

REMEDIATION ACTION PER 192.168.60.101

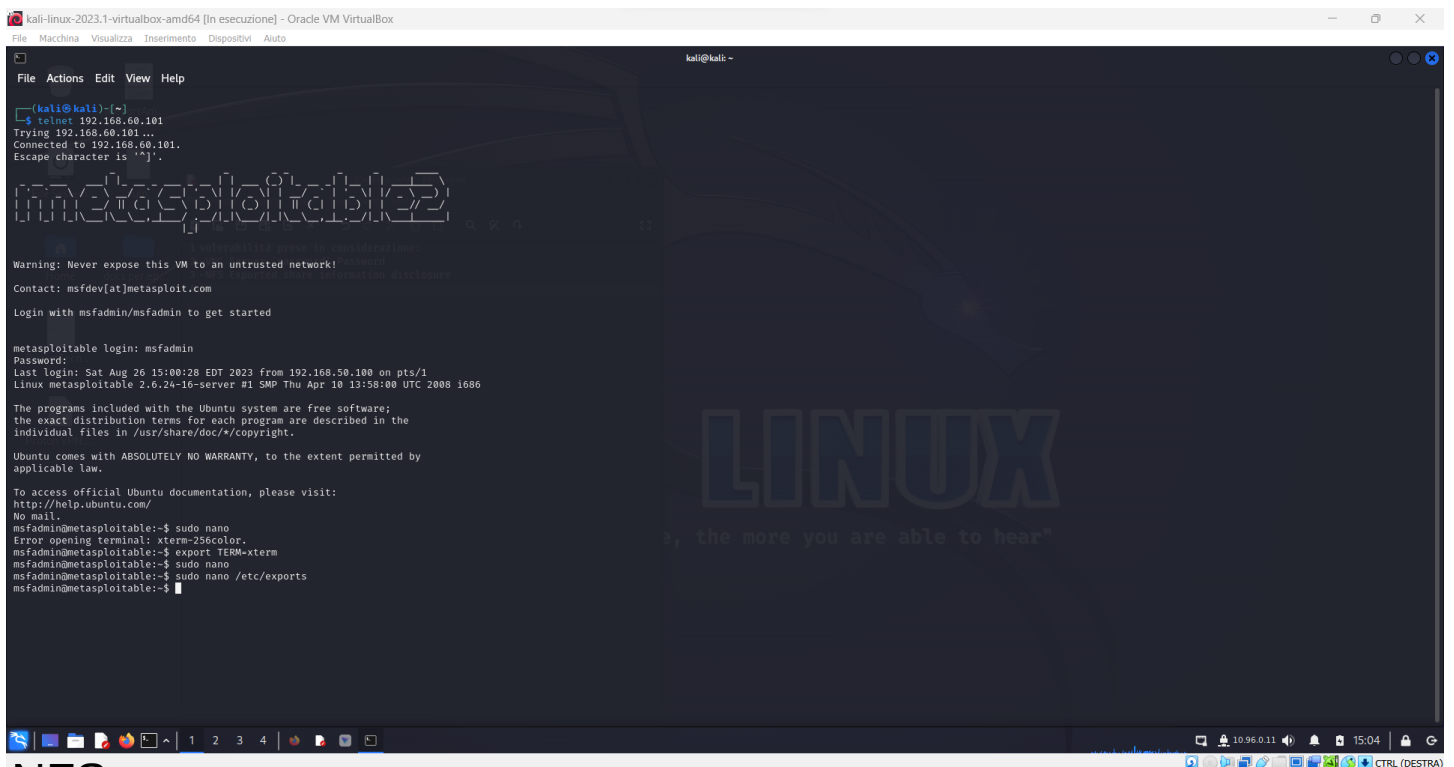
Vulnerabilità prese in esame:

- 11356 NFS exported share information disclosure
- 61708 VNC server 'password' Password
- 134862 Apache Tomcat AJP connector request injection (ghostcat)
- 20007 SSL version 2 and 3 protocol detection

Risoluzione della vulnerabilità NFS.

Attraverso l'utilizzo di telnet stabilisco una connessione in remoto con la macchina target.

Da qui andrò a modificare il file "exports" per impedire leaks di informazioni.



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Auto

kali@kali: ~
File  Actions  Edit  View  Help

kali@kali:~$ telnet 192.168.60.101
Trying 192.168.60.101...
Connected to 192.168.60.101.
Escape character is '^['.

msf5 (kali@kali) ~
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

msf5 login: msfadmin
Password:
Last login: Sat Aug 26 15:00:28 EDT 2023 from 192.168.50.100 on pts/1
Linux msf5 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686

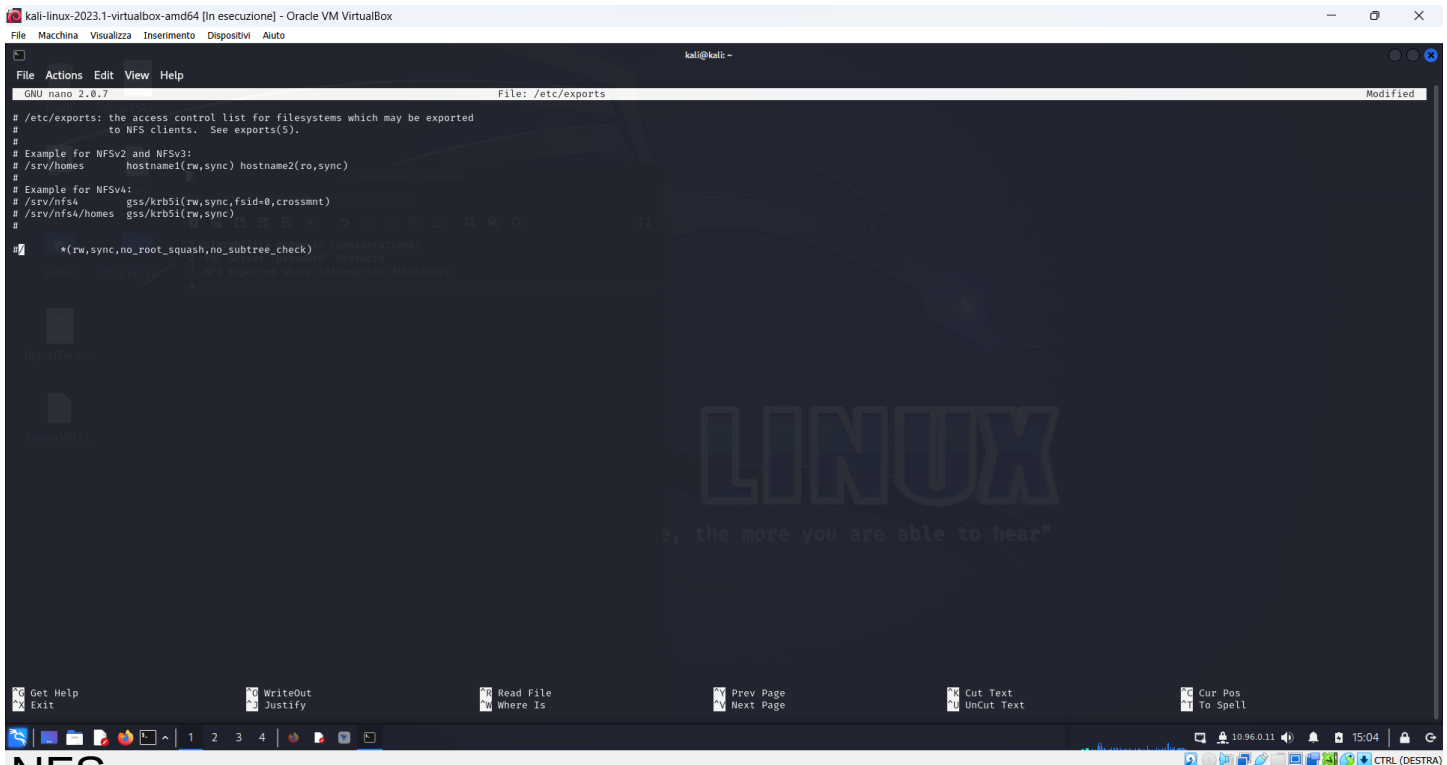
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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.
msf5 (kali@kali):~$ sudo nano
Error opening terminal: xterm-256color.
msf5 (kali@kali):~$ export TERM=xterm
msf5 (kali@kali):~$ sudo nano
msf5 (kali@kali):~$ sudo nano /etc/exports
msf5 (kali@kali):~$
```

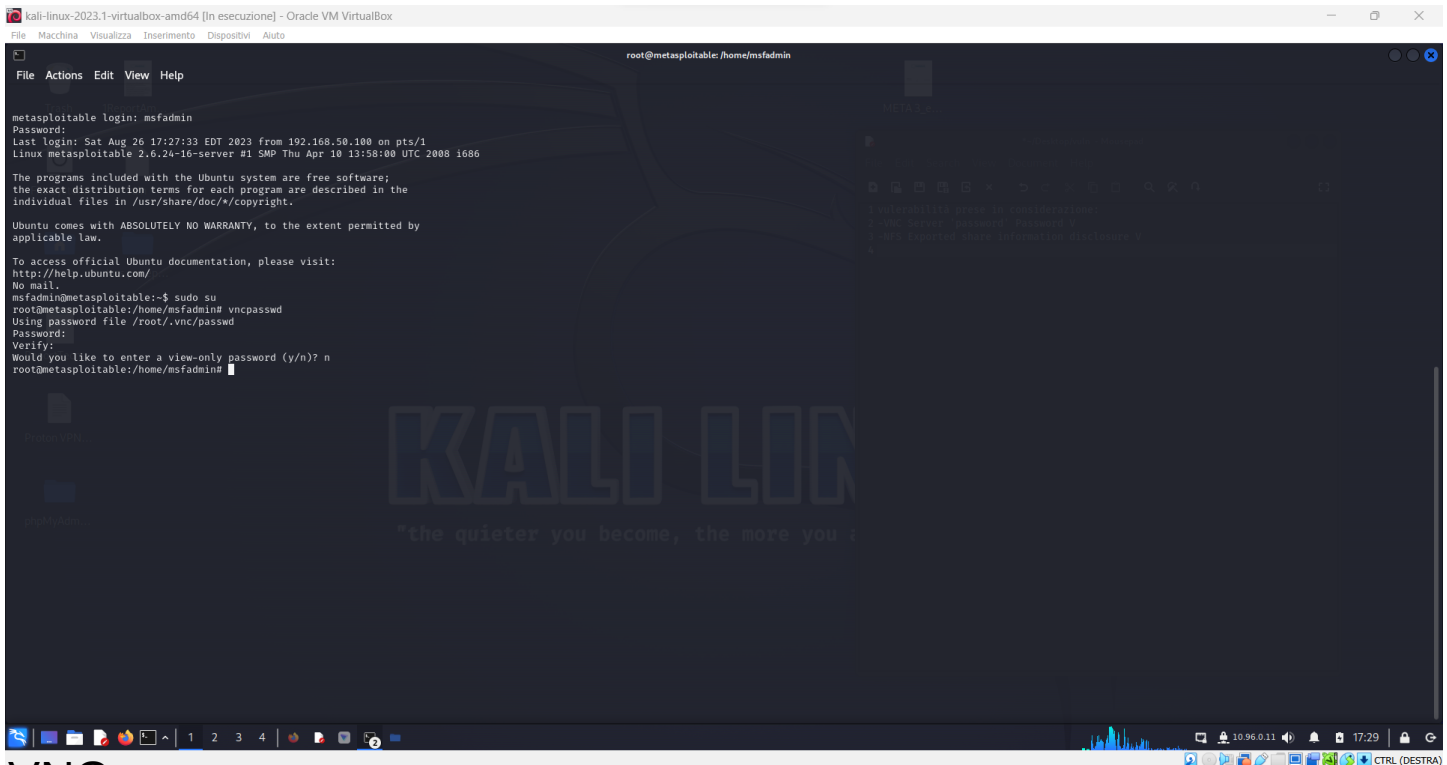
NFS

Come possiamo notare commentando l'ultima stringa e salvando il file viene bloccato il leak di informazioni.



NFS

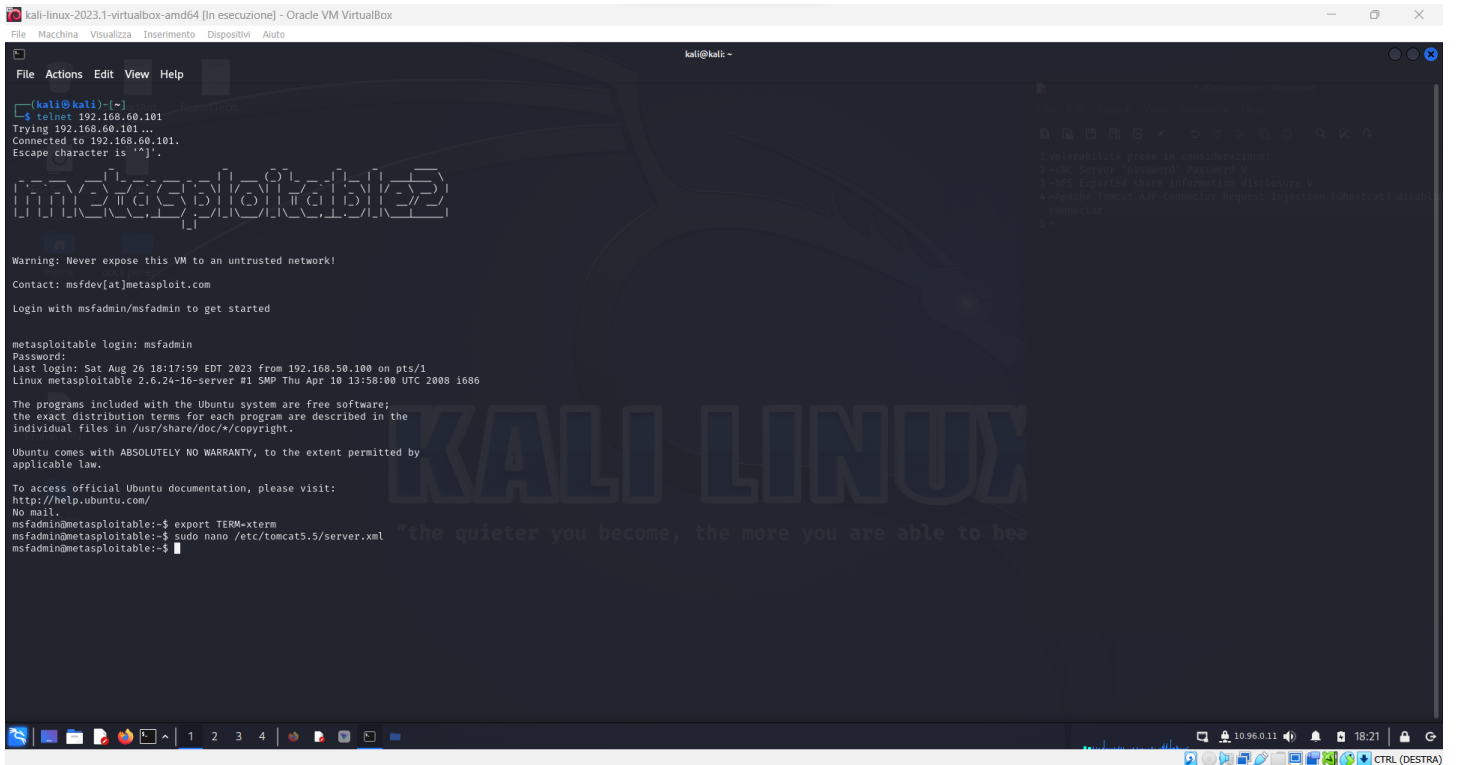
Risoluzione della vulnerabilità VNC.
sempre attraverso l'utilizzo di comandi remoti,andrò a richiamare il comando "vncpassword" che mi permetterà di scegliere una nuova password sicura per il server.



VNC

Risoluzione per la vulnerabilità AJP connector

Andando a modificare il file di configurazione “server.xml”
disattivo il connettore ajp.
(le uniche soluzioni erano l’update o la disattivazione)



```
kali@kali:~$ telnet 192.168.60.101
Trying 192.168.60.101 ...
Connected to 192.168.60.101.
Escape character is '^]'.

msf5 (kali@kali) ->

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

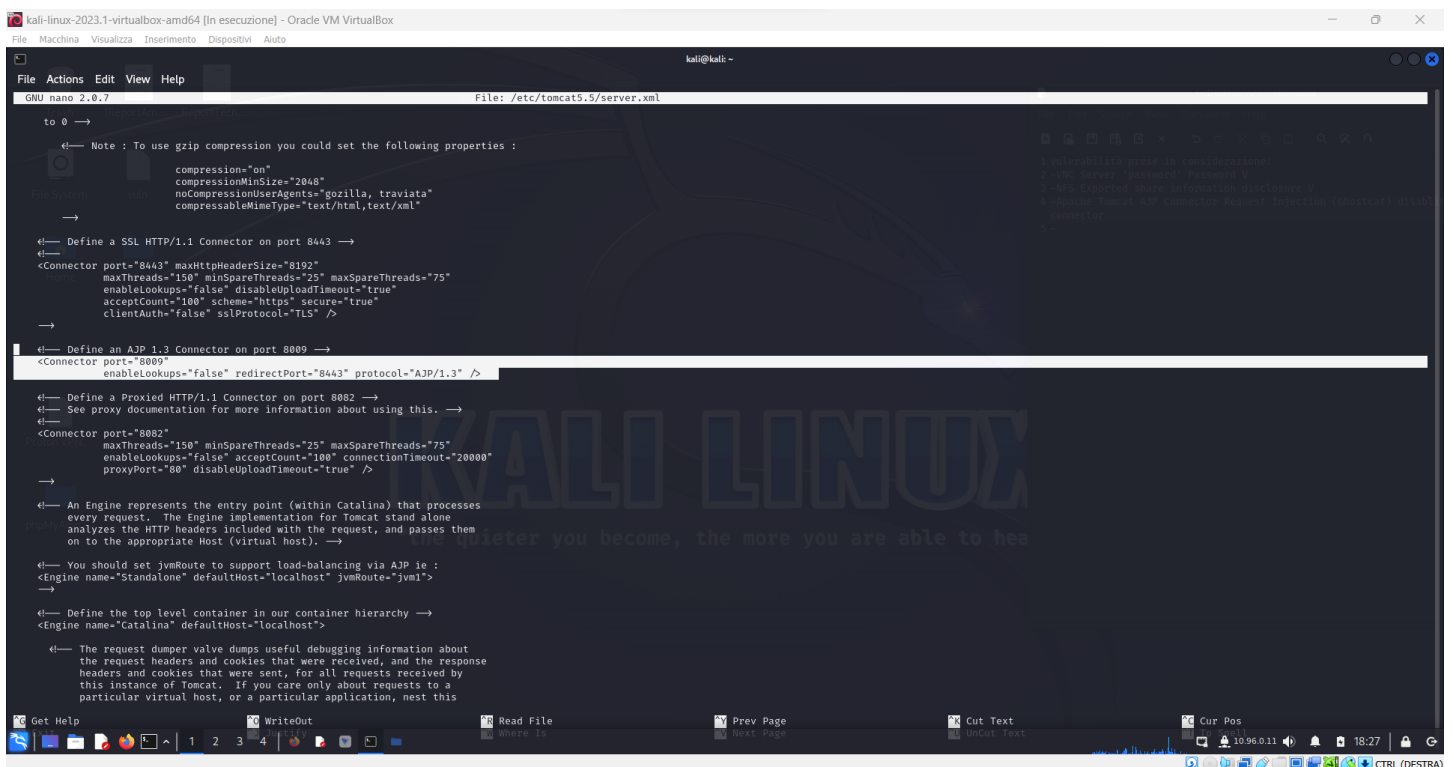
metasploit login: msfadmin
Password:
Last login: Sat Aug 26 18:17:59 EDT 2023 from 192.168.50.100 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$ export TERM=xterm
msfadmin@metasploitable:~$ sudo nano /etc/tomcat5.5/server.xml
msfadmin@metasploitable:~$
```

La stringa evidenziata indica la configurazione del connettore.



```
GNU nano 2.0.7 File: /etc/tomcat5.5/server.xml

to 0 ->

<!-- Note : To use gzip compression you could set the following properties :
-->
<!--
    compression="on"
    compressionMinSize="2048"
    noCompressionUserAgents="gozilla, traviata"
    compressableMimeType="text/html,text/xml"
-->

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
    The SSL protocol implementation is deprecated. Please use the
    APR implementation instead.
-->
<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" />

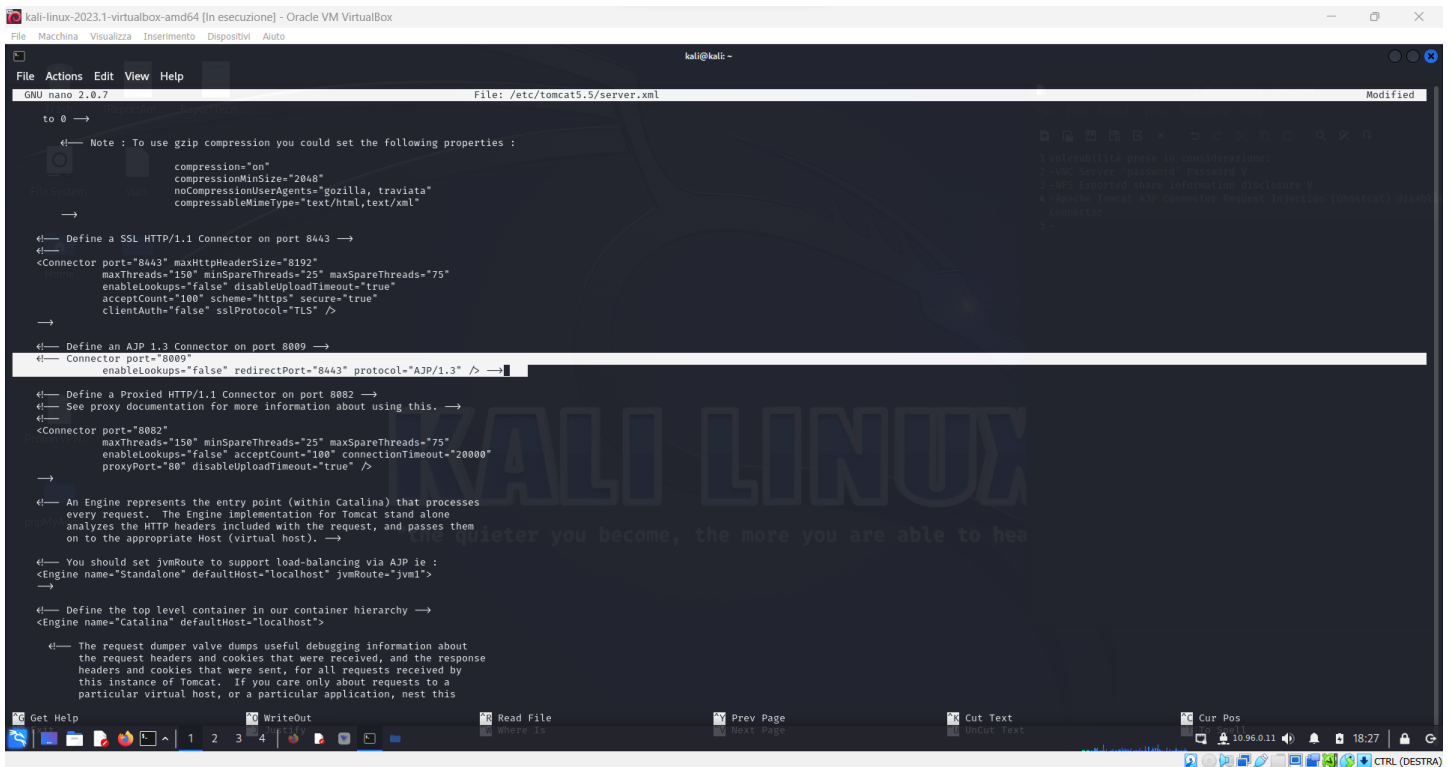
<!-- Define a Proxy HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<Connector port="8082"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" acceptCount="100" connectionTimeout="20000"
    proxyPort="80" 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). -->
<!-- You should set jvmRoute to support load-balancing via AJP ie :
-->
<Engine name="StandAlone" defaultHost="localhost" jvmRoute="jvm1">
    <!-- Define the top level container in our container hierarchy -->
    <Engine name="Catalina" defaultHost="localhost">

        <!-- The request dumper valve dumps useful debugging information about
the request headers and cookies that were received, and the response
headers and cookies that were sent, for all requests received by
this instance of Tomcat. If you care only about requests to a
particular virtual host, or a particular application, nest this
valve inside the host or application container -->
        <Valve className="org.apache.catalina.valves.RequestDumperValve"/>
    </Engine>
</Engine>

</Engine>
```

commentando la stringa viene di conseguenza disattivato il connettore,risolvendo in questo modo la vulnerabilità.



```
kali@kali:~$ nano /etc/tomcat5.5/server.xml
to 0 →
Note: To use gzip compression you could set the following properties :
    compression="on"
    compressionMinSize="2048"
    noCompressionUserAgents="gozilla, traviata"
    compressableMimeType="text/html,text/xml"

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"
    proxyPort="80" disableUploadTimeout="true" />

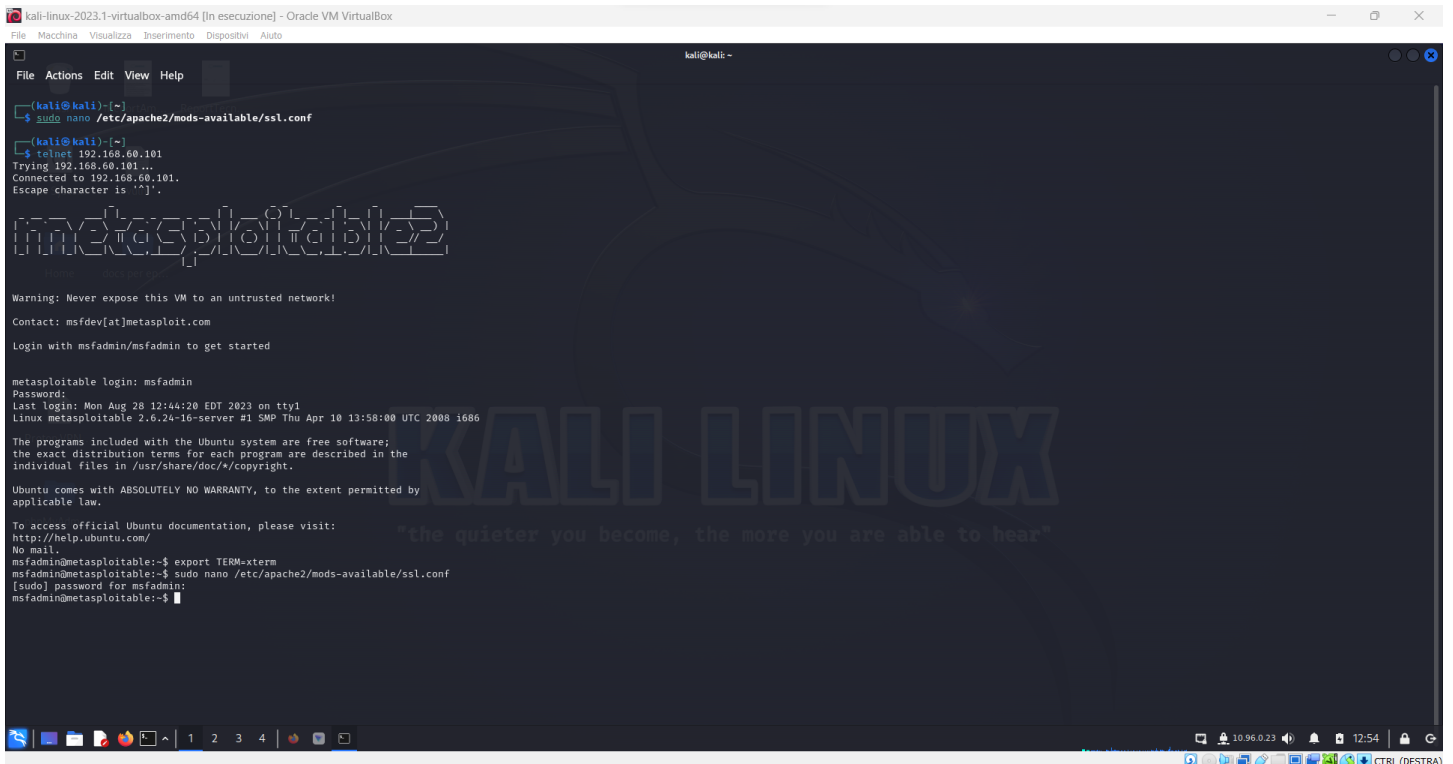
An Engine represents the entry point (within Catalina) that processes
every request. The Engine implementation for Tomcat stand alone
analyzes the HTTP headers included with the request, and passes them
on to the appropriate Host (virtual host).
<Engine name="Standalone" defaultHost="localhost" jvmRoute="jvm1">

You should set jvmRoute to support load-balancing via AJP ie :
<Engine name="Catalina" defaultHost="localhost">

The request dumper valve dumps useful debugging information about
the request headers and cookies that were received, and the response
headers and cookies that were sent, for all requests received by
this instance of Tomcat. If you care only about requests to a
particular virtual host, or a particular application, nest this
```

Risoluzione della vulnerabilità SSL.

Andando a modificare il file di configurazione ssl del server apache possiamo andare ad impostare i protocolli da utilizzare.



```
kali@kali:~$ nano /etc/apache2/mods-available/ssl.conf
(kali@kali):~$
(kali@kali):~$ telnet 192.168.68.101
Trying 192.168.68.101...
Connected to 192.168.68.101.
Escape character is '^['.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

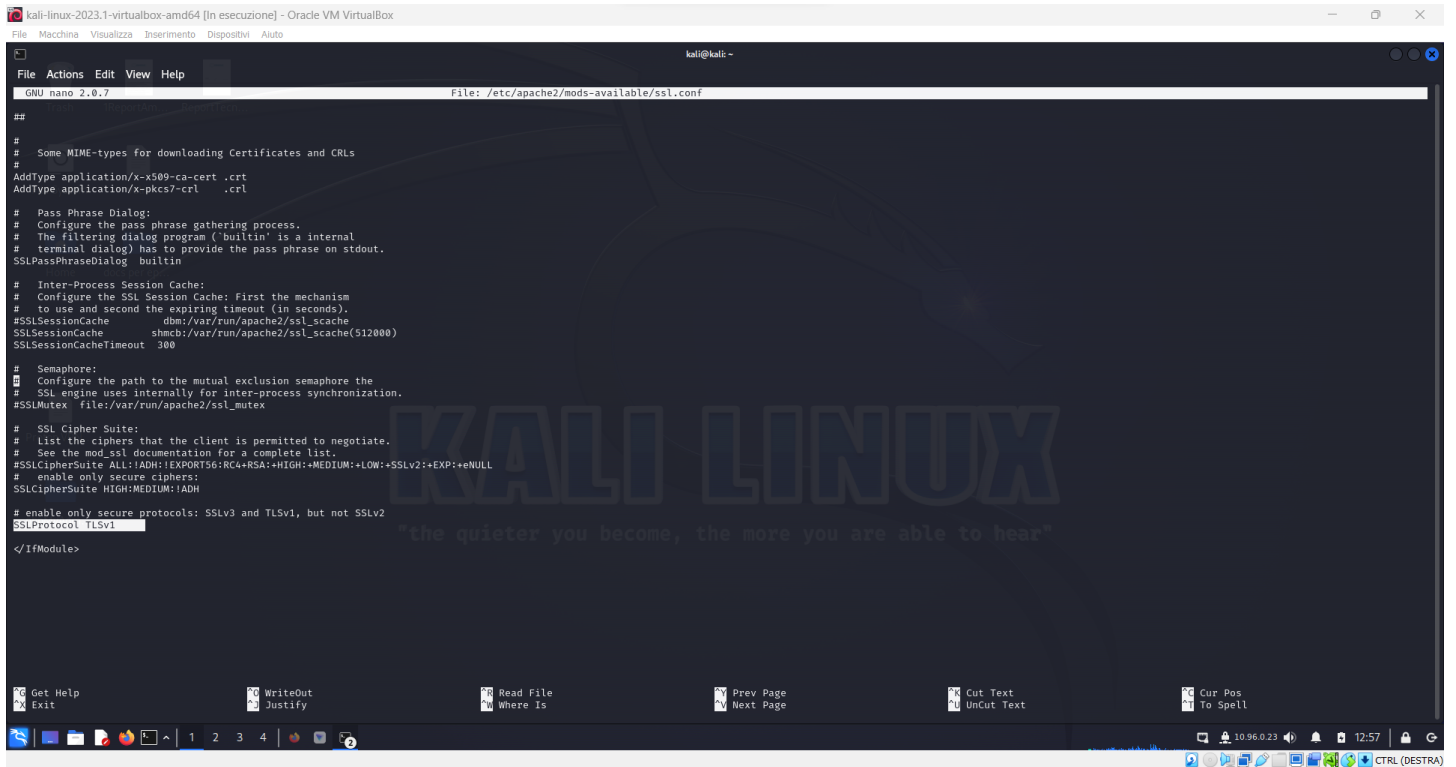
metasploitable login: msfadmin
Password:
Last login: Mon Aug 28 12:44:20 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$ export TERM=xterm
msfadmin@metasploitable:~$ sudo nano /etc/apache2/mods-available/ssl.conf
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

Come evidenziato imposto il protocollo tlsv1 nella configurazione. dopo aver salvato il file il server dovrebbe utilizzare quel tipo di protocollo.



```
kali@kali:~$ nano /etc/apache2/mods-available/ssl.conf
##
# Some MIME-types for downloading Certificates and CRLs
#
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl

# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is a internal
# terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog builtin

# Inter-Process Session Cache:
# Configure the SSL Session Cache: First the mechanism
# to use and second the expiring timeout (in seconds).
#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.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
# enable only secure ciphers:
SSLCipherSuite HIGH:MEDIUM:!ADH

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

</IfModule>
```