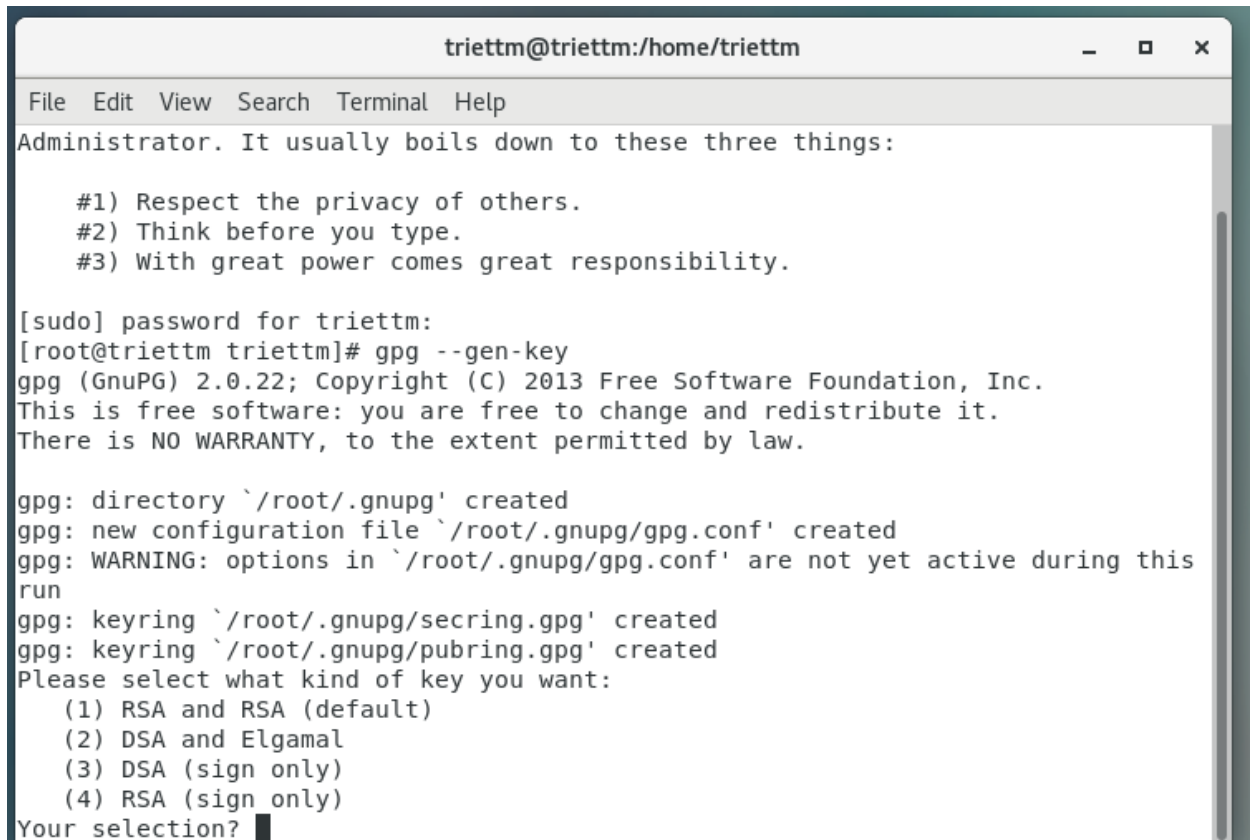


Tên: Trần Minh Triết

MSSV: SE172241

## Hands-on lab – combining gpg and tar for encrypted backups



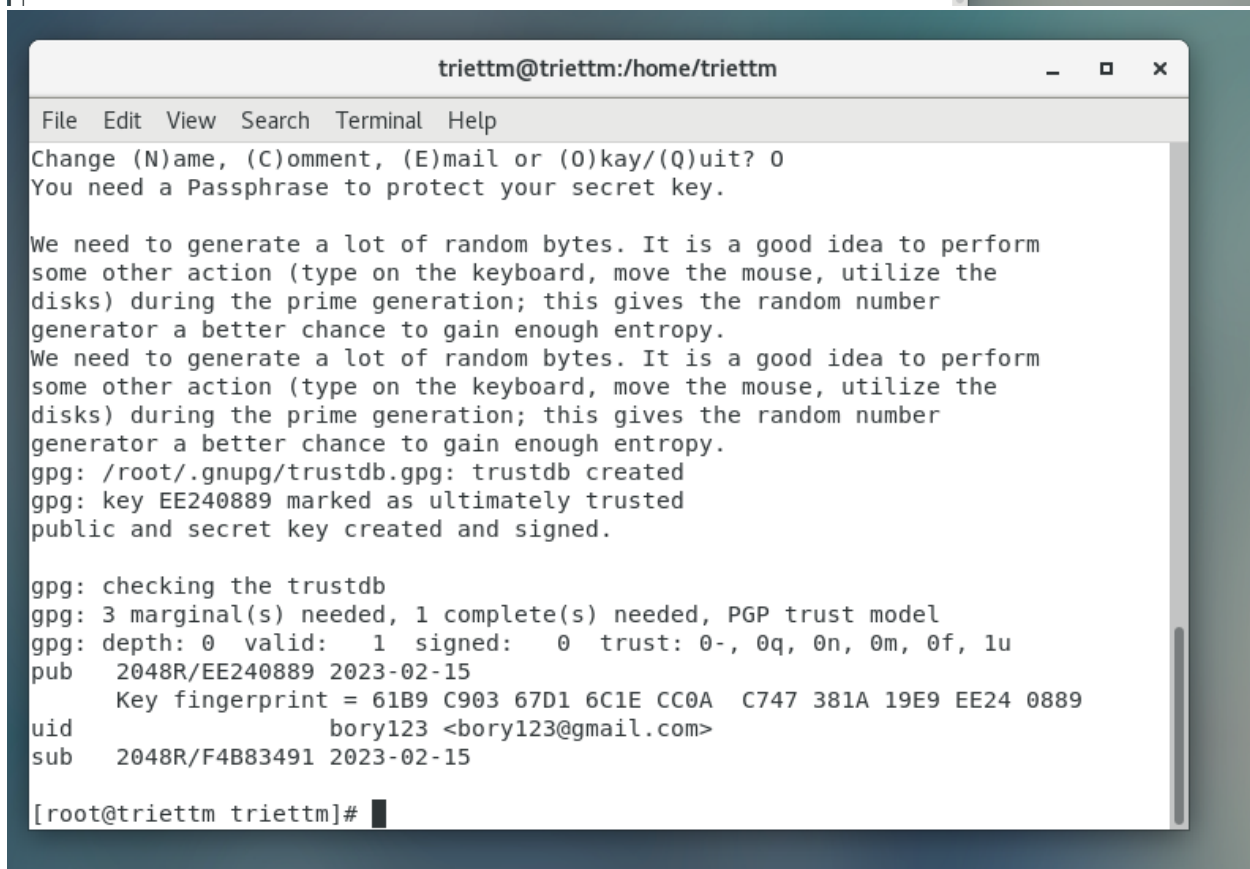
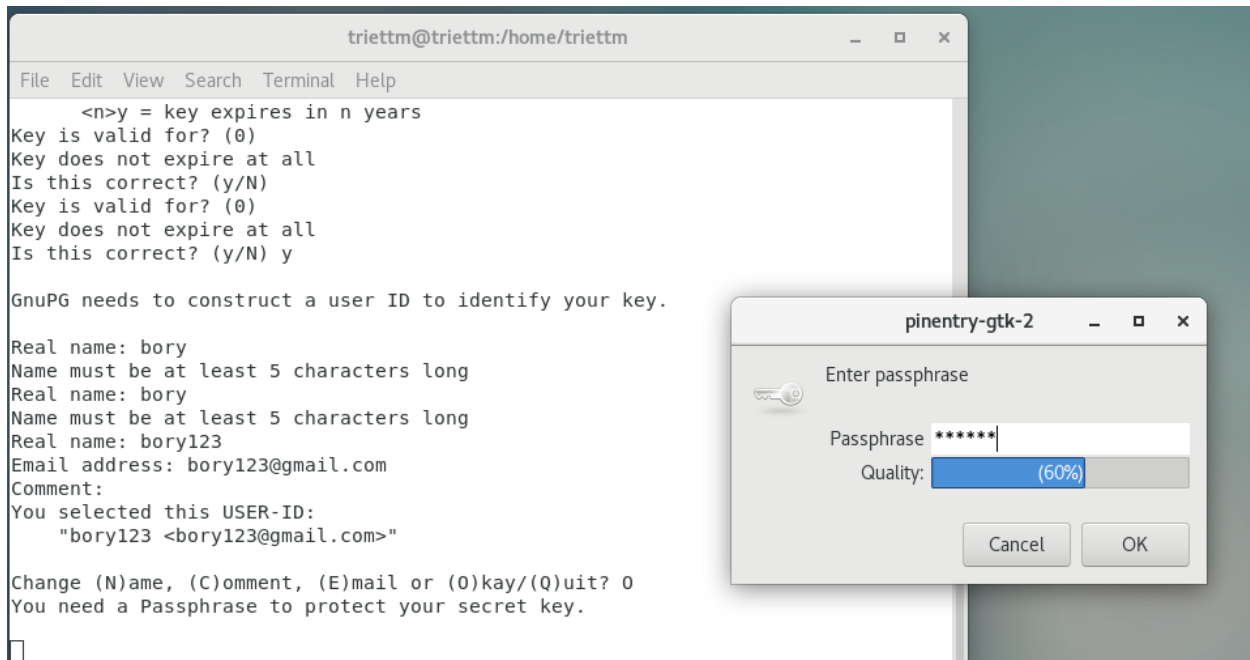
```
triettm@triettm:/home/triettm
File Edit View Search Terminal Help
Administrator. It usually boils down to these three things:

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

[sudo] password for triettm:
[root@triettm triettm]# gpg --gen-key
gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory `/root/.gnupg' created
gpg: new configuration file `/root/.gnupg/gpg.conf' created
gpg: WARNING: options in `/root/.gnupg/gpg.conf' are not yet active during this
run
gpg: keyring `/root/.gnupg/secring.gpg' created
gpg: keyring `/root/.gnupg/pubring.gpg' created
Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? █
```

Sử dụng câu lệnh `gpg --gen-key` để sinh ra key gpg để mã hóa file backup



```
[root@triettm triettm]# touch {file1.txt,file2.txt,file3.txt,file4.txt}
[root@triettm triettm]# ls
Desktop    Downloads  file2.txt  file4.txt  Pictures  Templates
Documents  file1.txt  file3.txt  Music      Public    Videos
[root@triettm triettm]#
```

Tạo ra 4 file mẫu để demo backup file

```
[root@triettm triettm]# sudo mkdir /backup
[root@triettm triettm]# sudo chown triettm: /backup
[root@triettm triettm]# sudo chmod 700 /backup
[root@triettm triettm]#
```

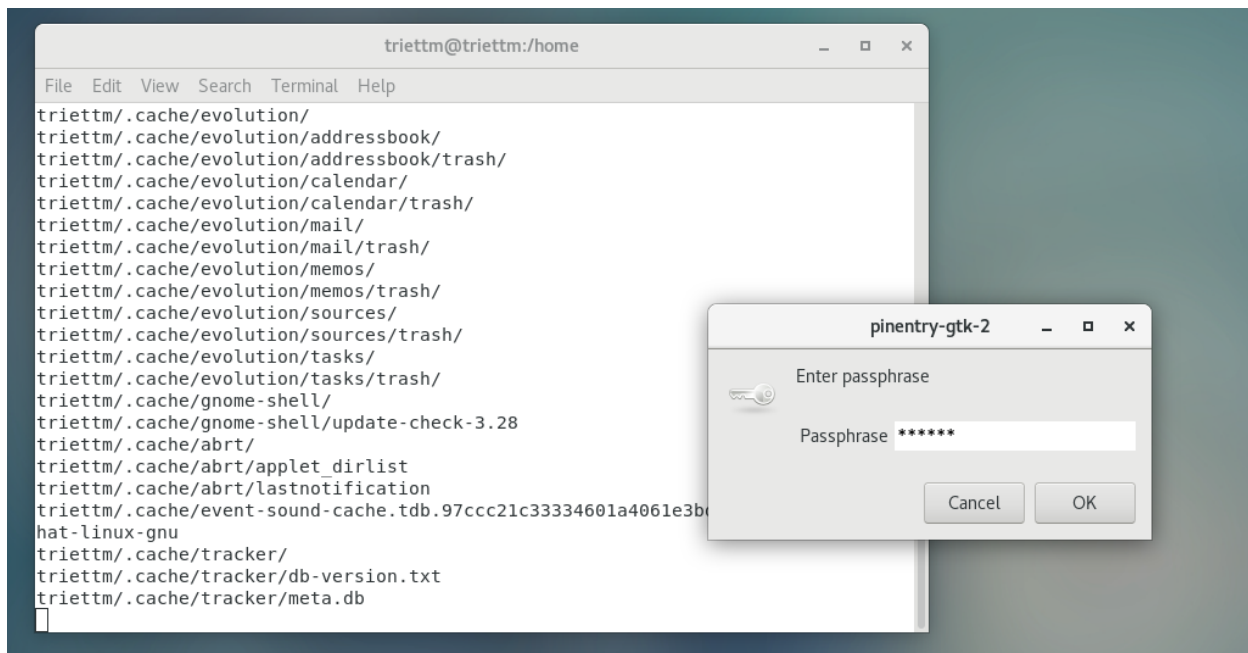
```

triettm@triettm:/home/triettm
File Edit View Search Terminal Help
[root@triettm triettm]# clear

[root@triettm triettm]# ls / -la
total 24
dr-xr-xr-x. 18 root    root    238 Feb 15 20:45 .
dr-xr-xr-x. 18 root    root    238 Feb 15 20:45 ..
drwx-----. 2 triettm triettm   6 Feb 15 20:45 backup
lrwxrwxrwx. 1 root    root      7 Jan  5 11:19 bin -> usr/bin
dr-xr-xr-x.  5 root    root   4096 Jan  5 11:27 boot
drwxr-xr-x. 20 root    root  3320 Jan  5 11:27 dev
drwxr-xr-x.145 root    root  8192 Jan  5 11:27 etc
drwxr-xr-x.  3 root    root    21 Jan  5 11:26 home
lrwxrwxrwx. 1 root    root      7 Jan  5 11:19 lib -> usr/lib
lrwxrwxrwx. 1 root    root      9 Jan  5 11:19 lib64 -> usr/lib64

```

Tạo folder backup ở root rồi đổi userowner thành triettm để chỉ một mình mình có thể access vào file này nhằm thực hiện backup các file và folder của user triettm.



```
triettm@triectm:/backup
```

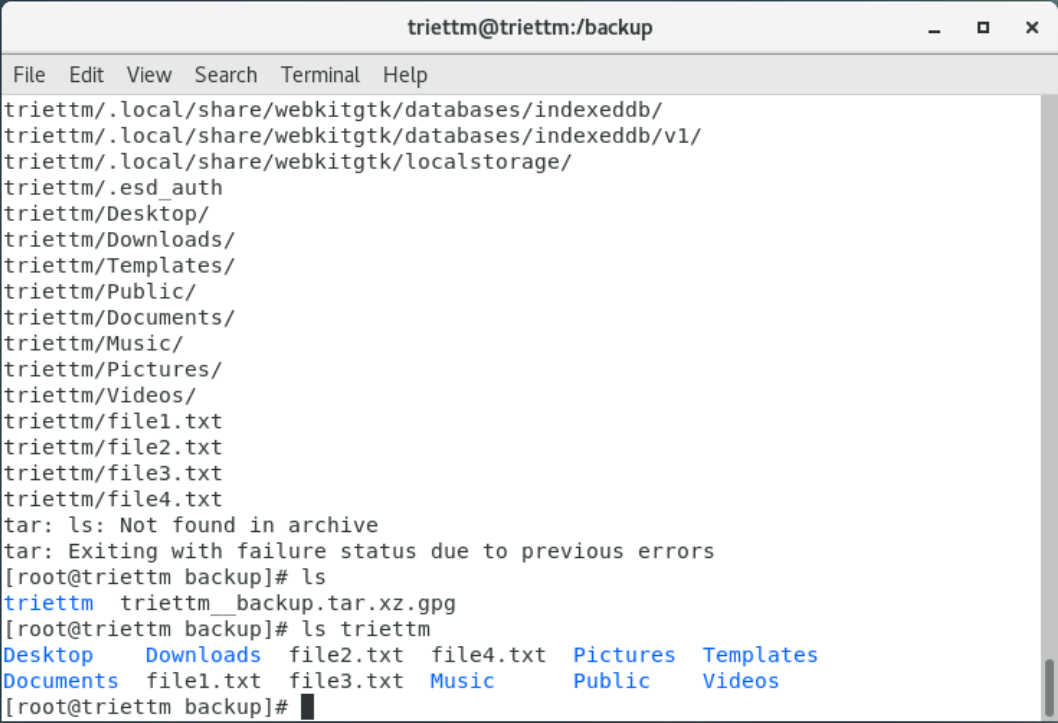
- □ ×

File Edit View Search Terminal Help

```
[root@triectm backup]# ls  
triectm__backup.tar.xz.gpg  
[root@triectm backup]# cat triectm_backup.tar.xz.gpg | head
```

G000,i00Q[00U0F000TJZ(0B0000C 0!0SGv0z7!0-00  
000C0PI0t0\$:0r0pr006K0R+000x0k\_.\$^dI:0R0J000}=kgN000n00i?00\_0MSe000,.0  
0000M060:cN0n0Q\* 0  
0! 800AXi03`8000000-^0n000ydF0 W0  
gil0IQ)0w0U000ö0vl0w000000]9)eA00000N006BL<00000H0um000009ku200#RK000W0b0  
000is\$00000D00  
000&Vv00R0y00xpX0G0H0m000+000S00f!0L0 &00'0Ph000T0:0?-0π00b0]00+-~0-  
0?Q000dj00k+0U03rq000uHa0V00000\So0l"000000700~0#\u0000  
  
 kEO)  
?  
c000D\*/r00B0TE"N-000s0?00R0K4xk 30R:\$j7b0Ip00  
m00000b0=NO0000340706000QV00000U0GN000  
%US000TE0+w)000 0800UOMo000"\$000G0 . w00x-500я0CE`(5200  
\$U0IG000R`)0005P0020,q0000\*0P0E00dIN0\$60P6U00EE00~å0f0q0500000F009=!0f5n  
q000Q/0000|qġ拐0!S0020:e000000E00008000,"3|Q0m070p0/0000I't0oÖrToe  
ed0h00V\_0Iq0`100:0Yg>003p>  
'Ek7,\*0200q>d000000"0Ueo;. \_00p.Uo+00\*-00)\000-O000L0  
  
 MHO  
]|0000S0

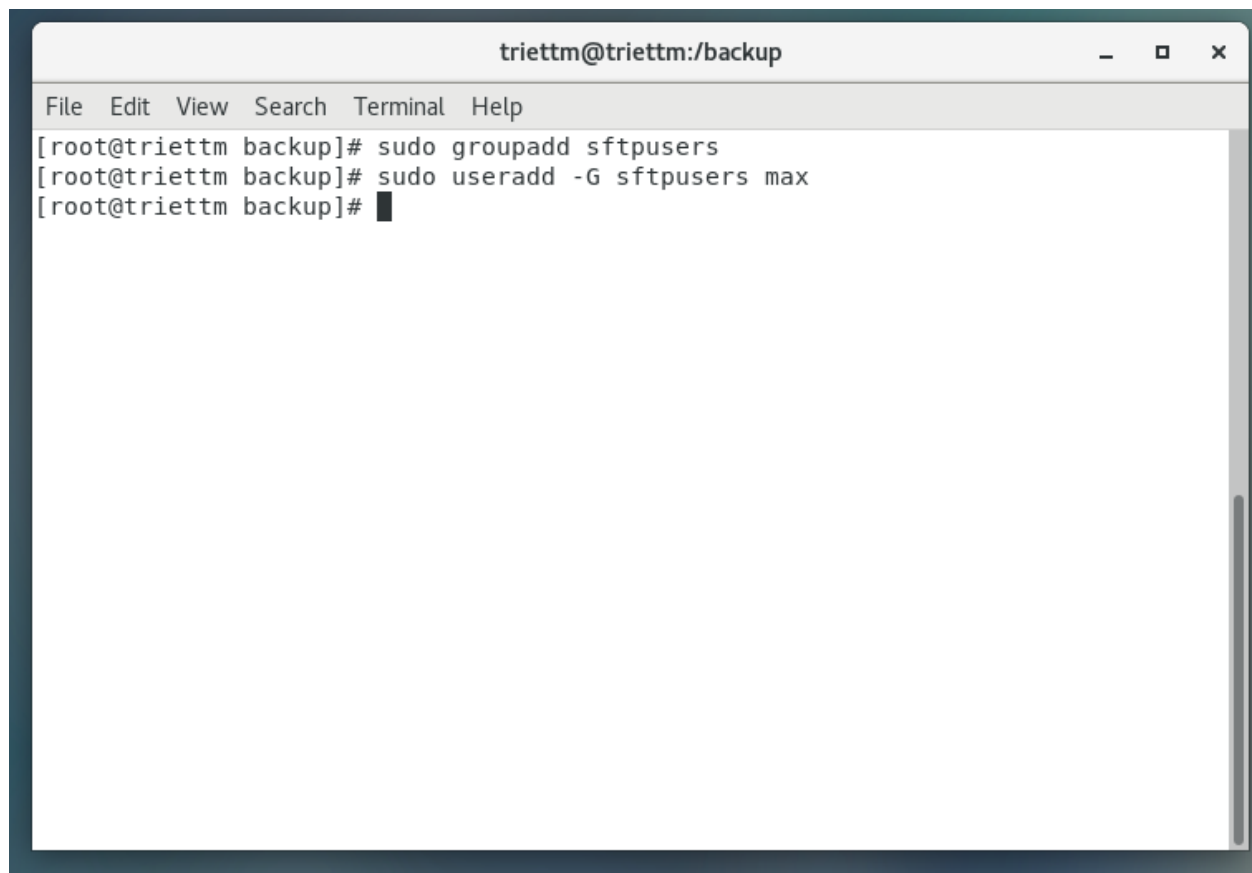
```
triettm@triettm:/backup
File Edit View Search Terminal Help
triettm/.local/share/nautilus/scripts/
triettm/.local/share/webkitgtk/
triettm/.local/share/webkitgtk/deviceidhashsalts/
triettm/.local/share/webkitgtk/deviceidhashsalts/1/
triettm/.local/share/webkitgtk/databases/
triettm/.local/share/webkitgtk/databases/indexeddb/
triettm/.local/share/webkitgtk/databases/indexeddb/v1/
triettm/.local/share/webkitgtk/localstorage/
triettm/.esd_auth
triettm/Desktop/
triettm/Downloads/
triettm/Templates/
triettm/Public/
triettm/Documents/
triettm/Music/
triettm/Pictures/
triettm/Videos/
triettm/file1.txt
triettm/file2.txt
triettm/file3.txt
triettm/file4.txt
tar: ls: Not found in archive
tar: Exiting with failure status due to previous errors
[root@triettm backup]#
```



```
triettm@triettm:/backup
File Edit View Search Terminal Help
triettm/.local/share/webkitgtk/databases/indexeddb/
triettm/.local/share/webkitgtk/databases/indexeddb/v1/
triettm/.local/share/webkitgtk/localstorage/
triettm/.esd_auth
triettm/Desktop/
triettm/Downloads/
triettm/Templates/
triettm/Public/
triettm/Documents/
triettm/Music/
triettm/Pictures/
triettm/Videos/
triettm/file1.txt
triettm/file2.txt
triettm/file3.txt
triettm/file4.txt
tar: ls: Not found in archive
tar: Exiting with failure status due to previous errors
[root@triettm backup]# ls
triettm  triettm_backup.tar.xz.gpg
[root@triettm backup]# ls triettm
Desktop  Downloads  file2.txt  file4.txt  Pictures  Templates
Documents  file1.txt  file3.txt  Music      Public     Videos
[root@triettm backup]#
```

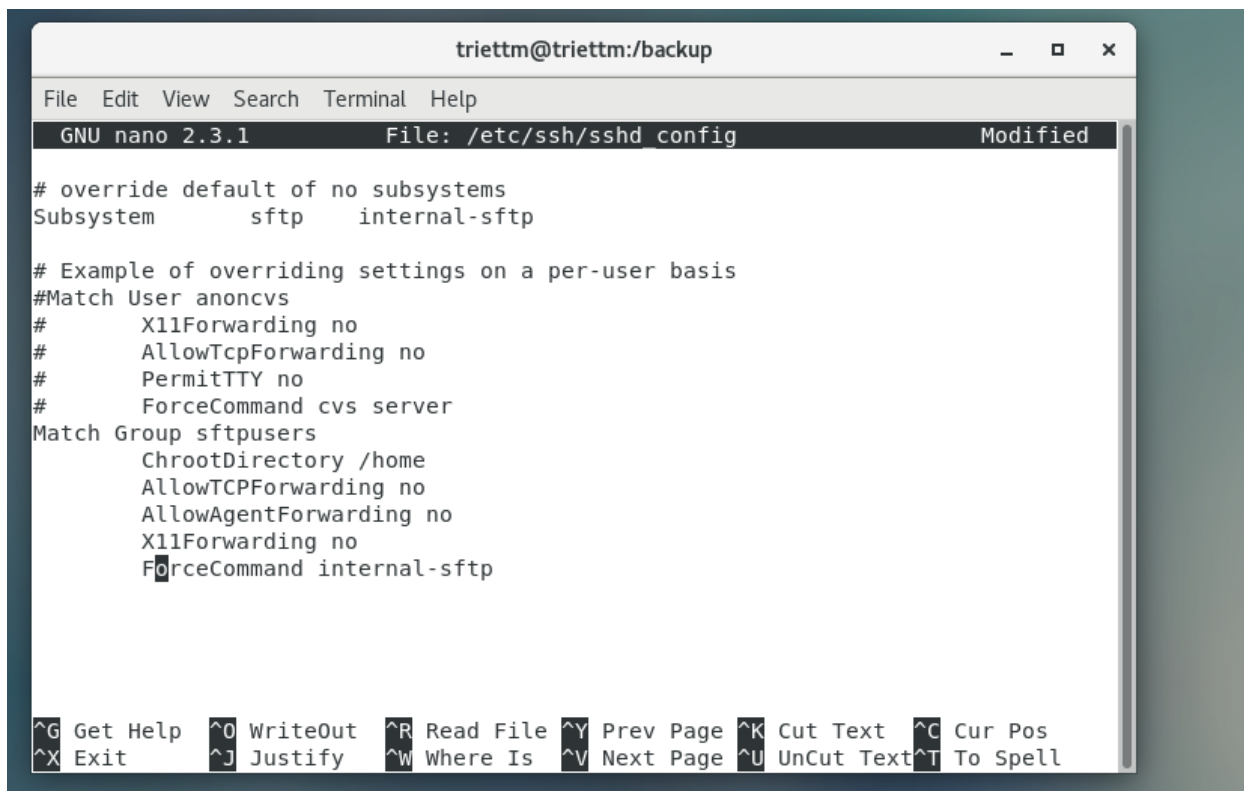
Ta đã tiến hành giải mã thành công

## Hands-on lab – setting up a chroot directory for sftpusers group

A terminal window titled 'triettm@triettm:/backup' with standard window controls. The terminal shows three commands being executed in sequence: 'sudo groupadd sftpusers', 'sudo useradd -G sftpusers max', and a final prompt. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'.

```
triettm@triettm:/backup
File Edit View Search Terminal Help
[root@triettm backup]# sudo groupadd sftpusers
[root@triettm backup]# sudo useradd -G sftpusers max
[root@triettm backup]#
```

Tạo group user mới và thêm user max vào group đó để tiến hành demo.



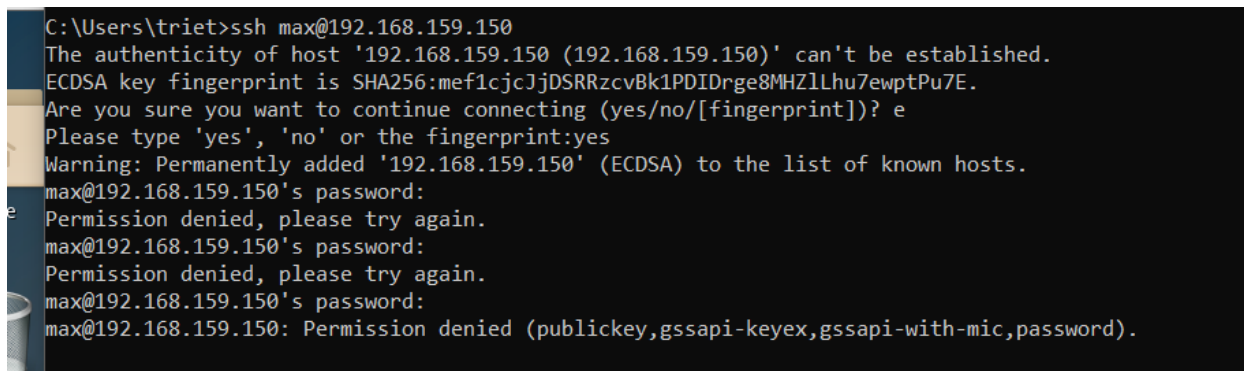
```
triettm@triettm:/backup
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/ssh/sshd_config Modified

# override default of no subsystems
Subsystem          sftp    internal-sftp

# Example of overriding settings on a per-user basis
#Match User anoncvs
#      X11Forwarding no
#      AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server
Match Group sftputers
      ChrootDirectory /home
      AllowTCPForwarding no
      AllowAgentForwarding no
      X11Forwarding no
      ForceCommand internal-sftp

^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
```

Dùng nano để chỉnh sửa file config /etc/ssh/sshd\_config để thiết lập không cho user kết nối bằng ssh nữa mà bằng sftp thôi. Chi tiết chỉnh sửa xem hình trên.



```
C:\Users\triet>ssh max@192.168.159.150
The authenticity of host '192.168.159.150 (192.168.159.150)' can't be established.
ECDSA key fingerprint is SHA256:mef1cjcJjDSRRzcvBk1PDIDrge8MHZlLhu7ewptPu7E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? e
Please type 'yes', 'no' or the fingerprint:yes
Warning: Permanently added '192.168.159.150' (ECDSA) to the list of known hosts.
max@192.168.159.150's password:
Permission denied, please try again.
max@192.168.159.150's password:
Permission denied, please try again.
max@192.168.159.150's password:
max@192.168.159.150: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```