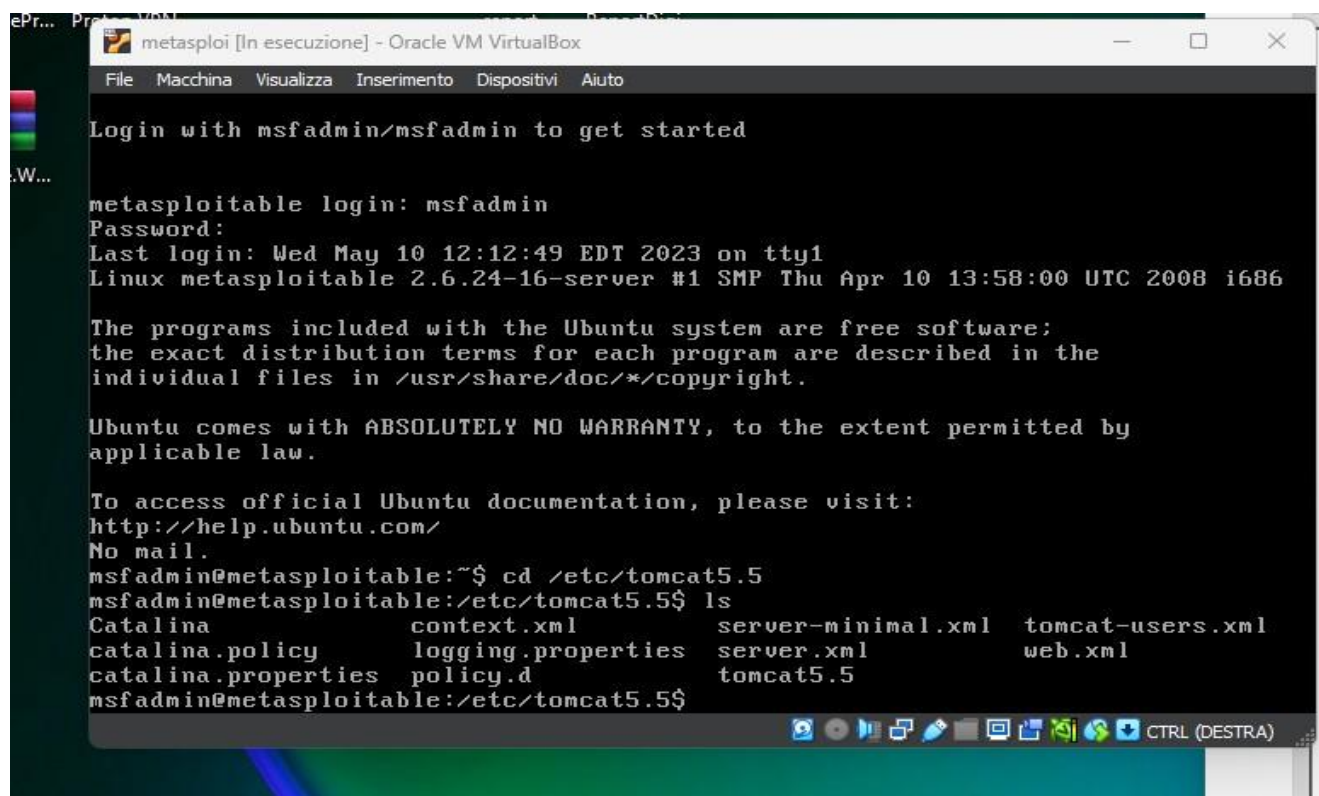


1-AJP connector su Tomcat

Vado su "cd /etc/tomcat5.5 e modifico il file:



```
metasploit [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

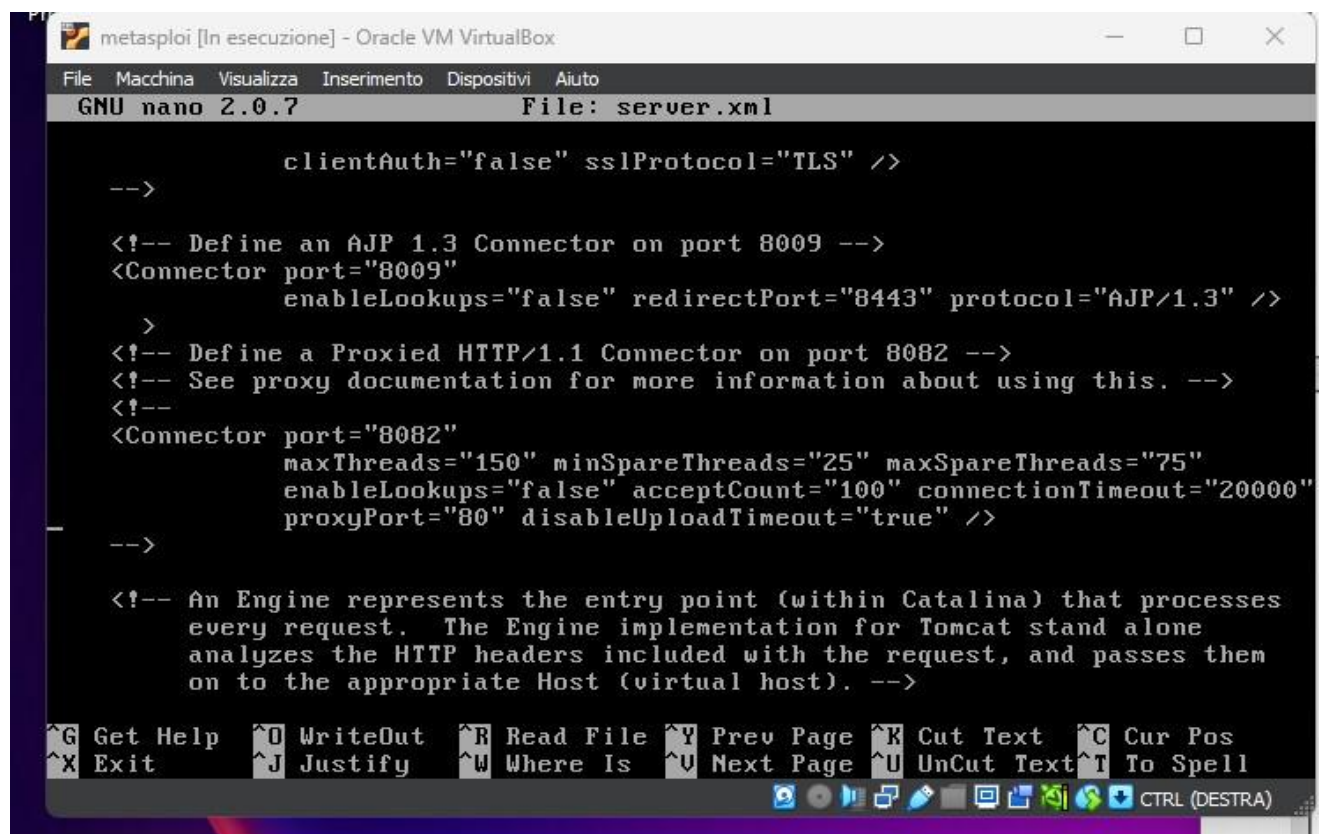
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Wed May 10 12:12:49 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ cd /etc/tomcat5.5
msfadmin@metasploitable:/etc/tomcat5.5$ ls
Catalina          context.xml        server-minimal.xml  tomcat-users.xml
catalina.policy   logging.properties  server.xml          web.xml
catalina.properties  policy.d          tomcat5.5
msfadmin@metasploitable:/etc/tomcat5.5$
```



```
metasploit [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7                               File: server.xml

      clientAuth="false" sslProtocol="TLS" />
-->

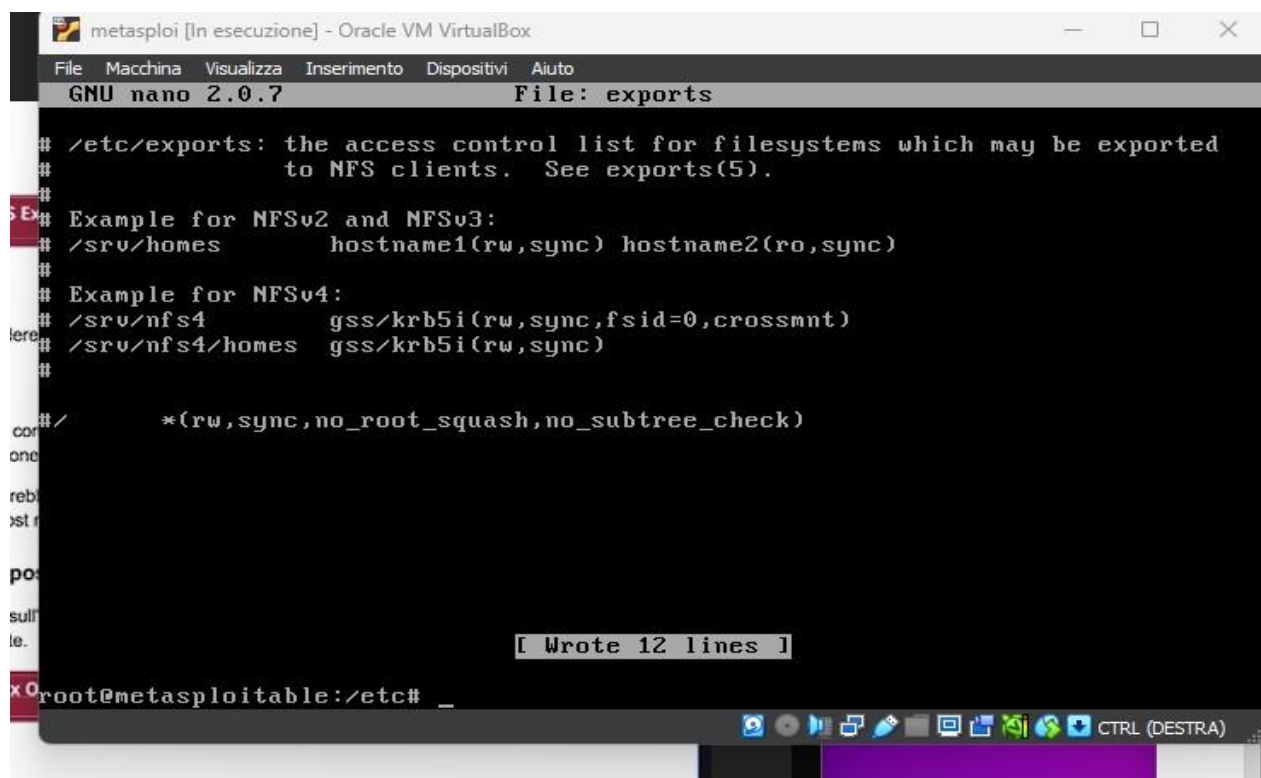
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
      enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />
-->
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
<Connector port="8082"
      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
      enableLookups="false" acceptCount="100" connectionTimeout="20000"
      proxyPort="80" disableUploadTimeout="true" />
-->

<!-- An Engine represents the entry point (within Catalina) that processes
every request. The Engine implementation for Tomcat stand alone
analyzes the HTTP headers included with the request, and passes them
on to the appropriate Host (virtual host). -->

^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify      ^W Where Is     ^U Next Page    ^U UnCut Text   ^T To Spell
CTRL (DESTRA)
```

Lo commento per disattivarlo.

2-Rimuovo la cartella root / dal file exports per risolvere la vulne.. di NFS:



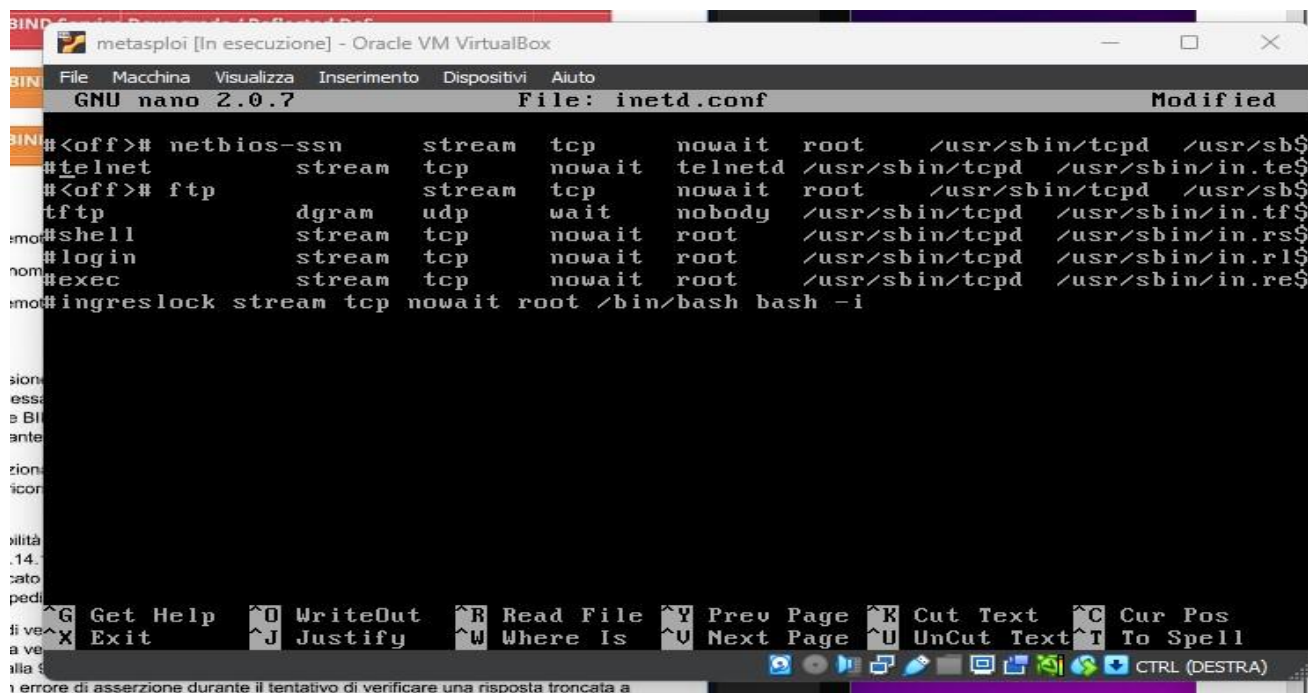
The screenshot shows a Metasploit terminal window titled "metasploit [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 editor, editing the file "/etc/exports". The file content is as follows:

```
# /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)
```

At the bottom of the terminal, the prompt "root@metasploitable:/etc#" is visible. A status bar at the bottom of the nano editor indicates "[Wrote 12 lines]".

3-Disattivo alcuni servizi in ascolto

In questo modo risolvo alcune backdoor.



The screenshot shows a Metasploit terminal window titled "metasploit [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 editor, editing the file "/etc/inetd.conf". The file content is as follows:

Service	Stream	Protocol	Wait	User	Program	Path
netbios-ssn	stream	tcp	nowait	root	/usr/sbin/tcpd	/usr/sbin/tcpd
telnet	stream	tcp	nowait	telnetd	/usr/sbin/tcpd	/usr/sbin/in.telnetd
ftp	stream	tcp	nowait	root	/usr/sbin/tcpd	/usr/sbin/ftpd
ftpp	dgram	udp	wait	nobody	/usr/sbin/tcpd	/usr/sbin/in.ftpd
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

```
#
```

At the bottom of the terminal, the prompt "root@metasploitable:/etc#" is visible. A status bar at the bottom of the nano editor shows various keyboard shortcuts like "Get Help", "WriteOut", "Read File", "Prev Page", "Cut Text", "Cur Pos", "Exit", "Justify", "Where Is", "Next Page", "UnCut Text", "To Spell".

-Queste sono 3 vulne.. HIGH risolte.

Vulnerabilità prima di risolvere:

Hosts 1 Vulnerabilities 39 Remediations 2 Notes 1 History 2

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.49.101	3 High, 3 Medium, 3 Low (Score: 80)

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0

Hosts 1 Vulnerabilities 39 Remediations 2 Notes 1 History 1

Search Actions 2 Actions

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	0	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: May 10 at 6:13 PM
- End: May 10 at 6:23 PM
- Elapsed: 9 minutes

Consigli come risolvere le vulnerabilità:

upgrade dei seguenti servizi, aggiornarli alla versione ultima o indicata.

- ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.
- Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Vulnerabilità 3 Risolte dopo le remediations:

sono state risolte 2 vulnerabilità CRITICAL - 1 HIGH.

Hosts 1Vulnerabilities 21Remediations 2Notes 9History 2

Filter Search Hosts 1 Host

Host

Vulnerabilities

192.168.49.101

1

2

2

1

34

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Vulnerabilities 21

Filter Search Vulnerabilities 21 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
HIGH	7.5		Samba Badlock Vulnerability	General	1	
MIXED	ISC Bind (Multiple Issues)	DNS	5	
LOW	2.6 *		X Server Detection	Service detection	1	
INFO	SMB (Multiple Issues)	Windows	6	
INFO	DNS (Multiple Issues)	DNS	3	
INFO			Nessus SYN scanner	Port scanners	9	
INFO			Apache Banner Linux Distribution Disclosure	Web Servers	1	
INFO			Common Platform Enumeration (CPE)	General	1	
INFO			

Host Details

IP: 192.168.49.101

MAC: 08:00:27:B1:AA:58

OS: Linux Kernel 2.6 on Ubuntu (gutsy)

Start: Today at 6:48 PM

End: Today at 6:58 PM

Elapsed: 10 minutes

KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info