

UNITÀ 2/ COMPITO 5/ SETTIMANA 1

Ho effettuato una scansione con Nessus trovando le seguenti criticità, quindi seguendo ciò che è richiesto dall'esercizio ho provato a correggere quelle sottolineate in rosso

The screenshot displays the Nessus Essentials web interface. The main table lists 69 vulnerabilities. The following table represents the data visible in the screenshot:

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	<u>NFS Exported Share Information Disclosure</u>	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		<u>VNC Server 'password' Password</u>	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		<u>Bind Shell Backdoor Detection</u>	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	SSL (Multiple Issues)	General	28
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2

Host Details (192.168.1.16):
IP: 192.168.1.16
MAC: 08:00:27:9A:22:5E
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: January 11 at 10:00 AM
End: January 11 at 10:19 AM
Elapsed: 19 minutes
KB: Download

Vulnerabilities Distribution:
Critical: 1
High: 1
Medium: 1
Low: 1
Info: 1

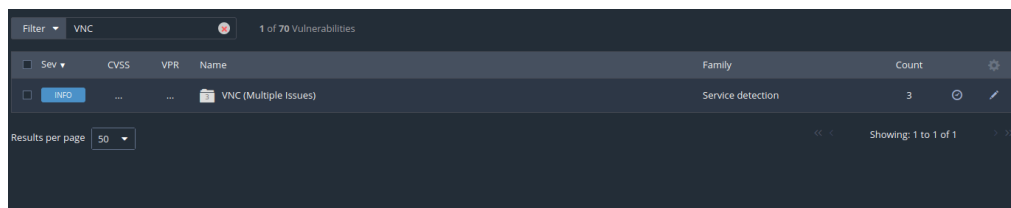
VNC SERVER' PASSWORD' PASSWORD

La prima criticità risolta è stata quella riguardante la password in quanto la più veloce e anche perchè era troppo banale, così andando su meta e tramite il comando << vncpasswd >>

```
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ msfadmin
-bash: msfadmin: command not found
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
msfadmin@metasploitable:~$ 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)? y
Password:
Warning: password truncated to the length of 8.
Verify:
msfadmin@metasploitable:~$ _
```

ne ho inserita una più sicura con almeno 8 caratteri perchè anche provando a metterne una più lunga veniva tagliata .



The screenshot shows a web-based interface for a vulnerability scanner. At the top, there's a filter set to 'VNC' and a count of '1 of 70 Vulnerabilities'. Below this is a table with columns: 'Sev', 'CVSS', 'VPR', 'Name', 'Family', and 'Count'. A single vulnerability is listed with a severity of 'INFO', a CVSS score of '...', a VPR of '...', and a name of 'VNC (Multiple Issues)'. The family is 'Service detection' and the count is '3'. At the bottom, there's a 'Results per page' dropdown set to '50' and a 'Showing: 1 to 1 of 1' indicator.

Sev	CVSS	VPR	Name	Family	Count
INFO	VNC (Multiple Issues)	Service detection	3

BLIND SHELL BACKDOOR DETECTION

Che causava l'infiltrazione da remoto così ho chiuso la backdoor entrando prima nel root tramite il comando << nano su >> e ovviamente inserendo la password.

Poi abbiamo usato il seguente comando << lsof -i :1524 >>

```
metasploitable login: msfadmin
Password:
Last login: Fri Jan 12 07:14:10 EST 2024 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/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd   4436 root    12u  IPv4  12008      TCP *:ingreslock (LISTEN)
root@metasploitable:/home/msfadmin# kill 4436
root@metasploitable:/home/msfadmin#
```

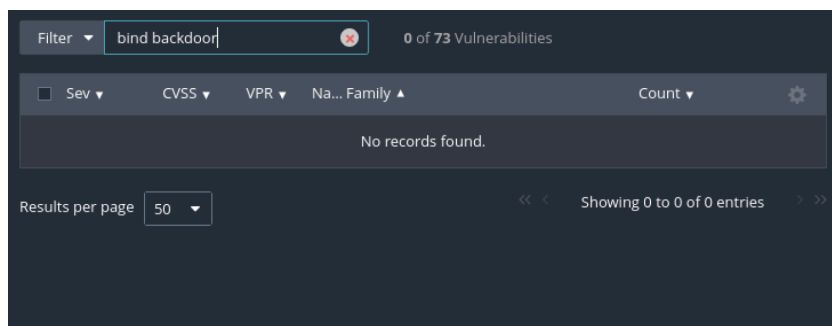
Una volta fatto ciò abbiamo visto la porta e l'abbiamo chiusa tramite il comando << kill 4436 >>

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[/home/kali]
# nmap -sS 192.168.1.19
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-12 08:44 EST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.1.19
Host is up (0.00036s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1099/tcp  open  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:9A:22:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Poi siamo andati su kali entrati nel root ed eseguito il comando `<< nmap -sS 192.168.1.19 >>` (indirizzo dell'ip) per verificare se la porta è stata chiusa.

Per far sì che ciò rimanga anche dopo il riavvio bisogna disabilitare il servizio

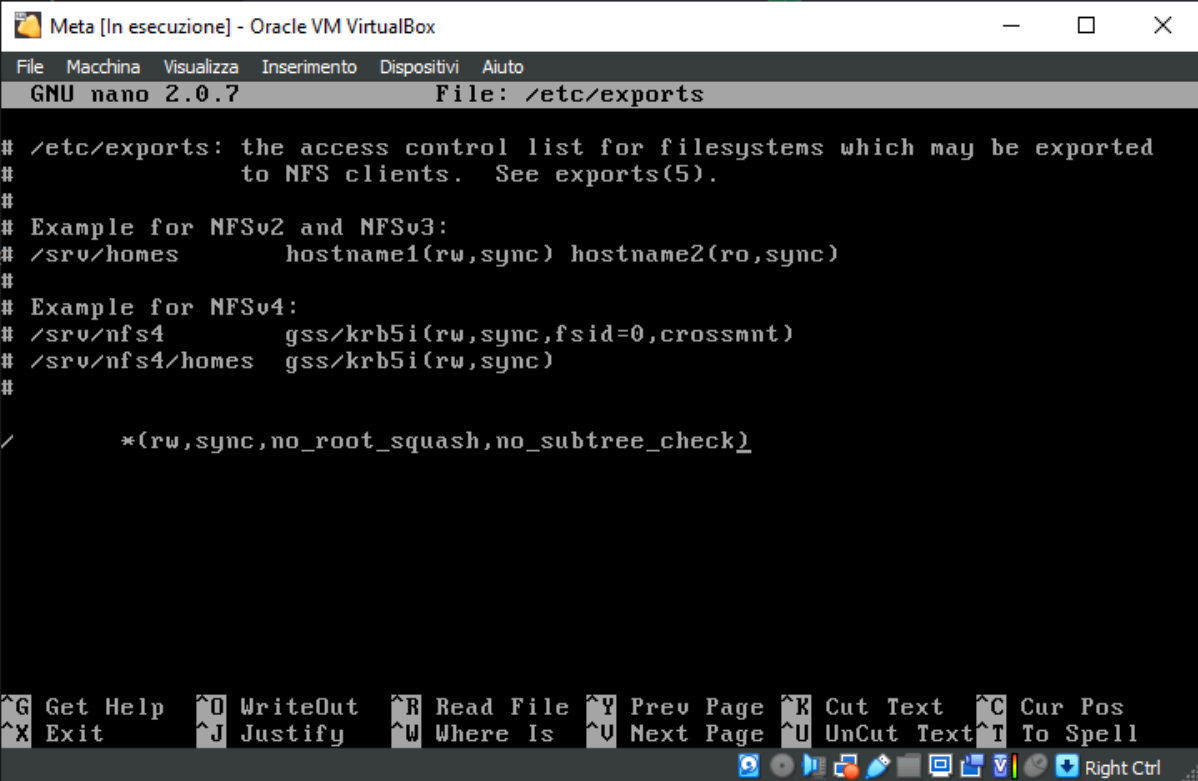


**Ora nessun criminale informatico può entrare
da remoto**

NFS EXPORTED SHARE INFORMATION DISCLOSURE

La vulnerabilità NFS exported share information si ha quando le condivisioni possono essere intercettate da host non autorizzati e potrebbero scrivere o far leggere file da remoto .

Quindi usando il comando << sudo nano /etc/exports >>



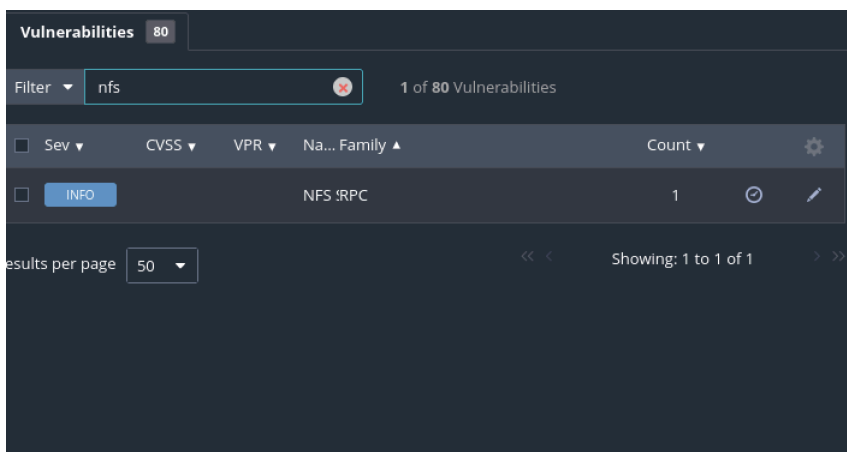
The screenshot shows a terminal window titled "Meta [In esecuzione] - Oracle VM VirtualBox". The window displays the contents of the file `/etc/exports` using the `nano` text editor. The file contains the following text:

```
# /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)
```

The terminal window also shows the `nano` editor's status bar at the bottom with various keyboard shortcuts like `^G Get Help`, `^O WriteOut`, `^R Read File`, `^Y Prev Page`, `^K Cut Text`, `^C Cur Pos`, `^X Exit`, `^J Justify`, `^W Where Is`, `^V Next Page`, `^U UnCut Text`, and `^T To Spell`.

quindi ho provveduto ad eliminare la stringa per evitare ciò

```
GNU nano 2.0.7      File: /etc/exports      Modified
# /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)
#
File Name to Write: /etc/exports
^G Get Help      ^T To Files      M-M Mac Format    M-P Prepend
^C Cancel        M-D DOS Format    M-A Append        M-B Backup File
```



così nessuno altro ha la possibilità di poter far leggere ne scrivere file.