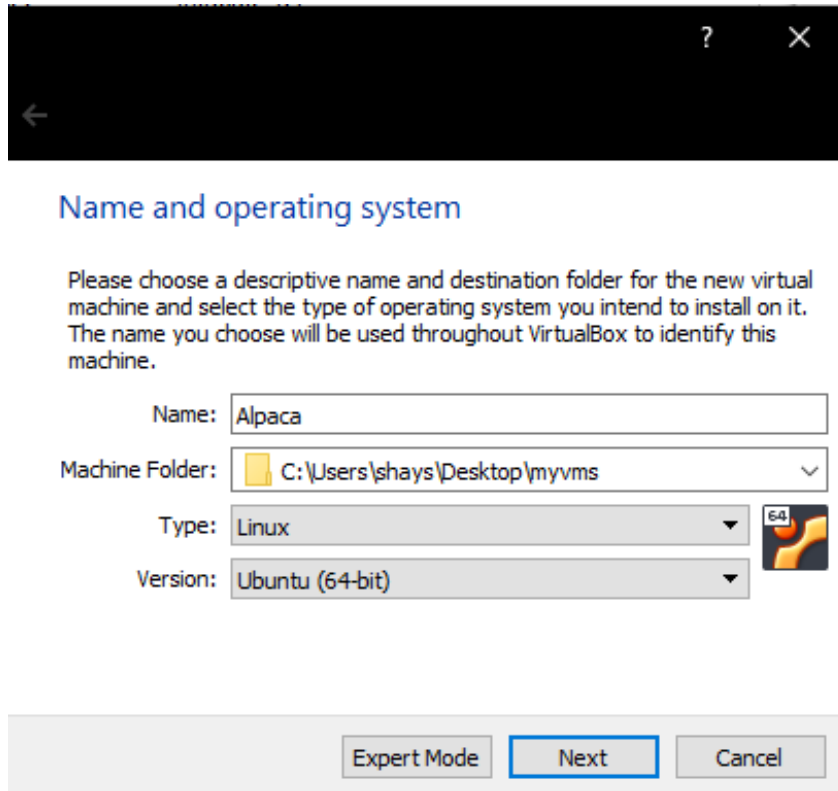


# COSC301 Assignment #3

## Step 1: Create a new Ubuntu 20.04 Client.



**Name and operating system**

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Machine Folder:

Type:

Version:

## Step 2: Enter sudo

sudo -i

## Step 3: Install Docker

### Set up docker repository

sudo apt-get update

```
sudo apt-get install \
    ca-certificates \
    curl \
    gnupg \
    lsb-release
```

```
sudo mkdir -p /etc/apt/keyrings
```

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
```

```
echo \
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu \
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

### Install docker engine

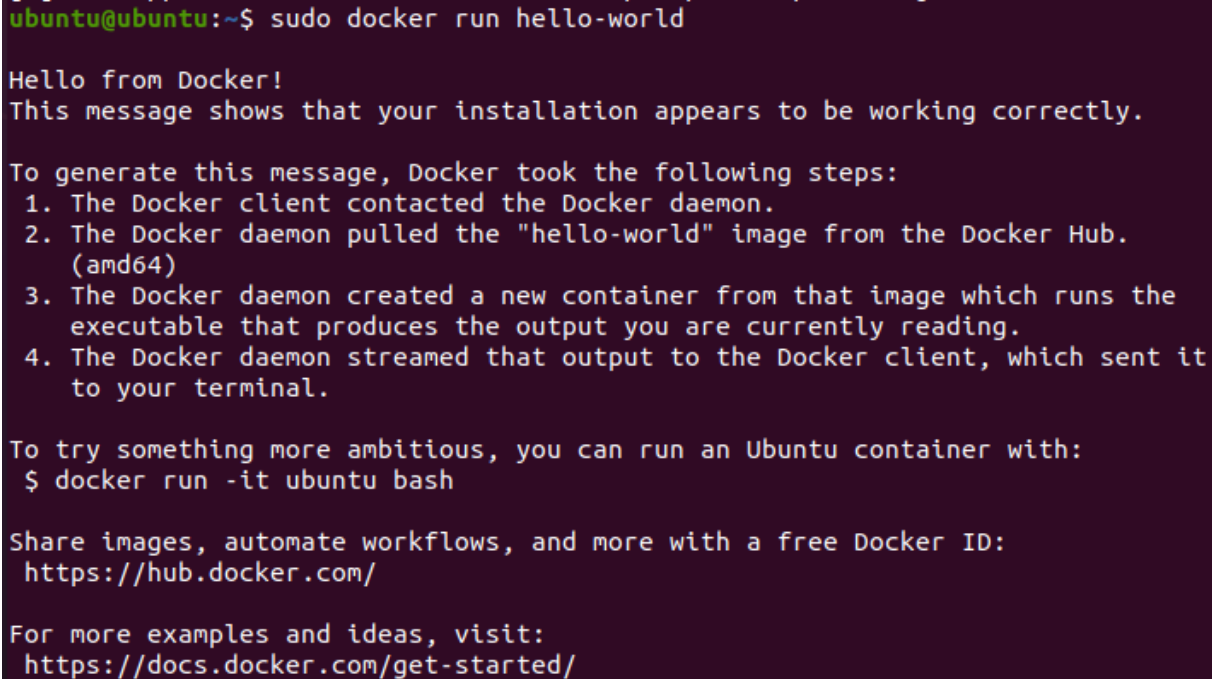
```
sudo apt-get update
```

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose-plugin
```

```
sudo apt-get install docker-ce=5:20.10.16~3-0~ubuntu-focal docker-ce-cli=5:20.10.16~3-0~ubuntu-focal  
containerd.io docker-compose-plugin
```

## Test docker

Sudo docker run hello-world

A terminal window with a dark purple background. The prompt is 'ubuntu@ubuntu:~\$'. The command 'sudo docker run hello-world' has been executed. The output is as follows:

```
ubuntu@ubuntu:~$ sudo docker run hello-world  
  
Hello from Docker!  
This message shows that your installation appears to be working correctly.  
  
To generate this message, Docker took the following steps:  
1. The Docker client contacted the Docker daemon.  
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.  
   (amd64)  
3. The Docker daemon created a new container from that image which runs the  
   executable that produces the output you are currently reading.  
4. The Docker daemon streamed that output to the Docker client, which sent it  
   to your terminal.  
  
To try something more ambitious, you can run an Ubuntu container with:  
$ docker run -it ubuntu bash  
  
Share images, automate workflows, and more with a free Docker ID:  
https://hub.docker.com/  
  
For more examples and ideas, visit:  
https://docs.docker.com/get-started/
```

## Step 4: Install python

```
apt-get install python3 python3-pip  
pip3 install docker-compose
```

## Step 5: Clone repository

```
Git clone https://github.com/RUB-NDS/alpaca-code.git
```

## Step 6: Run ./setup.sh

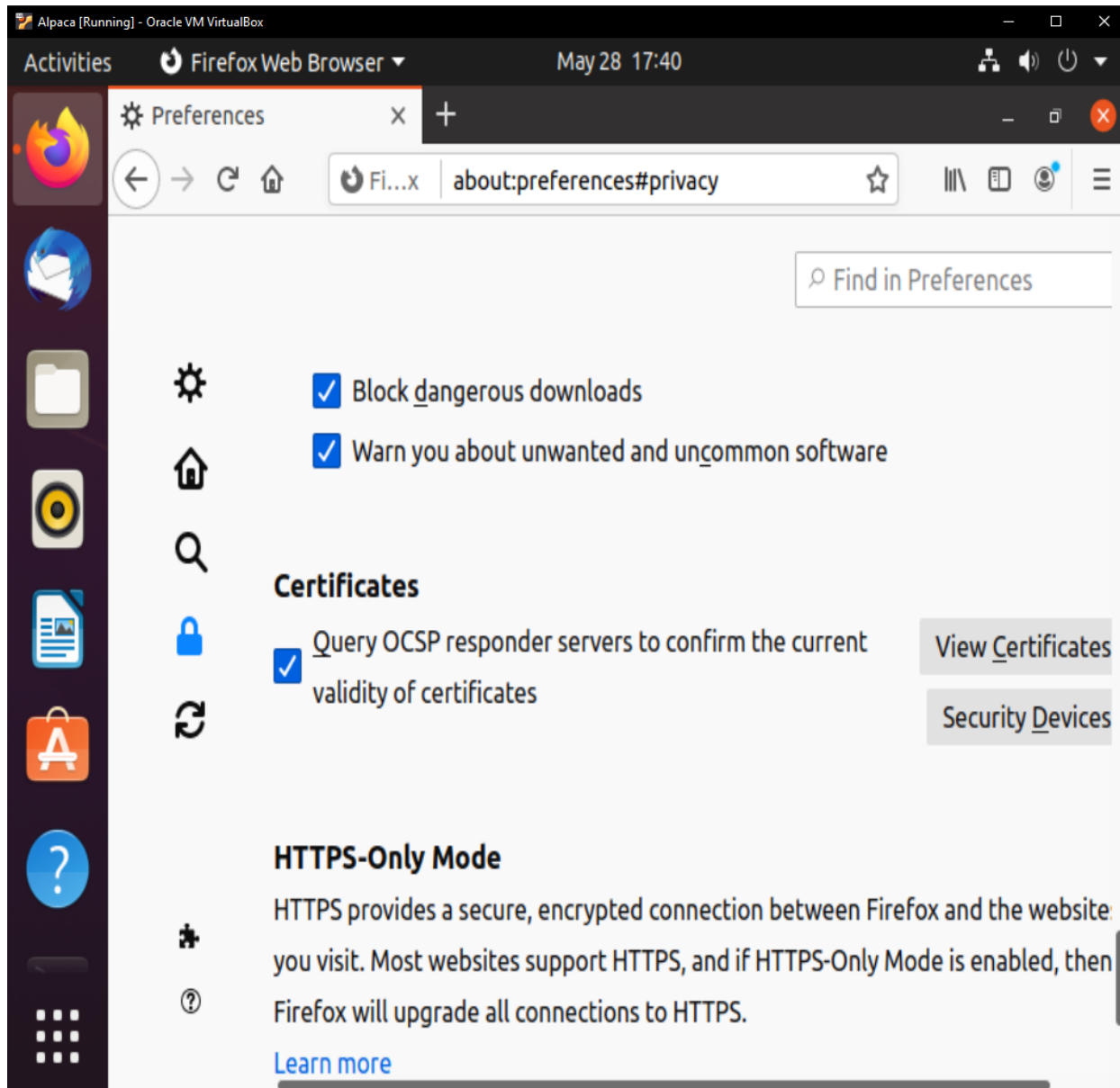
```
chmod +x setup.sh  
./setup.sh
```

## Step 7: Add ca.crt to firefox trusted CA's

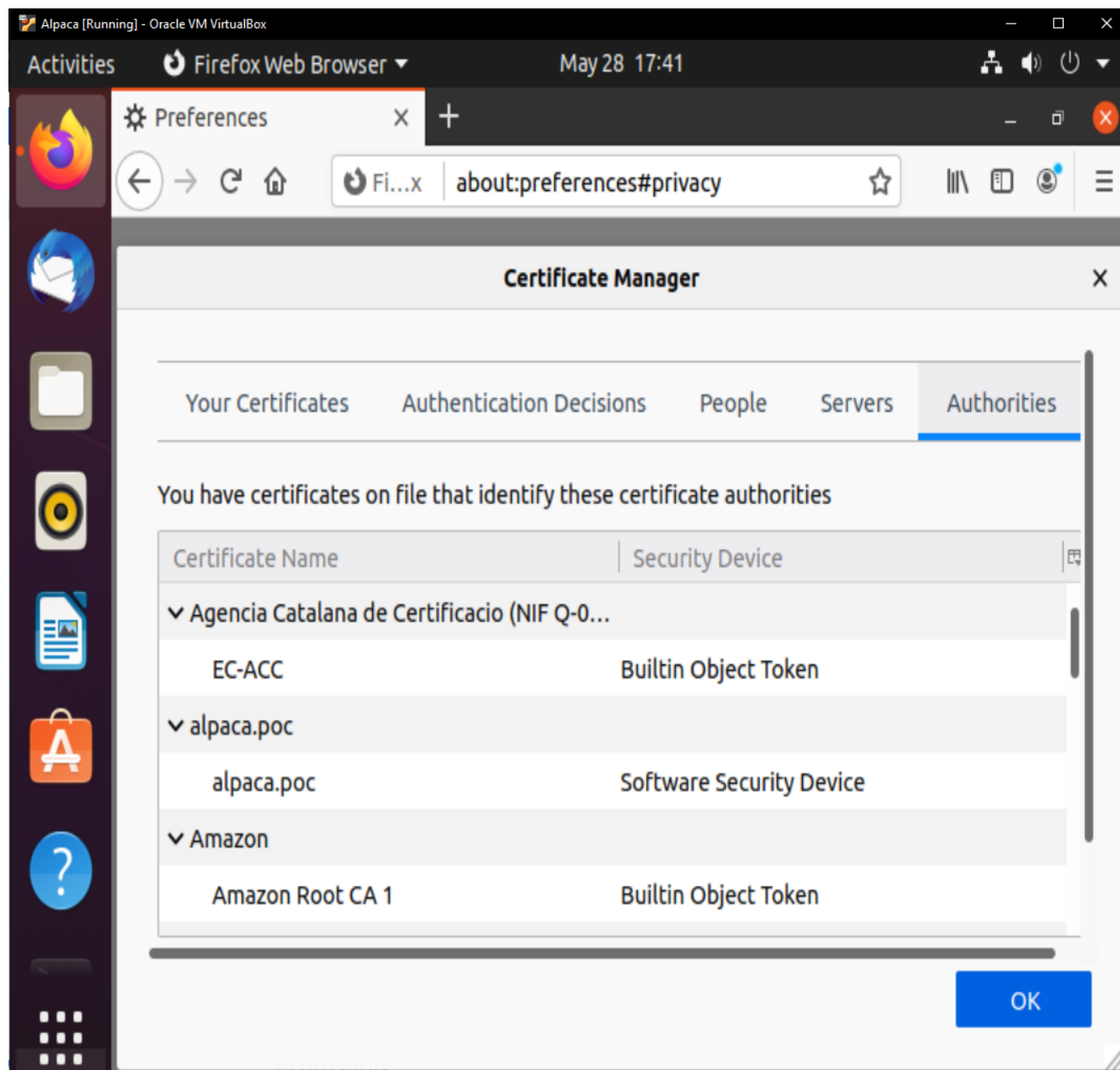
Copy ca.crt to user mal since firefox doesn't run with root and give permissions

```
cp ./pki/ca.crt /home/mal/  
chmod 775 /home/mal/ca.crt
```

To add ca.crt to firefox's trusted CA's go to firefox>preferences>padlock then scroll down and click "View Certificates"



Make sure you are in the “Authorities” tab and click “import” and select ca.crt just click both boxes and click ok



#### Step 8: Start docker (make sure you are in alpaca-code/testlab)

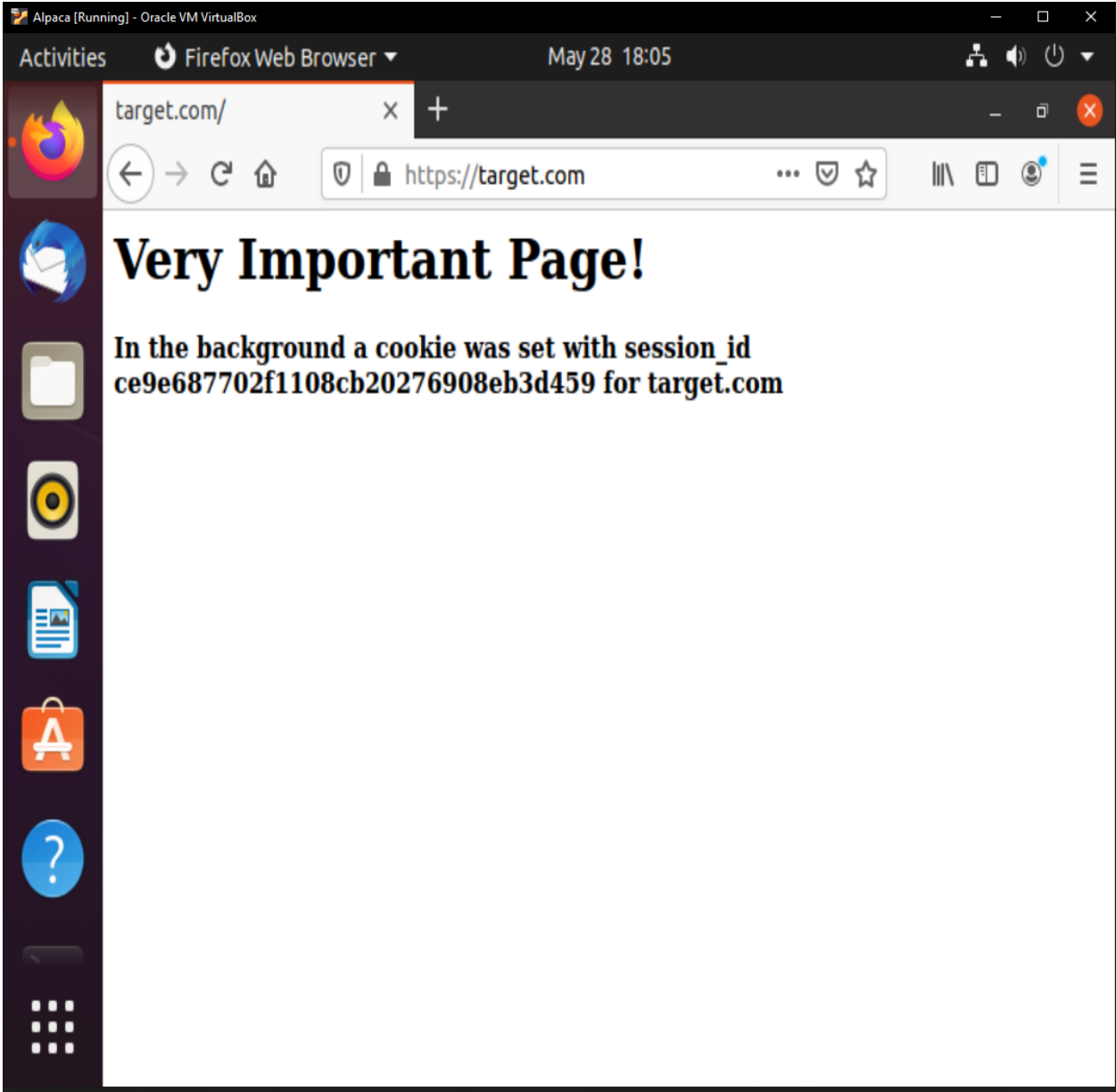
```
docker-compose -f servers/docker-compose.yml up -d nginx-target nginx-attacker vsftp
```

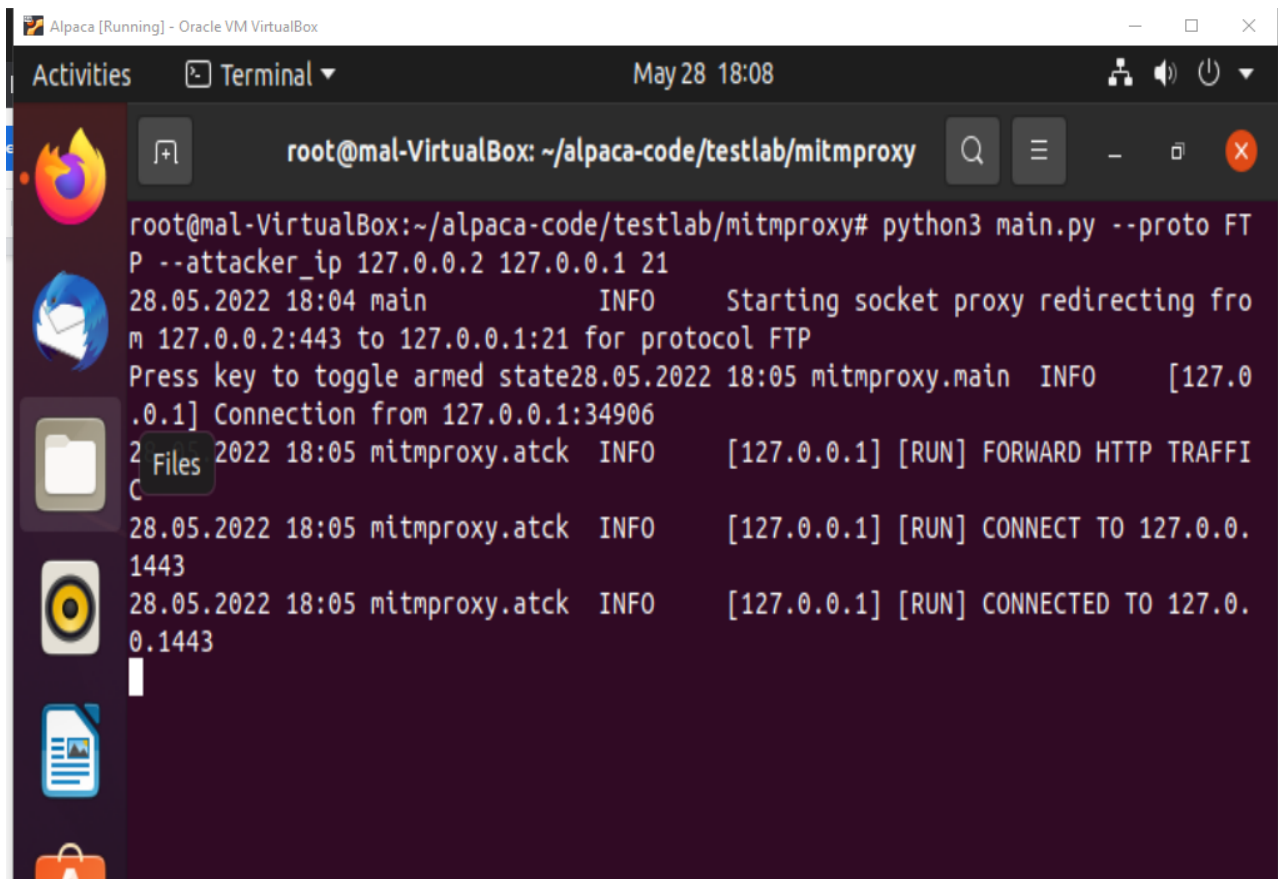
#### Step 9: Run the MitM-Proxy

```
cd mitmproxy
```

```
python3 main.py --proto FTP --attacker_ip 127.0.0.2 127.0.0.1 21
```

Proxy is now in unarmed mode visit <https://target.com>





```
root@mal-VirtualBox: ~/alpaca-code/testlab/mitmproxy# python3 main.py --proto FTP --attacker_ip 127.0.0.2 127.0.0.1 21
28.05.2022 18:04 main INFO Starting socket proxy redirecting from 127.0.0.2:443 to 127.0.0.1:21 for protocol FTP
Press key to toggle armed state28.05.2022 18:05 mitmproxy.main INFO [127.0.0.1] Connection from 127.0.0.1:34906
2022 18:05 mitmproxy.atck INFO [127.0.0.1] [RUN] FORWARD HTTP TRAFFIC
28.05.2022 18:05 mitmproxy.atck INFO [127.0.0.1] [RUN] CONNECT TO 127.0.0.1443
28.05.2022 18:05 mitmproxy.atck INFO [127.0.0.1] [RUN] CONNECTED TO 127.0.0.1443
```

Change Proxy to armed state

```
Press key to toggle armed state
28.05.2022 18:09 mitmproxy INFO ARMED STATE: True
Press key to toggle armed state
```

Go to <https://attacker.com>

