# A7011E Homework 1

Nico Ferrari (nicfer-0@student.ltu.se)

December 11, 2020

## 1. A comparison between the available operating systems for servers

Nowdays, chosing an operating system takes into account several factors, including: security, interface,recovery, costs, disk space etc. The most common OSs in for server, are Linux-based Operating Systems and Windows. Here a brief comparison between the different OSs: Linux based operating systems are based on the Linux kernel. Linux is the core of the operating systems and,according to some definitions of Operating System, can be defined as one itself. Linux is free and open-source so anyone can have access to the source code, modify it, analyze and contribute to the development. This allows to have contributors around the world which audit the software packages and can improve performances and security issues, which is something not possible with proprietary software. Various distributions have been developed based on this, for example Ubuntu. Most of the distributions available are community-driven project, some times even from a single person leading to maintainability problems and none of the distributions is as spread as Windows. One of most popular Linux server distributions, is Red Hat Enterprise Linux (RHEL)[6], first released in 2000 together with Fedora Linux, a free community-supported Linux distribution. New features are first implemented in Fedora and do not reach Red Hat until they are polished. Moreover, Red Hat Enterprise Linux offers 10-year life cycle support instead of an irregular cycle. Being an enterprise distro brings, togheter with patches, updates and upgrades, also expert technical support, and access to training and resources. Red Hat Linux comes with yearly price which can include the support (you can buy a *self-support* package which doesn't include phone/web support in limited time, but only updates, RedHat Knowledgebase and technical content on thir portal). A Linux System Administrator usally have an higher salary over Windows Systems Administrators due to the different required skillsets. While Windows OS try to keep everything as simple as possible creating its own ecosystem, Linux systems try to be as flexible as possible and make large use of scripts.

Windows server is developed by Microsoft and is a closed-source OS. Windows server operating system incurs a licensing cost which depends on the number of cores used. Moreover becomes necessary to buy additional licenses like Client Access Licenses and Management Licenses that gives a user the right to access the services of the server. It is also possible to buy a Software Assurance in order to guarantee support during upgrades and new software releases plus consulting services. Microsoft tries to build an ecosystem, keeping it as easy as possible for the user and/or system administrators. Moreover, since it is the most common operating system for desktop environment, the learning curve might not be as steep as with Linux environment. Due to its widespread and target it is more subject to cyber attacks. Since the OS is not open source, there is not such a huge community contributing to the security issues analysis as big as in Linux based systems.

Another alternative is FreeBSD, an opensource and free Unix-like OS. FreeBSD is famous for its stability and easy UI. It is well documented but not much used. Many software application are not supported by freeBSD and this might represent a big disadvantage. Nevertheless, since it is less used, it is subject to attacks less often, as shown in [2].

Also Solaris Oracle is an option for server OS. It is an Unix-like operating system but results not compatible with some platforms and software. Also Solaris comes with support after paying an yearly amount. New kernel and distibutions are currently being deployed, such as OmniOS [5] based on IllumOS [3] kernel (based on based on OpenSolaris). OmniOS. From a security point of view, illumOS reports only 4 CVE entries in the *https://www.cvedetails.com/* website. This is also because they are not as common as the other OSs. Moreover, they try to be more stable and bring new features to the kernel.

In order to create a webserver and amail server, i would suggest to use Ubuntu LTS. It is opensource but enterprise contracts can be bought in order to have support. Moreover each release will be supported for several years, improving then the stability of the OS and its maintenance. Now-days, the tool enabling web server and mail server are becoming much easier to configure thanks to new UI. If the employees already have knowledge in Linux Administration, it would be possible also to no install any Desktop environment, saving then resources.

## 2. cloud computing model and also a virtualization model

Cloud computing brings several benefits in terms of costs, because the company doesn't need to maintain its own hardware infrastructure. This technology, together with its benefits, brings also several security challenges, as described in [7] [1]. For a cloud computing model, Microsoft offers some plans with prices with change according to the amount of cores, ram and type of CPU[4]. Linux OSs are free so the do not need any license but, you must pay the support if required (as described before). Moreover, Linux usually required much less resources, becoming cheaper to host. In case of a virtualised model instead, Windows Server offers a *datacenter* edition, which is almost 10 time more expensiove than the normal windows server edition but allows the use of virtual machines on it. Also RedHat has a similar license, which becomes an advantage whene the company decides to run more than 7/8 virtual machines with RedHat. If the support is something not needed because the company already has the knowledge necessary to maintain it, I would definitely suggest to use a Linux OS without support, such as Ubuntu, which anyway has plenty of documentation. Windows, as described before, is the most user friendly OS, but becomes really expensive especially with few VMs.

## 3. Have you successfully completed Lab assignment (2)

For lab 2, beside using passwords which are 'stronger' than the ones suggested, I turned of the the internet connection (in this case NAT during the installation) (Figure 1) and decided to check the 'Enable Disk Encryption' check box as shown in Figure 2. The NAT connection has been enabled after the installation, in order to check for updates and install them (Figure 4). Other hardening operations have been to create a *security* group and add to this group the ltu user.

- FTP: i created a ssl key for ftp with the command: *openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/certificates/vsftpd.pem -out /etc/ssl/certificates/vsftpd.pem* and then I configured the settings in the vsftpd.conf file to use ssl encryption. in this way a layer of protection will be introduced over ftp. moreover also anonymous authentication is disabled (Figure 31).
- SSH: I allowed to perform ssh connections only the users of a specific group (security) and limited the amount of connection tries and connection at the same time (Shown in figure 12). If i will try to perform an ssh connection using a user which is not in the security group, the connection will not be allowed, as shown in Figure 13.

Figure 1:

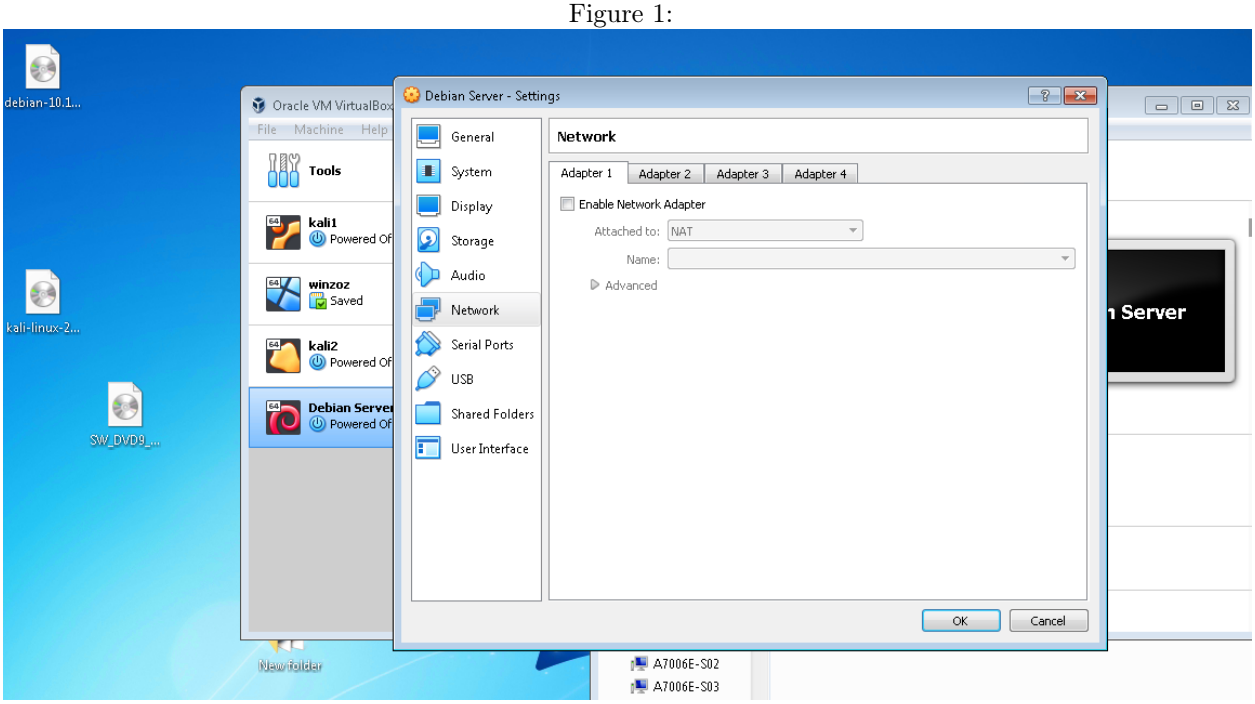



Figure 2:

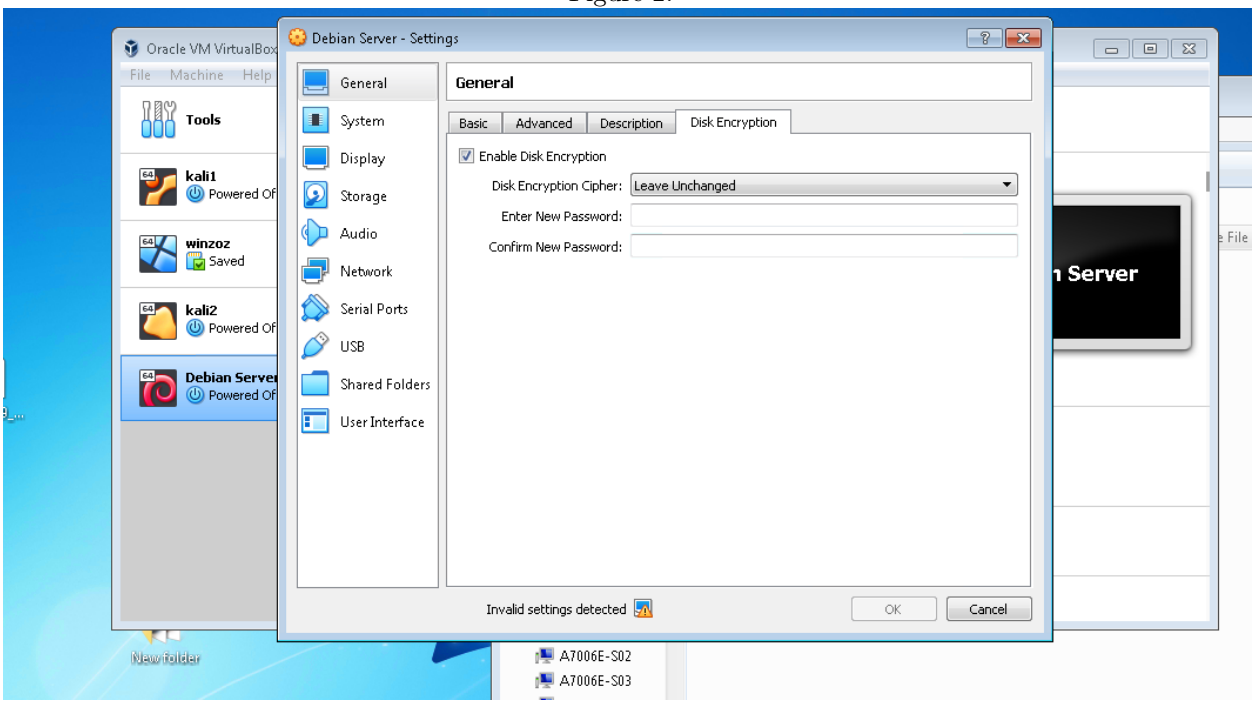


Figure 3:

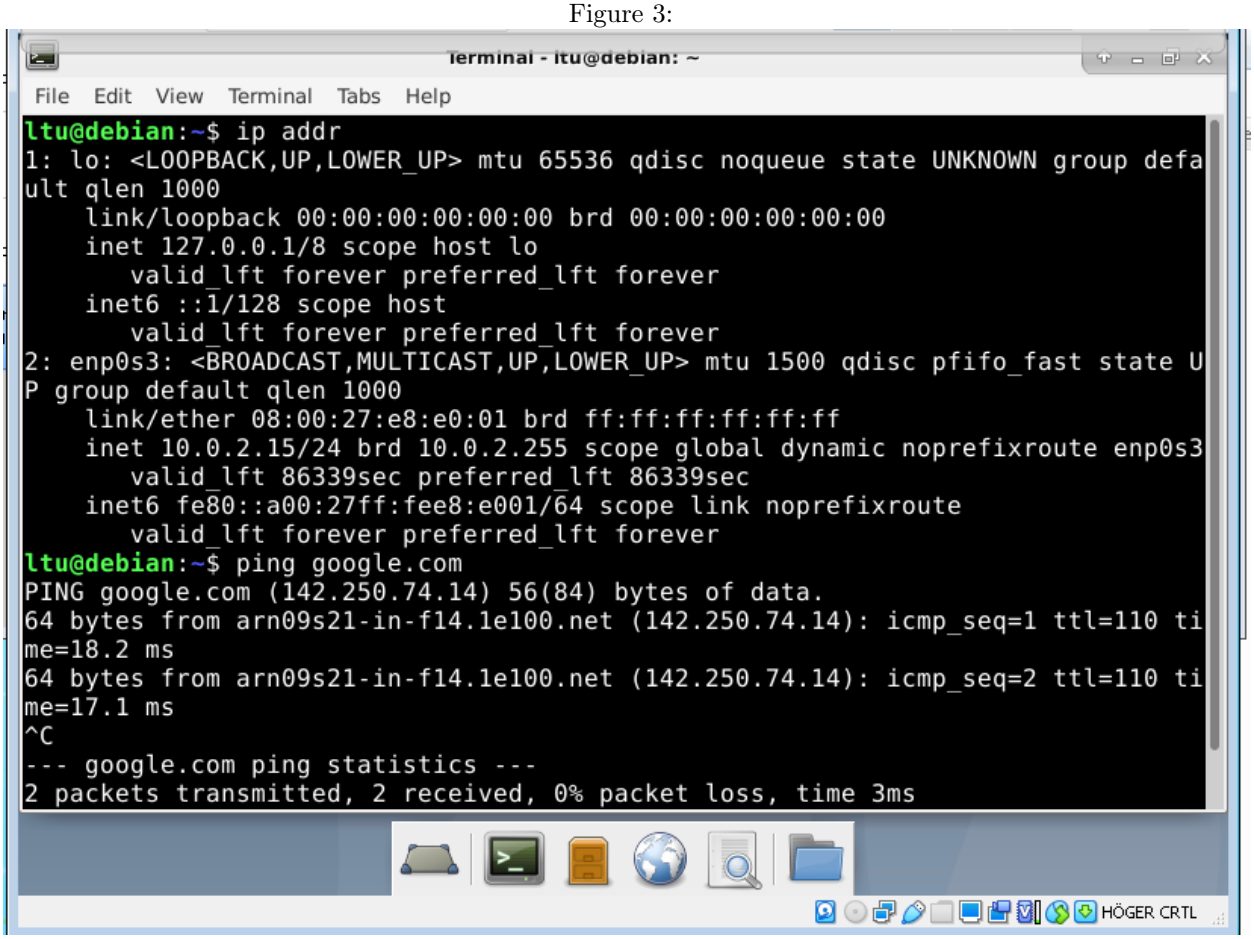
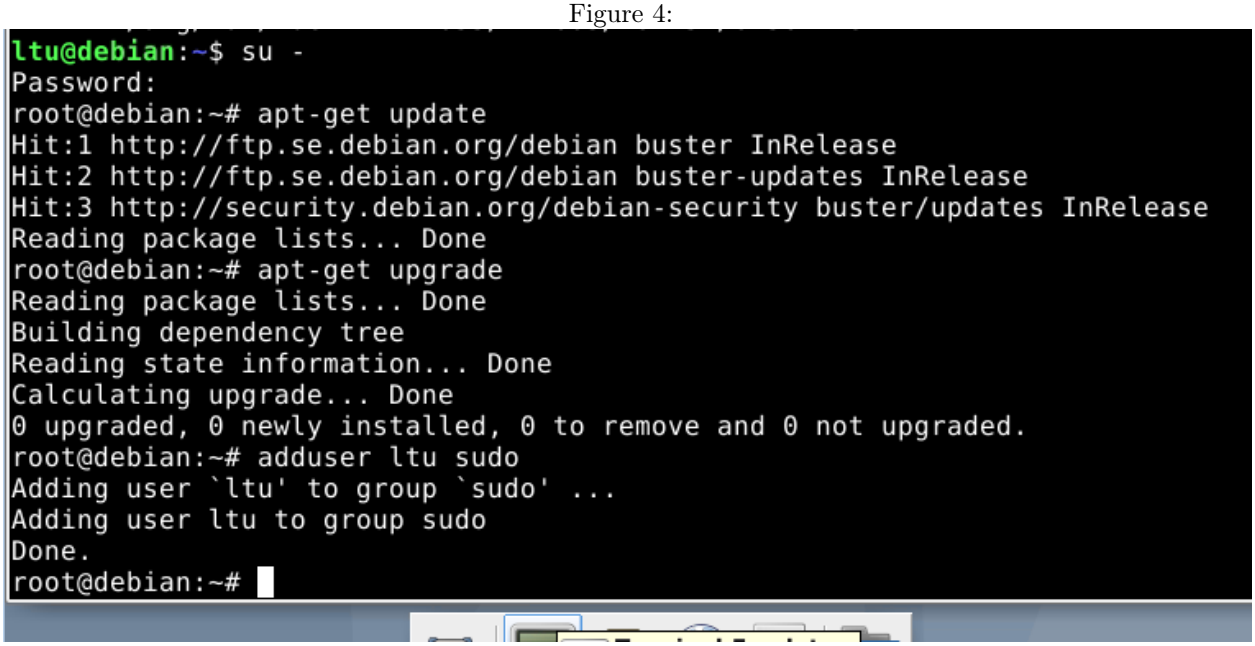

Terminal - ltu@debian: ~
File Edit View Terminal Tabs Help
ltu@debian:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state U
P group default qlen 1000
link/ether 08:00:27:e8:e0:01 brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
valid_lft 86339sec preferred_lft 86339sec
inet6 fe80::a00:27ff:fee8:e001/64 scope link noprefixroute
valid_lft forever preferred_lft forever
ltu@debian:~$ ping google.com
PING google.com (142.250.74.14) 56(84) bytes of data.
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=1 ttl=110 ti
me=18.2 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=2 ttl=110 ti
me=17.1 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
HÖGER CRTL

Figure 4:



```
ltu@debian:~$ su -
Password:
root@debian:~# apt-get update
Hit:1 http://ftp.se.debian.org/debian buster InRelease
Hit:2 http://ftp.se.debian.org/debian buster-updates InRelease
Hit:3 http://security.debian.org/debian-security buster/updates InRelease
Reading package lists... Done
root@debian:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@debian:~# adduser ltu sudo
Adding user `ltu' to group `sudo' ...
Adding user ltu to group sudo
Done.
root@debian:~#
```

Figure 5:

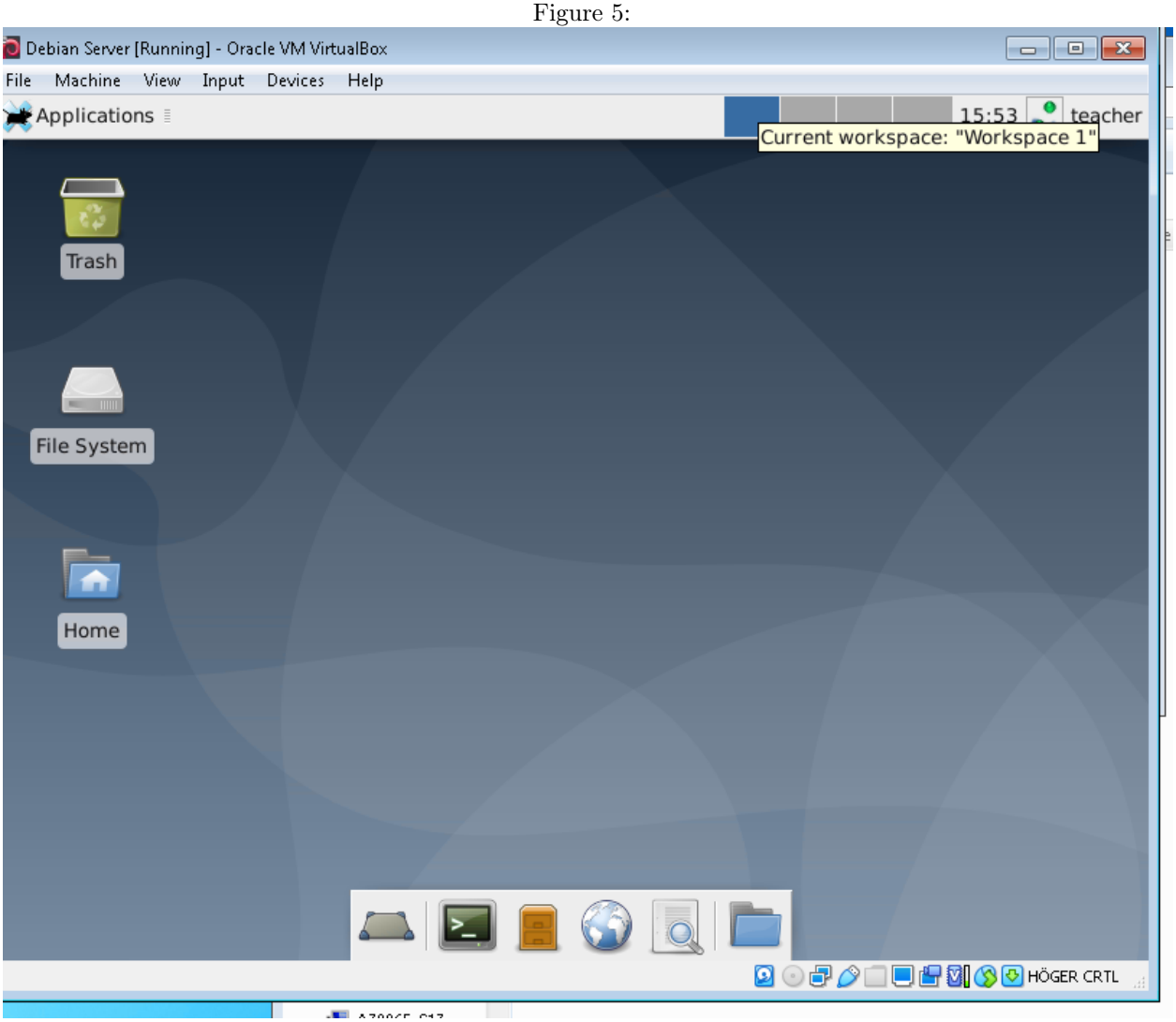



Figure 6:

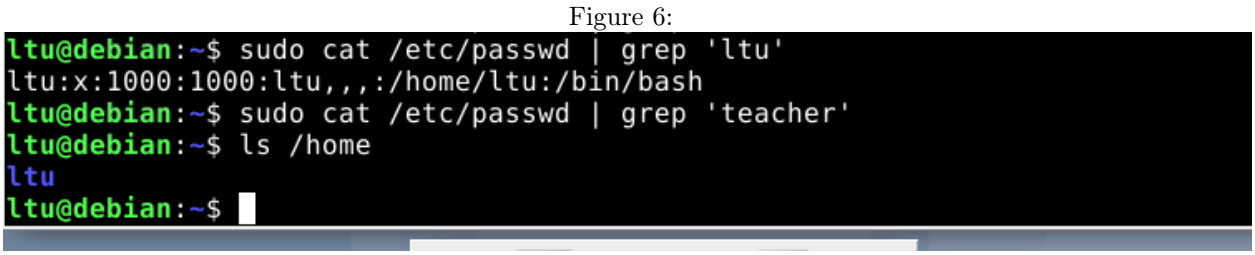
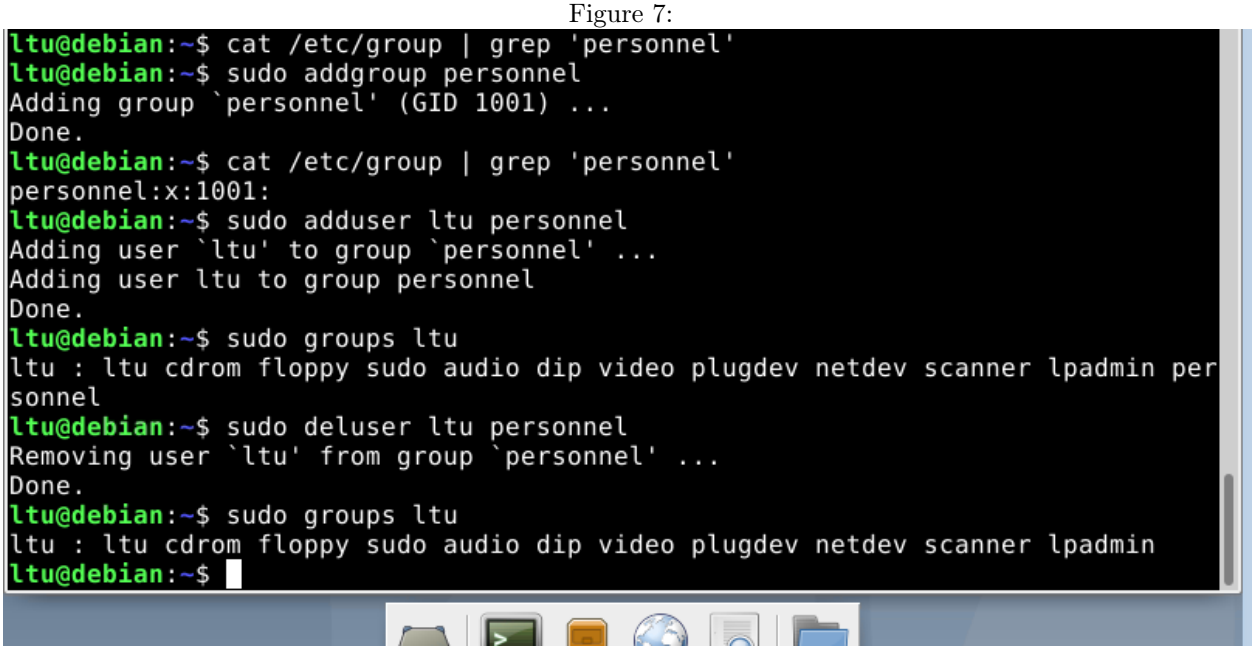


Figure 7:



```
ltu@debian:~$ cat /etc/group | grep 'personnel'
ltu@debian:~$ sudo addgroup personnel
Adding group `personnel' (GID 1001) ...
Done.
ltu@debian:~$ cat /etc/group | grep 'personnel'
personnel:x:1001:
ltu@debian:~$ sudo adduser ltu personnel
Adding user `ltu' to group `personnel' ...
Adding user ltu to group personnel
Done.
ltu@debian:~$ sudo groups ltu
ltu : ltu cdrom floppy sudo audio dip video plugdev netdev scanner lpadmin per
sonnel
ltu@debian:~$ sudo deluser ltu personnel
Removing user `ltu' from group `personnel' ...
Done.
ltu@debian:~$ sudo groups ltu
ltu : ltu cdrom floppy sudo audio dip video plugdev netdev scanner lpadmin
ltu@debian:~$
```

Figure 8:

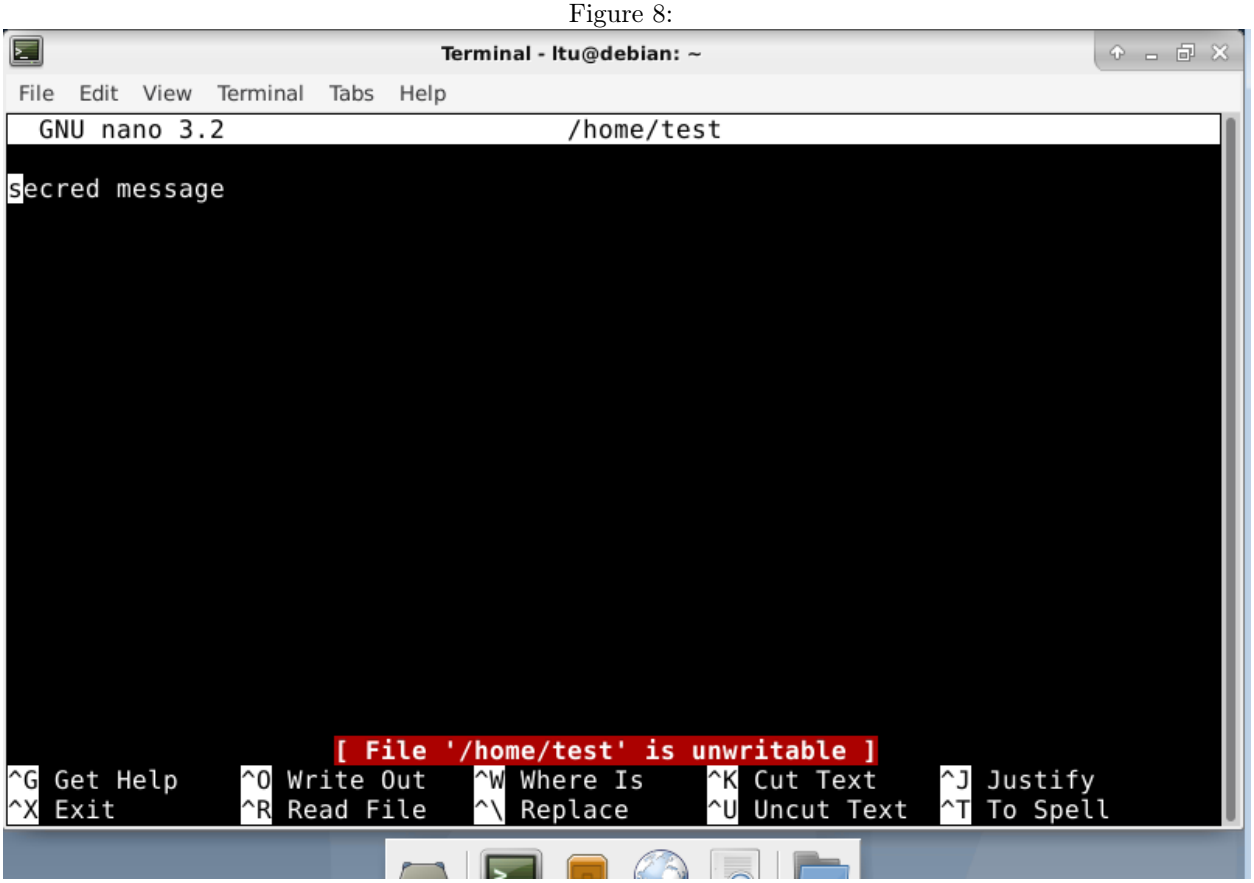

Terminal - ltu@debian: ~
File Edit View Terminal Tabs Help
GNU nano 3.2 /home/test
secred message
[ File '/home/test' is unwritable ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell

Figure 9:

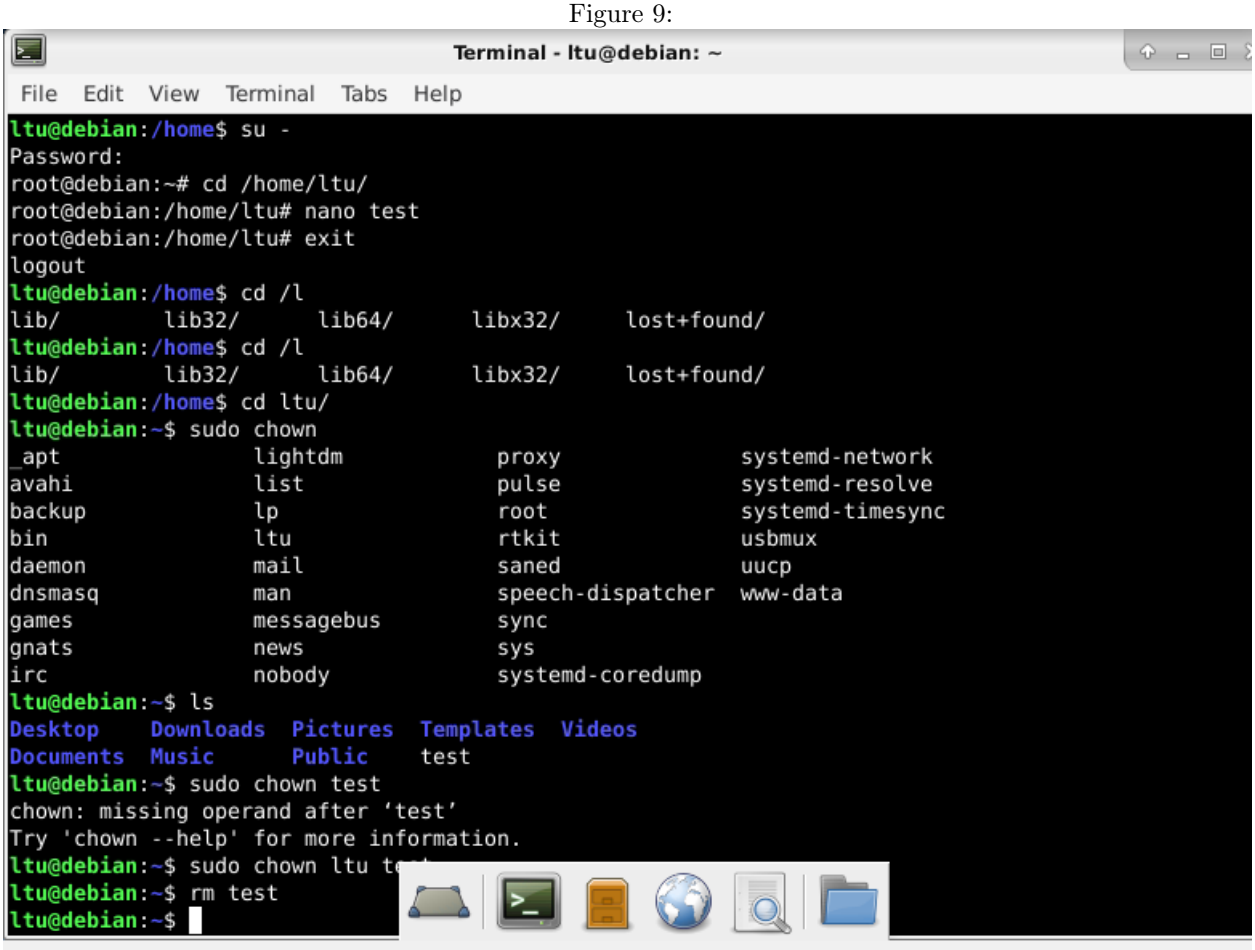

Terminal - ltu@debian: ~
File Edit View Terminal Tabs Help
ltu@debian:/home$ su -
Password:
root@debian:~# cd /home/ltu/
root@debian:/home/ltu# nano test
root@debian:/home/ltu# exit
logout
ltu@debian:/home$ cd /l
lib/ lib32/ lib64/ libx32/ lost+found/
ltu@debian:/home$ cd /l
lib/ lib32/ lib64/ libx32/ lost+found/
ltu@debian:/home$ cd ltu/
ltu@debian:~$ sudo chown
_apt lightdm proxy systemd-network
avahi list pulse systemd-resolve
backup lp root systemd-timesync
bin ltu rtkit usbmux
daemon mail saned uucp
dnsmasq man speech-dispatcher www-data
games messagebus sync
gnats news sys
irc nobody systemd-coredump
ltu@debian:~$ ls
Desktop Downloads Pictures Templates Videos
Documents Music Public test
ltu@debian:~$ sudo chown test
chown: missing operand after 'test'
Try 'chown --help' for more information.
ltu@debian:~$ sudo chown ltu
ltu@debian:~$ rm test
ltu@debian:~$

Figure 10:

```
ltu@debian:~$ su -
Password:
root@debian:~# cd /home/ltu/
root@debian:/home/ltu# nano secret
root@debian:/home/ltu# exit
logout
ltu@debian:~$ sudo chmod 777 secret
ltu@debian:~$ echo "test">> secret
ltu@debian:~$ cat secret
secret message
test
ltu@debian:~$ sudo chown ltu test
chown: cannot access 'test': No such file or directory
ltu@debian:~$ sudo chown ltu secret
ltu@debian:~$ ls -l secret
-rwxrwxrwx 1 ltu root 20 Nov 22 16:23 secret
ltu@debian:~$ chmod 755 secret
ltu@debian:~$ ls -l secret
-rwxr-xr-x 1 ltu root 20 Nov 22 16:23 secret
ltu@debian:~$ rm secret
ltu@debian:~$
```

part regarding SSH

Figure 11:

```
ltu@debian:~$ sudo dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:YBFhnf1KmHlSHfcikglOEzS9lDLSalMj4eUyEBEr3tk root@debian (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:zI269rplbjrj4/36fnrrpNOgqYetpoXiSjEK486Z/jI root@debian (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:d/ePawoZ5gQVQDngMXzdIAOCryt603t+bZRWAvJSVJA root@debian (ED25519)
rescue-ssh.target is a disabled or a static unit, not starting it.
ltu@debian:~$ sudo /etc/init.d/ssh start
[ ok ] Starting ssh (via systemctl): ssh.service.
ltu@debian:~$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:zI269rplbjrj4/36fnrrpNOgqYetpoXiSjEK486Z/jI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
ltu@localhost's password:
Linux debian 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes w                                                  extent
```

File Manager
Browse the file system

Figure 12:

```
File  Edit  View  Terminal  Tabs  Help
  GNU nano 3.2                    /etc/ssh/sshd_config

#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server
AllowGroups security
MaxAuthTries 3
MaxSessions 2
MaxStartups 2

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo
```

SSL> and </IfDefine> tags that enclose your SSL configuration.

Figure 13:

```
root@debian:~# ssh student@127.0.0.1
student@127.0.0.1's password:
Linux debian 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Could not chdir to home directory /home/student: No such file or directory
$ ls
bin   dev  home        initrd.img.old  lib32  libx32      media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lib64  lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
$ rm home
rm: cannot remove 'home': Is a directory
$ exit
Connection to 127.0.0.1 closed.
root@debian:~# useradd uselessUser
root@debian:~# passwd uselessUser
New password:
Retype new password:
passwd: password updated successfully
root@debian:~# ssh uselessUser@127.0.0.1
uselessUser@127.0.0.1's password:
Permission denied, please try again.
uselessUser@127.0.0.1's password:
```

Part regarding SAMBA:

Figure 14:

```
root@debian:~# sudo systemctl restart smbd.service
root@debian:~# nano -c /etc/samba/smb.conf
root@debian:~# sudo systemctl restart smbd.service
root@debian:~# smbclient //localhost/share
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Nov 22 16:48:08 2020
  ..                                  D        0  Sun Nov 22 16:48:08 2020

                11802792 blocks of size 1024. 7372256 blocks available
smb: \> exit
root@debian:~#
```

Figure 15:

```
root@debian:~# chmod 770 /home/security/
root@debian:~# nano -c /etc/samba/smb.conf
root@debian:~# smbpasswd -a ltu
New SMB password:
Retype new SMB password:
Mismatch - password unchanged.
Unable to get new password.
root@debian:~# smbpasswd -a ltu
New SMB password:
Retype new SMB password:
Added user ltu.
root@debian:~# usermod -G security ltu
root@debian:~# sudo systemctl res
rescue        reset-failed  restart
root@debian:~# sudo systemctl res
rescue        reset-failed  restart
root@debian:~# sudo systemctl restart smbd.service
```

Figure 16:

```
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: e
   Active: active (running) since Sun 2020-11-22 17:07:38 CST; 1min 29s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 3195 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (c
 Main PID: 3204 (smbd)
   Status: "smbd: ready to serve connections..."
    Tasks: 4 (limit: 4915)
   Memory: 6.7M
   CGroup: /system.slice/smbd.service
           ├─3204 /usr/sbin/smbd --foreground --no-process-group
           ├─3206 /usr/sbin/smbd --foreground --no-process-group
           ├─3207 /usr/sbin/smbd --foreground --no-process-group
           └─3208 /usr/sbin/smbd --foreground --no-process-group

Nov 22 17:07:38 debian systemd[1]: Starting Samba SMB Daemon...
Nov 22 17:07:38 debian systemd[1]: Started Samba SMB Daemon.
lines 1-19
```

Figure 17:

```
root@debian:~# testparm
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Registered MSG_REQ_POOL_USAGE
Registered MSG_REQ_DMALLOC_MARK and LOG_CHANGED
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Processing section "[share]"
Processing section "[Security]"
Unknown parameter encountered: "share mode"
Ignoring unknown parameter "share mode"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions
```

Figure 18:

```
root@debian:~# useradd student
root@debian:~# passwd student
New password:
Retype new password:
passwd: password updated successfully
root@debian:~# smbpasswd -a student
New SMB password:
Retype new SMB password:
Added user student.
root@debian:~# usermod -G security student
root@debian:~# sudo systemctl restart smbd.service
root@debian:~# smbclient //localhost/security -U student
Enter WORKGROUP\student's password:
Try "help" to get a list of possible commands.
smb: \> exit
root@debian:~#
```

DHCP

Figure 19:

```
ltu@debian: ~                                   ltu@debian: ~
ltu@debian:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qle
n 1000
    link/ether 08:00:27:e8:e0:01 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86360sec preferred_lft 86360sec
    inet6 fe80::a00:27ff:fee8:e001/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qle
n 1000
    link/ether 08:00:27:ae:38:33 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.30/24 brd 10.0.0.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feae:3833/64 scope link
       valid_lft forever preferred_lft forever
```

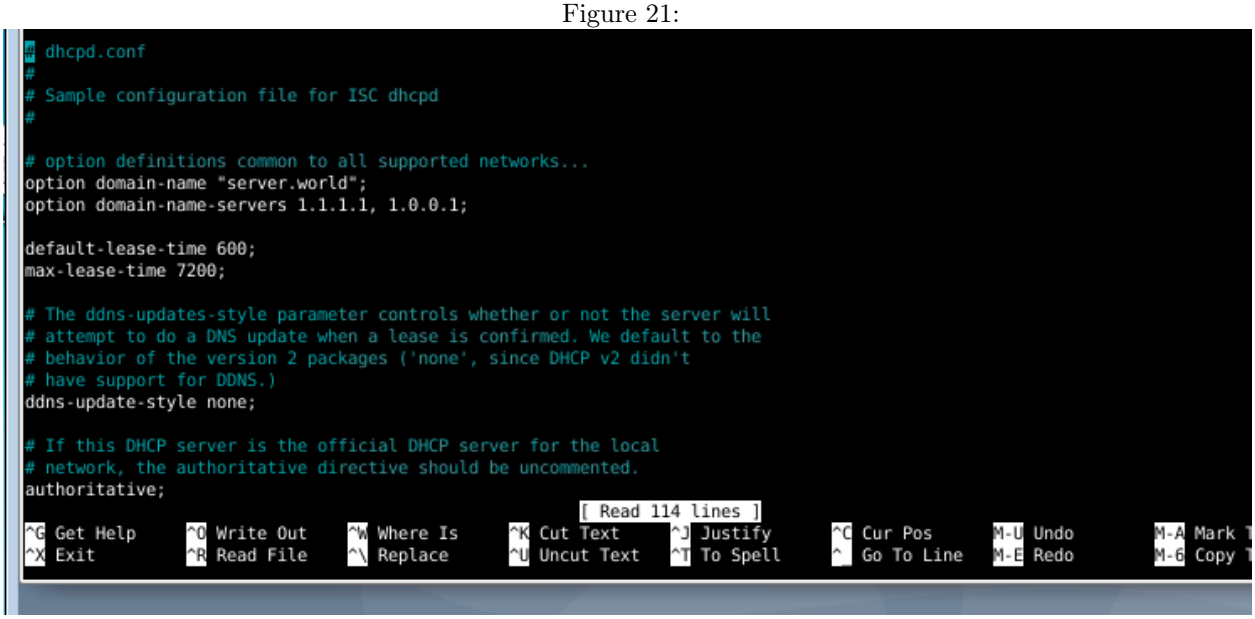
Figure 20:

```
  GNU nano 3.2                    /etc/dhcp/dhcpd.conf

#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
noipv6rs;
noipv6;
subnet 10.0.0.0 netmask 255.255.255.0 {
        option routers 10.0.0.30;
        option subnet-mask 255.255.255.0;
        range dynamic-bootp 10.0.0.200 10.0.0.254;
}

                    [ line 115/115 (100%), col 1/1 (100%), char 3646/3646 (100%) ]
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Tex
^X Exit       ^R Read File   ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo   M-6 Copy Tex
```

Figure 21:




WebServer

Figure 22:

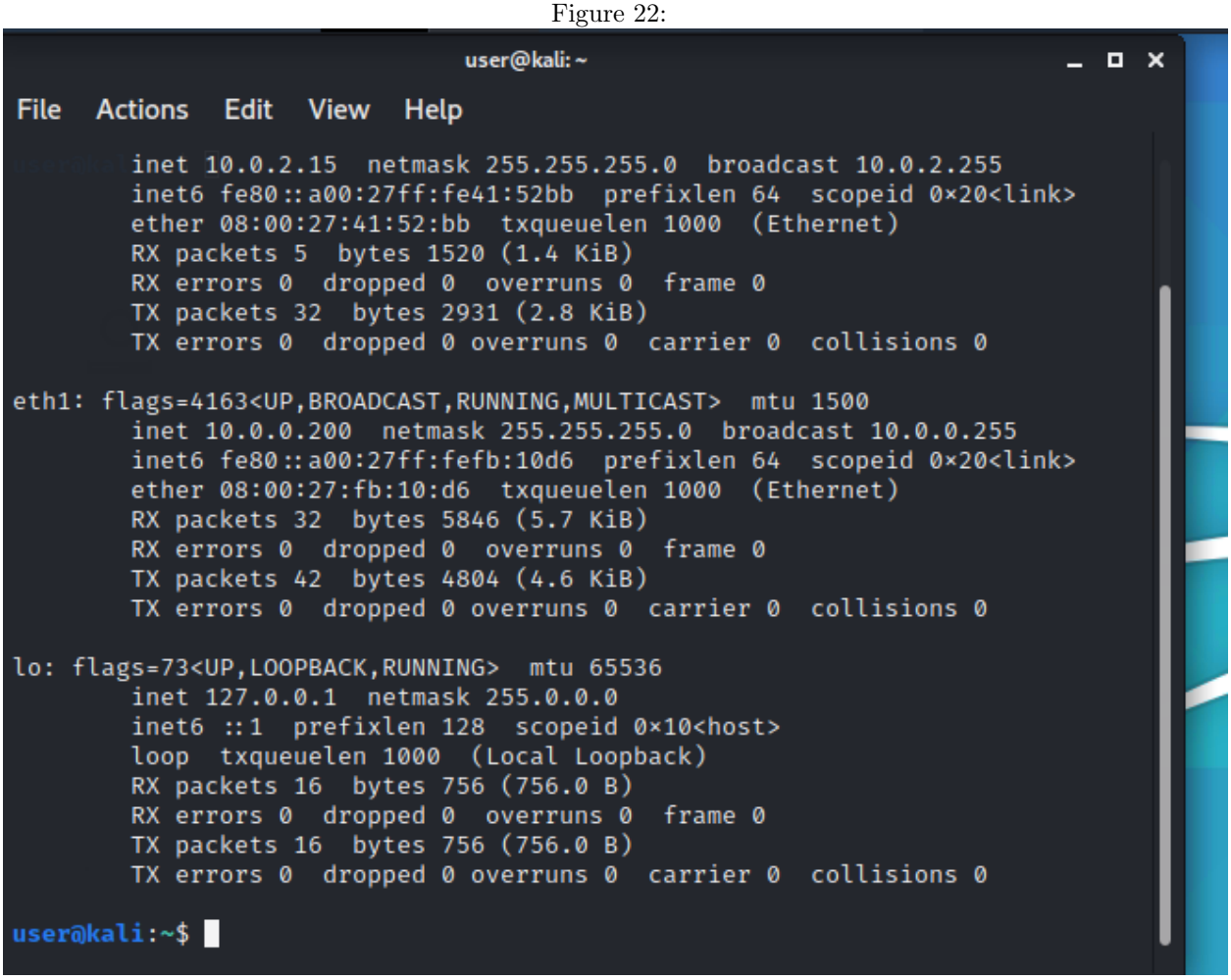

user@kali: ~
File Actions Edit View Help
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe41:52bb prefixlen 64 scopeid 0x20<link>
ether 08:00:27:41:52:bb txqueuelen 1000 (Ethernet)
RX packets 5 bytes 1520 (1.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 32 bytes 2931 (2.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.0.200 netmask 255.255.255.0 broadcast 10.0.0.255
inet6 fe80::a00:27ff:fefb:10d6 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:fb:10:d6 txqueuelen 1000 (Ethernet)
RX packets 32 bytes 5846 (5.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 42 bytes 4804 (4.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 16 bytes 756 (756.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16 bytes 756 (756.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
user@kali:~$

Figure 23:

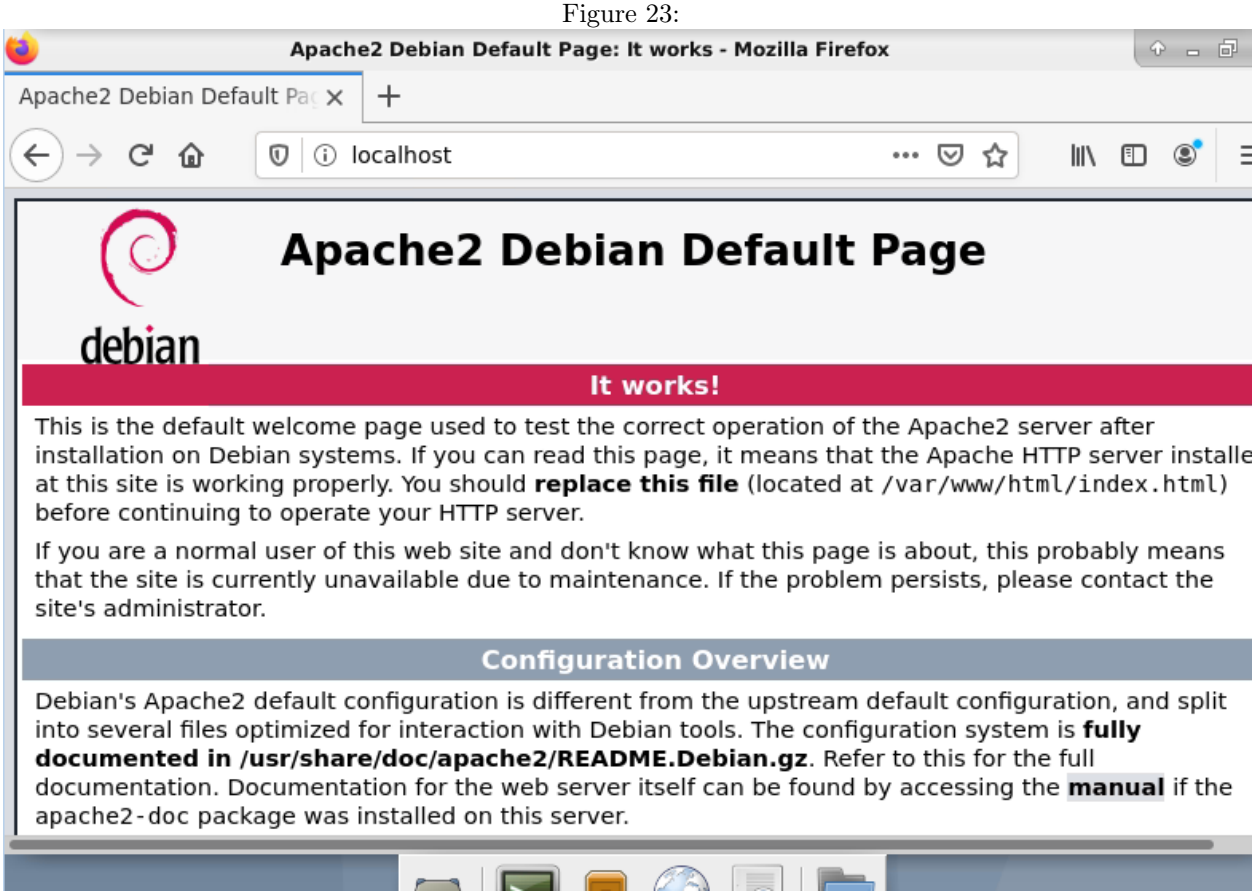

Apache2 Debian Default Page: It works - Mozilla Firefox
Apache2 Debian Default Pa
localhost
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installe at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.

Figure 24:

```
root@debian:~# sudo /etc/init.d/apache2 restart
[ ok ] Restarting apache2 (via systemctl): apache2.service.
root@debian:~# systemctl status mysql.service
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-11-23 02:02:02 CST; 40min ago
     Docs: man:mysqld(8)
           http://dev.mysql.com/doc/refman/en/using-systemd.html
  Process: 550 ExecStartPre=/usr/share/mysql-8.0/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
 Main PID: 629 (mysqld)
   Status: "Server is operational"
    Tasks: 37 (limit: 4915)
   Memory: 413.5M
   CGroup: /system.slice/mysql.service
           └─629 /usr/sbin/mysqld

Nov 23 02:01:52 debian systemd[1]: Starting MySQL Community Server...
Nov 23 02:01:57 debian mysqld[629]: 2020-11-23T08:01:57.745972Z 0 [System] [MY-010116] [Server] /usr/sbin/mysqld (mysqld 8.0.22)
Nov 23 02:01:57 debian mysqld[629]: 2020-11-23T08:01:57.908687Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started
Nov 23 02:02:00 debian mysqld[629]: 2020-11-23T08:02:00.211704Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.
Nov 23 02:02:01 debian mysqld[629]: 2020-11-23T08:02:01.326853Z 0 [System] [MY-011323] [Server] X Plugin ready for connections. B
Nov 23 02:02:02 debian mysqld[629]: 2020-11-23T08:02:02.064569Z 0 [Warning] [MY-010068] [Server] CA certificate ca.pem is self si
Nov 23 02:02:02 debian mysqld[629]: 2020-11-23T08:02:02.075986Z 0 [System] [MY-013602] [Server] Channel mysql_main configured to
Nov 23 02:02:02 debian mysqld[629]: 2020-11-23T08:02:02.299637Z 0 [System] [MY-010931] [Server] /usr/sbin/mysqld: ready for conne
Nov 23 02:02:02 debian systemd[1]: Started MySQL Community Server.
lines 1-22/22 (END)
```

Figure 25:

```
ltu@debian: ~                                   ltu@debian: ~

root@debian:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

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> select User,Host from mysql.user;
+------------------+-----------+
| User             | Host      |
+------------------+-----------+
| mysql.infoschema | localhost |
| mysql.session    | localhost |
| mysql.sys        | localhost |
| root             | localhost |
+------------------+-----------+
4 rows in set (0.01 sec)

mysql>
```

Figure 26:

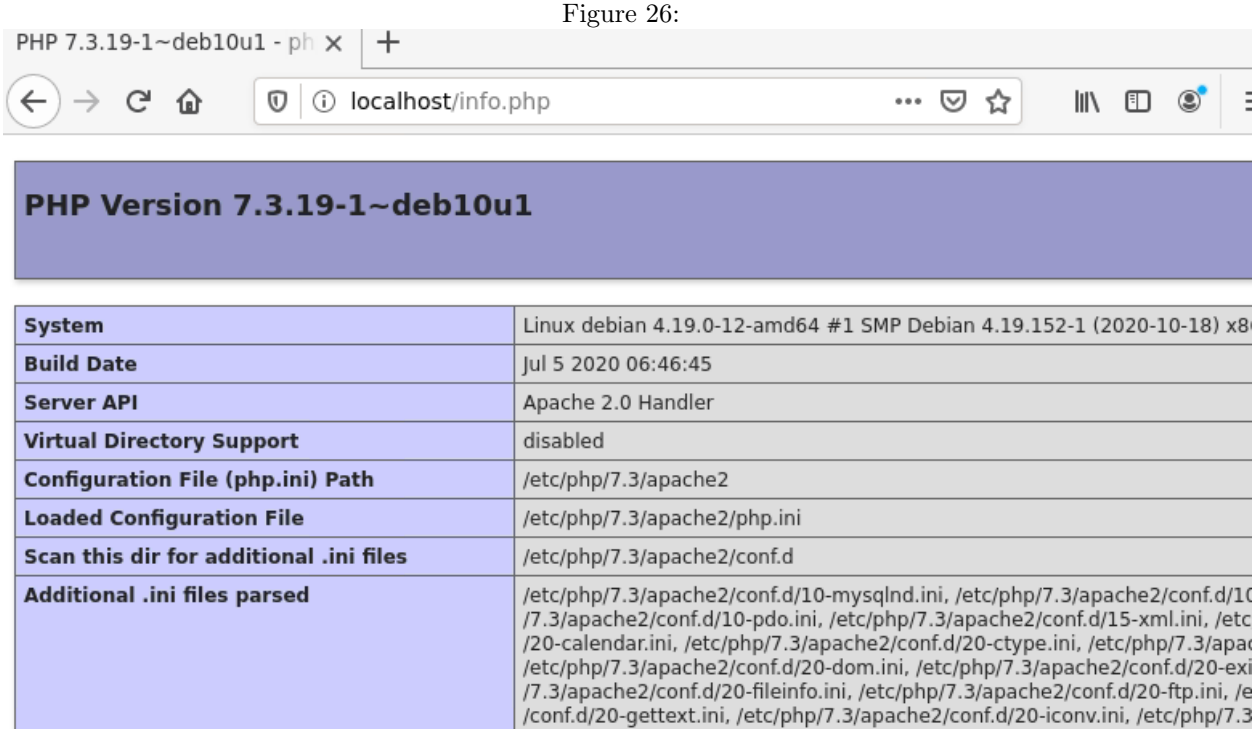
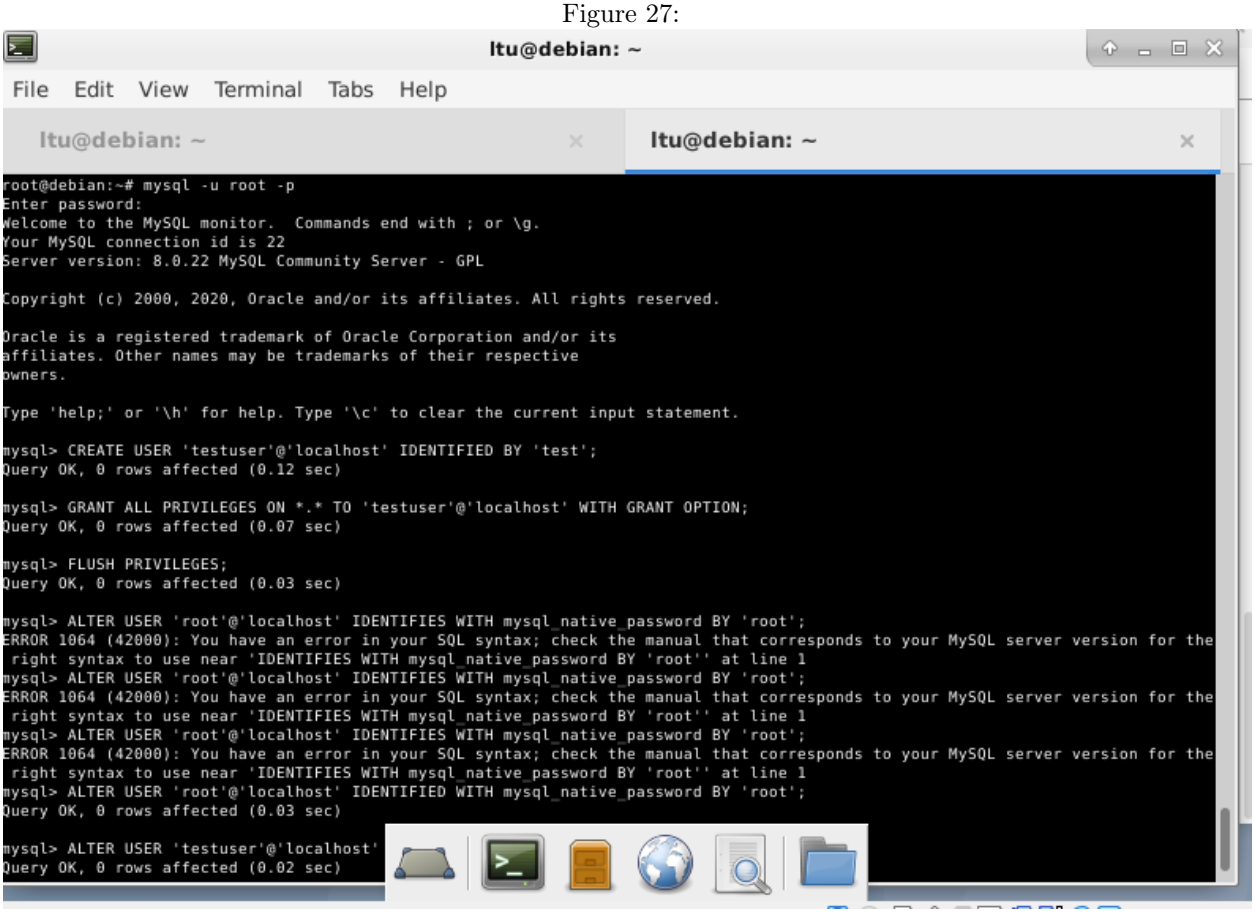

PHP 7.3.19-1~deb10u1 - ph
localhost/info.php
PHP Version 7.3.19-1~deb10u1
System
Linux debian 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x8
Build Date
Jul 5 2020 06:46:45
Server API
Apache 2.0 Handler
Virtual Directory Support
disabled
Configuration File (php.ini) Path
/etc/php/7.3/apache2
Loaded Configuration File
/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files
/etc/php/7.3/apache2/conf.d
Additional .ini files parsed
/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/1
/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc
/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apa
/etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exi
/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /e
/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3

Figure 27:



```
root@debian:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 22
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

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> CREATE USER 'testuser'@'localhost' IDENTIFIED BY 'test';
Query OK, 0 rows affected (0.12 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'testuser'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (0.07 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.03 sec)

mysql> ALTER USER 'root'@'localhost' IDENTIFIES WITH mysql_native_password BY 'root';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the
 right syntax to use near 'IDENTIFIES WITH mysql_native_password BY 'root'' at line 1
mysql> ALTER USER 'root'@'localhost' IDENTIFIES WITH mysql_native_password BY 'root';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the
 right syntax to use near 'IDENTIFIES WITH mysql_native_password BY 'root'' at line 1
mysql> ALTER USER 'root'@'localhost' IDENTIFIES WITH mysql_native_password BY 'root';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the
 right syntax to use near 'IDENTIFIES WITH mysql_native_password BY 'root'' at line 1
mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'root';
Query OK, 0 rows affected (0.03 sec)

mysql> ALTER USER 'testuser'@'localhost'
Query OK, 0 rows affected (0.02 sec)
```

Figure 28:

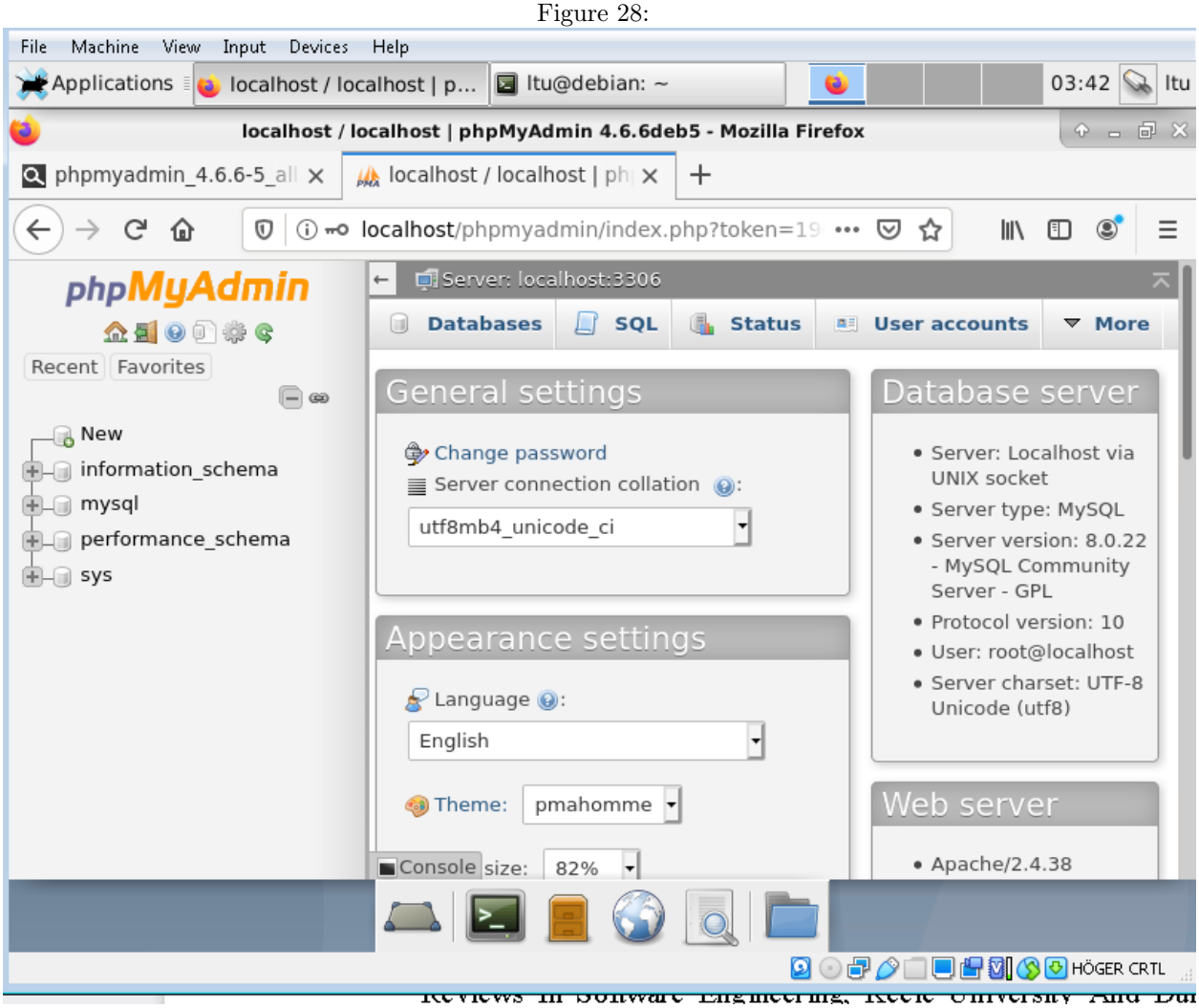
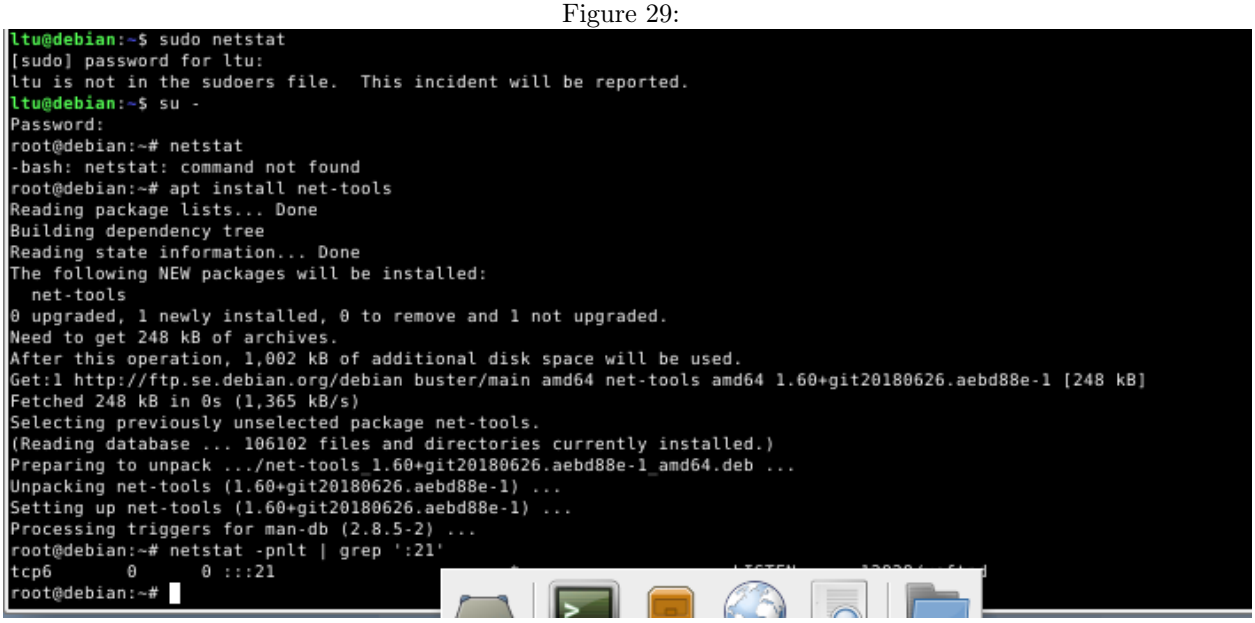

File Machine View Input Devices Help
Applications
localhost / localhost | p...
ltu@debian: ~
03:42
ltu
localhost / localhost | phpMyAdmin 4.6.6deb5 - Mozilla Firefox
phpmyadmin_4.6.6-5_all
localhost / localhost | ph
localhost/phpmyadmin/index.php?token=19
phpMyAdmin
Recent
Favorites
New
information_schema
mysql
performance_schema
sys
Server: localhost:3306
Databases
SQL
Status
User accounts
More
General settings
Change password
Server connection collation:
utf8mb4_unicode_ci
Appearance settings
Language:
English
Theme:
pmahomme
Console size:
82%
Database server
Server: Localhost via UNIX socket
Server type: MySQL
Server version: 8.0.22 - MySQL Community Server - GPL
Protocol version: 10
User: root@localhost
Server charset: UTF-8 Unicode (utf8)
Web server
Apache/2.4.38
HÖGER CRTL

Figure 29:



```
ltu@debian:~$ sudo netstat
[sudo] password for ltu:
ltu is not in the sudoers file.  This incident will be reported.
ltu@debian:~$ su -
Password:
root@debian:~# netstat
-bash: netstat: command not found
root@debian:~# apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 248 kB of archives.
After this operation, 1,002 kB of additional disk space will be used.
Get:1 http://ftp.se.debian.org/debian buster/main amd64 net-tools amd64 1.60+git20180626.aebd88e-1 [248 kB]
Fetched 248 kB in 0s (1,365 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 106102 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1_amd64.deb ...
Unpacking net-tools (1.60+git20180626.aebd88e-1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1) ...
Processing triggers for man-db (2.8.5-2) ...
root@debian:~# netstat -pnlt | grep ':21'
tcp6       0      0 :::21
root@debian:~#
```

Figure 30:

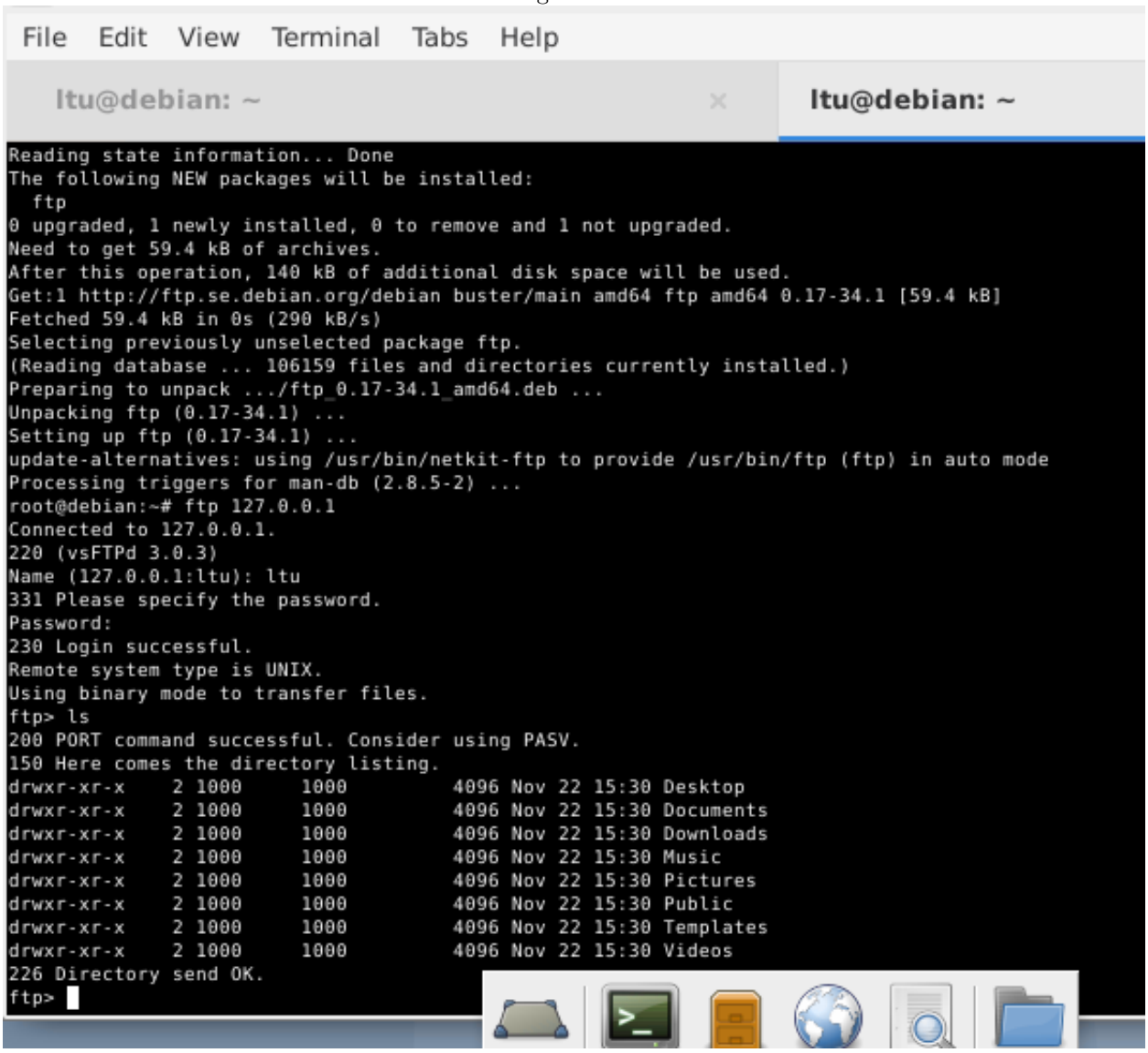
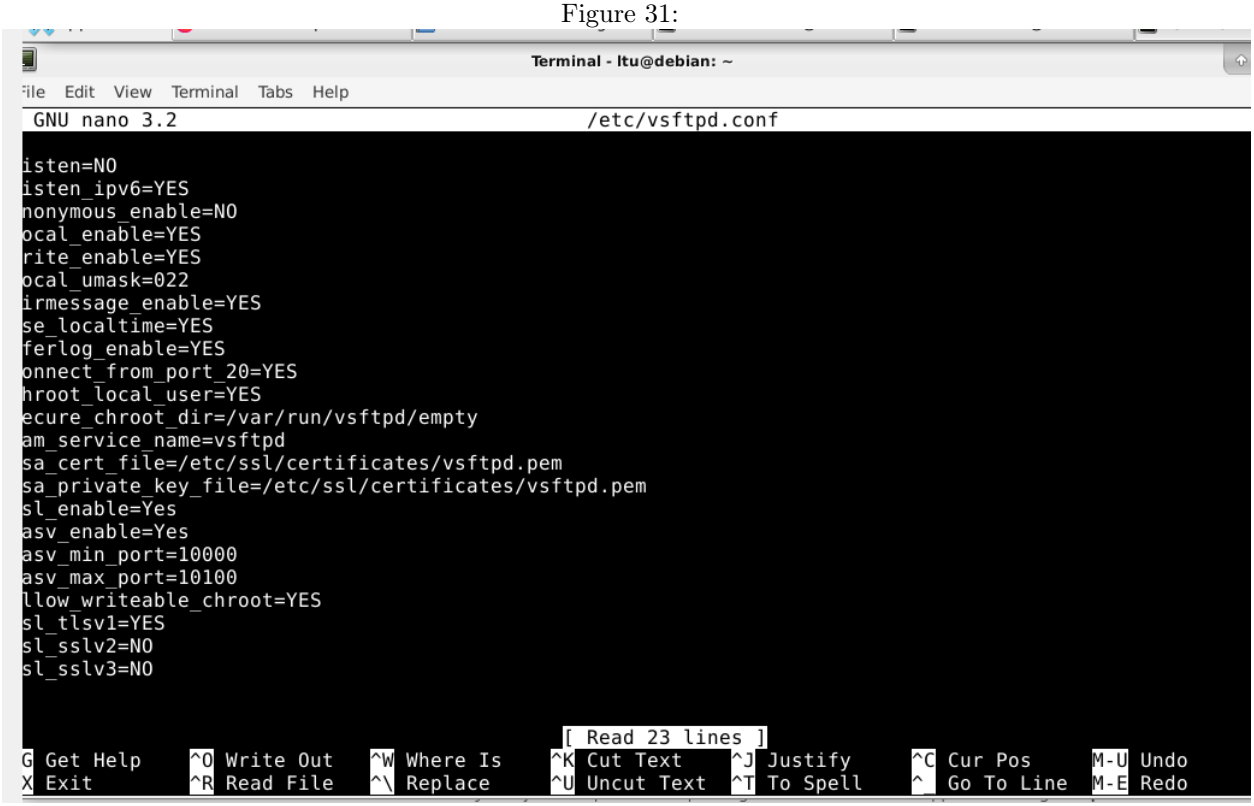

File Edit View Terminal Tabs Help
ltu@debian: ~
ltu@debian: ~
Reading state information... Done
The following NEW packages will be installed:
ftp
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 59.4 kB of archives.
After this operation, 140 kB of additional disk space will be used.
Get:1 http://ftp.se.debian.org/debian buster/main amd64 ftp amd64 0.17-34.1 [59.4 kB]
Fetched 59.4 kB in 0s (290 kB/s)
Selecting previously unselected package ftp.
(Reading database ... 106159 files and directories currently installed.)
Preparing to unpack .../ftp_0.17-34.1_amd64.deb ...
Unpacking ftp (0.17-34.1) ...
Setting up ftp (0.17-34.1) ...
update-alternatives: using /usr/bin/netkit-ftp to provide /usr/bin/ftp (ftp) in auto mode
Processing triggers for man-db (2.8.5-2) ...
root@debian:~# ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.3)
Name (127.0.0.1:ltu): ltu
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 2 1000 1000 4096 Nov 22 15:30 Desktop
drwxr-xr-x 2 1000 1000 4096 Nov 22 15:30 Documents
drwxr-xr-x 2 1000 1000 4096 Nov 22 15:30 Downloads
drwxr-xr-x 2 1000 1000 4096 Nov 22 15:30 Music
drwxr-xr-x 2 1000 1000 4096 Nov 22 15:30 Pictures
drwxr-xr-x 2 1000 1000 4096 Nov 22 15:30 Public
drwxr-xr-x 2 1000 1000 4096 Nov 22 15:30 Templates
drwxr-xr-x 2 1000 1000 4096 Nov 22 15:30 Videos
226 Directory send OK.
ftp>

Figure 31:




## 4. thoughts about this week

interesting topics, especially the *hands on* Debian!

## 5. References

[1] Audit Association for Computing Machinery. Special Interest Group on Security et al. *Cloud Computing '13 : proceedings of the 2013 International Workshop on Security in Cloud Computing : May 8, 2013, Hangzhou, China*, p. 70. ISBN: 9781450320672.

[2] Anatoliy Gorbenko et al. "Experience Report: Study of Vulnerabilities of Enterprise Operating Systems". In: *Proceedings - International Symposium on Software Reliability Engineering, ISSRE*. Vol. 2017-October. IEEE Computer Society, Nov. 2017, pp. 205–215. ISBN: 9781538609415. DOI: 10.1109/ISSRE.2017.20.

[3] *IllumOS*. https://illumos.org/. Accessed: 2020-12-03.

[4] *Microsoft Azure*. https://azure.microsoft.com/en-us/pricing/details/cloud-services. Accessed: 2020-12-03.

[5] *omniOS*. https://omniosce.org/. Accessed: 2020-12-03.

[6] *RedHat*. https://www.redhat.com/en. Accessed: 2020-12-03.

[7] Saurabh Singh, Young Sik Jeong, and Jong Hyuk Park. "A survey on cloud computing security: Issues, threats, and solutions". In: *Journal of Network and Computer Applications* 75 (Nov. 2016), pp. 200–222. ISSN: 10958592. DOI: 10.1016/j.jnca.2016.09.002.