

S5L5

- Adesso proviamo ad implementare le correzioni come prima siamo andati nella directory etc nel file exports ed abbiamo abilitato una whitelist degli host che possono accedere al NFS specificando l'ip di meta 192.168.50.101

```
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)
#
/mnt/newdisk      192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

ADESSO INVECE NELLA VOCE **VNC** SEGUENDO IL PERCORSO HOME/MSFADMIN SIAMO ANDATI AD INSERIRE UNA PASSWORD ALFANUMERICA

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
```

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# cd
root@metasploitable:~# ls -A
.bash_history  .filezilla  .gstreamer-0.10  reset_logs.sh  vnc.log
.bashrc        .fluxbox    .mozilla         .rhosts        .Xauthority
.config        .gconf      .profile         .ssh
Desktop        .gconfd     .purple          .vnc
root@metasploitable:~# cd .vnc
bash: cd .vnc: command not found
root@metasploitable:~# cd .vnc
root@metasploitable:~/vnc# ls
metasploitable:0.log  metasploitable:1.log  passwd
metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/vnc#
```

NESSUS HA TROVATO LA BINDSHELL BACKDOOR SULLA PORTA 1524 DI CONSEGUENZA ABBIAMO INSERITO UNA REGOLA FIREWALL CHE CHIUDE LA COMUNICAZIONE CON IL COMANDO DENY SULLA PORTA TCP ED UDP

```
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 su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To          Action From
--          -
1524:tcp    DENY  Anywhere
1524:udp    DENY  Anywhere

root@metasploitable:/home/msfadmin# _
```

IN FINALE ABBIAMO RISOLTO CON UNA REGOLA FIREWALL NEGARE LE COMUNICAZIONI SULLE PORTE 445 E 139 PERCHÉ LA CONNESSIONE AD INTERNET POTREBBE ESSERE TROPPO RISCHIOSA

```
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To
--
1524:tcp          DENY    Anywhere
1524:udp          DENY    Anywhere

root@metasploitable:/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:/home/msfadmin# ufw deny 139
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To
--
1524:tcp          DENY    Anywhere
1524:udp          DENY    Anywhere
445:tcp           DENY    Anywhere
445:udp           DENY    Anywhere
139:tcp           DENY    Anywhere
139:udp           DENY    Anywhere

root@metasploitable:/home/msfadmin# _
```