Lab #2: Bảng đánh giá

Cài đặt à cấu hình ClamAV

Khóa học: ____Malware Analysis and Reverse Engineering (IAM302) _____

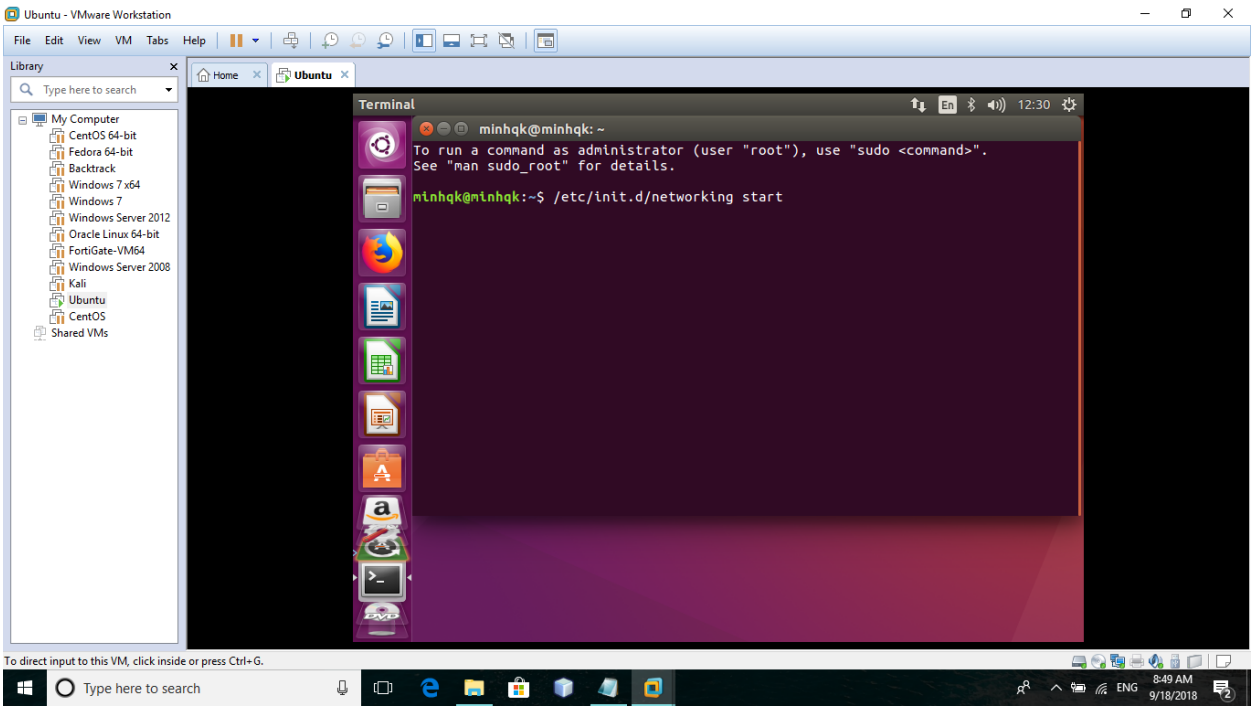
Họ và tên: _____ _____

Giảng viên hướng dẫn: _____ _____

Deadline: _____ _____

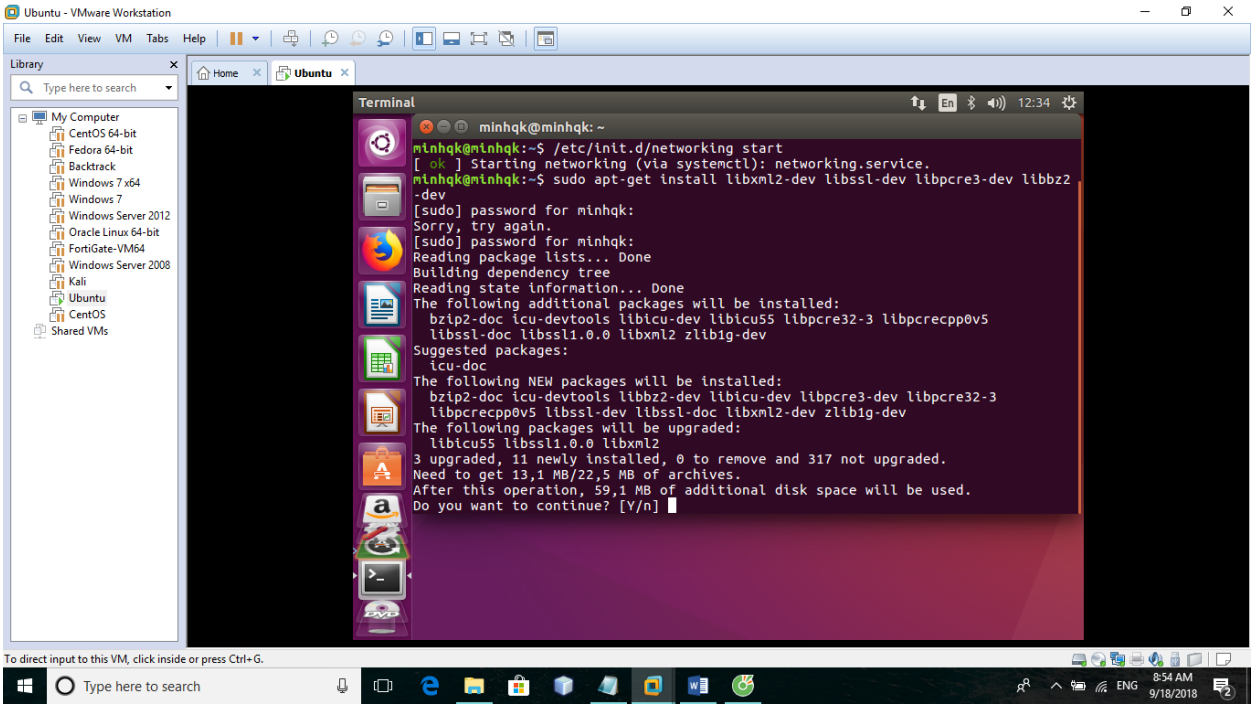
❖ Khởi động card mạng trong ubuntu lại trong máy ảo:

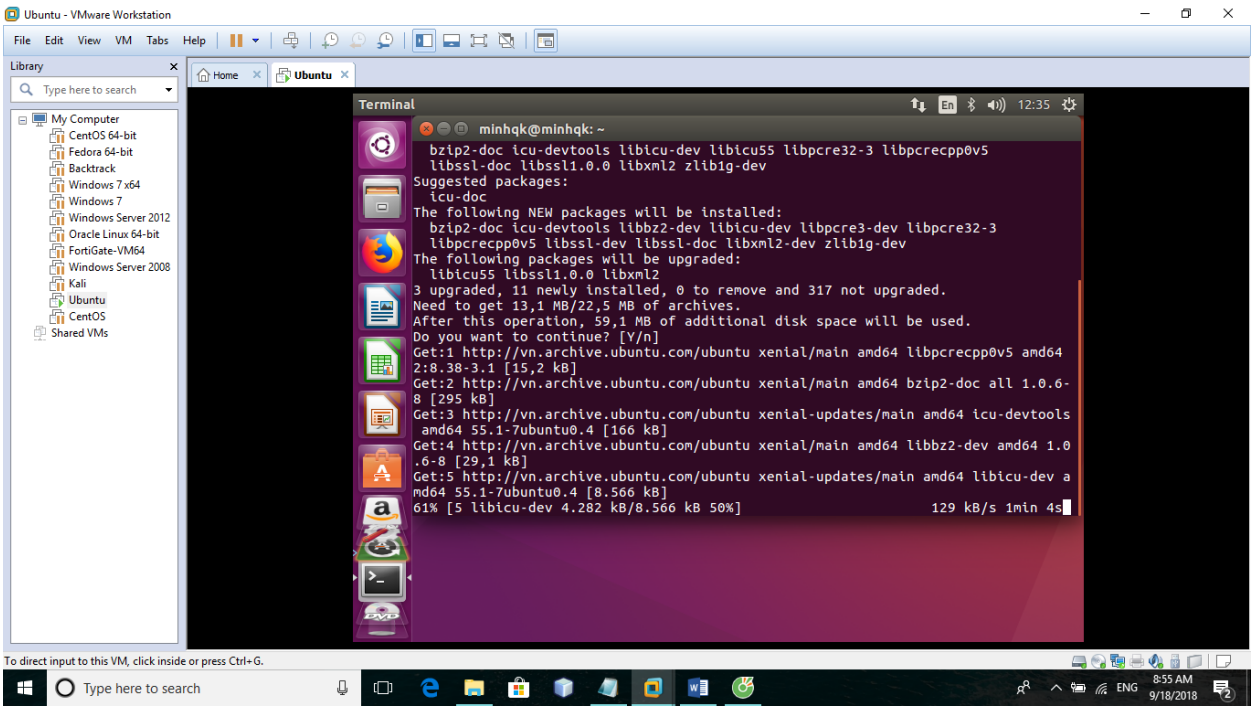
/etc/init.d/networking start

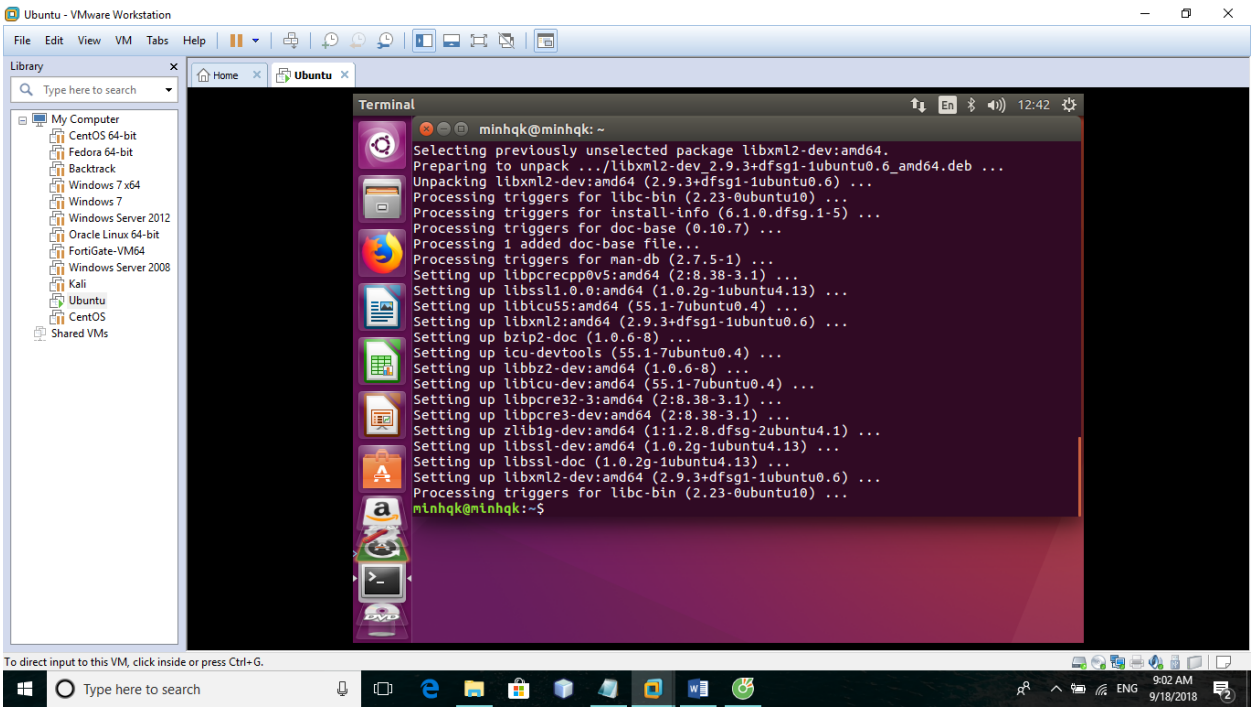


❖ Cập nhật và cài các thư viện cần thiết cho cài đặt ClamAV:

sudo apt-get install libxml2-dev libssl-dev libpcre3-dev libbz2-dev



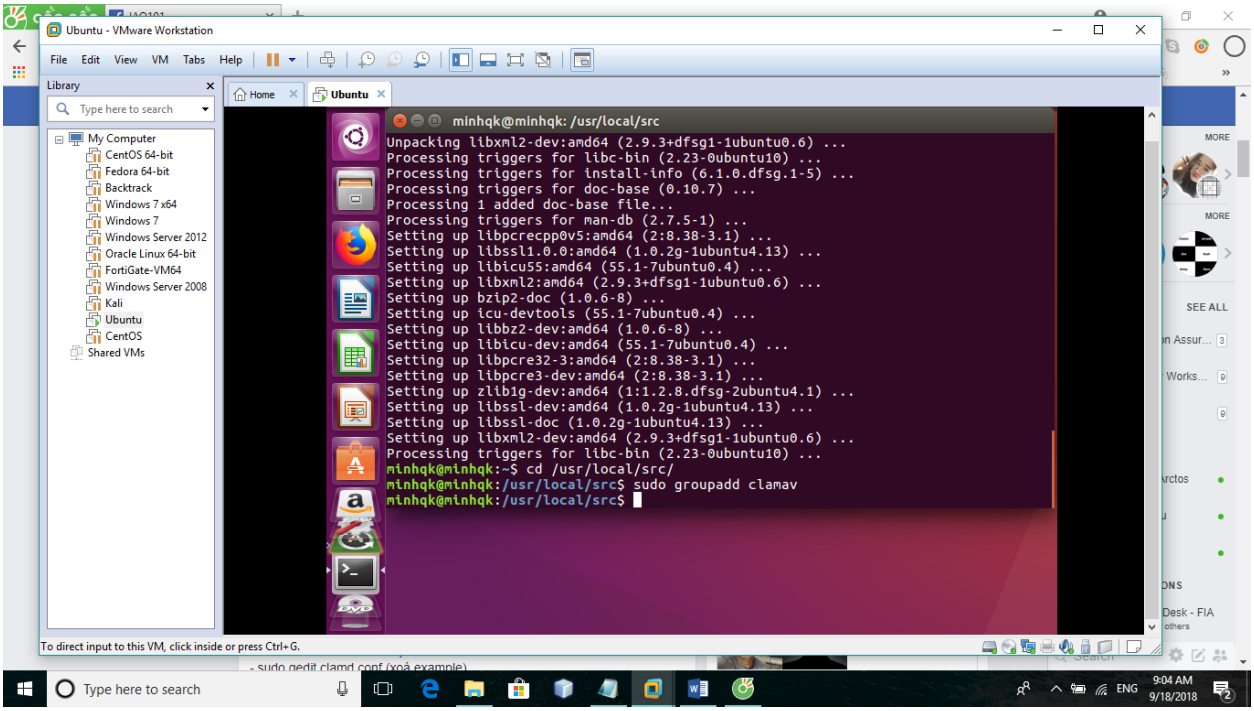




❖ Bắt đầu tạo group, user cũng như các folder cần thiết cho việc cài đặt ClamAV:

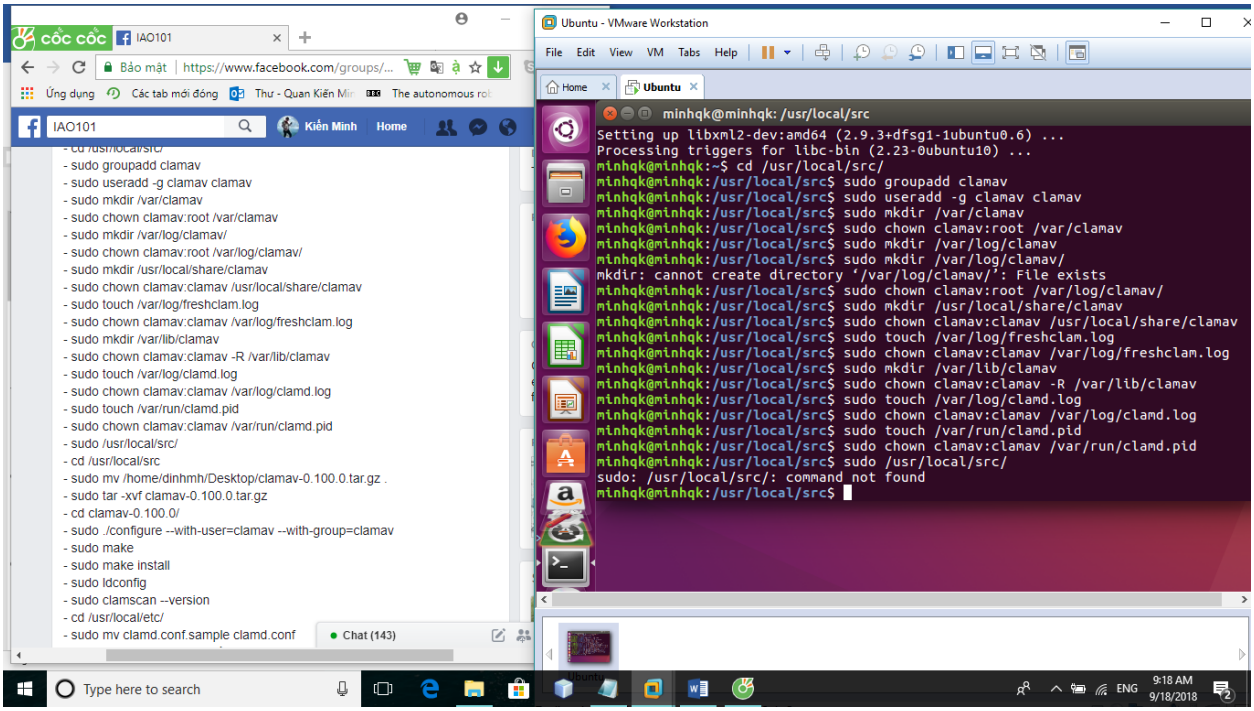
Vào thư mục /usr/local/src/: cd /usr/local/src/

Tạo group clamAV: sudo groupadd clamav



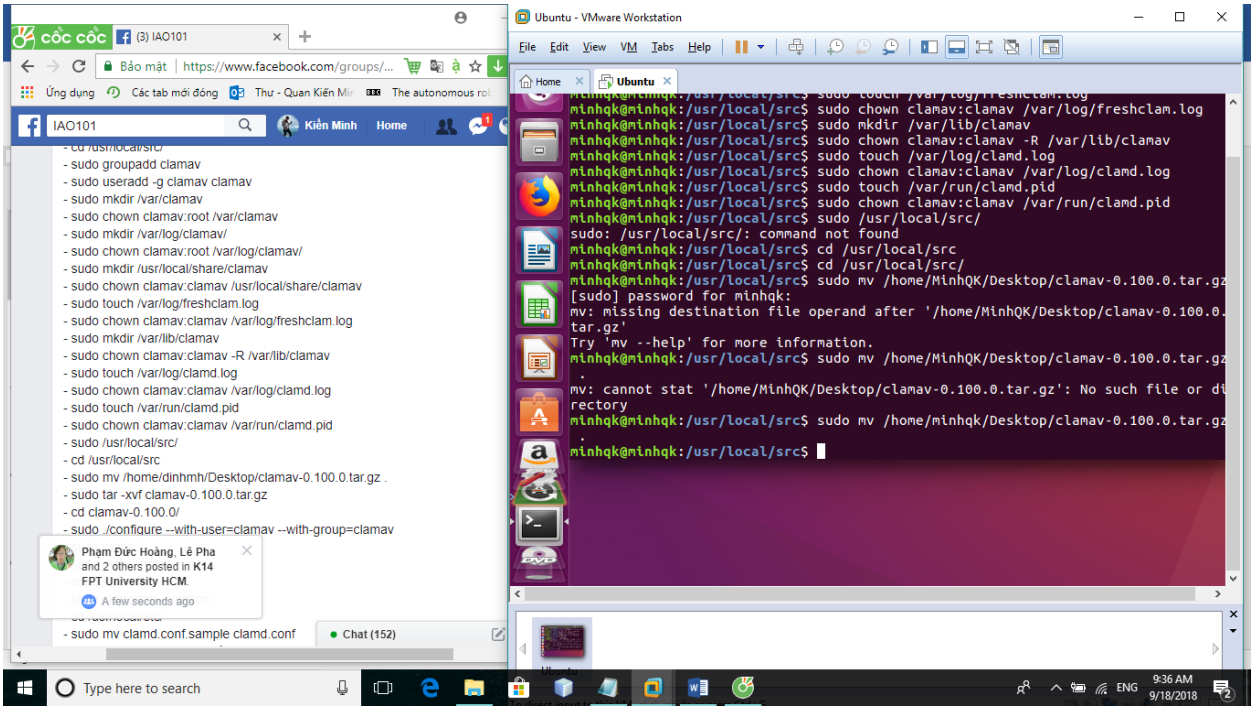
Thực hiện tiếp các câu lệnh sau để tạo các folder để ghi log mà user clamav có toàn quyền truy cập chỉnh sửa trên ấy:

- sudo useradd -g clamav clamav
- sudo mkdir /var/clamav
- sudo chown clamav:root /var/clamav
- sudo mkdir /var/log/clamav/
- sudo chown clamav:root /var/log/clamav/
- sudo mkdir /usr/local/share/clamav
- sudo chown clamav:clamav /usr/local/share/clamav
- sudo touch /var/log/freshclam.log
- sudo chown clamav:clamav /var/log/freshclam.log
- sudo mkdir /var/lib/clamav
- sudo chown clamav:clamav -R /var/lib/clamav
- sudo touch /var/log/clamd.log
- sudo chown clamav:clamav /var/log/clamd.log
- sudo touch /var/run/clamd.pid
- sudo chown clamav:clamav /var/run/clamd.pid
- cd /usr/local/src



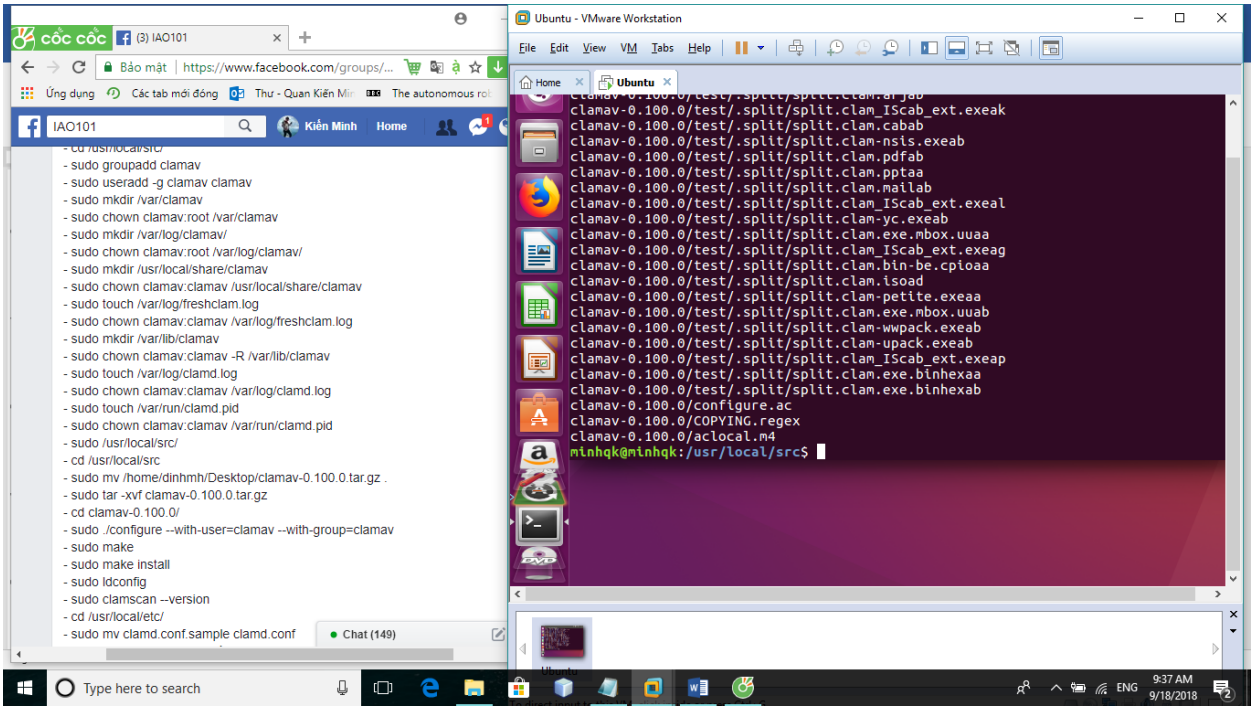
Về lại thư mục /user/local/src để copy file clamav-0.100.0.tar.gz vào /home/minhqk/Desktop:

sudo mv /home/minhqk/Desktop/clamav-0.100.0.tar.gz .

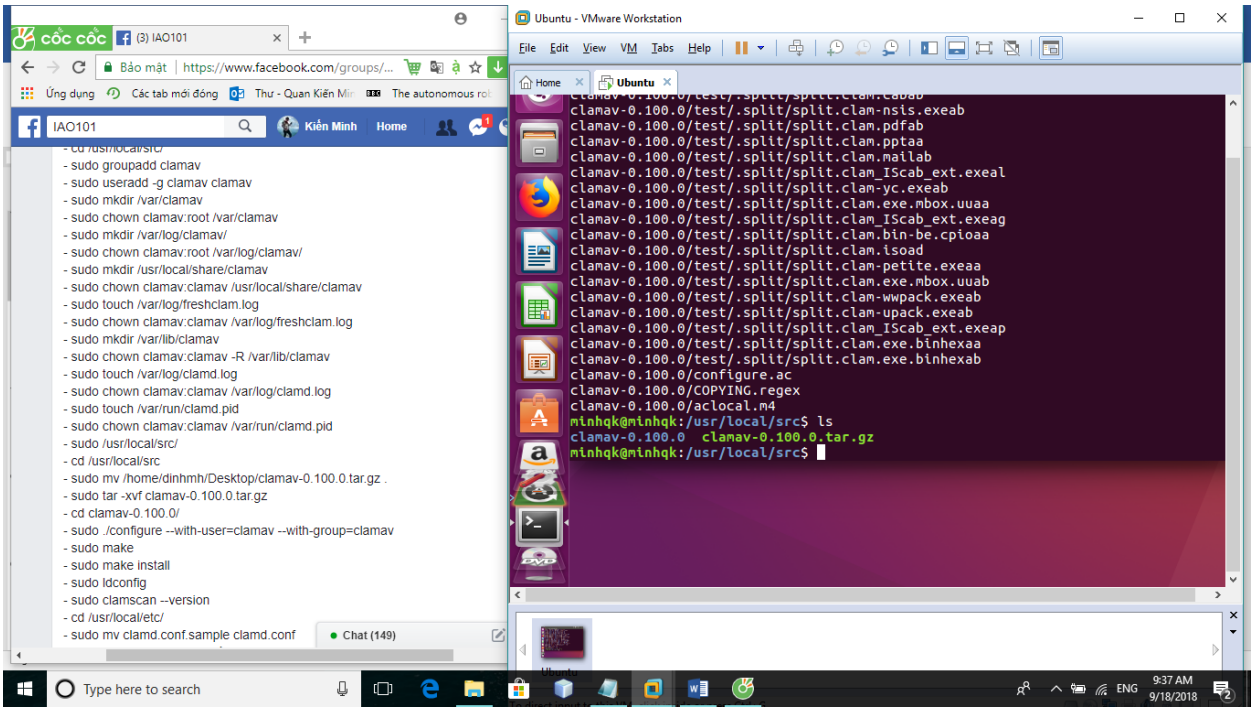


Tiếp đó là ta unzip file đó ra folder:

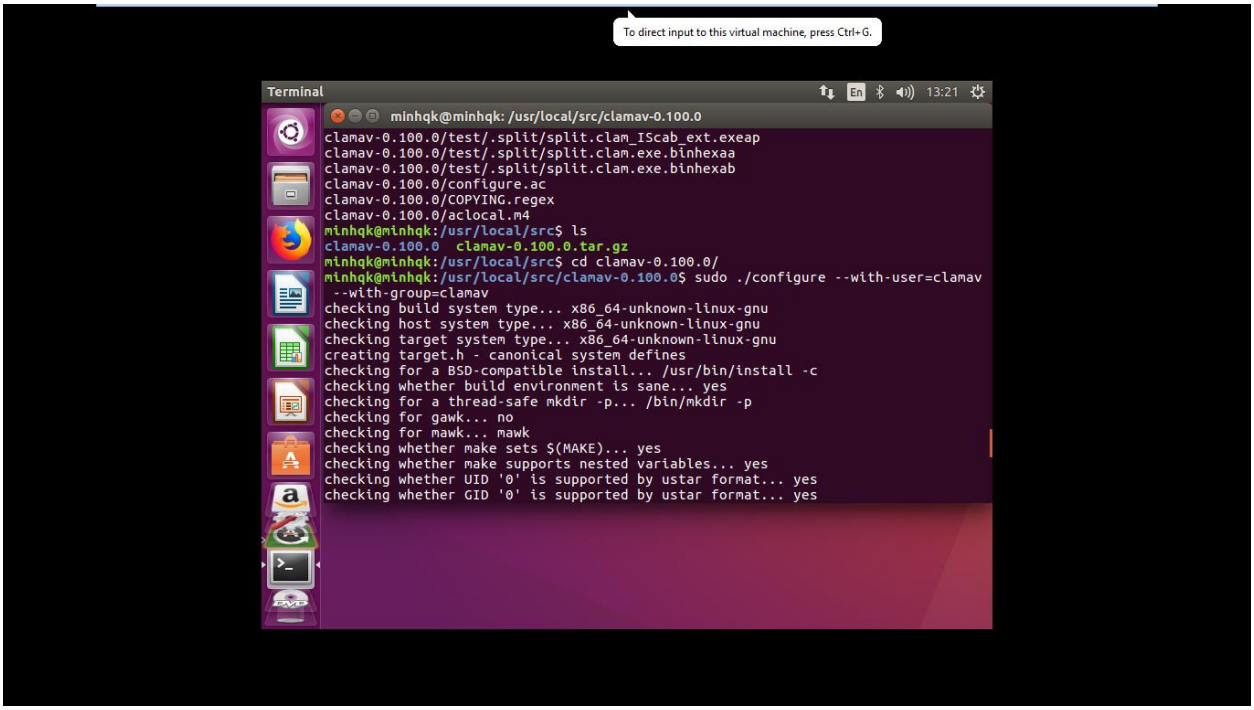
sudo tar -xvf clamav-0.100.0.tar.gz

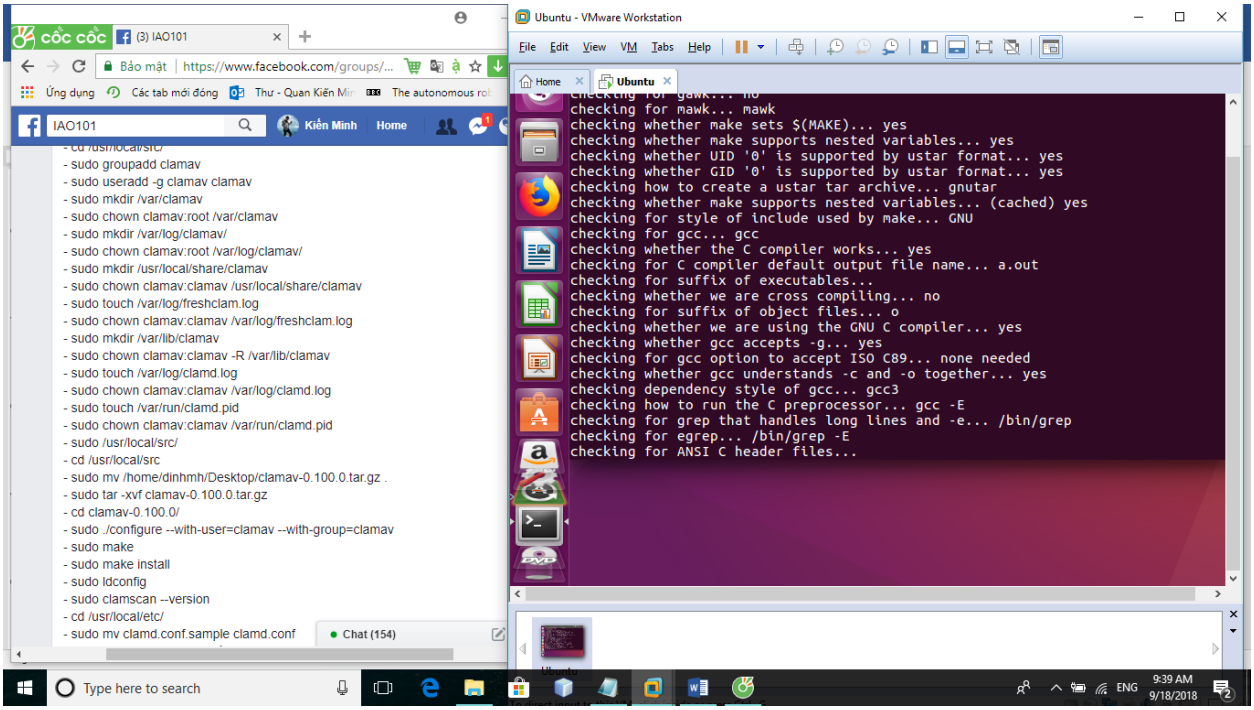


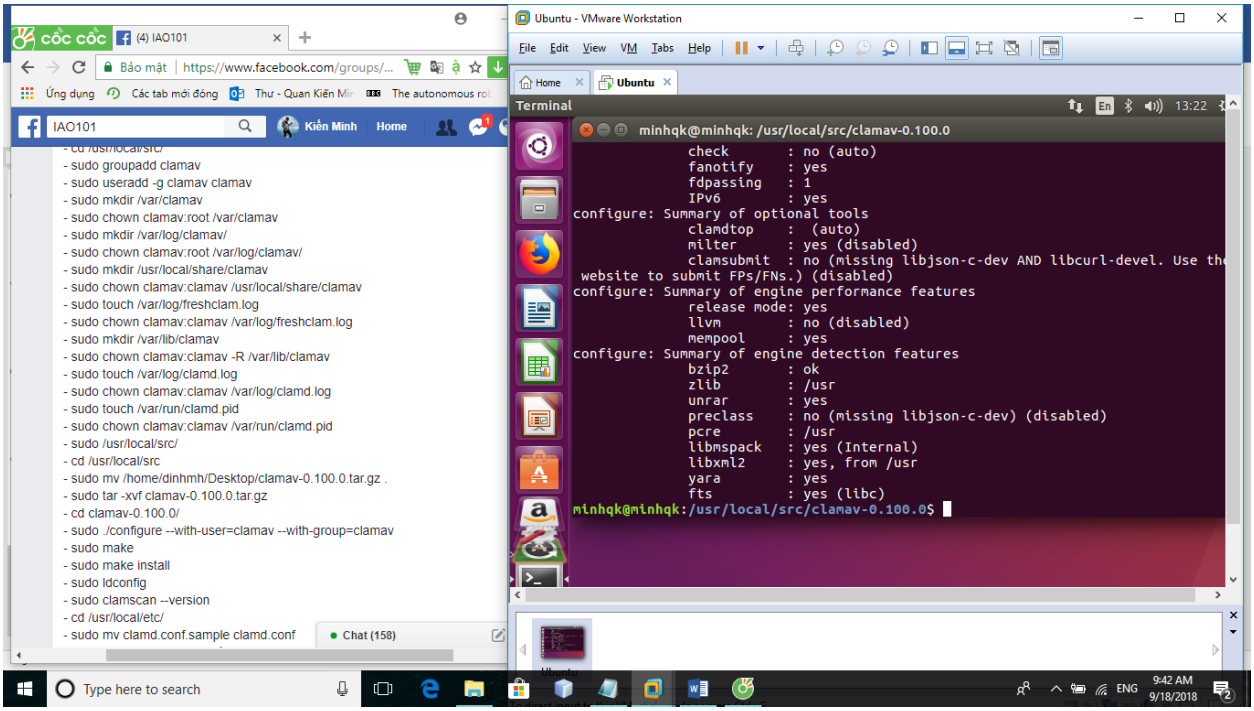
Tại folder hiện hành dùng command ls để list tất cả các file ra.



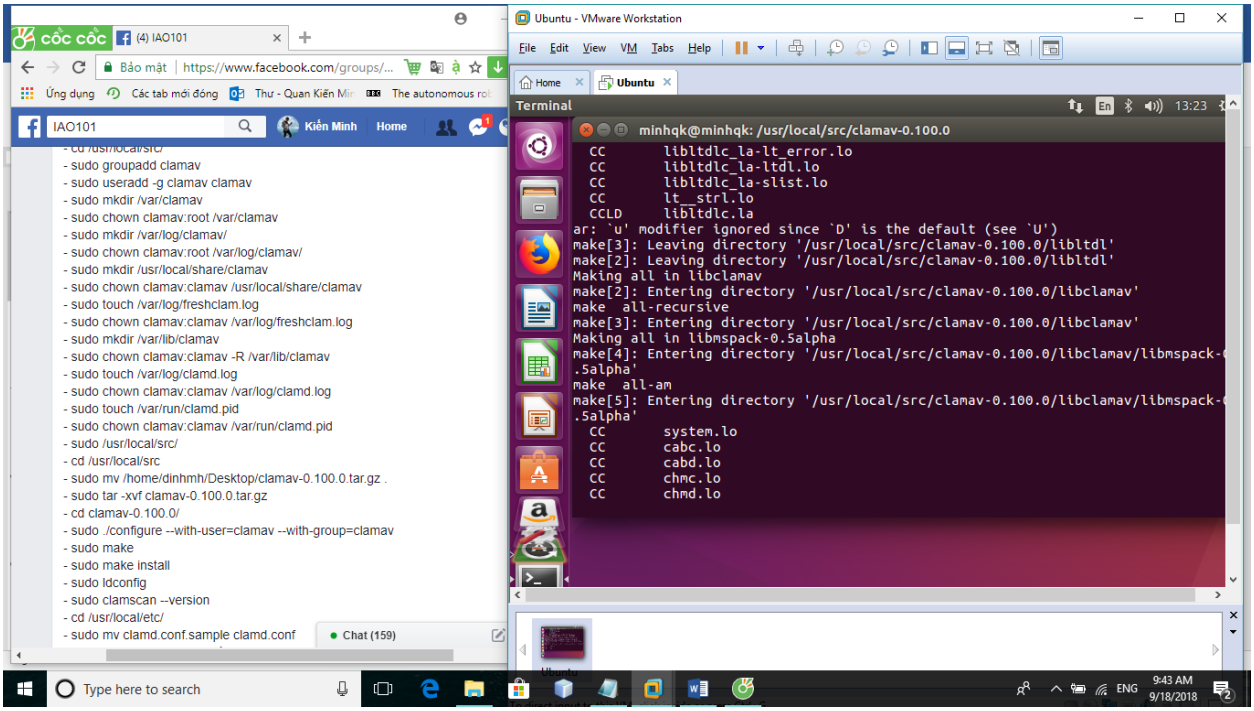
Sau đó ta vào thư mục clamav-0.100.0 với câu lệnh: cd clamav-0.100.0/. Kế tiếp chuẩn cho cấu hình clamav với group clamav mình đã tạo trước đó:
sudo ./configure --with-user=clamav --with-group=clamav

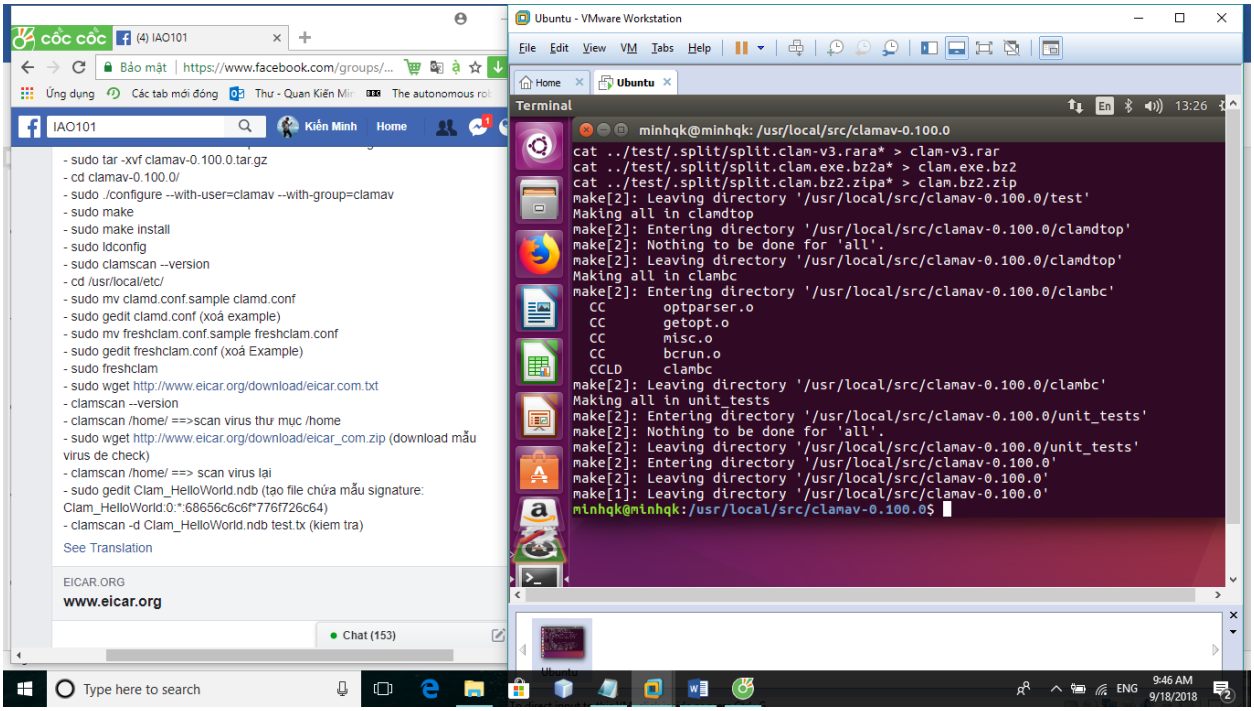




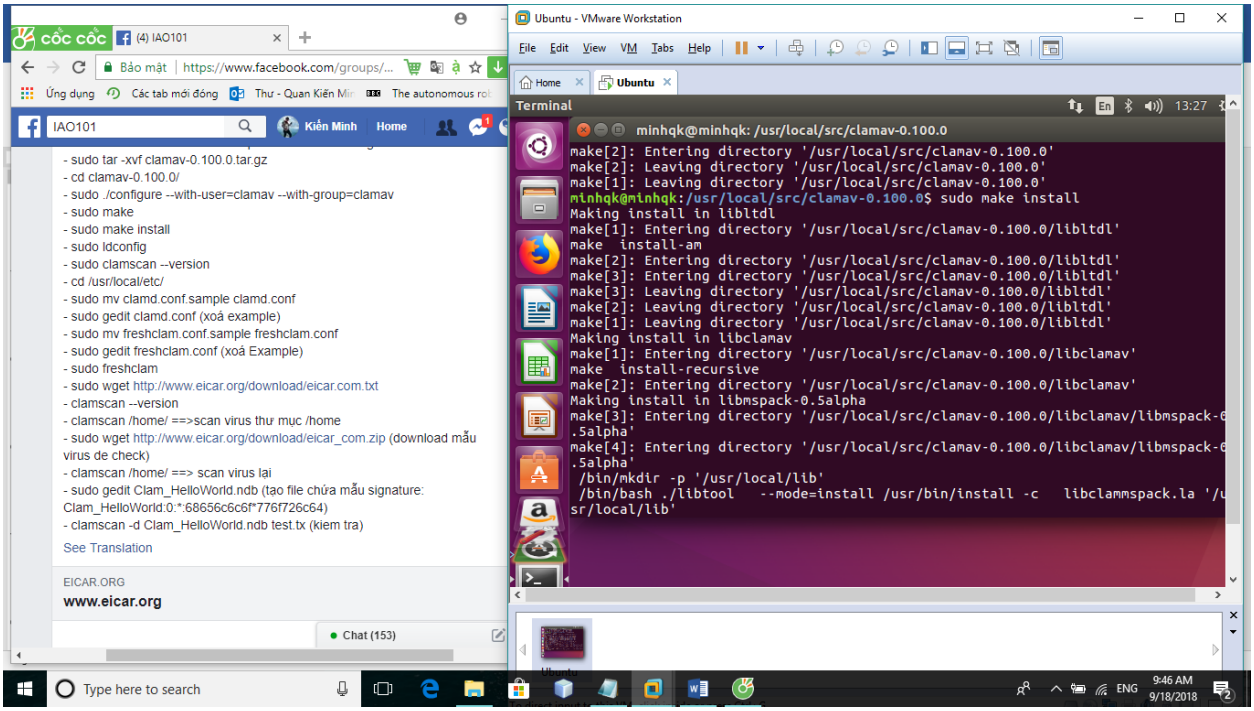


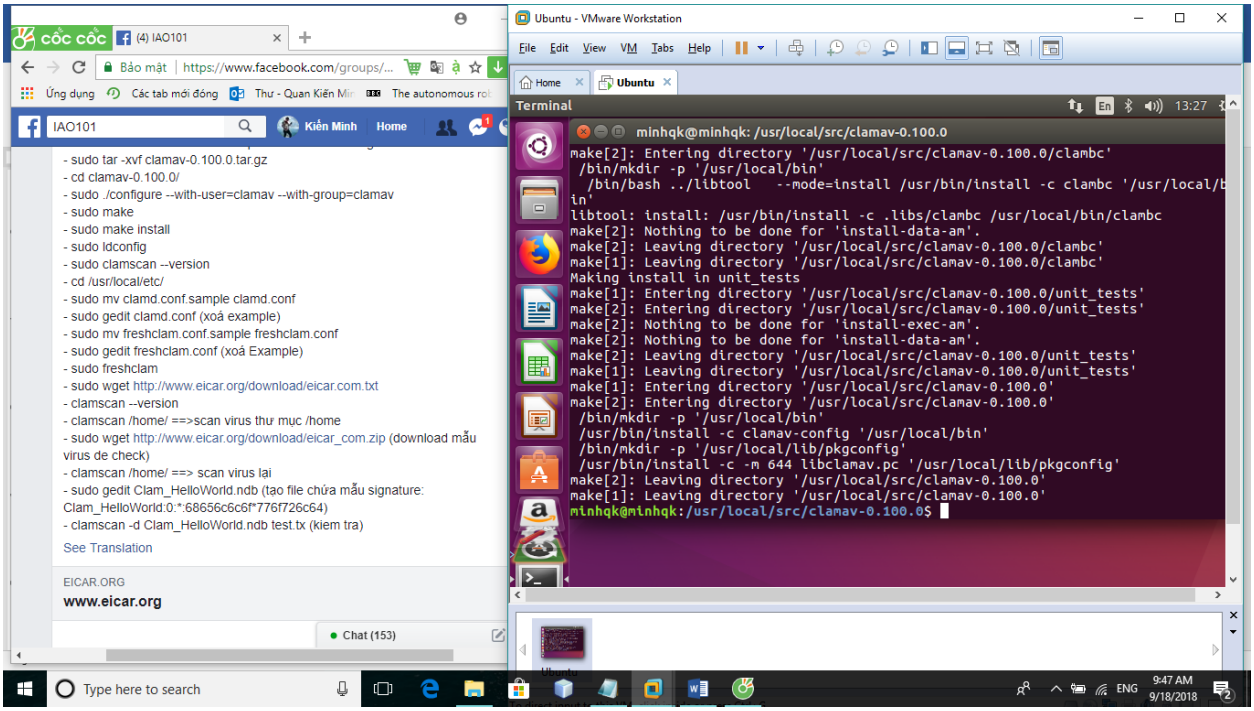
Tiếp đến ta dùng lệnh sudo make



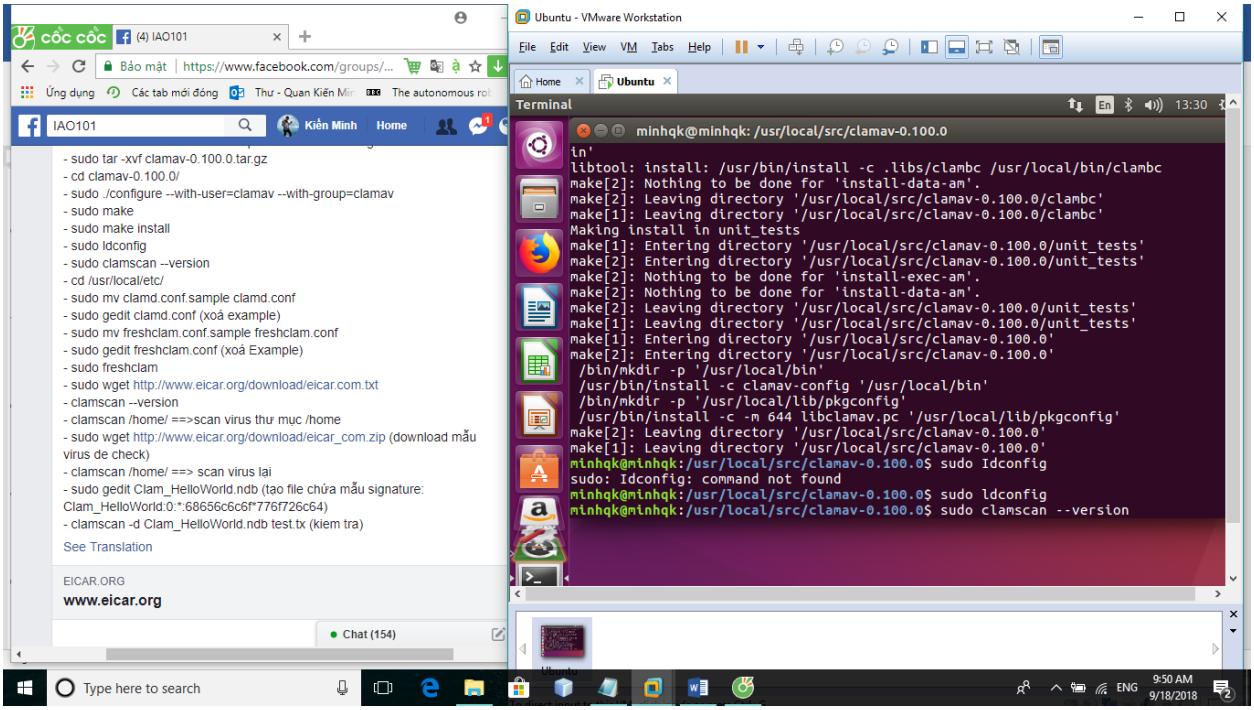


Và đây là bước chính thức install ClamAV bắt đầu: sudo make install

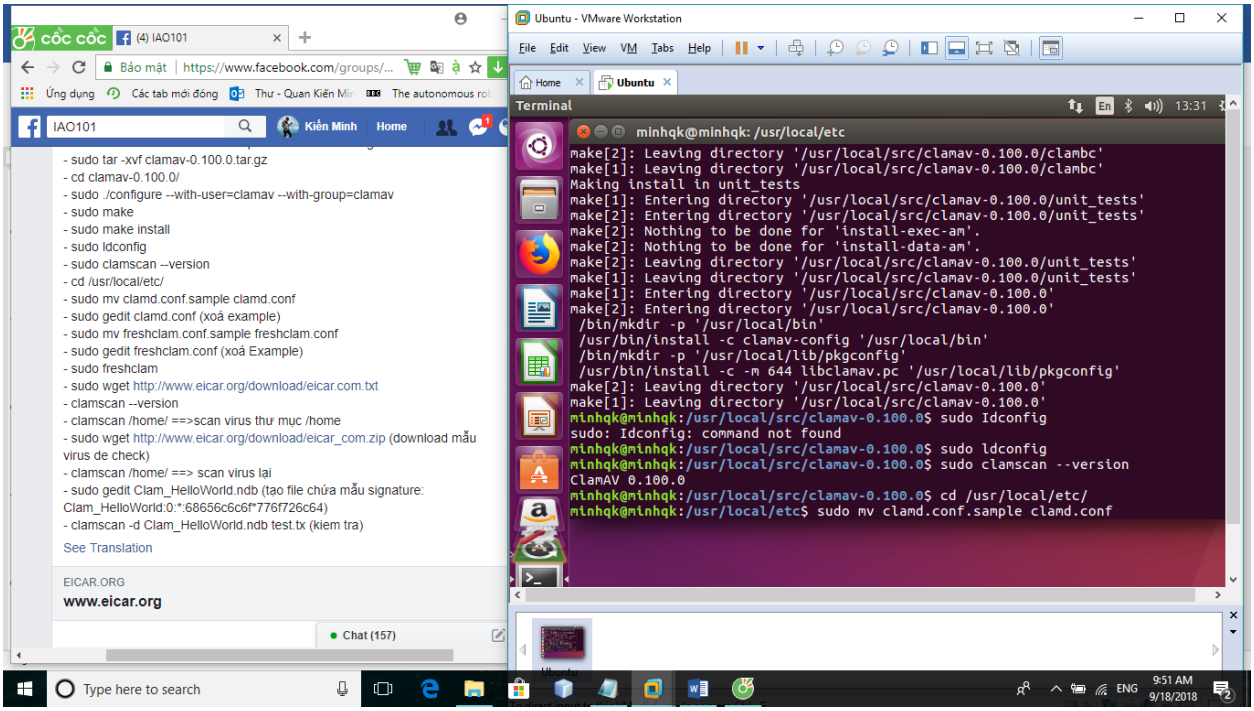




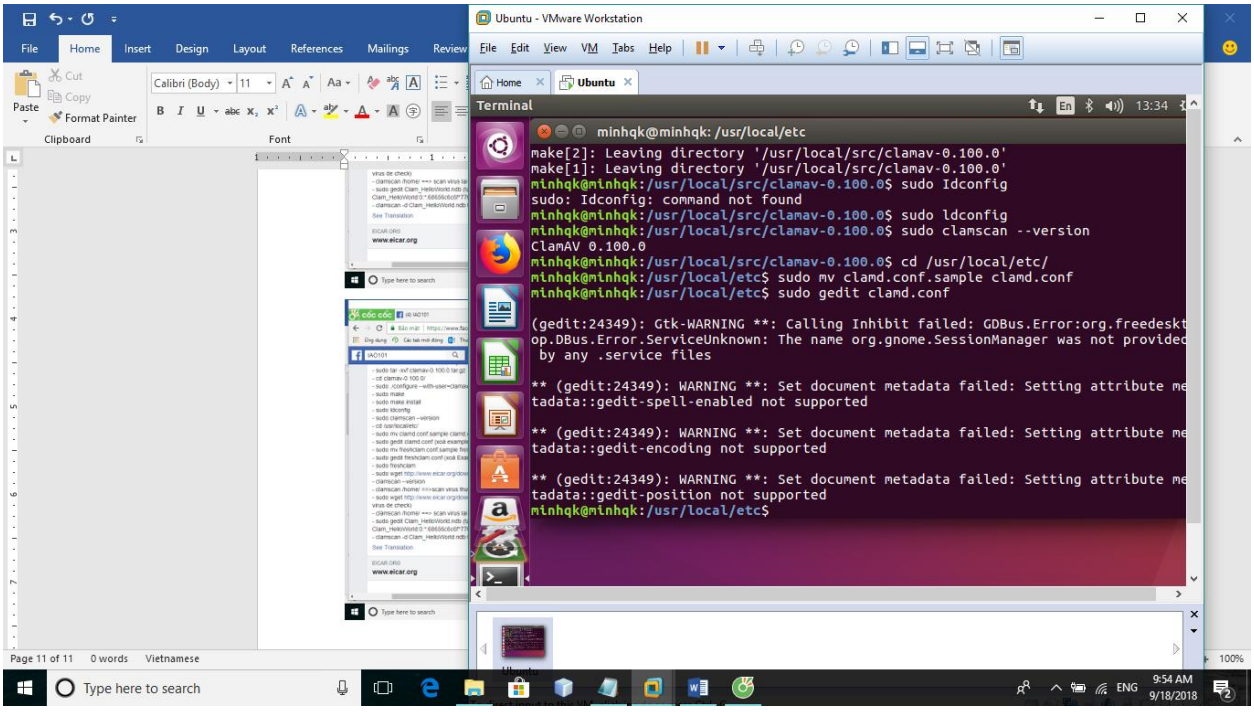
Dùng lệnh sudo lpconfig và sau đó kiểm tra version của clamav mới cài: clamscan –version

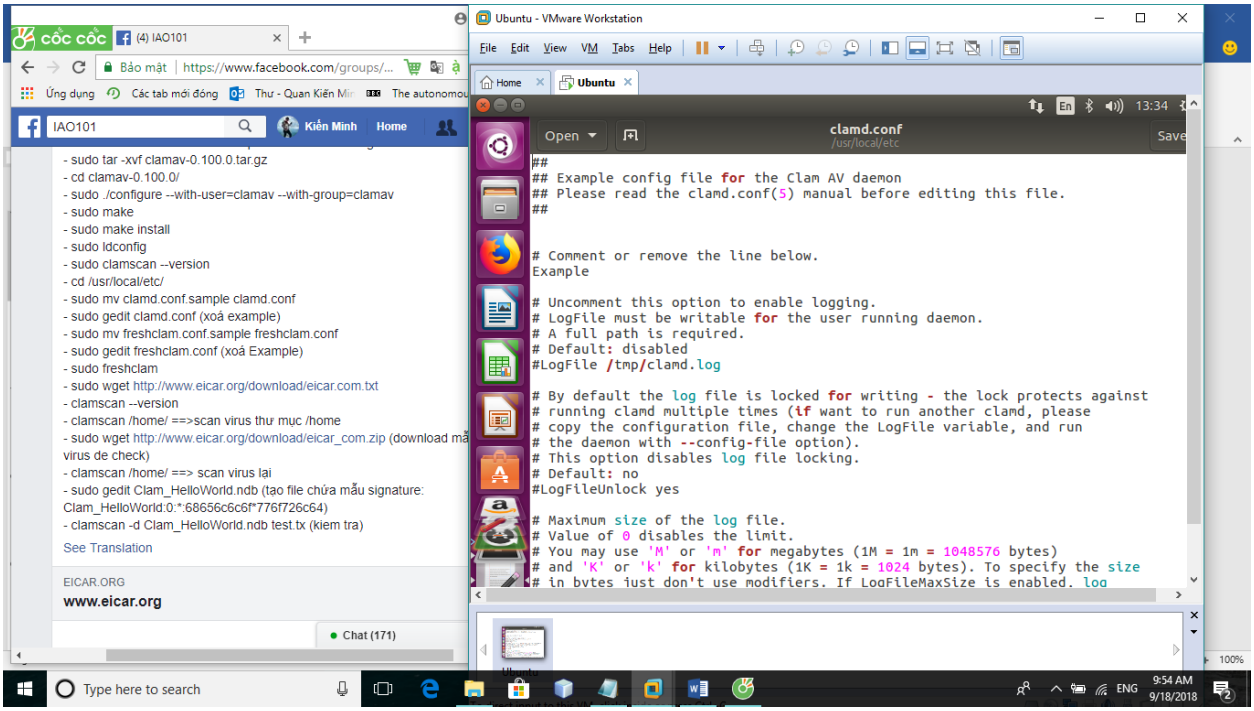


Copy clamd.conf.sample vào clamd.conf: sudo mv clamd.conf.sample clamd.conf

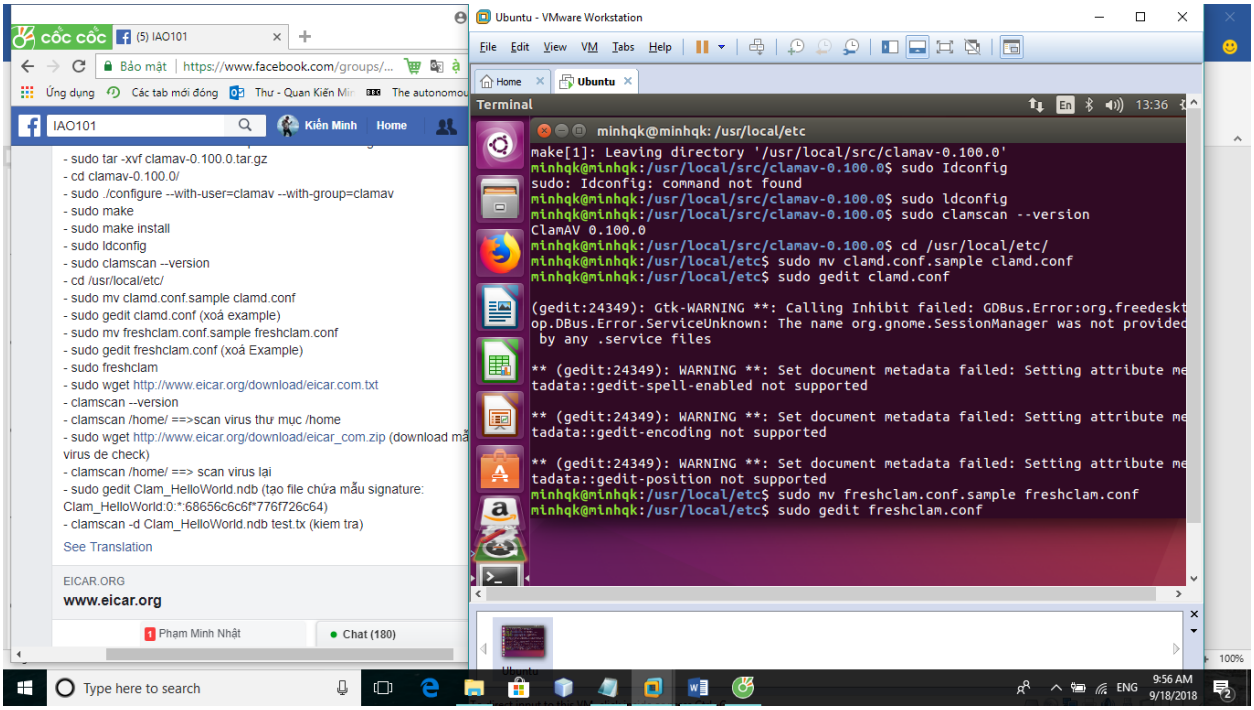


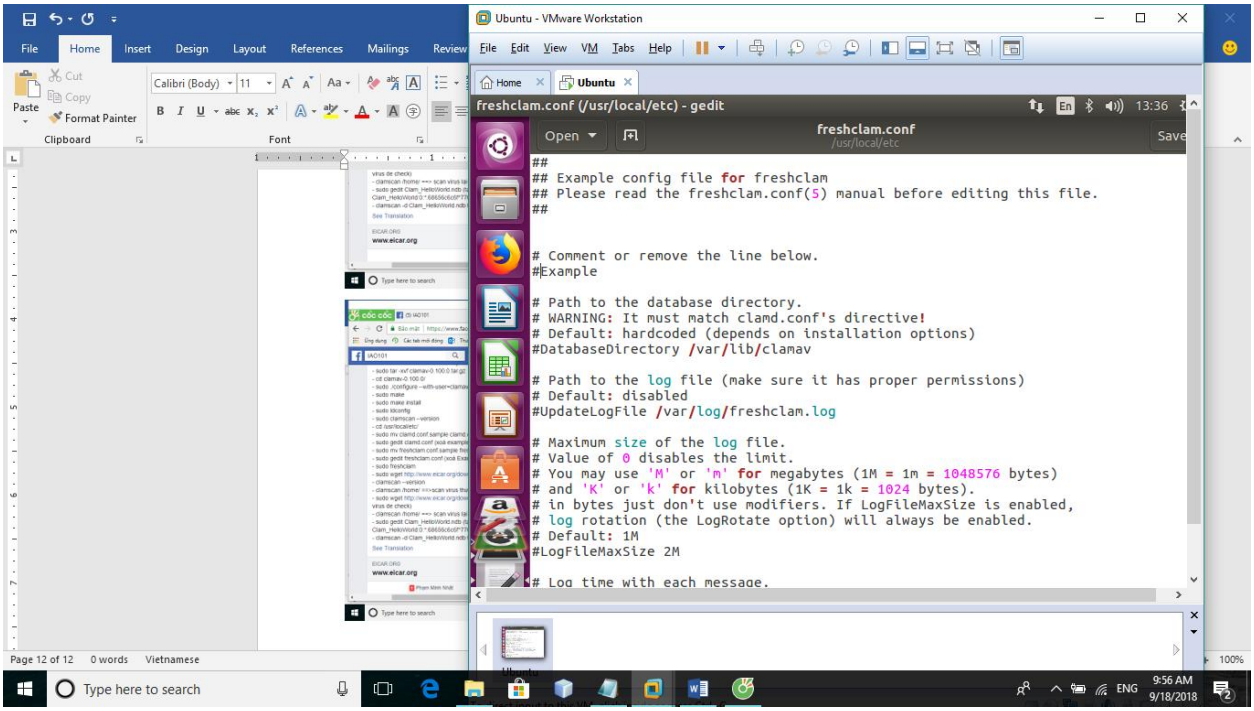
Dùng lệnh sudo gedit clamd.conf (xoá example)



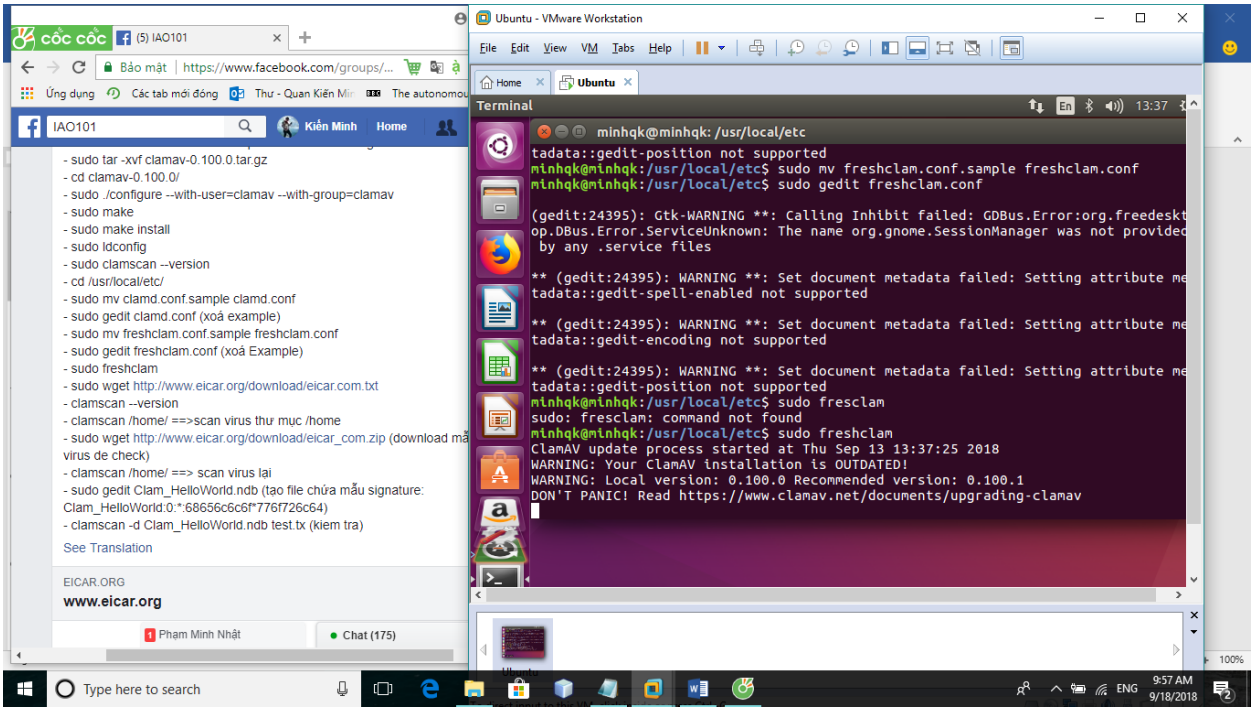


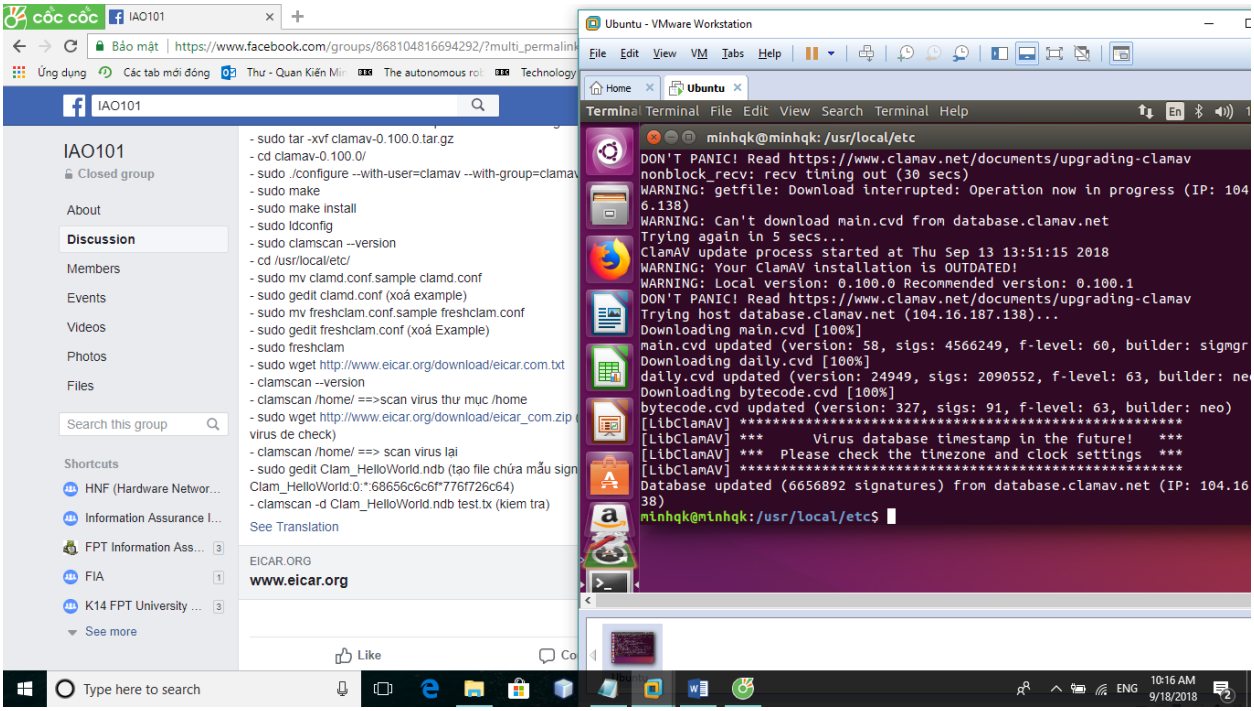
Làm tương tự cho freshclam.conf.sample: sudo mv freshclam.conf.sample freshclam.conf





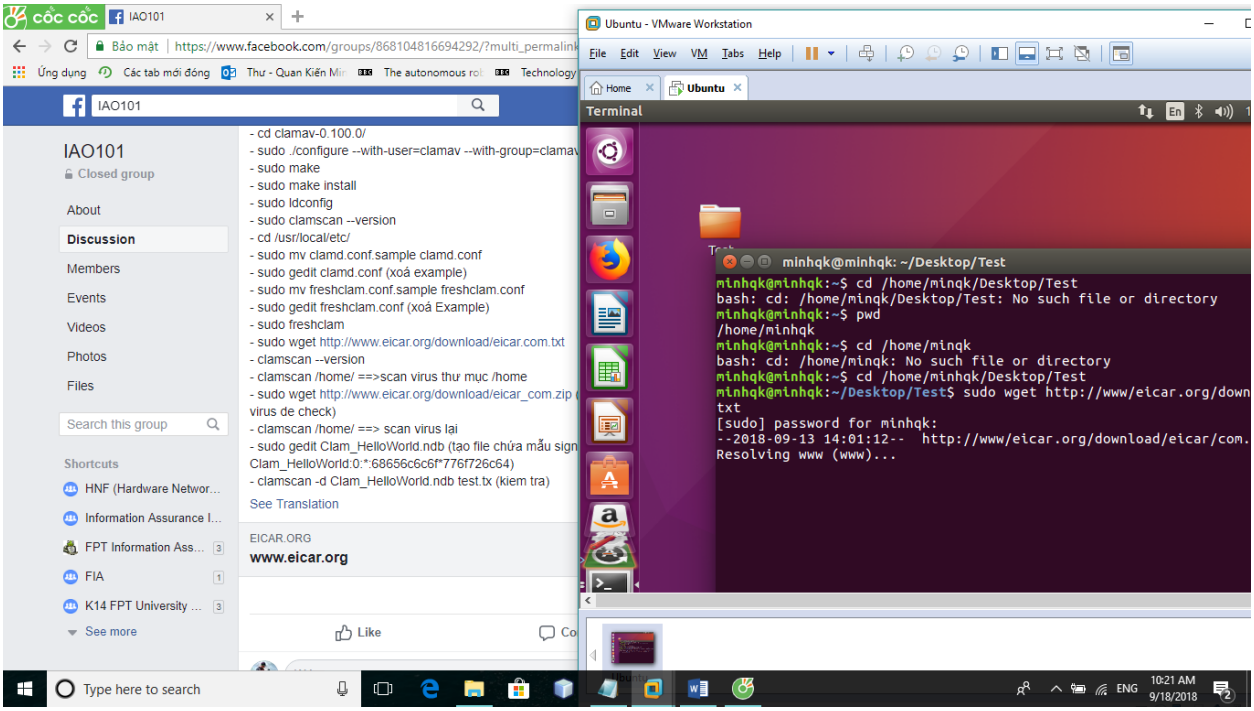
Và sau đây ta sẽ dùng lệnh sudo freshclam để download các file cài đặt ClamAV

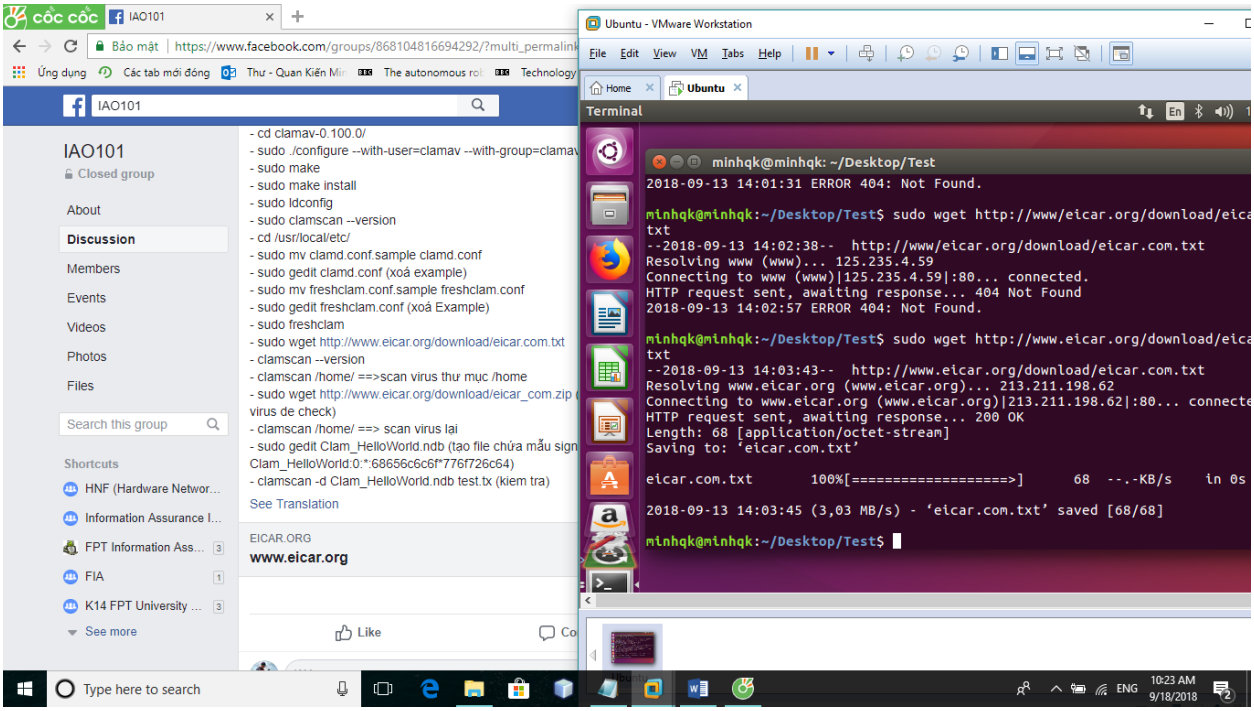




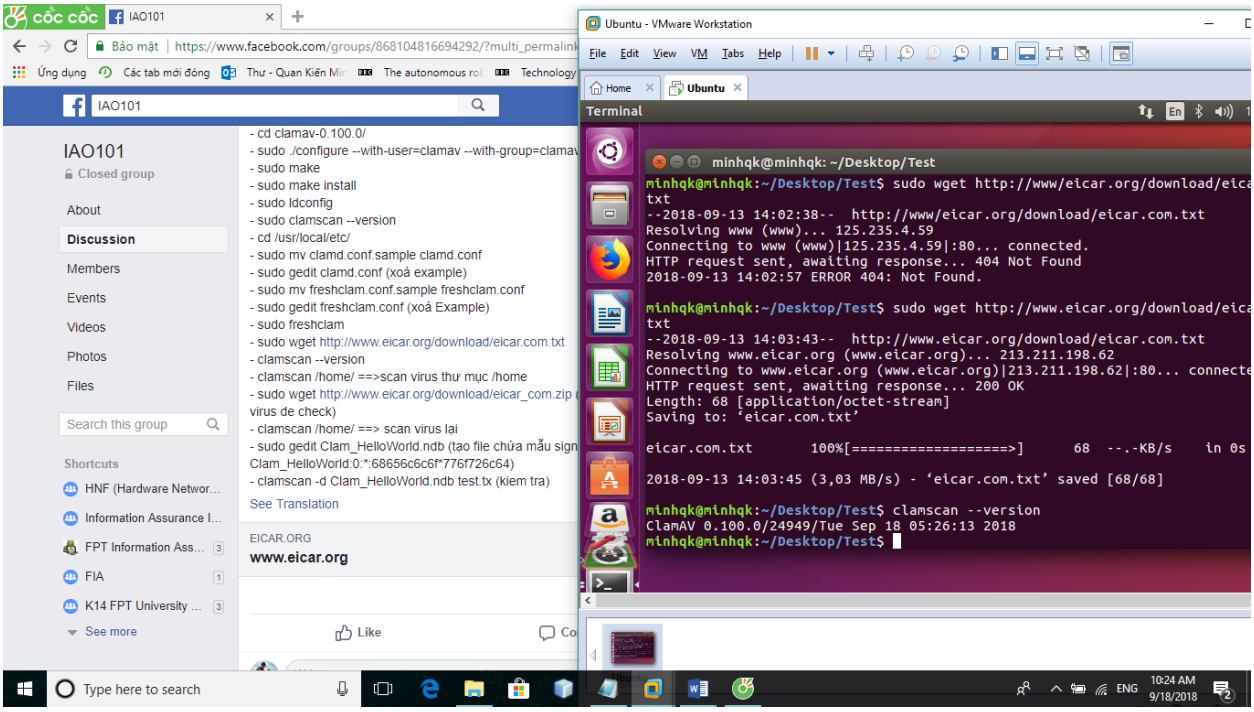
Sau khi download xong, ta sẽ tạo một thư mục tên Test và download file chứa virus vào đó để test thử ClamAV hoạt động như thế nào:

sudo wget http://www.eicar.org/download/eicar.com.txt

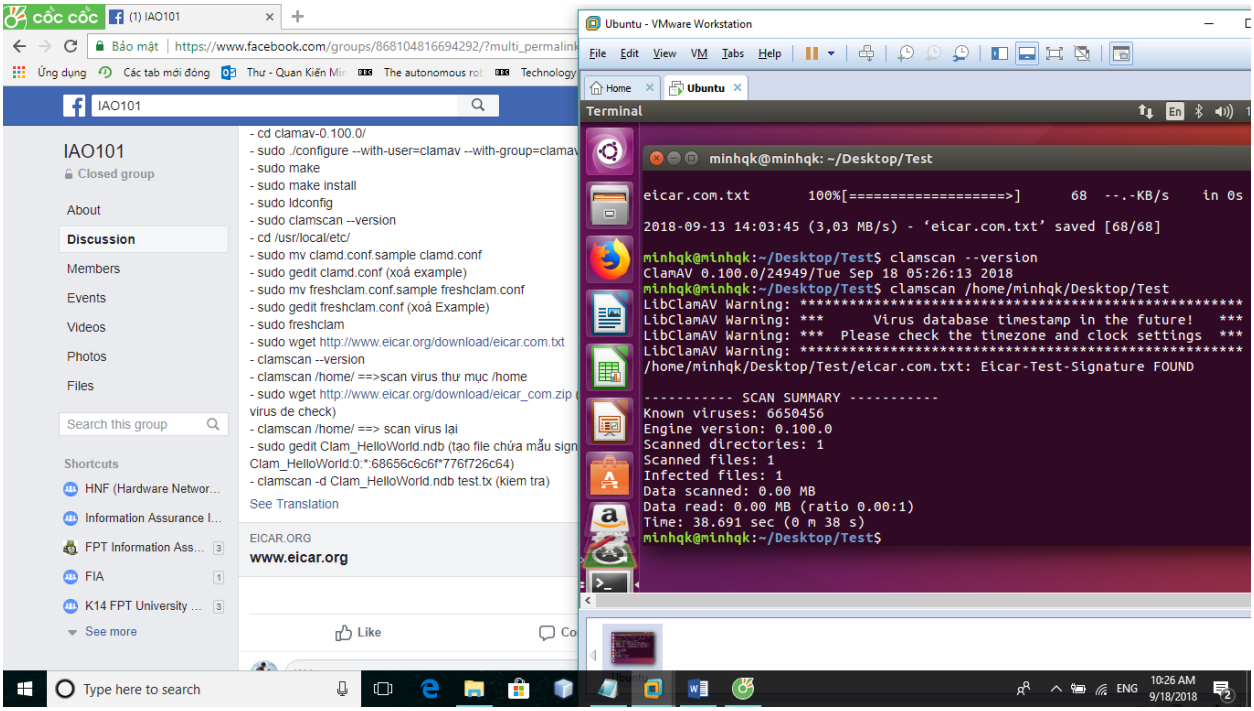




Xem version của ClamAV: clamscan --version

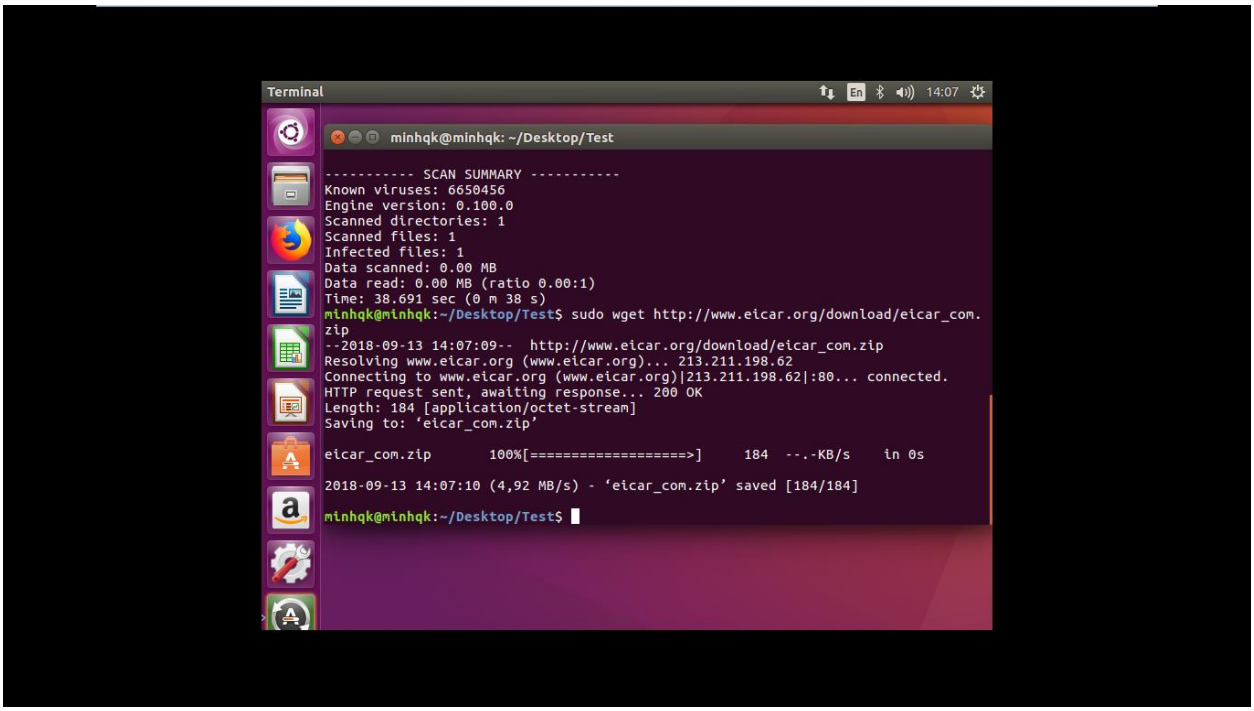


Và cuối cùng ta test ClamAV thôi: clamscan /home/minhqk/Desktop/Test

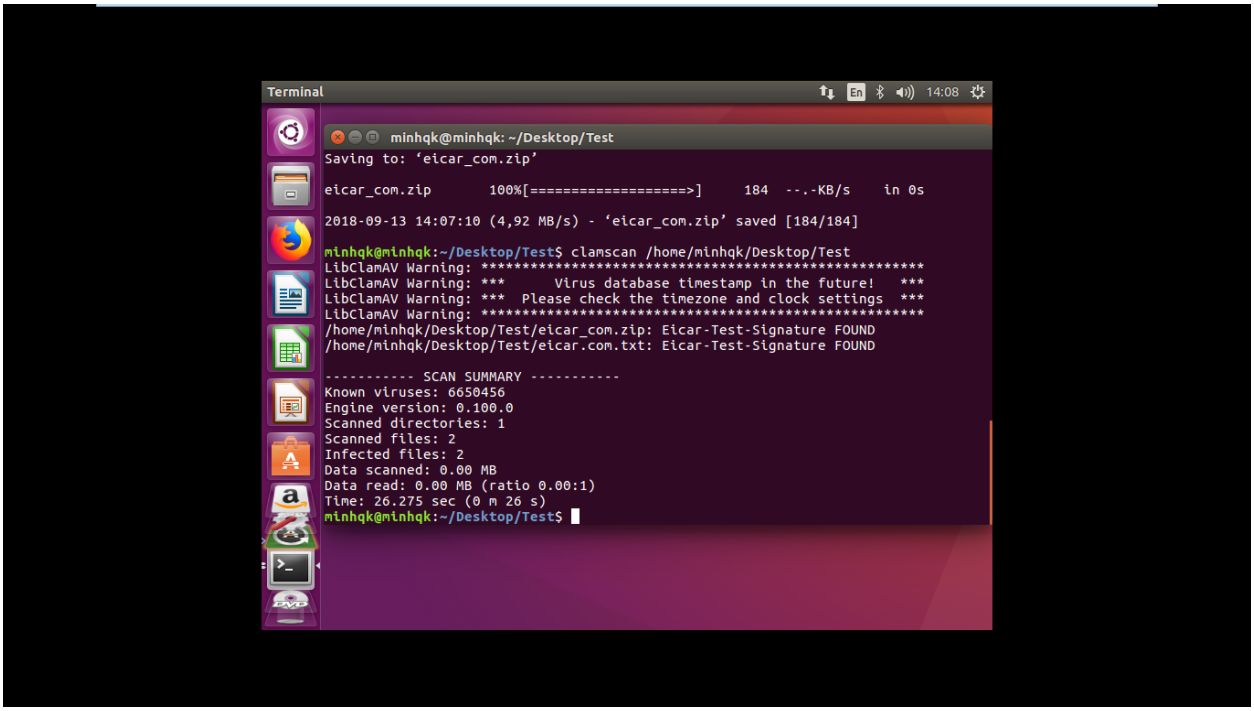


Ta thử tải thêm một file zip chứa mã độc nữa để test ClamAV:

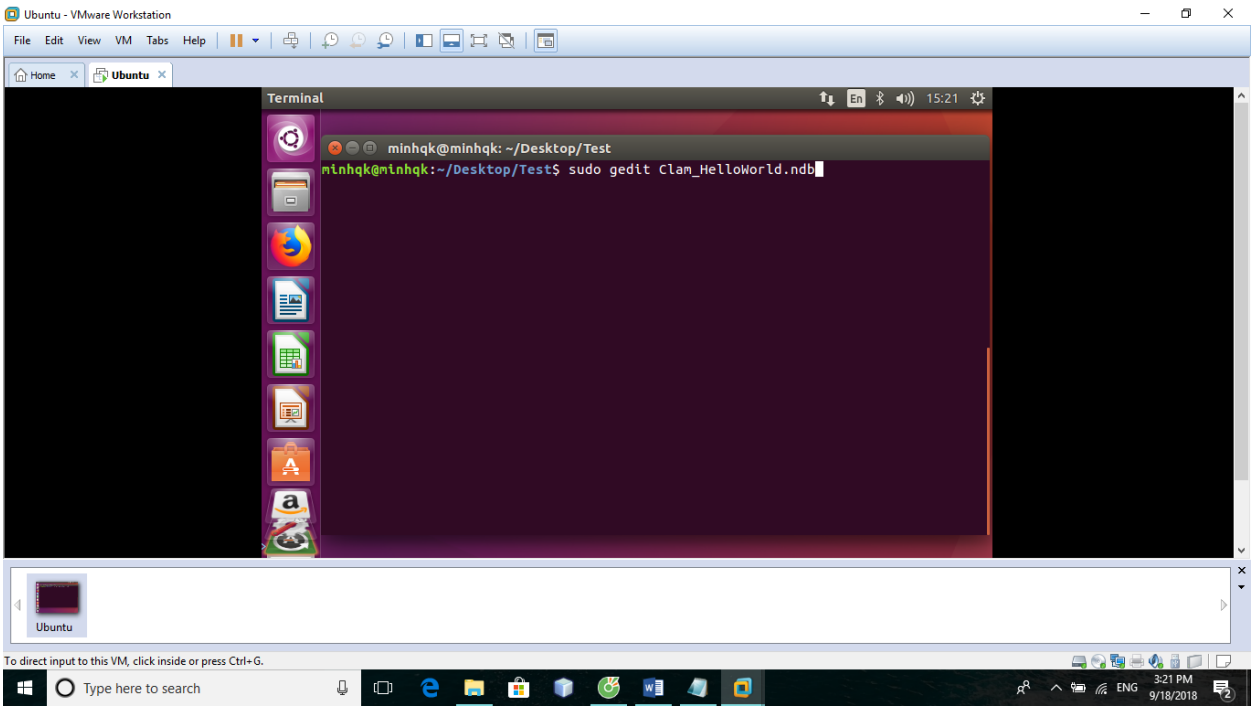
sudo wget http://www.eicar.org/download/eicar_com.zip



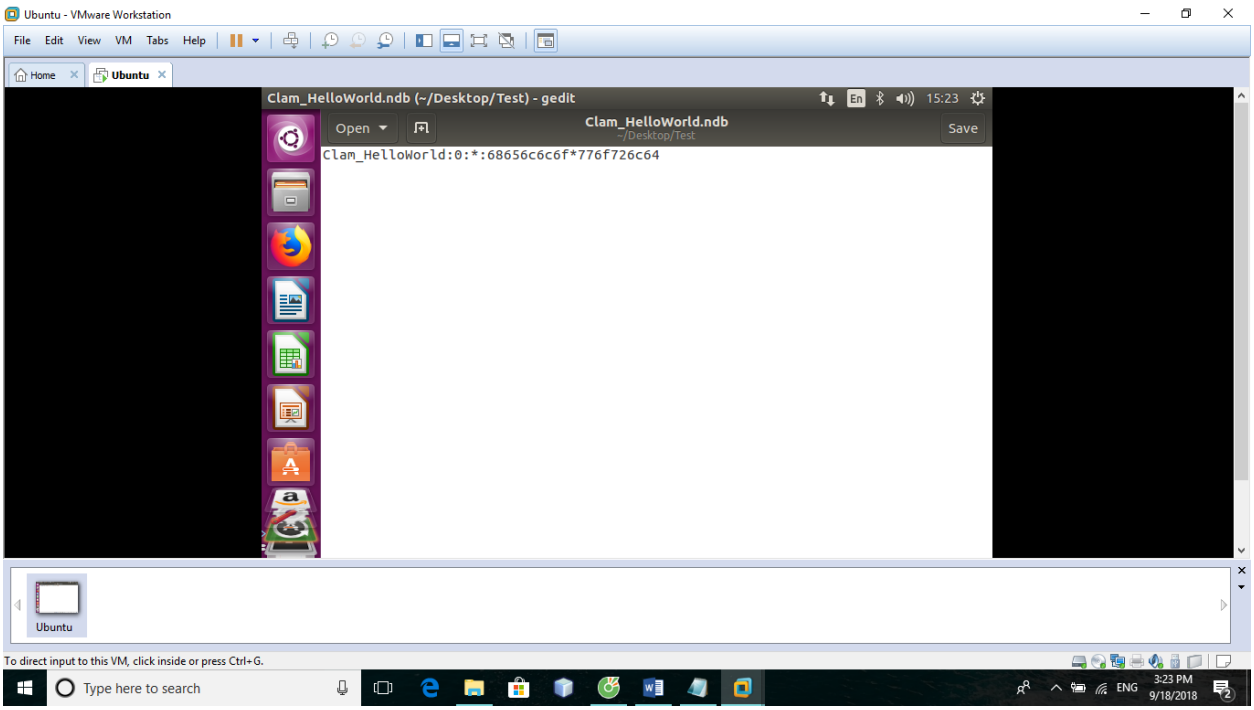
Và đây là kết quả scan: clamscan /home/minhqk/Desktop/Test



Dùng lệnh này để tạo ra signature cho clamav: sudo gedit Clam_HelloWorld.ndb

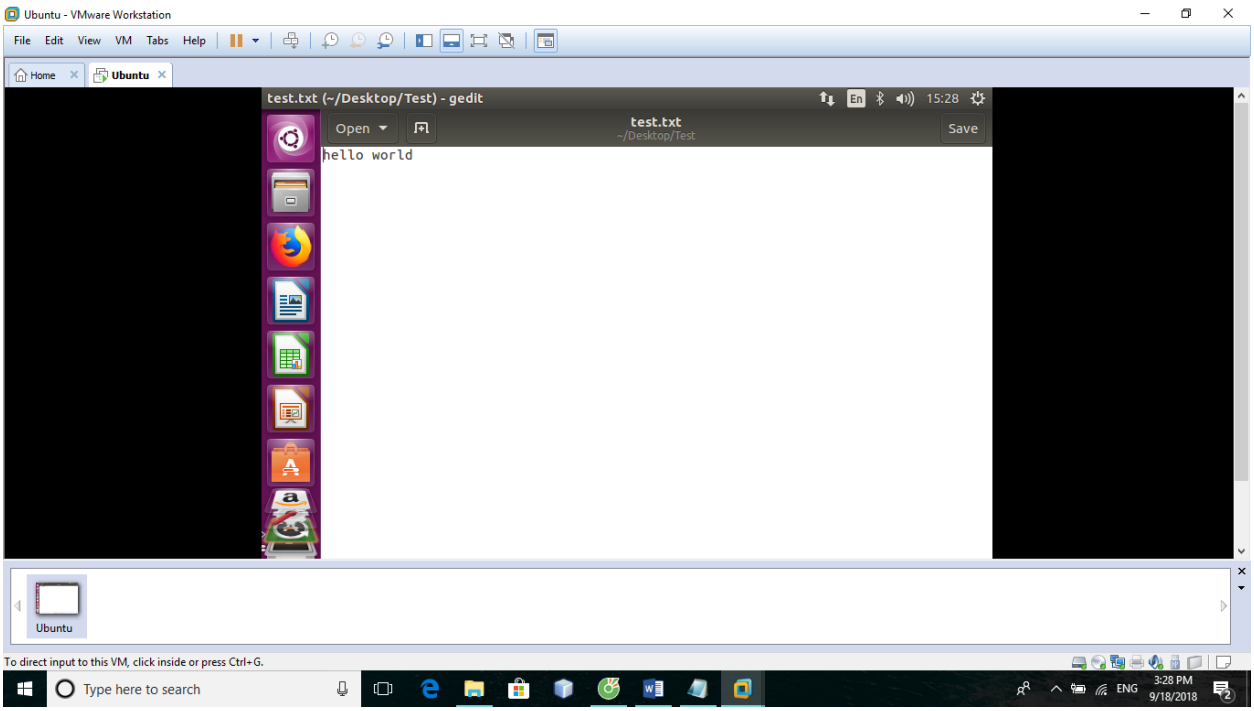


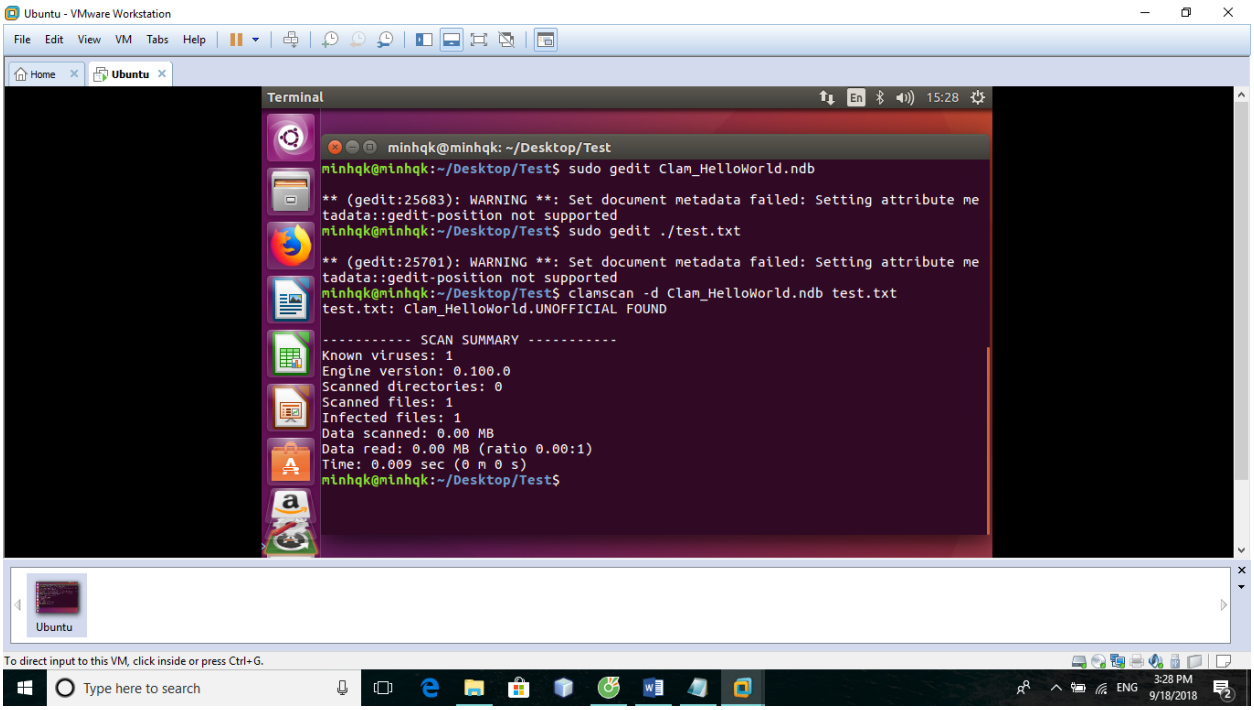
Sau đó ta nhập Clam_HelloWorld:0:*:68656c6c6f*776f726c64 này vào file Clam_HelloWorld.ndb. (File này sẽ signature để ClamAV scan file, cụ thể là nếu file txt nào chứa từ “hello” và từ “world” sẽ bị xem là bị tiêm mã độc)



Tiếp đến, ta tạo file test.txt bằng lệnh sudo touch ./test.txt, trong file này có sẽ chứa 2 từ “hello world”. Sau đó là ta dùng lệnh này để scan:

clamscan -d Clam_HelloWorld.ndb test.txt


Ubuntu - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu
test.txt (~/Desktop/Test) - gedit
15:28
Open
test.txt
~/Desktop/Test
Save
hello world
Ubuntu
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
3:28 PM
9/18/2018


Ubuntu - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu
Terminal
15:28
minhqk@minhqk: ~/Desktop/Test
minhqk@minhqk:~/Desktop/Test$ sudo gedit Clam_HelloWorld.ndb
** (gedit:25683): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
minhqk@minhqk:~/Desktop/Test$ sudo gedit ./test.txt
** (gedit:25701): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
minhqk@minhqk:~/Desktop/Test$ clamscan -d Clam_HelloWorld.ndb test.txt
test.txt: Clam_HelloWorld.UNOFFICIAL FOUND
----------- SCAN SUMMARY -----------
Known viruses: 1
Engine version: 0.100.0
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.009 sec (0 m 0 s)
minhqk@minhqk:~/Desktop/Test$
Ubuntu
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
3:28 PM
9/18/2018