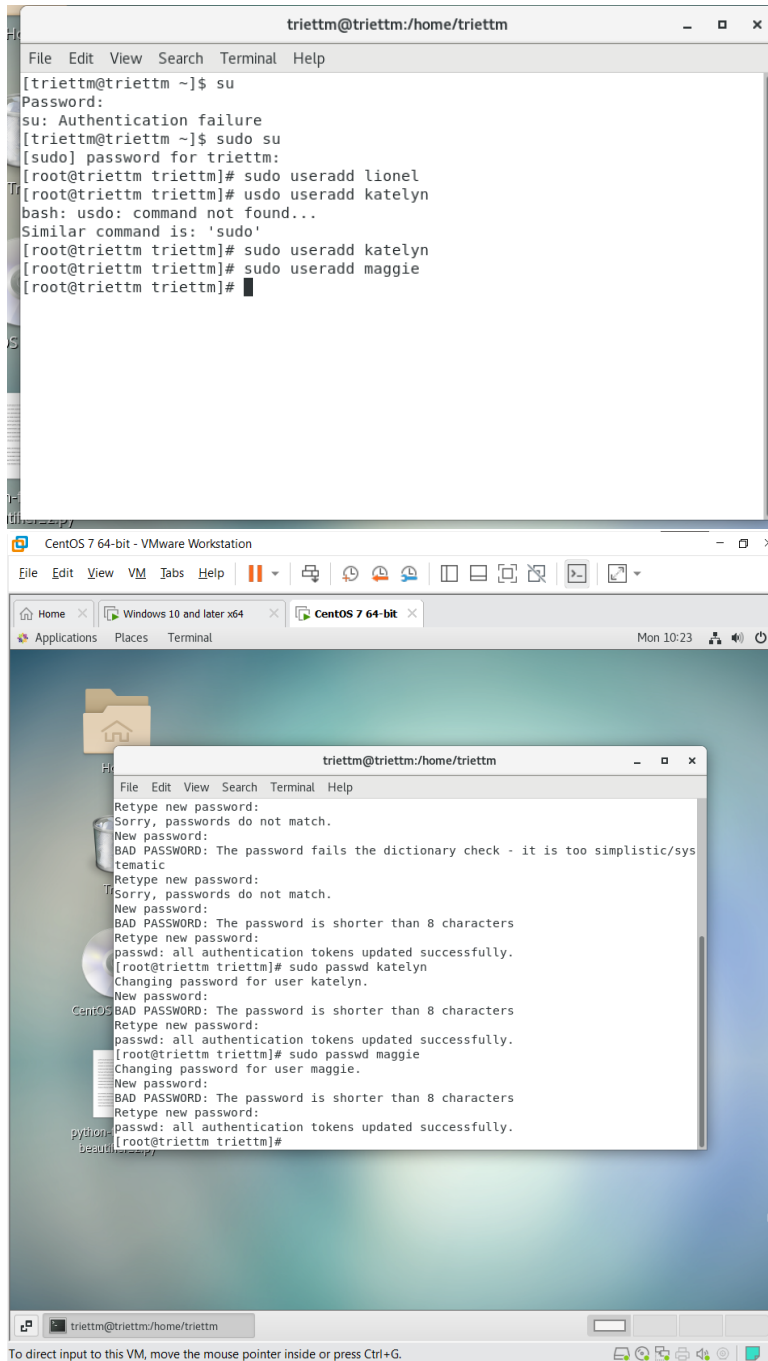


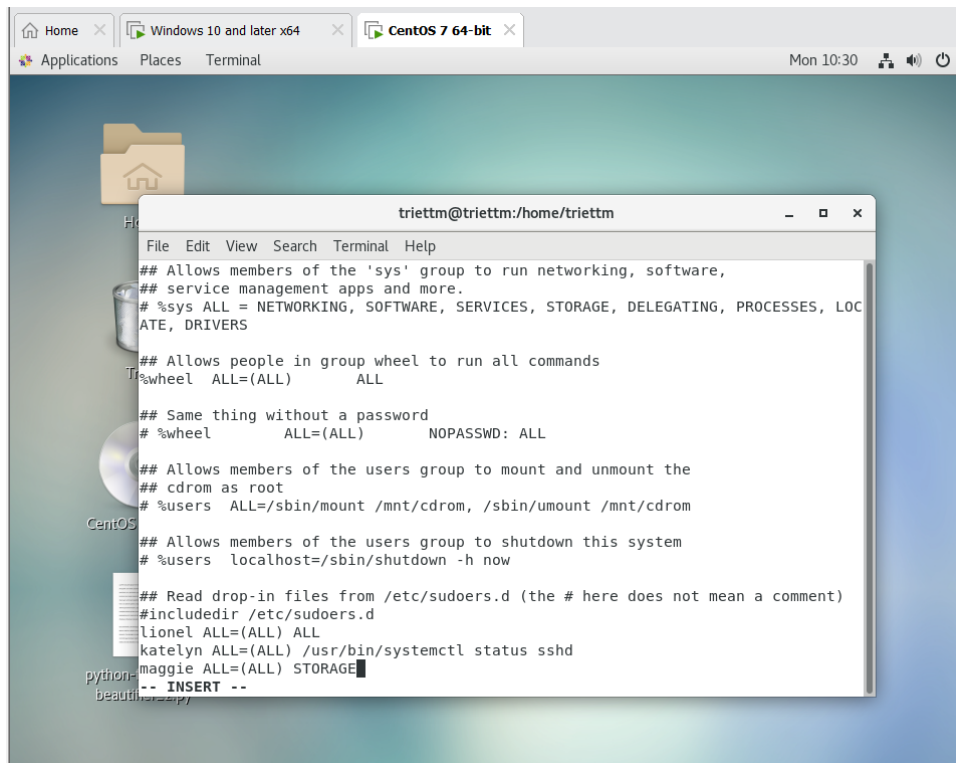
Name: Trần Minh Triết

MSSV: SE172241

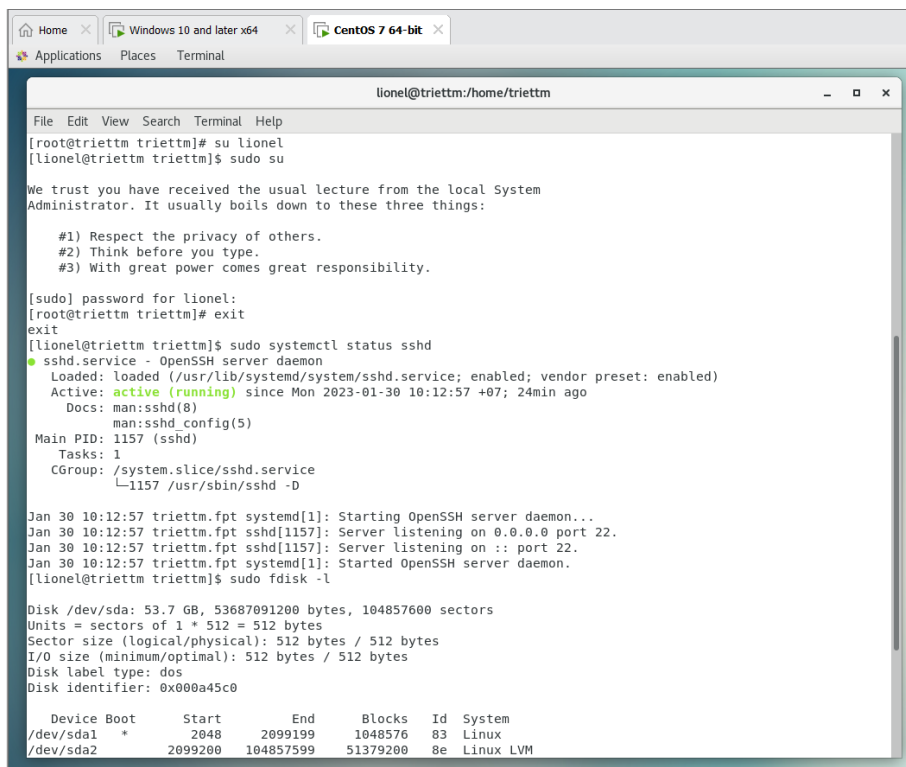
Hands-on lab for assigning limited sudo Privileges



Create three users lionel, katelyn, Maggie.

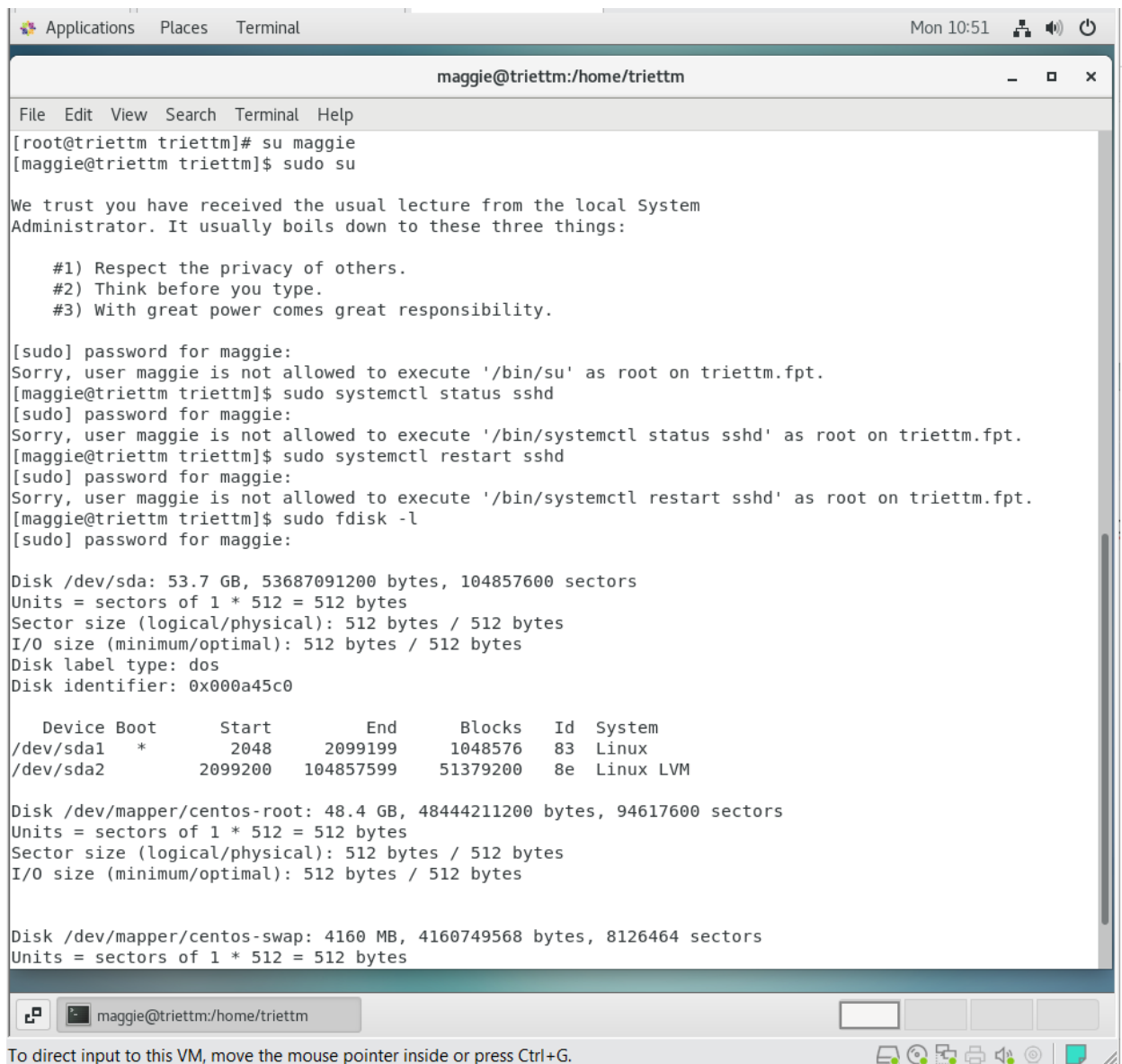


Config some privilege for three users that include: Lionel have all permission; katelyn can only access to systemctl status sshd; Maggie can only access to STORAGE like details about RAM, disk drive.



Lionel have all the privilege.

Katelyn user can only execute the command “systemctl status sshd” as well as can not execute any others privilege commands.



```
maggie@triettm:/home/triettm
File Edit View Search Terminal Help
[root@triettm triettm]# su maggie
[maggie@triettm triettm]$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for maggie:
Sorry, user maggie is not allowed to execute '/bin/su' as root on triettm.fpt.
[maggie@triettm triettm]$ sudo systemctl status sshd
[sudo] password for maggie:
Sorry, user maggie is not allowed to execute '/bin/systemctl status sshd' as root on triettm.fpt.
[maggie@triettm triettm]$ sudo systemctl restart sshd
[sudo] password for maggie:
Sorry, user maggie is not allowed to execute '/bin/systemctl restart sshd' as root on triettm.fpt.
[maggie@triettm triettm]$ sudo fdisk -l
[sudo] password for maggie:

Disk /dev/sda: 53.7 GB, 53687091200 bytes, 104857600 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: 0x000a45c0

   Device Boot      Start         End      Blocks    Id  System
/dev/sda1  *        2048     2099199     1048576    83  Linux
/dev/sda2             2099200    104857599     51379200    8e  Linux LVM

Disk /dev/mapper/centos-root: 48.4 GB, 48444211200 bytes, 94617600 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: 4160 MB, 4160749568 bytes, 8126464 sectors
Units = sectors of 1 * 512 = 512 bytes
```

Maggie user can only execute command “fdisk” to view details about disk.

Các config này được áp dụng khi này ta config vào file visudo nhằm phân quyền truy cập một cách vừa đủ cho các user.

Hands-on lab for disabling the sudo timer

```
Home x Windows 10 and later x64 x CentOS 7 64-bit x
Applications Places Terminal Mon 10:59

triettm@triettm:/home/triettm
File Edit View Search Terminal Help

[root@triettm triettm]# sudo fdisk -l

Disk /dev/sda: 53.7 GB, 53687091200 bytes, 104857600 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: 0x000a45c0

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *          2048       2099199       1048576   83   Linux
/dev/sda2             2099200     104857599       51379200   8e   Linux LVM

Disk /dev/mapper/centos-root: 48.4 GB, 48444211200 bytes, 94617600 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: 4160 MB, 4160749568 bytes, 8126464 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

[root@triettm triettm]# sudo systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-01-30 10:12:57 +07; 46min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 1157 (sshd)
     Tasks: 1
    CGroup: /system.slice/ssh.service
            └─1157 /usr/sbin/sshd -D

Jan 30 10:12:57 triettm.fpt systemd[1]: Starting OpenSSH server daemon...
Jan 30 10:12:57 triettm.fpt sshd[1157]: Server listening on 0.0.0.0 port 22.
Jan 30 10:12:57 triettm.fpt sshd[1157]: Server listening on :: port 22.
Jan 30 10:12:57 triettm.fpt systemd[1]: Started OpenSSH server daemon.
[root@triettm triettm]#
```

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

HomeWindows 10 and later x64CentOS 7 64-bit

ApplicationsPlacesTerminal

Mon 11:11

triettm@triettm:~

FileEditViewSearchTerminalHelp

```
[sudo] password for triettm:
visudo: /etc/sudoers.tmp unchanged
[triettm@triettm ~]$ clear

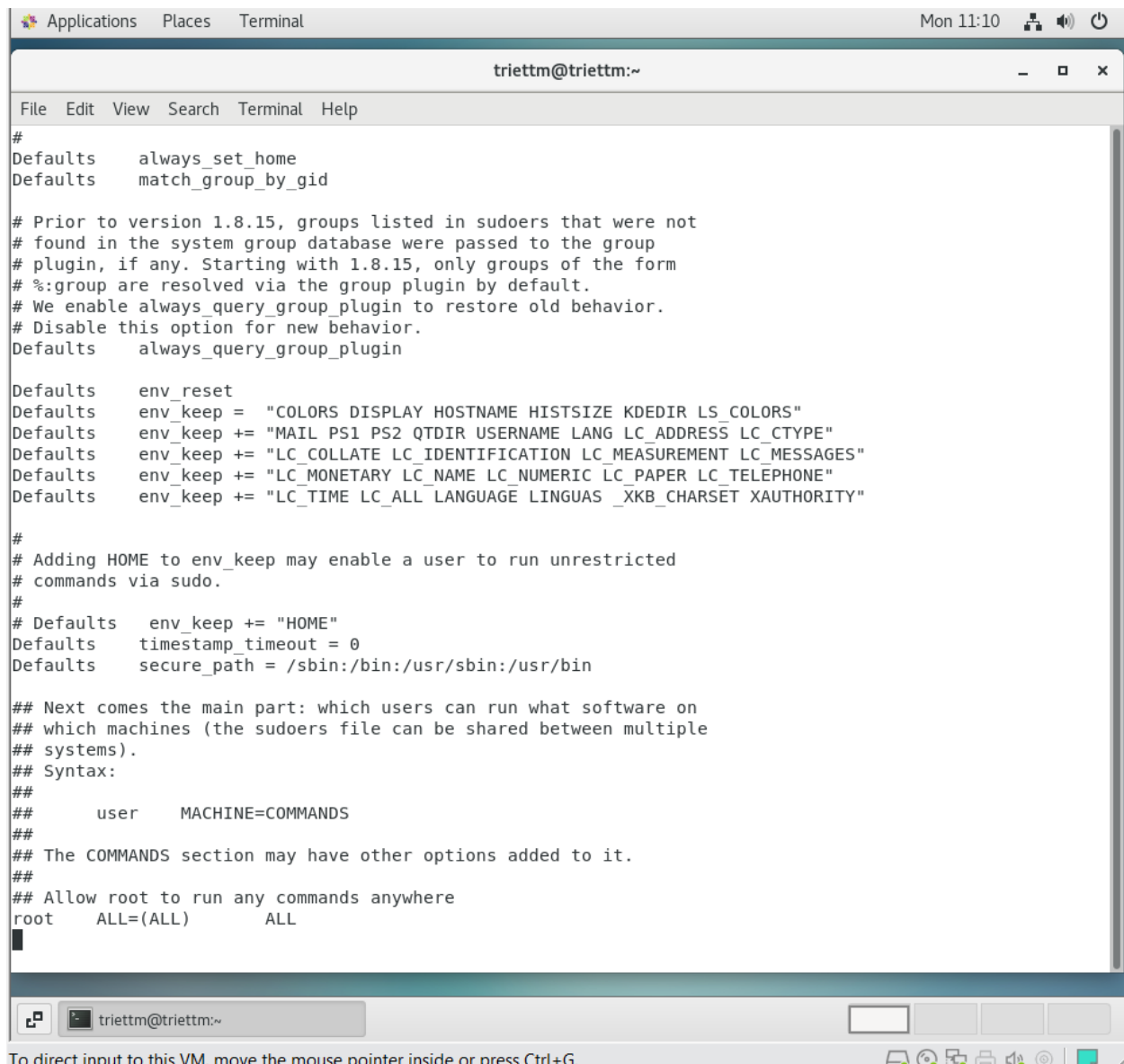
[triettm@triettm ~]$ sudo systemctl status sshd
[sudo] password for triettm:
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-01-30 10:12:57 +07; 57min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 1157 (sshd)
    Tasks: 1
   CGroup: /system.slice/sshd.service
           └─1157 /usr/sbin/sshd -D

Jan 30 10:12:57 triettm.fpt systemd[1]: Starting OpenSSH server daemon...
Jan 30 10:12:57 triettm.fpt sshd[1157]: Server listening on 0.0.0.0 port 22.
Jan 30 10:12:57 triettm.fpt sshd[1157]: Server listening on :: port 22.
Jan 30 10:12:57 triettm.fpt systemd[1]: Started OpenSSH server daemon.
[triettm@triettm ~]$ sudo iptables -L
[sudo] password for triettm:
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     ctstate RELATED,ESTABLISHED
ACCEPT     all  --  192.168.122.0/24       anywhere
```

triettm@triettm:~

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



```
#
Defaults    always_set_home
Defaults    match_group_by_gid

# Prior to version 1.8.15, groups listed in sudoers that were not
# found in the system group database were passed to the group
# plugin, if any. Starting with 1.8.15, only groups of the form
# %:group are resolved via the group plugin by default.
# We enable always_query_group_plugin to restore old behavior.
# Disable this option for new behavior.
Defaults    always_query_group_plugin

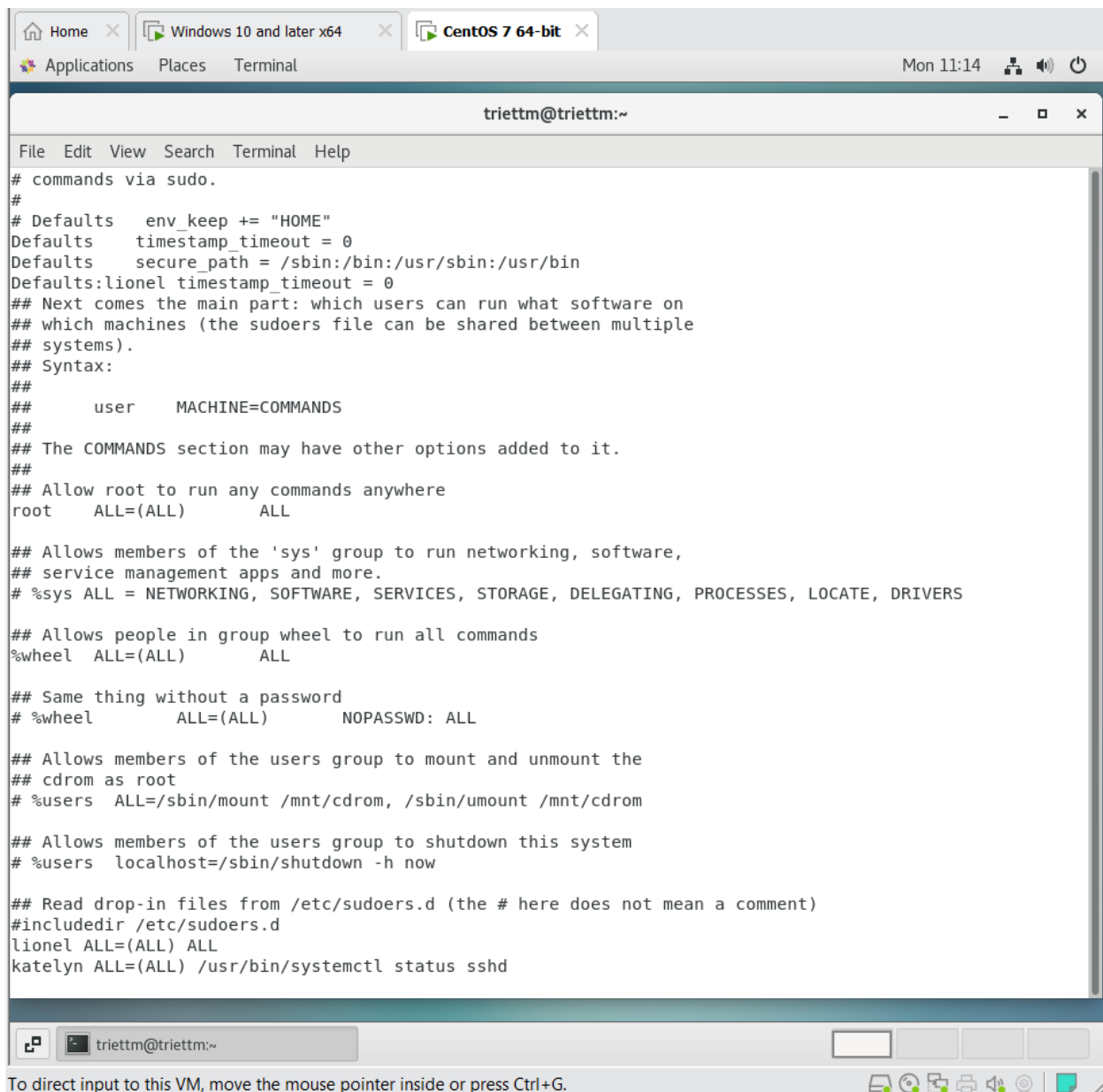
Defaults    env_reset
Defaults    env_keep = "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"

#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults    env_keep += "HOME"
Defaults    timestamp_timeout = 0
Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)    ALL
```

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

This time, you should see that you have to enter a password every time.



The image shows a Windows 10 virtual machine window titled 'CentOS 7 64-bit'. The terminal window is open, displaying the contents of the /etc/sudoers file. The file defines user permissions for root, the 'sys' group, the 'wheel' group, and the 'users' group. It includes comments explaining the syntax and the purpose of each section. The terminal prompt is 'triettm@triettm:~'.

```
# commands via sudo.
#
# Defaults    env_keep += "HOME"
Defaults     timestamp_timeout = 0
Defaults     secure_path = /sbin:/bin:/usr/sbin:/usr/bin
Defaults:lionel timestamp_timeout = 0
## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)        ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, 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
## cdrom as root
# %users    ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users    localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#include_dir /etc/sudoers.d
lionel ALL=(ALL) ALL
katelyn ALL=(ALL) /usr/bin/systemctl status sshd
```

At the bottom of the window, a status bar reads: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

```
Applications  Places  Terminal  Mon 11:15  [Icons] [Power]

lionel@triettm:/home/triettm

File Edit View Search Terminal Help

[triettm@triettm ~]$ su lionel
Password:
[lionel@triettm triettm]$ sudo fdisk -l
[sudo] password for lionel:

Disk /dev/sda: 53.7 GB, 53687091200 bytes, 104857600 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: 0x000a45c0

   Device Boot      Start         End      Blocks    Id  System
/dev/sda1  *        2048      2099199       1048576    83   Linux
/dev/sda2            2099200    104857599       51379200    8e   Linux LVM

Disk /dev/mapper/centos-root: 48.4 GB, 48444211200 bytes, 94617600 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: 4160 MB, 4160749568 bytes, 8126464 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

[lionel@triettm triettm]$ sudo systemctl status sshd
[sudo] password for lionel:
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-01-30 10:12:57 +07; 1h 2min ago
     Docs: man:ssh(8)
           man:ssh_config(5)
   Main PID: 1157 (sshd)
     Tasks: 1
    CGroup: /system.slice/ssh.service
            └─1157 /usr/sbin/sshd -D

Jan 30 10:12:57 triettm.fpt systemd[1]: Starting OpenSSH server daemon...
```

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

```

[lionel@triettm triettm]$ sudo iptables -L
[sudo] password for lionel:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            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

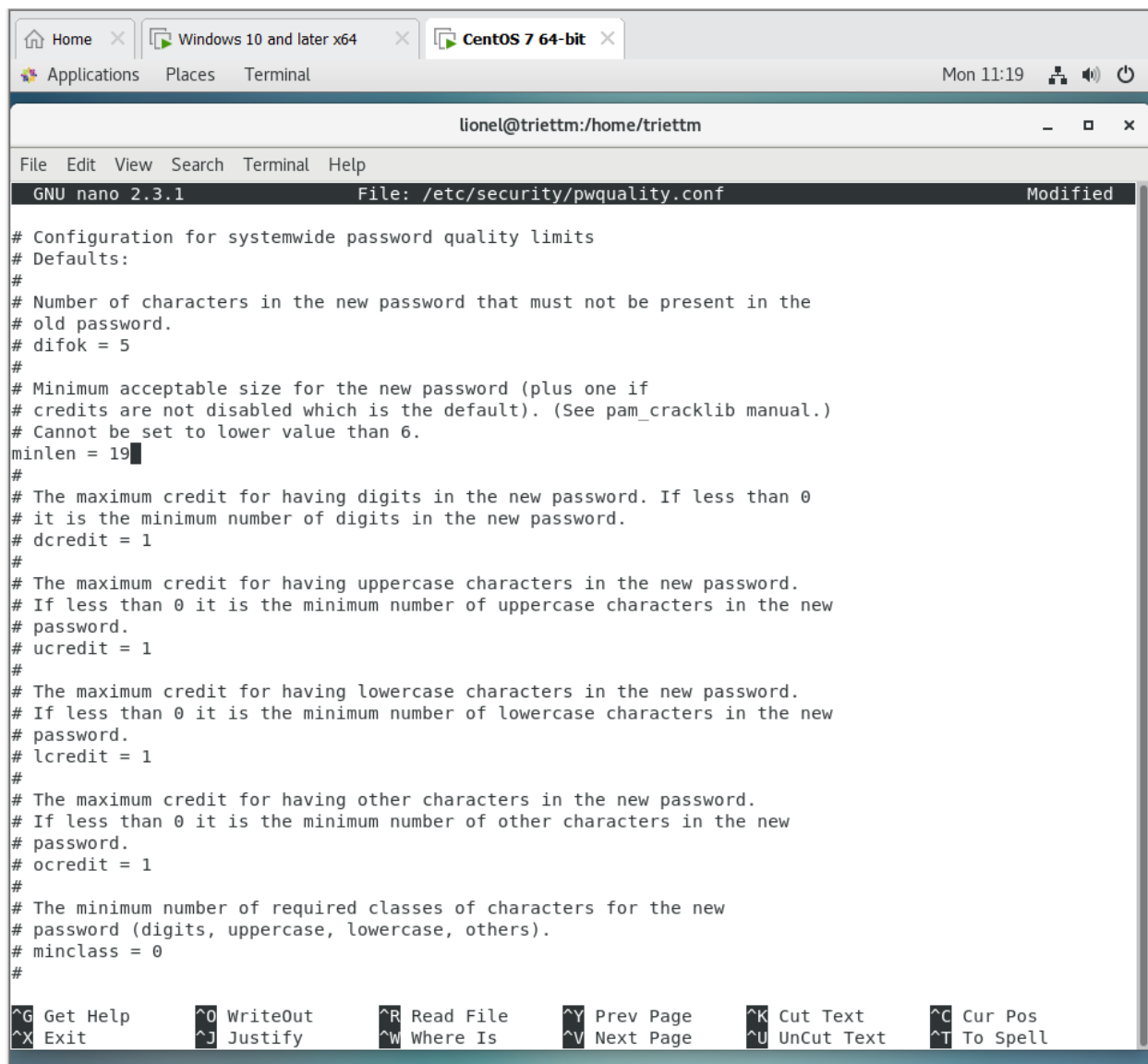
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination            ctstate RELATED,ESTABLISHED
ACCEPT     all  -- anywhere             192.168.122.0/24
ACCEPT     all  -- 192.168.122.0/24      anywhere
ACCEPT     all  -- anywhere             anywhere
REJECT     all  -- anywhere             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
FORWARD_IN_ZONES_SOURCE all -- anywhere             anywhere
FORWARD_IN_ZONES all -- anywhere             anywhere
FORWARD_OUT_ZONES_SOURCE all -- anywhere             anywhere
FORWARD_OUT_ZONES all -- anywhere             anywhere
DROP       all  -- anywhere             anywhere              ctstate INVALID
REJECT     all  -- anywhere             anywhere              reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination            udp dpt:bootpc
ACCEPT     udp  -- anywhere             anywhere

```

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

Hands-on lab for setting password complexity criteria



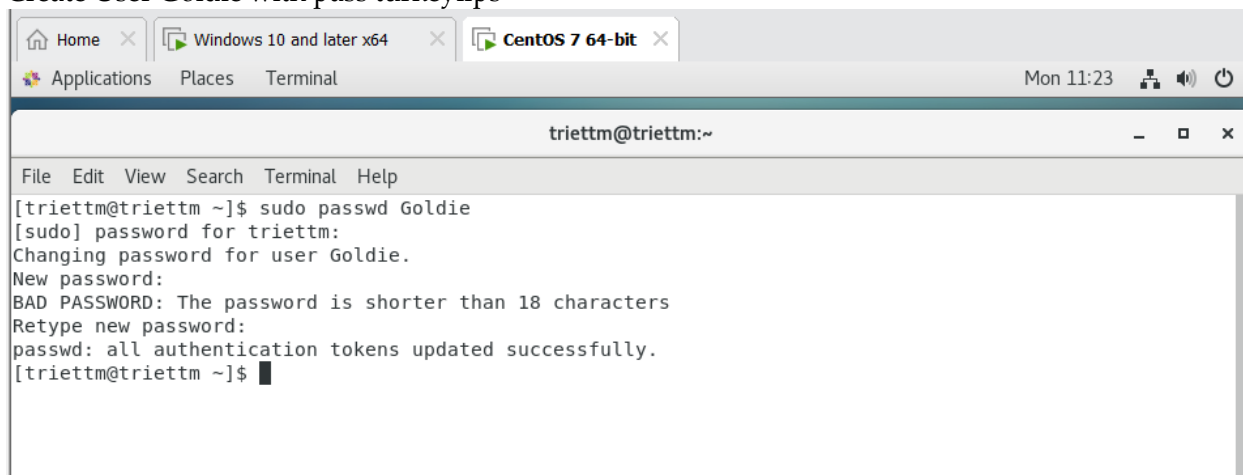
The screenshot shows a terminal window with a nano text editor open, editing the file `/etc/security/pwquality.conf`. The terminal title bar indicates the user is `lionel@triettm` in the directory `/home/triettm`. The nano editor's status bar shows `GNU nano 2.3.1` and `File: /etc/security/pwquality.conf`. The file content is a configuration for systemwide password quality limits, with comments and values for `minlen`, `dcredit`, `ucrcedit`, `lcredit`, `ocredit`, and `minclass`. The bottom of the nano editor shows a row of keyboard shortcuts: `^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`, and `^T To Spell`.

```
lionel@triettm:/home/triettm
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/security/pwquality.conf Modified

# 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.
# 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 = 0
#

^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
```

Create User Goldie with pass turkeylips



The screenshot shows a terminal window with the prompt `triettm@triettm:~`. The user has entered the command `sudo passwd Goldie`. The output shows the password for `triettm` is being changed to `Goldie`. The user is prompted for a new password, but the password is rejected because it is shorter than 18 characters. The user is then prompted to retype the new password, and the password is successfully updated. The terminal shows the final prompt `[triettm@triettm ~]$`.

```
triettm@triettm:~
File Edit View Search Terminal Help

[triettm@triettm ~]$ sudo passwd Goldie
[sudo] password for triettm:
Changing password for user Goldie.
New password:
BAD PASSWORD: The password is shorter than 18 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[triettm@triettm ~]$
```

With password: Turkeylips

```
[triettm@triettm ~]$ sudo passwd Goldie
[sudo] password for triettm:
Sorry, try again.
[sudo] password for triettm:
Changing password for user Goldie.
New password:
BAD PASSWORD: The password is shorter than 17 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[triettm@triettm ~]$ █
```

With password: Turkey93Lips

```
[triettm@triettm ~]$ sudo passwd Goldie
[sudo] password for triettm:
Changing password for user Goldie.
New password:
BAD PASSWORD: The password is shorter than 16 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[triettm@triettm ~]$ █
```

Now let's config others policy for password. Minclass define that the password have at least 3 class uppercase, lowercase or number. Maxrepeatclass define the maximum number of repetition of each class in the password.

```
triettm@triettm:~
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/security/pwquality.conf Modified

# 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 = 0
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.
# The check is disabled if the value is 0.
maxclassrepeat = 5
#
# Whether to check for the words from the passwd entry GECOS string of the user.
# The check is enabled if the value is not 0.
# gecheck = 0
#
# Path to the cracklib dictionaries. Default is to use the cracklib default.
# dictpath =

^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

triettm@triettm:~
```

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

Let's check out others password for Goldie.

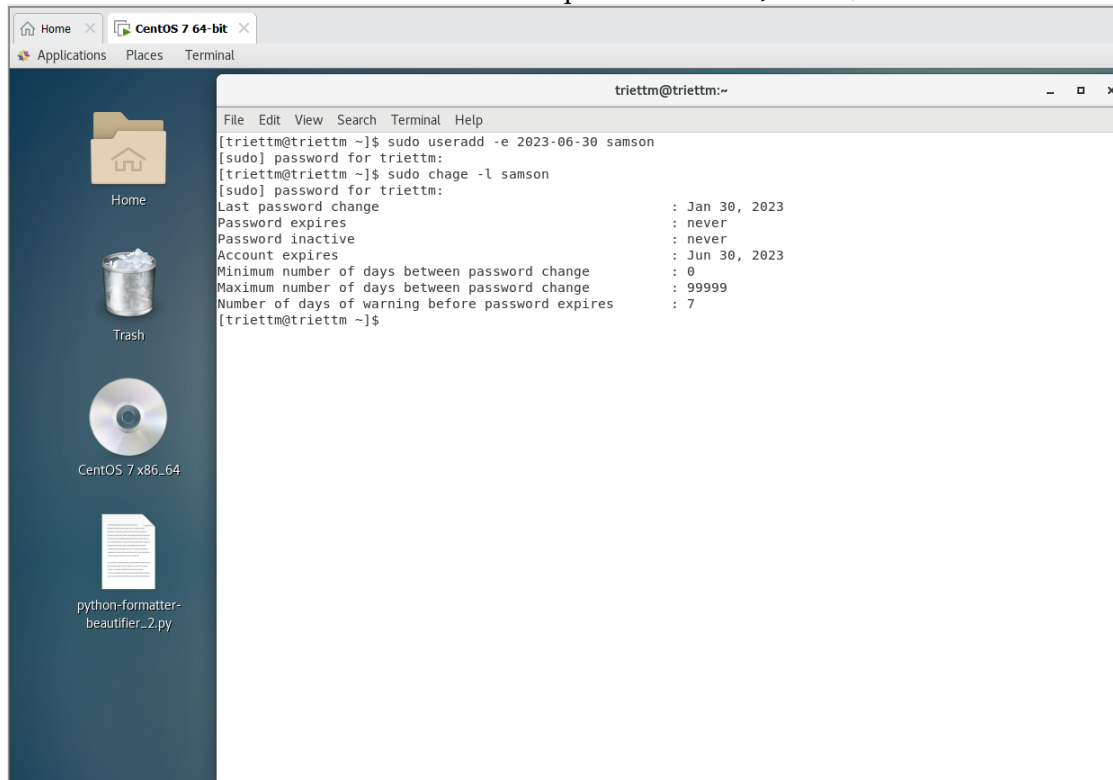
```
[triettm@triettm ~]$ sudo passwd Goldie
[sudo] password for triettm:
Sorry, try again.
[sudo] password for triettm:
Changing password for user Goldie.
New password:
BAD PASSWORD: The password contains more than 5 characters of the same class consecutively
Retype new password:
passwd: all authentication tokens updated successfully.
[triettm@triettm ~]$
```

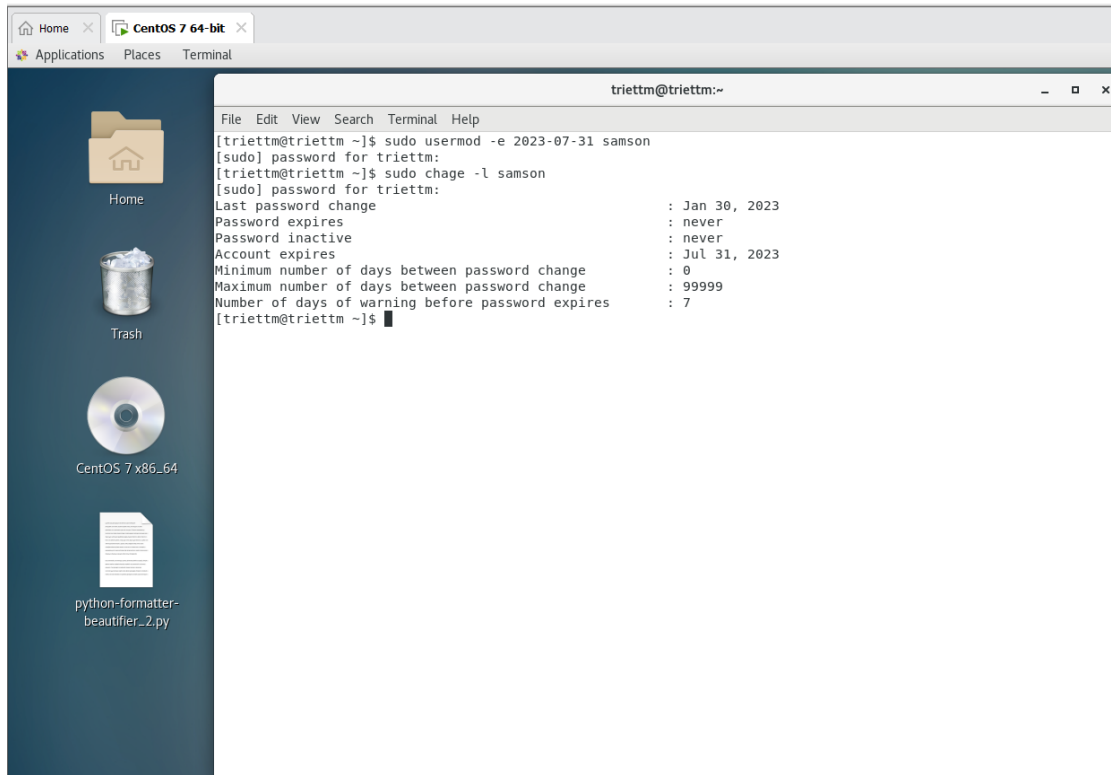
```
[triettm@triettm ~]$ sudo passwd Goldie
[sudo] password for triettm:
Changing password for user Goldie.
New password:
BAD PASSWORD: The password is shorter than 7 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[triettm@triettm ~]$
```



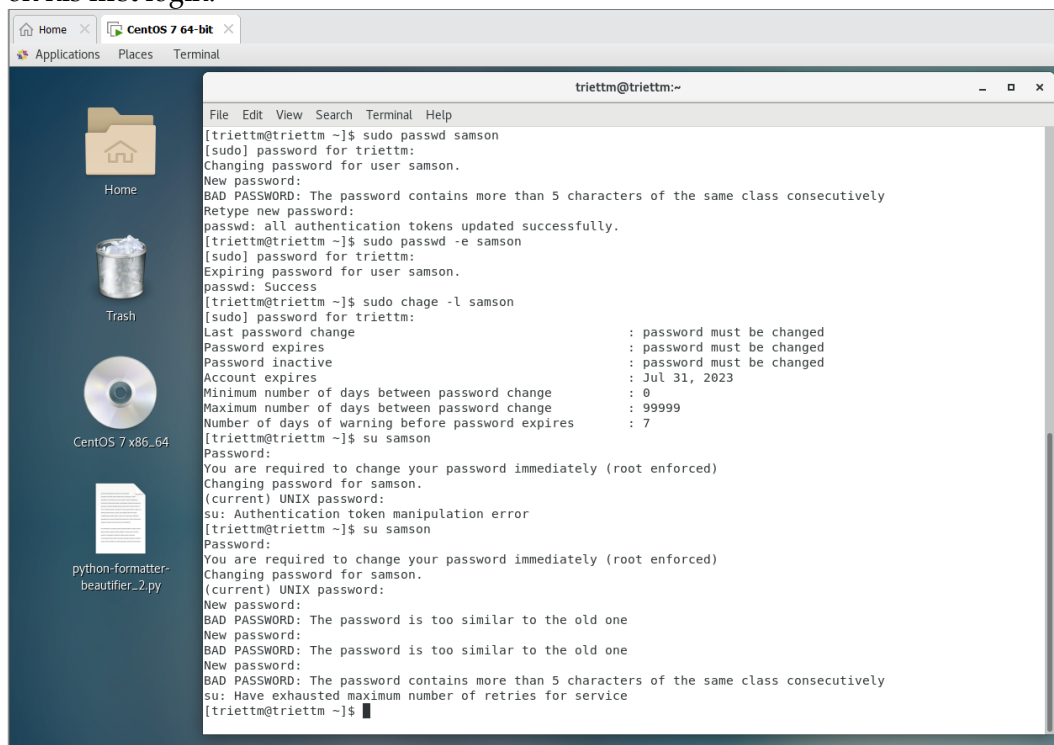
Hands-on lab for setting account and password expiry Data

Create a user account for Samson with the expiration date of June 30, 2023





Assign a password to Samson's account, then force him to change his password on his first login.



```
CentOS 7 64-bit
Applications Places Terminal

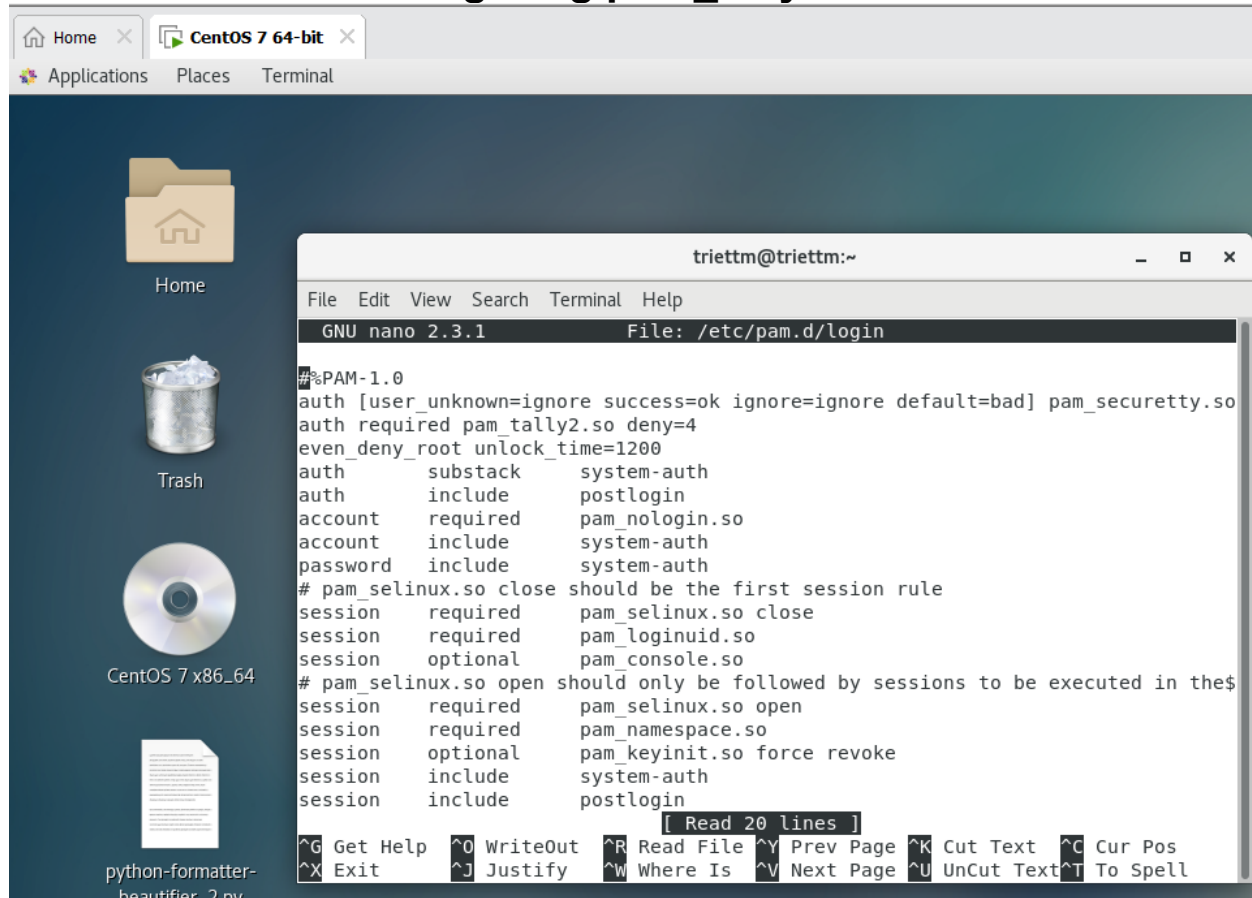
Home
Trash
CentOS 7 x86_64
python-formatter-beautifier_2.py

samson@triettm:/home/triettm
File Edit View Search Terminal Help

[triettm@triettm ~]$ su samson
Password:
You are required to change your password immediately (root enforced)
Changing password for samson.
(current) UNIX password:
New password:
BAD PASSWORD: The password contains more than 5 characters of the same class consecutively
New password:
BAD PASSWORD: The password contains more than 5 characters of the same class consecutively
New password:
Retype new password:
Sorry, passwords do not match.
su: Have exhausted maximum number of retries for service
[triettm@triettm ~]$ su samson
Password:
You are required to change your password immediately (root enforced)
Changing password for samson.
(current) UNIX password:
New password:
Retype new password:
[samson@triettm triettm]$

[triettm@triettm ~]$ sudo chage -m 5 -M 90 -I 2 -W 5 samson
[sudo] password for triettm:
[triettm@triettm ~]$ sudo chage -l samson
[sudo] password for triettm:
Last password change          : Jan 30, 2023
Password expires              : Apr 30, 2023
Password inactive             : May 02, 2023
Account expires               : Jul 31, 2023
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
[triettm@triettm ~]$
```

Hands-on lab for configuring pam_tally2



```
triettm@triettm:~  
File Edit View Search Terminal Help  
[triettm@triettm ~]$ sudo pam_tally2 --user=samson --reset  
[sudo] password for triettm:  
Login          Failures Latest failure    From  
samson          0  
[triettm@triettm ~]$
```