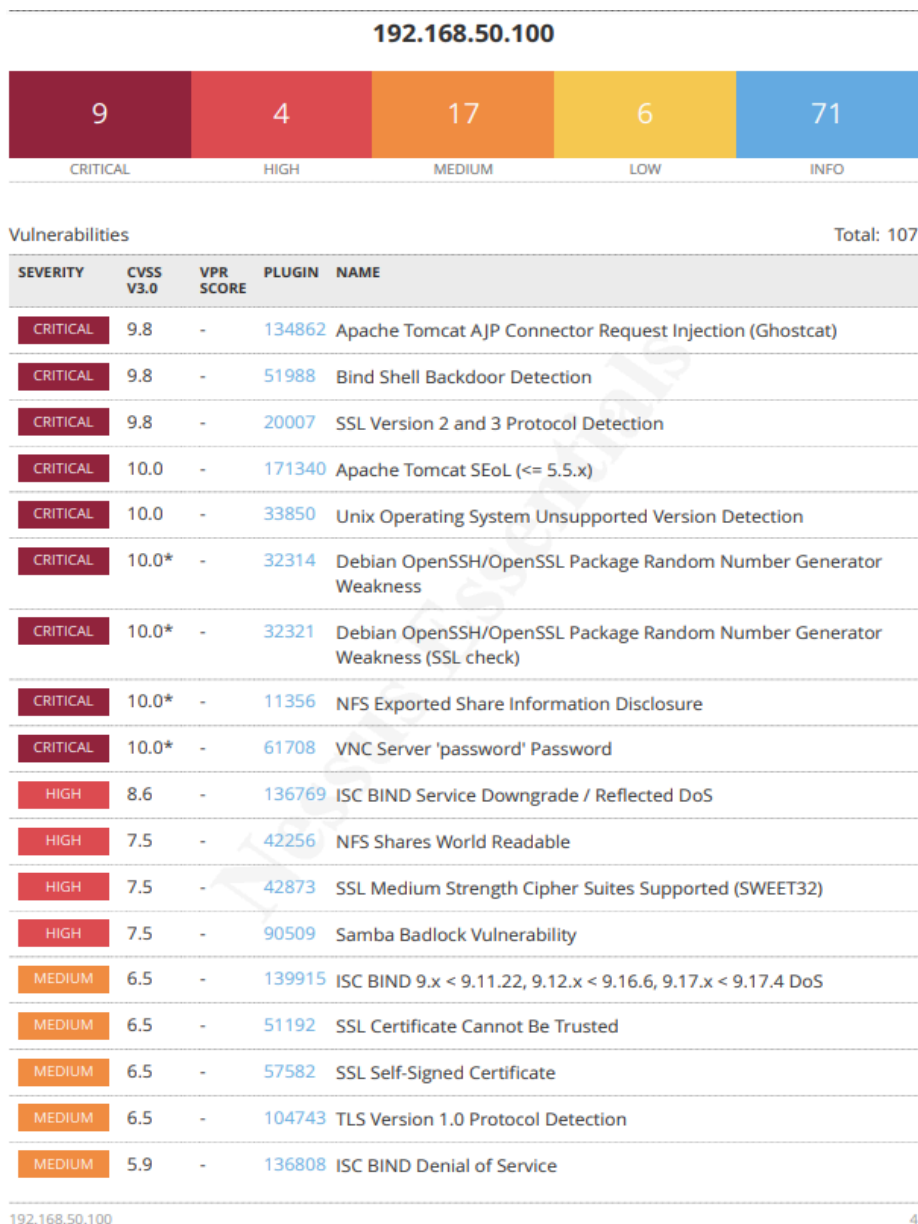


EPICODE

FINE MODULO 3

Traccia: Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche e provate ad implementare delle azioni di rimedio.

Avviando Nessus su Firefox da Kali ho effettuato un Basic Network Scan con target IP di Metasploitable, nel mio caso 192.168.50.100; al termine della scansione il risultato è questo:



Per portare a termine il progetto ho scelto tre vulnerabilità critiche tra le disponibili. Ho scelto di risolvere **Bind Shell Backdoor Detection**, **NFS Exported Share Information Disclosure**, **VNC Server 'password' Password**.

- Bind Shell Backdoor Detection (risoluzione)

Dopo avere controllato i dettagli nel report dettagliato di Nessus (vedi foto sotto);

51988 (1) - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/1524/wild_shell)

```
Nessus was able to execute the command "id" using the
following request :

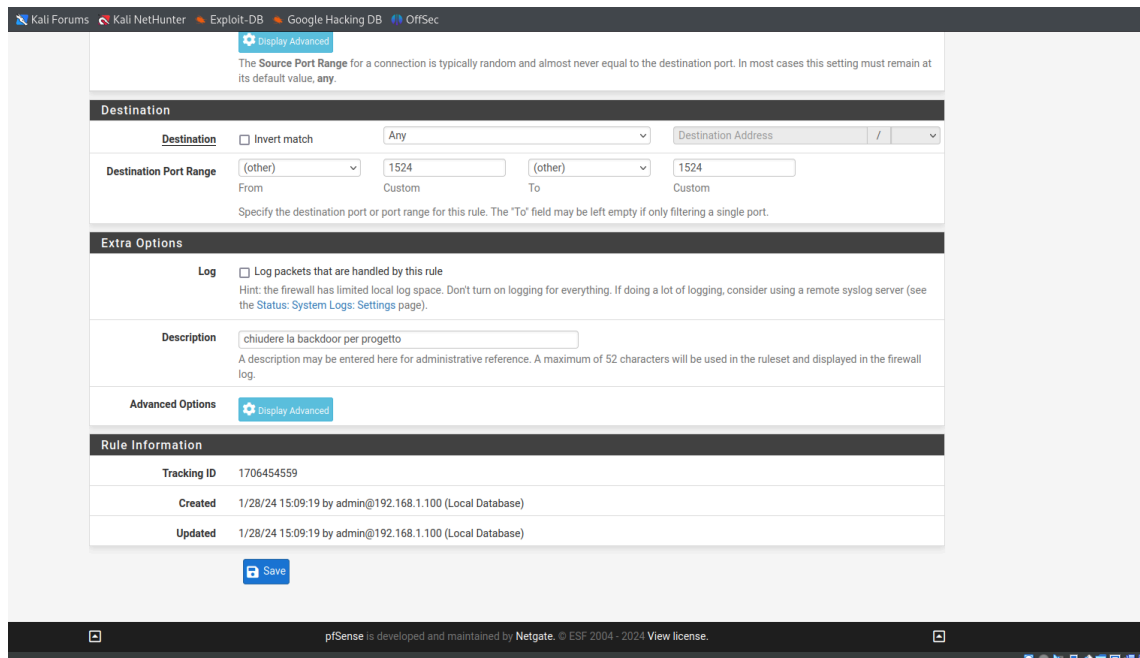
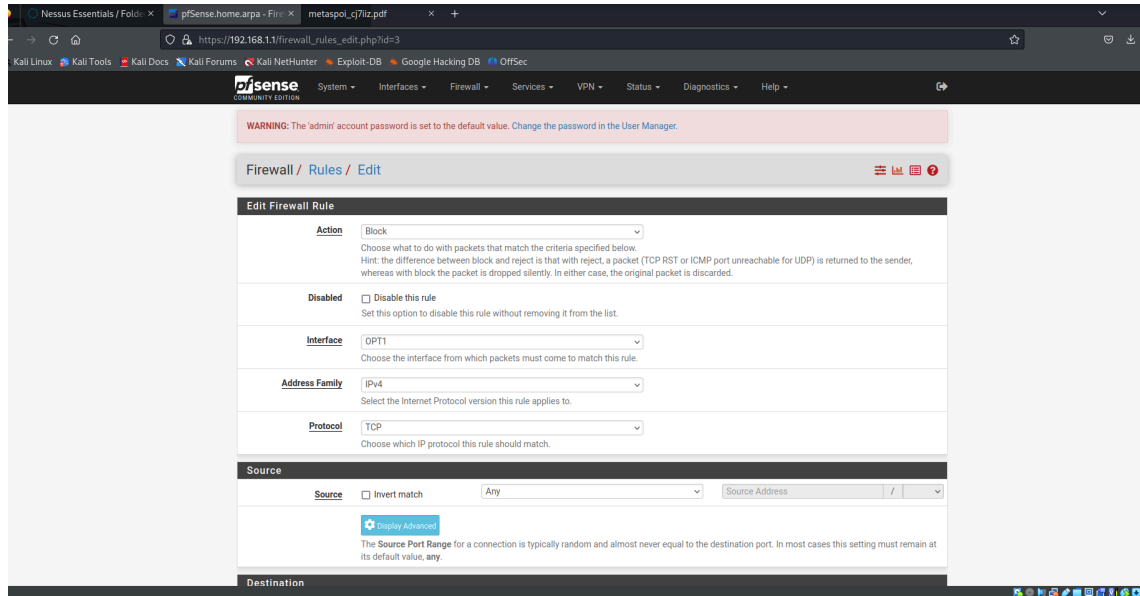
This produced the following truncated output (limited to 10 lines) :
..... snip .....
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
..... snip .....
```

51988 (1) - Bind Shell Backdoor Detection

17

Ho creato una regola nel Firewall per Metasploitable dove vado a bloccare la porta 1524 su pfSense:

- Nel menu principale di pfSense ho selezionato "Firewall", nel suo sottomenù ho selezionato 'Rules'
- Ho scelto l'interfaccia (OPT1/quella di Metasploitable) alla quale voglio bloccare la porta 1524
- Ho pigiato su 'Add' per creare e aggiungere una nuova regola
- Ho configurato la regola in questo modo (vedi foto sotto):



- VNC Server 'password' Password

61708 (1) - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

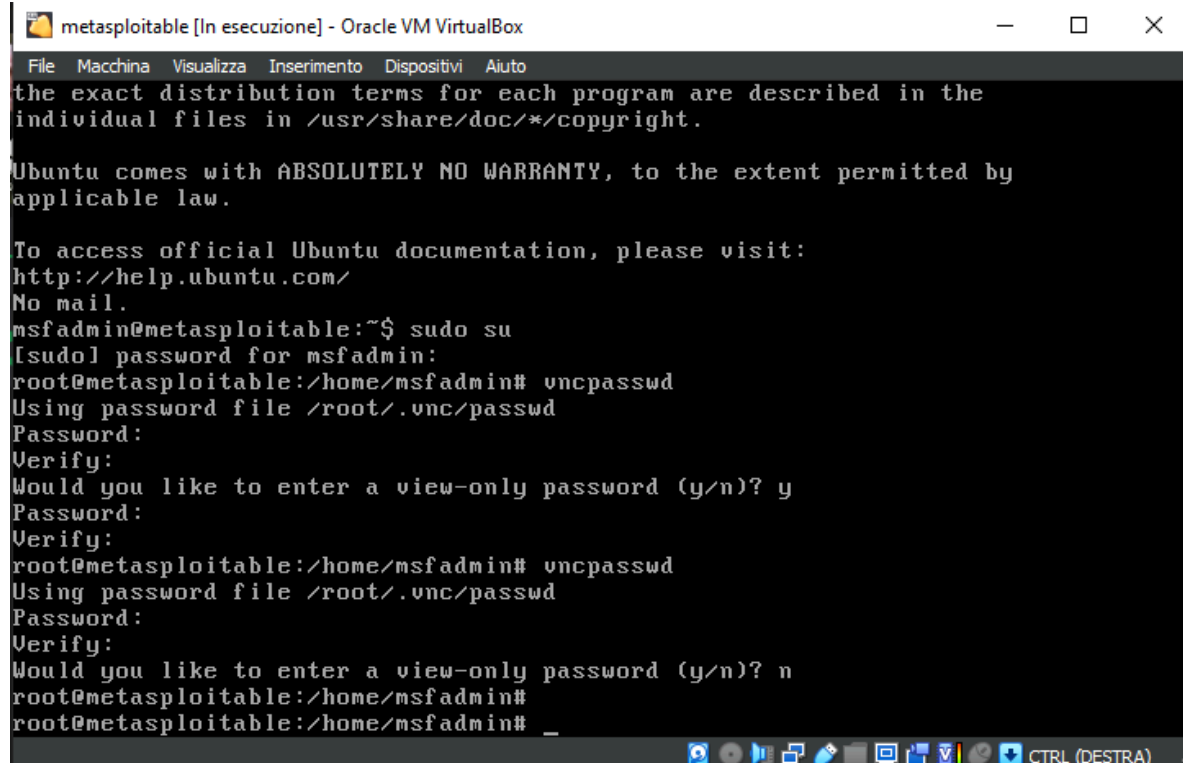
Plugin Output

192.168.50.100 (tcp/5900/vnc)

```
Nessus logged in using a password of "password".
```

Per risolvere questa vulnerabilità da terminale di Metasploitable ho lanciato il comando 'sudo su', così da avere i permessi di root, e successivamente ho lanciato 'vnc passwd', di seguito ho inserito la nuova password; passando al terminale di Kali e tramite il comando 'vncviewer 192.168.50.100(IP Meta)' ho controllato se la password fosse stata salvata.

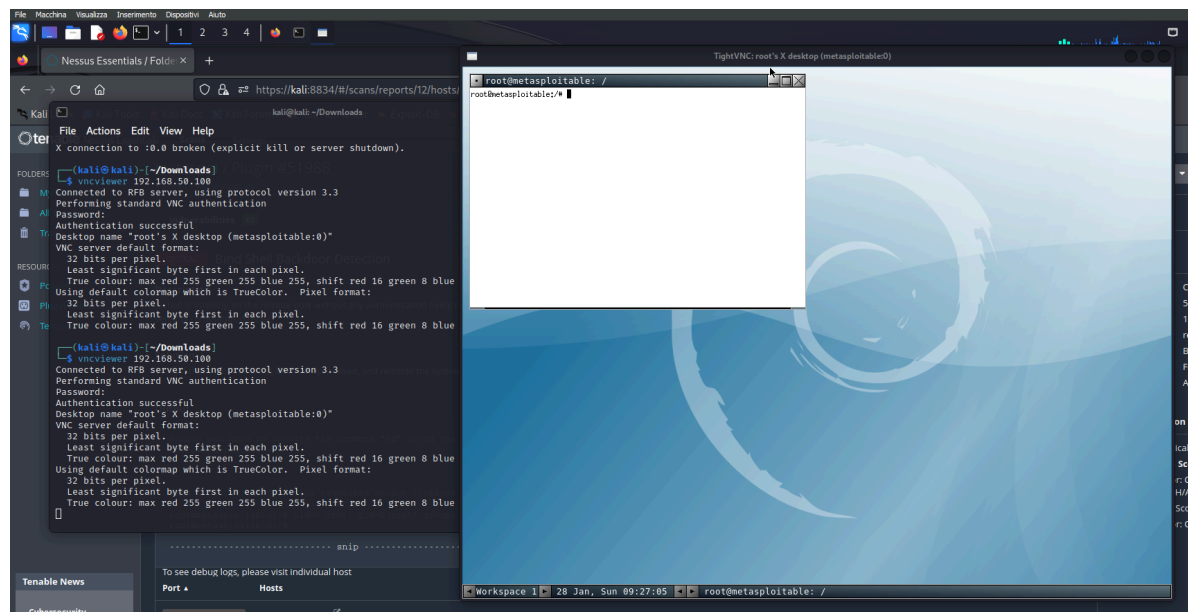
Sotto lascio gli screenshot



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
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 su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# _
```



- NFS Exported Share Information Disclosure

11356 (1) - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

Exploitable With

Metasploit (true)

Plugin Information

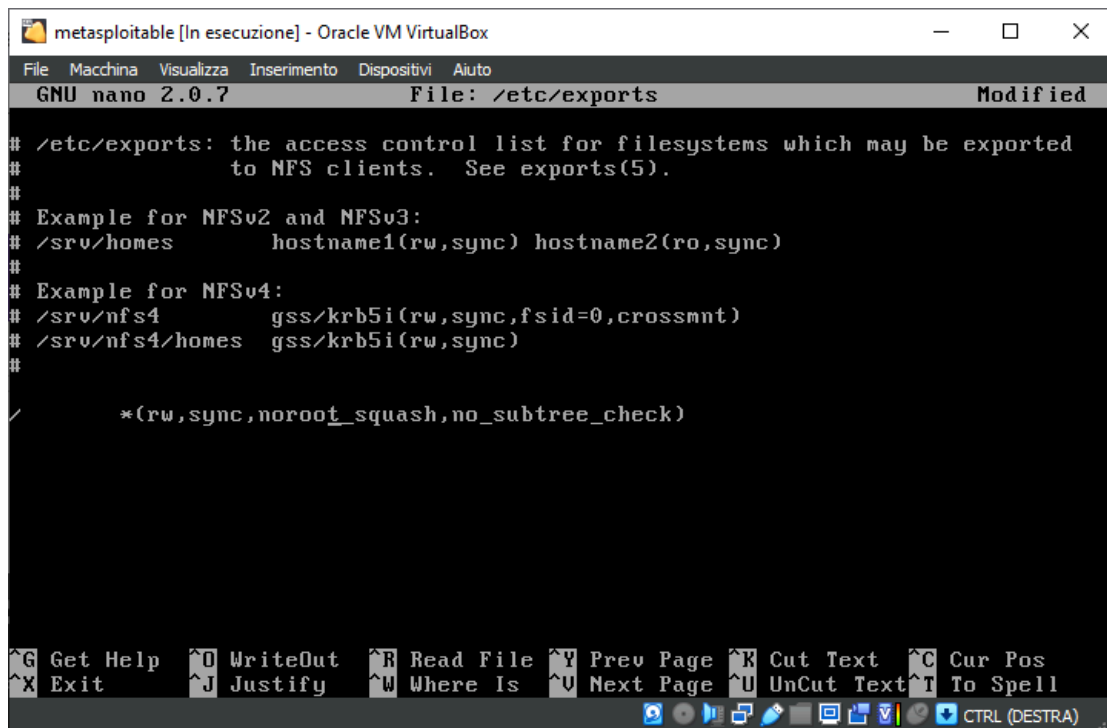
Published: 2003/03/12, Modified: 2023/08/30

Plugin Output

192.168.50.100 (udp/2049/rpc-nfs)

Per risolvere ho scelto di verificare e configurare il file `/etc/exports` sul server NFS. Limitando l'accesso solo agli host autorizzati e imposta le giuste autorizzazioni sui file esportati.

Sul terminale di Meta ho lanciato il comando `'sudo nano /etc/exports'` e ho applicato le modifiche, cancellando parte del contenuto:

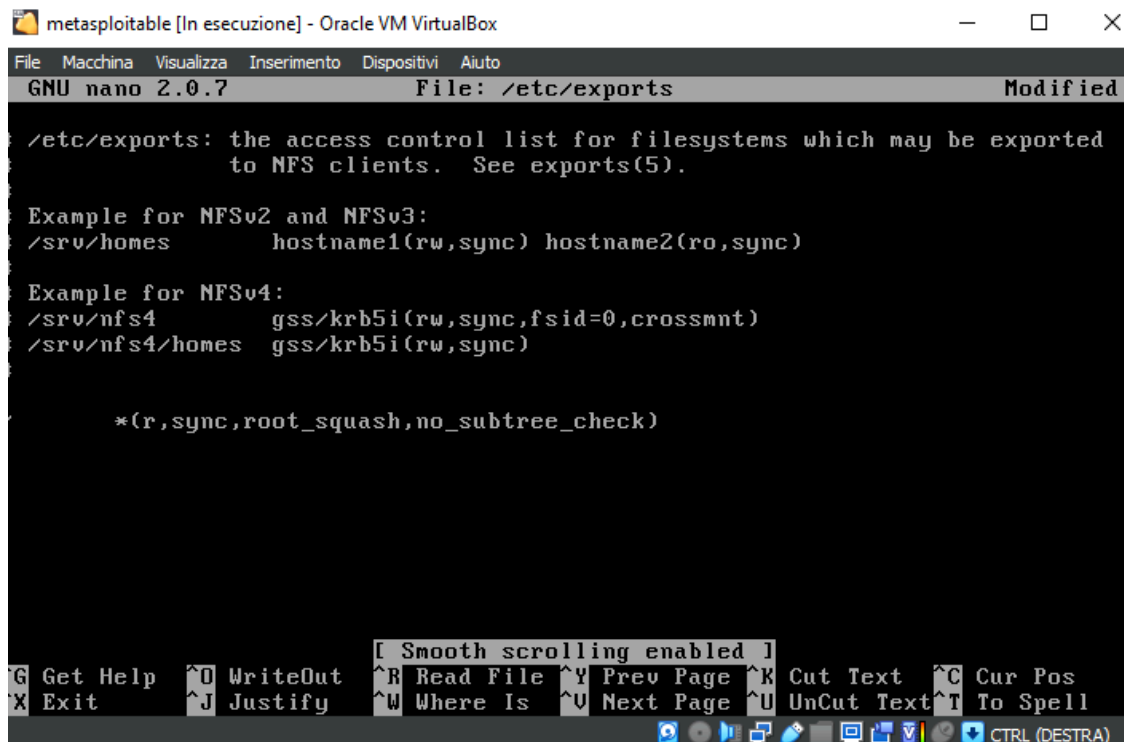


The screenshot shows a terminal window titled "metasploitable [In esecuzione] - Oracle VM VirtualBox". The window contains the GNU nano 2.0.7 editor editing the file /etc/exports. The file content is as follows:

```
# /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, noroot_squash, no_subtree_check)
```

The bottom of the window shows a status bar with various keyboard shortcuts and a toolbar with icons for file operations and a "CTRL (DESTRA)" button.

RISOLUZIONE:



The screenshot shows the same terminal window as before, but the /etc/exports file has been modified. The content is now:

```
# /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)
#
*(r, sync, root_squash, no_subtree_check)
```

The bottom of the window shows the same status bar, but with a message "[Smooth scrolling enabled]" appearing above the keyboard shortcuts.