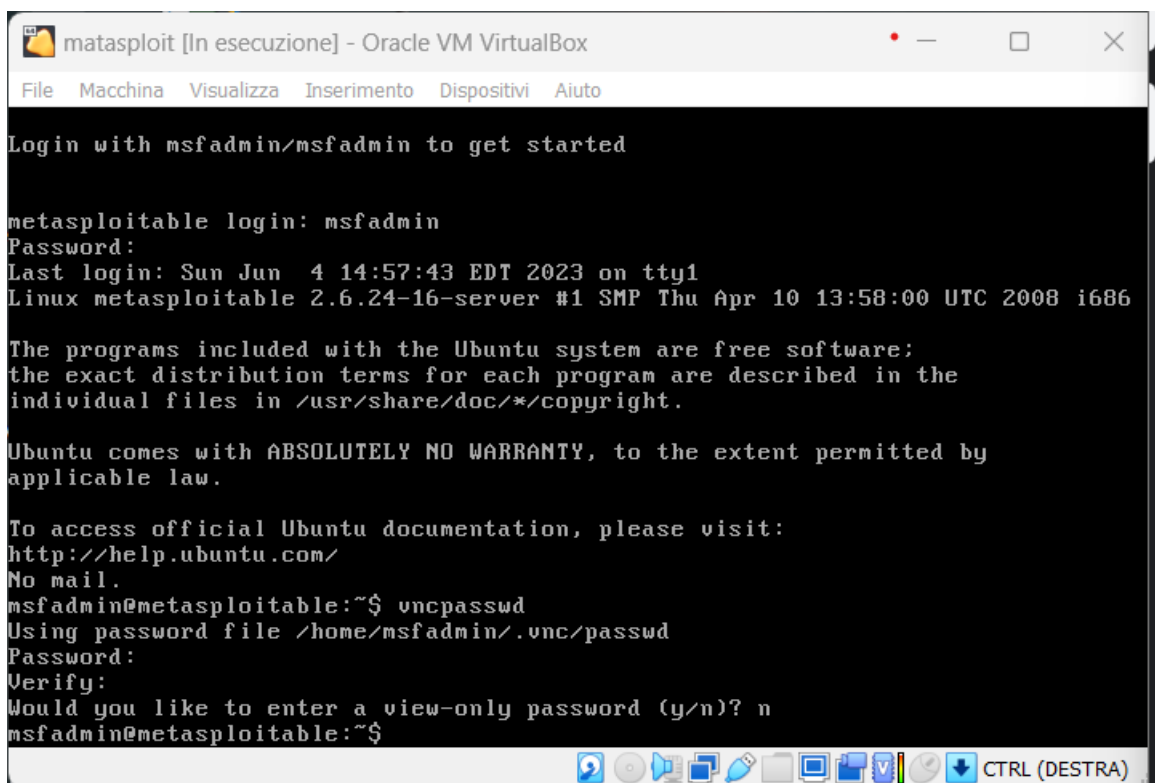


Report REMEDIATION

Avviate le macchine di kali e metasploit abbiamo fatto in modo che pingassero tramite pfsense, eseguito l'accesso su nessus e fatto partire una prima scansione abbiamo ottenuto un report contenente le criticità del sistema trovate dal programma a seguito di una scansione delle porte comuni. Il primo processo da andare ad eseguire sarebbe l'aggiornamento di unix questo passaggio ci permetterebbe di risolvere molte problematiche.

La prima problematica di cui mi sono occupato è stato il cambio password di VNC il quale aveva un password predefinita e con il comando "vncpasswd"



```
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: Sun Jun  4 14:57:43 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

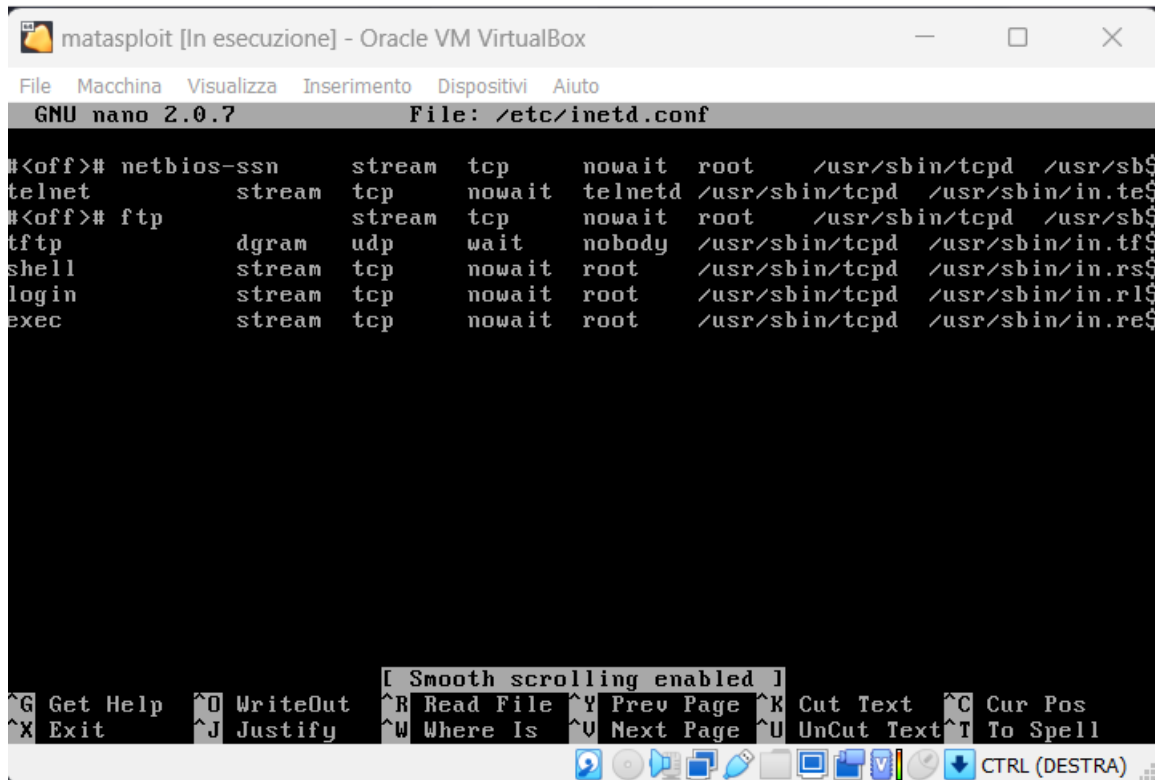
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```

La seconda problematica che si è presentata era legata alla possibilità da parte di un utente esterno attraverso una Backdoor di loggarsi come root.

Per fare ho editato con nano il file di configurazione `/etc/inetd.conf` andando a cancellare l'ultima stringa "ingresloock stream tcp nowait root /bin/bash bash -i" impedendo così l'accesso

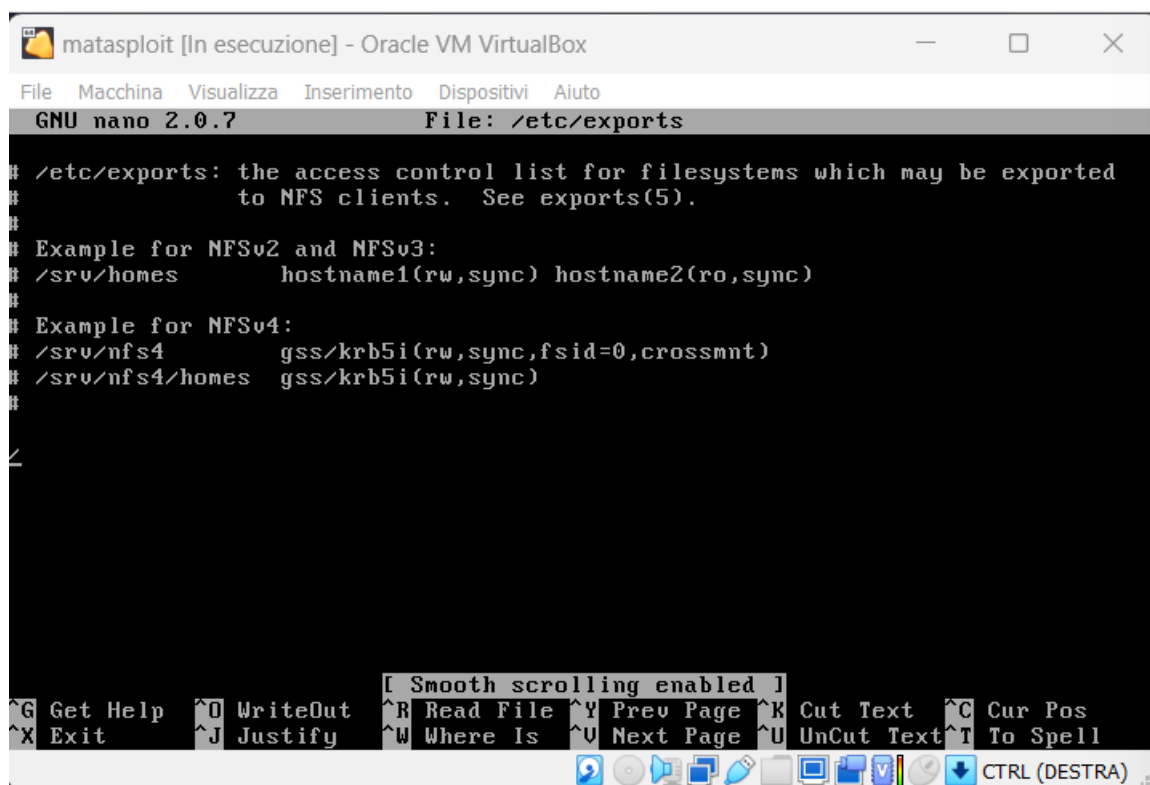


The screenshot shows a terminal window titled "matasploit [In esecuzione] - Oracle VM VirtualBox". Inside the terminal, the GNU nano 2.0.7 text editor is open, editing the file `/etc/inetd.conf`. The file content is as follows:

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
telnet               stream  tcp      nowait  telnetd /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.rsh
login                stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec                 stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
```

The terminal also displays a status bar at the bottom with various keyboard shortcuts and a "CTRL (DESTRA)" indicator.

La terza problematica affrontata è legata ai privilegi NFS i quali se non modificati permettono l'accesso a qualsiasi host quindi sono andato nella configurazione e con nano ho modificato `/etc/exports` eliminando anche in questo caso l'ultima stringa che permetteva l'accesso.



The screenshot shows a terminal window titled "matasploit [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 editor, editing the 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)
```

The bottom of the terminal shows the nano editor's help menu with various keyboard shortcuts for navigation and editing. A status bar at the bottom right indicates "CTRL (DESTRA)".