

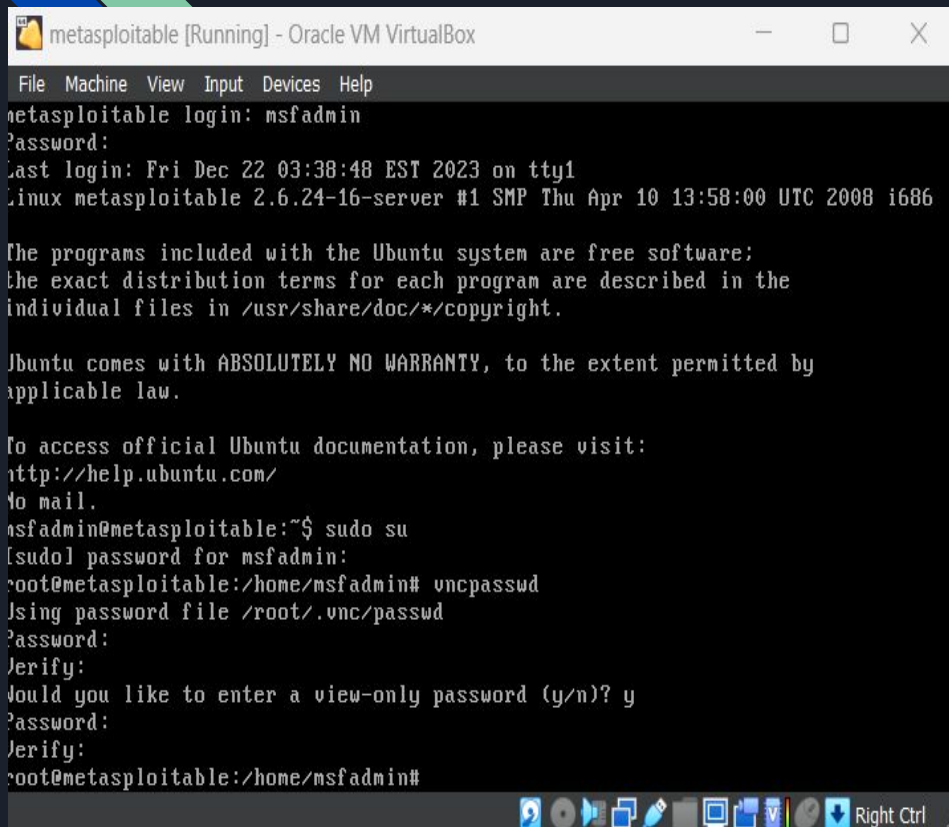


REPORT E FIX DELLE VULNERABILITA'

Vulnerabilita' scelte e fixate:

1. VNC Server Password
2. Bind Shell Backdoor
3. NFS Exported Share
4. Samba Badlock Vuln.

(1)VNC SERVER PASSWORD



```
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
metasploitable login: msfadmin
Password:
Last login: Fri Dec 22 03:38:48 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

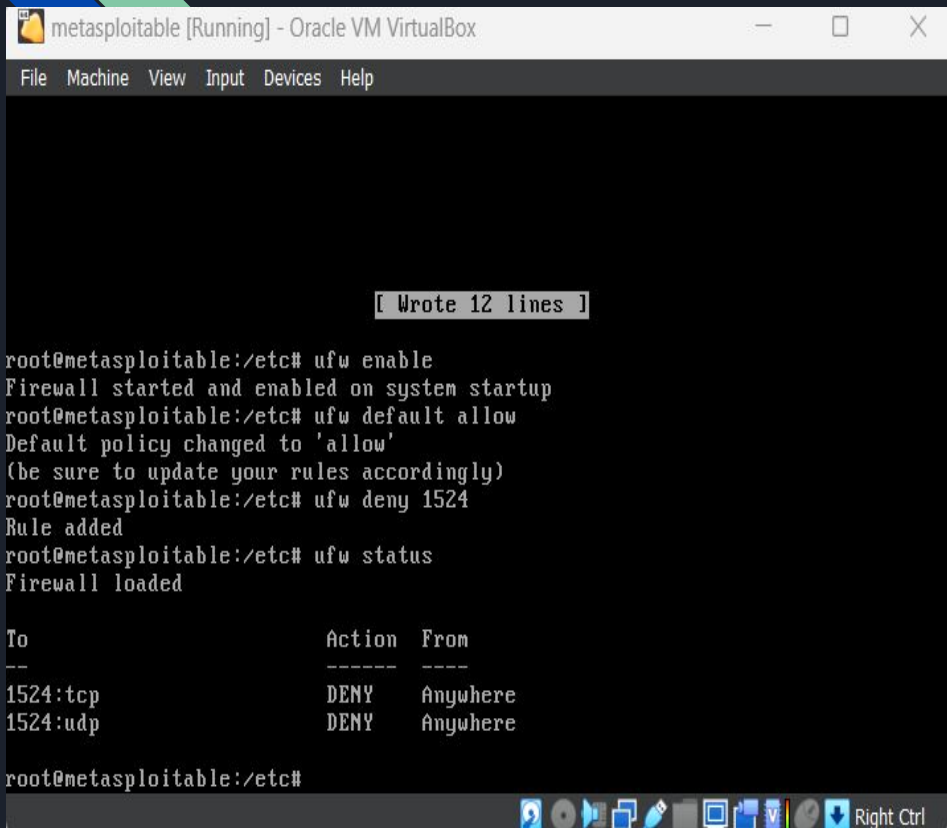
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
To 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#
```

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.

(2) BIND SHELL BACKDOOR



The screenshot shows a terminal window titled "metasploitable [Running] - Oracle VM VirtualBox". The terminal output shows the following commands and their results:

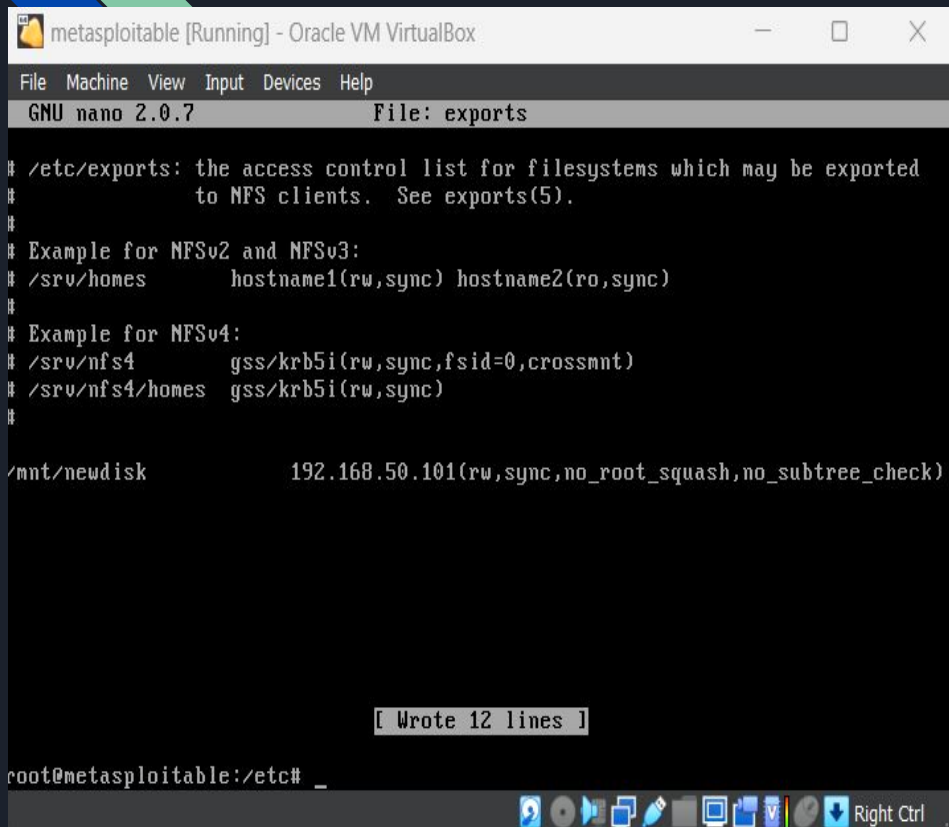
```
root@metasploitable:/etc# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/etc# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/etc# ufw deny 1524
Rule added
root@metasploitable:/etc# ufw status
Firewall loaded
```

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

The terminal ends with the prompt `root@metasploitable:/etc#`. A status bar at the bottom of the window shows various icons and the text "Right Ctrl".

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”.

(3) NFS EXPORTED SHARE



The screenshot shows a terminal window titled "metasploitable [Running] - Oracle VM VirtualBox". Inside the terminal, the GNU nano 2.0.7 text editor is open, editing the file "/etc/exports". The editor's status bar at the top indicates "File: exports" and "[Wrote 12 lines]". 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)
```

The terminal prompt at the bottom is "root@metasploitable:/etc# _". The VirtualBox window includes a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help", and a taskbar at the bottom with various icons and a "Right Ctrl" label.

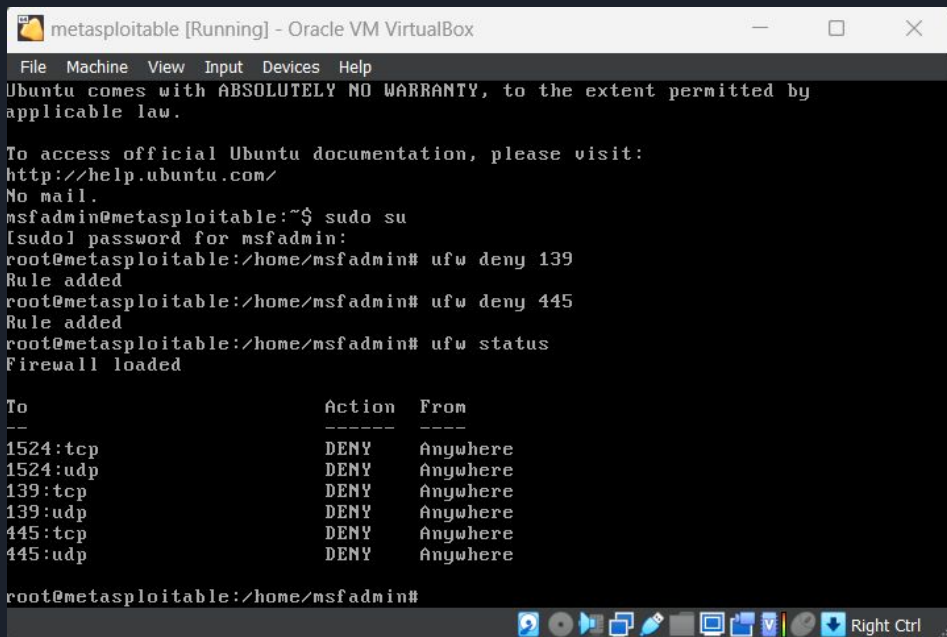
Per sistemare questa vulnerabilità siamo andati a cercare il file “exports” nella cartella /etc e siamo andati a indicare un montaggio di un nuovo disco dandogli come indirizzo ip quello della macchina stessa

(4.1) SAMBA BADLOCK VULNERABILITY

```
kali@kali: ~  
File Actions Edit View Help  
$ nmap -sv 192.168.50.101 -T5  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-22 10:57 EST  
Nmap scan report for 192.168.50.101  
Host is up (0.00030s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet   Linux telnetd  
25/tcp    open  smtp     Postfix smtpd  
53/tcp    open  domain   ISC BIND 9.4.2  
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind  2 (RPC #100000)  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec     netkit-rsh rexecd  
513/tcp   open  login    OpenBSD or Solaris rlogind  
514/tcp   open  shell    Netkit rshd  
1099/tcp  open  java-rmi  GNU Classpath grmiregistry  
1524/tcp  filtered ingreslock  
2049/tcp  open  nfs      2-4 (RPC #100003)  
2121/tcp  open  ftp      ProFTPD 1.3.1  
3306/tcp  open  mysql    MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc      VNC (protocol 3.3)  
6000/tcp  open  X11      (access denied)  
6667/tcp  open  irc      UnrealIRCd
```

Per sistemare questa vulnerabilità abbiamo iniziato con una scansione utilizzando il tool nmap per localizzare le porte che utilizza il servizio samba, in questo caso sono due (139TCP e 445TCP).

(4.2) SAMBA BADLOCK VULNERABILITY



```
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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# ufw deny 139
Rule added
root@metasploitable:/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

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

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

Ora che abbiamo trovato le porte utilizzate dai servizi Samba possiamo utilizzare il firewall come con la vulnerabilità numero 2 (Bind Shell Backdoor) e possiamo aggiungere delle regole a quelle porte così da sistemare questa vulnerabilità grazie a UFW e con pochi comandi.