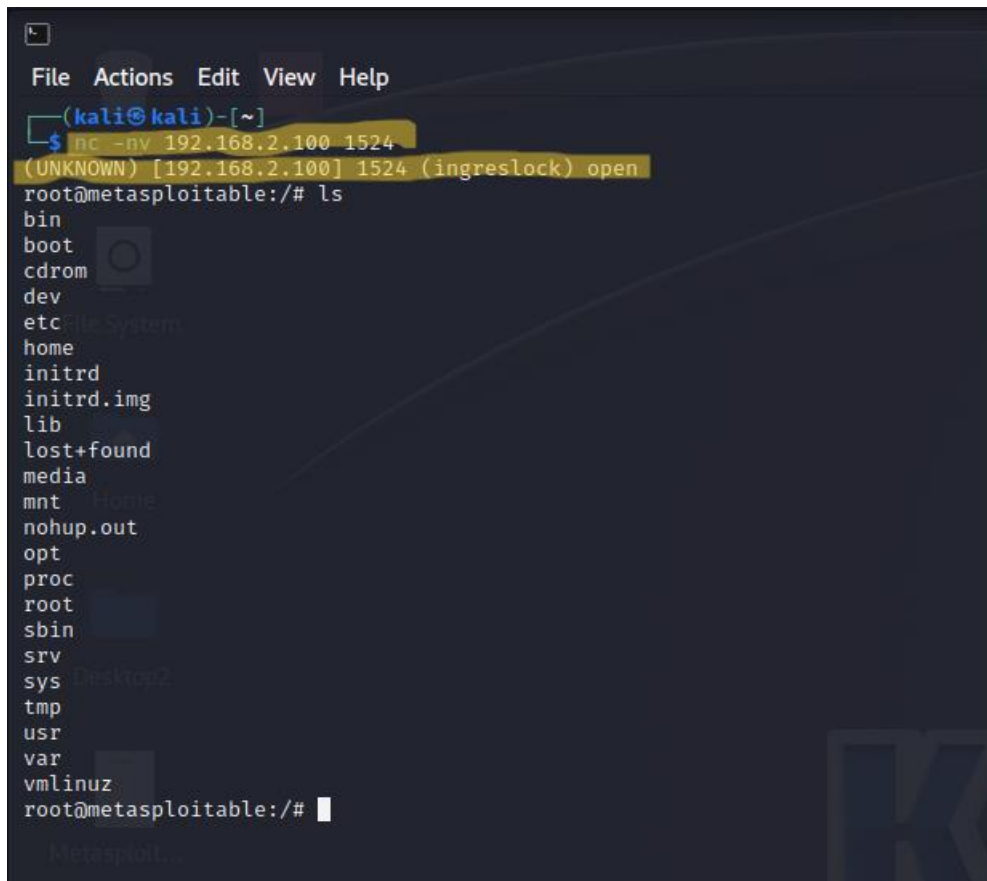


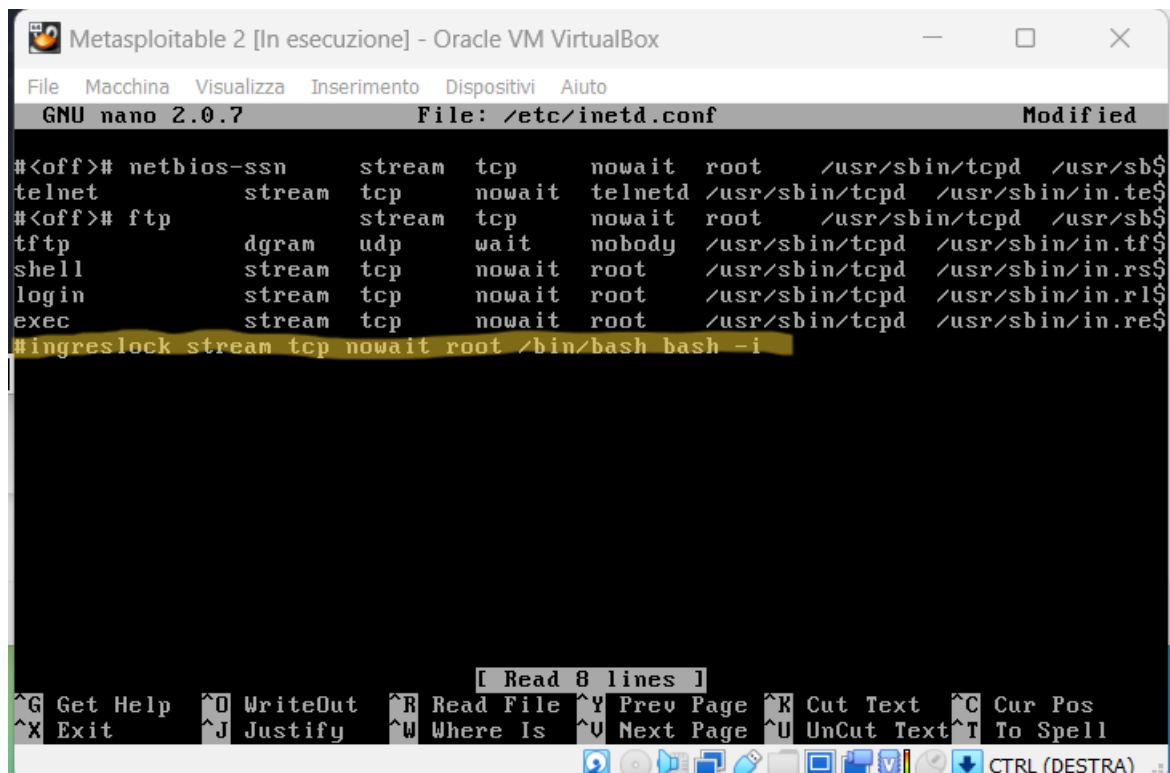
## 1) Bind Shell Backdoor Detection

Questa vulnerabilità era in grado di far accedere un terzo e permetteva ad esso di utilizzare la shell della macchina in remoto tramite Backdoor aperta nella porta 1524.



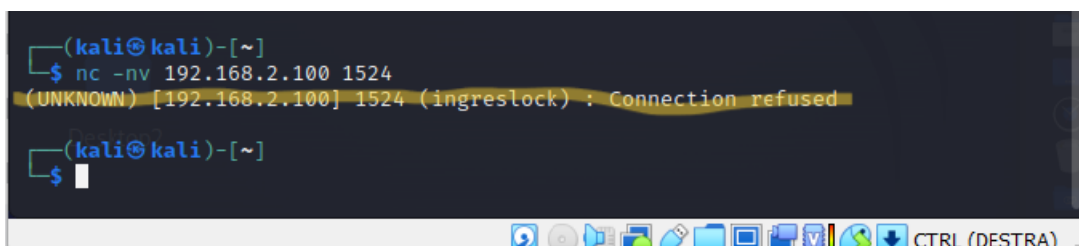
The screenshot shows a terminal window with a menu bar (File, Actions, Edit, View, Help) and a title bar. The prompt is `(kali@kali)-[~]`. The user enters `$ nc -nv 192.168.2.100 1524`. The response is `(UNKNOWN) [192.168.2.100] 1524 (ingreslock) open`. The prompt changes to `root@metasploitable:/#`. The user enters `ls`, and the output lists the following directories and files: `bin`, `boot`, `cdrom`, `dev`, `etc`, `home`, `initrd`, `initrd.img`, `lib`, `lost+found`, `media`, `mnt`, `nohup.out`, `opt`, `proc`, `root`, `sbin`, `srv`, `sys`, `tmp`, `usr`, `var`, `vmlinux`. The prompt returns to `root@metasploitable:/#`.

La correzione di tale vulnerabilità CRITICA è stata operata tramite la modifica del file `inetd.conf` così come da immagine, andando a far divenire un commento la riga `ingreslock`.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf Modified
#<off># netbios-ssn      stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet      stream  tcp    nowait  telnetd  /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp       dgram   udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tf$
shell      stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login      stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec       stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
#ingreslock stream tcp nowait root /bin/bash bash -i
```

Come prova della riuscita effettiva della modifica, tramite kali cerchiamo di connetterci alla macchina tramite la precedente backdoor, con risultato NEGATIVO.

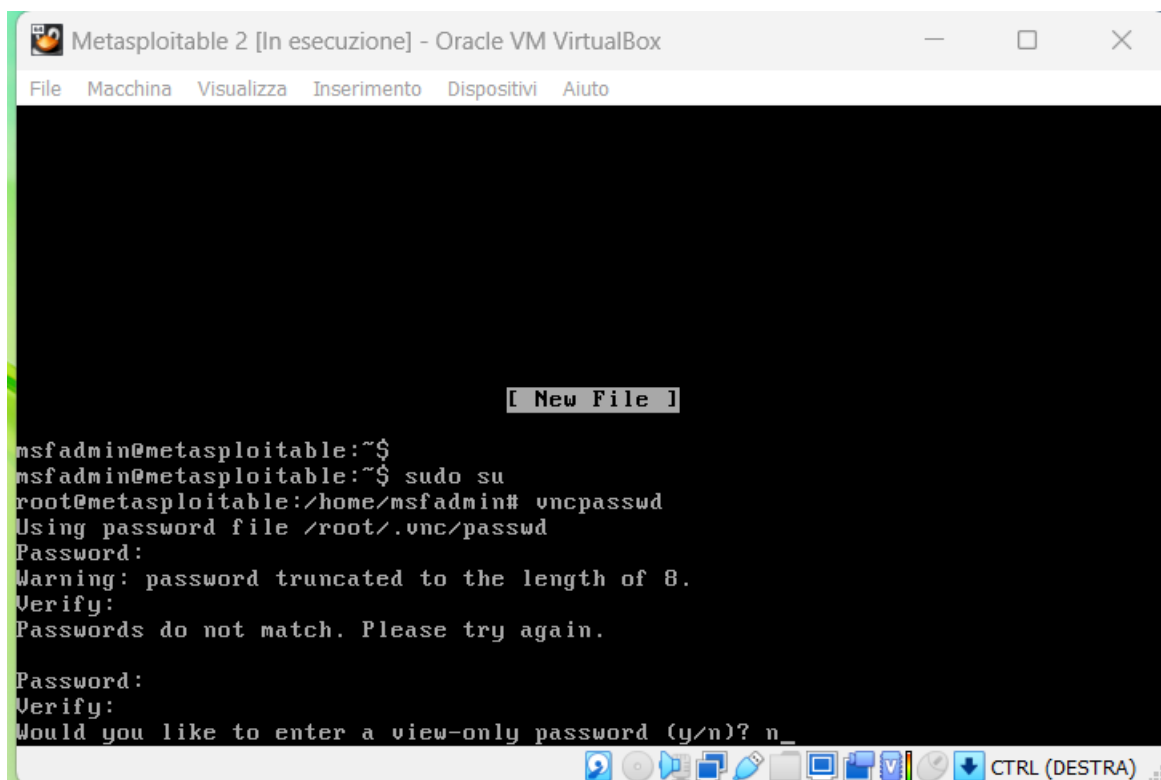


```
(kali@kali)-[~]
$ nc -nv 192.168.2.100 1524
(UNKNOWN) [192.168.2.100] 1524 (ingreslock) : Connection refused
(kali@kali)-[~]
$
```

## 2) VNC server "password" password

Per tale vulnerabilità, anch'essa critica, ci siamo mossi per la modifica della password di accesso tramite root, utilizzando o il comando sudo su per divenire root o utilizzando il solito comando sudo.

Fatto ciò, abbiamo cambiato la password tramite il comando vncpasswd.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

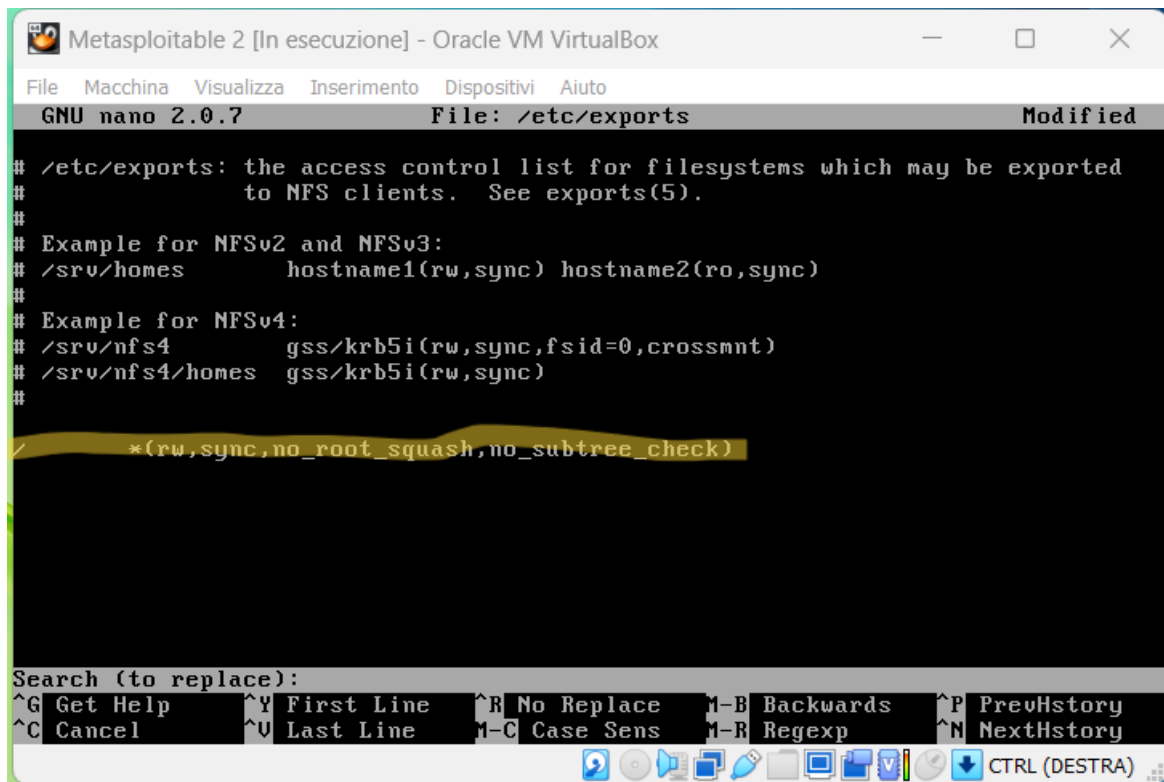
[ New File ]

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? n_
CTRL (DESTRA)
```

### 3) NFS Exported Share Information Disclosure

Per eliminare tale vulnerabilità abbiamo proceduto ad entrare all'interno del file `/etc/exports` per trovare la riga di comando incriminata, in questo caso, l'unica non commentata.



Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7 File: /etc/exports Modified

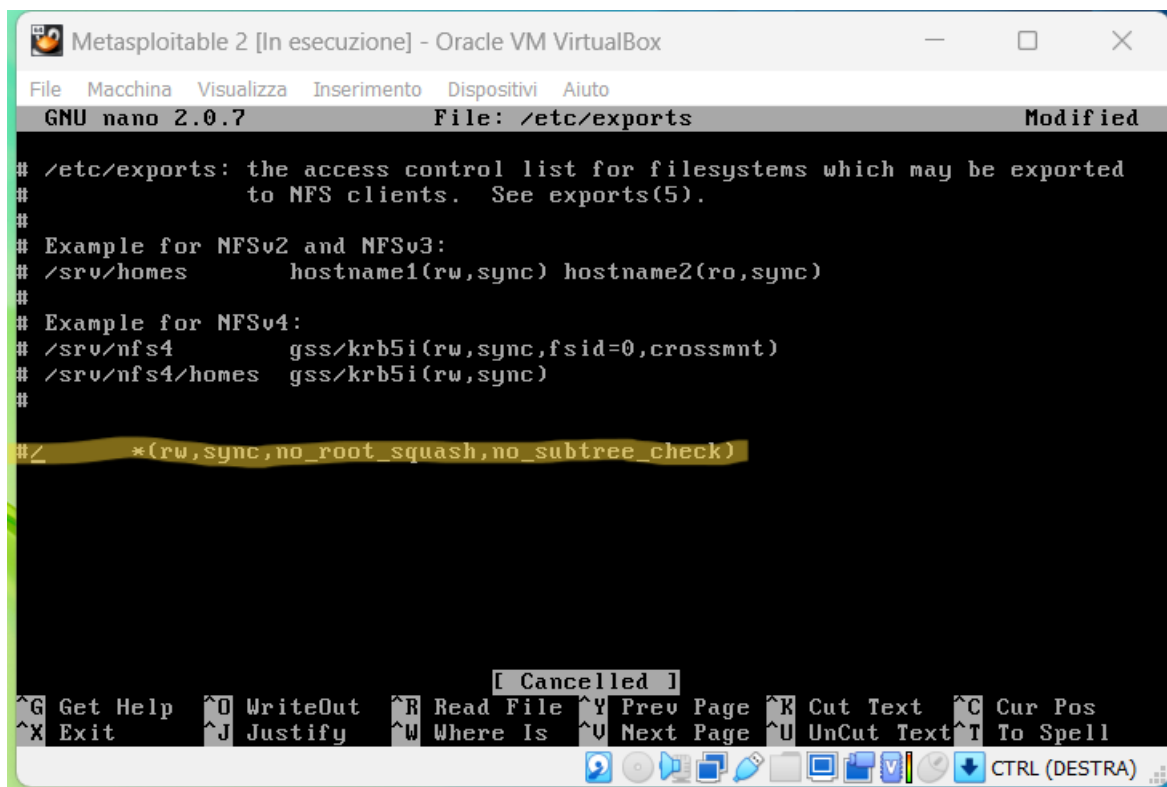
```
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw, sync) hostname2(ro, sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw, sync, fsid=0, crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,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

Search (to replace):

^G Get Help	^Y First Line	^R No Replace	^M-B Backwards	^P PrevHistory
^C Cancel	^V Last Line	^M-C Case Sens	^M-R Regexp	^N NextHistory

CTRL (DESTRA)

Una volta trovata la riga, si procede al commentarla.



Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7 File: /etc/exports Modified

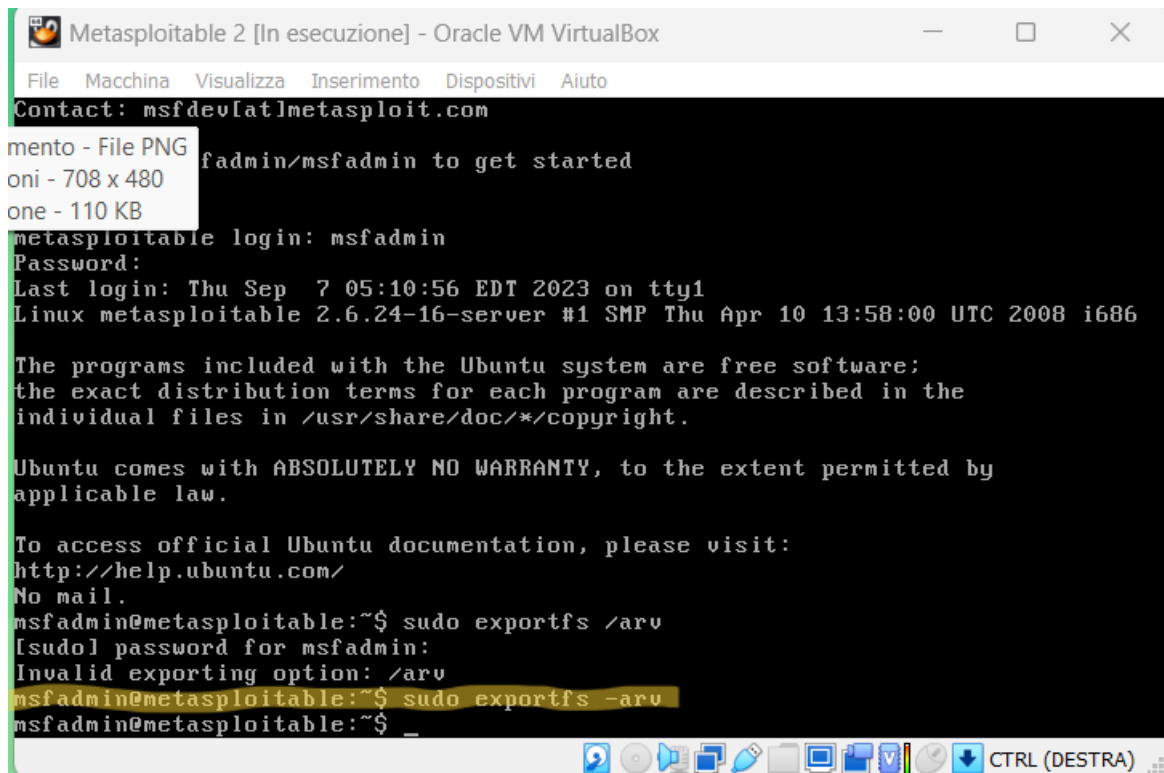
```
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw, sync) hostname2(ro, sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw, sync, fsid=0, crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,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

[ Cancelled ]

^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

CTRL (DESTRA)

Tramite questa procedura adesso avremo risolto la criticità.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Contact: msfdev[at]metasploit.com
mento - File PNG
oni - 708 x 480
one - 110 KB
metasploitable login: msfadmin
Password:
Last login: Thu Sep  7 05:10:56 EDT 2023 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 exportfs /arv
[sudo] password for msfadmin:
Invalid exporting option: /arv
msfadmin@metasploitable:~$ sudo exportfs -arv
msfadmin@metasploitable:~$ _
```

Come si può notare dallo screen.