

## Users

```

File Actions Edit View Help
(aravindh@kali)-[~]
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MySQL Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:105:105::/var/lib/gophish:/usr/sbin/nologin
iodine:x:106:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:107:106::/nonexistent:/usr/sbin/nologin
tcpdump:x:108:107::/nonexistent:/usr/sbin/nologin
miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:110:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:111:109::/var/lib/snmp:/bin/false
redis:x:112:111::/var/lib/redis:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:114:114::/var/lib/mosquitto:/usr/sbin/nologin
redsocks:x:115:115::/var/run/redsocks:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
sshd:x:116:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin
ssldh:x:118:118::/nonexistent:/usr/sbin/nologin
postgres:x:119:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:120:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
_gvm:x:121:122::/var/lib/opensvas:/usr/sbin/nologin
speech-dispatcher:x:122:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
inetsim:x:123:124::/var/lib/inetsim:/usr/sbin/nologin
pulse:x:124:125:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
geoclue:x:125:127::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:126:128:Light Display Manager:/var/lib/lightdm:/bin/false
saned:x:127:130::/var/lib/saned:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/:/usr/sbin/nologin
rtkit:x:128:131:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:129:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:130:133:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:131:134:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
aravindh:x:1000:1000:Aravindh,,,:/home/aravindh:/usr/bin/zsh
(aravindh@kali)-[~]
$

```

```
(aravindh@kali)-[~]  
$ cat /etc/group  
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:aravindh  
tty:x:5:  
disk:x:6:  
lp:x:7:  
mail:x:8:  
news:x:9:  
uucp:x:10:  
man:x:12:  
proxy:x:13:  
kmem:x:15:  
dialout:x:20:aravindh  
fax:x:21:  
voice:x:22:  
cdrom:x:24:aravindh  
floppy:x:25:aravindh  
tape:x:26:  
sudo:x:27:aravindh  
audio:x:29:pulse,aravindh  
dip:x:30:aravindh  
www-data:x:33:  
backup:x:34:  
operator:x:37:  
list:x:38:  
irc:x:39:  
src:x:40:  
shadow:x:42:  
utmp:x:43:  
video:x:44:aravindh  
sasl:x:45:  
plugdev:x:46:aravindh  
staff:x:50:  
games:x:60:  
users:x:100:aravindh  
nogroup:x:65534:
```

groups

password

```
cat: /etc/shadow: Permission denied

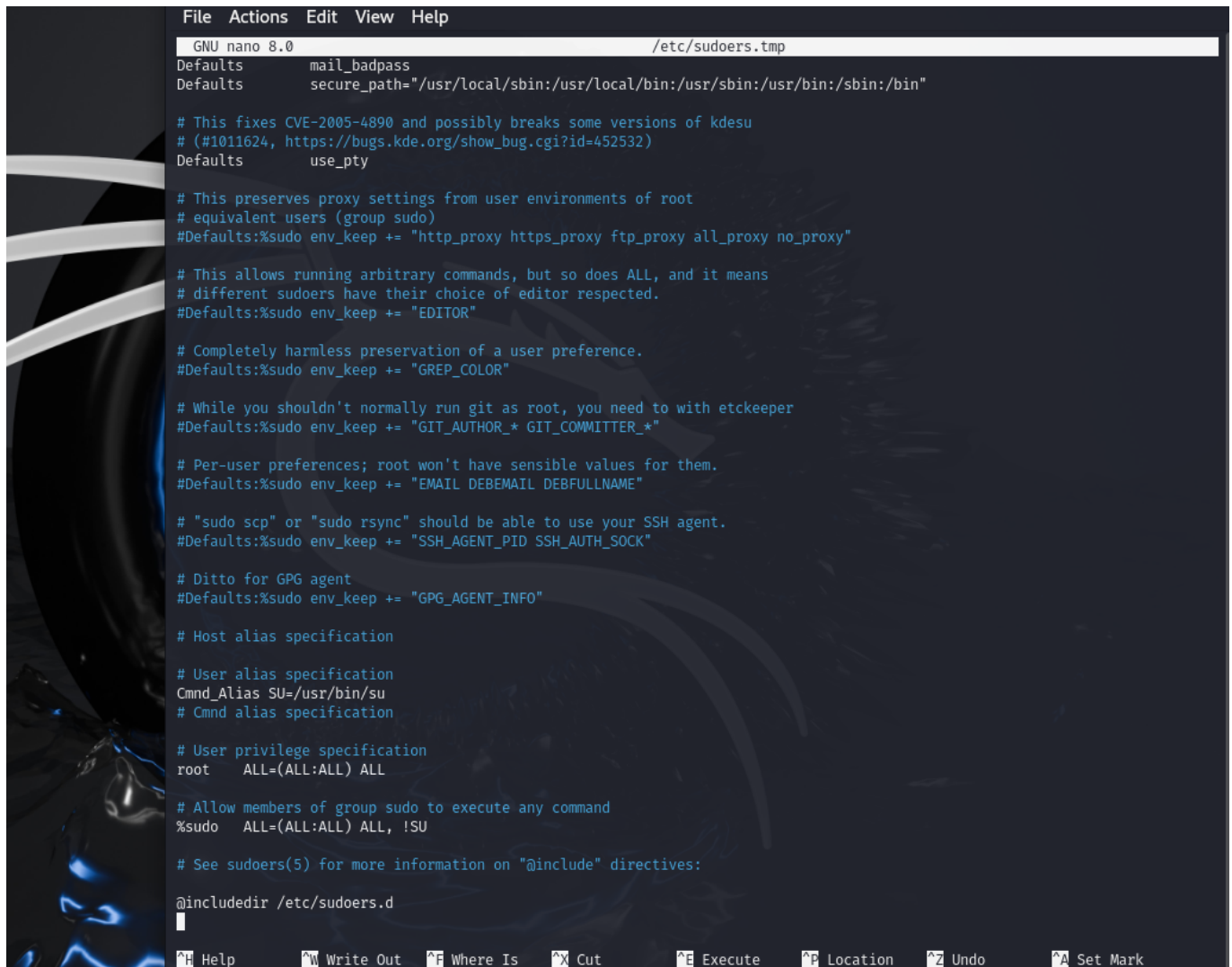
(aravindh@kali)-[~]
$ sudo cat /etc/shadow
root!!:19973:0:99999:7:::
daemon*:19973:0:99999:7:::
bin*:19973:0:99999:7:::
sys*:19973:0:99999:7:::
sync*:19973:0:99999:7:::
games*:19973:0:99999:7:::
man*:19973:0:99999:7:::
lp*:19973:0:99999:7:::
mail*:19973:0:99999:7:::
news*:19973:0:99999:7:::
uucp*:19973:0:99999:7:::
proxy*:19973:0:99999:7:::
www-data*:19973:0:99999:7:::
backup*:19973:0:99999:7:::
list*:19973:0:99999:7:::
irc*:19973:0:99999:7:::
_apt*:19973:0:99999:7:::
nobody*:19973:0:99999:7:::
systemd-networkd!:19973:0:99999:7:::
_galera!:19973:0:99999:7:::
mysql!:19973:0:99999:7:::
tss!:19973:0:99999:7:::
strongswan!:19973:0:99999:7:::
systemd-timesyncd!:19973:0:99999:7:::
rwhod!:19973:0:99999:7:::
_gophish!:19973:0:99999:7:::
iodine!:19973:0:99999:7:::
messagebus!:19973:0:99999:7:::
tcpdump!:19973:0:99999:7:::
miredo!:19973:0:99999:7:::
_rpc!:19973:0:99999:7:::
Debian-snmpp!:19973:0:99999:7:::
redis!:19973:0:99999:7:::
usbmux!:19973:0:99999:7:::
```

shells

```
(aravindh@kali)-[~]
$ cat /etc/shells
# /etc/shells: valid login shells
/bin/sh
/usr/bin/sh
/bin/bash
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/bin/dash
/usr/bin/dash
/usr/bin/pwsh
/opt/microsoft/powershell/7/pwsh
/usr/bin/screen
/usr/bin/tmux
/bin/zsh
/usr/bin/zsh
/usr/bin/zsh

(aravindh@kali)-[~]
$
```

restrict sudo su



```
File Actions Edit View Help
GNU nano 8.0 /etc/sudoers.tmp
Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification
Cmnd_Alias SU=/usr/bin/su
# Cmnd alias specification

# User privilege specification
root ALL=(ALL:ALL) ALL

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

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

@includedir /etc/sudoers.d
^H Help ^W Write Out ^F Where Is ^X Cut ^E Execute ^P Location ^Z Undo ^A Set Mark
```

create user and group ,addgroup to user, del user and group

```
File Actions Edit View Help
(aravindh@kali)-[~]
$ sudo useradd salar
[sudo] password for aravindh:

(aravindh@kali)-[~]
$ sudo groupadd remoteusers

(aravindh@kali)-[~]
$ sudo usermod -aG remoteusers salar

(aravindh@kali)-[~]
$ sudo passwd salar
New password:
Retype new password:
passwd: password updated successfully

(aravindh@kali)-[~]
$ sudo userdel salar

(aravindh@kali)-[~]
$ sudo groupdel remoteusers

(aravindh@kali)-[~]
$
```

changing directory from /(root) to ~

```
(aravindh@kali)-[~]
$ cd /

(aravindh@kali)-[/]
$ cd

(aravindh@kali)-[~]
$
```

(home)

to check particular file permissions

```
(aravindh@kali)-[~]
$ ls
1.txt Desktop Documents Downloads Music Pictures Public Templates Videos

(aravindh@kali)-[~]
$ ls -la 1.txt
-rw-rw-r-- 1 aravindh aravindh 0 Sep  8 06:32 1.txt

(aravindh@kali)-[~]
$
```

file permissions d- directory l-linked directory r- read w- write x-execute

assigning permissions for file:

Octal	Binary	File Mode
0	000	---
1	001	--X
2	010	-W-
3	011	-WX
4	100	r--
5	101	r-X
6	110	rw-
7	111	rwX

creating new file 2.txt and

removing all permissions

```
(aravindh@kali)-[~]
$ touch 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
-rw-rw-r-- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod 000 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
----- 1 aravindh aravindh 0 Sep  8 07:02 2.txt
```



```
File Actions Edit View Help
(aravindh@kali)-[~]
$ chmod 777 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
-rwxrwxrwx 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod 444 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
-r--r--r-- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod 333 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
--wx-wx-wx 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod 222 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
--w--w--w- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$
```

```
(aravindh@kali)-[~]
$ chmod 000 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
----- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod +r 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
-r--r--r-- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod +w 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
-rw-rw-r-- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod 000 2.txt

(aravindh@kali)-[~]
$ chmod +w 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
--w--w---- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod 000 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
----- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod +x 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
--x--x--x 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$ chmod -x 2.txt

(aravindh@kali)-[~]
$ ls -la 2.txt
----- 1 aravindh aravindh 0 Sep  8 07:02 2.txt

(aravindh@kali)-[~]
$
```



```

(aravindh@kali)-[~]
$ ls -la
total 132
drwx----- 16 aravindh aravindh 4096 Sep  8 07:02 .
drwxr-xr-x  3 root      root      4096 Sep  7 07:17 ..
-rw-----  1 aravindh aravindh    0 Sep  7 07:21 .ICEauthority
-rw-----  1 aravindh aravindh   49 Sep  7 07:21 .Xauthority
-rw-r--r--  1 aravindh aravindh  220 Sep  7 07:17 .bash_logout
-rw-r--r--  1 aravindh aravindh 5551 Sep  7 07:17 .bashrc
-rw-r--r--  1 aravindh aravindh 3526 Sep  7 07:17 .bashrc.original
drwxrwxr-x  9 aravindh aravindh 4096 Sep  8 05:06 .cache
drwxr-xr-x 14 aravindh aravindh 4096 Sep  8 05:11 .config
-rw-r--r--  1 aravindh aravindh   35 Sep  7 07:21 .dmrc
-rw-r--r--  1 aravindh aravindh 11759 Sep  7 07:17 .face
lrwxrwxrwx  1 aravindh aravindh    5 Sep  7 07:17 .face.icon -> .face
drwx-----  3 aravindh aravindh 4096 Sep  7 07:21 .gnupg
drwxr-xr-x  3 aravindh aravindh 4096 Sep  7 07:17 .java
drwxr-xr-x  4 aravindh aravindh 4096 Sep  7 07:21 .local
drwx-----  4 aravindh aravindh 4096 Sep  8 05:06 .mozilla
-rw-r--r--  1 aravindh aravindh  807 Sep  7 07:17 .profile
-rw-r--r--  1 aravindh aravindh    0 Sep  8 05:10 .sudo_as_admin_successful
-rw-----  1 aravindh aravindh 1286 Sep  8 05:15 .viminfo
-rw-----  1 aravindh aravindh 6305 Sep  8 06:53 .xsession-errors
-rw-----  1 aravindh aravindh 1502 Sep  8 06:53 .zsh_history
-rw-r--r--  1 aravindh aravindh 10868 Sep  7 07:17 .zshrc
-rw-rw-r--  1 aravindh aravindh    0 Sep  8 06:32 1.txt
-----  1 aravindh aravindh    0 Sep  8 07:02 2.txt
drwxr-xr-x  2 aravindh aravindh 4096 Sep  7 07:21 Desktop
drwxr-xr-x  2 aravindh aravindh 4096 Sep  8 05:19 Documents
drwxr-xr-x  2 aravindh aravindh 4096 Sep  7 07:21 Downloads
drwxr-xr-x  2 aravindh aravindh 4096 Sep  7 07:21 Music
drwxr-xr-x  2 aravindh aravindh 4096 Sep  7 07:21 Pictures
drwxr-xr-x  2 aravindh aravindh 4096 Sep  7 07:21 Public
drwxr-xr-x  2 aravindh aravindh 4096 Sep  7 07:21 Templates
drwxr-xr-x  2 aravindh aravindh 4096 Sep  7 07:21 Videos

(aravindh@kali)-[~]
$

```

pattern follows as **file permission no.of files user group Size Date**

```
drwx----- 16 aravindh aravindh 4096 Sep  8 07:02 .
```