


# Epicode S5/L5 Cybersecurity

Remediation

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.



Nell'esercizio di oggi viene richiesto di  
rimediare ad alcune vulnerabilità che abbiamo  
visto nel report Nessus il giorno precedente.

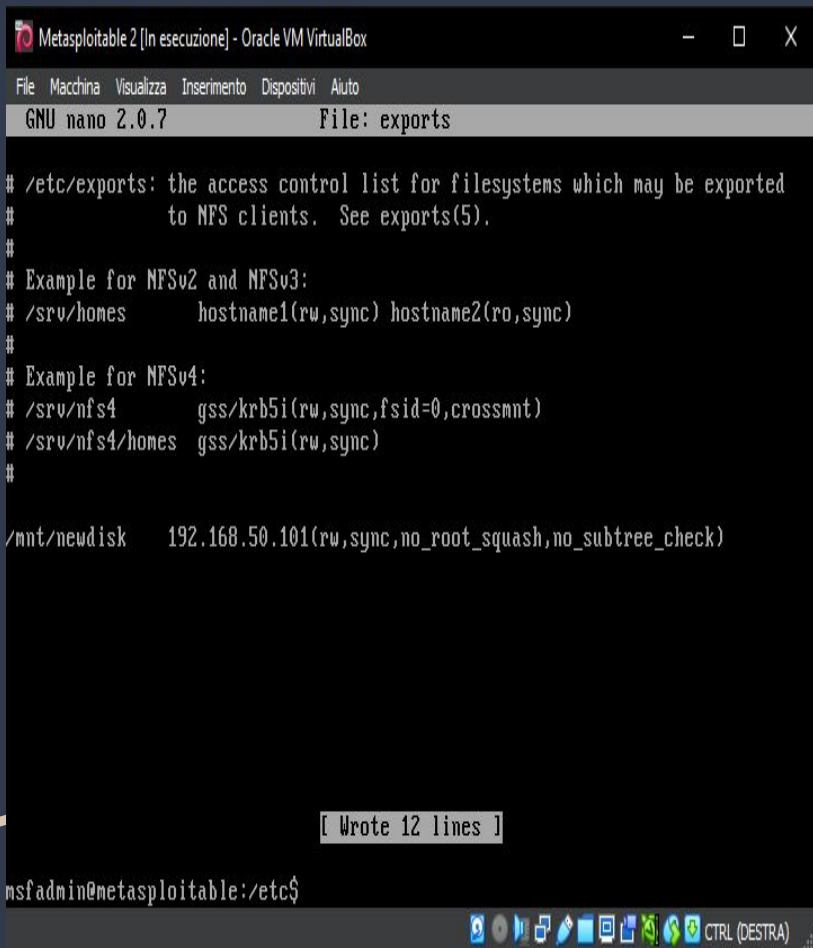
Ne abbiamo selezionate tre:

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ ufw enable
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded
msfadmin@metasploitable:~$ ufw status
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

To                Action From
--                -
1524:tcp           DENY  Anywhere
1524:udp           DENY  Anywhere

msfadmin@metasploitable:~$ _
```

La prima vulnerabilità a cui andiamo a porre rimedio è una porta in ascolto. Per farlo, abilitiamo il firewall di meta UFW e creiamo una regola per chiuderla.



The screenshot shows a terminal window titled "Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 text 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)
#
/mnt/newdisk     192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```

At the bottom of the terminal, a status bar indicates "[ Wrote 12 lines ]". The prompt at the bottom is "msfadmin@metasploitable:/etc\$". The bottom of the window shows a taskbar with various icons and the text "CTRL (DESTRA)".

La seconda invece, si tratta del “NFS Exported Share Information Disclosure”, una lista di filesystems che può essere sovrascritta esternamente. Andiamo quindi a modificare il file in maniera tale che solo gli host autorizzati possano modificarla.

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

To          Action  From
--          -
1524:tcp    DENY    Anywhere
1524:udp    DENY    Anywhere

msfadmin@metasploitable:~$ sudo ls -la
.          .distcc      .mysql_history  .sudo_as_admin_successful
..         .esercizio.py.swp  .profile        vulnerable
.bash_history  .gconf      .rhosts
clientbackdoor.py  .gconfd    .ssh
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# ls -la
.          .distcc      .mysql_history  .sudo_as_admin_successful
..         .esercizio.py.swp  .profile        vulnerable
.bash_history  .gconf      .rhosts
clientbackdoor.py  .gconfd    .ssh
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# reboot
```

La terza vulnerabilità che corregeremo è invece una password debole per il server VNC. Per farlo, accediamo alla directory e, utilizzando il comando `vncpasswd`, andiamo a modificarla.