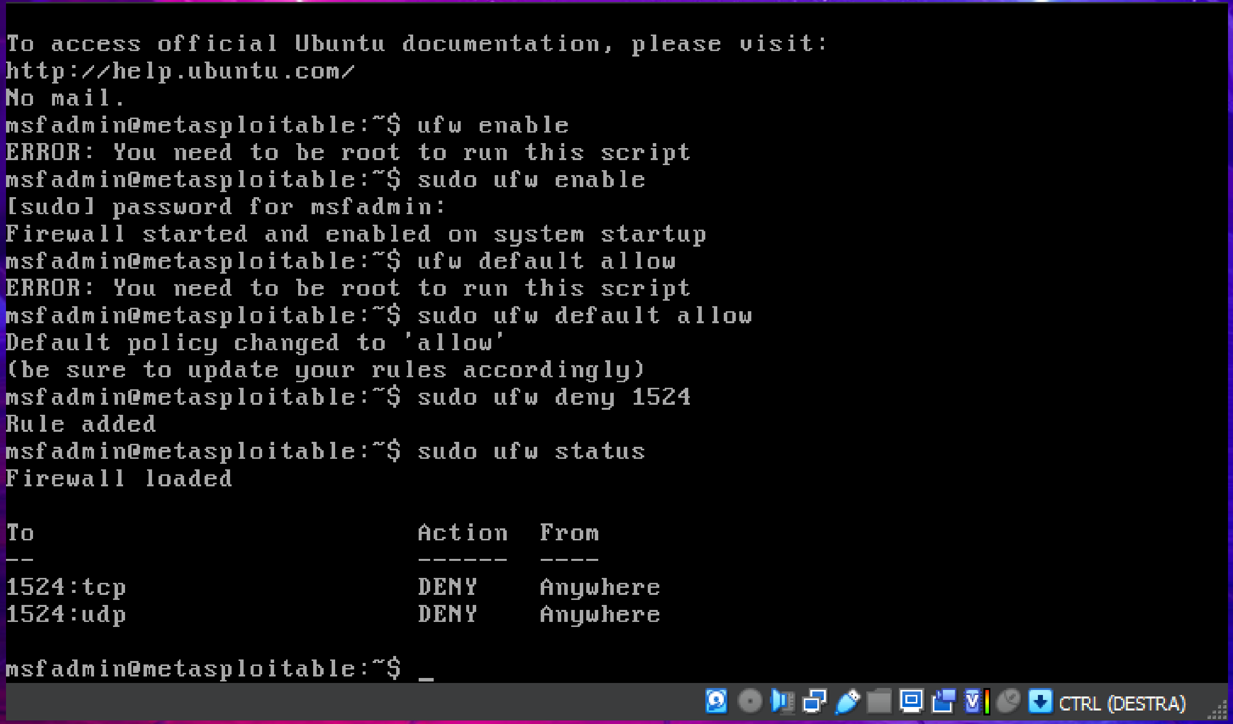
Amedeo Natalizi

PROGETTO S5/L5

Spiegazione dei passaggi della remediation

BIND SHELL BACKDOOR DETECION

CI È STATA SEGNALATA UNA POSSIBILE PRESENZA DI BACKDOOR SULLA PORTA 1524. SONO QUINDI INTERVENUTO ENTRANDO NELLE IMPOSTAZIONI DEL FIREWALL E ANDANDO AD IMPOSTARE LE REGOLE DI DEFAULT PER LA PORTA.



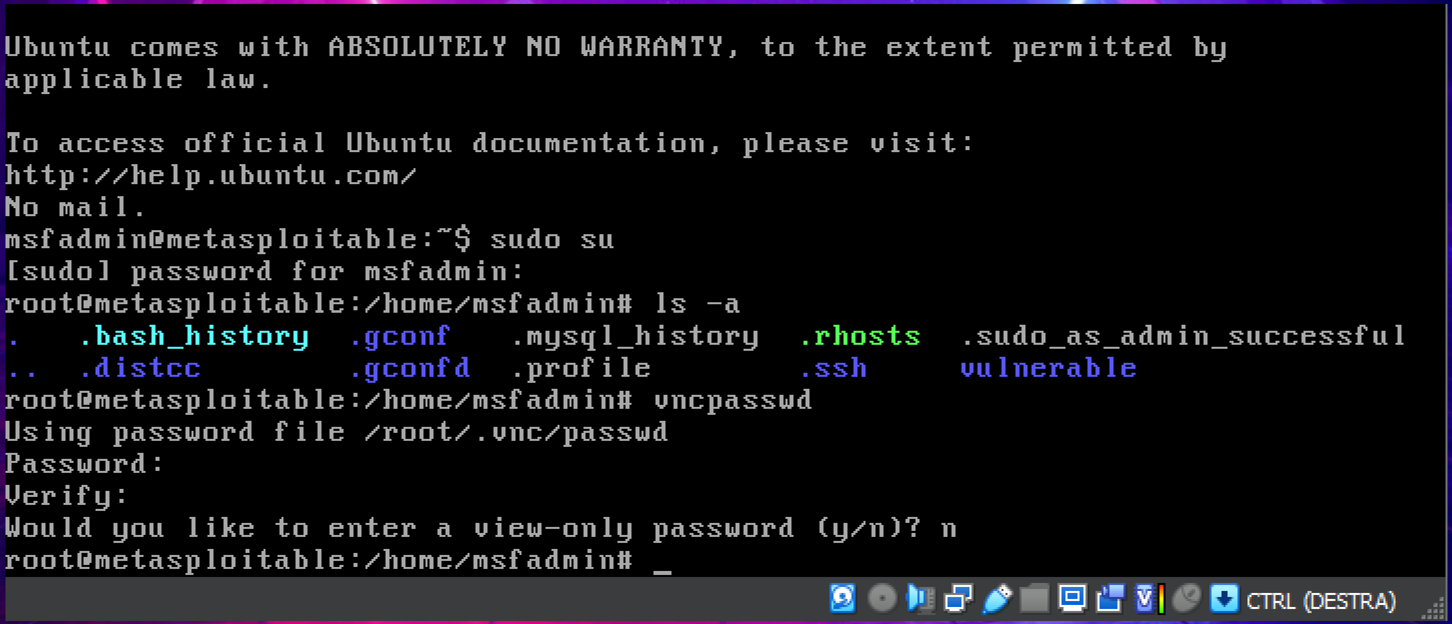
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ufw enable
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ ufw default allow
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

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

msfadmin@metasploitable:~$ _
```

VNC SERVER <PASSWORD> PASSOWRD

PASSWORD TROPPO DEBOLE RILEVATA PER IL SERVER VNC. MI SONO OCCUPATO DI INSERIRE UNA PASSWORD PIÙ SICURA CON CARATTERI ALFANUMERICI

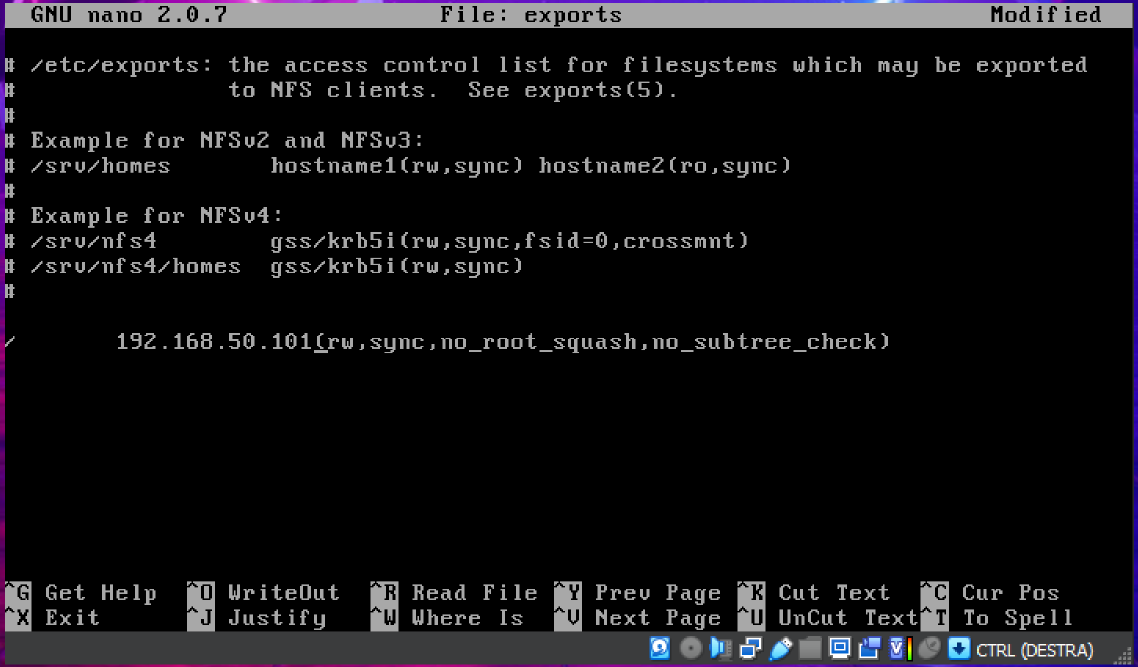


```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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# ls -a
.   .bash_history  .gconf   .mysql_history  .rhosts  .sudo_as_admin_successful
..  .distcc        .gconfd  .profile        .ssh     vulnerable
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# _
```

NFS EXPORTED SHARE INFORMATION DISCLOSURES

ACCESSO AL NFS TROPPO VULNERABILE. HO MODIFICATO GLI ACCESSI CONSENTENDOLI SOLO ALLA MACCHINA LINUX ANDANDO A MODIFICARE IL FILE EXPORTS



```
  GNU nano 2.0.7                File: 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)
#


/       192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```