

```
metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

/etc/X11/rgb
root      4645   0.0   0.0   2724  1188  ?      S    08:51   0:00 /bin/sh /root/.
vnc/xstartup
msfadmin  4746   0.0   0.7  17372 15528 tty1    S    08:53   0:00 Xtightvnc :1 -d
esktop X -auth /home/msfadmin/.Xauthority -geometry 1024x768 -depth 24 -rfbwait
120000 -rfbauth /home/msfadmin/.vnc/passwd -rfbport 5901 -fp /usr/X11R6/lib/X11/
fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/us
r/X11R6/lib/X11/fonts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X
11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/font
s/X11/100dpi/ -co /etc/X11/rgb
msfadmin  4804   0.0   0.0   3004   752 tty1    R+   09:00   0:00 grep vnc
msfadmin@metasploitable:~$ sudo kill -9 4637
msfadmin@metasploitable:~$ sudo kill -9 4645
msfadmin@metasploitable:~$ sudo kill -9 4746
msfadmin@metasploitable:~$ sudo kill -9 4804
msfadmin@metasploitable:~$ vncserver :1

Warning: metasploitable:1 is taken because of /tmp/.X1-lock
Remove this file if there is no X server metasploitable:1
A VNC server is already running as :1
msfadmin@metasploitable:~$ sudo ls-l ~/.vnc/passwd
sudo: ls-l: command not found
msfadmin@metasploitable:~$ sudo ls -l ~/.vnc/passwd
-rw----- 1 msfadmin msfadmin 16 2024-07-28 08:26 /home/msfadmin/.vnc/passwd
msfadmin@metasploitable:~$ _
```

VNC PASSWORD

Per rimuovere la vulnerabilità abbiamo rimosso tutti i processi con la vecchia password. In seguito creato una nuova password con il comando `vncpasswd` e fatto ripartire il server con il comando `vncserver :1`

```
metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

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)
#
# 192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

[ Read 14 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

NFS Exported Share Information Disclosure

Per rimuovere la vulnerabilità abbiamo rimosso l'* che permetteva l'accesso a qualsiasi host

modificandolo e inserendo l'IP della macchina in modo tale da avere come unico host la macchina stessa

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
-bash: grep:1524: command not found
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4458/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4458/exe
lrwxrwxrwx 1 root root 0 2024-07-28 09:50 /proc/4458/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ sudo rm -f /usr/sbin/xinetd
```

Bind Shell Backdoor Detection

Una volta trovata la backdoor tramite il comando nmap -p con il range di porte da 0-65535 con il nome ingresslock porta1524(la porta era indicata anche sul report).

Con il comando sudo netstat -tulnp | grep :1524 abbiamo trovato il file xinetd con il PID4458

Poi con sudo ls -l /proc/PID processo/exe abbiamo trovato il path del file

con il comando sudo rm -f (-f su meta) abbiamo eliminato il file come in figura