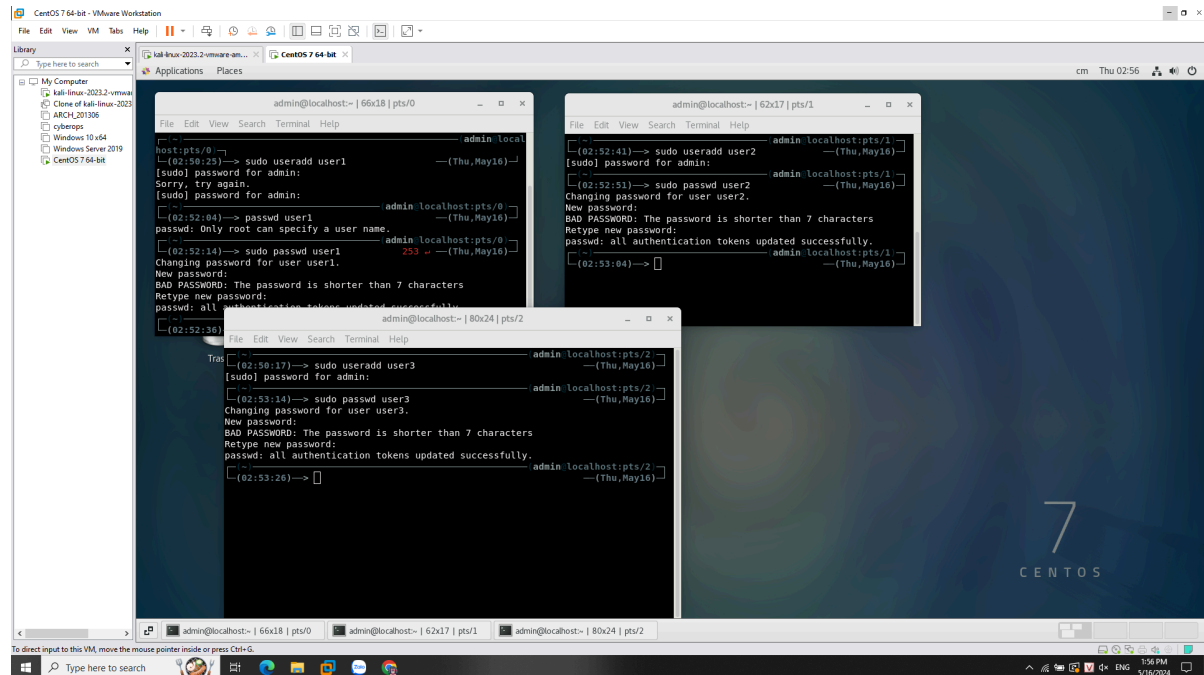


LAB 3 - Securing administrative and normal user accounts

2.1 – Assigning limited sudo privileges

Create and set paswd for three user

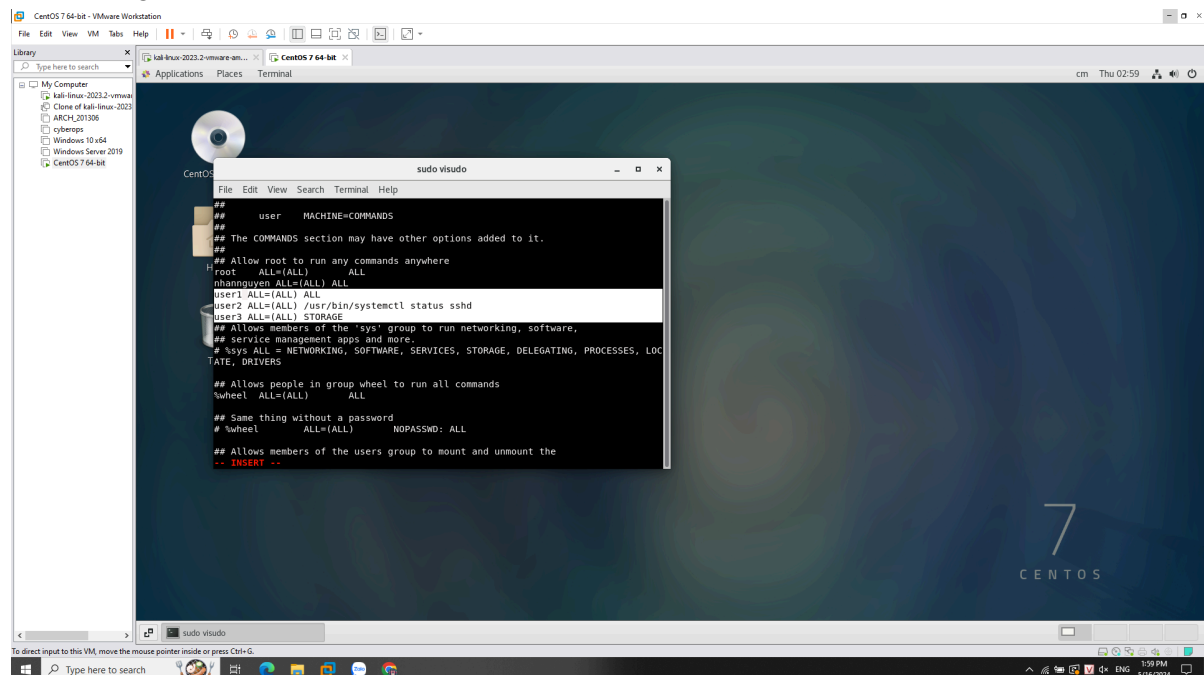


```
admin@localhost:~| 66x18 | pts/0
File Edit View Search Terminal Help
--(Thu,May16)--
[02:50:25]--> sudo useradd user1
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
--(Thu,May16)--
[02:52:04]--> passwd user1
passwd: Only root can specify a user name.
--(Thu,May16)--
[02:52:14]--> sudo passwd user1
Changing password for user user1.
New password:
BAD PASSWORD: The password is shorter than 7 characters
Retype new password:
passwd: all authentication tokens updated successfully.
--(Thu,May16)--
[02:52:36]-->

admin@localhost:~| 62x17 | pts/1
File Edit View Search Terminal Help
--(Thu,May16)--
[02:52:43]--> sudo useradd user2
[sudo] password for admin:
--(Thu,May16)--
[02:52:51]--> sudo passwd user2
Changing password for user user2.
New password:
BAD PASSWORD: The password is shorter than 7 characters
Retype new password:
passwd: all authentication tokens updated successfully.
--(Thu,May16)--
[02:53:04]-->

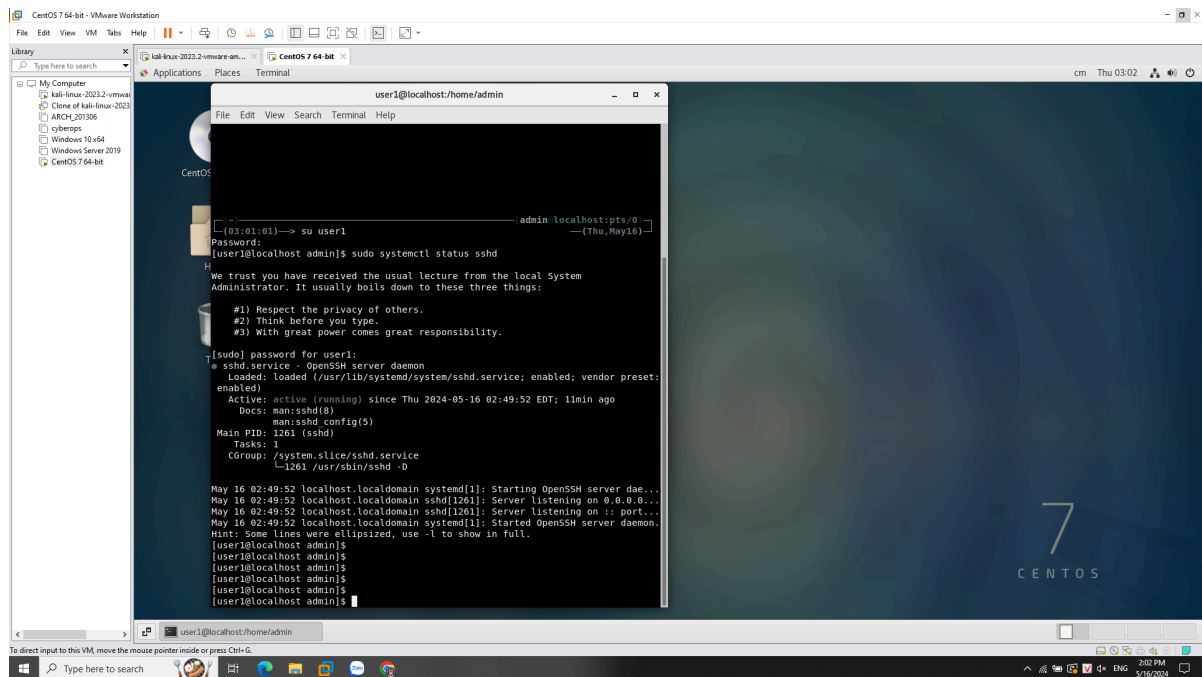
admin@localhost:~| 80x24 | pts/2
File Edit View Search Terminal Help
--(Thu,May16)--
[02:50:17]--> sudo useradd user3
[sudo] password for admin:
--(Thu,May16)--
[02:53:14]--> sudo passwd user3
Changing password for user user3.
New password:
BAD PASSWORD: The password is shorter than 7 characters
Retype new password:
passwd: all authentication tokens updated successfully.
--(Thu,May16)--
[02:53:26]-->
```

Set privilege for three created user accounts

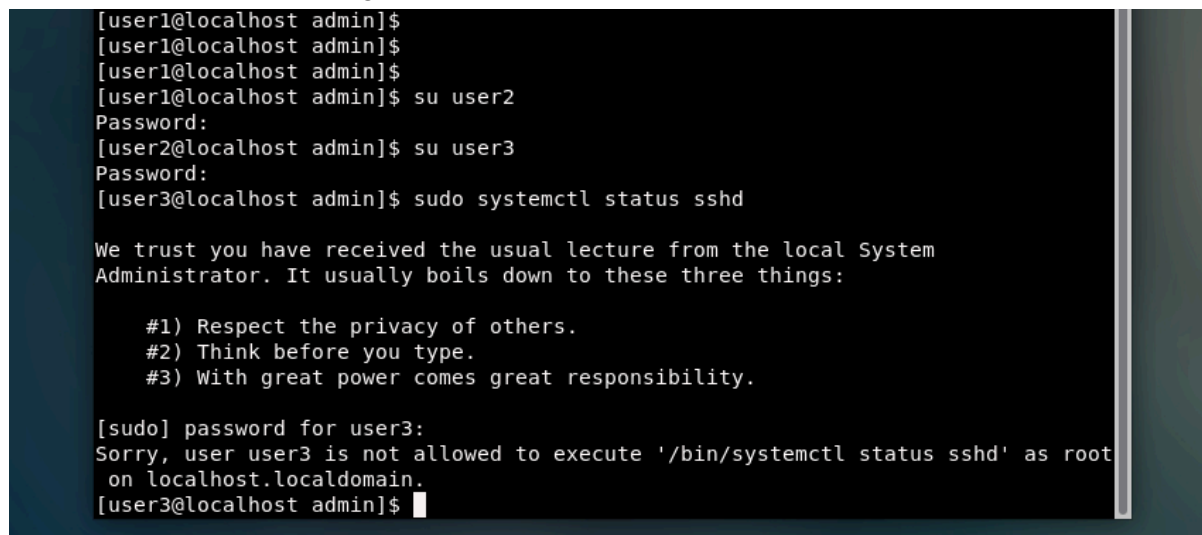


```
sudo visudo
##
## user MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root ALL=(ALL) ALL
nhandnguyen ALL=(ALL) ALL
user1 ALL=(ALL) ALL
user2 ALL=(ALL) /usr/bin/systemctl status sshd
user3 ALL=(ALL) STORAGE
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
#sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOC
TATE, DRIVERS
## Allows people in group wheel to run all commands
%wheel ALL=(ALL) ALL
## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
## Allows members of the users group to mount and unmount the
-- INSERT --
```

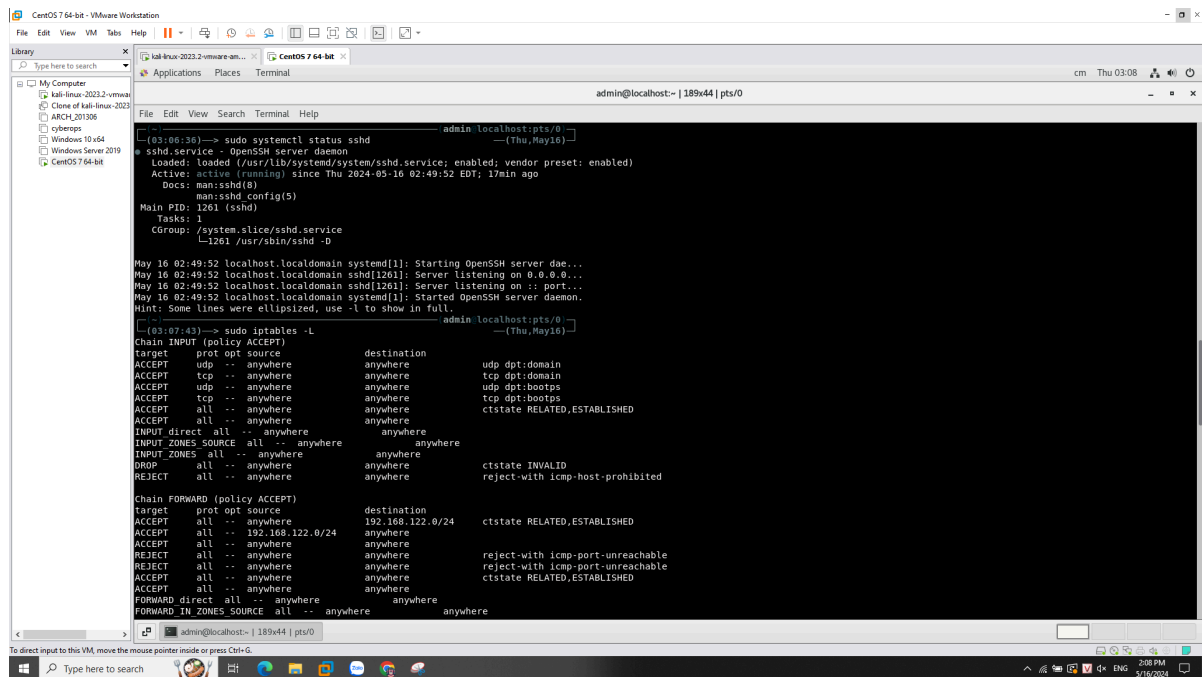
Check privilege of user



User3 are not allow to configure ssh, so it restricted



2.2 – Disabling the sudo timer

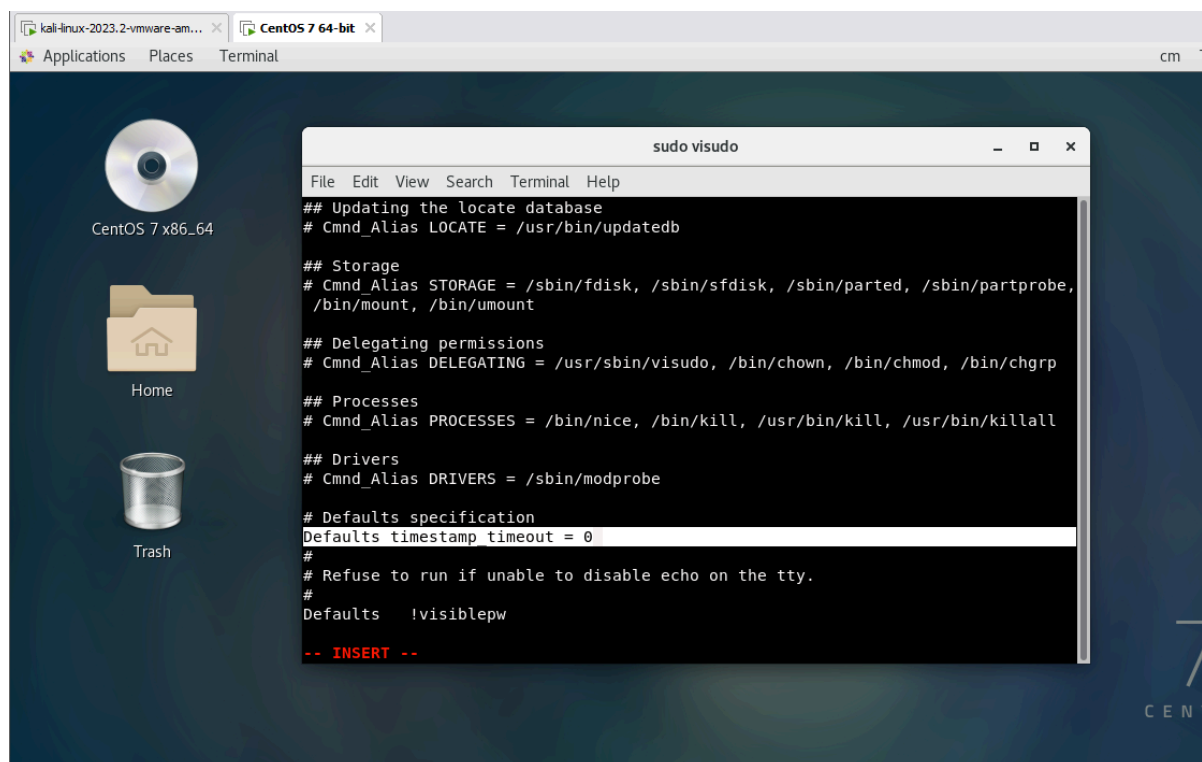


```
admin@localhost:~$ sudo systemctl status sshd
--(Thu, May 16)--
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-05-16 02:49:52 EDT; 17min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 1261 (sshd)
      Tasks: 1
   CGroup: /system.slice/ssh.service
           └─1261 /usr/sbin/sshd -D

May 16 02:49:52 localhost.localdomain systemd[1]: Starting OpenSSH server daemo...
May 16 02:49:52 localhost.localdomain sshd[1261]: Server listening on 0.0.0.0 port...
May 16 02:49:52 localhost.localdomain sshd[1261]: Server listening on :: port...
May 16 02:49:52 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
Hint: Some lines were ellipsized, use -l to show in full.

admin@localhost:~$ sudo iptables -L
--(Thu, May 16)--
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT udp -- anywhere anywhere udp dpt:domain
ACCEPT tcp -- anywhere anywhere tcp dpt:domain
ACCEPT udp -- anywhere anywhere udp dpt:bootps
ACCEPT tcp -- anywhere anywhere tcp dpt:bootps
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere
INPUT direct all -- anywhere anywhere
INPUT_ZONES_SOURCE all -- anywhere anywhere
INPUT_ZONES all -- anywhere anywhere
DROP all -- anywhere anywhere ctstate INVALID
REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere 192.168.122.0/24 anywhere ctstate RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere anywhere
REJECT all -- anywhere anywhere reject-with icmp-port-unreachable
REJECT all -- anywhere anywhere reject-with icmp-port-unreachable
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere
FORWARD direct all -- anywhere anywhere anywhere
FORWARD_IN_ZONES_SOURCE all -- anywhere anywhere anywhere
```



After modified "Defaults:user1 timestamp_timeout = 0" then it ask for password every time login again

```
user1@localhost:/home/admin
File Edit View Search Terminal Help
t.localdomain.
[user2@localhost admin]$ su admin
Password:
[admin@localhost:pts/0]
[03:16:34]—> sudo visudo
[sudo] password for admin:
Warning: /etc/sudoers:104 Cmd_Alias "STORAGE" referenced but not defined
[admin@localhost:pts/0]
[03:17:15]—> su user1
Password:
[user1@localhost admin]$ sudo fdisk -l
[sudo] password for user1:

Disk /dev/sda: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000adc8a

    Device Boot      Start         End      Blocks   Id  System
/dev/sda1    *        2048     2099199     1048576    83  Linux
/dev/sda2            2099200     41943039     19921920    8e  Linux LVM

Disk /dev/mapper/centos-root: 18.2 GB, 18249416704 bytes, 35643392 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/centos-swap: 2147 MB, 2147483648 bytes, 4194304 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[user1@localhost admin]$ S
```

View own privilege

```
[user1@localhost admin]$ sudo -l
[sudo] password for user1:
Matching Defaults entries for user1 on localhost:
    timestamp_timeout=0, !visiblepw, always_set_home, match_group_by_gid,
    always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME
    HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG
    LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION
    LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS
    _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

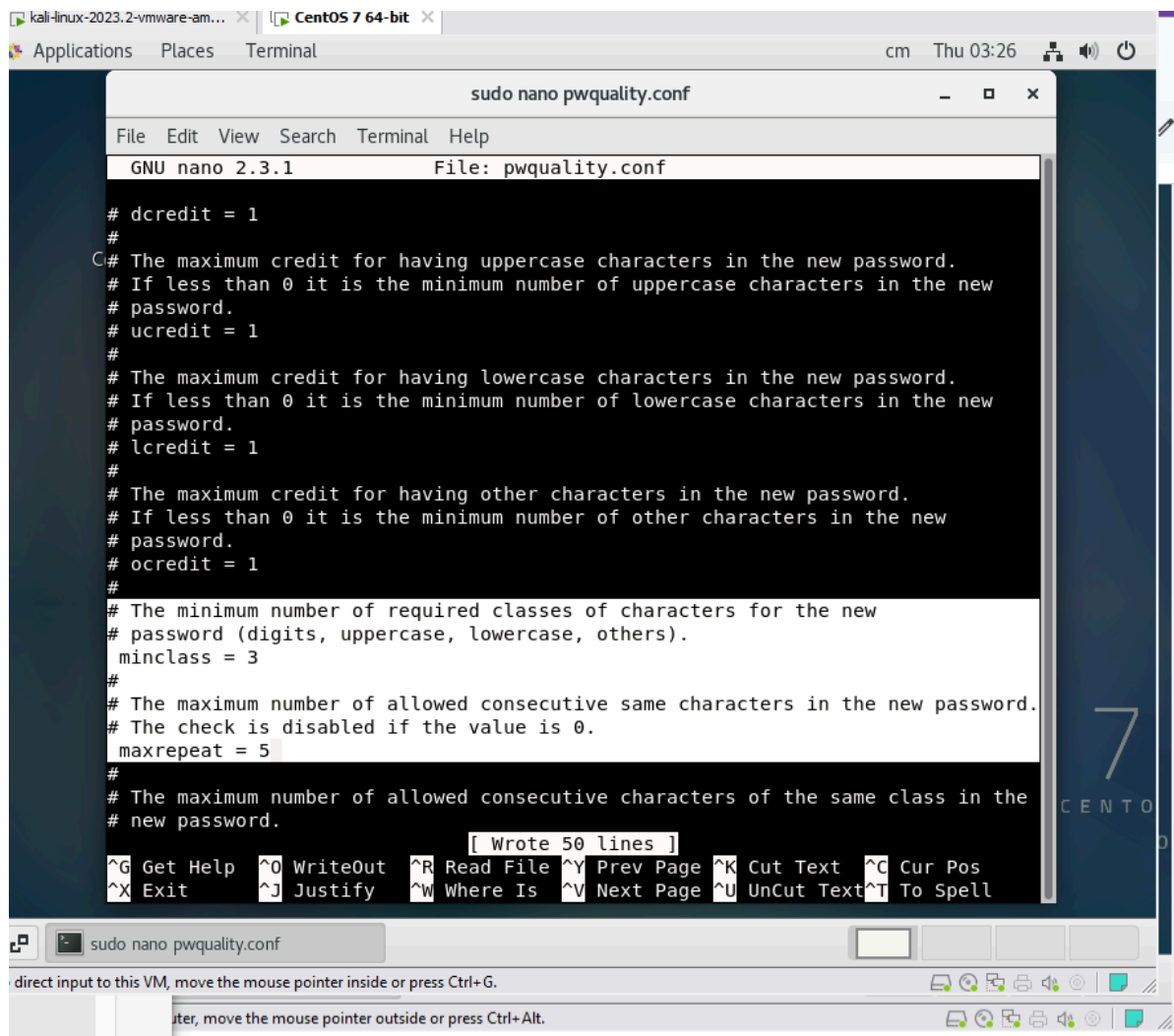
User user1 may run the following commands on localhost:
    (ALL) ALL
[user1@localhost admin]$
```

3.2 – Setting password complexity criteria

Set min-length for password

```
sudo nano pwquality.conf
File Edit View Search Terminal Help
GNU nano 2.3.1 File: pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 5
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 19
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 1
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 1
#
# The maximum credit for having other characters in the new password.
[ Read 50 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Change the parameter of min-class and max-repeat

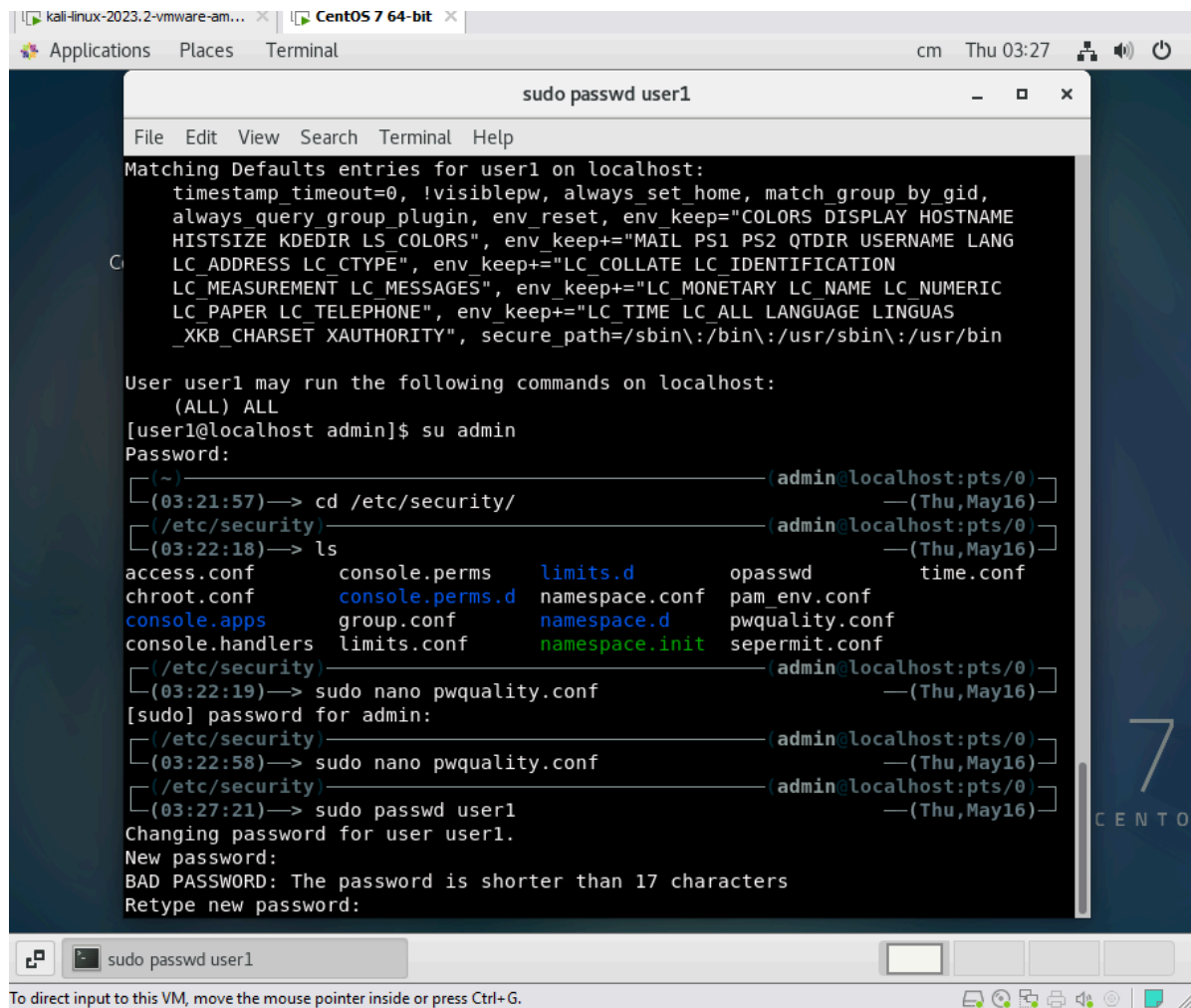


```
sudo nano pwquality.conf
File Edit View Search Terminal Help
GNU nano 2.3.1 File: pwquality.conf

# dcredit = 1
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
minclass = 3
#
# The maximum number of allowed consecutive same characters in the new password.
# The check is disabled if the value is 0.
maxrepeat = 5
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.

[ Wrote 50 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

The terminal ask for re-enter new password if it mismatch the rule



```
kali-linux-2023.2-vmware-am... CentOS 7 64-bit
Applications Places Terminal cm Thu 03:27

sudo passwd user1
File Edit View Search Terminal Help

Matching Defaults entries for user1 on localhost:
timestamp_timeout=0, !visiblepw, always_set_home, match_group_by_gid,
always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME
HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG
LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION
LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC
LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS
_XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User user1 may run the following commands on localhost:
(ALL) ALL
[user1@localhost admin]$ su admin
Password:
[~] (admin@localhost:pts/0)
(03:21:57) -> cd /etc/security/ (Thu, May 16)
(/etc/security) (admin@localhost:pts/0)
(03:22:18) -> ls (Thu, May 16)
access.conf console.perms limits.d opasswd time.conf
chroot.conf console.perms.d namespace.conf pam_env.conf
console.apps group.conf namespace.d pwquality.conf
console.handlers limits.conf namespace.init sepermit.conf
(/etc/security) (admin@localhost:pts/0)
(03:22:19) -> sudo nano pwquality.conf (Thu, May 16)
[sudo] password for admin:
(/etc/security) (admin@localhost:pts/0)
(03:22:58) -> sudo nano pwquality.conf (Thu, May 16)
(/etc/security) (admin@localhost:pts/0)
(03:27:21) -> sudo passwd user1 (Thu, May 16)
Changing password for user user1.
New password:
BAD PASSWORD: The password is shorter than 17 characters
Retype new password:
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

3.3 – Setting account and password expiry data

I've create a tempuser which have expired day is 2025-06-30 and then change it into 2025-07-31


```
admin@localhost:/etc/security | 80x32 | pts/0
File Edit View Search Terminal Help
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:22:58) -> sudo nano pwquality.conf ] (Thu, May16)
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:27:21) -> sudo passwd user1 ] (Thu, May16)
54 Changing password for user user1.
New password:
BAD PASSWORD: The password is shorter than 17 characters
Retype new password:
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:28:57) -> sudo useradd -e 2025-06-30 tempuser ] 130 ↵ (Thu, May16)
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:30:16) -> sudo chage -l tempuser ] (Thu, May16)
Last password change : May 16, 2024
Password expires : never
Password inactive : never
Account expires : Jun 30, 2025
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:30:31) -> sudo usermod -e 2025-07-31 tempuser ] (Thu, May16)
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:31:25) -> sudo chage -l tempuser ] (Thu, May16)
Last password change : May 16, 2024
Password expires : never
Password inactive : never
Account expires : Jul 31, 2025
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:31:34) -> ] (Thu, May16)
```

Assign password and set a five-day waiting period for changing passwords


```
admin@localhost:/etc/security | 80x44 | pts/0
File Edit View Search Terminal Help
Password:
su: Authentication failure
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:34:06) ] -> sudo passwd tempuser 1 ↵ —(Thu,May16)
Changing password for user tempuser.
New password:
BAD PASSWORD: The password contains less than 3 character classes
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains less than 3 character classes
Retype new password:
passwd: all authentication tokens updated successfully.
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:35:08) ] -> sudo chage -m 5 -M 90 -l 2 -W 5 tempuser —(Thu,May16)
Usage: chage [options] LOGIN

Options:
  -d, --lastday LAST_DAY      set date of last password change to LAST_DAY
  -E, --expiredate EXPIRE_DATE set account expiration date to EXPIRE_DATE
  -h, --help                  display this help message and exit
  -I, --inactive INACTIVE     set password inactive after expiration
                              to INACTIVE
  -l, --list                   show account aging information
  -m, --mindays MIN_DAYS      set minimum number of days before password
                              change to MIN_DAYS
  -M, --maxdays MAX_DAYS     set maximum number of days before password
                              change to MAX_DAYS
  -R, --root CHROOT_DIR       directory to chroot into
  -W, --warndays WARN_DAYS    set expiration warning days to WARN_DAYS

[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:35:56) ] -> sudo chage -m 5 -M 90 -I 2 -W 5 tempuser 2 ↵ —(Thu,May16)
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:36:15) ] -> sudo chage -l tempuser —(Thu,May16)
Last password change                : May 16, 2024
Password expires                     : Aug 14, 2024
Password inactive                    : Aug 16, 2024
Account expires                      : Jul 31, 2025
Minimum number of days between password change : 5
Maximum number of days between password change : 90
Number of days of warning before password expires : 5
[ (/etc/security) ] (admin@localhost:pts/0)
[ (03:36:35) ] -> [ ] —(Thu,May16)
```