

Name : Muhammad Hamza
ID : 21k-3815
Sec : BS-SE-4A

QUESTION 1

```
student@student-OptiPlex-7070: ~
GNU nano 6.2 /etc/squid/squid.conf
include /etc/squid/conf.d/*.conf

acl localnet src 172.16.16.65
acl blocksite dstdomain "/etc/squid/blocksite"
http_access deny blocksite
http_access allow localnet

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# TAG: adapted_http_access
#     Allowing or Denying access based on defined access lists
#
#     Essentially identical to http_access, but runs after redirectors

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

```
student@student-OptiPlex-7070: ~
GNU nano 6.2 /etc/squid/squid.conf
#
#     easily accept requests destined to this port.
#
#     If you run Squid on a dual-homed machine with an internal
#     and an external interface we recommend you to specify the
#     internal address:port in http_port. This way Squid will only be
#     visible on the internal address.
#
#
# Squid normally listens to port 3128
http_port 8080

# TAG: https_port
#     Usage: [ip:]port [mode] tls-cert=certificate.pem [options]
#
#     The socket address where Squid will listen for client requests made
#     over TLS or SSL connections. Commonly referred to as HTTPS.
#
#     This is most useful for situations where you are running squid in
#     accelerator mode and you want to do the TLS work at the accelerator

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

```
student@student-OptiPlex-7070: ~  
GNU nano 6.2 /etc/squid/blocksite *  
www.facebook.com  
www.youtube.com  
www.wikipedia.org  
[ Read 3 lines ]  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

Network Proxy

☐ Automatic

☒ Manual

☐ Disabled

HTTP Proxy

172.16.16.25

8080

—

+

HTTPS Proxy

172.16.16.25

8080

—

+

FTP Proxy

0

—

+

Socks Host

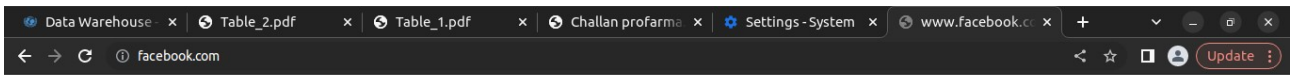
0

—

+

Ignore Hosts

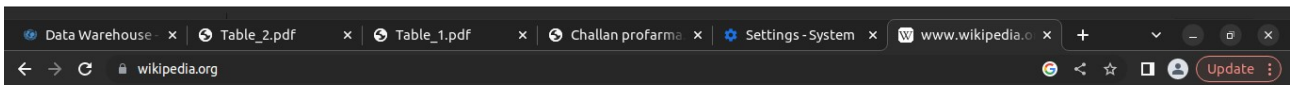
localhost, 127.0.0.0/8, ::1



This site can't be reached

The webpage at <https://www.facebook.com/> might be temporarily down or it may have moved permanently to a new web address.

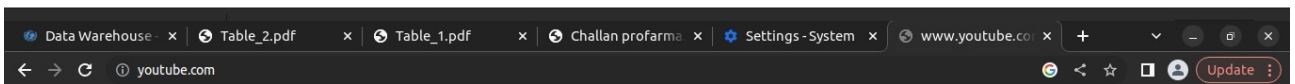
ERR_TUNNEL_CONNECTION_FAILED



This site can't be reached

The webpage at <https://www.wikipedia.org/> might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED



This site can't be reached

The webpage at <https://www.youtube.com/> might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED



QUESTION 2

1)

```
student@student-OptiPlex-7070: ~  
student@student-OptiPlex-7070:~$ sudo systemctl disable apache2  
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install disable apache2  
Removed /etc/systemd/system/multi-user.target.wants/apache2.service.  
student@student-OptiPlex-7070:~$
```

```
student@student-OptiPlex-7070: ~  
apache-htcacheclean.service      disabled      enabled  
apache-htcacheclean@.service    disabled      enabled  
apache2.service                 disabled      enabled  
apache2@.service               disabled      enabled  
apparmor.service               enabled       enabled  
apport-autoreport.service       static        -  
apport-forward@.service         static        -  
apport.service                 generated     -  
apt-daily-upgrade.service       static        -  
apt-daily.service              static        -  
apt-news.service               static        -  
autovt@.service                alias         -  
avahi-daemon.service           enabled       enabled  
bluetooth.service              enabled       enabled  
bolt.service                   static        -  
brltty-udev.service            static        -  
lines 1-23  
student@student-OptiPlex-7070:~$ sudo systemctl disable bluetooth  
Synchronizing state of bluetooth.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install disable bluetooth  
Removed /etc/systemd/system/bluetooth.target.wants/bluetooth.service.  
Removed /etc/systemd/system/dbus-org.bluez.service.  
student@student-OptiPlex-7070:~$
```

UNIT FILE	STATE	VENDOR PRESET
accounts-daemon.service	enabled	enabled
acpid.service	disabled	enabled
alsa-restore.service	static	-
alsa-state.service	static	-
alsa-utils.service	masked	enabled
anacron.service	enabled	enabled
apache-htcacheclean.service	disabled	enabled
apache-htcacheclean@.service	disabled	enabled
apache2.service	disabled	enabled
apache2@.service	disabled	enabled
apparmor.service	enabled	enabled
apport-autoreport.service	static	-
apport-forward@.service	static	-
apport.service	generated	-
apt-daily-upgrade.service	static	-
apt-daily.service	static	-
apt-news.service	static	-
autovt@.service	alias	-
avahi-daemon.service	enabled	enabled
bluetooth.service	disabled	enabled
bolt.service	static	-
brltty-udev.service	static	-

lines 1-23

2)

The unattended upgrade only upgrades unattended updated files which are in the list since samba and squid are not in the list they cannot be automatically upgraded.

```

student@student-OptiPlex-7070: ~
pulseaudio-module-bluetooth/jammy-updates 1:15.99.1+dfsg1-1ubuntu2.1 amd64 [upgradable from: 1:15.99.1+dfsg1-1ubuntu2]
pulseaudio-utils/jammy-updates 1:15.99.1+dfsg1-1ubuntu2.1 amd64 [upgradable from: 1:15.99.1+dfsg1-1ubuntu2]
pulseaudio/jammy-updates 1:15.99.1+dfsg1-1ubuntu2.1 amd64 [upgradable from: 1:15.99.1+dfsg1-1ubuntu2]
python3-apport/jammy-updates,jammy-updates,jammy-security,jammy-security 2:20.11-0ubuntu82.4 all [upgradable from: 2:20.11-0ubuntu82.3]
python3-macaronibakery/jammy-updates,jammy-updates 1:3.1-2ubuntu0.1 all [upgradable from: 1:3.1-2]
python3-problem-report/jammy-updates,jammy-updates,jammy-security,jammy-security 2:20.11-0ubuntu82.4 all [upgradable from: 2:20.11-0ubuntu82.3]
python3-software-properties/jammy-updates,jammy-updates 0.99.22.6 all [upgradable from: 0.99.22.5]
python3-tz/jammy-updates,jammy-updates 2022.1-1ubuntu0.22.04.1 all [upgradable from: 2022.1-1ubuntu0.22.04.0]
python3-uno/jammy-updates 1:7.3.7-0ubuntu0.22.04.2 amd64 [upgradable from: 1:7.3.7-0ubuntu0.22.04.1]
shim-signed/jammy-updates 1:51.3+15.7-0ubuntu1 amd64 [upgradable from: 1:51+15.4-0ubuntu9]
software-properties-common/jammy-updates,jammy-updates 0.99.22.6 all [upgradable from: 0.99.22.5]
software-properties-gtk/jammy-updates,jammy-updates 0.99.22.6 all [upgradable from: 0.99.22.5]
systemd-hwe-hwdb/jammy-updates,jammy-updates 249.11.3 all [upgradable from: 249.11.2]
systemd-oem/jammy-updates 249.11-0ubuntu3.9 amd64 [upgradable from: 249.11-0ubuntu3.7]
systemd-sysv/jammy-updates 249.11-0ubuntu3.9 amd64 [upgradable from: 249.11-0ubuntu3.7]
systemd-timesyncd/jammy-updates 249.11-0ubuntu3.9 amd64 [upgradable from: 249.11-0ubuntu3.7]
systemd/jammy-updates 249.11-0ubuntu3.9 amd64 [upgradable from: 249.11-0ubuntu3.7]
tcpdump/jammy-updates 4.99.1-3ubuntu0.1 amd64 [upgradable from: 4.99.1-3build2]
thermald/jammy-updates 2.4.9-1ubuntu0.2 amd64 [upgradable from: 2.4.9-1ubuntu0.1]
thunderbird-gnome-support/jammy-updates,jammy-security 1:102.10.0+build2-0ubuntu0.22.04.1 amd64 [upgradable from: 1:102.9.0+build1-0ubuntu0.22.04.1]
thunderbird-locale-en-us/jammy-updates,jammy-updates,jammy-security,jammy-security 1:102.10.0+build2-0ubuntu0.22.04.1 all [upgradable from: 1:102.9.0+build1-0ubuntu0.22.04.1]
thunderbird-locale-en/jammy-updates,jammy-security 1:102.10.0+build2-0ubuntu0.22.04.1 amd64 [upgradable from: 1:102.9.0+build1-0ubuntu0.22.04.1]
thunderbird/jammy-updates,jammy-security 1:102.10.0+build2-0ubuntu0.22.04.1 amd64 [upgradable from: 1:102.9.0+build1-0ubuntu0.22.04.1]
tzdata/jammy-updates,jammy-updates 2023c-0ubuntu0.22.04.1 all [upgradable from: 2022g-0ubuntu0.22.04.1]
ubuntu-advantage-tools/jammy-updates 27.14.4-22.04 amd64 [upgradable from: 27.13.5-22.04.1]
udev/jammy-updates 249.11-0ubuntu3.9 amd64 [upgradable from: 249.11-0ubuntu3.7]
uno-libs-private/jammy-updates 1:7.3.7-0ubuntu0.22.04.2 amd64 [upgradable from: 1:7.3.7-0ubuntu0.22.04.1]
update-notifier-common/jammy-updates,jammy-updates 3.192.54.6 all [upgradable from: 3.192.54.5]
update-notifier/jammy-updates 3.192.54.6 amd64 [upgradable from: 3.192.54.5]
ure/jammy-updates 1:7.3.7-0ubuntu0.22.04.2 amd64 [upgradable from: 1:7.3.7-0ubuntu0.22.04.1]
vin-common/jammy-updates,jammy-updates,jammy-security,jammy-security 2:8.2.3995-1ubuntu2.7 all [upgradable from: 2:8.2.3995-1ubuntu2.5]
vin-tiny/jammy-updates,jammy-security 2:8.2.3995-1ubuntu2.7 amd64 [upgradable from: 2:8.2.3995-1ubuntu2.5]
xserver-common/jammy-updates,jammy-updates 2:21.1.4-2ubuntu1.7-22.04.1 all [upgradable from: 2:21.1.3-2ubuntu2.9]
xserver-xephyr/jammy-updates 2:21.1.4-2ubuntu1.7-22.04.1 amd64 [upgradable from: 2:21.1.3-2ubuntu2.9]
xserver-xorg-core/jammy-updates 2:21.1.4-2ubuntu1.7-22.04.1 amd64 [upgradable from: 2:21.1.3-2ubuntu2.9]

```

3)


```
student@student-OptiPlex-7070: ~  
student@student-OptiPlex-7070:~$ sudo nano /etc/squid/blocksite  
[sudo] password for student:  
student@student-OptiPlex-7070:~$ sudo systemctl restart squid  
student@student-OptiPlex-7070:~$ sudo apt update  
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]  
Hit:2 https://dl.google.com/linux/chrome/deb stable InRelease  
Hit:3 http://pk.archive.ubuntu.com/ubuntu jammy InRelease  
Hit:4 https://ppa.launchpadcontent.net/ondrej/php/ubuntu jammy InRelease  
Get:5 http://pk.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]  
Get:6 http://pk.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]  
Get:7 http://pk.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1,062 kB]  
Get:8 http://pk.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [484 kB]  
Get:9 http://pk.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [14.1 kB]  
Fetched 1,897 kB in 6s (299 kB/s)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
152 packages can be upgraded. Run 'apt list --upgradable' to see them.  
student@student-OptiPlex-7070:~$ sudo apt upgrade  
Reading package lists... Done  
Building dependency tree... Done
```

```
student@student-OptiPlex-7070: ~  
Found initrd image: /boot/initrd.img-5.19.0-38-generic  
Found linux image: /boot/vmlinuz-5.19.0-35-generic  
Found initrd image: /boot/initrd.img-5.19.0-35-generic  
Found linux image: /boot/vmlinuz-5.15.0-71-generic  
Found initrd image: /boot/initrd.img-5.15.0-71-generic  
Memtest86+ needs a 16-bit boot, that is not available on EFI, exiting  
Warning: os-prober will be executed to detect other bootable partitions.  
Its output will be used to detect bootable binaries on them and create new boot  
entries.  
Found Windows Boot Manager on /dev/sda2@/EFI/Microsoft/Boot/bootmgfw.efi  
Adding boot menu entry for UEFI Firmware Settings ...  
done  
student@student-OptiPlex-7070:~$ sudo apt install linux-generic  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
linux-generic is already the newest version (5.15.0.71.69).  
The following packages were automatically installed and are no longer required:  
  libflashrom1 libftdi1-2 libllvm13 linux-headers-5.19.0-35-generic  
  linux-hwe-5.19-headers-5.19.0-35 linux-image-5.19.0-35-generic  
  linux-modules-5.19.0-35-generic linux-modules-extra-5.19.0-35-generic  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.  
student@student-OptiPlex-7070:~$
```

```
devil@Devil: ~  
devil@Devil:~$ sudo apt-get install ufw  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
ufw is already the newest version (0.36.1-4build1).  
ufw set to manually installed.  
The following packages were automatically installed and are no longer required:  
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver  
intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58  
libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchromaprint1  
libcodec2-1.0 libdavid5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1  
libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13 libmfx1  
libmysofa1 libnorm1 libopenmpt0 libpcr2-32-0 libpgm-5.3-0 libpostproc55  
librabbitmq4 librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0  
libsratom-0-0 libsrtp1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5  
libudfread0 libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1  
libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common  
libzvbi0 linux-headers-5.15.0-60 linux-headers-5.15.0-60-generic  
linux-headers-5.19.0-32-generic linux-hwe-5.19-headers-5.19.0-32  
linux-image-5.19.0-32-generic linux-modules-5.19.0-32-generic  
linux-modules-extra-5.19.0-32-generic mesa-va-drivers mesa-udpau-drivers  
pocketsphinx-en-us va-driver-all vdpau-driver-all  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

```
devil@Devil: ~  
devil@Devil:~$ sudo apt-get install firewalld  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver  
intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58  
libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchromaprint1  
libcodec2-1.0 libdavid5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1  
libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13 libmfx1  
libmysofa1 libnorm1 libopenmpt0 libpcr2-32-0 libpgm-5.3-0 libpostproc55  
librabbitmq4 librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0  
libsratom-0-0 libsrtp1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5  
libudfread0 libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1  
libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common  
libzvbi0 linux-headers-5.15.0-60 linux-headers-5.15.0-60-generic  
linux-headers-5.19.0-32-generic linux-hwe-5.19-headers-5.19.0-32  
linux-image-5.19.0-32-generic linux-modules-5.19.0-32-generic  
linux-modules-extra-5.19.0-32-generic mesa-va-drivers mesa-udpau-drivers  
pocketsphinx-en-us va-driver-all vdpau-driver-all  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
ipset libipset13 python3-attr python3-cap-ng python3-firewall  
python3-jsonschema python3-nftables python3-pyrsistent python3-setuptools
```

```
devil@Devil: ~  
devil@Devil:~$ sudo dpkg -l | grep nftables  
ii  libnftables1:amd64 1.0.2-1ubuntu3  
    amd64           Netfilter nftables high level userspace API library  
ii  libnftnl11:amd64 1.2.1-1build1  
    amd64           Netfilter nftables userspace API library  
ii  nftables 1.0.2-1ubuntu3  
    amd64           Program to control packet filtering rules by Netfilter proje  
ct  
ii  python3-nftables 1.0.2-1ubuntu3  
    amd64           nftables/libnftables python3 module  
devil@Devil:~$
```

```
devil@Devil: ~  
devil@Devil:~$ sudo systemctl start nftables  
devil@Devil:~$
```



```
devil@Devil: ~  
GNU nano 6.2 /etc/ufw/ufw.conf *  
# /etc/ufw/ufw.conf  
#  
# Set to yes to start on boot. If setting this remotely, be sure to add a rule  
# to allow your remote connection before starting ufw. Eg: 'ufw allow 22/tcp'  
ENABLED=no  
RULE=deny in tcp 22  
# Please use the 'ufw' command to set the loglevel. Eg: 'ufw logging medium'.  
# See 'man ufw' for details.  
LOGLEVEL=low  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

```
devil@Devil: ~  
GNU nano 6.2 /etc/nftables.conf *  
#!/usr/sbin/nft -f  
  
flush ruleset  
  
table inet filter {  
    chain input {  
        type filter hook input priority 0;  
        ct state established,related,new tcp dport 22 accept  
        ct state established,related,new tcp dport { 80,443 } accept  
        ct state established,related,new udp dport 53 accept  
        tcp dport ssh accept  
        drop  
    }  
    chain forward {  
        type filter hook forward priority 0;  
        drop  
    }  
    chain output {  
        type filter hook output priority 0;  
        ct state established,related,new accept  
    }  
}
```

```
devil@Devil: ~  
devil@Devil:~$ sudo nano /etc/nftables.conf  
devil@Devil:~$ sudo nft -f /etc/nftables.conf  
devil@Devil:~$ sudo nft list ruleset  
table inet filter {  
    chain input {  
        type filter hook input priority filter; policy accept;  
        ct state established,related,new tcp dport 22 accept  
        ct state established,related,new tcp dport { 80, 443 } accept  
        ct state established,related,new udp dport 53 accept  
        tcp dport 22 accept  
        drop  
    }  
  
    chain forward {  
        type filter hook forward priority filter; policy accept;  
        drop  
    }  
  
    chain output {  
        type filter hook output priority filter; policy accept;  
        ct state established,related,new accept  
    }  
}  
devil@Devil:~$ sudo systemctl enable nftables
```

```
table inet filter {  
    chain input {  
        type filter hook input priority filter; policy accept;  
        ct state established,related,new tcp dport 22 accept  
        ct state established,related,new tcp dport { 80, 443 } accept  
        ct state established,related,new udp dport 53 accept  
        tcp dport 22 accept  
        drop  
    }  
  
    chain forward {  
        type filter hook forward priority filter; policy accept;  
        drop  
    }  
  
    chain output {  
        type filter hook output priority filter; policy accept;  
        ct state established,related,new accept  
    }  
}  
devil@Devil:~$ sudo systemctl enable nftables  
Created symlink /etc/systemd/system/sysinit.target.wants/nftables.service → /lib  
/systemd/system/nftables.service.  
devil@Devil:~$
```

```
devil@Devil: ~  
devil@Devil:~$ sudo nano /etc/pam.d/common-password  
devil@Devil:~$ sudo nano /etc/login.defs  
devil@Devil:~$ sudo nano /etc/login.defs  
devil@Devil:~$
```

```
GNU nano 6.2 /etc/pam.d/common-password *  
#between Debian 11 and older releases replace "yescrypt" with "sha512"  
#for compatibility . The "obscure" option replaces the old  
# 'OBSCURE_CHECKS_ENAB' option in login.defs. See the pam_unix manpage  
#for other options.  
  
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.  
# To take advantage of this, it is recommended that you configure any  
# local modules either before or after the default block, and use  
# pam-auth-update to manage selection of other modules. See  
# pam-auth-update(8) for details.  
  
# 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  
password requisite pam_pwquality.so minlen=8 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1  
# 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  
  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-6 Copy
```

```
GNU nano 6.2 /etc/login.defs *  
# PASS_MAX_DAYS Maximum number of days a password may be used.  
# PASS_MIN_DAYS Minimum number of days allowed between password changes.  
# PASS_WARN_AGE Number of days warning given before a password expires.  
#  
PASS_MAX_DAYS 90  
PASS_MIN_DAYS 0  
PASS_WARN_AGE 14  
PASS_MIN_LEN 8  
PASS_HISTORY 5  
  
#  
# Min/max values for automatic uid selection in useradd  
#  
UID_MIN 1000  
UID_MAX 60000  
# System accounts  
#SYS_UID_MIN 100  
#SYS_UID_MAX 999  
#  
  
^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
```

```
devil@Devil: ~  
devil@Devil:~$ sudo nano /etc/pam.d/common-password  
devil@Devil:~$ sudo nano /etc/login.defs  
devil@Devil:~$ sudo nano /etc/login.defs  
devil@Devil:~$ sudo nano /etc/pam.d/common-password  
devil@Devil:~$ sudo nano /etc/pam.d/common-password  
devil@Devil:~$ sudo chage -d 0 devil
```

6)

```
devil@Devil: ~  
devil@Devil:~$ mkdir 21k-3815  
devil@Devil:~$ chown devil 21k-3815  
devil@Devil:~$ chgrp sensitive-group 21k-3815  
chgrp: invalid group: 'sensitive-group'  
devil@Devil:~$ chmod u+rw 21k-3815  
devil@Devil:~$ chmod g+r 21k-3815  
devil@Devil:~$ chmod o-rwx 21k-3815  
devil@Devil:~$ setfacl -m u:devil:rw 21k-3815  
devil@Devil:~$ ls -la  
total 131908  
drwxrwx---+ 30 devil devil 4096 07:36 1 .  
drwxr-xr-x 4 root root 4096 04:15 11 ..  
drwxrwx---+ 2 devil devil 4096 21 07:36 1 21k-3815  
drwxrwxr-x 2 devil devil 4096 23:09 10 .android  
-rw-rwx---+ 1 devil devil 27704 19:27 30 .bash_history  
-rw-rwxr---+ 1 devil devil 220 18:27 29 .bash_logout  
-rw-rwxr---+ 1 devil devil 3771 18:27 29 .bashrc  
drwxrwx---+ 20 devil devil 4096 23:09 10 .cache  
drwxrwx---+ 20 devil devil 4096 23:09 10 .config  
-rw----- 1 devil devil 115 01:28 7 dead.letter  
drwxrwxr-x+ 6 devil devil 4096 23:37 23 Desktop  
drwxrwxr-x+ 2 devil devil 4096 18:36 29 Documents  
drwxrwxr-x 3 devil devil 4096 22:55 21 .dotnet  
drwxrwxr-x+ 5 devil devil 4096 06:02 1 Downloads
```

7)

```
devil@Devil: ~
GNU nano 6.2 /etc/sudoers.tmp *

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
21k-3815 ALL=(ALL) /bin/ls
# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@include /etc/sudoers.d

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
useradd: user '21k-3815' already exists
devil@Devil:~$
```

```
devil@Devil: ~
[sudo] password for devil:
devil@Devil:~$ sudo usermod -aG hello 21k-3815
usermod: group 'hello' does not exist
devil@Devil:~$ sudo visudo
devil@Devil:~$ sudo tail -f /var/log/syslog
May  1 18:42:56 Devil systemd[2504]: Starting Tracker metadata extractor...
May  1 18:42:56 Devil dbus-daemon[2523]: [session uid=1000 pid=2523] Successfully activated service 'org.freedesktop.Tracker3.Miner.Extract'
May  1 18:42:56 Devil systemd[2504]: Started Tracker metadata extractor.
May  1 18:43:01 Devil gnome-shell[2690]: meta_window_set_stack_position_no_sync: assertion 'window->stack_position >= 0' failed
May  1 18:43:37 Devil NetworkManager[726]: <info> [1682948617.9159] dhcp4 (enp0s8): state changed new lease, address=192.168.56.101
May  1 18:45:08 Devil firefox_firefox.desktop[4359]: ATTENTION: default value of option mesa_glthread overridden by environment.
May  1 18:47:04 Devil dbus-daemon[2523]: [session uid=1000 pid=2523] Activating via systemd: service name='org.freedesktop.Tracker3.Miner.Extract' unit='tracker-extract-3.service' requested by ':1.11' (uid=1000 pid=2626 comm="/usr/libexec/tracker-miner-fs-3 ")
May  1 18:47:04 Devil systemd[2504]: Starting Tracker metadata extractor...
May  1 18:47:04 Devil dbus-daemon[2523]: [session uid=1000 pid=2523] Successfully activated service 'org.freedesktop.Tracker3.Miner.Extract'
May  1 18:47:04 Devil systemd[2504]: Started Tracker metadata extractor.
```



```
devil@Devil: ~  
devil@Devil:~$ sudo last  
devil      tty2          tty2          Mon May  1 05:49      gone - no logout  
reboot     system boot  6.1.12        Mon May  1 05:47      still running  
devil      tty2          tty2          Sun Apr 30 18:16 -   down (01:10)  
reboot     system boot  6.1.12        Sun Apr 30 18:15 -   19:27 (01:12)  
devil      tty2          tty2          Mon Apr 10 22:40 -   down (01:04)  
reboot     system boot  6.1.12        Mon Apr 10 22:36 -   23:44 (01:08)  
devil      tty2          tty2          Mon Apr 10 22:27 -   down (00:08)  
reboot     system boot  6.1.12        Mon Apr 10 22:25 -   22:35 (00:09)  
devil      tty2          tty2          Mon Apr 10 22:10 -   down (00:14)  
reboot     system boot  6.1.12        Mon Apr 10 22:08 -   22:24 (00:15)  
devil      tty2          tty2          Thu Mar 23 20:32 -   down (1+09:46)  
reboot     system boot  6.1.12        Thu Mar 23 20:31 -   06:19 (1+09:48)  
devil      tty2          tty2          Tue Mar 21 20:47 -   down (05:18)  
reboot     system boot  6.1.12        Tue Mar 21 20:45 -   02:05 (05:19)  
devil      tty2          tty2          Mon Mar 20 01:54 -   down (22:03)  
reboot     system boot  6.1.12        Mon Mar 20 01:53 -   23:58 (22:05)  
devil      tty2          tty2          Tue Mar  7 01:26 -   down (00:03)  
reboot     system boot  6.1.12        Tue Mar  7 01:24 -   01:29 (00:05)  
devil      tty2          tty2          Mon Mar  6 20:25 -   down (04:48)  
reboot     system boot  6.1.12        Mon Mar  6 20:24 -   01:14 (04:50)  
devil      tty2          tty2          Wed Feb 22 19:15 -   down (02:46)  
reboot     system boot  6.1.12        Wed Feb 22 19:13 -   22:01 (02:47)  
devil      tty2          tty2          Wed Feb 22 01:15 -   down (00:33)
```

```
devil@Devil: ~  
devil@Devil:~$ sudo w  
18:48:31 up 1:57, 2 users, load average: 1.01, 1.27, 1.94  
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT  
devil     tty2     tty2          05:49   13:00m 0.06s  0.06s /usr/libexec/gn  
devil     pts/1    -            18:48   0.00s  0.01s  0.00s sudo w  
devil@Devil:~$
```

```
devil pts/1 - 18:48 0.00s 0.01s 0.00s sudo w
devil@Devil:~$ sudo apt-get install auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
 intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58
 libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchromaprint1
 libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1
 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13 libmfx1
 libmysofa1 libnorm1 libopenmpt0 libpcre2-32-0 libpgm-5.3-0 libpostproc55
 librabbitmq4 librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0
 libsratom-0-0 libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5
 libudfread0 libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1
 libvidstab1.1 libx265-199 libxvidcore4 libzing2 libzmq5 libzvbi-common
 libzvbi0 linux-headers-5.15.0-60 linux-headers-5.15.0-60-generic
 linux-headers-5.19.0-32-generic linux-hwe-5.19-headers-5.19.0-32
 linux-image-5.19.0-32-generic linux-modules-5.19.0-32-generic
 linux-modules-extra-5.19.0-32-generic mesa-va-drivers mesa-va-drivers
 pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 libauparse0
```

```
devil@Devil:~$ sudo apt-get install auditd
Preparing to unpack .../libauparse0_1%3a3.0.7-1build1_amd64.deb ...
Unpacking libauparse0:amd64 (1:3.0.7-1build1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a3.0.7-1build1_amd64.deb ...
Unpacking auditd (1:3.0.7-1build1) ...
Setting up libauparse0:amd64 (1:3.0.7-1build1) ...
Setting up auditd (1:3.0.7-1build1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service → /li
b/systemd/system/auditd.service.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
devil@Devil:~$ sudo auitctl -e 1
sudo: auitctl: command not found
devil@Devil:~$ sudo auditctl -e 1
enabled 1
failure 1
pid 72302
rate_limit 0
backlog_limit 8192
lost 0
backlog 3
backlog_wait_time 60000
backlog_wait_time_actual 0
devil@Devil:~$
```