

## REMEDIATION METASPLOITABLE

Durante una prima scansione del sistema metasploitable vengono scoperte diverse vulnerabilità critiche , delle quali ne verranno prese in esame solo alcune.

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

La prima presa in esame è :

Bind Shell Backdoor Detection

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
----------	-----	---	-------	-------------------------------

Questa criticità indica un servizio in ascolto su una porta remota senza autenticazione; al fine di risolvere questa vulnerabilità basta modificare il file

## inetd.conf

```
GNU nano 2.0.7      File: inetd.conf

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
telnet               stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
tftp                 dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
ingreslock stream tcp nowait root /bin/bash bash -i
```

Andando ad eliminare l'ultima stringa presente

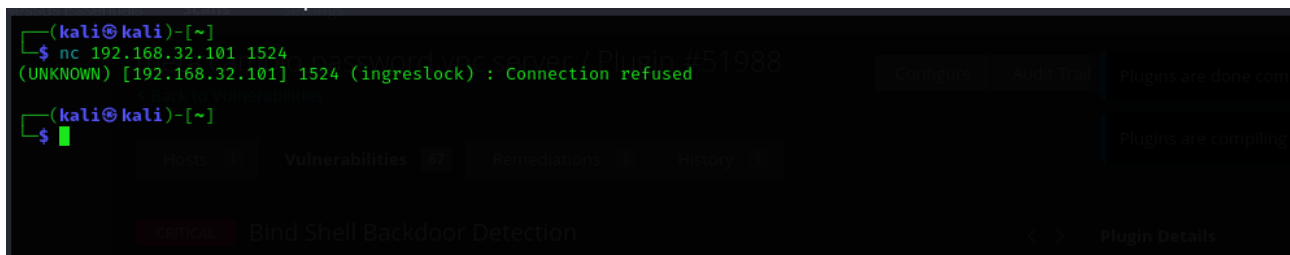
Ingreslock stream tcp nowait root /bin/bash bash -i

```
GNU nano 2.0.7      File: inetd.conf      Modified

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
telnet               stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
tftp                 dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
-
```

Facendo una prova da un altro client vedremo che non sarà più possibile connettersi alla porta 1524

```
(kali@kali)-[~]
$ nc 192.168.32.101 1524
(UNKNOWN) [192.168.32.101] 1524 (ingreslock) : Connection refused
(kali@kali)-[~]
$
```



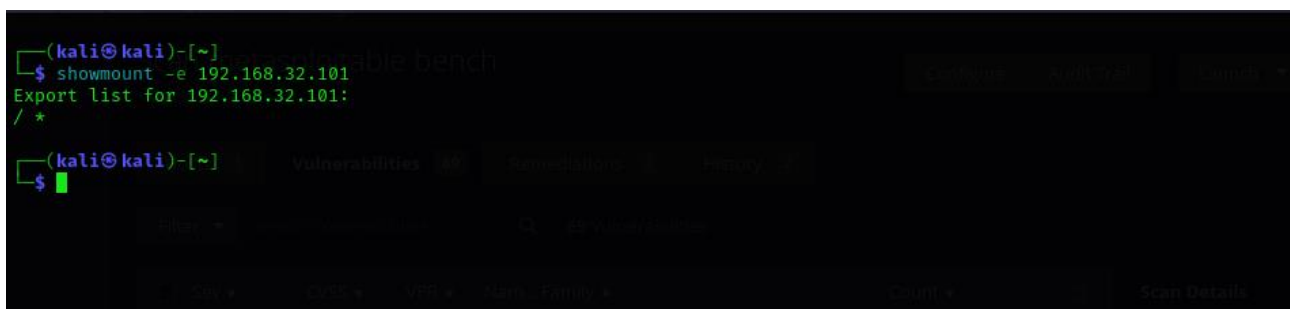
La seconda vulnerabilità presa in esame è

## NFS Exported Share Information Disclosure

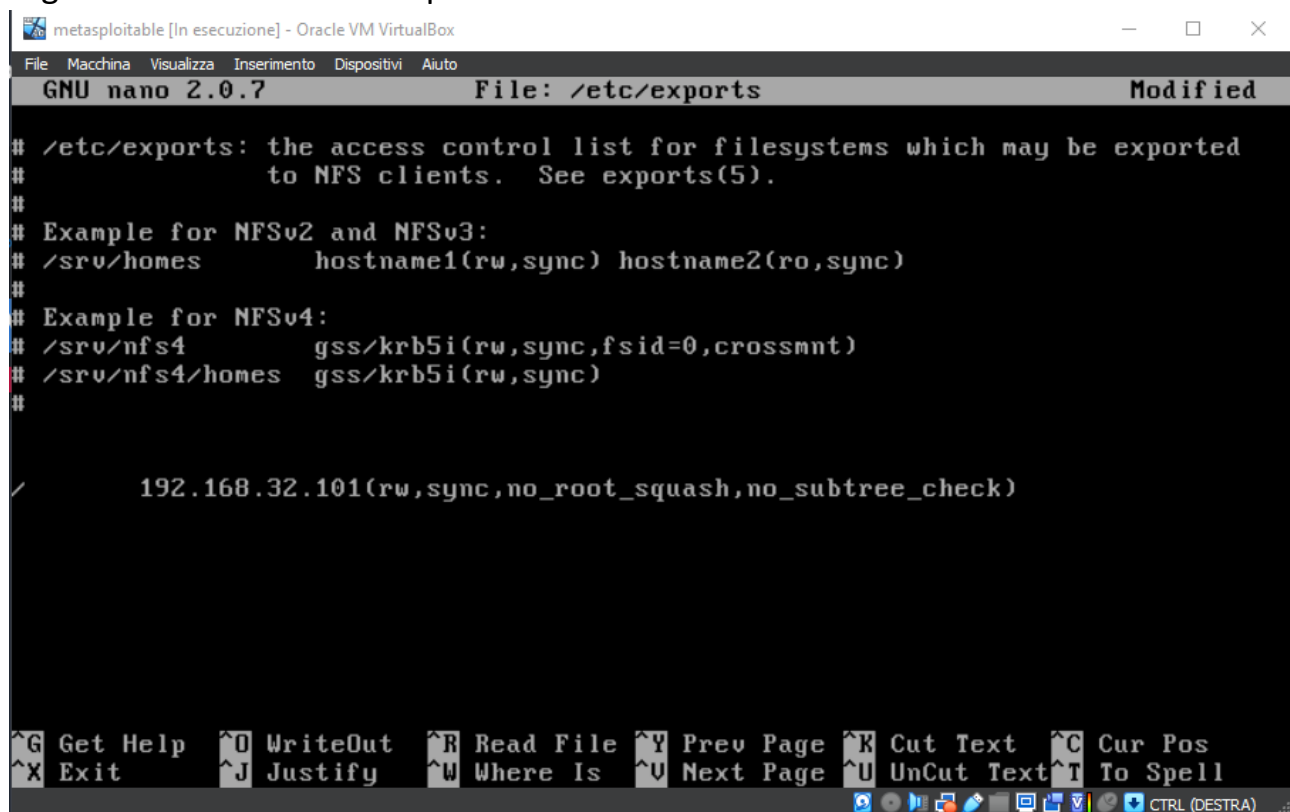
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
----------	-------	---	-------	---

Questa criticità indica che le condivisioni NFS esportate dal server remoto potrebbero essere “montate” da un host in scansione senza richiesta di autorizzazioni.

```
(kali@kali)-[~]
$ showmount -e 192.168.32.101
Export list for 192.168.32.101:
/ *
```



Per modificare i permessi basta semplicemente modificare il file /etc/exports togliendo l'accesso a chiunque



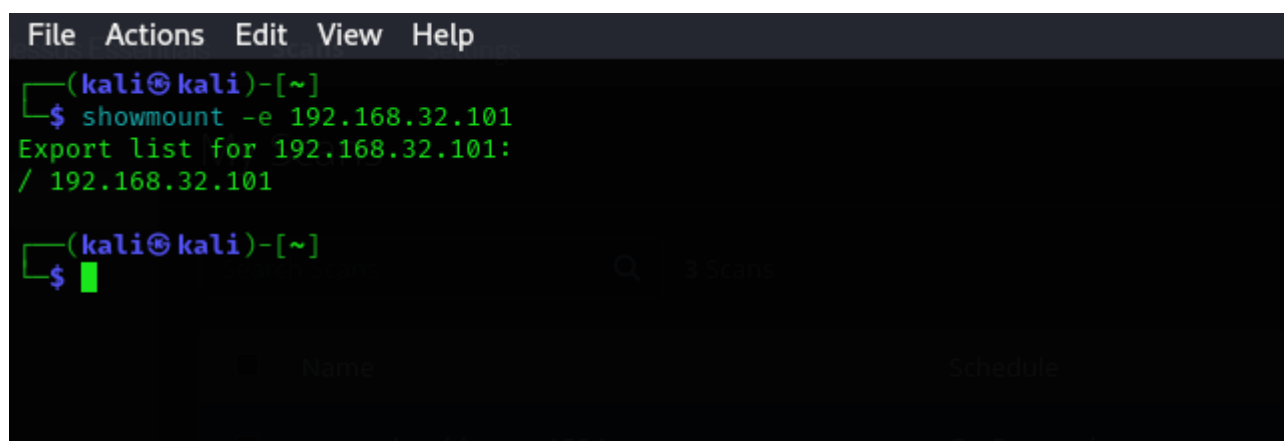
The screenshot shows a terminal window titled 'metasploitable [In esecuzione] - Oracle VM VirtualBox'. The window displays the contents of the /etc/exports file using the GNU nano 2.0.7 editor. The file contains comments and examples for NFSv2, NFSv3, and NFSv4, followed by a line for 192.168.32.101 with permissions (rw, sync, no\_root\_squash, no\_subtree\_check). The terminal window has a menu bar with 'File', 'Macchina', 'Visualizza', 'Inserimento', 'Dispositivi', and 'Aiuto'. The status bar at the bottom shows various keyboard shortcuts and a 'CTRL (DESTRA)' indicator.

```
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)
#

/ 192.168.32.101(rw,sync,no_root_squash,no_subtree_check)
```

Con una successiva scansione da un altro client potremmo vedere che le condivisioni NFS potranno essere modificate solamente dall'host 192.168.32.101



The screenshot shows a terminal window with a menu bar containing 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal displays the output of the 'showmount -e 192.168.32.101' command, which shows the export list for 192.168.32.101 as '/ 192.168.32.101'. The prompt is '(kali㉿kali)-[~]' and the command is '\$ showmount -e 192.168.32.101'. Below the output, there is a section with a search bar and a table with columns 'Name' and 'Schedule'.

```
File Actions Edit View Help

(kali㉿kali)-[~]
$ showmount -e 192.168.32.101
Export list for 192.168.32.101:
/ 192.168.32.101

(kali㉿kali)-[~]
$
```

La terza criticità presa in esame è

VNC Server 'password' Password

CRITICAL

10.0\*

-

61708

VNC Server 'password' Password

Questa criticità identifica una password troppo debole per il nostro server VNC, in questo caso la password in questione è “password”

```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@metasploitable:/home/msfadmin# pgrep vnc
4573
root@metasploitable:/home/msfadmin# kill 4573
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# tightvncserver

New 'X' desktop is metasploitable:1

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:1.log

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

Per risolvere è bastato chiudere il processo del server VNC (tight)

Modificare la password tramite comando

**vncpasswd**

E successivamente riavviare il server con comando

**Tightvncserver**

Nella scan iniziale sono presenti delle vulnerabilità con risoluzione comune.

Per esempio :

CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Over per risolvere la criticità basta semplicemente aggiornare il sistema a delle versioni più recenti tramite comando apposito ( in questo test non verrà svolto l’upgrade del sistema , in quanto laboratorio di lavoro e per non “intaccare” le vulnerabilità presenti).