





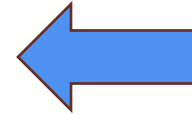
Report

- 
- Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.



Progetto della
settimana 5

REPORT NESSUS



Clicca qui

Oggi andremmo a risolvere queste vulnerabilità

→	CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
→	CRITICAL	10.0*	-	61708	VNC Server 'password' Password
	HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
→	HIGH	7.5	-	42256	NFS Shares World Readable

UnrealIRCd Backdoor Detection

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.1.85
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-12 09:07 EST
Nmap scan report for 192.168.1.85
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
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?
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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  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
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:45:EA:E4 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

La vulnerabilità indica che c'è una versione di UnrealIRCd con una backdoor nella porta "6667" della macchina, che consente a un utente malintenzionato di entrare nel computer molto facilmente.

Cos'è la Backdoor?

Una backdoor è una via secondaria o una porta segreta in un sistema o un software che consente a un utente non autorizzato di bypassare le normali procedure di autenticazione o sicurezza.

Soluzione UnrealIRCd Backdoor Detection

Commando:

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 6667 -j DROP
msfadmin@metasploitable:~$ _
```

Revisione delle porte:

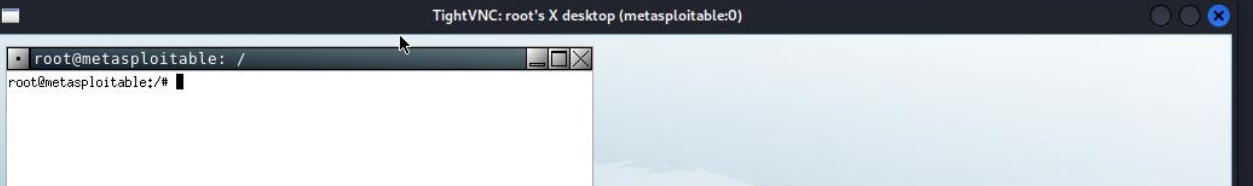
```
6000/tcp open      X11           (access denied)
6667/tcp filtered irc           using protocol version 3.2
8009/tcp open      ajp13         Apache Jserv (Protocol v1.3)
8180/tcp open      http          Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:15:5A:5E (Oracle VM VirtualBox virtual NIC)
```

Per solucionar questa vulnerabilità dobbiamo eseguire un comando: "sudo iptables -A INPUT -p tcp --dport 6667 -j DROP".

Questo comando aggiunge una regola iptables che scarta tutti i pacchetti TCP in ingresso diretti alla porta 6667. Cioè impedisce che il traffico avvenga su quella porta.

VNC Server 'password' Password

```
(kali㉿kali)-[~]
└─$ sudo vncviewer 192.168.1.85
[sudo] password for kali:
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



- Questa vulnerabilità indica che il server VNC è protetto con una password debole, cioè: password.
- Una persona terza potrebbe sfruttare questa situazione per prendere il controllo del sistema, attraverso un BruteForce.

Cos'è la VNC?

La VNC, è un sistema che consente a un utente di controllare e visualizzare il desktop, interagendo con il sistema di un computer da un altro dispositivo o attraverso una connessione di rete.

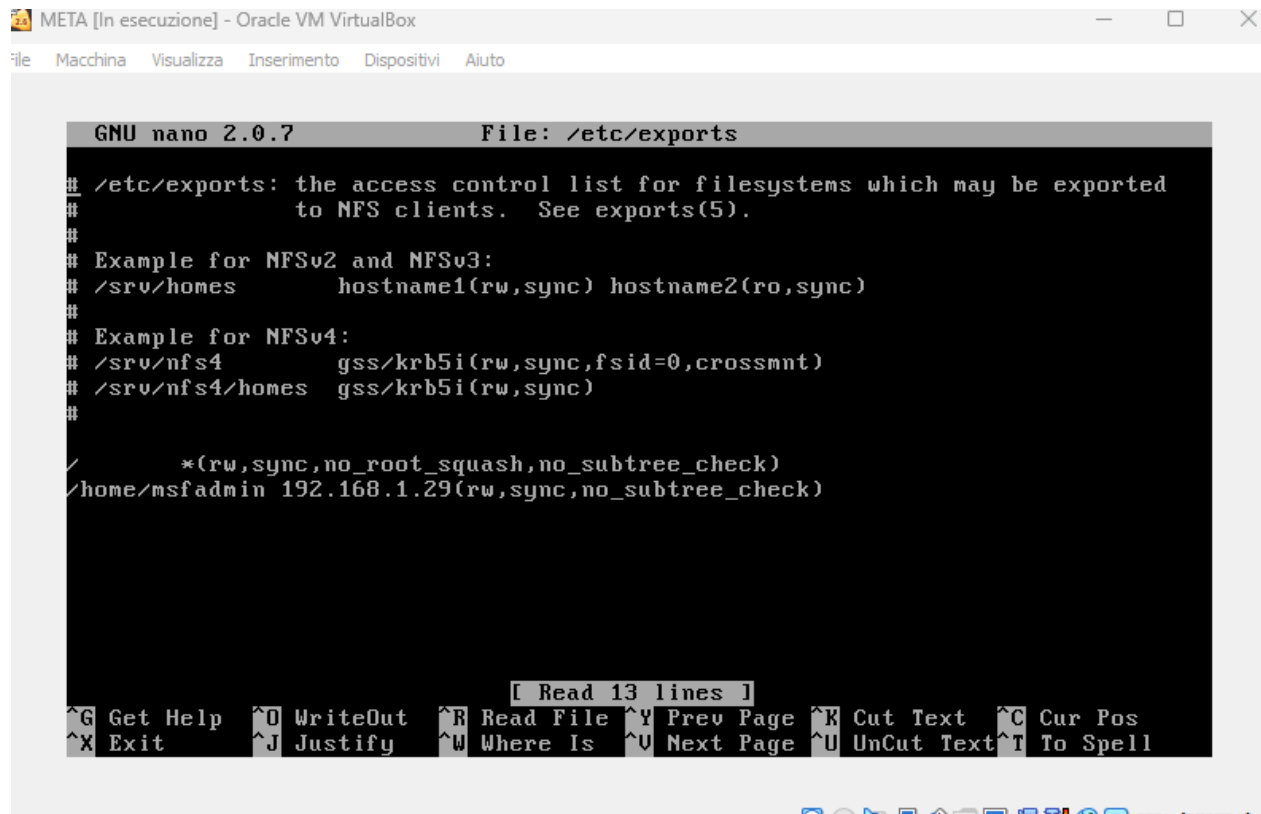
Soluzione VNC Server 'password' Password

```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ls -la
.          .distcc  .gconfd  .rhosts  .vnc
..         .fluxbox .mysql_history .ssh     vulnerable
.bash_history .gconf  .profile .sudo_as_admin_successful .Xauthority
msfadmin@metasploitable:~$ cd .vnc
msfadmin@metasploitable:~/vnc$ ls -la
.  .. -change metasploitable:1.log metasploitable:1.pid passwd xstartup
msfadmin@metasploitable:~/vnc$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~/vnc$ _
```

Per risolvere questa vulnerabilità bisogna:

- Dirigersi nella directory: `/.vnc`
- Attraverso il comando: `vncpasswd`, ci permette di cambiare la password.

NFS Shares World Readable



The screenshot shows a terminal window titled "META [In esecuzione] - Oracle VM VirtualBox". Inside, the GNU nano 2.0.7 editor is open, editing the file /etc/exports. The file content 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)
#
/*(rw,sync,no_root_squash,no_subtree_check)
/home/msfadmin 192.168.1.29(rw,sync,no_subtree_check)
```

The bottom of the terminal shows the nano editor's command palette with options like Get Help, Exit, WriteOut, Justify, Read File, Where Is, Prev Page, Next Page, Cut Text, UnCut Text, Cur Pos, and To Spell.

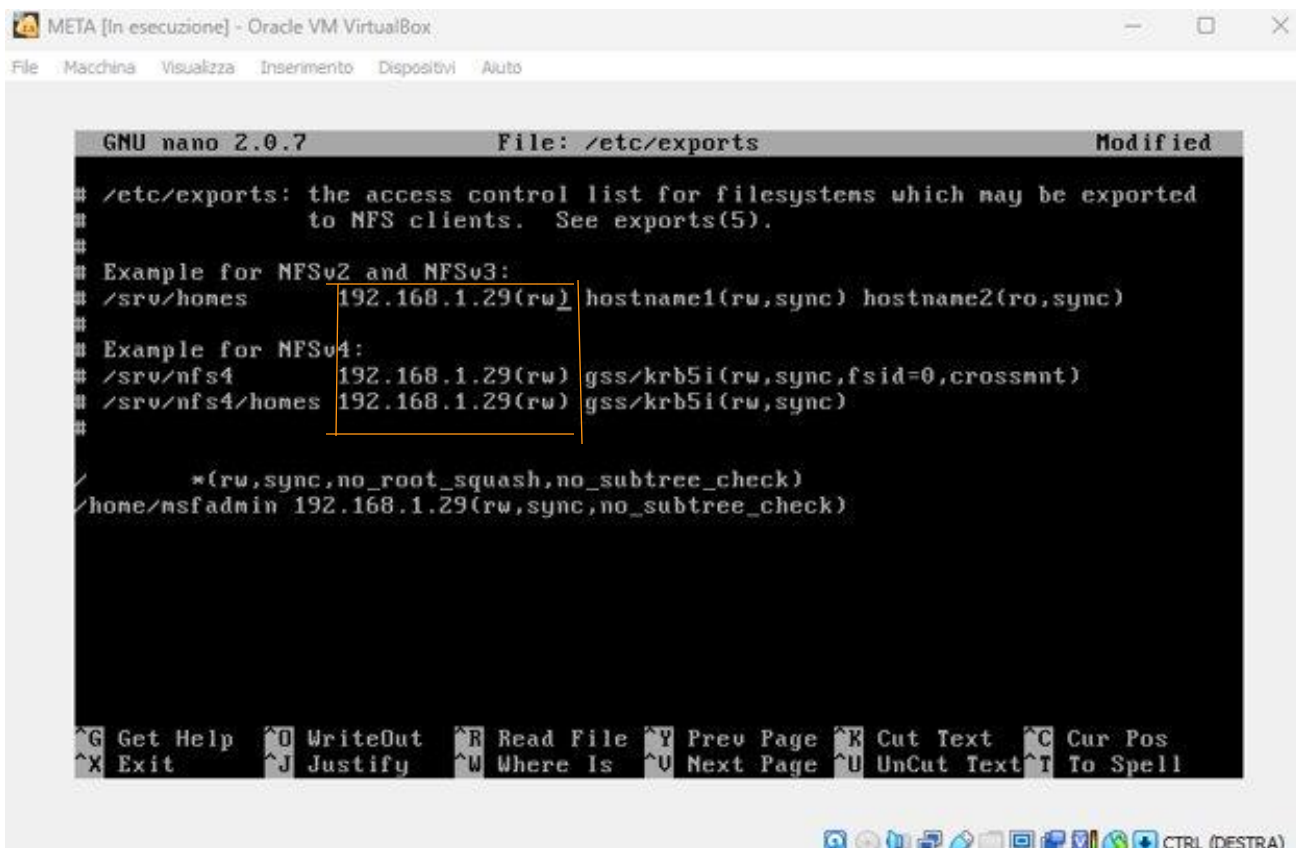
La vulnerabilità consiste che il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso agli Host.

Questo comporta che qualsiasi host in rete potrebbe potenzialmente accedere alle condivisioni NFS, attraverso attacchi di Tipo: Man-in-the-Middle.

Cos'è il NFS?

Il NFS, è un protocollo di rete che consente la condivisione di risorse di file tra computer su una rete.

Soluzione NFS Shares World Readable



The screenshot shows a terminal window titled "META [In esecuzione] - Oracle VM VirtualBox". Inside, the GNU nano 2.0.7 editor is open, editing the file /etc/exports. The file content 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 192.168.1.29(rw) hostname1(rw, sync) hostname2(ro, sync)
#
# Example for NFSv4:
# /srv/nfs4 192.168.1.29(rw) gss/krb5i(rw, sync, fsid=0, crossmnt)
# /srv/nfs4/homes 192.168.1.29(rw) gss/krb5i(rw, sync)
#
/*(rw, sync, no_root_squash, no_subtree_check)
/home/msfadmin 192.168.1.29(rw, sync, no_subtree_check)
```

The line `192.168.1.29(rw)` in the NFSv3 example is highlighted with a yellow box. The terminal window has a menu bar with options: File, Macchina, Visualizza, Inserimento, Dispositivi, Aiuto. At the bottom, there is a status bar with various keyboard shortcuts and the text "CTRL (DESTRA)".

Per solucionar questa vulnerabilità bisogna:

- Andare nel file /etc/exports, sarebbe il file che elenca le condivisioni NFS.
- Modificare le linee corrispondenti alle condivisioni NFS, restringendo accesso ad uno o più host.

Conferma della risoluzione

Vulnerabilities

Total: 112

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	-	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure

Dal secondo Report di Nessus, si convalida che le vulnerabilità sono state risolte.