

LAB 04

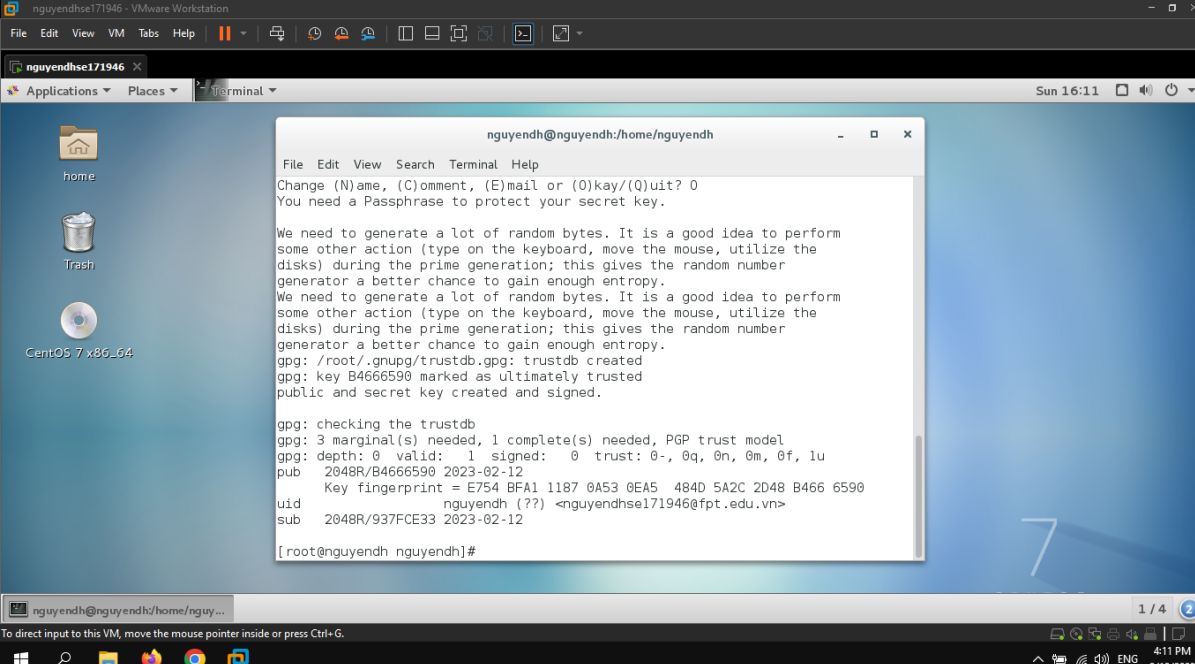
Thầy Mai Hoàng Đình
Trường đại học FPT

Người thực hiện

Đặng Hoàng Nguyên

HANDS-ON LAB - COMBINING GPG AND TAR FOR ENCRYPTED BACKUPS

Tạo **key gpg** với tên user là **nguyendh** bằng câu lệnh **gpg --gen-key**

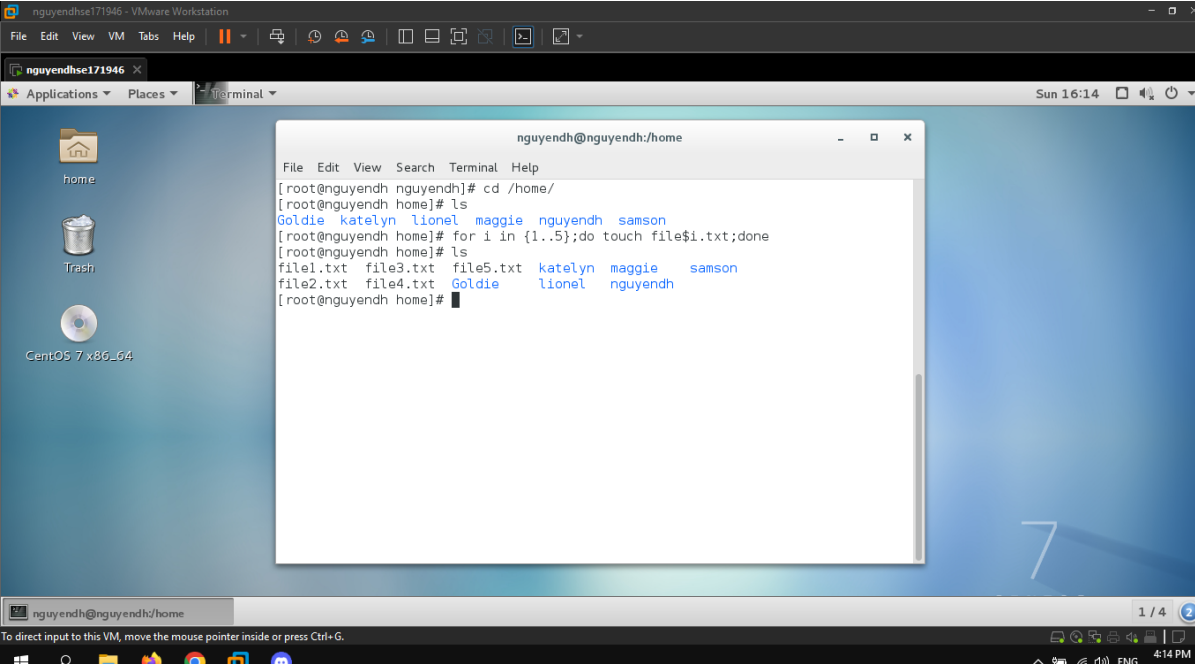


```
nguyendh@nguyendh:/home/nguyendh
File Edit View Search Terminal Help
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? 0
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key B4666590 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
pub 2048R/B4666590 2023-02-12
Key fingerprint = E754 BFA1 1187 0A53 0EA5 484D 5A2C 2D48 B466 6590
uid nguyendh (??) <nguyendhse171946@fpt.edu.vn>
sub 2048R/937FCE33 2023-02-12
[root@nguyendh nguyendh]#
```

Tạo 5 file txt trong thư mục **directory**. Cho chạy vòng **for** từ 1 tới 5, tạo 5 file txt lần lượt **file1 file2 file3 file4 file5**



```
nguyendh@nguyendh:/home
File Edit View Search Terminal Help
[root@nguyendh nguyendh]# cd /home/
[root@nguyendh home]# ls
Goldie katelyn lionel maggie nguyendh samson
[root@nguyendh home]# for i in {1..5};do touch file$i.txt;done
[root@nguyendh home]# ls
file1.txt file3.txt file5.txt katelyn maggie samson
file2.txt file4.txt Goldie lionel nguyendh
[root@nguyendh home]#
```

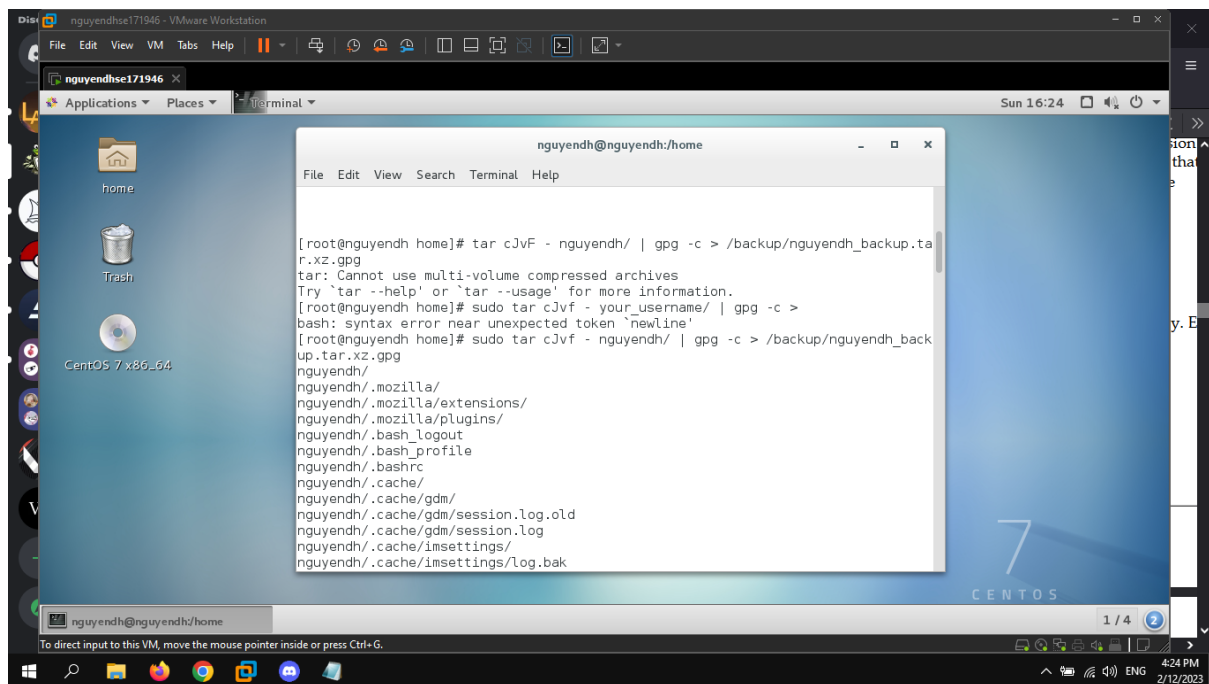
Tạo một file backup tại thư mục **root** với người dùng có thể mở là **nguyendh** cùng với toàn lệnh thực hiện đối với user **nguyendh**

```

[root@nguyendh home]# mkdir /backup
[root@nguyendh home]# chown nguyendh: /backup/
[root@nguyendh home]# chmod 700 /backup/
[root@nguyendh home]# ls
file1.txt  file3.txt  file5.txt  katelyn  maggie    samson
file2.txt  file4.txt  Goldie     lionel   nguyendh
[root@nguyendh home]# ls -la /
total 32
dr-xr-xr-x. 18 root      root      288 Feb 12 16:18 .
dr-xr-xr-x. 18 root      root      288 Feb 12 16:18 ..
-rw-r--r--.  1 root      root         0 Jan  5 05:06 1
-rw-r--r--.  1 root      root         0 Jan 11 09:07 .autorelabel
drwx-----  2 nguyendh  nguyendh    6 Feb 12 16:18 backup

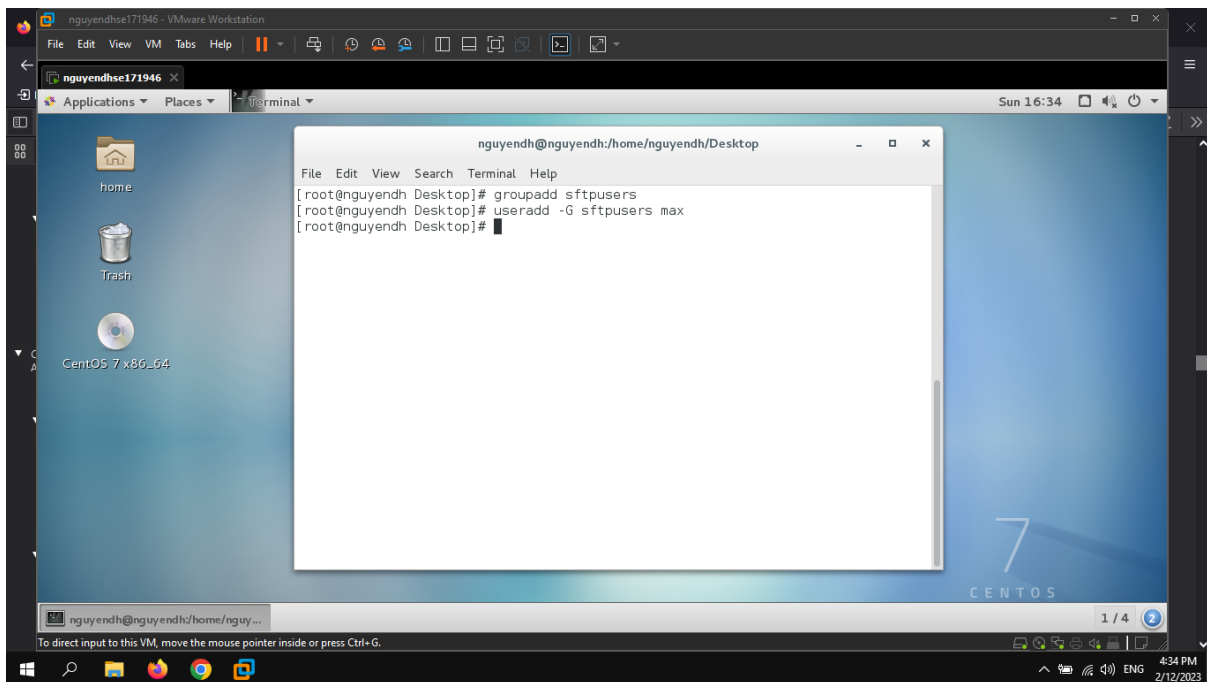
```

Tại thư mục home, ta tạo ra một file backup với câu lệnh **tar cJvF** để nén dữ liệu, sau đó dùng câu lệnh **gpg -c** để encrypt nó vào /backup với tên gọi mới là nguyendh_backup.tar.xz.gpg.



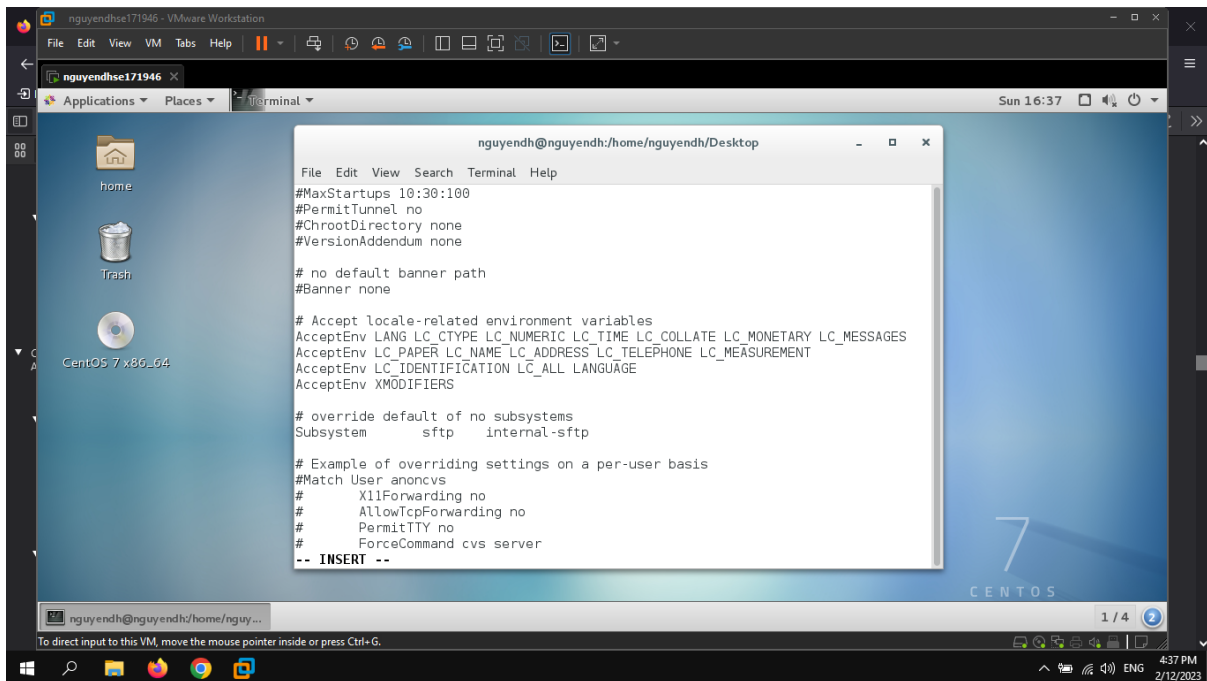
Cat thử để xem đã mã hóa chưa ?

HANDS-ON: SETTING UP A CHROOT DIRECTORY FOR SFTPUERS GROUP

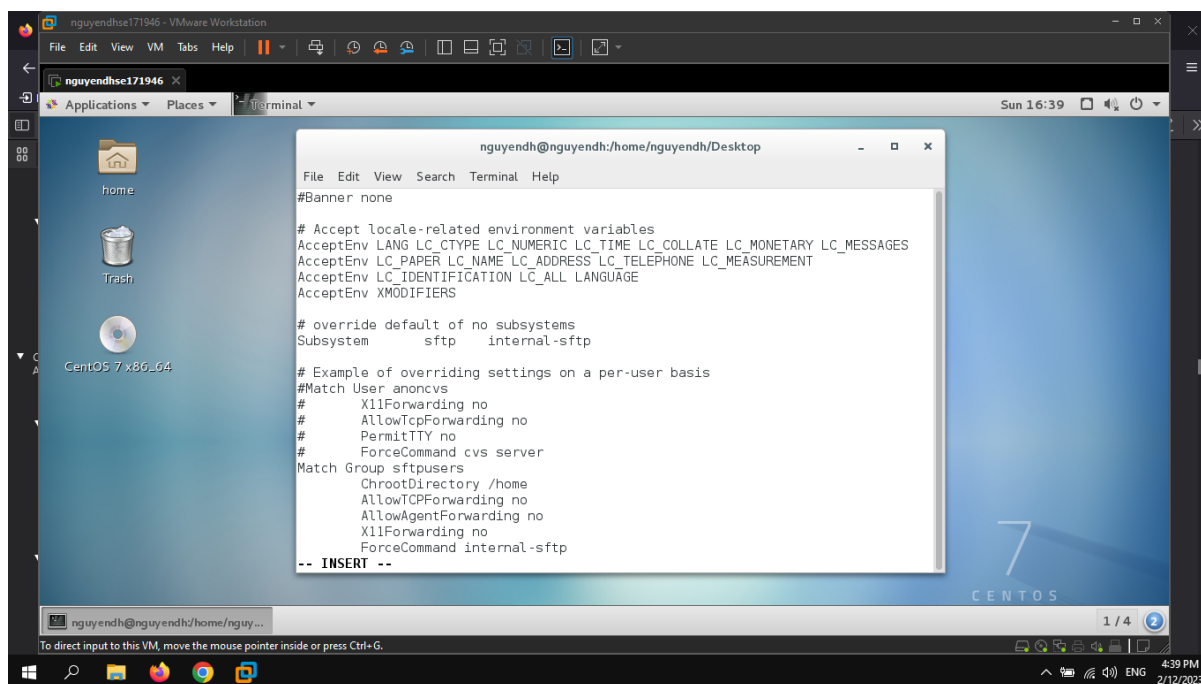


Sử dụng câu lệnh **groupadd + tên nhóm** để tạo ra nhóm trong Centos

Sau đó add người dùng tên max và group sftputers thông qua câu lệnh **useradd -G**



Sử dụng **vi** hoặc **nano** để truy cập vào file `/etc/ssh/sshd_config` và chỉnh Subsystem sftp internal-sftp như hình



Các câu lệnh này được thêm vào để configure cho sftpuser:

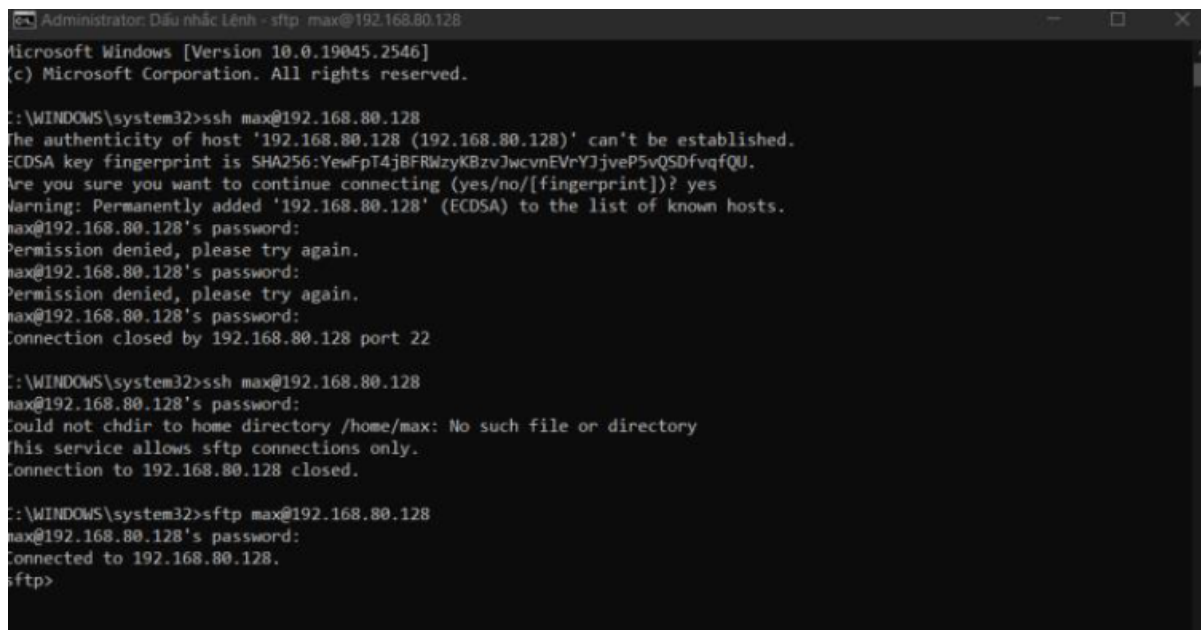
ChrootDirectory: Người dùng sẽ bị khóa trong thư mục `"/home"` và sẽ không thể truy cập bất kỳ thư mục nào khác ngoài thư mục này.

AllowTCPForwarding: Người dùng không được phép sử dụng chuyển tiếp TCP, đây là tính năng cho phép máy khách chuyển tiếp lưu lượng từ cổng này sang cổng khác.

AllowAgentForwarding:, đây là tính năng cho phép sử dụng quy trình ssh-agent đang chạy để giữ khóa riêng.

X11Forwarding: Người dùng không được phép sử dụng X11Forwarding, đây là tính năng cho phép máy khách chuyển tiếp lưu lượng X11 đến máy chủ.

ForceCommand: Người dùng buộc phải sử dụng lệnh `internal-sftp`, đây là cơ chế truyền tệp an toàn được tích hợp trong máy chủ SSH.



Ở đây ta thấy được rằng nếu ssh thì sẽ không được nhưng nếu thực hiện lệnh sftp để truy cập thì ta có thể vào một cách dễ dàng