

# Progetto S5L5 di Ciaschini Giorgio del 23/02/2024

Attraverso “Nessus” sono andato a fare uno scanning sulla rete della macchina Metasploitable e ho trovato diverse criticità di diversi livelli.

Ho iniziato a risolvere quelle più critiche partendo da “Bind Shell Backdoor Detection”:

CRITICAL

Bind Shell Backdoor Detection

<

>

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

Nessus was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :

----- snip -----

root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)

root@metasploitable:/#

----- snip -----

To see debug logs, please visit individual host

Port	Hosts
1524 / tcp / wild_shell	192.168.49.101

Plugin Details

Severity:

Critical

ID:

51988

Version:

1.10

Type:

remote

Family:

Backdoors

Published:

February 15, 2011

Modified:

April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:/I:C/A:C

L’ho risolto aprendo Metasploitable e sono andato a lavorare sulla porta 1524 e ho utilizzato questo comando:

```
root@metasploitable:/home/msfadmin# sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
```

Successivamente grazie all’utilizzo di “nmap” che è più rapido sotto alcuni aspetti ho fatto una revisione e il risultato è che la porta “1524” interessata è stata filtrata andando a risolvere così la criticità “Bind Shell Backdoor Detection”. Di seguito lo screenshot:

```

Host is up (0.00014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  filtered ingreslock
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:CA:2B:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds

```

Un'altra criticità che ho risolto è “**NFS Exported Share Information Disclosure**”

CRITICAL

NFS Exported Share Information Disclosure

**Description**

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

**Output**

```

The following NFS shares could be mounted :

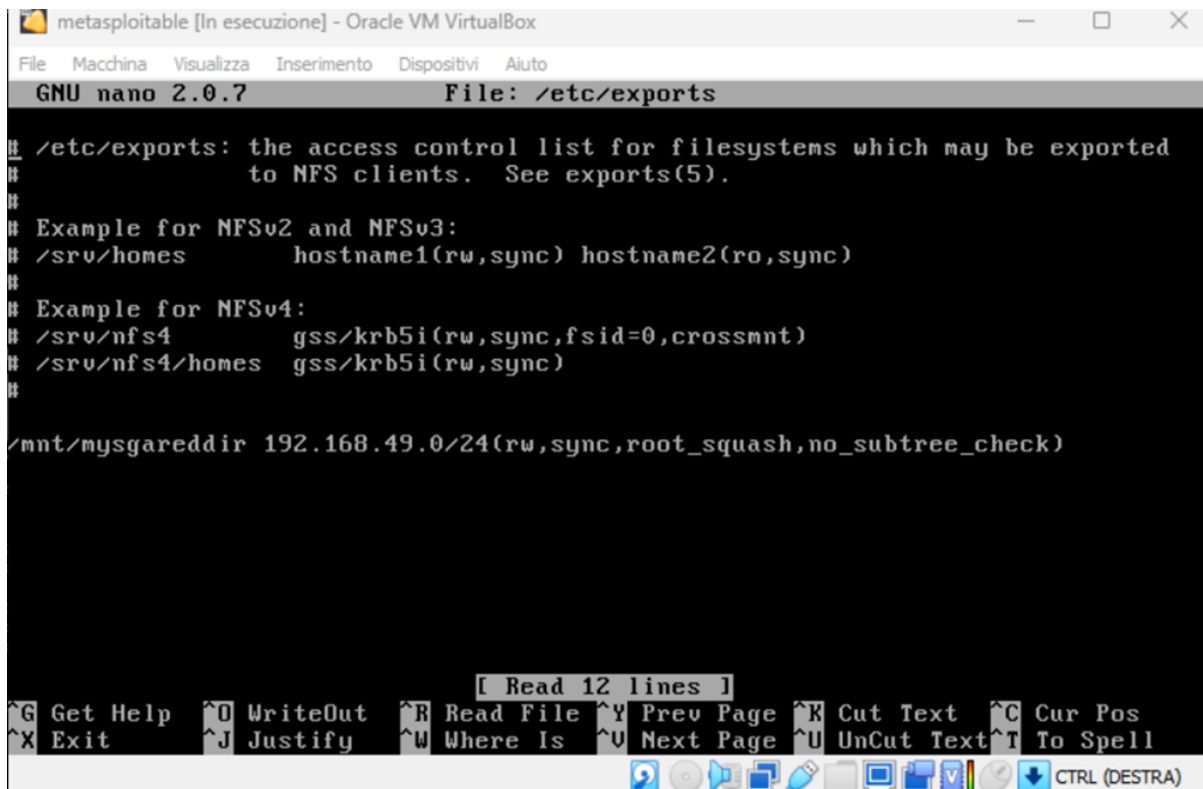
+ /
+ Contents of / :
- .
- ..
- 7E,UTW.)R
- bin
- boot
more...

```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.49.101

Dopo aver verificato la veridicità sono andato a modificare all'interno di metasploitable le configurazioni in modo tale da limitare gli accessi agli utenti con lo stesso IpNetwork:

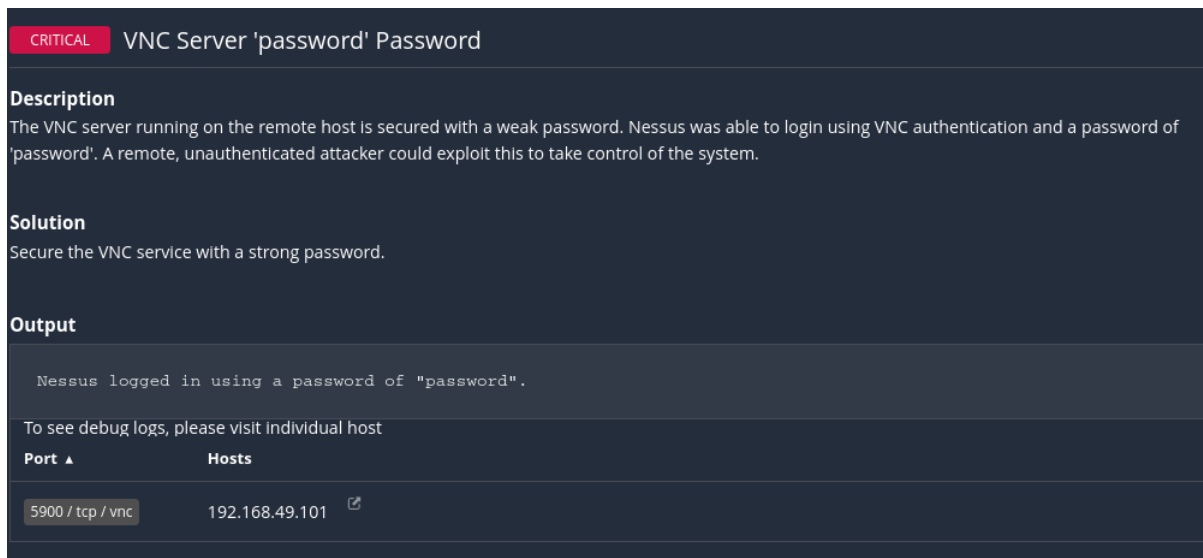


The screenshot shows a terminal window titled "metasploitable [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 text editor, editing the file /etc/exports. The content of the file is as follows:

```
# /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/mysgareddir 192.168.49.0/24(rw,sync,root_squash,no_subtree_check)
```

The bottom of the terminal shows the nano editor's status bar with various keyboard shortcuts and a toolbar with icons for file operations and a "CTRL (DESTRA)" button.

Ho risolto invece la criticità “VNC Server ‘password’ Password” andando a modificare la password all’interno della macchina.



The screenshot displays a Nessus vulnerability report for the issue "VNC Server 'password' Password". The report is categorized as "CRITICAL".

**Description**  
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

**Solution**  
Secure the VNC service with a strong password.

**Output**  
Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.49.101

Di seguito il procedimento eseguito:

```

Last login: Fri Feb 23 06:36:08 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:
root@metasploitable:/home/msfadmin# ls
vulnerable
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# _

```

Ho risolto anche le seguenti criticità “**rlogin Service Detection** e **rsh Service Detection**”:

Severity	Score	CVSS	Service	Count	Actions
<input type="checkbox"/> HIGH	7.5 *	5.9	rlogin Service Det...	1	🔄 ✎
<input type="checkbox"/> HIGH	7.5 *	5.9	rsh Service Detec...	1	🔄 ✎

```

#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
telnet                  stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
tftp                   dgram   udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
#shell                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
#login                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec                   stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i

```

## Report finale

Possiamo dire che le criticità sono state risolte tutte con successo come si evince dalla seguente immagine.

Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔍 ✎
<input type="checkbox"/> MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	🔍 ✎
<input type="checkbox"/> MIXED	...	...	Phpmyadmin (Multiple Issues)	CGI abuses	4	🔍 ✎
<input type="checkbox"/> CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	🔍 ✎
<input type="checkbox"/> MIXED	...	...	PHP (Multiple Issues)	CGI abuses	3	🔍 ✎
<input type="checkbox"/> HIGH	8.3		CGI Generic SQL Injection (blind)	CGI abuses	1	🔍 ✎
<input type="checkbox"/> HIGH	7.5 *		CGI Generic Command Execution	CGI abuses	1	🔍 ✎
<input type="checkbox"/> HIGH	7.5 *		CGI Generic Remote File Inclusion	CGI abuses	1	🔍 ✎
<input type="checkbox"/> HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1	🔍 ✎
<input type="checkbox"/> MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5	🔍 ✎
<input type="checkbox"/> MIXED	...	...	Twiki (Multiple Issues)	CGI abuses	2	🔍 ✎
<input type="checkbox"/> MEDIUM	6.8 *		CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1	🔍 ✎