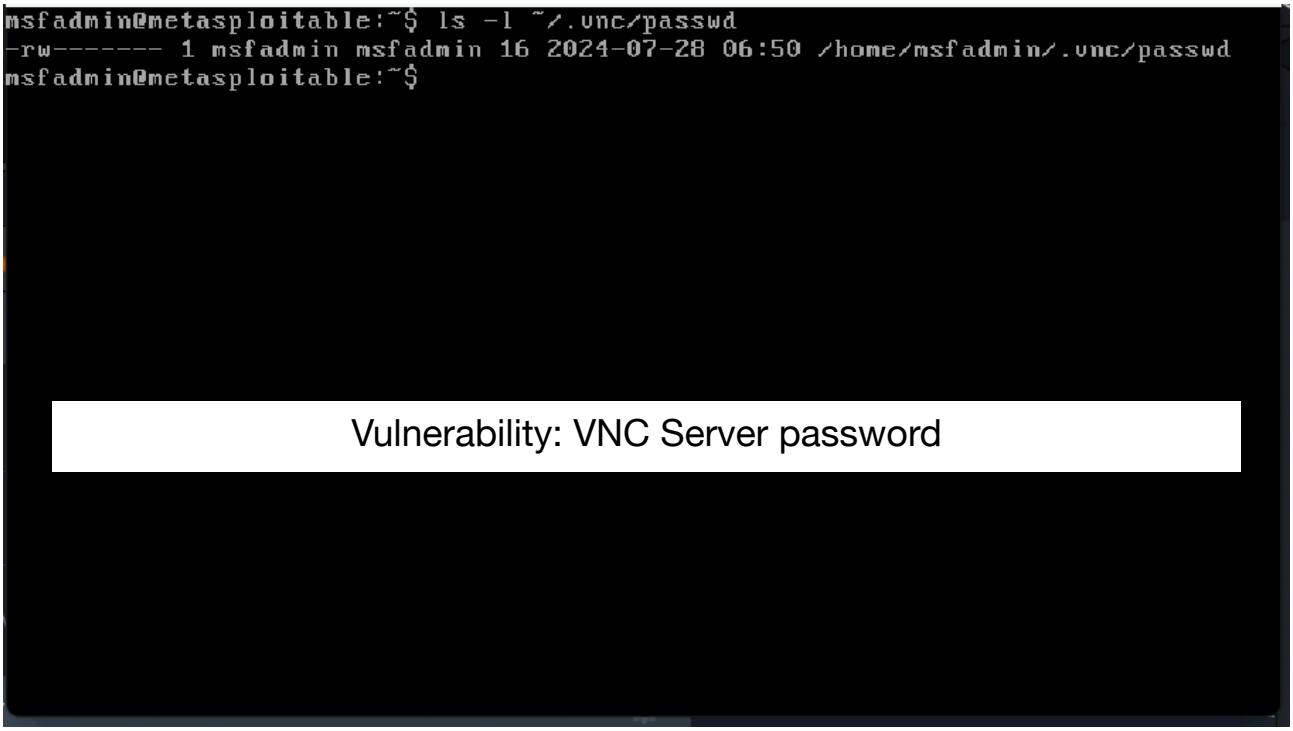
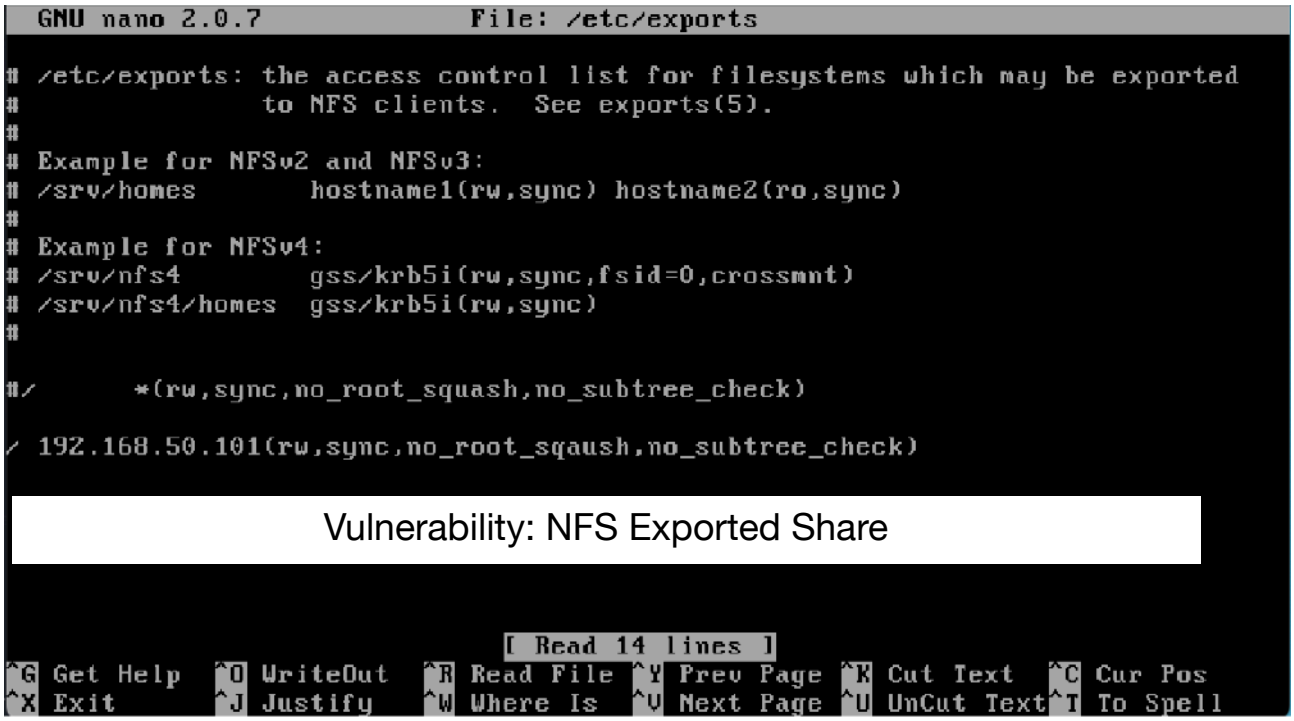


Lanciando il comando vncpasswd modifico la password del server vnc in modo da renderla più sicura. Lo screenshot dimostra la modifica la password in data 28/07/24.



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 restare 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 (de
leted)
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 punto 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|sta
tus}
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”