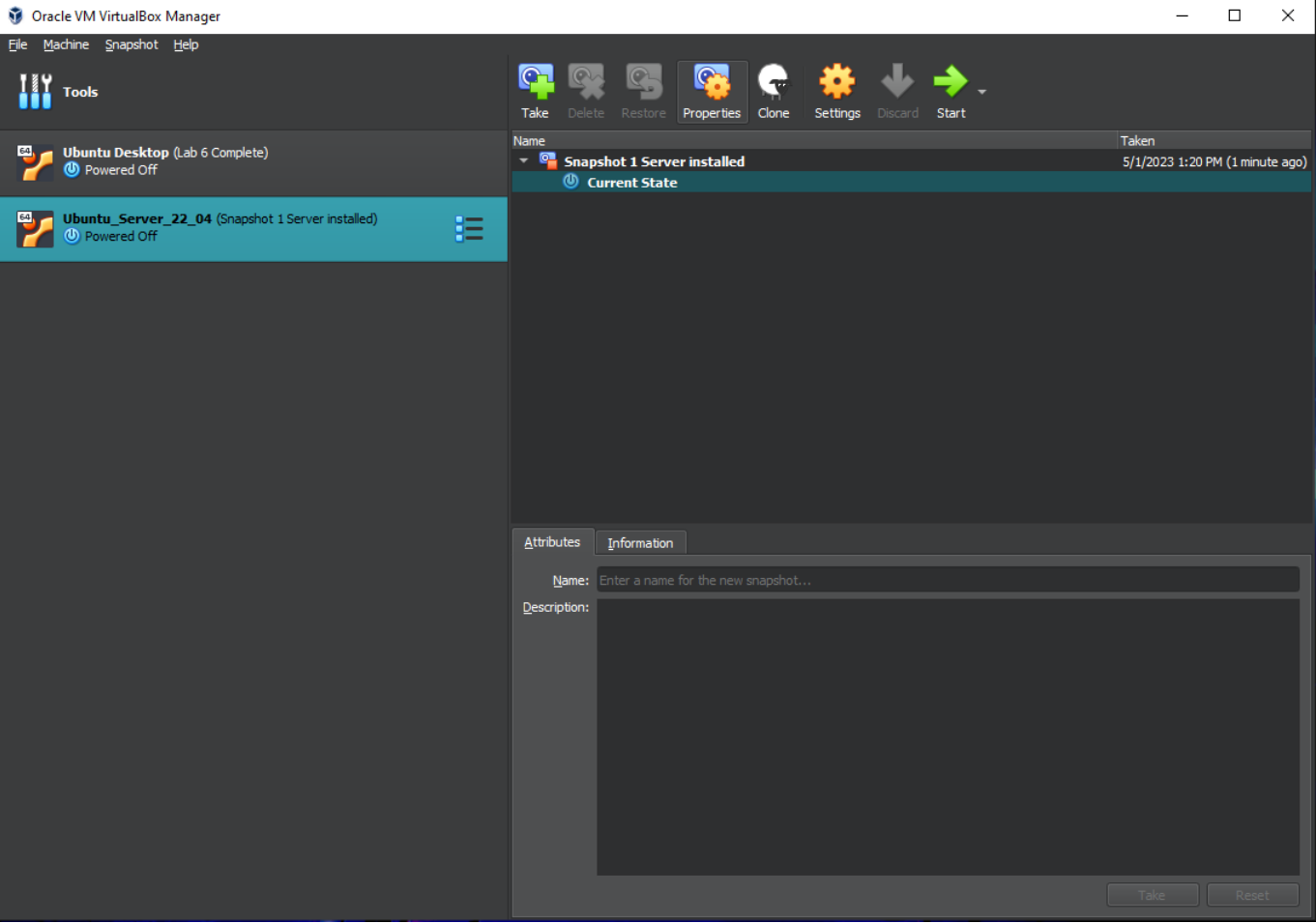
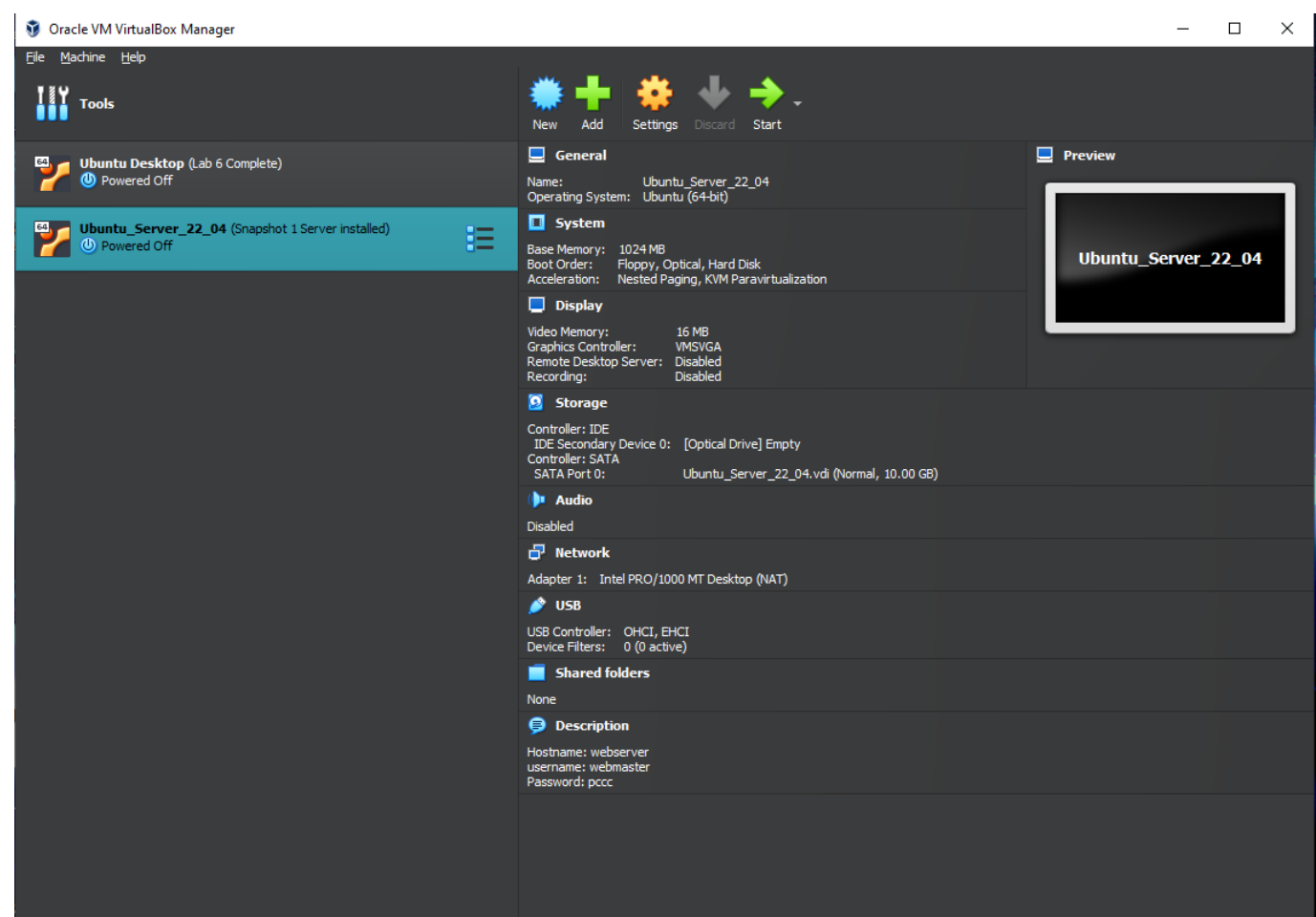


# Deliverable 2

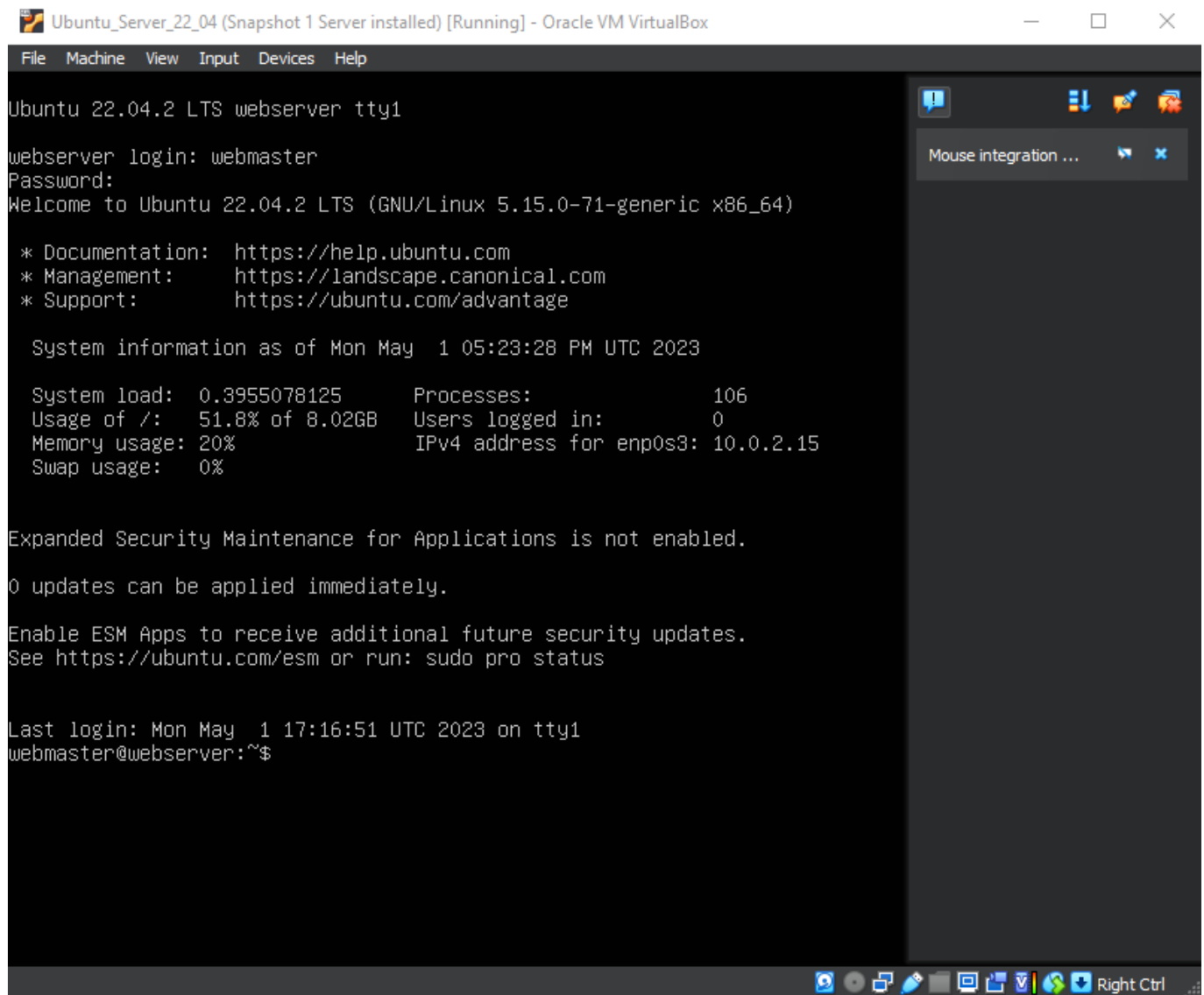
## Screenshot of the virtual machine hardware configuration

Here is a screenshot of the virtual machine hardware configuration:





Screenshot of the login screen

**Here is a screenshot of the login screen:**

The screenshot shows a terminal window titled "Ubuntu\_Server\_22\_04 (Snapshot 1 Server installed) [Running] - Oracle VM VirtualBox". The terminal displays the login process for a user named "webmaster" on an Ubuntu 22.04.2 LTS webserver. The output includes system information, login status, and a prompt for the user to enable ESM (Expanded Security Maintenance) for Applications.

```
Ubuntu 22.04.2 LTS webserver tty1
webserver login: webmaster
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  1 05:23:28 PM UTC 2023

System load:  0.3955078125      Processes:           106
Usage of /:   51.8% of 8.02GB   Users logged in:     0
Memory usage: 20%              IPv4 address for enp0s3: 10.0.2.15
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  1 17:16:51 UTC 2023 on tty1
webmaster@webserver:~$
```

**Screenshot connecting to the server with ssh**

## Here is a screenshot of connecting to the server with ssh:

```

1/1 ~ + [ ] [ ]
Tilix: webmaster@webserver: ~
1: webmaster@webserver: ~
jdeguzman@cis106:~$ ssh webmaster@webserver
webmaster@webserver'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  1 07:54:41 PM UTC 2023

System load:          0.0
Usage of /:            52.8% of 8.02GB
Memory usage:         22%
Swap usage:           0%
Processes:            106
Users logged in:       0
IPv4 address for enp0s3: 192.168.1.158
IPv6 address for enp0s3: 2600:4041:4450:a900:a00:27ff:fe4b:9c2c

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  1 19:14:37 2023 from 192.168.1.159
webmaster@webserver:~$

```

## Screenshot of commands

- Here is a screenshot of the command `systemctl status apache2 --no-pager`:

```

webmaster@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 2023-05-01 19:22:13 UTC; 38min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 766 (apache2)
    Tasks: 55 (limit: 1026)
   Memory: 7.8M
      CPU: 99ms
   CGroup: /system.slice/apache2.service
           └─766 /usr/sbin/apache2 -k start
             └─767 /usr/sbin/apache2 -k start
               └─768 /usr/sbin/apache2 -k start

May 01 19:22:12 webserver systemd[1]: Starting The Apache HTTP Server...
May 01 19:22:13 webserver systemd[1]: Started The Apache HTTP Server.
webmaster@webserver:~$ _

```

- Here is a screenshot of the command `systemctl status sshd --no-pager`:

```
webmaster@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 2023-05-01 19:22:13 UTC; 40min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 755 (sshd)
    Tasks: 1 (limit: 1026)
   Memory: 7.6M
      CPU: 41ms
   CGroup: /system.slice/ssh.service
           └─755 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 01 19:22:12 webserver systemd[1]: Starting OpenBSD Secure Shell server...
May 01 19:22:13 webserver sshd[755]: Server listening on 0.0.0.0 port 22.
May 01 19:22:13 webserver sshd[755]: Server listening on :: port 22.
May 01 19:22:13 webserver systemd[1]: Started OpenBSD Secure Shell server.
May 01 19:54:41 webserver sshd[1080]: Accepted password for webmaster from 192.168.1.159 port 22 ssh2
May 01 19:54:41 webserver sshd[1080]: pam_unix(sshd:session): session opened for user webmaster(uid=0)
Hint: Some lines were ellipsized, use -l to show in full.
webmaster@webserver:~$
```

- Here is a screenshot of the command `systemctl status ufw --no-pager`:

```
webmaster@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 2023-05-01 19:22:10 UTC; 42min ago
     Docs: man:ufw(8)
  Main PID: 567 (code=exited, status=0/SUCCESS)
      CPU: 37ms

May 01 19:22:10 webserver systemd[1]: Starting Uncomplicated firewall...
May 01 19:22:10 webserver systemd[1]: Finished Uncomplicated firewall.
webmaster@webserver:~$
```

## Screenshots of the last 10 lines of the following log files

- Here is a screenshot of Apache access logs:

```
webmaster@webserver:~$ tail -n 10 /var/log/apache2/access.log
192.168.1.8 - - [01/May/2023:19:09:20 +0000] "GET /js/scripts.js HTTP/1.1" 200 1024 "http://192.168.1.158/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.8 - - [01/May/2023:19:09:20 +0000] "GET /assets/img/ipad.png HTTP/1.1" 304 250 "http://192.168.1.158/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.8 - - [01/May/2023:19:09:20 +0000] "GET /assets/img/bg-masthead.jpg HTTP/1.1" 304 250 "http://192.168.1.158/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.8 - - [01/May/2023:19:09:20 +0000] "GET /assets/img/demo-image-01.jpg HTTP/1.1" 304 250 "http://192.168.1.158/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.8 - - [01/May/2023:19:09:20 +0000] "GET /assets/img/demo-image-02.jpg HTTP/1.1" 304 250 "http://192.168.1.158/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.8 - - [01/May/2023:19:09:20 +0000] "GET /assets/img/bg-signup.jpg HTTP/1.1" 304 250 "http://192.168.1.158/css/styles.css" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.8 - - [01/May/2023:19:09:20 +0000] "GET /assets/favicon.ico HTTP/1.1" 304 249 "http://192.168.1.158/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
192.168.1.8 - - [01/May/2023:19:10:11 +0000] "-" 408 0 "-" "-"
192.168.1.8 - - [01/May/2023:19:10:11 +0000] "-" 408 0 "-" "-"
192.168.1.1 - - [01/May/2023:19:22:17 +0000] "GET / HTTP/1.1" 200 12963 "-" "-"
```

- Here is a screenshot of Apache error logs:

```
webmaster@webserver:~$ tail -n 10 /var/log/apache2/error.log
[Mon May 01 18:42:26.591743 2023] [core:notice] [pid 761:tid 139717812012928] AH00094: Command line:
'/usr/sbin/apache2'
[Mon May 01 18:45:57.808818 2023] [mpm_event:notice] [pid 761:tid 139717812012928] AH00492: caught S
IGWINCH, shutting down gracefully
[Mon May 01 18:45:57.850527 2023] [mpm_event:notice] [pid 1347:tid 139764741912448] AH00489: Apache/
2.4.52 (Ubuntu) configured -- resuming normal operations
[Mon May 01 18:45:57.850605 2023] [core:notice] [pid 1347:tid 139764741912448] AH00094: Command line
: '/usr/sbin/apache2'
[Mon May 01 18:48:24.017575 2023] [mpm_event:notice] [pid 1347:tid 139764741912448] AH00492: caught
SIGWINCH, shutting down gracefully
[Mon May 01 18:52:32.224702 2023] [mpm_event:notice] [pid 760:tid 140101108909952] AH00489: Apache/2
.4.52 (Ubuntu) configured -- resuming normal operations
[Mon May 01 18:52:32.232881 2023] [core:notice] [pid 760:tid 140101108909952] AH00094: Command line:
'/usr/sbin/apache2'
[Mon May 01 19:14:58.778197 2023] [mpm_event:notice] [pid 760:tid 140101108909952] AH00492: caught S
IGWINCH, shutting down gracefully
[Mon May 01 19:22:13.277326 2023] [mpm_event:notice] [pid 766:tid 140148568074112] AH00489: Apache/2
.4.52 (Ubuntu) configured -- resuming normal operations
[Mon May 01 19:22:13.279891 2023] [core:notice] [pid 766:tid 140148568074112] AH00094: Command line:
'/usr/sbin/apache2'
```

- Here is a screenshot of SSH auth logs:

```
webmaster@webserver:~$ tail -n 10 /var/log/auth.log
May  1 19:22:13 webserver sshd[755]: Server listening on 0.0.0.0 port 22.
May  1 19:22:13 webserver sshd[755]: Server listening on :: port 22.
May  1 19:22:13 webserver systemd-logind[713]: New seat seat0.
May  1 19:22:13 webserver systemd-logind[713]: Watching system buttons on /dev/input/event0 (Power B
utton)
May  1 19:22:13 webserver systemd-logind[713]: Watching system buttons on /dev/input/event1 (Sleep B
utton)
May  1 19:22:13 webserver systemd-logind[713]: Watching system buttons on /dev/input/event2 (AT Tran
slated Set 2 keyboard)
May  1 19:54:41 webserver sshd[1080]: Accepted password for webmaster from 192.168.1.159 port 36270
ssh2
May  1 19:54:41 webserver sshd[1080]: pam_unix(sshd:session): session opened for user webmaster(uid=
1000) by (uid=0)
May  1 19:54:41 webserver systemd-logind[713]: New session 1 of user webmaster.
May  1 19:54:41 webserver systemd: pam_unix(systemd-user:session): session opened for user webmaster
(uid=1000) by (uid=0)
```

## Screenshot of the following configuration

- Here is a screenshot of the sites-available config file:

```
1/1  +  [Icons]  [Close]  Tilix: webmaster@webserver: ~
1: webmaster@webserver: ~
GNU nano 6.2 /etc/apache2/sites-available/my_website.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName my_website
    ServerAlias www.my_website
    DocumentRoot /var/www/my_website
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```



- Here is a screenshot of the apache2.config file:



```
1: webmaster@webserver: ~  
GNU nano 6.2 /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  
# customized anytime.  
#  
# * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/  
# directories contain particular configuration snippets which manage modules,  
# global configuration fragments, or virtual host configurations,  
# respectively.  
#  
# They are activated by symlinking available configuration files from their  
# respective *-available/ counterparts. These should be managed by using our  
# helpers a2enmod/a2dismod, a2ensite/a2dissite and a2enconf/a2disconf. See  
# their respective man pages for detailed information.  
#  
# * The binary is called apache2. Due to the use of environment variables, in  
# the default configuration, apache2 needs to be started/stopped with  
# /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not  
# work with the default configuration.
```

```
# Global configuration
#
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE! If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the Mutex documentation (available
# at <URL:http://httpd.apache.org/docs/2.4/mod/core.html#mutex>);
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
#ServerRoot "/etc/apache2"
#
# The accept serialization lock file MUST BE STORED ON A LOCAL DISK.
#
#Mutex file:${APACHE_LOCK_DIR} default
#
# The directory where shm and other runtime files will be stored.
#

DefaultRuntimeDir ${APACHE_RUN_DIR}

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
# This needs to be set in /etc/apache2/envvars
#
PidFile ${APACHE_PID_FILE}

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.

MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 5

# These need to be set in /etc/apache2/envvars
User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostnameLookups Off

# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
```



```
ErrorLog ${APACHE_LOG_DIR}/error.log

#
# LogLevel: Control the severity of messages logged to the error_log.
# Available values: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the log level for particular modules, e.g.
# "LogLevel info ssl:warn"
#
LogLevel warn

# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

# Include list of ports to listen on
Include ports.conf

# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.

<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>

<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

#<Directory /srv/>
#     Options Indexes FollowSymLinks
#     AllowOverride None
#     Require all granted
#</Directory>

# AccessFileName: The name of the file to look for in each directory
# for additional configuration directives. See also the AllowOverride
# directive.
#
```

```

AccessFileName .htaccess

#
# The following lines prevent .htaccess and .htpasswd files from being
# 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 %O
# (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 %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" 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

```

## Screenshot of the ip address and website being accessed

- Here is a screenshot of the ip address and the website:

