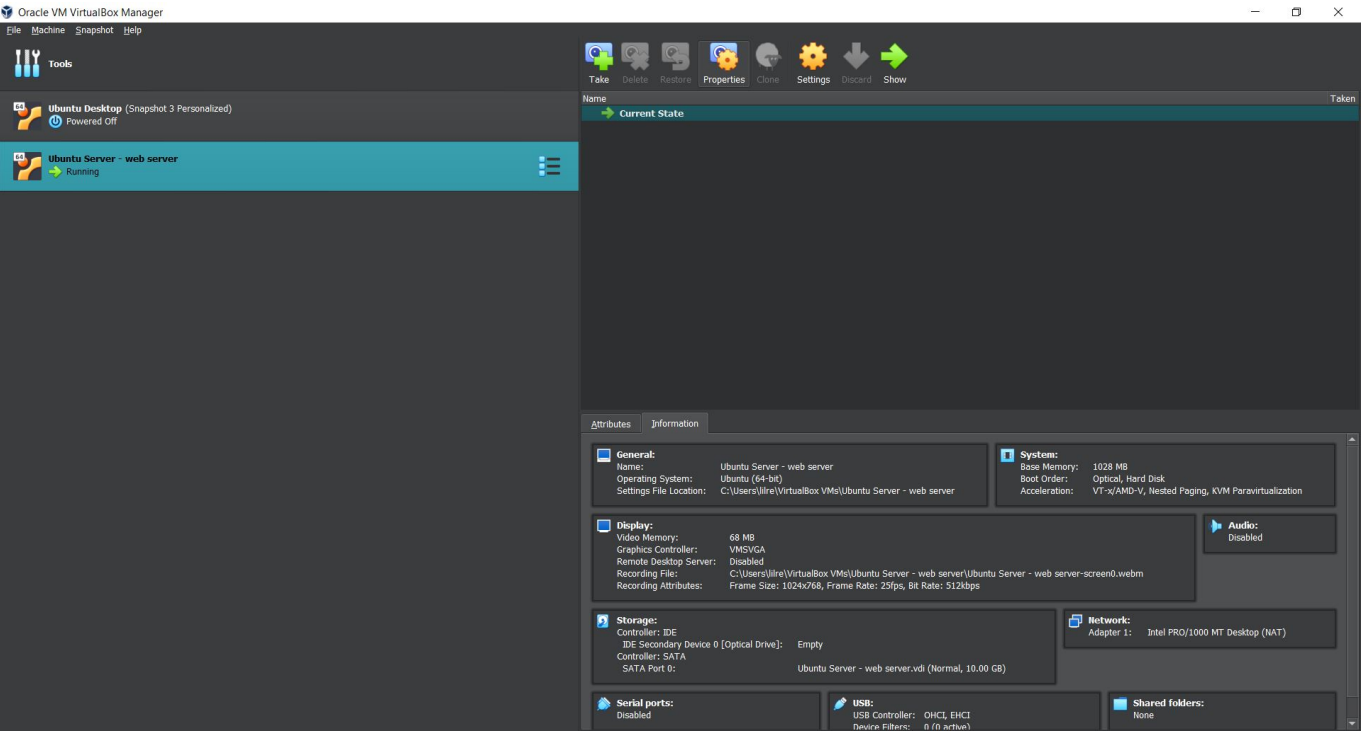


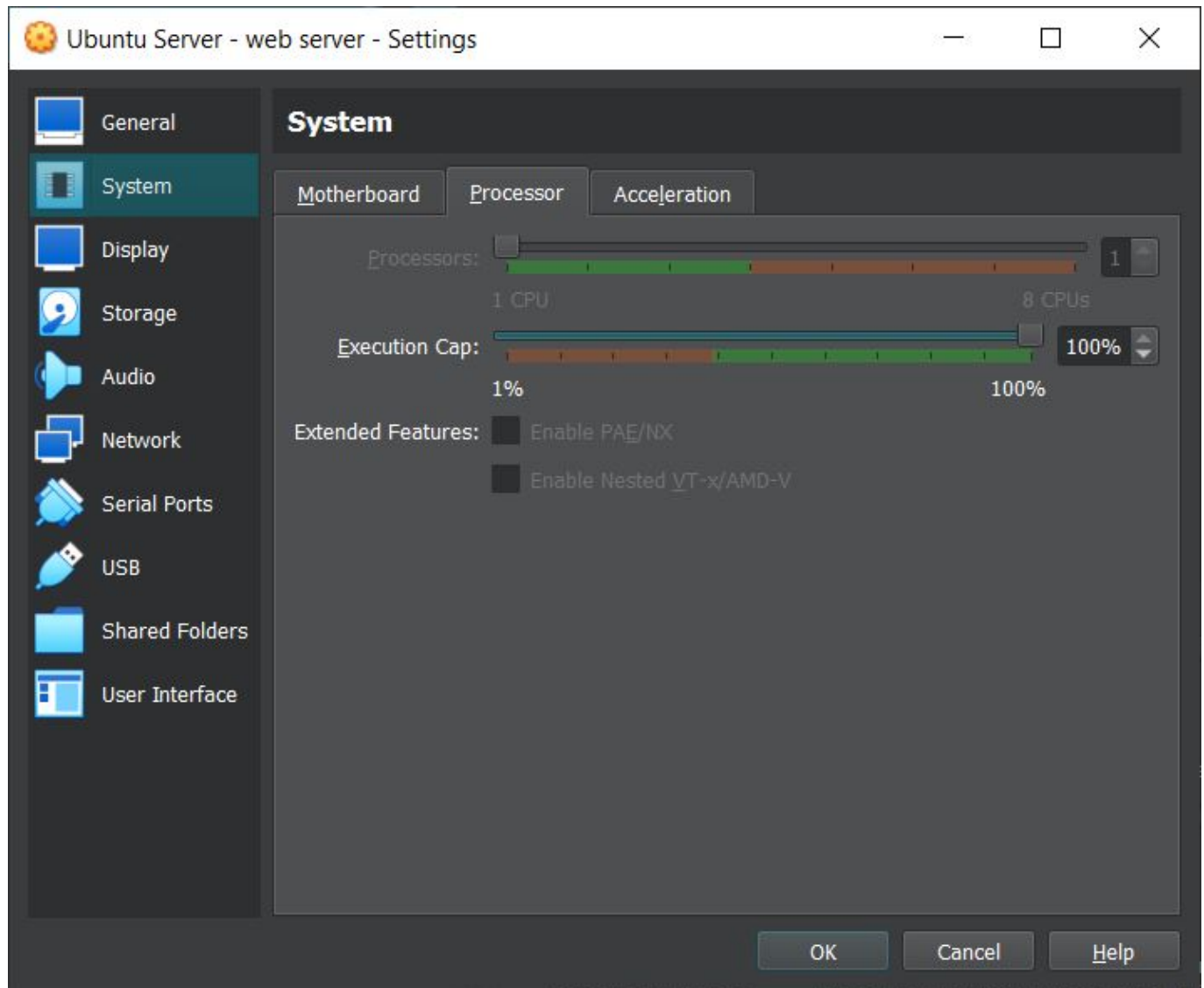
Deliverable 2 Submission

Question 1

Screenshot of hardware information.

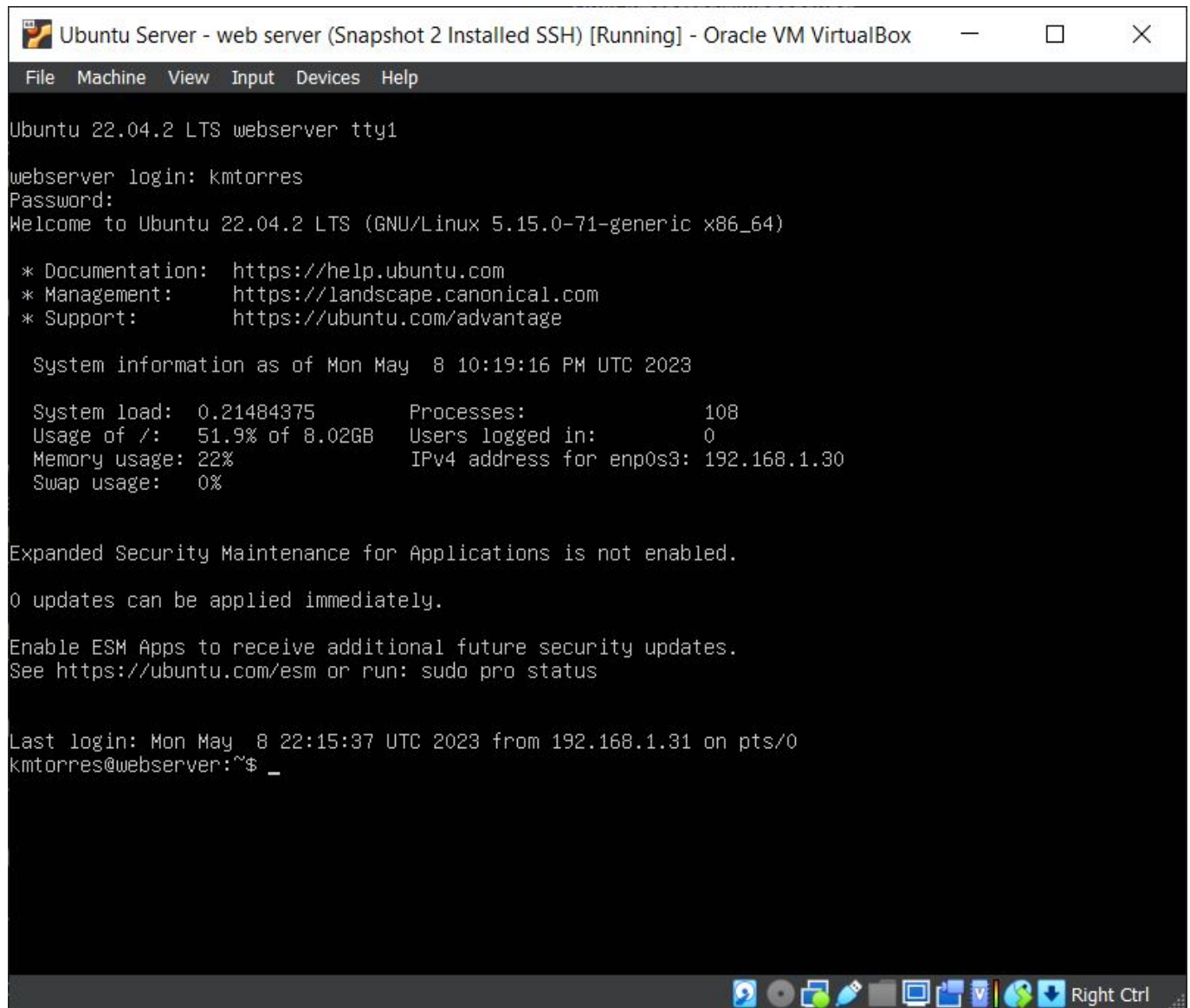


Screenshot of CPUs.



Question 2

Screenshot of login screen of the server right after logging in.



```
Ubuntu Server - web server (Snapshot 2 Installed SSH) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Ubuntu 22.04.2 LTS webserver tty1
webserver login: kmtorres
Password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-71-generic x86_64)

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

System information as of Mon May  8 10:19:16 PM UTC 2023

System load:  0.21484375      Processes:            108
Usage of /:   51.9% of 8.02GB  Users logged in:      0
Memory usage: 22%            IPv4 address for enp0s3: 192.168.1.30
Swap usage:   0%

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: Mon May  8 22:15:37 UTC 2023 from 192.168.1.31 on pts/0
kmtorres@webserver:~$ _
```

Question 3

Screenshot of connecting to the server with ssh from Ubuntu Desktop.

```
1: kmtorres@webserver: ~  
kmtorres@webserver:~$ exit  
logout  
Connection to 192.168.1.30 closed.  
kmtorres46747@cis106:~$ ssh kmtorres@192.168.1.30  
kmtorres@192.168.1.30's password:  
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-71-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Mon May  8 10:46:12 PM UTC 2023  
  
System load:  0.0           Processes:            106  
Usage of /:   51.9% of 8.02GB Users logged in:      1  
Memory usage: 22%          IPv4 address for enp0s3: 192.168.1.30  
Swap usage:   0%  
  
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: Mon May  8 22:19:35 2023 from 192.168.1.31  
kmtorres@webserver:~$
```

Question 4

Screenshot of using command `systemctl status apache2 --no-pager`

```
kmtorres@webserver:~$ systemctl status apache2 --no-pager  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)  
   Active: active (running) since Mon 2023-05-08 22:39:56 UTC; 8min ago  
     Docs: https://httpd.apache.org/docs/2.4/  
  Process: 1373 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
 Main PID: 1377 (apache2)  
    Tasks: 55 (limit: 1028)  
   Memory: 5.2M  
      CPU: 46ms  
   CGroup: /system.slice/apache2.service  
           └─1377 /usr/sbin/apache2 -k start  
             └─1378 /usr/sbin/apache2 -k start  
               └─1379 /usr/sbin/apache2 -k start  
  
May 08 22:39:56 webserver systemd[1]: apache2.service: Deactivated successfully.  
May 08 22:39:56 webserver systemd[1]: Stopped The Apache HTTP Server.  
May 08 22:39:56 webserver systemd[1]: Starting The Apache HTTP Server...  
May 08 22:39:56 webserver systemd[1]: Started The Apache HTTP Server.
```


Screenshot of using command `systemctl status sshd --no-pager`

```
kmtorres@webserver:~$ systemctl status sshd --no-pager
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-05-08 22:19:05 UTC; 30min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 710 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 754 (sshd)
    Tasks: 1 (limit: 1028)
   Memory: 6.8M
      CPU: 74ms
   CGroup: /system.slice/ssh.service
           └─754 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 08 22:19:05 webserver sshd[754]: Server listening on 0.0.0.0 port 22.
May 08 22:19:05 webserver sshd[754]: Server listening on :: port 22.
May 08 22:19:05 webserver systemd[1]: Started OpenBSD Secure Shell server.
May 08 22:19:23 webserver sshd[1079]: pam_unix(sshd:auth): authentication failure; logname=km...torres
May 08 22:19:25 webserver sshd[1079]: Failed password for kmtorres from 192.168.1.31 port 22 ssh2
May 08 22:19:30 webserver sshd[1079]: Failed password for kmtorres from 192.168.1.31 port 22 ssh2
May 08 22:19:35 webserver sshd[1079]: Accepted password for kmtorres from 192.168.1.31 port 22 ssh2
May 08 22:19:35 webserver sshd[1079]: pam_unix(sshd:session): session opened for user km...uid=0)
May 08 22:46:12 webserver sshd[1439]: Accepted password for kmtorres from 192.168.1.31 port 22 ssh2
May 08 22:46:12 webserver sshd[1439]: pam_unix(sshd:session): session opened for user km...uid=0)
Hint: Some lines were ellipsized, use -l to show in full.
```

Screenshot of using command `systemctl status ufw --no-pager`

```
kmtorres@webserver:~$ systemctl status ufw --no-pager
● ufw.service - Uncomplicated firewall
   Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
   Active: active (exited) since Mon 2023-05-08 22:19:02 UTC; 30min ago
     Docs: man:ufw(8)
  Process: 564 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0/SUCCESS)
 Main PID: 564 (code=exited, status=0/SUCCESS)
      CPU: 37ms

May 08 22:19:02 webserver systemd[1]: Starting Uncomplicated firewall...
May 08 22:19:02 webserver systemd[1]: Finished Uncomplicated firewall.
```

Question 5

Screenshot of the last 10 lines of the follow files:

- Apache: access.log
- Apache: error.log

- SSH: auth.log

```
kmtorres@webserver:~$ tail /var/log/apache2/access.log
192.168.1.5 - - [08/May/2023:21:53:16 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.5 - - [08/May/2023:21:53:16 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.1.30/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
ecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.5 - - [08/May/2023:21:53:17 +0000] "GET /favicon.ico HTTP/1.1" 404 490 "http://192.168.1.30/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/112.0.0.0 Safari/537.36"
192.168.1.31 - - [08/May/2023:22:40:19 +0000] "GET / HTTP/1.1" 200 451 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"
192.168.1.31 - - [08/May/2023:22:40:19 +0000] "GET /favicon.ico HTTP/1.1" 404 490 "http://192.168.1.30/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"
192.168.1.31 - - [08/May/2023:22:43:06 +0000] "GET / HTTP/1.1" 200 451 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"
kmtorres@webserver:~$ tail /var/log/apache2/error.log
[Mon May 08 22:16:42.446113 2023] [mpm_event:notice] [pid 761:tid 139845218508352] AH00492: caught SIGWINCH, shutting down gracefully
[Mon May 08 22:19:05.411269 2023] [mpm_event:notice] [pid 762:tid 139838206678912] AH00489: Apache/2.4.52 (Ubuntu) configured -- resuming normal operations
[Mon May 08 22:19:05.415644 2023] [core:notice] [pid 762:tid 139838206678912] AH00094: Command line: '/usr/sbin/apache2'
[Mon May 08 22:38:02.244613 2023] [mpm_event:notice] [pid 762:tid 139838206678912] AH00493: SIGUSR1 received. Doing graceful restart
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
[Mon May 08 22:38:02.251073 2023] [mpm_event:notice] [pid 762:tid 139838206678912] AH00489: Apache/2.4.52 (Ubuntu) configured -- resuming normal operations
[Mon May 08 22:38:02.251082 2023] [core:notice] [pid 762:tid 139838206678912] AH00094: Command line: '/usr/sbin/apache2'
[Mon May 08 22:39:56.749679 2023] [mpm_event:notice] [pid 762:tid 139838206678912] AH00492: caught SIGWINCH, shutting down gracefully
[Mon May 08 22:39:56.801789 2023] [mpm_event:notice] [pid 1377:tid 140644767602560] AH00489: Apache/2.4.52 (Ubuntu) configured -- resuming normal operations
[Mon May 08 22:39:56.802000 2023] [core:notice] [pid 1377:tid 140644767602560] AH00094: Command line: '/usr/sbin/apache2'
kmtorres@webserver:~$ tail /var/log/auth.log
May 8 22:39:56 webserver sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kmtorres(uid=1000)
May 8 22:39:56 webserver sudo: pam_unix(sudo:session): session closed for user root
May 8 22:45:46 webserver sshd[1125]: Received disconnect from 192.168.1.31 port 57312:11: disconnected by user
May 8 22:45:46 webserver sshd[1125]: Disconnected from user kmtorres 192.168.1.31 port 57312
May 8 22:45:46 webserver sshd[1079]: pam_unix(sshd:session): session closed for user kmtorres
May 8 22:45:46 webserver systemd-logind[711]: Session 3 logged out. Waiting for processes to exit.
May 8 22:45:46 webserver systemd-logind[711]: Removed session 3.
May 8 22:46:12 webserver sshd[1439]: Accepted password for kmtorres from 192.168.1.31 port 57468 ssh2
May 8 22:46:12 webserver sshd[1439]: pam_unix(sshd:session): session opened for user kmtorres(uid=1000) by (uid=0)
May 8 22:46:12 webserver systemd-logind[711]: New session 4 of user kmtorres.
```

Question 6

Screenshot of the sites-available config file.

```
kmtorres@webserver:~$ cat /etc/apache2/sites-available/website.conf
<VirtualHost *:80>
    ServerAdmin kmtorres@localhost
    ServerName website
    ServerAlias www.website
    DocumentRoot /var/www/website
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Screenshot of the top of the apache2.conf file

- Everything is on the default configuration.

```
kmtorres@webserver:~$ cat /etc/apache2/apache2.conf
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information about
# the directives and /usr/share/doc/apache2/README.Debian about Debian specific
# hints.
#
#
# Summary of how the Apache 2 configuration works in Debian:
# The Apache 2 web server configuration in Debian is quite different to
# upstream's suggested way to configure the web server. This is because Debian's
# default Apache2 installation attempts to make adding and removing modules,
# virtual hosts, and extra configuration directives as flexible as possible, in
# order to make automating the changes and administering the server as easy as
# possible.
#
# It is split into several files forming the configuration hierarchy outlined
# below, all located in the /etc/apache2/ directory:
#
#     /etc/apache2/
#     |-- apache2.conf
#     |   `-- ports.conf
#     |-- mods-enabled
#     |   |-- *.load
#     |   `-- *.conf
#     |-- conf-enabled
#     |   `-- *.conf
#     `-- sites-enabled
#         `-- *.conf
#
#
# * apache2.conf is the main configuration file (this file). It puts the pieces
# together by including all remaining configuration files when starting up the
# web server.
#
# * ports.conf is always included from the main configuration file. It is
# supposed to determine listening ports for incoming connections which can be
```

Screenshot of the bottom of the apache2.conf file.

- Highlighted the only manual change.

```
# viewed by Web clients.
#
<FilesMatch "^\.ht">
    Require all denied
</FilesMatch>

#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %0
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %0 \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %0 \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %0" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
ServerName 127.0.0.1
kmtorres@webserver:~$ _
```

Question 7

Screenshot showing the ip address of my server and the website being accessed from the Ubuntu Desktop virtual machine.

