

VNC PASSWORD

Andiamo a cambiare la password di default di VNC. Per prima cosa ci andiamo a loggare come amministratori in quanto vogliamo cambiare la password dell'utenza root, poi usiamo il comando **vncpasswd** per inserire una nuova password. VNC accetta password di massimo 8 caratteri, sono andato ad inserire una nuova password contenente una maiuscola, un carattere speciale, dei caratteri standard e dei numeri:

```
msfadmin@metasploitable:~$ sudo su
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#
```

Per verificare che il cambio sia andato a buon fine proviamo a loggarci da kali utilizzando il comando **vncviewer**:

```
(luca@kali)-[~]
$ vncviewer 192.168.2.100
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
```

Usando “password” l'autenticazione è fallita, che è quello che volevamo

BIND SHELL BACKDOOR DETECTION

Eseguendo una scansione con nmap andiamo a cercare su quale porta sia in ascolto la bindshell:

```
(luca@kali)-[~]
$ nmap -sV 192.168.2.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 11:47 CEST
Nmap scan report for 192.168.2.100
Host is up (0.016s 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?
514/tcp   open  shell          Netkit rshd
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          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
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

E' in ascolto sulla porta TCP 1524. Andiamo quindi a creare una regola dal firewall pfsense per impedire le richieste verso l'ip di metasploitable su tale porta. Appliciamo la regola in ingresso sull'interfaccia LAN in ascolto verso Kali:

Firewall / Rules / Edit

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match Single host or alias 192.168.2.100 /

Destination Port Range (other) 1524 (other) 1524
From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

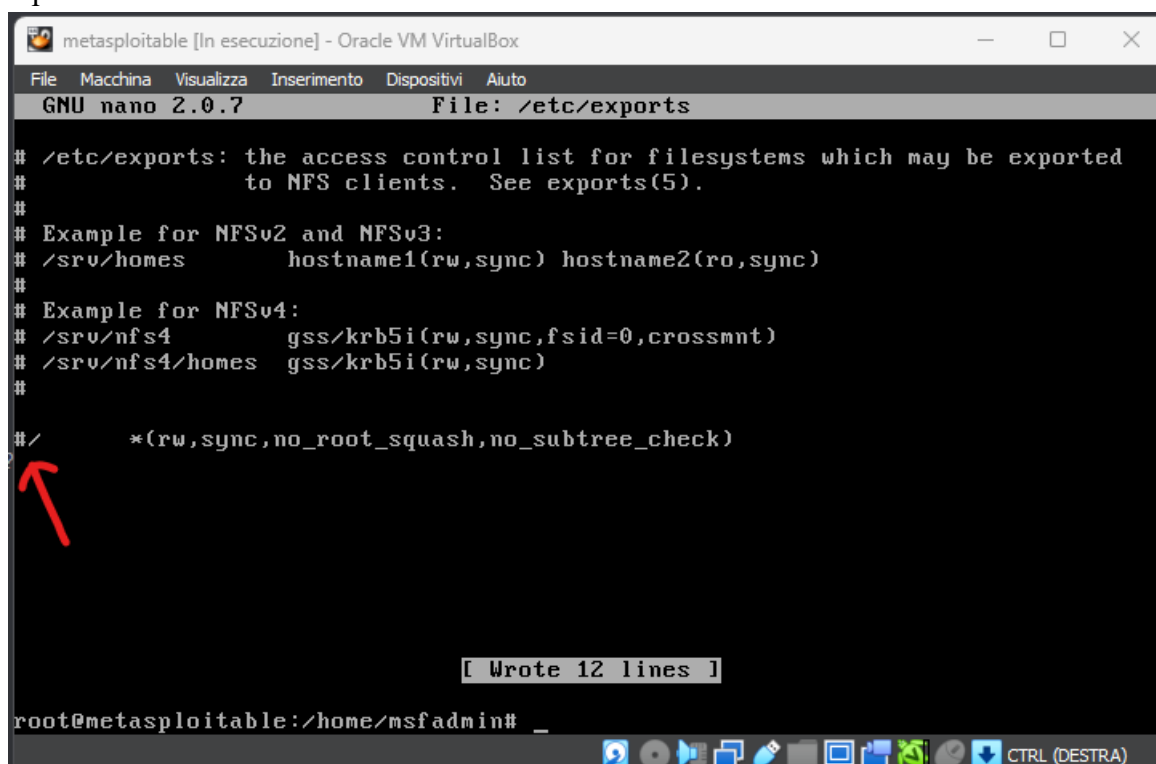
Per verificare andiamo a rieseguire il version scan con nmap. Notiamo che questa volta la porta risulta su filtered:

```
(luca@kali)-[~]
$ nmap -sV 192.168.2.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 12:27 CEST
Nmap scan report for 192.168.2.100
Host is up (0.013s 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?
514/tcp   open      shell        Netkit rshd
1099/tcp  open      java-rmi     GNU Classpath grmiregistry
1524/tcp  filtered  ingreslock   2.4 (RPC #100003)
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: Hosts: metasploitable.localdomain, 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 180.51 seconds
```

NFS Exported Share Information Disclosure

Andiamo a modificare il file di esportazione del servizio NFS. Commentiamo l'ultima riga con #, in questo modo non andremo ad esportare tutto il filesystem di default usando NFS (è infatti presente il percorso /*):



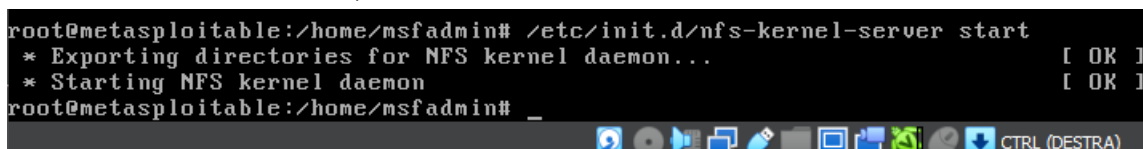
```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports

# /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)
#
# /* *(rw,sync,no_root_squash,no_subtree_check)

[ Wrote 12 lines ]

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

Andiamo poi ad avviare il servizio in modo che rifaccia l'export delle directory secondo le nostre modifiche, usando il comando `/etc/init.d/nfs-kernel-server start`:



```
root@metasploitable:/home/msfadmin# /etc/init.d/nfs-kernel-server start
* Exporting directories for NFS kernel daemon... [ OK ]
* Starting NFS kernel daemon [ OK ]
root@metasploitable:/home/msfadmin#
```

REXECd SERVICE DETECTION

Non ho implementato nessuna remediation in quanto nel report iniziale da nessun non è stata rilevata questa vulnerabilità