

## SCANSIONE COMPLETA METASPOITABLE

L'esercitazione di oggi consisteva nell'intervento su alcune vulnerabilità di livello Critical.

- **NFS Exported Share Information Disclosure**
- **VNC Server 'password' Password**
- **Blind Shell Backdoor Detection**

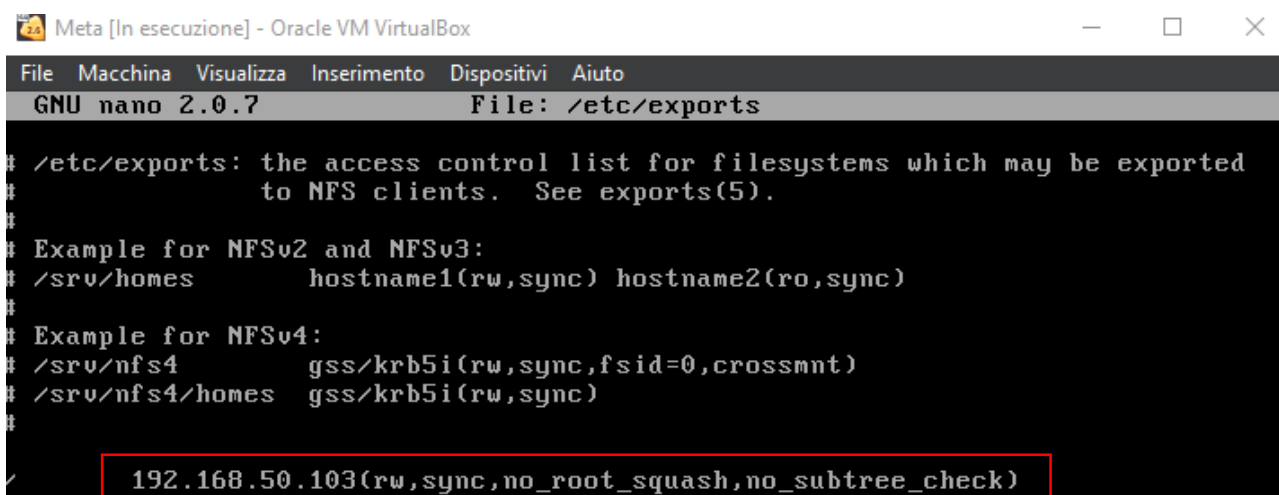
Modalità Intervento.

Per prima cosa ho effettuato una semplice scansione -sV (TCP os detection) con Nmap per individuare le porte su cui erano presenti due vulnerabilità (NFS P:2049 – BLINDSHELL P:1524)

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-25 04:31 EST
Nmap scan report for 192.168.50.103
Host is up (0.00029s 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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi        GNU Classpath grmiregistry
1524/tcp  open  bindshell       Metasploitable root shell
2049/tcp  open  nfs             2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
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
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
8180/tcp  open  http            Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 193.60 seconds
```

**NFS Exported Share Information Disclosure** come vulnerabilità riscontrata consisteva nella possibilità di chiunque connesso con metasploitable di avere accesso ai Network File System. Siamo intervenuti modificando i privilegi di "root" all'interno di Metasploitable.

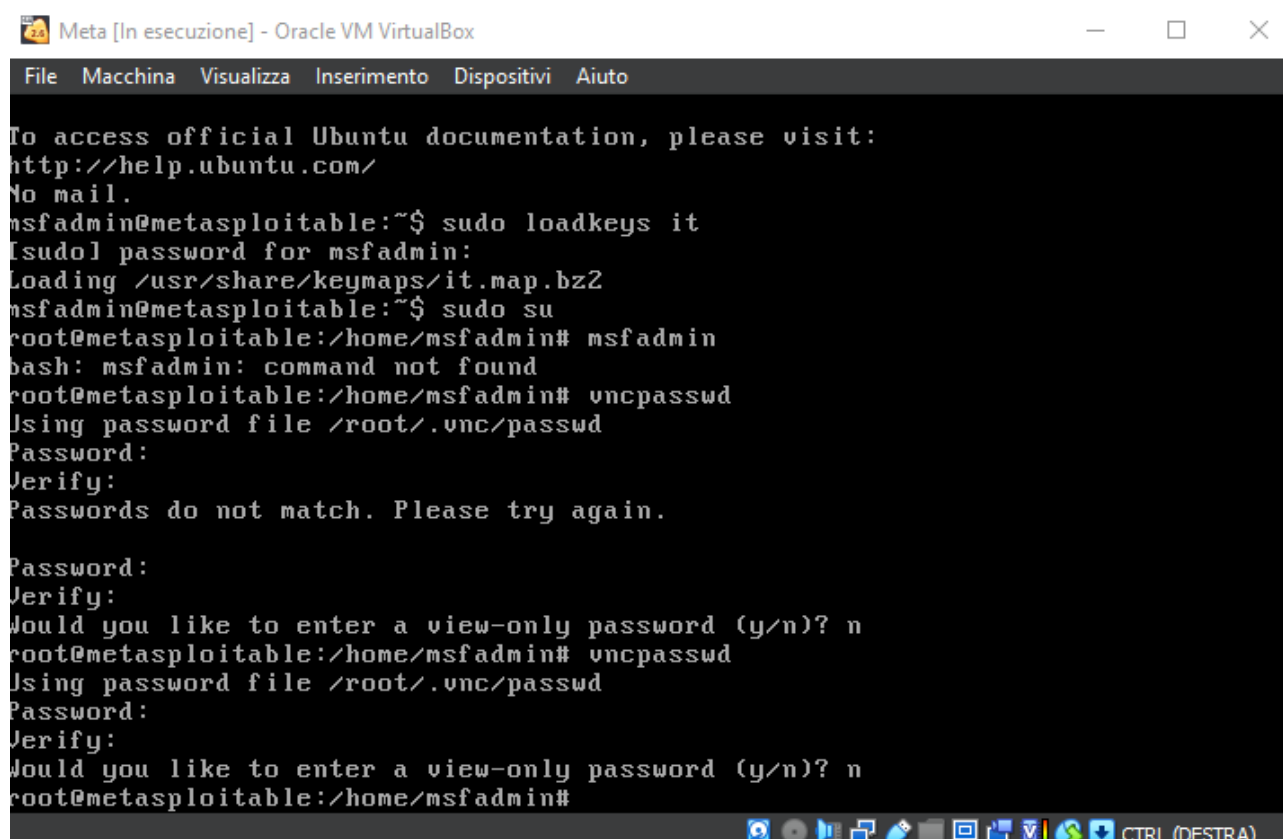


```
Meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports

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

Modificando Exports (controlla quali file system vengono esportati su host remoti) abbiamo modificato il campo inserendo l'IP di metasploitable. In modo da renderlo l'unico in possesso dei privilegi root.

**VNC Server 'password' Password** come vulnerabilità riscontrata consisteva in una password molto debole e molto facile da scoprire. Modificare il file VNC (Virtual Network Computing) /passwd inserendo una password più complessa

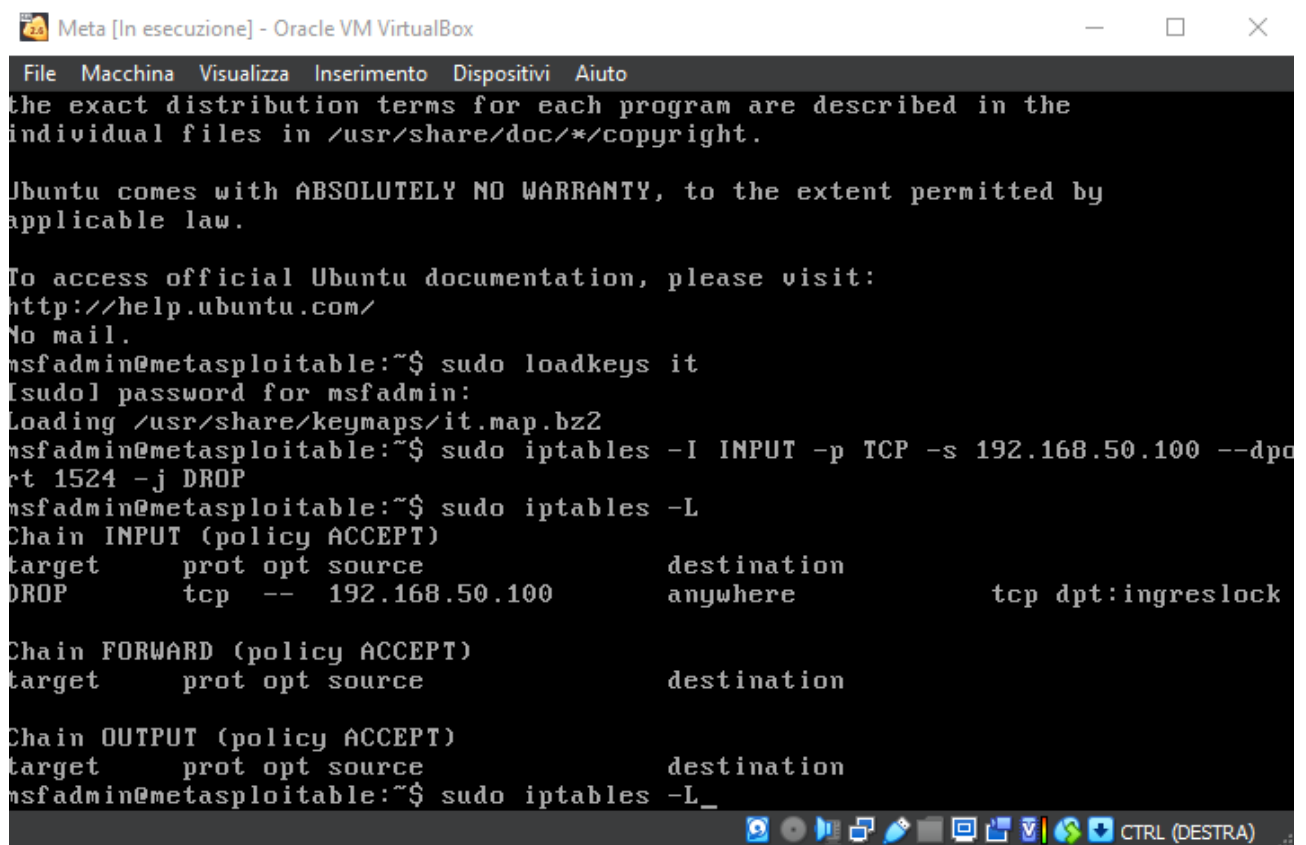


```
Meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# msfadmin
bash: msfadmin: command not found
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? n
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#
```

**Blind Shell Backdoor Detection** questa vulnerabilità consisteva in una shell in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla connettendosi alla porta remota e inviando direttamente i comandi. Abbiamo così attivato il firewall iptables con una chain di comandi che hanno permesso di bloccare l'ingresso della nostra macchina attaccante (KALI) tramite il suo indirizzo IP



```
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 loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p TCP -s 192.168.50.100 --dpt
et 1524 -j DROP
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp dpt:ingreslock
DROP      tcp  --  192.168.50.100         anywhere              tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
msfadmin@metasploitable:~$ sudo iptables -L_
```