

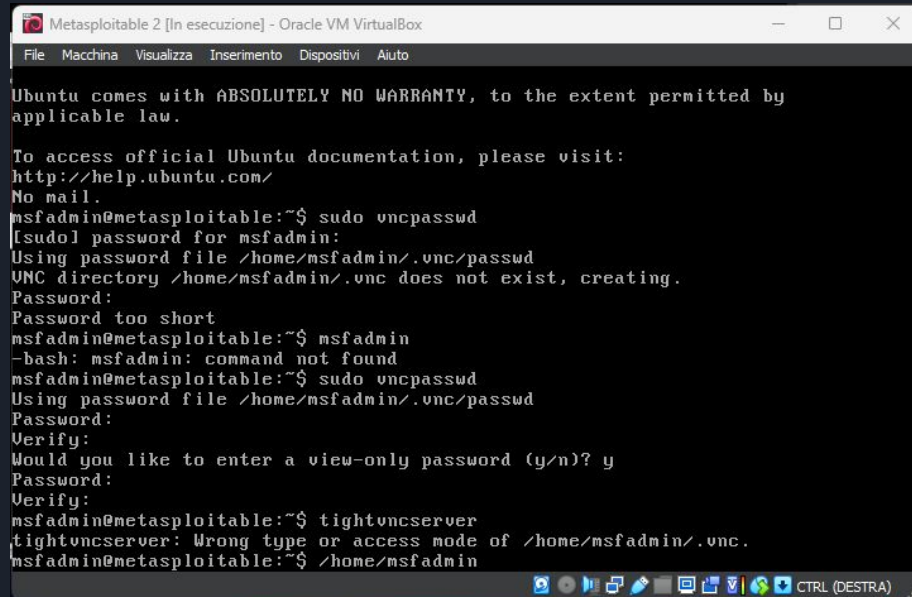


Consegna S5L5

Remediation delle vulnerabilità

VNC Server Password

Per modificare la password del VNC Server, troviamo all'interno della directory msfadmin, con il comando ls-a, il directory .vnc. All'interno di questa directory, andremo a eseguire il comando "vncpasswd" per cambiare la password. Alla fine riavviamo la macchina.



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

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 vncpasswd
[sudo] password for msfadmin:
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Password too short
msfadmin@metasploitable:~$ msfadmin
-bash: msfadmin: command not found
msfadmin@metasploitable:~$ sudo vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$ tightvncserver
tightvncserver: Wrong type or access mode of /home/msfadmin/.vnc.
msfadmin@metasploitable:~$ /home/msfadmin
```

NFS Exported share information disclosure

Per quanto riguarda questa vulnerabilità, la remediation da applicare è quella di inserire all'interno della sottocartella del root /etc. La prima cosa da fare è quella di visualizzare all'interno delle sottocartelle del root con "ls -a". Cerchiamo la directory "/etc" e apriamo il file "exports", all'interno di questo file, andremo a modificare l'* in fondo alla pagina con l'ip della nostra macchina. Una volta fatto, riavviamo la macchina.

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: exports

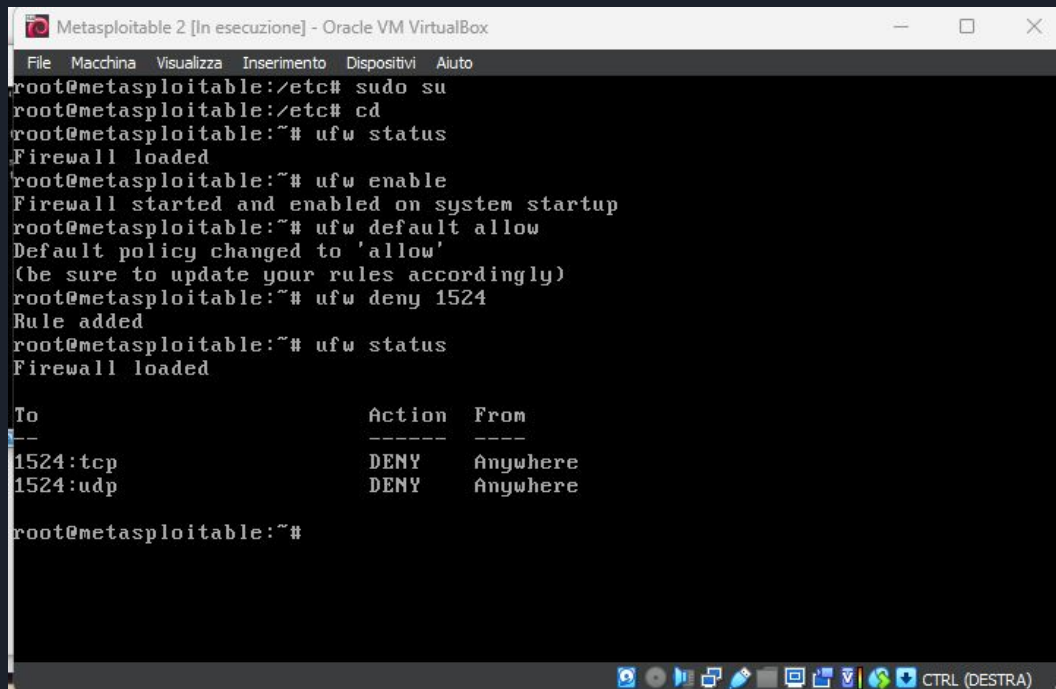
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: exports

# /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 192.168.32.102(rw,sync,no_root_squash,no_subtree_check)
```

Bind shell backdoor detection

Per quanto riguarda la risoluzione di questa vulnerabilità, ho abilitato il firewall di Metasploitable con il comando “UFW ENABLE”. Dopodichè, ho detto al firewall di acconsentire a tutte le regole di default con “UFW DEFAULT ALLOW”.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
root@metasploitable:/etc# sudo su
root@metasploitable:/etc# cd
root@metasploitable:~# ufw status
Firewall loaded
root@metasploitable:~# ufw enable
Firewall started and enabled on system startup
root@metasploitable:~# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:~# ufw deny 1524
Rule added
root@metasploitable:~# ufw status
Firewall loaded

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

root@metasploitable:~#
```

Samba Badlock Vulnerability

Come per la vulnerabilità precedente andremo ad aggiungere delle regole ad hoc per il firewall ma stavolta sulle porte 139 e 445

```
Sorry, try again.
[sudo] password for msfadmin:
sudo: pam_authenticate: Conversation error
msfadmin@metasploitable:~$ sudo sssssssu
[sudo] password for msfadmin:
sudo: pam_authenticate: Conversation error
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:/home/msfadmin# ufw deny 139
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded
```

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

```
root@metasploitable:/home/msfadmin# _
```