

REMEDIATION DELLE VULNERABILITA'

Vulnerabilità risolte:

- NFS Exported Share Information Disclosure
- Bind Shell Backdoor Detection
- VNC server 'password' Password

1. NFS Exported Share Information Disclosure

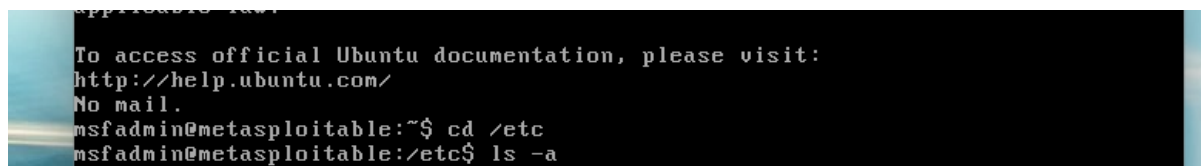
Per quanto riguarda la prima vulnerabilità, la remediation da applicare è quella di inserire all'interno della sottocartella del root “/etc”.

Come primo passo si visualizza l'interno delle sottocartelle del root con il comando “ls -a”.

Si cerca la directory “/etc” e si apre il file “exports”.

All'interno di questo file si modifica l'* in fondo alla pagina, inserendo l'IP della nostra macchina Metasploitable.

Una volta fatto si riavvia la macchina.



```
msfadmin@metasploitable:~$ cd /etc
msfadmin@metasploitable:/etc$ ls -a
```

The screenshot shows a terminal window with a black background and white text. The prompt is 'msfadmin@metasploitable:~\$'. The user enters 'cd /etc' and the prompt changes to 'msfadmin@metasploitable:/etc\$'. Then the user enters 'ls -a'.

Meta5 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
distcc
dpkg
e2fsck.conf
emacs
environment
esound
event.d
exports
fdmount.conf
firefox-3.0
fonts
fstab
ftpchroot
ftputils
fuse.conf
gai.conf
gconf
gdm
groff
group
group-
grub.d
gshadow
gshadow-
msfadmin@metasploitable:/etc$ sudo nano exports
```

mailname
manpath.config
mediaprm
menu
menu-methods
mime.types
mke2fs.conf
modprobe.d
modules
motd
motd.tail
mtab
mysql
nanorc
network
networks
nsswitch.conf
opt
pam.conf
pam.d
pango
passwd
passwd-
pcmcia

sudoers
su-to-rootrc
sysctl.conf
syslog.conf
terminfo
timezone
tomcat5.5
ucf.conf
udev
ufw
unreal
updatedb.conf
update-manager
vim
vsftpd.conf
w3m
wgetrc
wpa_supplicant
X11
xinetd.conf
xinetd.d
zsh_command_not_found

CTRL (DESTRA)

Meta5 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7 File: 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)
#
/mnt/newdisk 192.168.1.101(rw,sync,no_root_squash,no_subtree_check)
```

[Read 12 lines]

Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell

CTRL (DESTRA)

2. Bind Shell Backdoor Detection

Per risolvere questa vulnerabilità si deve abilitare il firewall di Metasploitable con il comando “ufw enable”.

Successivamente il firewall deve acconsentire a tutte le regole di default e si utilizza il comando “ufw default allow”.

Finito ciò si riavvia la macchina.

```
Meta5 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
--bash: d: command not found
msfadmin@metasploitable:/etc$ cd ..
msfadmin@metasploitable:/$ UFW ENABLE
--bash:UFW: command not found
msfadmin@metasploitable:/$ sudo UFW ENABLE
[sudo] password for msfadmin:
sudo: UFW: command not found
msfadmin@metasploitable:/$ sudo ufw enable
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

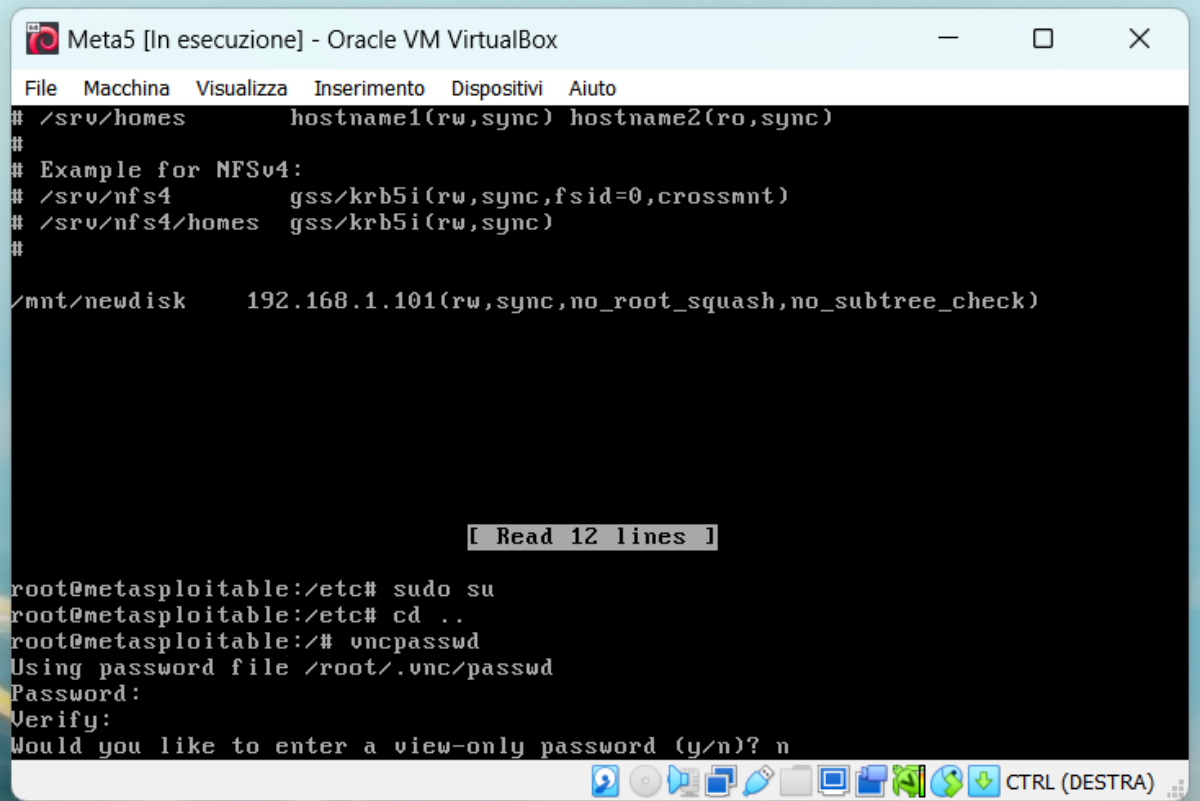
msfadmin@metasploitable:/$ _
```

3. VNC Server 'password' Password

Si deve modificare la password del VNC Server.

Per fare ciò si utilizza il comando “vncpasswd” e si cambia la password, scegliendone una più robusta e di massimo 8 caratteri.

Dopodiché si riavvia la macchina.



```
Meta5 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
# /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      192.168.1.101(rw, sync, no_root_squash, no_subtree_check)

[ Read 12 lines ]

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