Consegna progetto W12D4

Misure correttive sui servizi:

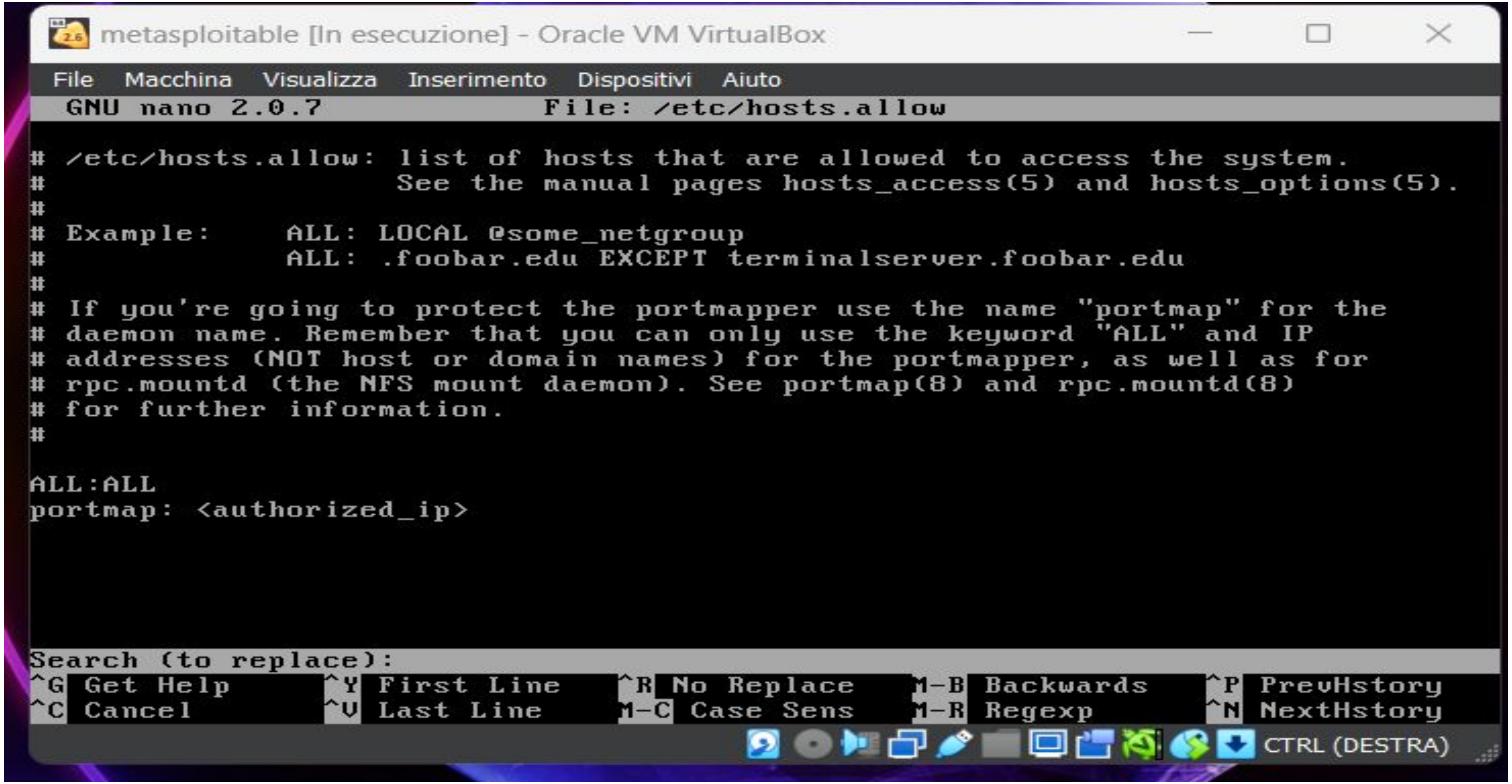
1. Bind Shell Backdoor Detection

2. VNC Server ‘password’ password

3. NFS exported share information disclosure

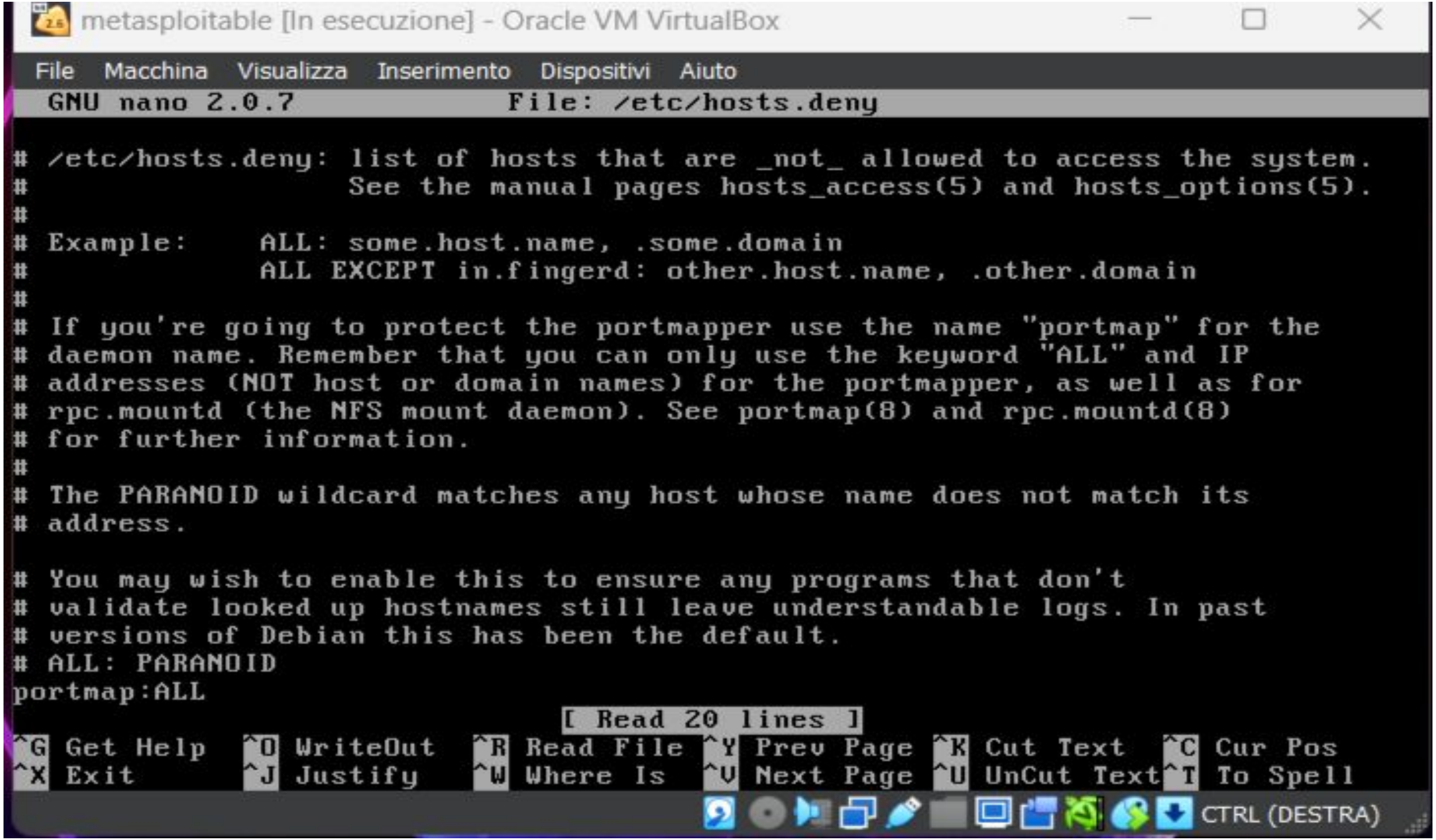
4. Apache Tomcat AJP Connector Request Injection (ghostcat)

NFS exported share information disclosure



metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)

```
  GNU nano 2.0.7                  File: /etc/hosts.allow

# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#

ALL:ALL
portmap: <authorized_ip>





Search (to replace):
^G Get Help      ^Y First Line    ^R No Replace    M-B Backwards    ^P PrevHstory
^C Cancel        ^V Last Line     M-C Case Sens    M-R Regexp       ^N NextHstory
```


metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)

```
  GNU nano 2.0.7              File: /etc/hosts.deny

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.

# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
portmap:ALL
                              [ Read 20 lines ]
^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
```

Comandi utilizzati: NFS

1.

/etc/hosts.deny:

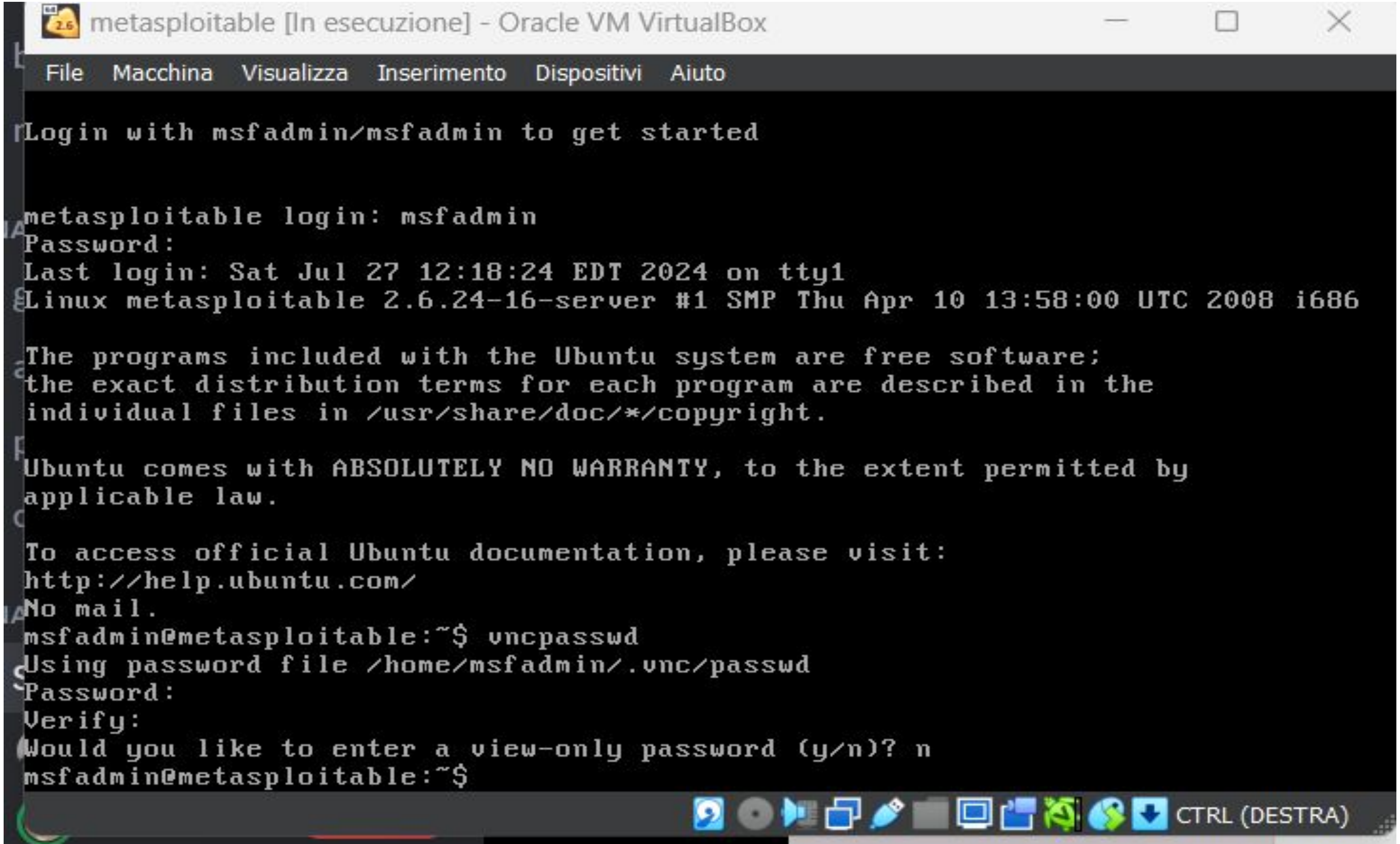
```
sudo nano /etc/hosts.deny
portmap: <authorized_ip>
```

2.

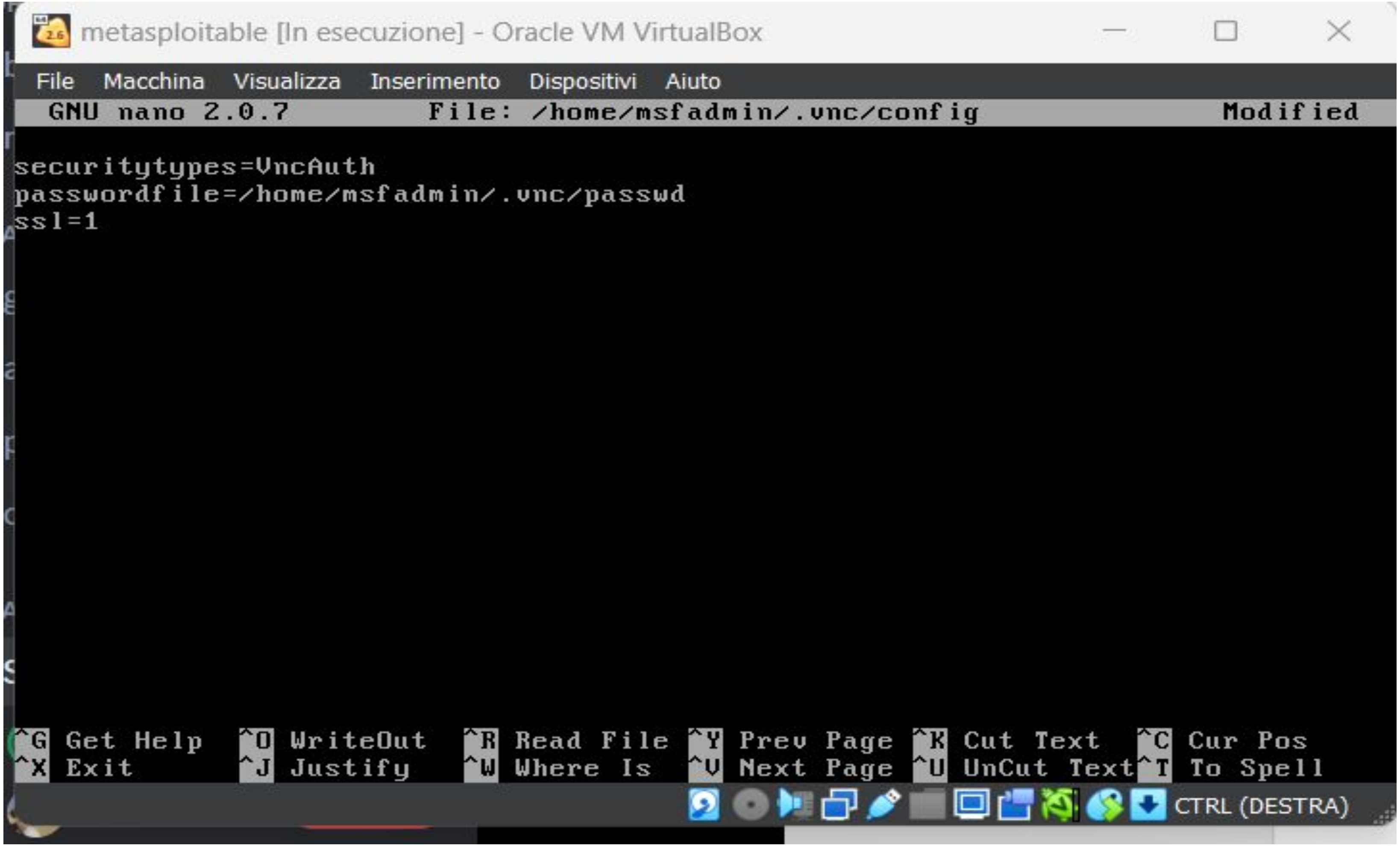
/etc/hosts.allow:

```
sudo nano /etc/hosts.allow
portmap: ALL
```

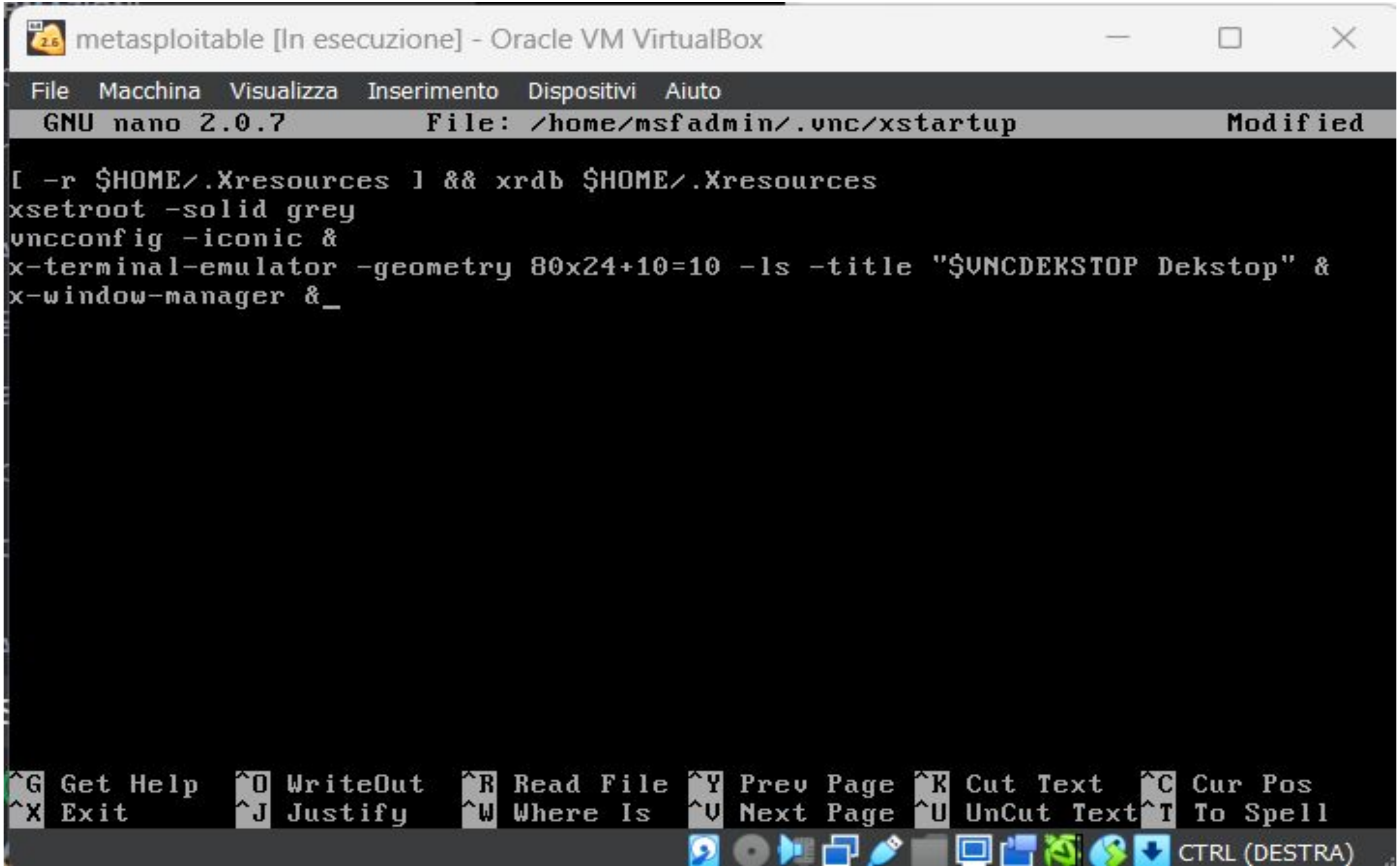
VNC Server ‘password’ password



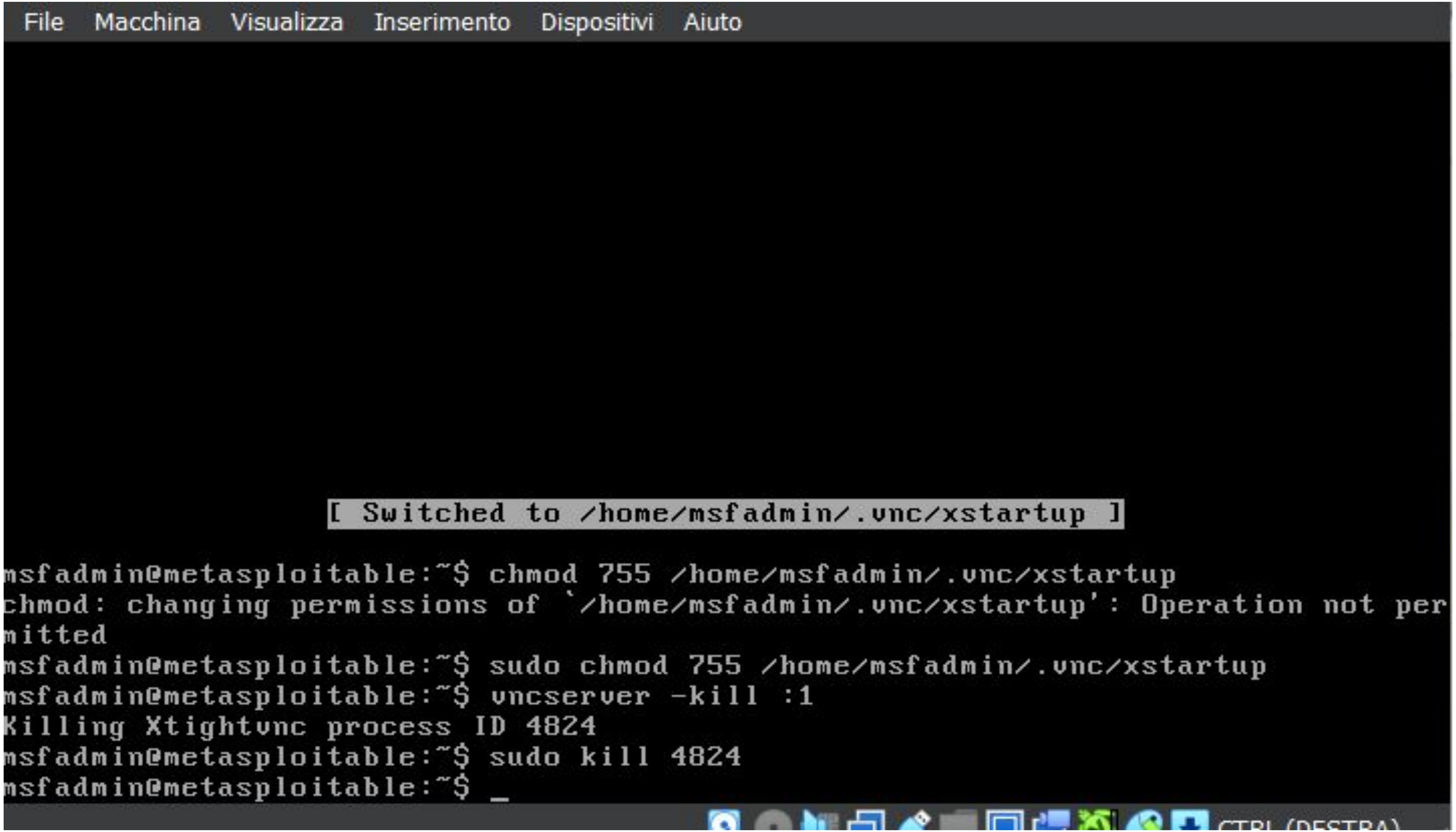
```
Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sat Jul 27 12:18:24 EDT 2024 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:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```



```
  GNU nano 2.0.7           File: /home/msfadmin/.vnc/config              Modified

securitytypes=VncAuth
passwordfile=/home/msfadmin/.vnc/passwd
ssl=1

^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
```



```
  GNU nano 2.0.7          File: /home/msfadmin/.vnc/xstartup                Modified

[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
xsetroot -solid grey
vncconfig -iconic &
x-terminal-emulator -geometry 80x24+10=10 -ls -title "$VNCDEKSTOP Dekstop" &
x-window-manager &_

^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
```



```
[ Switched to /home/msfadmin/.vnc/xstartup ]

msfadmin@metasploitable:~$ chmod 755 /home/msfadmin/.vnc/xstartup
chmod: changing permissions of `/home/msfadmin/.vnc/xstartup': Operation not per
mitted
msfadmin@metasploitable:~$ sudo chmod 755 /home/msfadmin/.vnc/xstartup
msfadmin@metasploitable:~$ vncserver -kill :1
Killing Xtightvnc process ID 4824
msfadmin@metasploitable:~$ sudo kill 4824
msfadmin@metasploitable:~$ _
```

Comandi utilizzati: VNC passwd

1. **vncpasswd**

/home/msfadmin/.vnc/config:

```
 sudo nano /home/msfadmin/.vnc/config
```

```
securitytypes=VncAuth

passwordfile=/home/msfadmin/.vnc/passwd

ssl=1
```

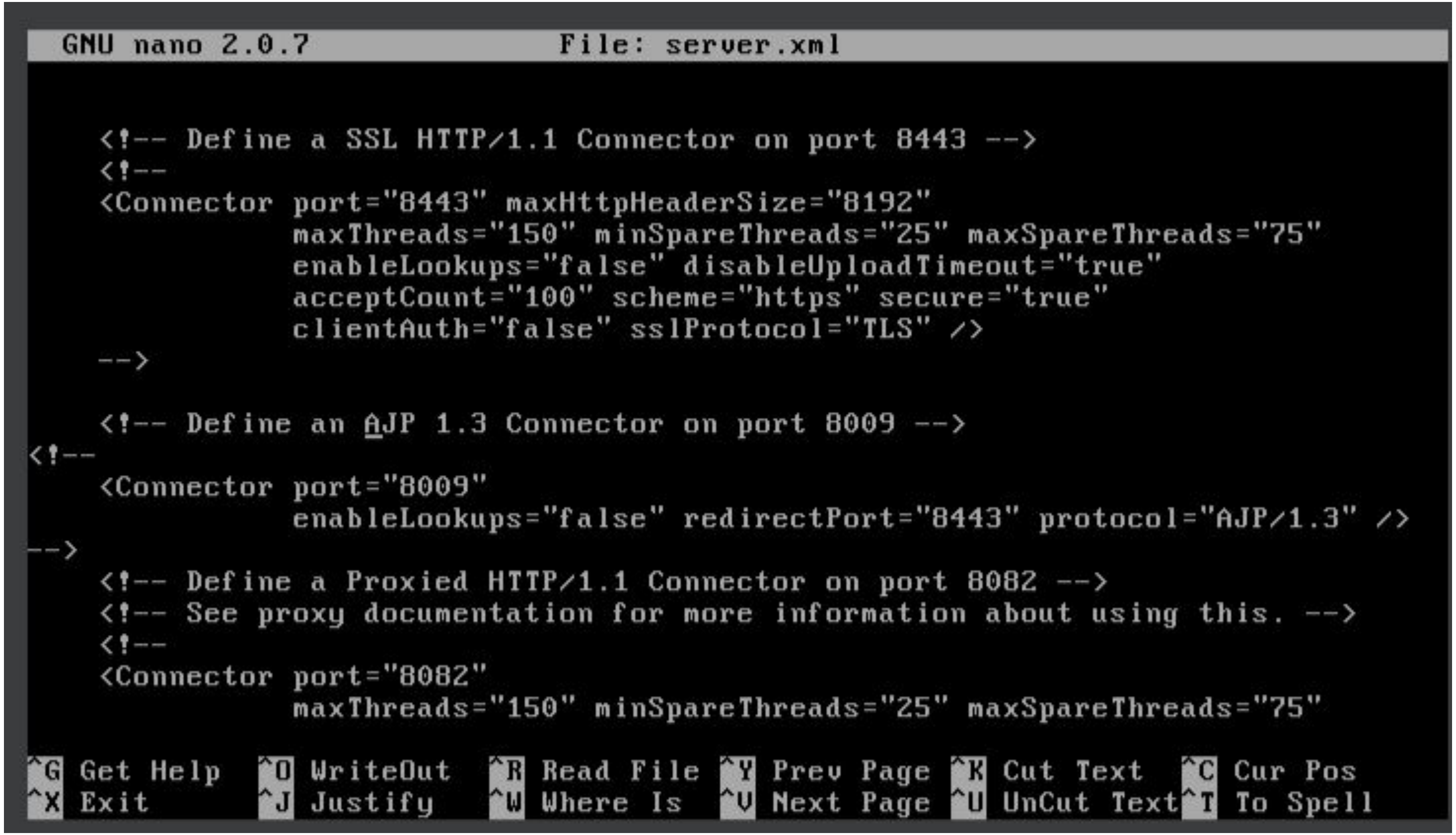
2.

Modifico il file xstartup: sudo nano /home/msfadmin/.vnc/xstartup

```
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources xsetroot -solid grey vncconfig -iconic & x-terminal-emulator
-geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" & x-window-manager &
```

3.**Rendo eseguibile il file xstartup: chmod 755 /home/msfadmin/.vnc/xstartup, infine killo il processo con : sudo kill 4824 (ID)**

Apache Tomcat AJP Connector Request Injection



```
  GNU nano 2.0.7                 File: server.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"

^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
```

Comandi utilizzati: Apache Tomcat AJP

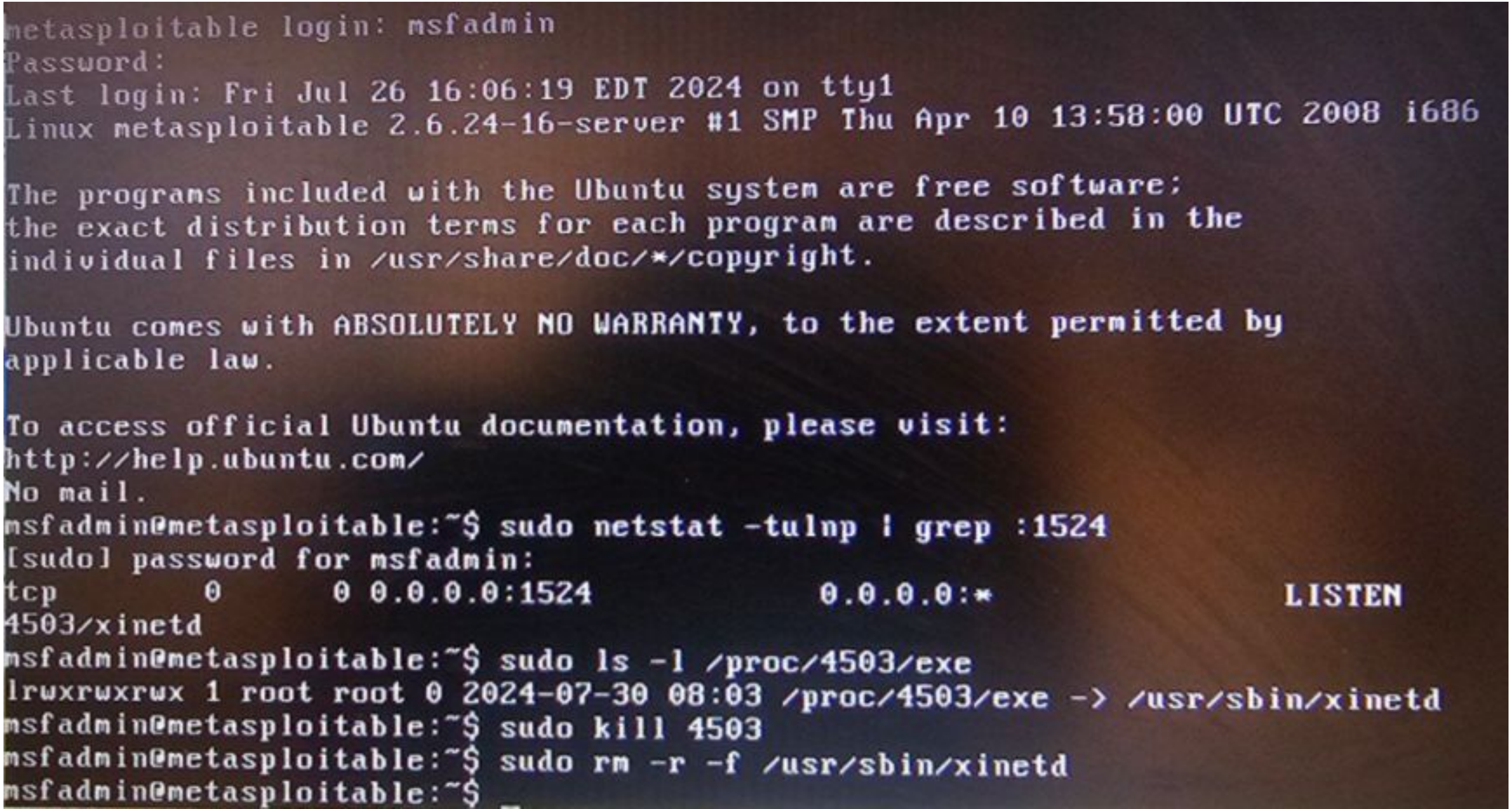
1.

```
sudo nano /etc/tomcat/server.xml
```

Modifico il connettore AJP, dopodichè riavvio il servizio Tomcat con :

```
sudo systemctl restart tomcat
```

Bind Shell Backdoor Detection



```
metasploitable login: msfadmin
Password:
Last login: Fri Jul 26 16:06:19 EDT 2024 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:~$ sudo netstat -tulnp | grep :1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
4503/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4503/exe
lrwxrwxrwx 1 root root 0 2024-07-30 08:03 /proc/4503/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ sudo kill 4503
msfadmin@metasploitable:~$ sudo rm -r -f /usr/sbin/xinetd
msfadmin@metasploitable:~$
```

Comandi utilizzati: Bind Shell

1.

```
sudo netstat -tulnp | grep :1524
```

Visualizzazione del processo: sudo ls -l /proc/4503/exe

2.

Termino il processo con: sudo kill 4503 , ed infine rimuovo la backdoor con: sudo rm -r -f /usr/sbin/xinetd