

Deliverable 2

VM Config

These are the specs of the VM for the Ubuntu Server

Oracle VM VirtualBox Manager

File Machine Help

Tools

New Add Settings Discard Show

64 Ubuntu Desktop (Snapshot 3 Lab 3 Co...)

Running

64 Ubuntu Server (Snapshot 1)

Running

General

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

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 128 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: Ubuntu Server.vdi (Normal, 10.00 GB)

Audio

Disabled

Network

Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Wireless-AC 9560 160MHz)

USB

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

Shared folders

None

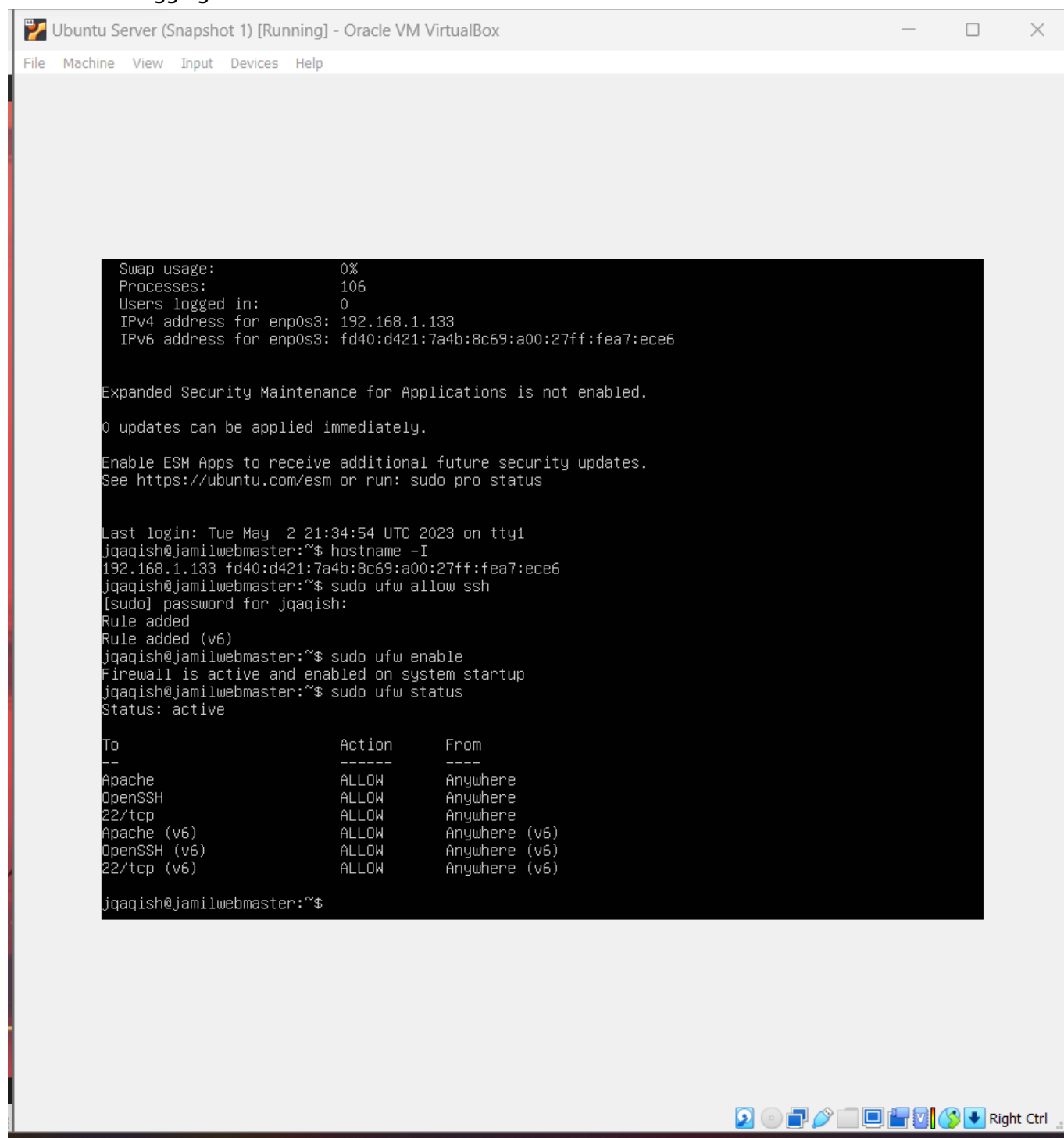
Description

None

Preview

```
root@kali:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
games:x:5:12:games:/usr/games:/usr/sbin/nologin
ftp:x:6:6:ftp:/var:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
cron:x:11:11:cron:/var/spool/cron:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:36:36:www-list:/var/list:/usr/sbin/nologin
_apt:x:37:37:::/var/lib/apt/lists:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:ubuntu:/home/ubuntu:/usr/sbin/nologin
root@kali:~#
```

Screen after logging into the Server



The screenshot shows a terminal window titled "Ubuntu Server (Snapshot 1) [Running] - Oracle VM VirtualBox". The terminal output displays system statistics, security notices, login history, and the configuration of the UFW firewall.

```
Swap usage:          0%
Processes:           106
Users logged in:      0
IPv4 address for enp0s3: 192.168.1.133
IPv6 address for enp0s3: fd40:d421:7a4b:8c69:a00:27ff:fea7:ece6

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: Tue May  2 21:34:54 UTC 2023 on tty1
jqaqish@jamilwebmaster:~$ hostname -I
192.168.1.133 fd40:d421:7a4b:8c69:a00:27ff:fea7:ece6
jqaqish@jamilwebmaster:~$ sudo ufw allow ssh
[sudo] password for jqaqish:
Rule added
Rule added (v6)
jqaqish@jamilwebmaster:~$ sudo ufw enable
Firewall is active and enabled on system startup
jqaqish@jamilwebmaster:~$ sudo ufw status
Status: active

To Action From
--
Apache ALLOW Anywhere
OpenSSH ALLOW Anywhere
22/tcp ALLOW Anywhere
Apache (v6) ALLOW Anywhere (v6)
OpenSSH (v6) ALLOW Anywhere (v6)
22/tcp (v6) ALLOW Anywhere (v6)

jqaqish@jamilwebmaster:~$
```

Command Screenshots

```

https://cis106.com/project/webserverProject/
Tilix: jqaqish@jamilwebmaster: ~

1:jqaqish@jamilwebmaster: ~
jqaqish@jamilwebmaster:~$ 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 09:29:14 UTC; 23min ago
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 761 (apache2)
      Tasks: 55 (limit: 1026)
     Memory: 7.8M
        CPU: 140ms
    CGroup: /system.slice/apache2.service
            └─761 /usr/sbin/apache2 -k start
              765 /usr/sbin/apache2 -k start
              766 /usr/sbin/apache2 -k start

May 08 09:29:14 jamilwebmaster systemd[1]: Starting The Apache HTTP Server...
May 08 09:29:14 jamilwebmaster apache2[752]: AH00558: apache2: Could not r...age
May 08 09:29:14 jamilwebmaster systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
jqaqish@jamilwebmaster:~$ _

```

```

Applications Places
Tilix: jqaqish@jamilwebmaster: ~

1:jqaqish@jamilwebmaster: ~
jqaqish@jamilwebmaster:~$ 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 09:29:14 UTC; 25min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 753 (sshd)
      Tasks: 1 (limit: 1026)
     Memory: 6.8M
        CPU: 114ms
    CGroup: /system.slice/ssh.service
            └─753 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 08 09:44:31 jamilwebmaster sshd[1221]: pam_unix(sshd:auth): authenticat...1.33
May 08 09:44:32 jamilwebmaster sshd[1221]: Failed password for invalid user...ssh2
May 08 09:44:40 jamilwebmaster sshd[1221]: pam_unix(sshd:auth): check pass;...nown
May 08 09:44:42 jamilwebmaster sshd[1221]: Failed password for invalid user...ssh2
May 08 09:45:22 jamilwebmaster sshd[1221]: pam_unix(sshd:auth): check pass;...nown
May 08 09:45:24 jamilwebmaster sshd[1221]: Failed password for invalid user...ssh2
May 08 09:45:25 jamilwebmaster sshd[1221]: Connection closed by invalid use...uth]
May 08 09:45:25 jamilwebmaster sshd[1221]: PAM 2 more authentication failur...1.33
May 08 09:46:09 jamilwebmaster sshd[1224]: Accepted password for jqaqish fr...ssh2
May 08 09:46:09 jamilwebmaster sshd[1224]: pam_unix(sshd:session): session _d=0)
Hint: Some lines were ellipsized, use -l to show in full.

```

```

jqaqish@jamilwebmaster:~$ _

Applications Places

Tilix: jqaqish@jamilwebmaster: ~

1:jqaqish@jamilwebmaster:~ ~

jqaqish@jamilwebmaster:~$ 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 09:29:09 UTC; 26min ago
     Docs: man:ufw(8)
   Main PID: 566 (code=exited, status=0/SUCCESS)
    CPU: 53ms

May 08 09:29:09 jamilwebmaster systemd[1]: Starting Uncomplicated firewall...
May 08 09:29:09 jamilwebmaster systemd[1]: Finished Uncomplicated firewall.
jqaqish@jamilwebmaster:~$ _

```

The last 10 lines of Apache access log

```

Applications Places

Tilix: Jqaqish@Jqaqish-VirtualBox: ~

1:jqaqish@Jqaqish-VirtualBox:~ ~

jqaqish@Jqaqish-VirtualBox:~$ sudo tail -f /var/log
local/ lock/ log/
jqaqish@Jqaqish-VirtualBox:~$ sudo tail -f /var/log/apache2/access.log
[sudo] password for jqaqish:
10.0.2.15 - - [02/May/2023:12:38:52 -0400] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"

```

Last 10 lines of Apache error log

```

Applications Places

Tilix: Jqaqish@Jqaqish-VirtualBox: ~

1:jqaqish@Jqaqish-VirtualBox:~ ~

jqaqish@Jqaqish-VirtualBox:~$ sudo tail -f /var/log/apache2/error.log
[sudo] password for jqaqish:
[Tue May 02 12:40:34.333230 2023] [mpm_event:notice] [pid 5836:tid 140203682293632] AH00489: Apache/2.4.52 (Ubuntu) configured -- resuming normal operations
[Tue May 02 12:40:34.333481 2023] [core:notice] [pid 5836:tid 140203682293632] AH00094: Command line: '/usr/sbin/apache2'
[Tue May 02 12:40:47.823781 2023] [mpm_event:notice] [pid 5836:tid 140203682293632] AH00492: caught SIGWINCH, shutting down gracefully
[Tue May 02 12:40:47.900507 2023] [mpm_event:notice] [pid 5906:tid 140681862064000] AH00489: Apache/2.4.52 (Ubuntu) configured -- resuming normal operations
[Tue May 02 12:40:47.900678 2023] [core:notice] [pid 5906:tid 140681862064000] AH00094: Command line: '/usr/sbin/apache2'
[Tue May 02 12:40:56.957051 2023] [mpm_event:notice] [pid 5906:tid 140681862064000] 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
[Tue May 02 12:40:56.970081 2023] [mpm_event:notice] [pid 5906:tid 140681862064000] AH00489: Apache/2.4.52 (Ubuntu) configured -- resuming normal operations
[Tue May 02 12:40:56.970096 2023] [core:notice] [pid 5906:tid 140681862064000] AH00094: Command line: '/usr/sbin/apache2'
[Tue May 02 12:58:10.352805 2023] [mpm_event:notice] [pid 5906:tid 140681862064000] AH00491: caught SIGTERM, shutting down

```

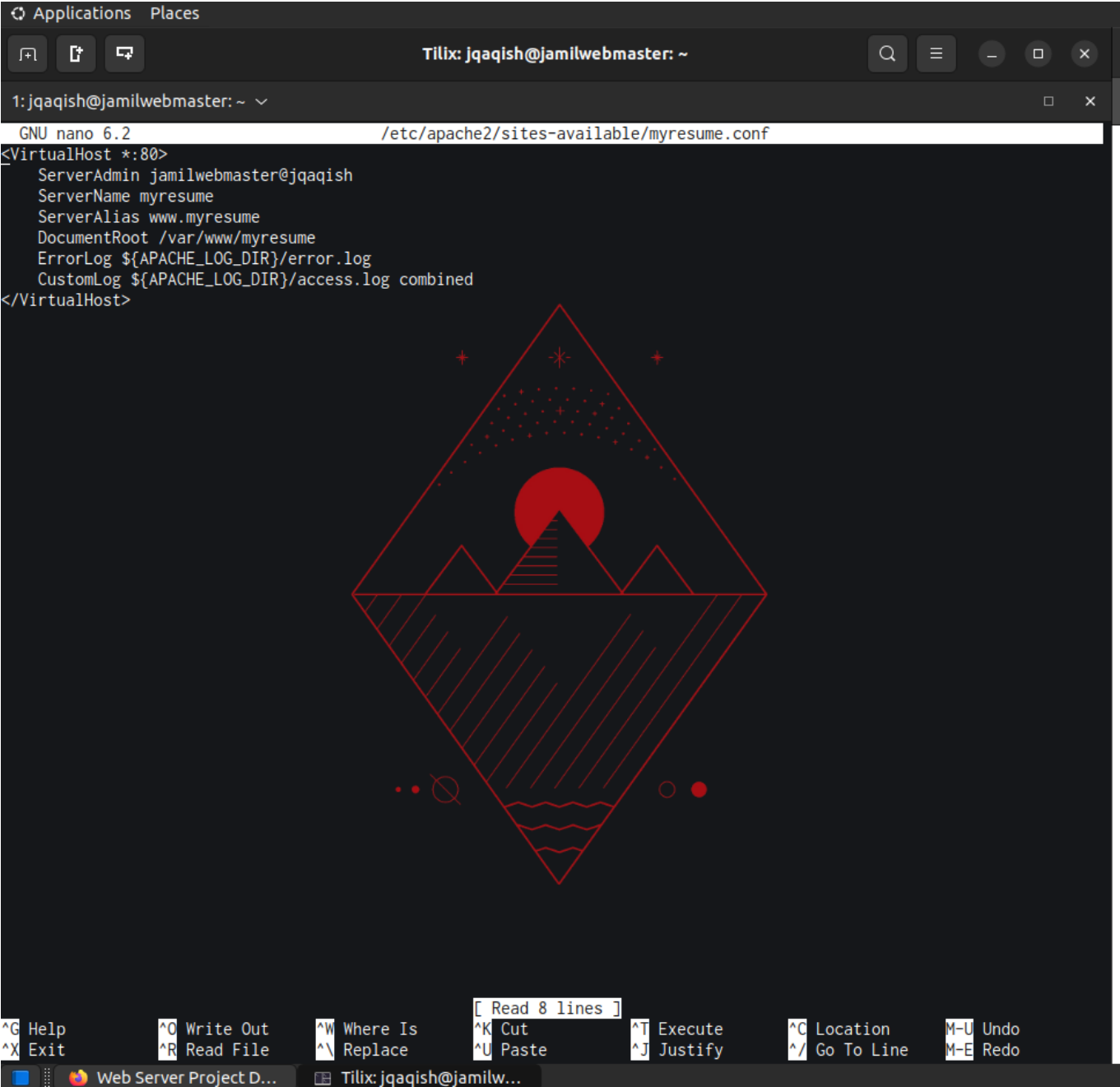
Las 10 lines of SSH auth.log

```

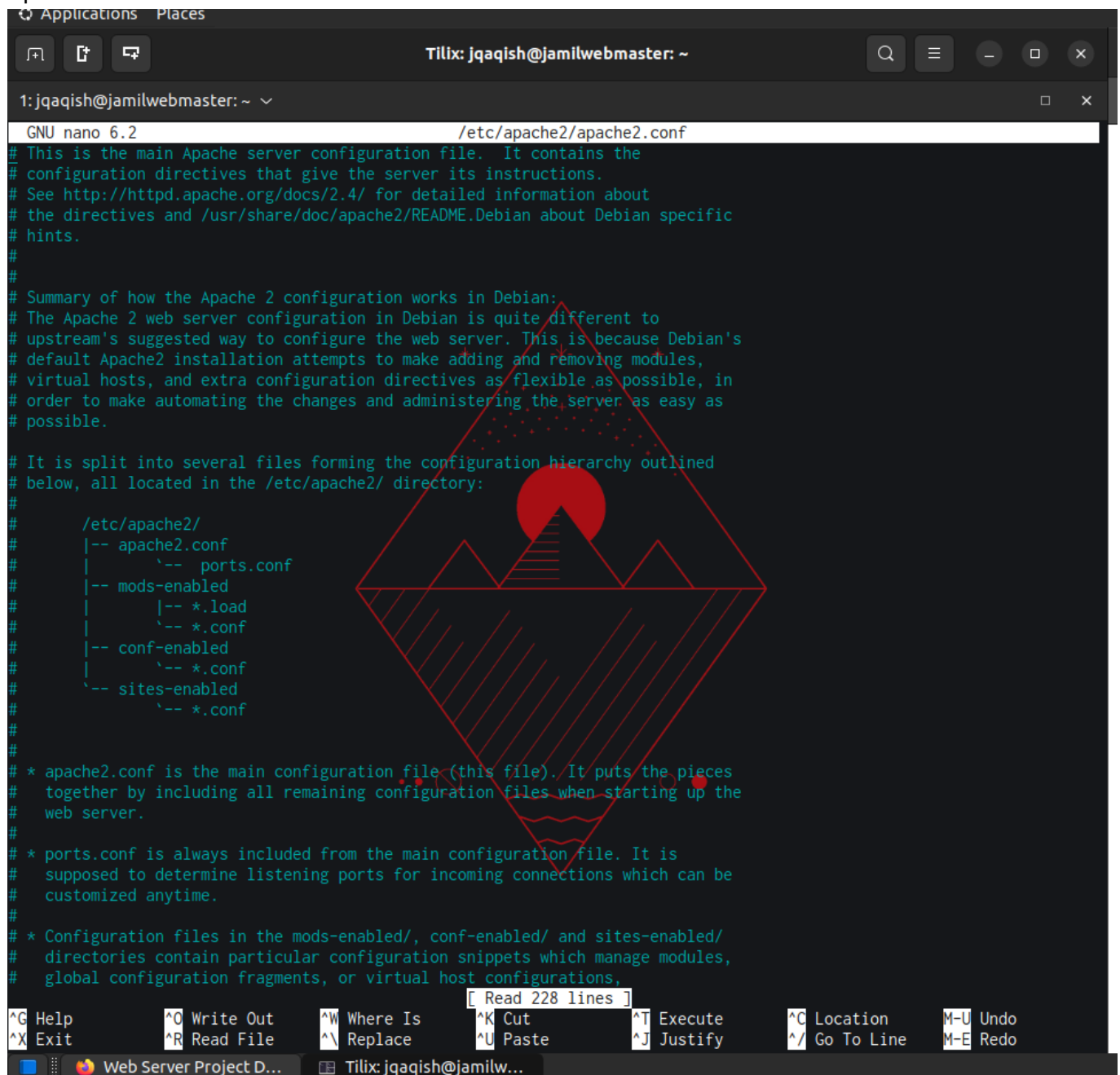
jqaqish@Jqaqish-VirtualBox:~$ sudo grep -m10 sshd /var/log/auth.log
May 2 15:17:14 jqaqish-VirtualBox useradd[4663]: new user: name=sshd, UID=130, GID=65534, home=/run/ssh, shell=/usr/sbin/nologin, from=none
May 2 15:17:14 jqaqish-VirtualBox usermod[4670]: change user 'sshd' password
May 2 15:17:14 jqaqish-VirtualBox chage[4677]: changed password expiry for sshd
May 2 15:17:16 jqaqish-VirtualBox sshd[4787]: Server listening on 0.0.0.0 port 22.
May 2 15:17:16 jqaqish-VirtualBox sshd[4787]: Server listening on :: port 22.
May 8 05:15:24 jqaqish-VirtualBox sshd[733]: Server listening on 0.0.0.0 port 22.
May 8 05:15:24 jqaqish-VirtualBox sshd[733]: Server listening on :: port 22.
May 8 05:27:03 jqaqish-VirtualBox sshd[4606]: Invalid user jamilwebmaster from 10.0.2.15 port 46622
May 8 05:27:12 jqaqish-VirtualBox sshd[4606]: pam_unix(sshd:auth): check pass; user unknown
May 8 05:27:12 jqaqish-VirtualBox sshd[4606]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.15
jqaqish@Jqaqish-VirtualBox:~$ _

```

Site config file



Apache2 conf file



```
Applications  Places

Tilix: jqaqish@jamilwebmaster: ~

1:jqaqish@jamilwebmaster: ~ ▾

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,
[ Read 228 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste      ^J Justify   ^_ Go To Line M-E Redo

Web Server Project D...  Tilix: jqaqish@jamilw...
```

Website Access

