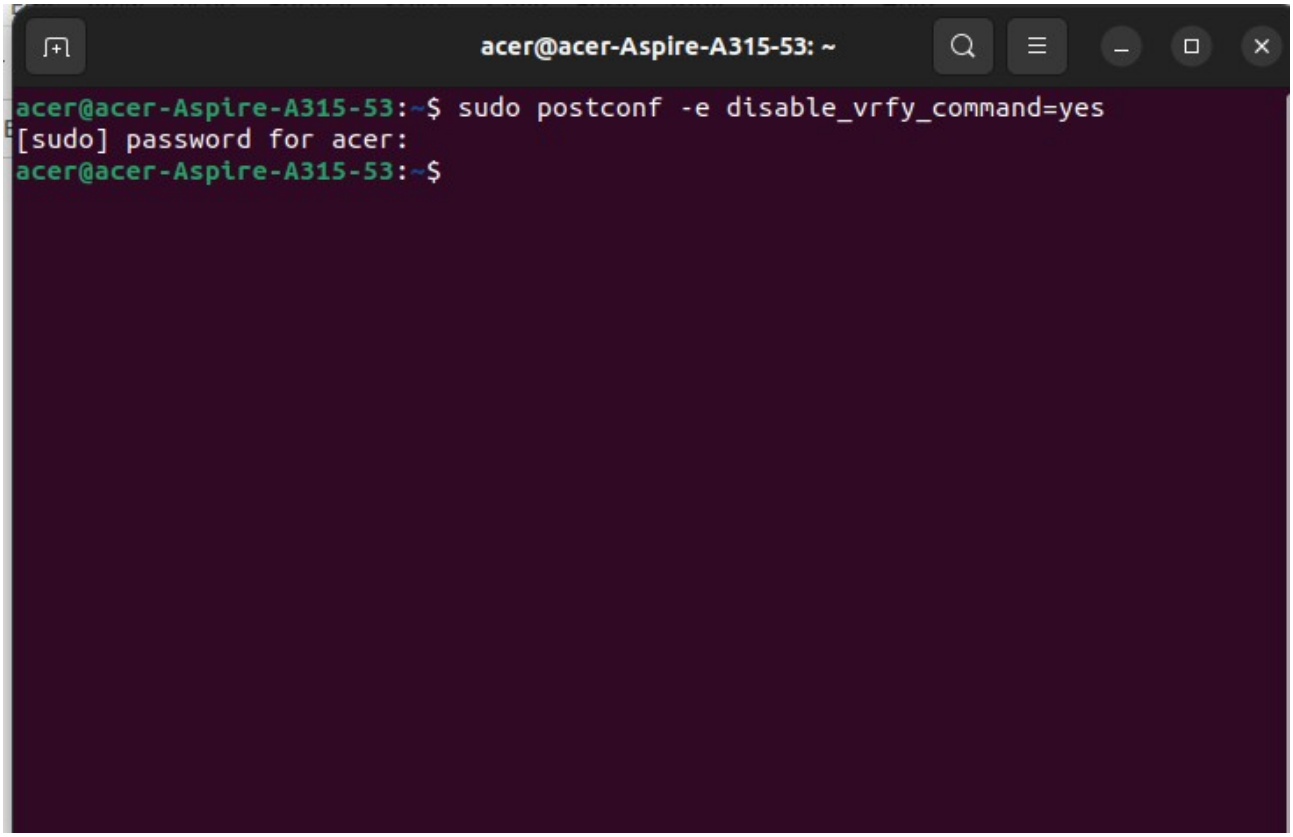
In the Linus report was displaed potential warning :

* 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/

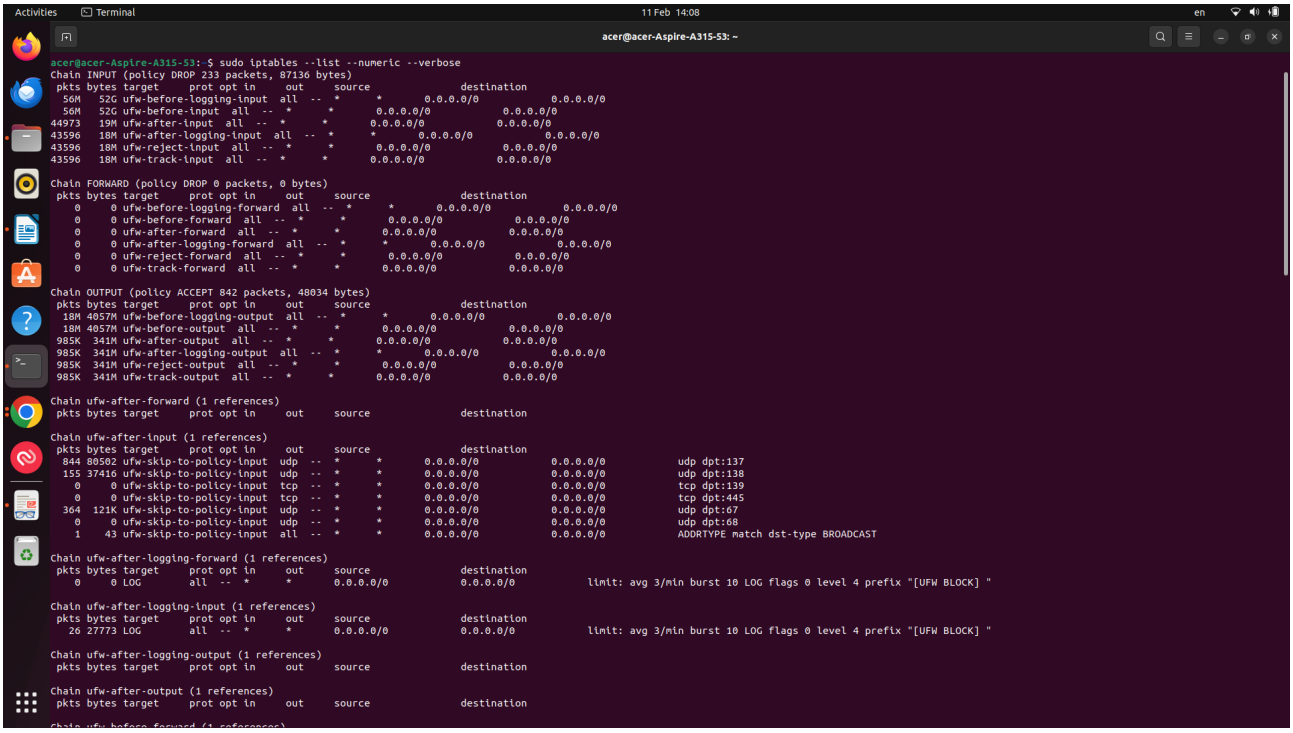


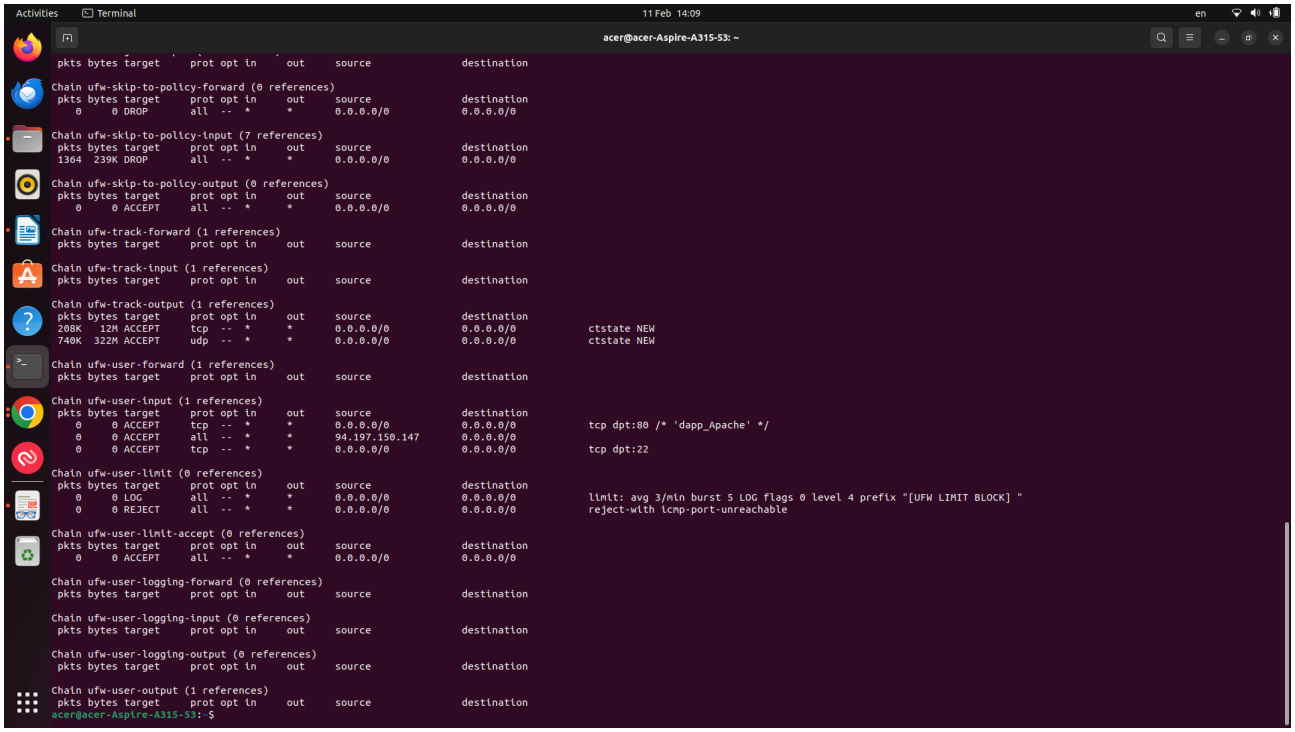
8. In the Linus report was displaed potential warning :

* 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.





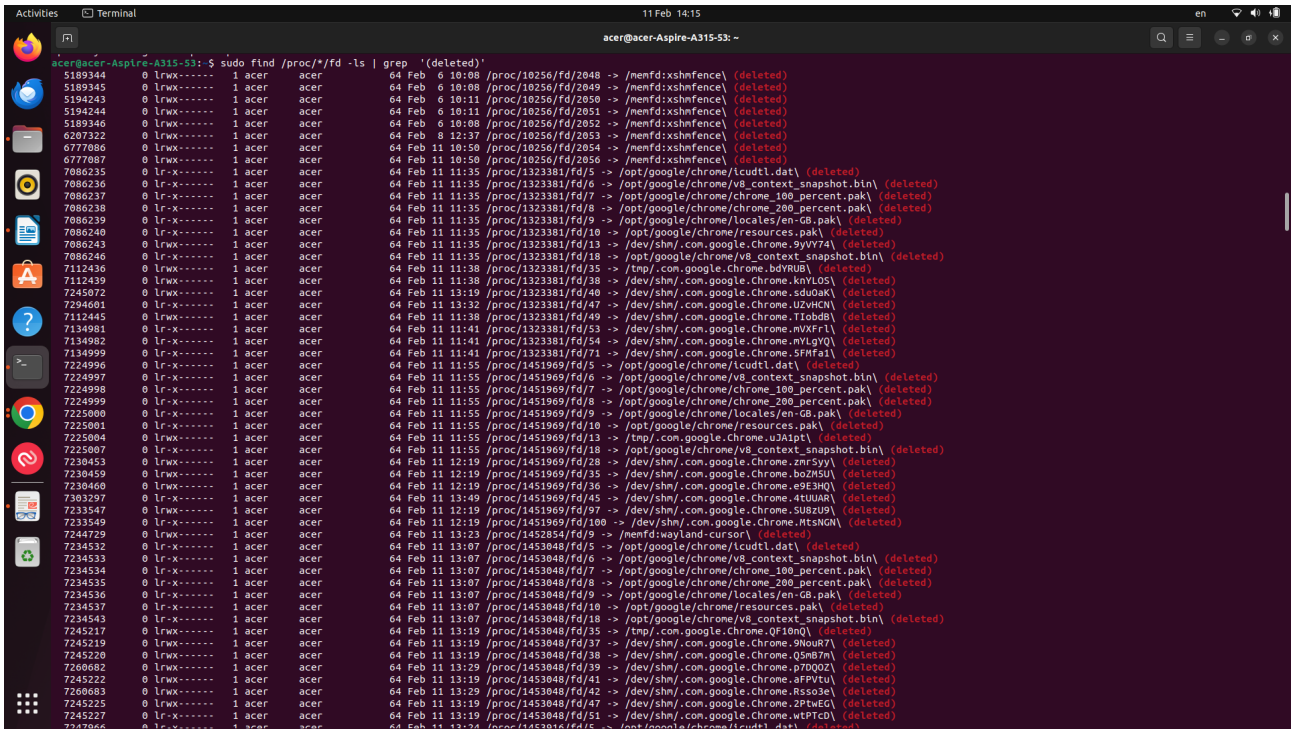
9. In the Linus report was displaed potential warning :

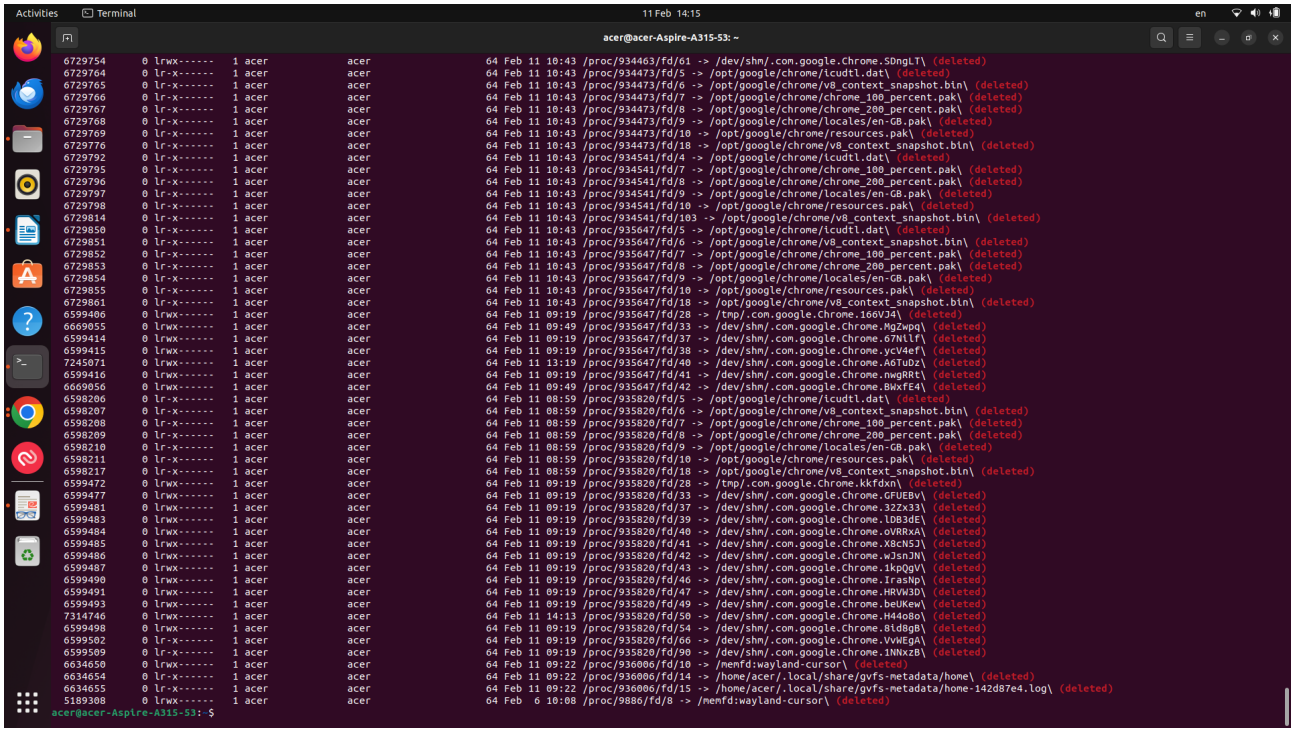
* Check what deleted files are still in use and why. [LOGG-2190]

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

I have checked that deleted files by the command

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





10. In the Linus report was displaed potential warning :

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

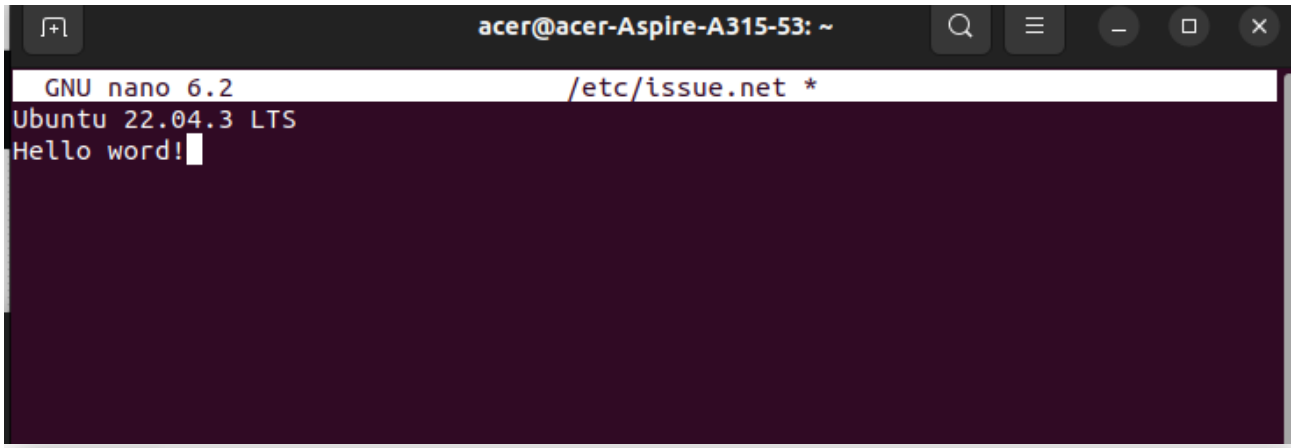
https://cisofy.com/lynis/controls/BANN-7126/

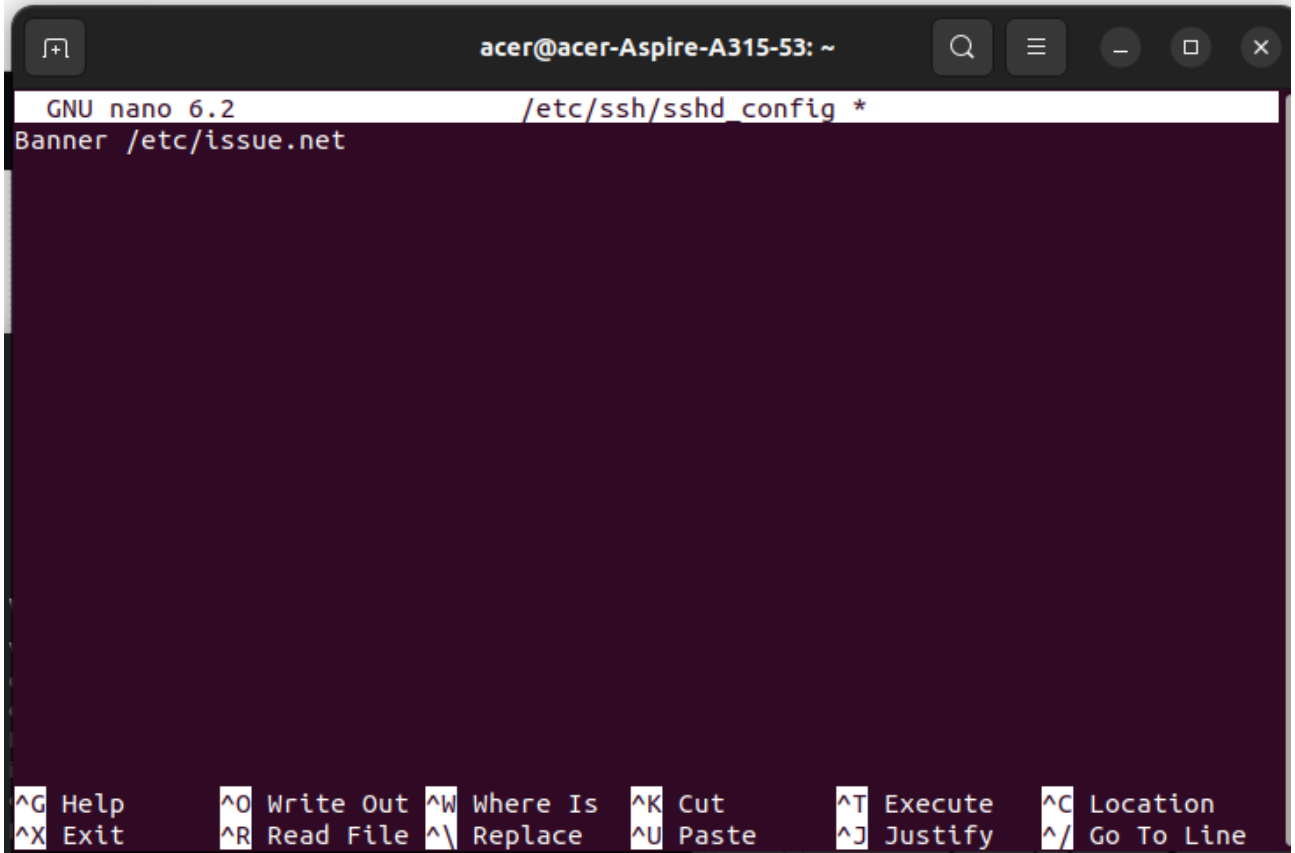
* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

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

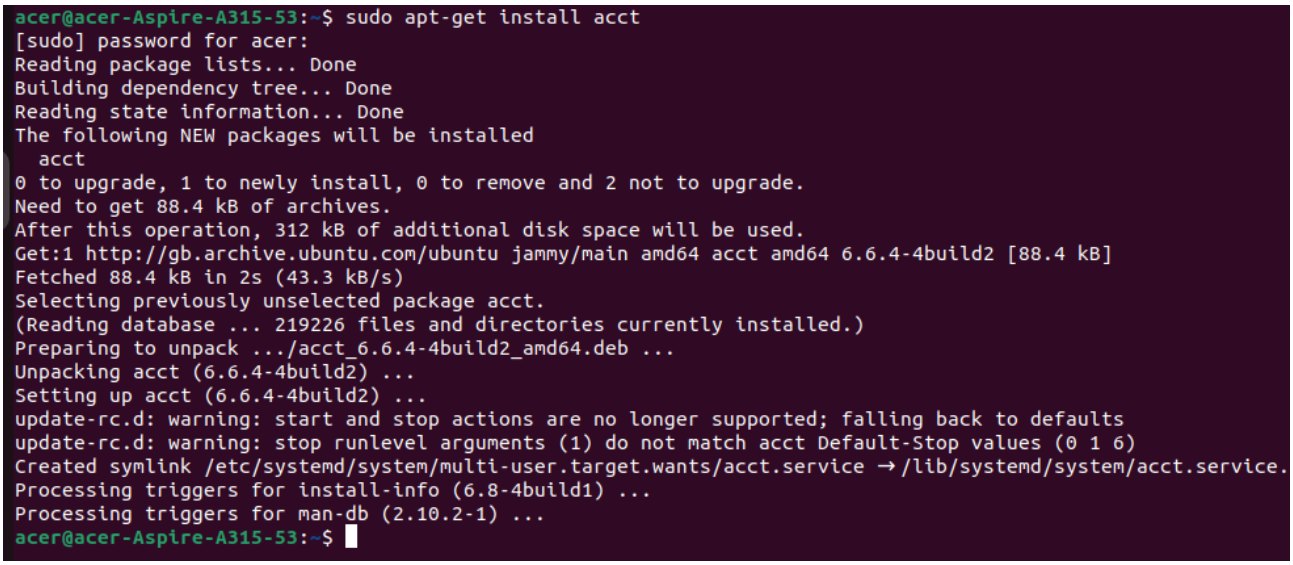
One of the easiest way to protect and secure SSH logins by displaying warming message to UN-authorized users or display welcome or informational messages to authorized users.

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





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.



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
        total      526.71
acer@acer-Aspire-A315-53:~$ sudo sa
     273     164.87re       2.01cp         0avio  99324877k
      39       1.71re       0.90cp         0avio 293928960k   AuctionV8Helper*
      59       4.23re       0.81cp         0avio 197879843k   ThreadPoolForeg*
       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 displaed potential warning :

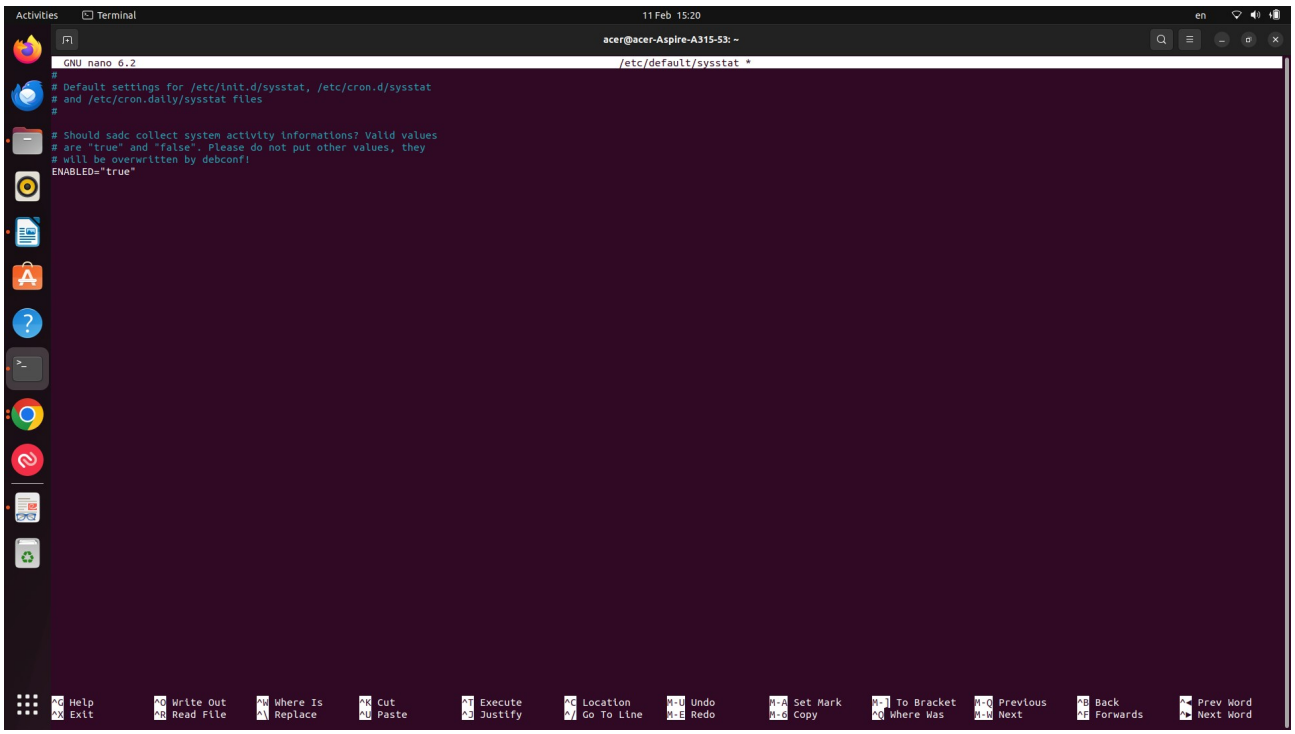
* Enable sysstat to collect accounting (no results) [ACCT-9626]

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

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

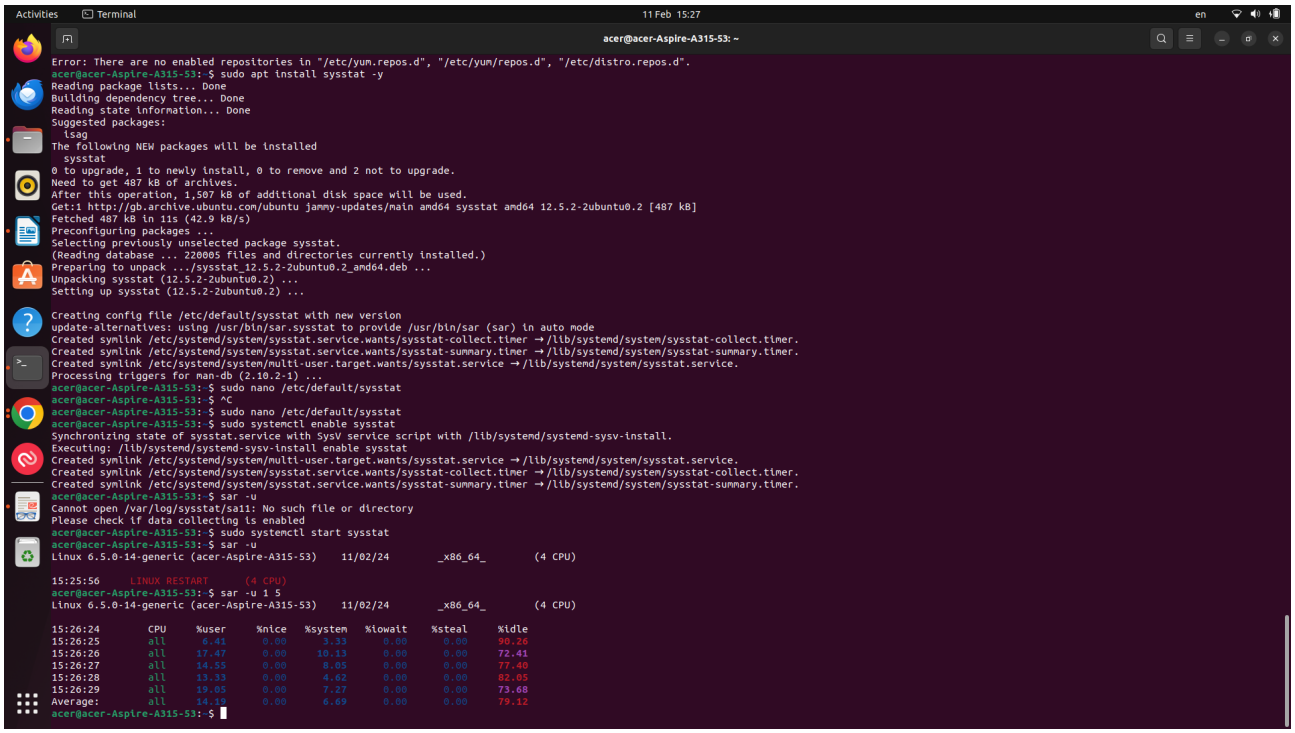
sudo apt install sysstat -y

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



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

sudo systemctl enable sysstat
sudo systemctl start sysstat



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

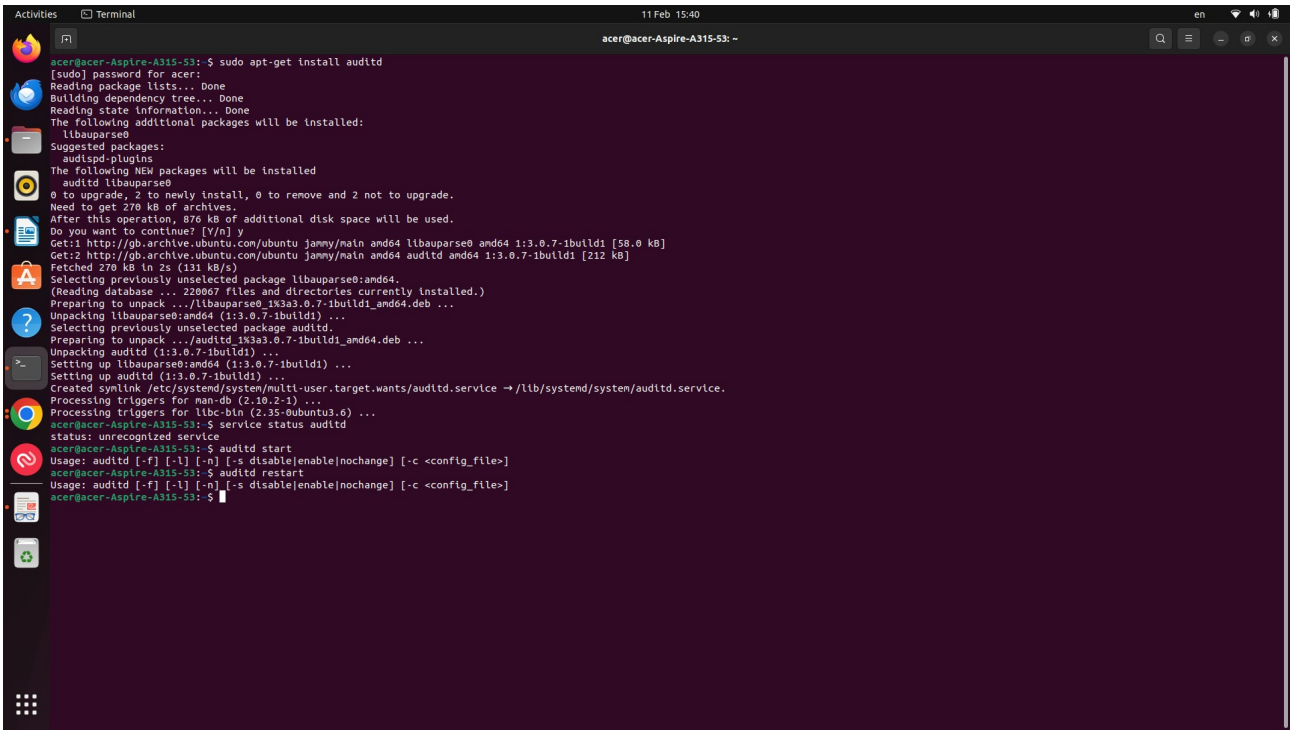
I view the CPU utilization data in more depth. Nowadays most the CPUs are multi-core. To view the utilization details of each core individually use the -P ALL command.

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

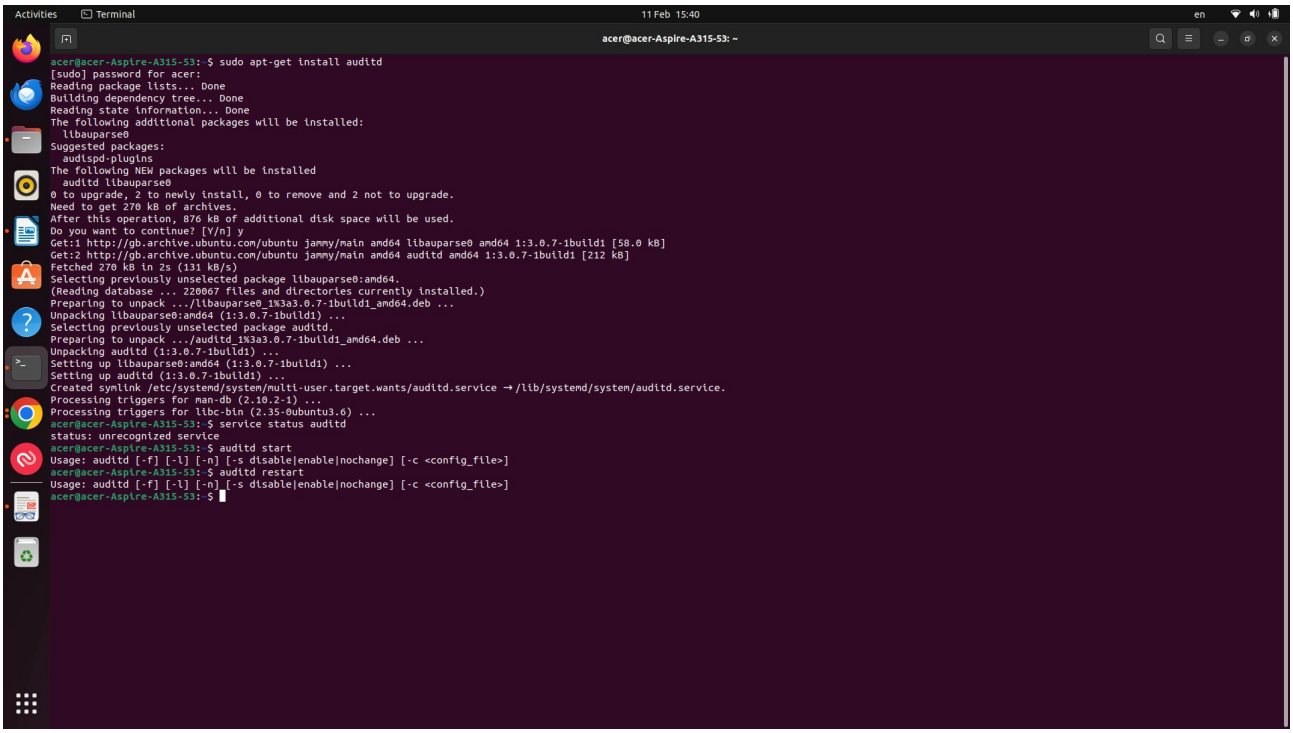
Sysstat also stores monitoring data in files. I see the historical data with the sar command.



13. In the Linus report was displaed potential warning :

* Enable auditd to collect audit information [ACCT-9628]

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



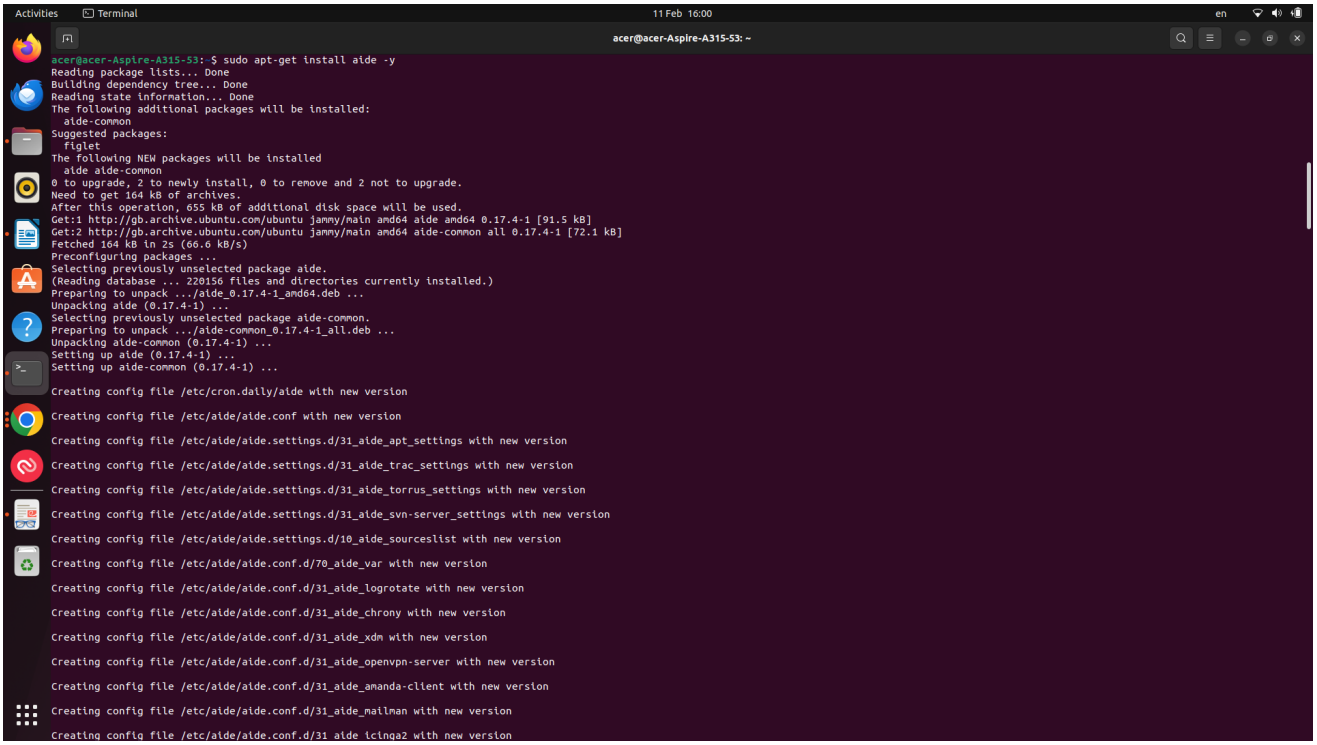
14. In the Linus report was displaed potential warning :

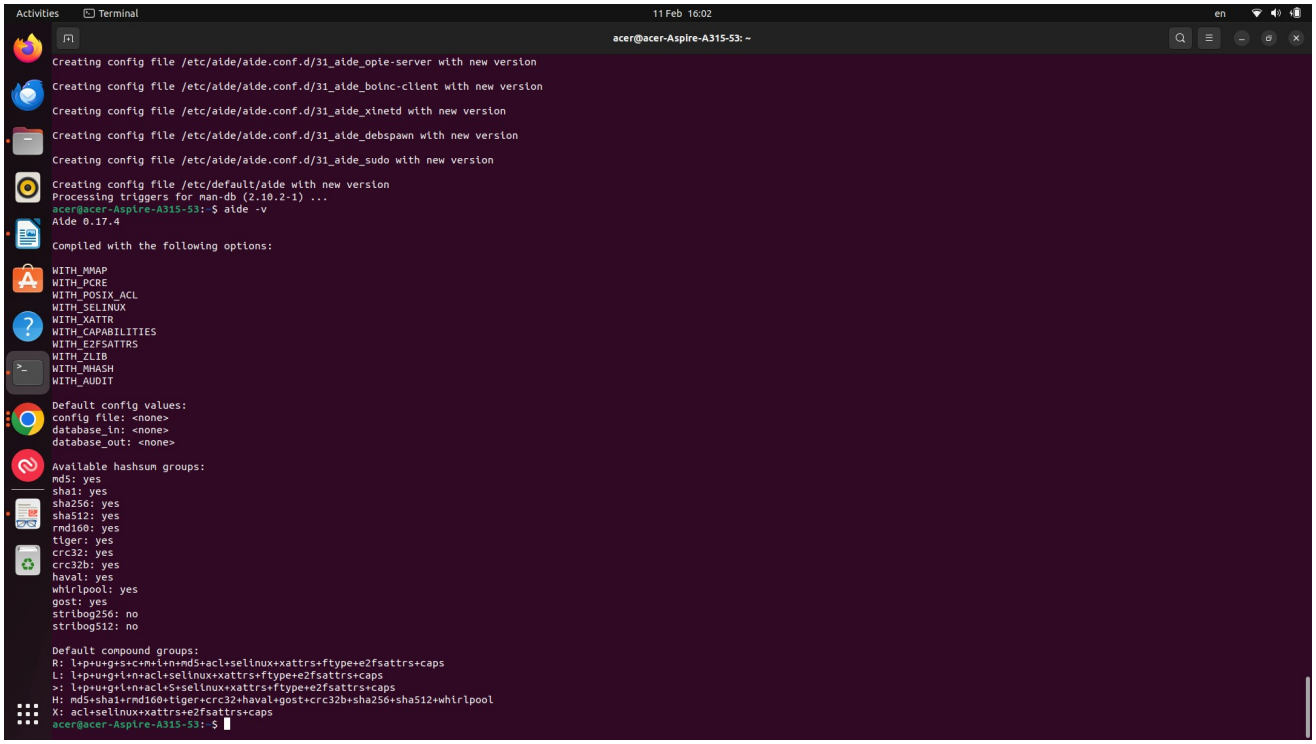
* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]

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

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

sudo apt-get install aide -y





15. In the Linus report was displaed potential warning :

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

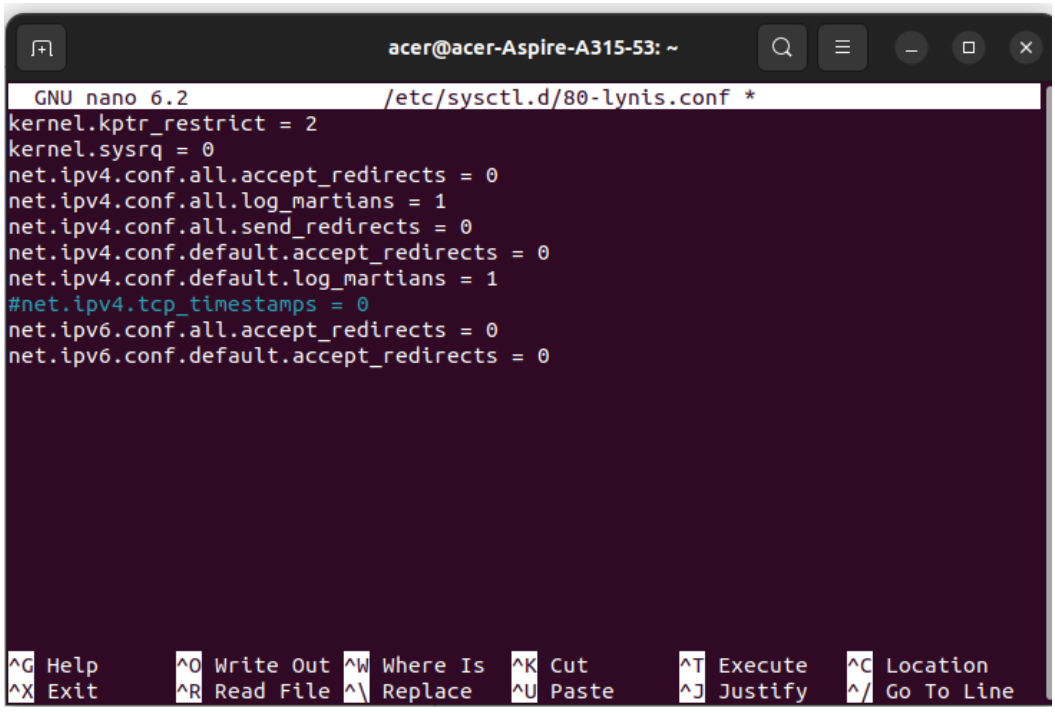
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)

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

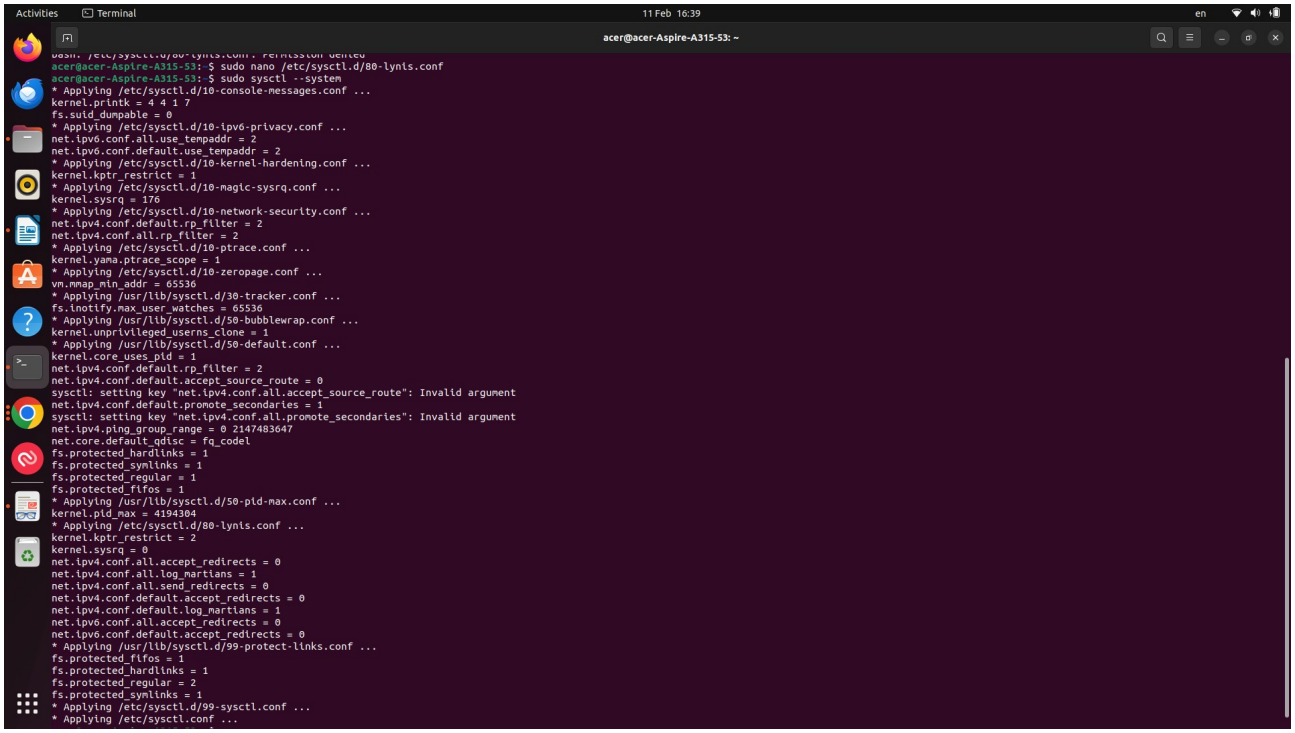
First get a backup of the default settings just in case:

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

Then create the config file:



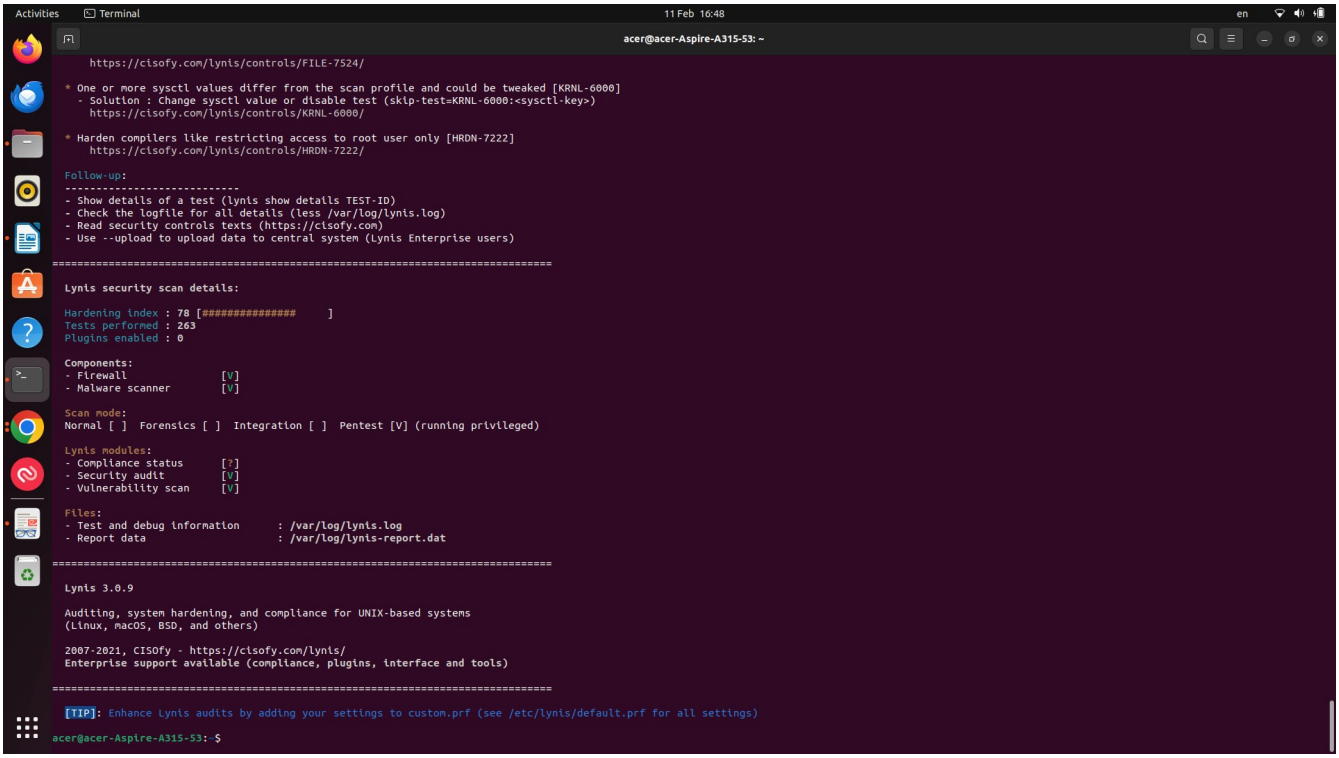
And then applied the settings:



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.



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://cisofy.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://cisofy.com/lynis/controls/BOOT-5264/

* 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/

* 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/

* 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/

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

https://cisofy.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/

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].