

```
name: sahil v patel
course: cis 106
semester: spring 23
```

Deliverable 2

1. What are the server hardware specifications (virtual machine settings)?

Oracle VM VirtualBox Manager

File Machine Help

Tools

Ubuntu cis 106 (lab 4 completed) Powered Off

UbuntuServer (Snapshot 1) Running

General

Name: UbuntuServer
Operating System: Ubuntu (64-bit)

System

Base Memory: 2048 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: UbuntuServer.vdi (Normal, 25.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Realtek RTL852BE WIFI 6 802.11ax PCIe Adapter)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

2. What is Ubuntu server log in screen?

webserver@webmaster: ~

webserver@192.168.12.61's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64)

* Documentation: <https://help.ubuntu.com>
* Management: <https://landscape.canonical.com>
* Support: <https://ubuntu.com/advantage>

System information as of Sun Dec 3 03:44:19 AM UTC 2023

System load: 1.04345703125
Usage of /: 44.5% of 11.21GB
Memory usage: 12%
Swap usage: 0%
Processes: 143
Users logged in: 0
IPv4 address for enp0s3: 192.168.12.61
IPv6 address for enp0s3: fd8e:327b:4e98:0:a00:27ff:fe92:5d06
IPv6 address for enp0s3: 2607:fb91:1302:540d:a00:27ff:fe92:5d06

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: `sudo pro status`

Last login: Sun Dec 3 03:41:36 UTC 2023 from 192.168.12.152 on pts/0
webserver@webmaster:~\$

3. What is the IP address of your Ubuntu Server Virtual Machine?

```
192.168.12.61
```

4. How do you enable the Ubuntu Firewall?

```
sudo ufw enable
```

5. How do you check if the Ubuntu Firewall is running?

```
sudo ufw status
```

6. How do you disable the Ubuntu Firewall?

```
sudo ufw disable
```

7. How do you add Apache to the Firewall?

```
sudo ufw allow 'Apache'
```

8. What is the command you used to install Apache?

```
apt-get install apache2
```

9. What is the command you use to check if Apache is running?

```
sudo systemctl status apache2
```

10. What is the command you use to stop Apache?

```
sudo systemctl stop apache2
```

11. What is the command you use to restart Apache?

```
sudo systemctl restart apache2
```

12. What is the command used to test Apache configuration?

```
sudo apache2ctl configtest
```

13. What is the command used to check the installed version of Apache?

```
apache2 -v
```

14. What are the most common commands to troubleshoot Apache errors? Provide a brief description of each command.

`sudo systemctl status apache2`: This command provides the current status of the Apache service, including whether it is active, inactive, or encountering errors.

`sudo apachectl configtest`: Verifies the syntax of your Apache configuration files without restarting the server. It helps identify syntax errors in your configuration. `sudo tail -f /var/log/apache2/error.log`: Displays the last few lines of the Apache error for monitoring errors as they occur.

15. Which are Apache Log Files, and what are they used for? Provide examples and screenshots.

Access Log: Location: Typically found in the logs directory of the Apache installation. Purpose: Records all requests made to the server, including details such as the IP address of the client, the requested resource, the HTTP status code, and the user agent. **Example:** `sudo tail -n 20 /var/log/apache2/error.log` command:

Error Log: Location: Also found in the logs directory. Purpose: Captures information about server errors, warnings, and other critical events. It helps administrators diagnose and address issues. **Example:** `sudo tail -n 20 /var/log/apache2/access.log`