

```
msfadmin@metasploitable:~$ ls -l ~/.unc/passwd
-rw----- 1 msfadmin msfadmin 16 2024-07-28 06:50 /home/msfadmin/.unc/passwd
msfadmin@metasploitable:~$
```

Vulnerability: VNC Server password

Lanciando il comando `vncpasswd` modifico la password del server vnc in modo da renderla più sicura. Lo screenshot dimostra la modifica la password in data 28/07/24.

```
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)
#
#
# * (rw,sync,no_root_squash,no_subtree_check)
/ 192.168.50.101(rw,sync,no_root_sqaush,no_subtree_check)

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

Vulnerability: NFS Exported Share

Accedendo al file “exports” ho commentato la riga di comando che permetteva l’accesso a qualsiasi host e ho inserito l’ip dell’host che può leggere/modificare le directory del server. A questo punto facciamo il restart del server con il comando “`sudo /etc/init.d/nfs-kernel-server restart`”

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4628/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4628/exe
lrwxrwxrwx 1 root root 0 2024-07-28 09:50 /proc/4628/exe -> /usr/sbin/xinetd (deleted)
msfadmin@metasploitable:~$
```

Vulnerability: Bind Shell Backdoor

Essendo a conoscenza della porta dove agiva la backdoor leggendo sul report, abbiamo comunque testato con nmap da Kali Linux, lanciando il comando “nmap -p 0-65535 192.168.50.101”. A questo punto dalla macchina Metasploitable con il comando “netstat”, passando la porta 1524, troviamo il PID. Lanciamo il comando “ls” e il path del PID per identificare il path completo dove si trova il file della backdoor, a questo lo eliminiamo

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS" />
-->

# <!-- Define an AJP 1.3 Connector on port 8009 -->
# <Connector port="8009"
#           enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />

<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
```

Vulnerability: Apache Tomcat AJP Connector

```
msfadmin@metasploitable:/$ sudo /etc/init.d/tomcat5.5
* Usage: /etc/init.d/tomcat5.5 {start|stop|restart|try-restart|force-reload|status}
msfadmin@metasploitable:/$ sudo /etc/init.d/tomcat5.5 restart
* Stopping Tomcat servlet engine tomcat5.5 [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
msfadmin@metasploitable:/$
```

Lanciando il comando sudo nano /etc/tomcat5.5/server.xml andiamo a modificare il file, commentando le righe, che definiscono il “connettore AJP” sulla porta 8009 e sulla porta di appoggio 8443; così facendo disabilitiamo la porta. A questo punto facciamo il restart del server con il comando “sudo /etc/init.d/tomcat5.5 restart”