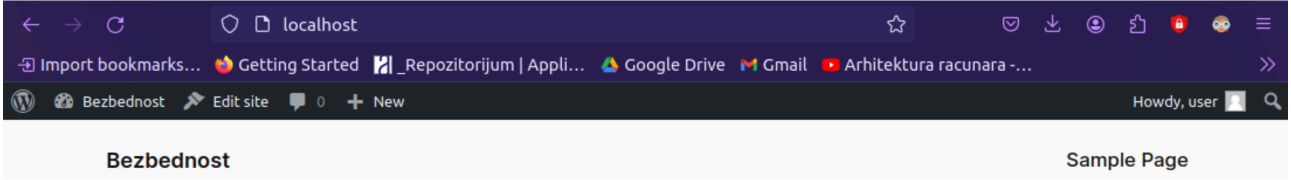
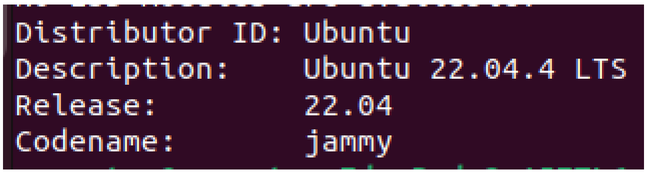
Domaći 5 – SV70/2020

Application:



System review

Operating system



```
Distributor ID: Ubuntu
Description:    Ubuntu 22.04.4 LTS
Release:        22.04
Codename:       jammy
```

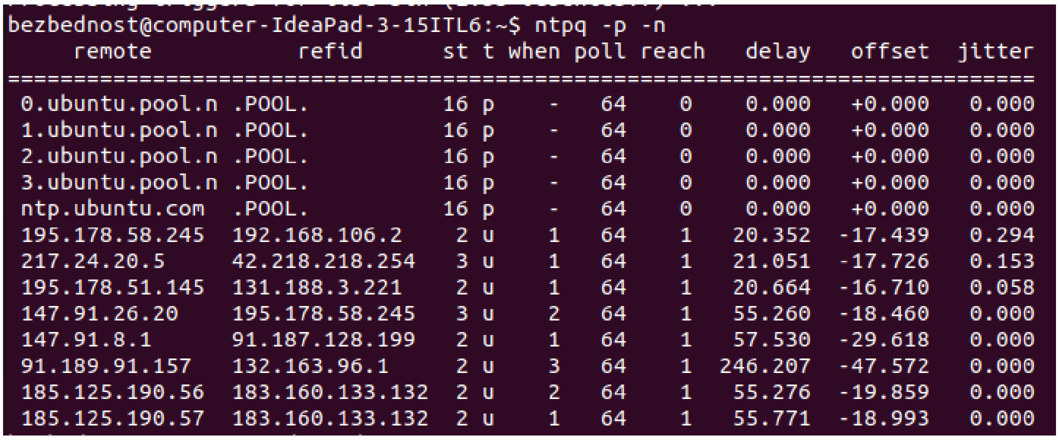
Kernel

Linux computer-IdeaPad-3-15ITL6 6.5.0-28-generic #29~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Apr 4 14:39:20 UTC 2 x86_64 x86_64 x86_64 GNU/Linux

22:55:00 up 14 days, 1:44, 6 users, load average: 0,57, 0,64, 0,62

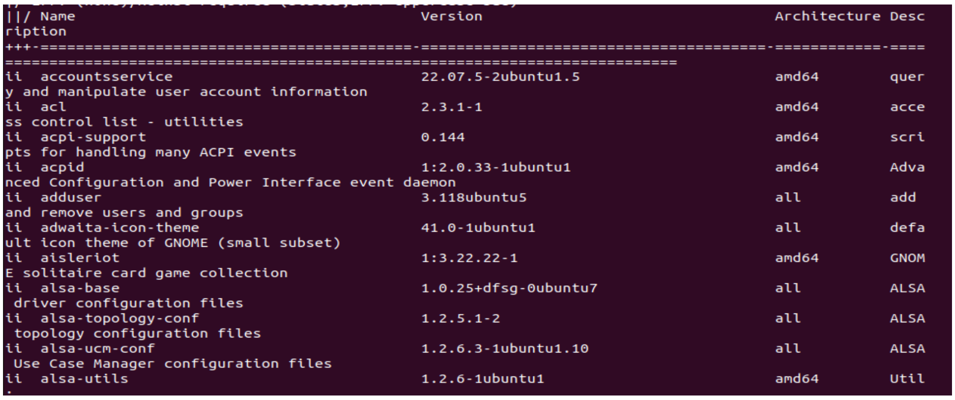
Time management

/etc/timezone:
Europe/Rome



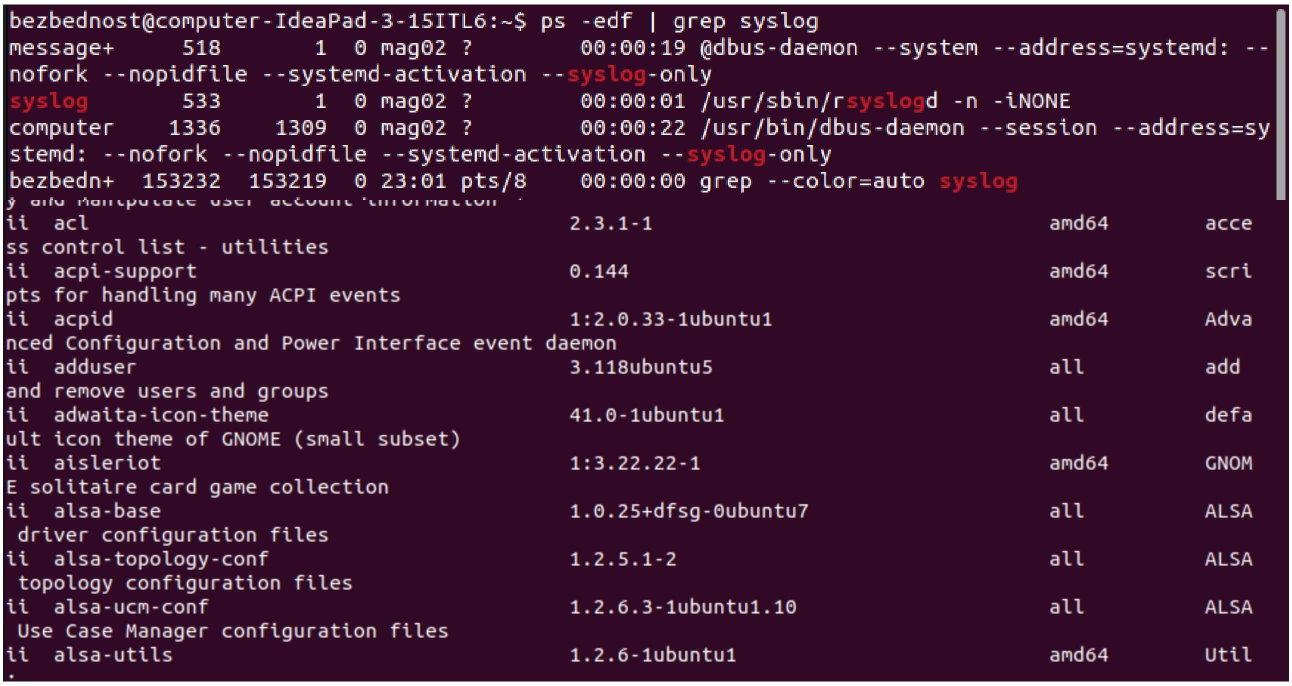
```
bezbednost@computer-IdeaPad-3-15ITL6:~$ ntpq -p -n
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 0.ubuntu.pool.n .POOL.          16 p    -   64    0    0.000   +0.000   0.000
 1.ubuntu.pool.n .POOL.          16 p    -   64    0    0.000   +0.000   0.000
 2.ubuntu.pool.n .POOL.          16 p    -   64    0    0.000   +0.000   0.000
 3.ubuntu.pool.n .POOL.          16 p    -   64    0    0.000   +0.000   0.000
 ntp.ubuntu.com  .POOL.          16 p    -   64    0    0.000   +0.000   0.000
 195.178.58.245  192.168.106.2    2 u    1   64    1   20.352  -17.439   0.294
 217.24.20.5     42.218.218.254   3 u    1   64    1   21.051  -17.726   0.153
 195.178.51.145  131.188.3.221    2 u    1   64    1   20.664  -16.710   0.058
 147.91.26.20    195.178.58.245   3 u    2   64    1   55.260  -18.460   0.000
 147.91.8.1      91.187.128.199   2 u    1   64    1   57.530  -29.618   0.000
 91.189.91.157   132.163.96.1     2 u    3   64    1  246.207  -47.572   0.000
 185.125.190.56  183.160.133.132  2 u    2   64    1   55.276  -19.859   0.000
 185.125.190.57  183.160.133.132  2 u    1   64    1   55.771  -18.993   0.000
```

Packages installed:

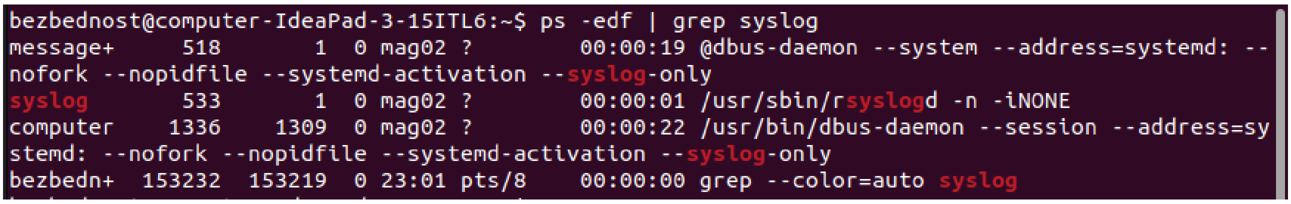


```
||/ Name                                       Version                                 Architecture Desc
ription
+++-==========================================-=======================================-============-====
===========================================================================
ii  accountsservice                            22.07.5-2ubuntu1.5                      amd64        quer
y and manipulate user account information
ii  acl                                        2.3.1-1                                 amd64        acce
ss control list - utilities
ii  acpi-support                               0.144                                   amd64        scri
pts for handling many ACPI events
ii  acpid                                      1:2.0.33-1ubuntu1                       amd64        Adva
nced Configuration and Power Interface event daemon
ii  adduser                                    3.118ubuntu5                            all          add
and remove users and groups
ii  adwaita-icon-theme                         41.0-1ubuntu1                           all          defa
ult icon theme of GNOME (small subset)
ii  aisleriot                                  1:3.22.22-1                             amd64        GNOM
E solitaire card game collection
ii  alsa-base                                  1.0.25+dfsg-0ubuntu7                    all          ALSA
 driver configuration files
ii  alsa-topology-conf                         1.2.5.1-2                               all          ALSA
 topology configuration files
ii  alsa-ucm-conf                              1.2.6.3-1ubuntu1.10                     all          ALSA
 Use Case Manager configuration files
ii  alsa-utils                                 1.2.6-1ubuntu1                          amd64        Util
```

Logging

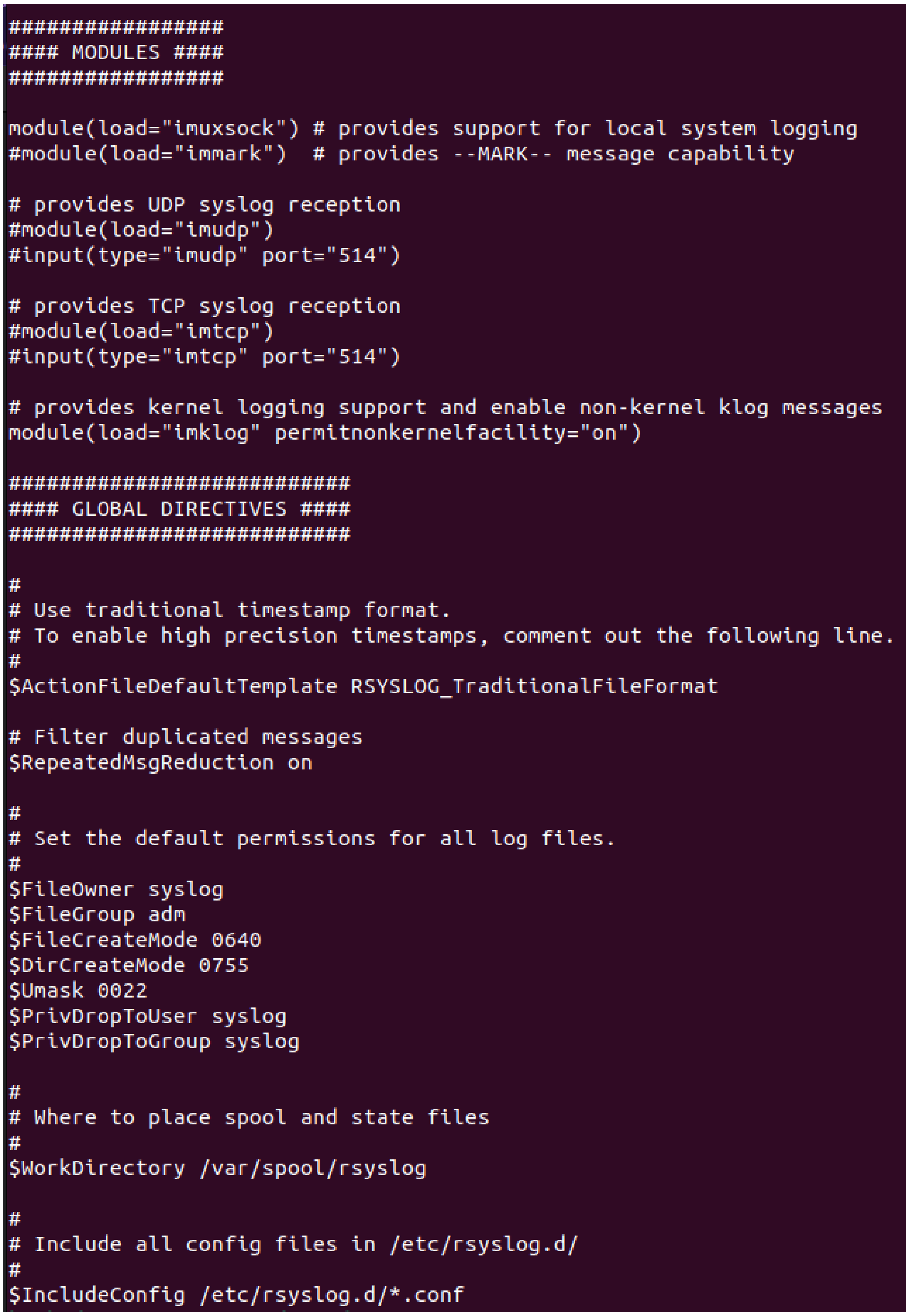


```
bezbednost@computer-IdeaPad-3-15ITL6:~$ ps -edf | grep syslog
message+     518       1  0 mag02 ?        00:00:19 @dbus-daemon --system --address=systemd: --
nofork --nopidfile --systemd-activation --syslog-only
syslog       533       1  0 mag02 ?        00:00:01 /usr/sbin/rsyslogd -n -iNONE
computer    1336    1309  0 mag02 ?        00:00:22 /usr/bin/dbus-daemon --session --address=sy
stemd: --nofork --nopidfile --systemd-activation --syslog-only
bezbedn+  153232  153219  0 23:01 pts/8    00:00:00 grep --color=auto syslog
y and manipulate user account information
ii  acl                                         2.3.1-1                                  amd64        acce
ss control list - utilities
ii  acpi-support                                0.144                                    amd64        scri
pts for handling many ACPI events
ii  acpid                                       1:2.0.33-1ubuntu1                        amd64        Adva
nced Configuration and Power Interface event daemon
ii  adduser                                     3.118ubuntu5                             all          add
and remove users and groups
ii  adwaita-icon-theme                          41.0-1ubuntu1                            all          defa
ult icon theme of GNOME (small subset)
ii  aisleriot                                   1:3.22.22-1                              amd64        GNOM
E solitaire card game collection
ii  alsa-base                                   1.0.25+dfsg-0ubuntu7                     all          ALSA
 driver configuration files
ii  alsa-topology-conf                          1.2.5.1-2                                all          ALSA
 topology configuration files
ii  alsa-ucm-conf                               1.2.6.3-1ubuntu1.10                      all          ALSA
 Use Case Manager configuration files
ii  alsa-utils                                  1.2.6-1ubuntu1                           amd64        Util
```



```
bezbednost@computer-IdeaPad-3-15ITL6:~$ ps -edf | grep syslog
message+     518       1  0 mag02 ?        00:00:19 @dbus-daemon --system --address=systemd: --
nofork --nopidfile --systemd-activation --syslog-only
syslog       533       1  0 mag02 ?        00:00:01 /usr/sbin/rsyslogd -n -iNONE
computer    1336    1309  0 mag02 ?        00:00:22 /usr/bin/dbus-daemon --session --address=sy
stemd: --nofork --nopidfile --systemd-activation --syslog-only
bezbedn+  153232  153219  0 23:01 pts/8    00:00:00 grep --color=auto syslog
```

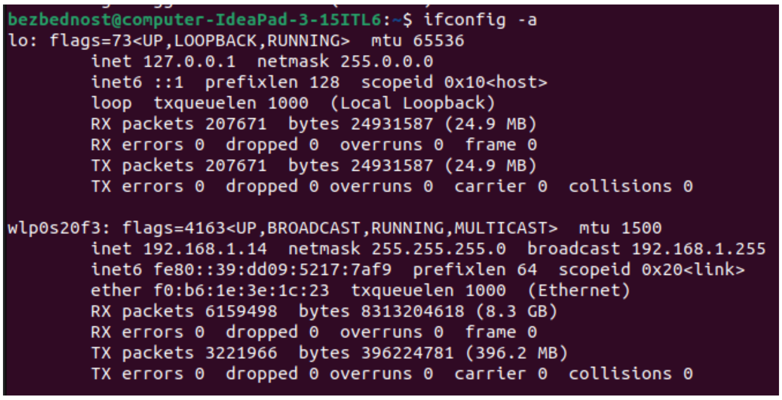
/etc/rsyslog.conf



```
#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
```

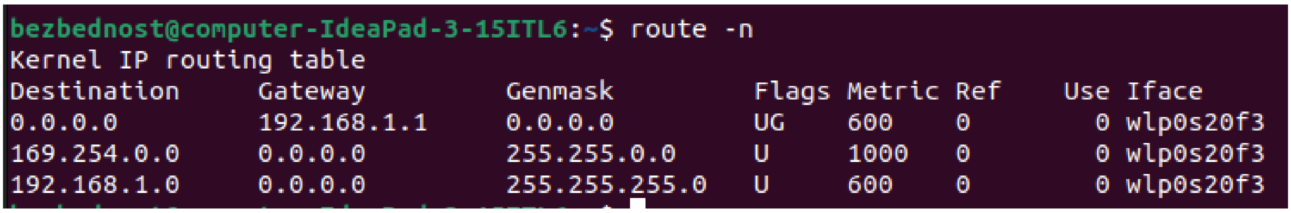
Network review

Network interfaces:



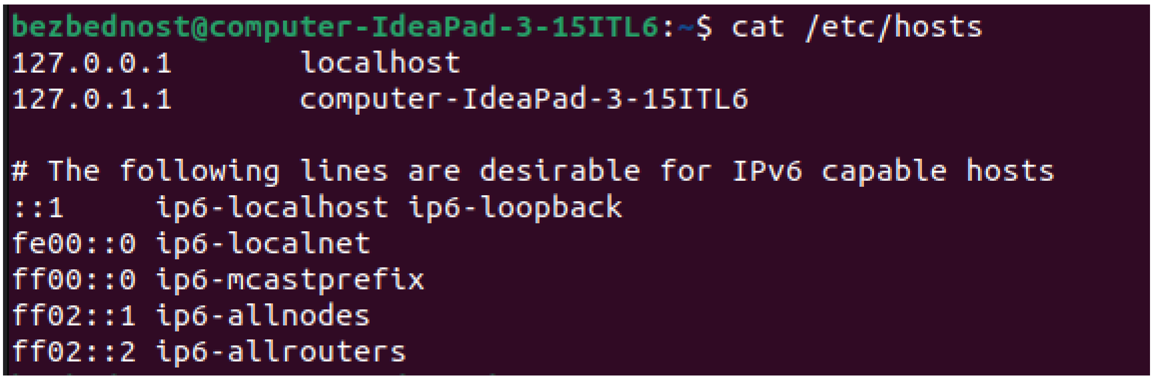
```
bezbednost@computer-IdeaPad-3-15ITL6:~$ ifconfig -a
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 207671  bytes 24931587 (24.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 207671  bytes 24931587 (24.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.14  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::39:dd09:5217:7af9  prefixlen 64  scopeid 0x20<link>
        ether f0:b6:1e:3e:1c:23  txqueuelen 1000  (Ethernet)
        RX packets 6159498  bytes 8313204618 (8.3 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3221966  bytes 396224781 (396.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

System routes:



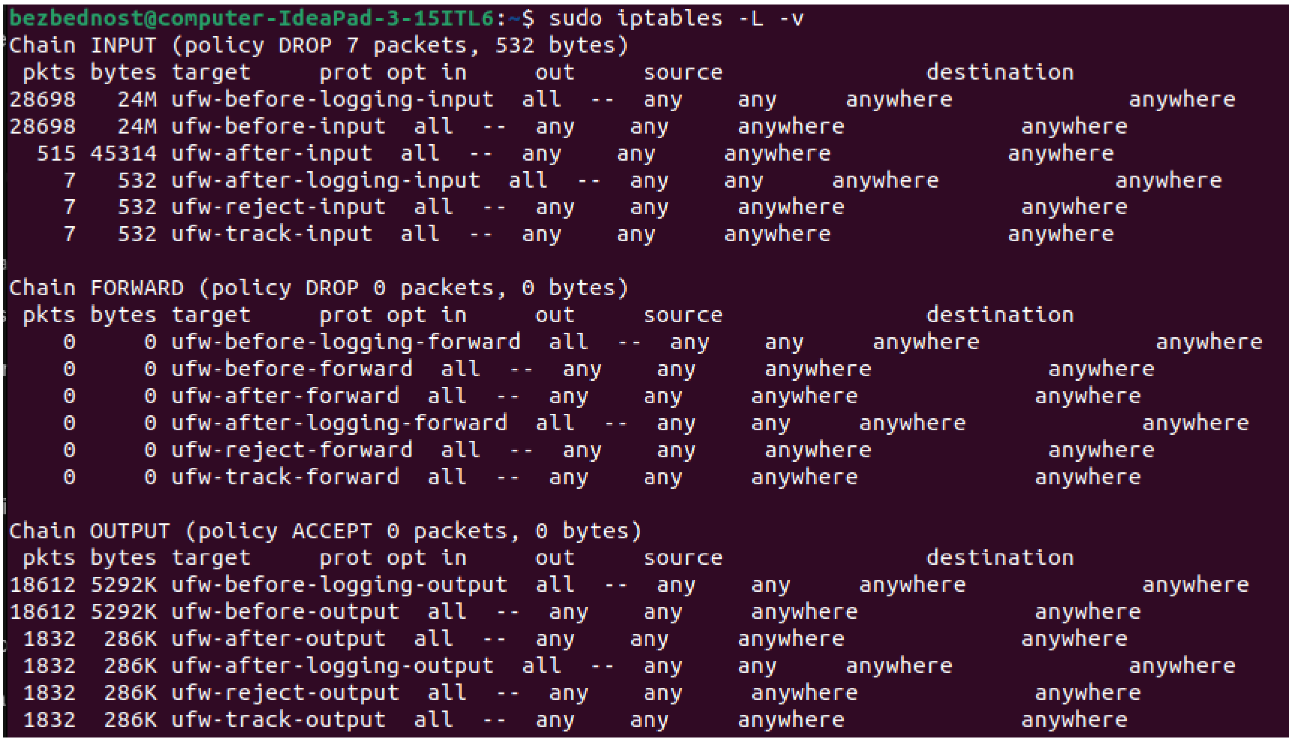
```
bezbednost@computer-IdeaPad-3-15ITL6:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    600    0        0 wlp0s20f3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp0s20f3
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp0s20f3
```

DNS configuration:

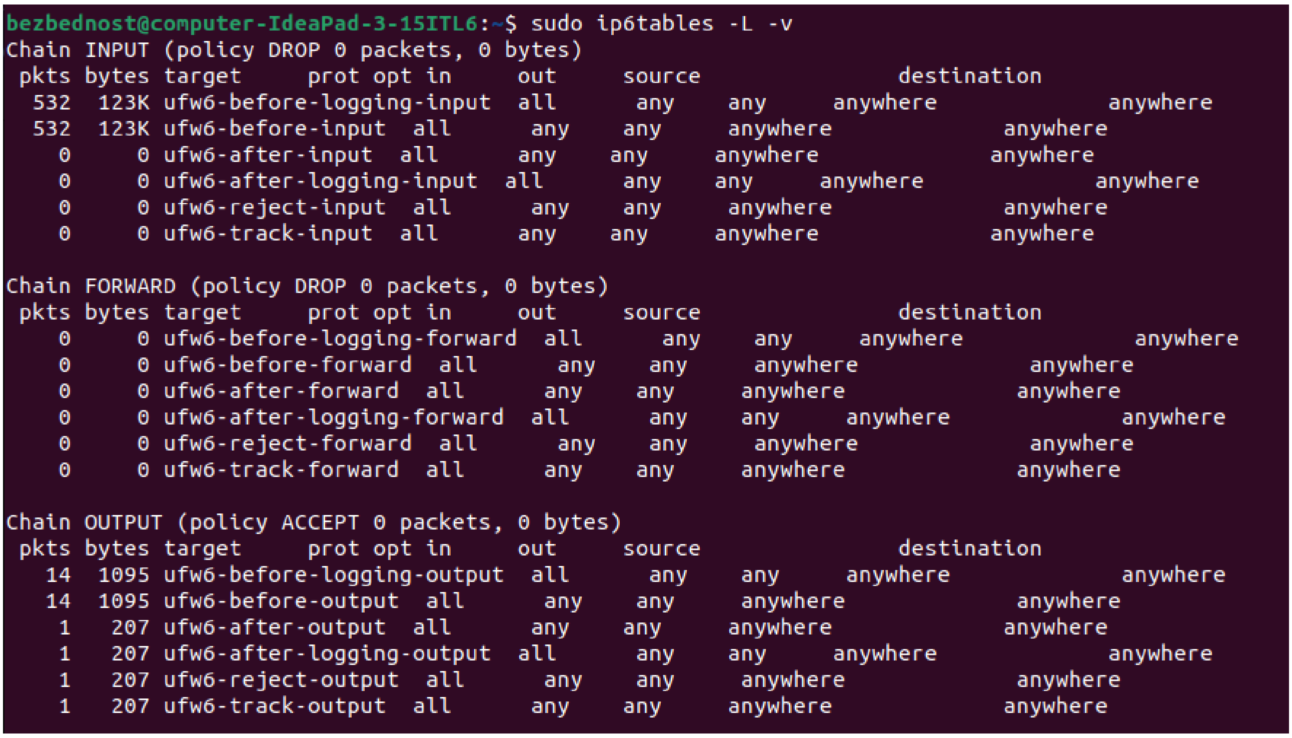


```
bezbednost@computer-IdeaPad-3-15ITL6:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       computer-IdeaPad-3-15ITL6

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Firewall rules



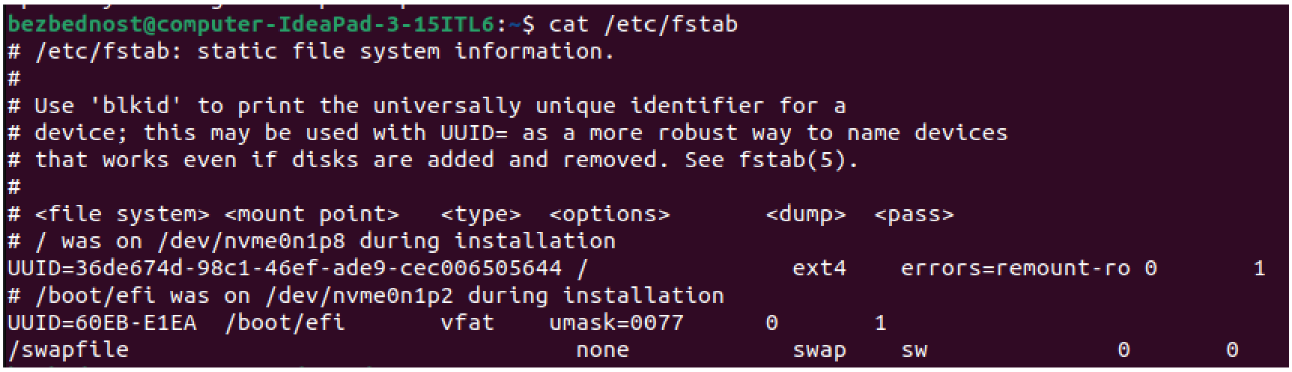
```
bezbednost@computer-IdeaPad-3-15ITL6:~$ sudo iptables -L -v
Chain INPUT (policy DROP 7 packets, 532 bytes)
 pkts bytes target     prot opt in     out     source               destination
28698   24M ufw-before-logging-input  all  --  any    any     anywhere             anywhere
28698   24M ufw-before-input  all  --  any    any     anywhere             anywhere
  515 45314 ufw-after-input  all  --  any    any     anywhere             anywhere
    7   532 ufw-after-logging-input  all  --  any    any     anywhere             anywhere
    7   532 ufw-reject-input  all  --  any    any     anywhere             anywhere
    7   532 ufw-track-input  all  --  any    any     anywhere             anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ufw-before-logging-forward  all  --  any    any     anywhere             anywhere
    0     0 ufw-before-forward  all  --  any    any     anywhere             anywhere
    0     0 ufw-after-forward  all  --  any    any     anywhere             anywhere
    0     0 ufw-after-logging-forward  all  --  any    any     anywhere             anywhere
    0     0 ufw-reject-forward  all  --  any    any     anywhere             anywhere
    0     0 ufw-track-forward  all  --  any    any     anywhere             anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
18612 5292K ufw-before-logging-output  all  --  any    any     anywhere             anywhere
18612 5292K ufw-before-output  all  --  any    any     anywhere             anywhere
 1832  286K ufw-after-output  all  --  any    any     anywhere             anywhere
 1832  286K ufw-after-logging-output  all  --  any    any     anywhere             anywhere
 1832  286K ufw-reject-output  all  --  any    any     anywhere             anywhere
 1832  286K ufw-track-output  all  --  any    any     anywhere             anywhere
```



```
bezbednost@computer-IdeaPad-3-15ITL6:~$ sudo ip6tables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  532  123K ufw6-before-logging-input  all      any    any     anywhere             anywhere
  532  123K ufw6-before-input  all      any    any     anywhere             anywhere
    0     0 ufw6-after-input  all      any    any     anywhere             anywhere
    0     0 ufw6-after-logging-input  all      any    any     anywhere             anywhere
    0     0 ufw6-reject-input  all      any    any     anywhere             anywhere
    0     0 ufw6-track-input  all      any    any     anywhere             anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ufw6-before-logging-forward  all      any    any     anywhere             anywhere
    0     0 ufw6-before-forward  all      any    any     anywhere             anywhere
    0     0 ufw6-after-forward  all      any    any     anywhere             anywhere
    0     0 ufw6-after-logging-forward  all      any    any     anywhere             anywhere
    0     0 ufw6-reject-forward  all      any    any     anywhere             anywhere
    0     0 ufw6-track-forward  all      any    any     anywhere             anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   14  1095 ufw6-before-logging-output  all      any    any     anywhere             anywhere
   14  1095 ufw6-before-output  all      any    any     anywhere             anywhere
    1   207 ufw6-after-output  all      any    any     anywhere             anywhere
    1   207 ufw6-after-logging-output  all      any    any     anywhere             anywhere
    1   207 ufw6-reject-output  all      any    any     anywhere             anywhere
    1   207 ufw6-track-output  all      any    any     anywhere             anywhere
```

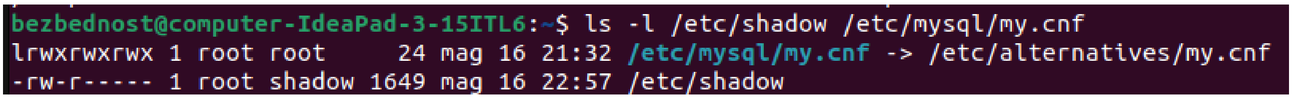
Filesystem review

Mountend partitions:



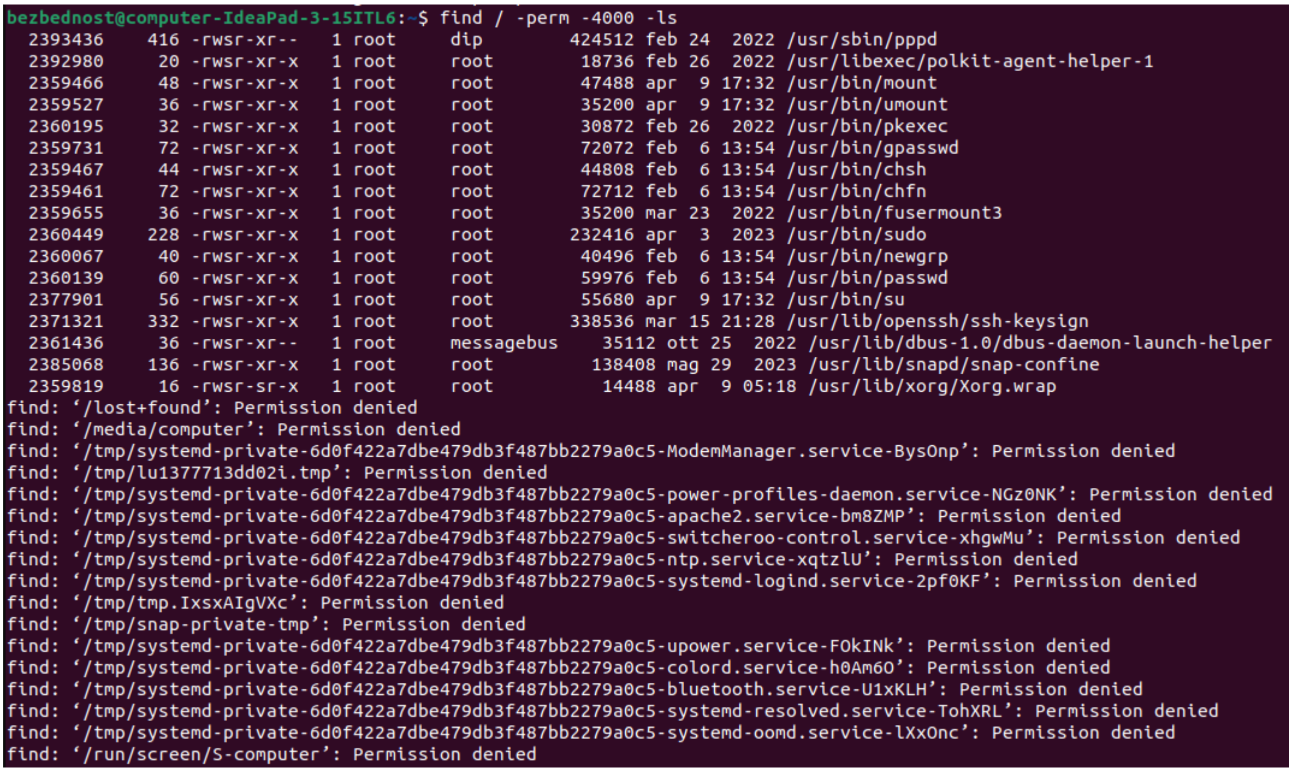
```
bezbednost@computer-IdeaPad-3-15ITL6:~$ cat /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/nvme0n1p8 during installation
UUID=36de674d-98c1-46ef-ade9-cec006505644 /               ext4    errors=remount-ro 0       1
# /boot/efi was on /dev/nvme0n1p2 during installation
UUID=60EB-E1EA  /boot/efi       vfat    umask=0077      0       1
/swapfile                                 none            swap    sw              0       0
```

Sensitive files:



```
bezbednost@computer-IdeaPad-3-15ITL6:~$ ls -l /etc/shadow /etc/mysql/my.cnf
lrwxrwxrwx 1 root root     24 mag 16 21:32 /etc/mysql/my.cnf -> /etc/alternatives/my.cnf
-rw-r----- 1 root shadow 1649 mag 16 22:57 /etc/shadow
```

Setuid

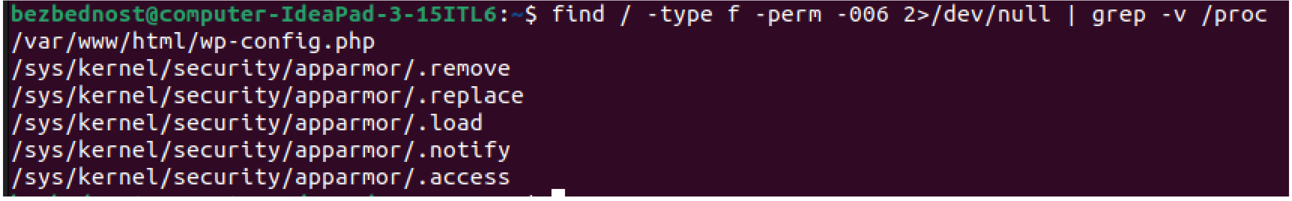


```
bezbednost@computer-IdeaPad-3-15ITL6:~$ find / -perm -4000 -ls
  2393436    416 -rwsr-xr--   1 root     dip        424512 feb 24  2022 /usr/sbin/pppd
  2392980     20 -rwsr-xr-x   1 root     root        18736 feb 26  2022 /usr/libexec/polkit-agent-helper-1
  2359466     48 -rwsr-xr-x   1 root     root        47488 apr  9 17:32 /usr/bin/mount
  2359527     36 -rwsr-xr-x   1 root     root        35200 apr  9 17:32 /usr/bin/umount
  2360195     32 -rwsr-xr-x   1 root     root        30872 feb 26  2022 /usr/bin/pkexec
  2359731     72 -rwsr-xr-x   1 root     root        72072 feb  6 13:54 /usr/bin/gpasswd
  2359467     44 -rwsr-xr-x   1 root     root        44808 feb  6 13:54 /usr/bin/chsh
  2359461     72 -rwsr-xr-x   1 root     root        72712 feb  6 13:54 /usr/bin/chfn
  2359655     36 -rwsr-xr-x   1 root     root        35200 mar 23  2022 /usr/bin/fusermount3
  2360449    228 -rwsr-xr-x   1 root     root       232416 apr  3  2023 /usr/bin/sudo
  2360067     40 -rwsr-xr-x   1 root     root        40496 feb  6 13:54 /usr/bin/newgrp
  2360139     60 -rwsr-xr-x   1 root     root        59976 feb  6 13:54 /usr/bin/passwd
  2377901     56 -rwsr-xr-x   1 root     root        55680 apr  9 17:32 /usr/bin/su
  2371321    332 -rwsr-xr-x   1 root     root       338536 mar 15 21:28 /usr/lib/openssh/ssh-keysign
  2361436     36 -rwsr-xr--   1 root     messagebus    35112 ott 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
  2385068    136 -rwsr-xr-x   1 root     root         138408 mag 29  2023 /usr/lib/snapd/snap-confine
  2359819     16 -rwsr-sr-x   1 root     root          14488 apr  9 05:18 /usr/lib/xorg/Xorg.wrap
find: ‘/lost+found’: Permission denied
find: ‘/media/computer’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-ModemManager.service-BysOnp’: Permission denied
find: ‘/tmp/lu1377713dd02i.tmp’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-power-profiles-daemon.service-NGz0NK’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-apache2.service-bm8ZMP’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-switcheroo-control.service-xhgwMu’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-ntp.service-xqtzlU’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-systemd-logind.service-2pf0KF’: Permission denied
find: ‘/tmp/tmp.IxsxAIgVXc’: Permission denied
find: ‘/tmp/snap-private-tmp’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-upower.service-FOkINk’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-colord.service-h0Am6O’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-bluetooth.service-U1xKLH’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-systemd-resolved.service-TohXRL’: Permission denied
find: ‘/tmp/systemd-private-6d0f422a7dbe479db3f487bb2279a0c5-systemd-oomd.service-lXxOnc’: Permission denied
find: ‘/run/screen/S-computer’: Permission denied
```

….

Normal files

Readable and writeable by all users:



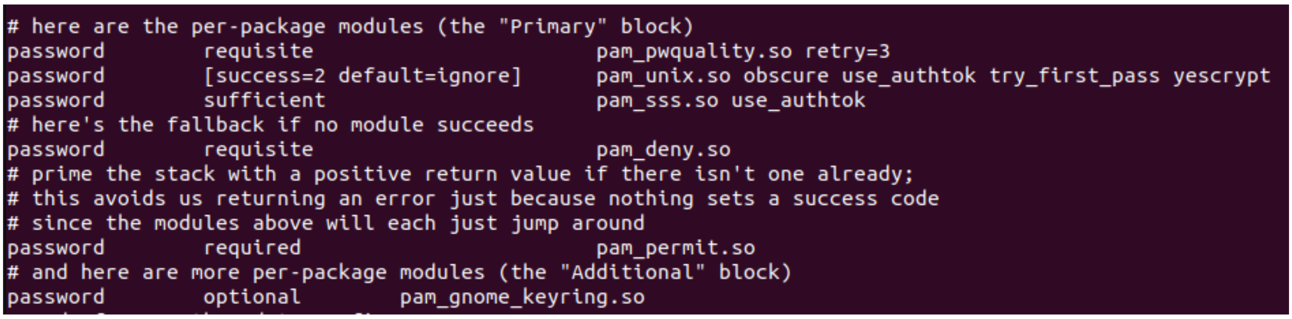
```
bezbednost@computer-IdeaPad-3-15ITL6:~$ find / -type f -perm -006 2>/dev/null | grep -v /proc
/var/www/html/wp-config.php
/sys/kernel/security/apparmor/.remove
/sys/kernel/security/apparmor/.replace
/sys/kernel/security/apparmor/.load
/sys/kernel/security/apparmor/.notify
/sys/kernel/security/apparmor/.access
```

Backup

Doesn’t exist.

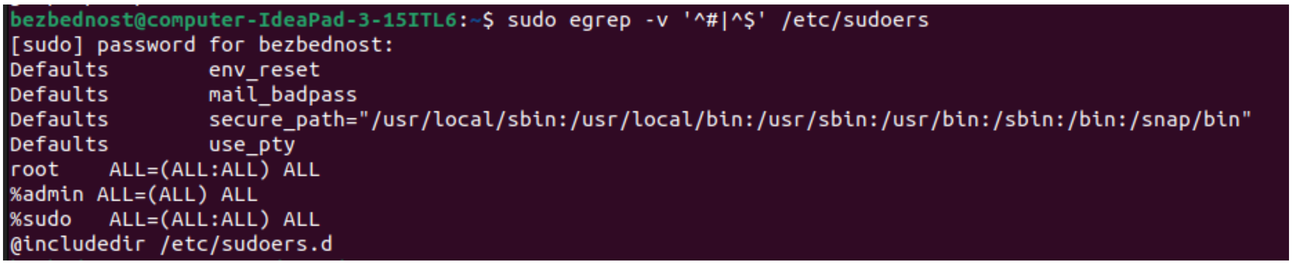
Users review

/etc/pam.d/common-password



```
# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3
password        [success=2 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
password        sufficient                      pam_sss.so use_authtok
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
```

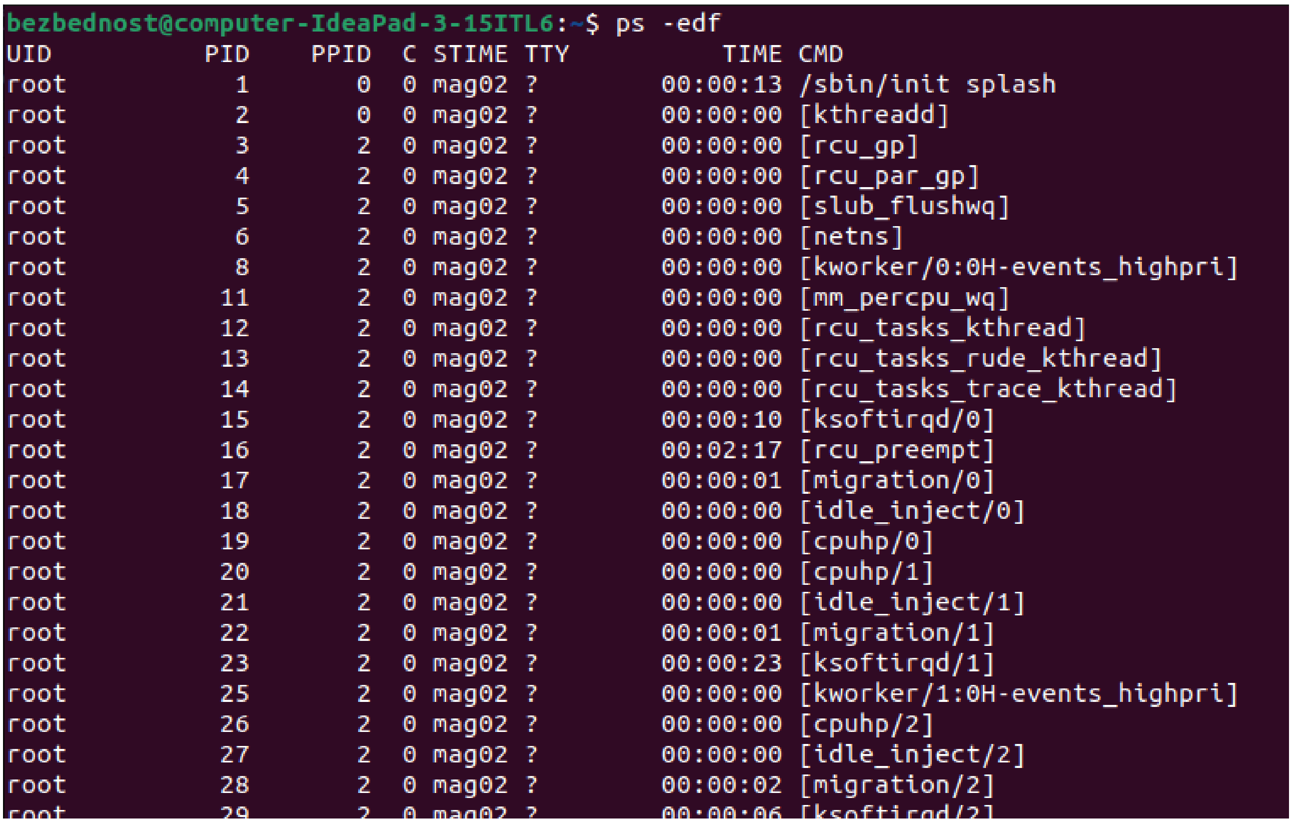
Reviewing the sudo configuration:



```
bezbednost@computer-IdeaPad-3-15ITL6:~$ sudo egrep -v '^#|^$' /etc/sudoers
[sudo] password for bezbednost:
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
Defaults        use_pty
root    ALL=(ALL:ALL) ALL
%admin ALL=(ALL) ALL
%sudo   ALL=(ALL:ALL) ALL
@includedir /etc/sudoers.d
```

Services review

Identifying running services:



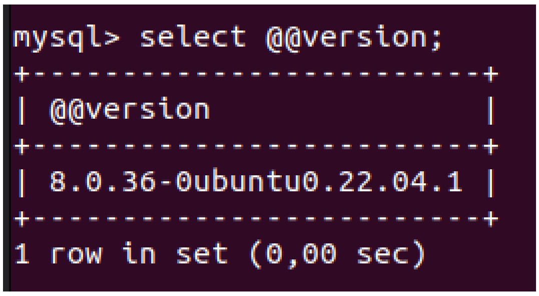
```
bezbednost@computer-IdeaPad-3-15ITL6:~$ ps -edf
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 mag02 ?        00:00:13 /sbin/init splash
root           2       0  0 mag02 ?        00:00:00 [kthreadd]
root           3       2  0 mag02 ?        00:00:00 [rcu_gp]
root           4       2  0 mag02 ?        00:00:00 [rcu_par_gp]
root           5       2  0 mag02 ?        00:00:00 [slub_flushwq]
root           6       2  0 mag02 ?        00:00:00 [netns]
root           8       2  0 mag02 ?        00:00:00 [kworker/0:0H-events_highpri]
root          11       2  0 mag02 ?        00:00:00 [mm_percpu_wq]
root          12       2  0 mag02 ?        00:00:00 [rcu_tasks_kthread]
root          13       2  0 mag02 ?        00:00:00 [rcu_tasks_rude_kthread]
root          14       2  0 mag02 ?        00:00:00 [rcu_tasks_trace_kthread]
root          15       2  0 mag02 ?        00:00:10 [ksoftirqd/0]
root          16       2  0 mag02 ?        00:02:17 [rcu_preempt]
root          17       2  0 mag02 ?        00:00:01 [migration/0]
root          18       2  0 mag02 ?        00:00:00 [idle_inject/0]
root          19       2  0 mag02 ?        00:00:00 [cpuhp/0]
root          20       2  0 mag02 ?        00:00:00 [cpuhp/1]
root          21       2  0 mag02 ?        00:00:00 [idle_inject/1]
root          22       2  0 mag02 ?        00:00:01 [migration/1]
root          23       2  0 mag02 ?        00:00:23 [ksoftirqd/1]
root          25       2  0 mag02 ?        00:00:00 [kworker/1:0H-events_highpri]
root          26       2  0 mag02 ?        00:00:00 [cpuhp/2]
root          27       2  0 mag02 ?        00:00:00 [idle_inject/2]
root          28       2  0 mag02 ?        00:00:02 [migration/2]
root          29       2  0 mag02 ?        00:00:06 [ksoftirqd/2]
```

…

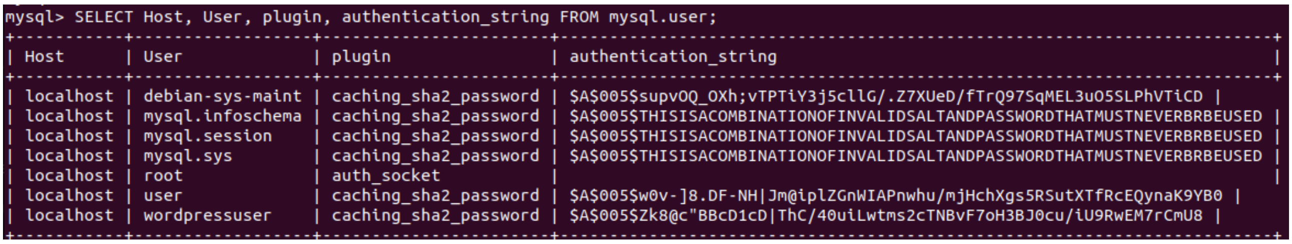
Service listening on UDP:
None.

TCP services:
None.

MySQL

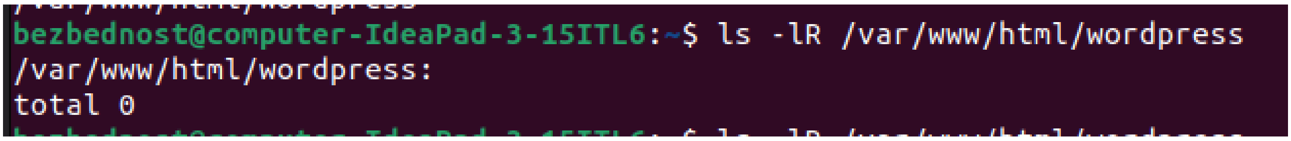


```
mysql> select @@version;
+-------------------------+
| @@version               |
+-------------------------+
| 8.0.36-0ubuntu0.22.04.1 |
+-------------------------+
1 row in set (0,00 sec)
```

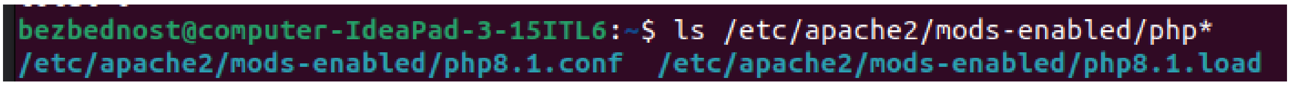


```
mysql> SELECT Host, User, plugin, authentication_string FROM mysql.user;
+-----------+------------------+-----------------------+------------------------------------------------------------------------+
| Host      | User             | plugin                | authentication_string                                                  |
+-----------+------------------+-----------------------+------------------------------------------------------------------------+
| localhost | debian-sys-maint | caching_sha2_password | $A$005$supvOQ_OXh;vTPTiY3j5cllG/.Z7XUeD/fTrQ97SqMEL3uO5SLPhVTiCD |
| localhost | mysql.infoschema | caching_sha2_password | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| localhost | mysql.session    | caching_sha2_password | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| localhost | mysql.sys        | caching_sha2_password | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| localhost | root             | auth_socket           |                                                                        |
| localhost | user             | caching_sha2_password | $A$005$w0v-]8.DF-NH|Jm@iplZGnWIAPnwhu/mjHchXgs5RSutXTfRcEQynaK9YB0 |
| localhost | wordpressuser    | caching_sha2_password | $A$005$Zk8@c"BBcD1cD|ThC/40uiLwtms2cTNBvF7oH3BJ0cu/iU9RwEM7rCmU8 |
+-----------+------------------+-----------------------+------------------------------------------------------------------------+
```

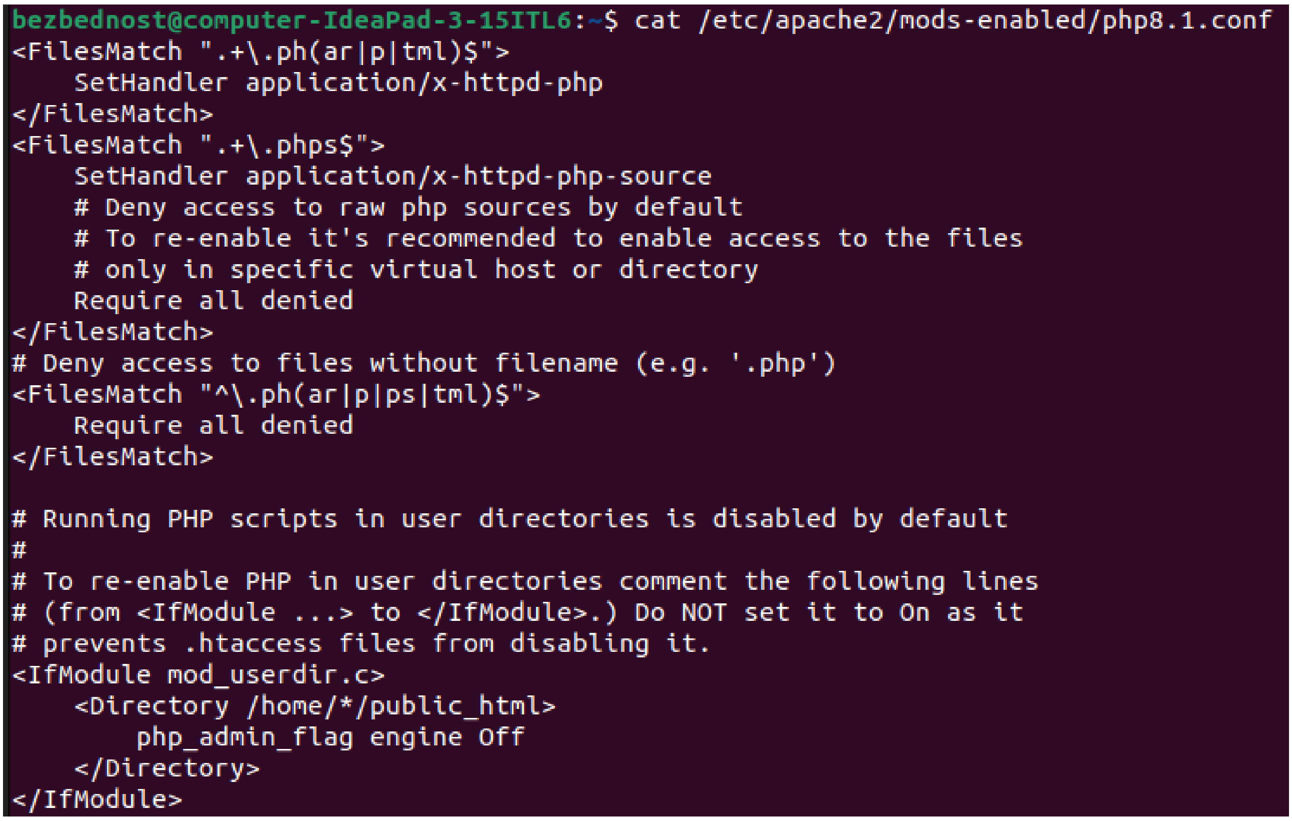
Apache configuration



```
bezbednost@computer-IdeaPad-3-15ITL6:~$ ls -lR /var/www/html/wordpress
/var/www/html/wordpress:
total 0
```

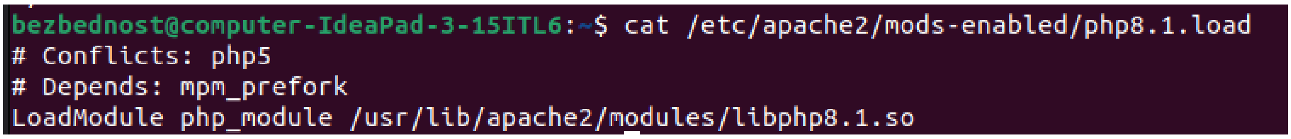


```
bezbednost@computer-IdeaPad-3-15ITL6:~$ ls /etc/apache2/mods-enabled/php*
/etc/apache2/mods-enabled/php8.1.conf  /etc/apache2/mods-enabled/php8.1.load
```



```
bezbednost@computer-IdeaPad-3-15ITL6:~$ cat /etc/apache2/mods-enabled/php8.1.conf
<FilesMatch ".+\.ph(ar|p|tml)$">
    SetHandler application/x-httpd-php
</FilesMatch>
<FilesMatch ".+\.phps$">
    SetHandler application/x-httpd-php-source
    # Deny access to raw php sources by default
    # To re-enable it's recommended to enable access to the files
    # only in specific virtual host or directory
    Require all denied
</FilesMatch>
# Deny access to files without filename (e.g. '.php')
<FilesMatch "^\.ph(ar|p|ps|tml)$">
    Require all denied
</FilesMatch>

# Running PHP scripts in user directories is disabled by default
#
# To re-enable PHP in user directories comment the following lines
# (from <IfModule ...> to </IfModule>.) Do NOT set it to On as it
# prevents .htaccess files from disabling it.
<IfModule mod_userdir.c>
    <Directory /home/*/public_html>
        php_admin_flag engine Off
    </Directory>
</IfModule>
```

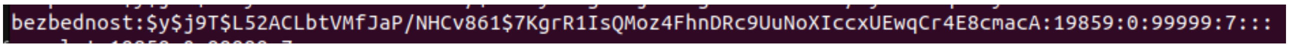
PHP configuration



```
bezbednost@computer-IdeaPad-3-15ITL6:~$ cat /etc/apache2/mods-enabled/php8.1.load
# Conflicts: php5
# Depends: mpm_prefork
LoadModule php_module /usr/lib/apache2/modules/libphp8.1.so
```

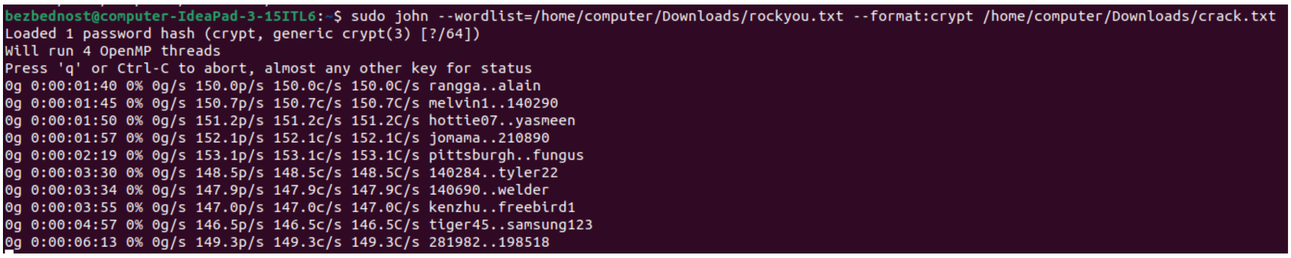
Lozinka

/etc/shadow



```
bezbednost:$y$j9T$L52ACLbtVMfJaP/NHCv861$7KgrR1IsQMoz4FhnDRc9UuNoXIccxUEwqCr4E8cmacA:19859:0:99999:7:::
```

yescrypt



```
bezbednost@computer-IdeaPad-3-15ITL6:~$ sudo john --wordlist=/home/computer/Downloads/rockyou.txt --format:crypt /home/computer/Downloads/crack.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:40 0% 0g/s 150.0p/s 150.0c/s 150.0C/s rangga..alain
0g 0:00:01:45 0% 0g/s 150.7p/s 150.7c/s 150.7C/s melvin1..140290
0g 0:00:01:50 0% 0g/s 151.2p/s 151.2c/s 151.2C/s hottie07..yasmeen
0g 0:00:01:57 0% 0g/s 152.1p/s 152.1c/s 152.1C/s jomama..210890
0g 0:00:02:19 0% 0g/s 153.1p/s 153.1c/s 153.1C/s pittsburgh..fungus
0g 0:00:03:30 0% 0g/s 148.5p/s 148.5c/s 148.5C/s 140284..tyler22
0g 0:00:03:34 0% 0g/s 147.9p/s 147.9c/s 147.9C/s 140690..welder
0g 0:00:03:55 0% 0g/s 147.0p/s 147.0c/s 147.0C/s kenzhu..freebird1
0g 0:00:04:57 0% 0g/s 146.5p/s 146.5c/s 146.5C/s tiger45..samsung123
0g 0:00:06:13 0% 0g/s 149.3p/s 149.3c/s 149.3C/s 281982..198518
```