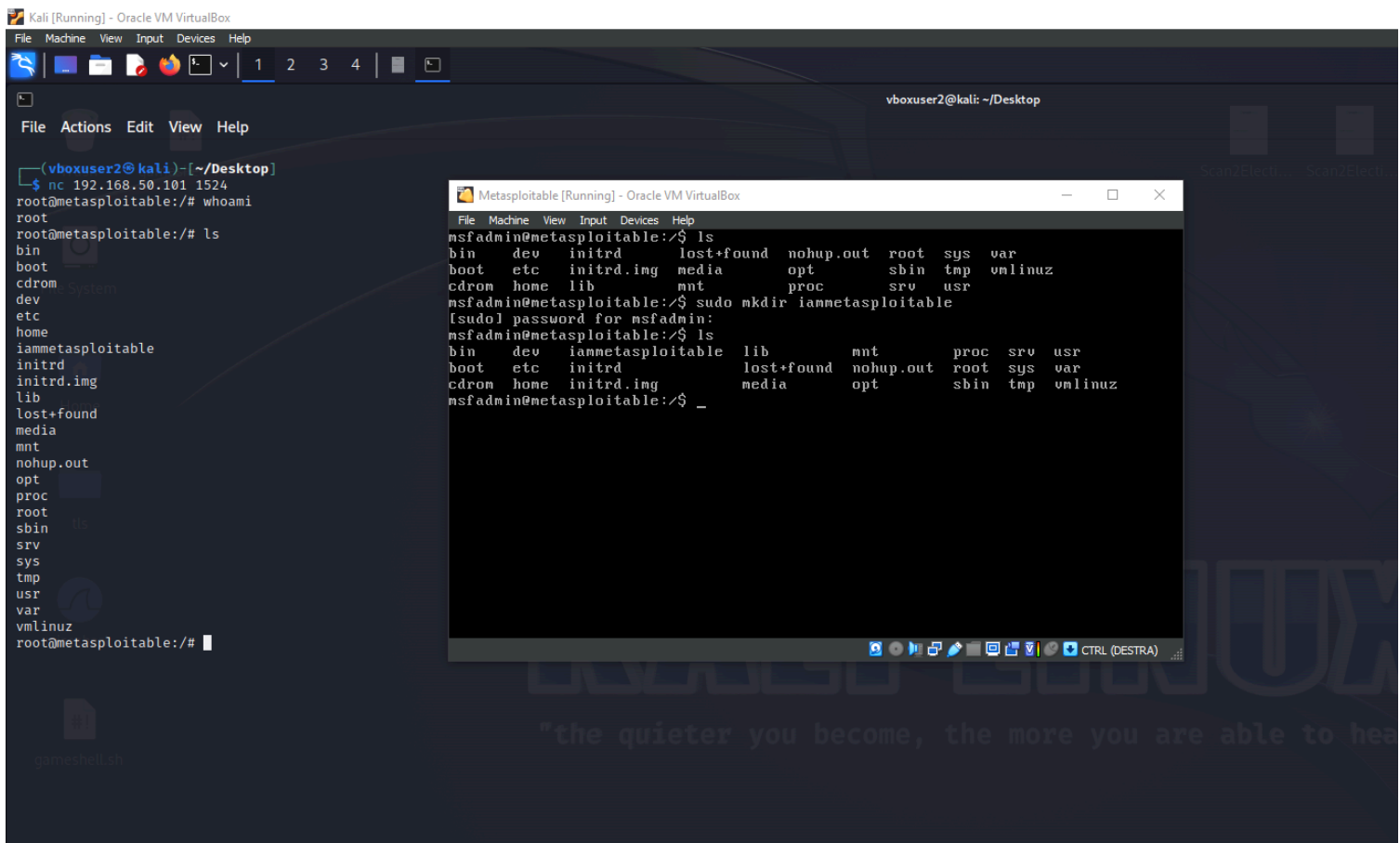


REMEDIATION 1: Bind Shell Backdoor

Metasploitable tiene di default una porta aperta per iniezione di reverse shell tramite netcat. Una veloce ricerca su google, ci dice che si tratta della porta 1524, porta comunemente impiegata nel primo decennio dei 2000' dal software di gestione database, "Ingres", per il blocco di parti del suo servizio. Confermiamo che sia il caso anche nella nostra macchina testando se è possibile infiltrarsi nel target con quella porta, e tramite una scansione di nmap.

La creazione di una cartella personalizzata ci conferma che stiamo guardando proprio dentro la macchina target.



```
File Machine View Input Devices Help
metasploitable login: msfadmin
Password:
Last login: Sat Jan 27 16:58:52 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

msfadmin@metasploitable:/$ nmap 127.0.0.1

Starting Nmap 4.53 ( http://insecure.org ) at 2024-01-28 10:47 EST
Interesting ports on localhost (127.0.0.1):
Not shown: 1691 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
953/tcp   open  rndc
1524/tcp  open  ingreslock
```

Nmap nello specifico, ci tagga quella porta come “ingreslock”, confermando le nostre supposizioni.

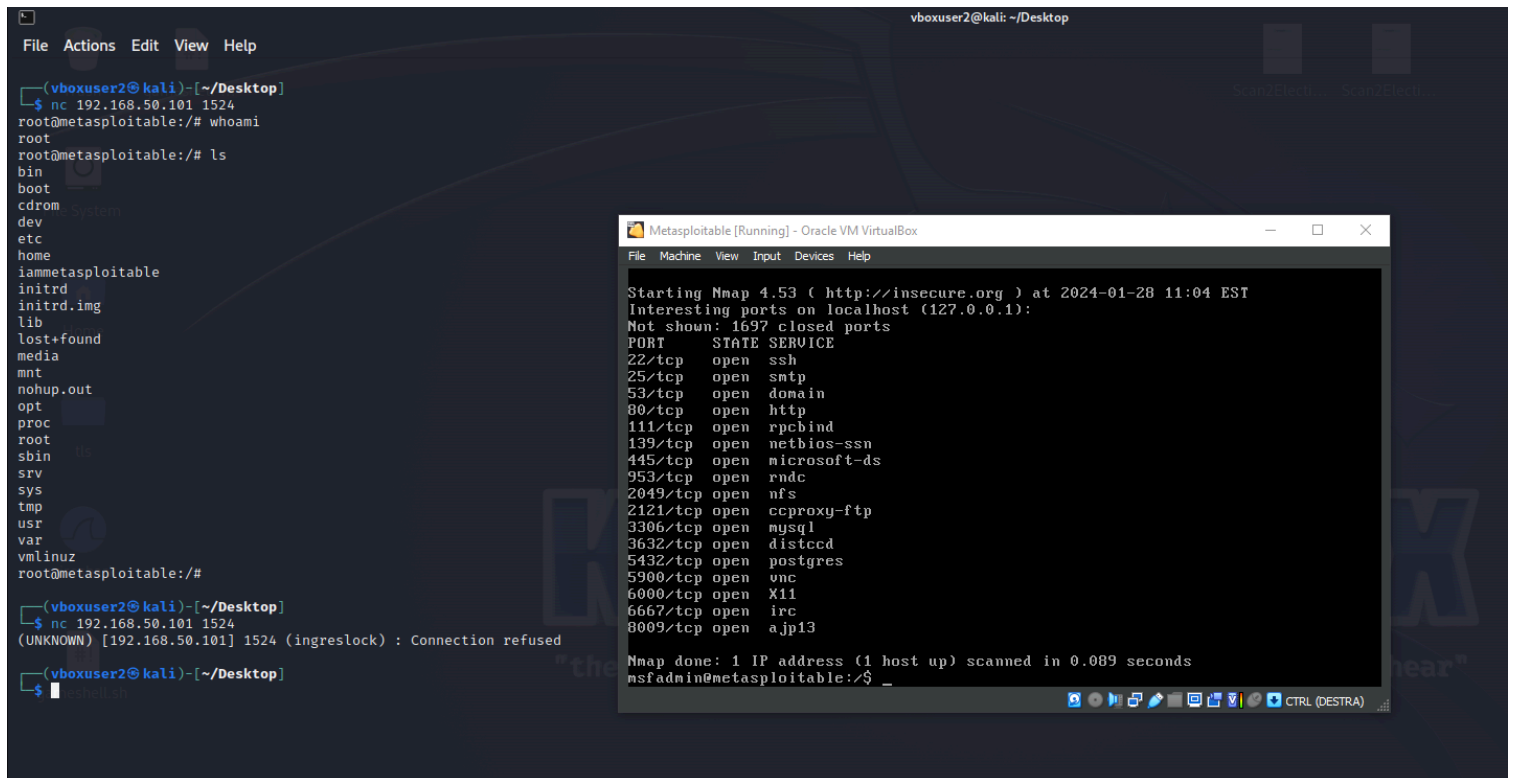
Secondo la CVE-2007-3336 (<https://www.cvedetails.com/cve/CVE-2007-3336/>) e la CVE-2007-6334 (<https://www.cvedetails.com/cve/CVE-2007-6334/>), i servizi aperti di questo software concedono l'esecuzione in remoto di codice e l'assegnazione impropria di permessi alla macchina che si collega a quella porta.

Tramite fuser, possiamo procedere all'eliminazione della vulnerabilità, chiudendo la porta, con il comando: `fuser -k -n tcp 1524`

```
tasks: 101 total; 1 running; 100 sleeping; 0 stopped; 0 zombie
msfadmin@metasploitable:/$ sudo fuser -k -n tcp 1524
1524/tcp:      4511  4828
msfadmin@metasploitable:/$ nmap 127.0.0.1

Starting Nmap 4.53 ( http://insecure.org ) at 2024-01-28 11:04 EST
Interesting ports on localhost (127.0.0.1):
Not shown: 1697 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
953/tcp   open  rndc
```

La shell può anche essere terminata tramite lo stesso servizio uccidendo il suo PID, trovabile tramite: `fuser -v -n tcp 1524` - che lista tutti i processi in ascolto su quella porta.



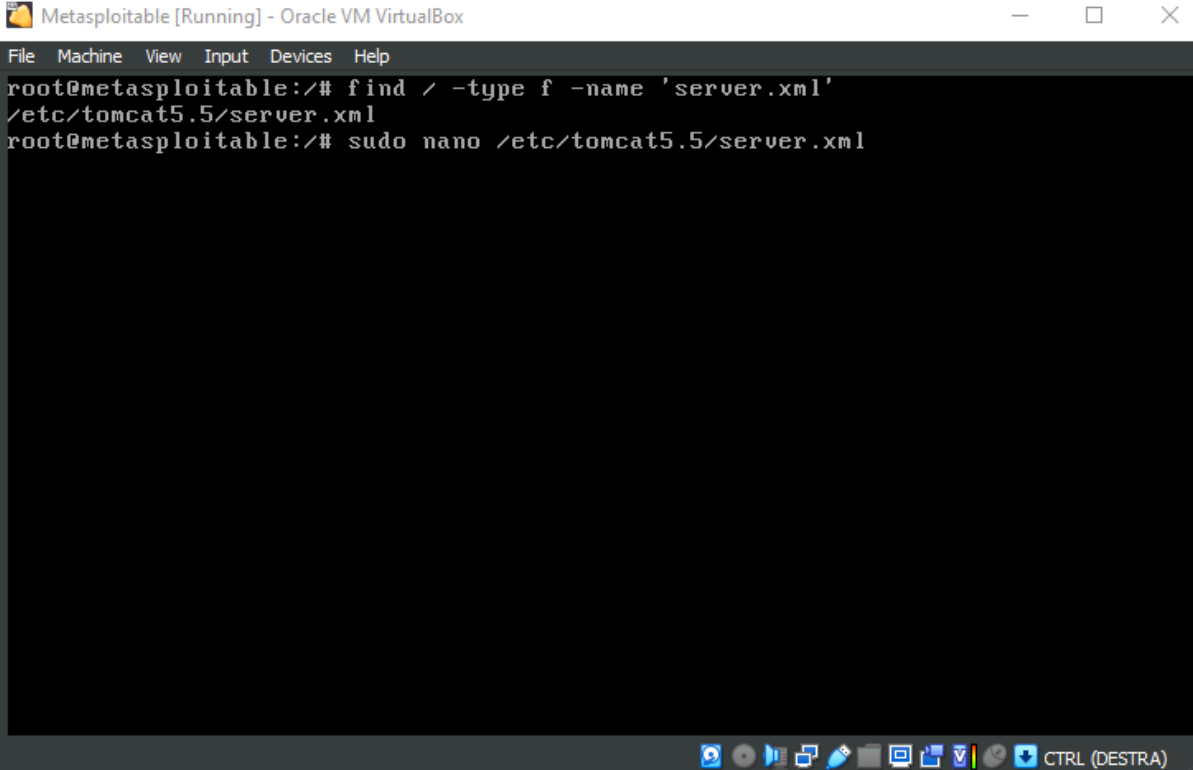
La porta risulta chiusa ed è adesso impossibile accedere alla macchina tramite lo stesso trucco. Il servizio di ingres sulla porta 1524 è obsoleto e presente in metasploit solo per fini didattici.

REMEDIATION 2: Ghostcat

Secondo la CVE-2020-1938, versioni di Tomcat appartenenti all'ultima decade soffrono di una vulnerabilità che permette RCE tramite un proprio connettore AJP, ritenuto automaticamente dall'applicativo come una fonte attendibile e facilmente accessibile dall'esterno.

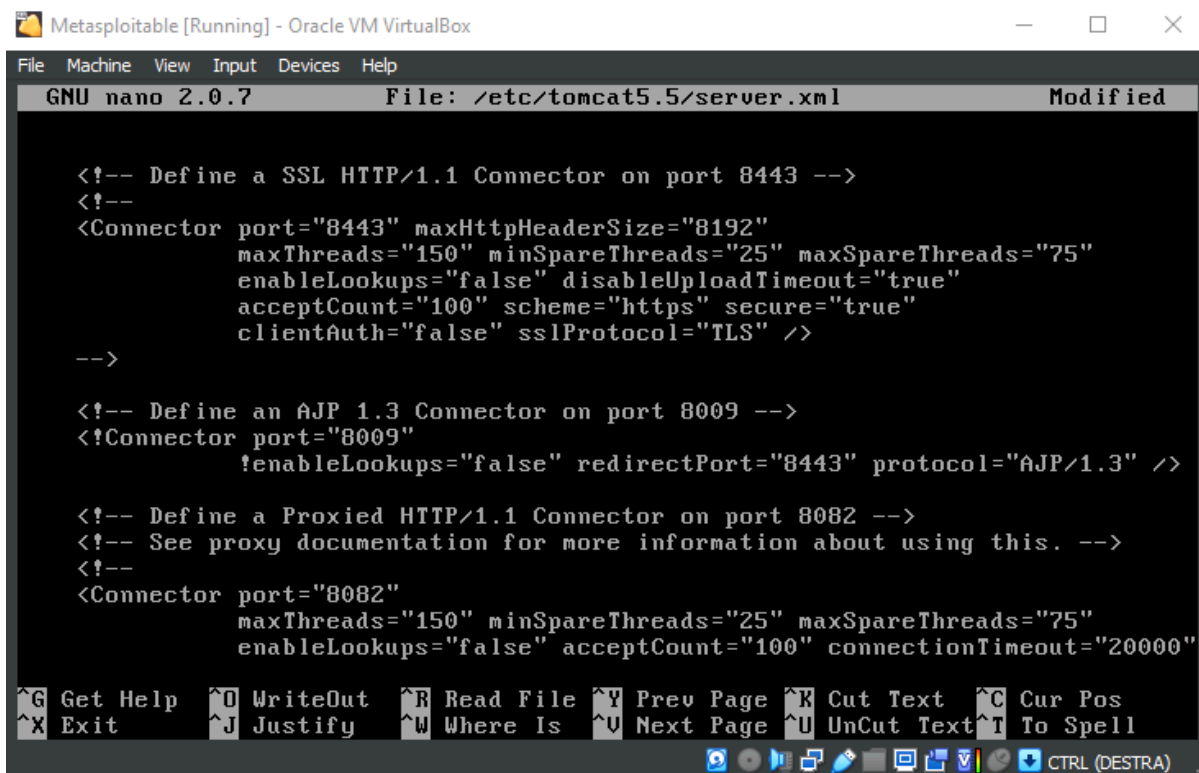
Per ovviare al problema si possono scegliere due strade: Aggiornare il software ad una delle seguenti versioni: 9.0.31, 8.5.51, oppure 7.0.100.

In alternativa, si può disabilitare il connettore direttamente dalla configurazione di Tomcat.



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@metasploitable:/# find / -type f -name 'server.xml'
/etc/tomcat5.5/server.xml
root@metasploitable:/# sudo nano /etc/tomcat5.5/server.xml
```

Cerchiamo il file xml di configurazione del server Tomcat e lo apriamo con un editor di testo.



The screenshot shows a virtual machine window titled "Metasploitable [Running] - Oracle VM VirtualBox". Inside the VM, the GNU nano 2.0.7 text editor is open, editing the file /etc/tomcat5.5/server.xml. The file contains XML configuration for Tomcat connectors. The first connector is an SSL HTTP/1.1 connector on port 8443. The second connector is an AJP 1.3 connector on port 8009, which is commented out with a '!'. The third connector is a proxied HTTP/1.1 connector on port 8082. The nano editor's status bar at the bottom shows various keyboard shortcuts like ^G Get Help, ^O WriteOut, ^R Read File, etc.

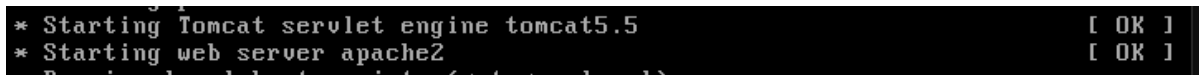
```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
          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. -->
<!--
<Connector port="8082"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" acceptCount="100" connectionTimeout="20000"
```

Si cerca la linea che contiene le informazioni rilevanti al funzionamento del connettore AJP e la si commenta con un '!' all'inizio della riga.

Riavviando Tomcat oppure la macchina avremo risolto questa vulnerabilità. Sarà ancora possibile connettersi alle pagine del webserver e Tomcat sorpasserà l'integrity check all'avvio del sistema operativo.



The screenshot shows a terminal window with the following output:

```
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local host scripts (etc/no-local)
```

REMEDIATION 3: NFS SHARE INFORMATION DISCLOSURE

Il Network File System è un sistema di condivisione directory da server remoti.

Di default, questo servizio è configurato per essere usato da ogni utente con il massimo dei permessi.

```
(root@kali)-[/home/vboxuser2]
# nmap nfs-ls 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-28 12:47 EST
Failed to resolve "nfs-ls".
Nmap scan report for 192.168.50.101
Host is up (0.000082s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1099/tcp  open  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:FF:E3:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.33 seconds

(root@kali)-[/home/vboxuser2]
# showmount -e 192.168.50.101
Export list for 192.168.50.101:
/ *

(root@kali)-[/home/vboxuser2]
# mkdir tmpnfs

(root@kali)-[/home/vboxuser2]
# cd tmpnfs

(root@kali)-[/home/vboxuser2/tmpnfs]
# mount -o nolock -t nfs 192.168.50.101:/ tmpnfs
mount.nfs: mount point tmpnfs does not exist

(root@kali)-[/home/vboxuser2/tmpnfs]
# cd ..

(root@kali)-[/home/vboxuser2]
# mount -o nolock -t nfs 192.168.50.101:/ tmpnfs

(root@kali)-[/home/vboxuser2]
```

La dicitura “ / * “ ci conferma che possediamo i permessi di root sulla macchina server una volta effettuato l’accesso, mentre è assente un qualsiasi controllo credenziali che tenga fuori utenti non desiderati

```
(root@kali)-[/home/vboxuser2] 9.0 134852 Apache Tomcat AJP Connector Request Injection (Ghos
# ssh-keygen
Generating public/private rsa key pair. 31968 Bind Shell Backdoor Detection
Enter file in which to save the key (/root/.ssh/id_rsa): 6007 SSL Version 2 and 3 Protocol Detection
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub Vendor DNS Query ID Field Prediction Cache
The key fingerprint is:
SHA256:TMi8WQqNc0/spLPBGuAYnIMnUzJ/MvkvvhR8BY6ERS0 root@kali ing System Unsupported Version Detection
The key's randomart image is:
+--[RSA 3072]--+
|o+=....
|+BE+. * o
|+=6.B * *
| O.@ = 8
|. + o O S
|. . o +
|. . .
+--[SHA256]--+
+-----+
10.0* 7.4 32314 Debian OpenSSH/OpenSSL Package Random Number
Weakness
10.0* 7.4 32321 Debian OpenSSH/OpenSSL Package Random Number
Weakness (SSL check)
10.0* 5.9 11356 NFS Exported Share information Disclosure
10.0* 61708 VNC Server 'password' Password

5.2 136789 ISC BIND Service Downgrade / Reflected DoS
# cat ssh/id_rsa.pub >> /home/vboxuser2/tmpnfs/root/.ssh/authorized_keys
cat: ssh/id_rsa.pub: No such file or directory
NFS Shares World Readable

(root@kali)-[/home/vboxuser2]
# cat .ssh/id_rsa.pub >> /home/vboxuser2/tmpnfs/root/.ssh/authorized_keys
```

Generando una chiave SSH da poi depositare nella directory di controllo dell'SSH sul server, possiamo rendere qualsiasi macchina attaccante automaticamente affidabile per intrusioni future.

Per evitare questa problematica, creiamo uno usergroup protetto da password nella macchina server

```
msfadmin@metasploitable:~$ sudo useradd shareuser
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ id shareuser
uid=1003(shareuser) gid=1003(shareuser) groups=1003(shareuser)
msfadmin@metasploitable:~$ sudo passwd shareuser
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$ _
```

E poi assegniamo questo gruppo ai permessi della cartella condivisa di NFS tramite accesso al file "exports", che si trova sotto /etc.

```
microspionabile [running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.0.7 File: 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)
#
/ shareuser(rw,sync,no_root_squash,no_subtree_check)
```

La vulnerabilità viene così risolta. Creando uno usergroup con le stesse informazioni di nome ed id sulla macchina client, riusciamo ad accedere al server. Ogni usergroup è protetto da una password.

REMEDIATION 4: VNC Password

Di default, la password del servizio VNC, sharing grafico di desktop, non è impostata. Il ciò permette a chiunque di connettersi ad un host tramite il comando: `vncviewer **ip**`.

L'impostazione di una password avviene semplicemente richiamando il comando `vncpasswd` da `su` o `sudo`, ed impostando una password con un minimo di complessità.

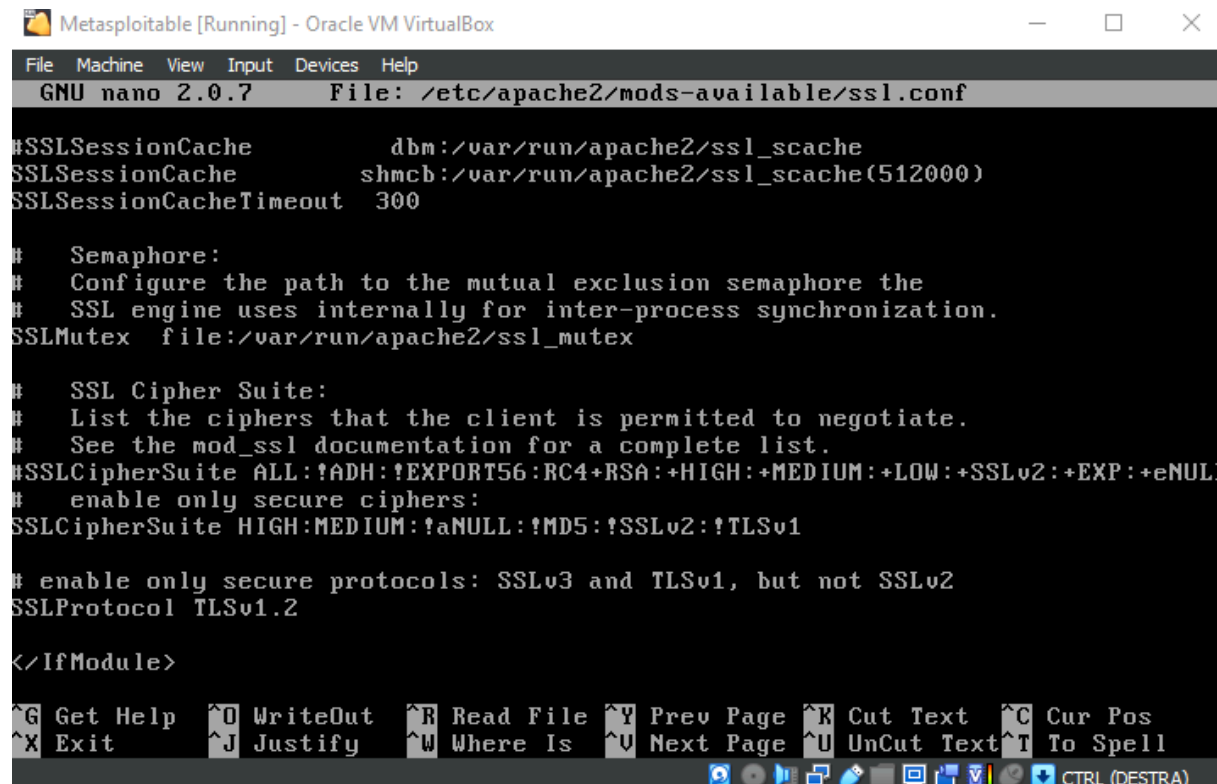
```
(root@kali)-[/home/vboxuser2]
# vncviewer 192.168.50.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Tutti gli accessi adesso sono regolati da una password.

Altre Remediation

Altre vulnerabilità sono scomparse gradualmente con il lavoro sulle Remediation elencate in questo file.

Lavoro è stato fatto sulla sostituzione dei protocolli SSL 2 e 3, tramite configurazione del file ssl.conf di apache2, ma senza successo.



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.0.7 File: /etc/apache2/mods-available/ssl.conf

#SSLSessionCache          dbm:/var/run/apache2/ssl_scache
SSLSessionCache           shmcb:/var/run/apache2/ssl_scache(512000)
SSLSessionCacheTimeout    300

#
# Semaphore:
# Configure the path to the mutual exclusion semaphore the
# SSL engine uses internally for inter-process synchronization.
SSLMutex file:/var/run/apache2/ssl_mutex

#
# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
# enable only secure ciphers:
SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SSLv2:!TLSv1

# enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
SSLProtocol TLSv1.2

</IfModule>

^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)
```