

Obiettivo: correggere dalle 2 alle 4

Abbiamo cercato le vulnerabilità su metasploitable 2 da kali utilizzando nessus.

La scansione iniziale riportava:

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	🔄 ✓
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄 ✓
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	🔄 ✓
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	🔄 ✓
<input type="checkbox"/>	MIXED	—	—	4 Apache Tomcat (Multiple Issues)	Web Servers	4	🔄 ✓
<input type="checkbox"/>	MIXED	—	—	4 Phpmyadmin (Multiple Issues)	CGI abuses	4	🔄 ✓
<input type="checkbox"/>	CRITICAL	—	—	2 SSL (Multiple Issues)	Gain a shell remotely	3	🔄 ✓
<input type="checkbox"/>	MIXED	—	—	3 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	5.9	Samba Badlock Vulnerability	General	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		NFS Shares World Readable	RPC	1	🔄 ✓
<input type="checkbox"/>	MIXED	—	—	5 ISC Bind (Multiple Issues)	DNS	5	🔄 ✓
<input type="checkbox"/>	MIXED	—	—	2 Twiki (Multiple Issues)	CGI abuses	2	🔄 ✓

abbiamo individuato delle vulnerabilità da poter risolvere senza dare problemi all'operativa del sistema preso in esame.

Abbiamo per prima cosa risolto la vulnerabilità di vnc

complete / Plugin #61708
[Back to Vulnerabilities](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 33 Remediations 4 History 6

CRITICAL VNC Server 'password' Password

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 192.168.43.101

Plugin Details

Severity: Critical
ID: 61708
Version: Nessus: 1.2.8
Type: remote
Family: Gain a shell remotely
Published: August 29, 2012
Modified: September 24, 2015

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#MIMP/NINCL/ANU/NPCC/ICAC/C
Vulnerability Information

Default Account: true
Exploited by Nessus: true

per risolverlo siamo entrati in root (sudo su) e abbiamo cambiato la password con vncpasswd

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

[ Read 12 lines ]

msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  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 vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Error: bad ownership on /home/msfadmin/.vnc
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# sudo 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#
```

a seguire abbiamo preso in esame la vulnerabilità della backdoor aperta sulla porta 1524

General

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

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

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

..... smip
root@metasploitable:/# id=0 (root) gid=0 (root) groups=0 (root)
root@metasploitable:/#
..... smip
To see debug logs, please visit individual host

Port

Hosts

1524 / tcp / www_shell

192.168.43.101

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
/AUI:N/SU:C/H/TH:H/AH

CVSS v2.0 Base Score 10.0

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

per risolvere questo problema siamo entrati in iptables dando il comando per aggiungere la regola che blocca le connessioni con la porta 1524

A screenshot of a VirtualBox window titled "metasploitable [In esecuzione] - Oracle VM VirtualBox". The terminal window shows a user "msfadmin" at "metasploitable" running several commands. First, they run "sudo echo MYUNCPASSWORD | vncpasswd -f ~/.secret/passvnc", which produces a truncated output. Then they run "vncpasswd -t". Next, they run "sudo su" to become "root". Finally, they run "sudo iptables -A INPUT -p tcp --dport 1524 -j DROP". The terminal output shows the user becoming root and the successful execution of the iptables command.

e nelle tabelle del router troviamo:

```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/mnt/mysgareddir 192.168.49.0/24(rw,sync,root_squash,no_subtree_check)

[ Read 12 lines ]

msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:ingreslock
DROP      tcp  --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
msfadmin@metasploitable:~$ _
```

per la vulnerabilita relativa ai file nfs:

complete / Plugin #11356

[Back to Vulnerabilities](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 93 Remediations 4 History 6

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 / :
- .
- .
- bin
- boot
- ...
MORE ...
To see debug logs, please visit individual host

Port Hosts

2049 /udp /rpc.ports 192.168.49.101

Plugin Details

Severity: Critical
ID: 11356
Version: 1.21
Type: remote
Family: RPC
Published: March 12, 2003
Modified: August 30, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/R:C/A:C

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 1, 1985

Exploitable With

Metasploit (NFS Mount Scanner)

abbiamo modificato il file exports presente per limitare gli ho host che possono entrare nei file condivisi

```

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)
#
/mnt/mysharedir 192.168.49.0/24(rw,sync,root_squash,no_subtree_check)

[ Wrote 12 lines ]

root@metasploitable:/home/msfadmin#

```

per concludere abbiamo individuato un'ulteriore vulnerabilità di service detection

<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service Det...	Service detection	1		
<input type="checkbox"/>	HIGH	7.5 *	5.9	rsh Service Detec...	Service detection	1		

per poterla risolvere siamo andati a modificare il file `inetd.conf` andando a commentare le righe di login ed exec:

```

metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf Modified

#<off># netbios-ssn  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp         stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
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

[ Unknown Command ]

^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 ^T To Spell

CTRL (DESTRA)

```

così facendo abbiamo risolto alcuni tra i problemi critici e alti presenti nel sistema senza rallentare l'operatività dei sistemi.

La nuova scansione Nessus riporta:

Vulnerabilities 90						
Filter	Search Vulnerabilities		90 Vulnerabilities			
<input type="checkbox"/> Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/> MEDIUM	Apache Tomcat (Multiple Issues)	Web Servers	4	
<input type="checkbox"/> MEDIUM	Phpmyadmin (Multiple Issues)	CGI abuses	4	
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/> MEDIUM	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"/> MEDIUM	ISC Bind (Multiple Issues)	DNS	5	
<input type="checkbox"/> MEDIUM	Twiki (Multiple Issues)	CGI abuses	2	
<input type="checkbox"/> MEDIUM	6.8 *		CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1	

come possiamo vedere nelle vulnerabilità di livello critico e alto non sono più presenti i problemi riscontrati in precedenza