

Report Penetration Test

Critical Vulnerability Fix

- Andremo ad analizzare la macchina di Metasploitable con indirizzo IP 192.168.1.63 con Nessus tramite Kali e proveremo a sistemare 4/5 **Vulnerabilità Critiche**.
- Iniziamo con una scansione avanzata della macchina di Metasploitable .

192.168.1.63



Vulnerabilities

Total: 122

| SEVERITY | CVSS | VPR SCORE | PLUGIN | NAME |
|----------|-------|-----------|--------|---|
| CRITICAL | 9.8 | 9.0 | 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 | 10.0 | - | 171340 | Apache Tomcat SEoL (<= 5.5.x) |
| CRITICAL | 10.0 | - | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 5.1 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 5.1 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 5.9 | 11356 | NFS Exported Share Information Disclosure |
| 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 |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 5.9 | 90509 | Samba Badlock Vulnerability |

- Abbiamo trovato 10 vulnerabilità critiche .
- Andremo a spiegare e fixare le 5 vulnerabilità cerchiare in giallo nei prossimi step .

- Prima vulnerabilità

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

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.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

- Andremo a vedere il file del service inetd che occupa la nostra porta 1524 : /etc/inetd.conf tramite il comando cat .
- La porta 1524 è accessibile da chiunque quindi per risolvere il problema andremo a cancellare l'ultima riga dove c'è scritto :

```
msfadmin@metasploitable:~$ cat /etc/inetd.conf
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbi
n/smbd
telnet      stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
netd
#<off># ftp            stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbi
n/in.ftpd
tftp        dgram   udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tft
pd /srv/tftp
shell       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
d
login       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlo
gind
exec        stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rex
ecd
ingreslock  stream  tcp      nowait  root    /bin/bash bash -i
```

- Editiamo il file tramite il lettore di testo nano e cancelliamo la riga .

```
msfadmin@metasploitable:~$ sudo nano /etc/inetd.conf
```

| 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\$ | |

```
(kali@kali)-[~]
$ nc 192.168.1.63 1524
(UNKNOWN) [192.168.1.63] 1524 (ingreslock) : Connection refused
```

- Per la seconda vulnerabilità Nessus ci segnala che sul VNC server
- c'è una password debole e quindi andremo a cambiarla tramite il root di Metasploitable .

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak 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.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:I/C/A:C)

```
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
```

- Per la terza vulnerabilità Nessus ci segnala che è possibile tramite host remoto accedere alla porta 2049 su cui NFS è in esecuzione .

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

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.

Risk Factor

Critical

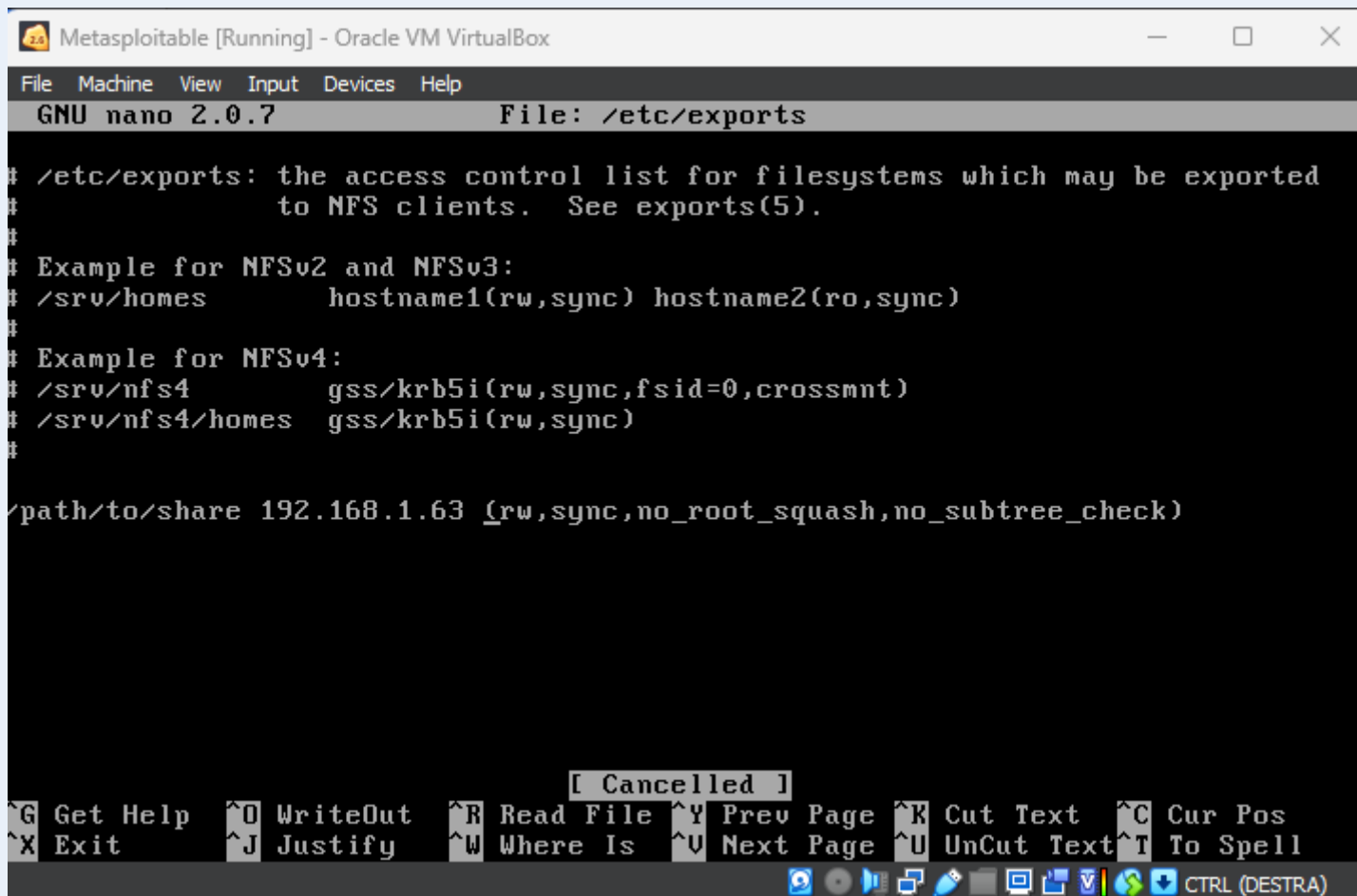
VPR Score

5.9

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

- Per risolvere questa vulnerabilità aggiungeremo una regola che impedisce a host esterni di accedervi tramite il comando :
- `/path/to/share 192.168.1.63` prima delle parentesi nel file
- `/etc/exports` sempre editato tramite nano .



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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)
#
/path/to/share 192.168.1.63 (rw,sync,no_root_squash,no_subtree_check)

[ Cancelled ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

- Quarta vulnerabilità : Ci sono più modi per risolvere questa vulnerabilità noi ne vedremo uno .

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

- Questa vulnerabilità ci indica che su una porta c'è l'app di Apache Tomcat che è molto vulnerabile sia perché attaccabile sia perché la password di base di Apache Tomcat è molto debole e facilmente estraibile tramite BruteForce.

```
GNU nano 2.0.7      File: server.xml      Modified
-->      clientAuth="false" sslProtocol="TLS" />
-->
<!-- Define an AJP 1.3 Connector on port 8009 -->
<!--
<Connector port="8009"
      enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />
-->
```

- Vado quindi a modificare il file di Tomcat server.xml all'interno della directory di configurazione e aggiungo "

In caso questo non dovesse risolvere il problema dovremo andare a modificare l'ID e la password nel file di configurazione del login di Tomcat o se possibile andare ad aggiornare la versione di Tomcat con una più aggiornata e sicura di quella presente .

- Quinta Vulnerabilità

46882 - UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

See Also

<https://seclists.org/fulldisclosure/2010/Jun/277>

<https://seclists.org/fulldisclosure/2010/Jun/284>

<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Risk Factor

Critical

VPR Score

7.4

- Il server IRC contiene una backdoor ed è in ascolto sulla porta 6667 quindi attaccabile da qualunque host remoto . Per risolvere il problema andremo prima a verificare l'exploit e successivamente a cambiare la regola tramite "ip tables " su Metasploitable.

- Di seguito vediamo come effettuare molto velocemente l'exploit della vulnerabilità .

```
(root@kali)-[/home/kali] (Local Loopback)
# service postgresql start
Rx errors 0 dropped 0 overruns 0 frame 0

(root@kali)-[/home/kali] es 8123397 (7.7 MiB)
# service postgresql status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
   Active: active (exited) since Wed 2024-03-06 15:09:51 EST; 6s ago
   Process: 74417 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 74417 (code=exited, status=0/SUCCESS)
   CPU: 965us
```

```
(root@kali)-[/home/kali] ed 0 overruns 0 frame 0
# msfconsole
tx errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,_____,RUNNING> mtu 65536
    inet 1.1.1.1 netmask 255.0.0.0
    ether 00:0c:29:14:00:00 txqueuelen 1000 (0.0 MiB)
    RX packets 1607 (7.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 (0.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6 >

      ( 3 C )  /|__ / Metasploit! \
      ;d'. _*_ _.' \__ \

      '(. ,....'/'
```

```
=[ metasploit v6.3.27-dev ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]
```

Metasploit tip: Enable HTTP request and response logging
with `set HttpTrace true`
Metasploit Documentation: <https://docs.metasploit.com/>

msf6 > █

- Nella scansione finale come possiamo vedere abbiamo risolto 4 vulnerabilità critiche ma ci rimane una falsa positiva della UnrealRCd Backdoor che però abbiamo verificato manualmente tramite l'exploit.

