

Remediation Meta

61708 VNC Server 'password' Password

Per questa vulnerabilità mi sono loggato su MetaSploitable utilizzando i diritti di root mediante il comando SUDOSU, secondariamente ho utilizzato il comando **VNCPASSWD** per modificare la password problematica con una più sicura.

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# _
```

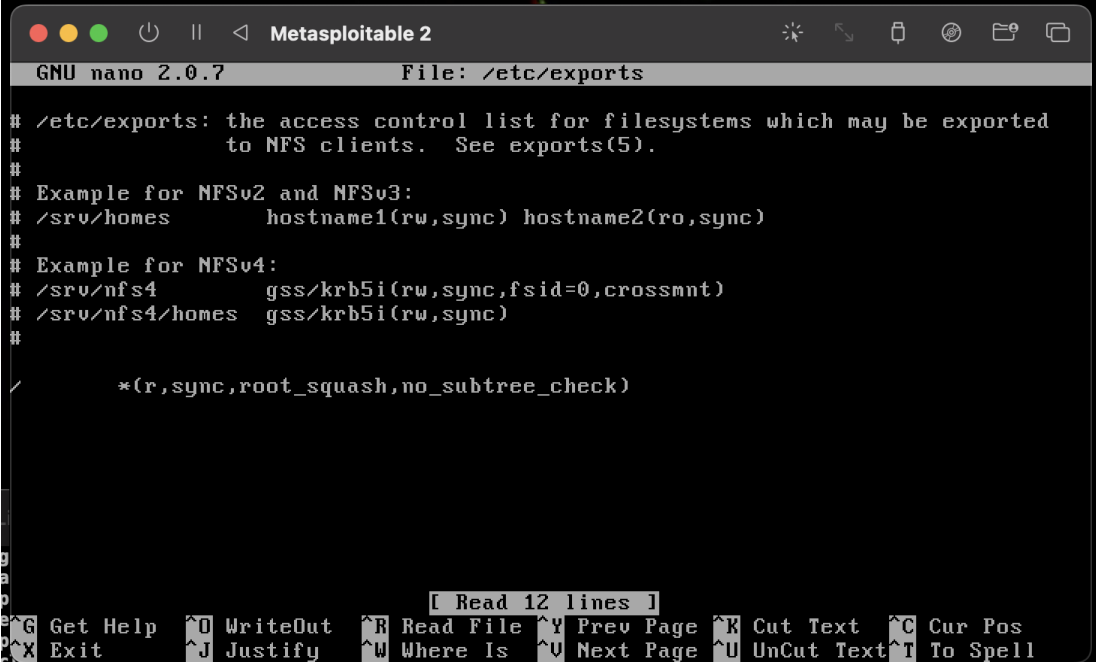
11356 NFS Exported Share Information Disclosure

Per questa vulnerabilità sempre dalla macchina Metasploitable2 ho eseguito il comando SUDO NANO /ETC/EXPORTS per accedere al file di configurazione NFS come qui di seguito

```
GNU nano 2.0.7 File: /etc/exports Modified

# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/*(rw,sync,no_root_squash,no_subtree_check)
```

Dopodichè ho modificato la dicitura "rw" in "r" e cambiando la dicitura "no_root_squash" in "root_squash" salvando il tutto come sotto mostrato.

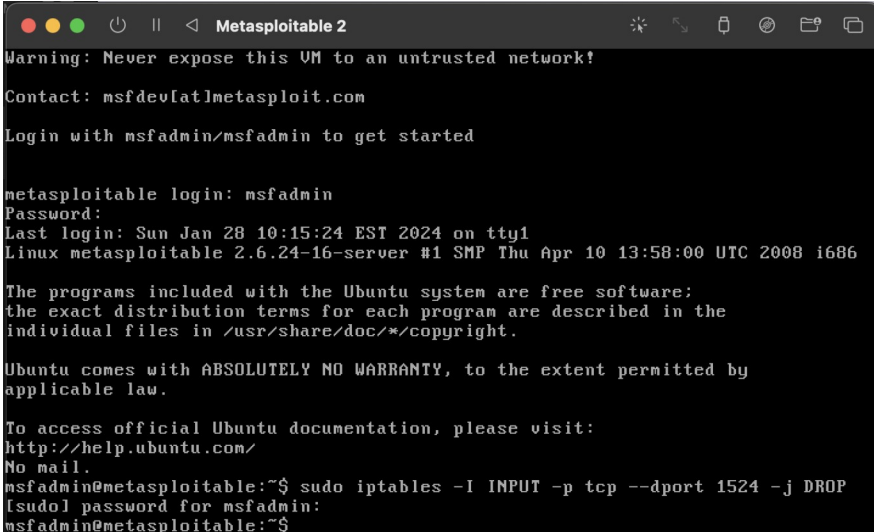


```
Metasploitable 2
GNU nano 2.0.7 File: /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw, sync) hostname2(ro, sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw, sync, fsid=0, crossmnt)
# /srv/nfs4/homes gss/krb5i(rw, sync)
#
*(r, sync, root_squash, no_subtree_check)
```

Infine ho riavviato la macchina con SUDO REBOOT

51998 Bind Shell Backdoor Detection

Per questa vulnerabilità ho eseguito il comando `sudo -I INPUT -p tcp --destination-port 1524 -j DROP` dove "1524" è la porta specificata da NESSUS come vulnerabile.



```
Metasploitable 2
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: Sun Jan 28 10:15:24 EST 2024 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:~$ sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```