

Vulnerability Assessment

Made by: Max Aldrovandi



Traccia:

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.

Scansione delle vulnerabilità tramite l'utilizzo di Nessus

192.168.40.200



Vulnerabilities

Total: 107

SEVERITY	CVSS V3.0	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	-	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*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS

Per la scansione delle vulnerabilità abbiamo utilizzato **Nessus**, un software proprietario di tipo **client-server** che permette la scansione di numerosi tipi di **vulnerabilità**.

Le vulnerabilità in Nessus vengono classificate in ordine di pericolosità, di seguito le classi di rischio utilizzate da Nessus:

1. **Critical:** Queste sono le vulnerabilità più gravi e possono consentire a un attaccante di ottenere un accesso completo e non autorizzato al sistema o di compromettere seriamente la sicurezza del sistema.
2. **High:** Le vulnerabilità classificate come "High" rappresentano un rischio significativo e possono consentire a un attaccante di compromettere la sicurezza del sistema o di accedere a risorse sensibili.
3. **Medium:** Queste vulnerabilità rappresentano un rischio moderato e potrebbero consentire a un attaccante di ottenere un certo livello di accesso non autorizzato o di compromettere la sicurezza del sistema in misura limitata.
4. **Low:** Le vulnerabilità "Low" rappresentano un rischio relativamente minore e potrebbero non essere sfruttabili senza altre vulnerabilità o senza circostanze particolari.

5. **Info:** Questa categoria include le vulnerabilità che non consentono un accesso diretto o un compromesso del sistema, ma forniscono informazioni sensibili o utili agli attaccanti.

Ai fini del report abbiamo deciso di utilizzare la **lista sommaria** delle **vulnerabilità** fornitaci da Nessus in seguito alla nostra prima scansione della macchina virtuale **'Metasploitable'**.

Una volta identificate le vulnerabilità abbiamo proseguito col **'fixing'** delle medesime.

Fix p.'61708' “VNC Server 'password' Password”

The screenshot displays the Metasploitable interface for Plugin #61708, titled "VNC Server 'password' Password". The interface is divided into several sections:

- Vulnerabilities:** A tab showing 64 vulnerabilities, with the current one highlighted as "CRITICAL".
- Description:** A text block stating: "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:** A text block stating: "Secure the VNC service with a strong password."
- Output:** A section showing the results of a scan, including a message: "Nessus logged in using a password of 'password'." and a table of hosts.
- Plugin Details:** A sidebar on the right containing metadata such as Severity (Critical), ID (61708), Version (\$Revision: 1.2 \$), Type (remote), Family (Gain a shell remotely), Published (August 29, 2012), and Modified (September 24, 2015).
- Risk Information:** A section showing the Risk Factor (Critical), CVSS v2.0 Base Score (10.0), and CVSS v2.0 Vector (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C).
- Vulnerability Information:** A section showing the Default Account (true) and Exploited by Nessus (true).

Per 'fixare' questa vulnerabilità abbiamo proceduto con la chiusura della **porta 5900** sul terminale di **Metasploitable**, in quanto il protocollo VNC era associato a quella porta.

VNC (Virtual Network Computing) è un sistema di **accesso remoto** che consente a un utente di controllare un computer da un altro dispositivo attraverso una connessione di rete.

Nel nostro caso questa funzionalità non era neccessaria, quindi abbiamo proceduto con la chiusura diretta della porta. In futuro se dovesse essere necessario utilizzare il protocollo VNC si potrà riaprire la porta 5900 e proteggerla con una password forte ed eventualmente un firewall.

Per la chiusura della porta abbiamo utilizzato il comando:

sudo iptables -A INPUT -p tcp --dport 5900 -j DROP

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5900 -j DROP
```

Successivamente abbiamo salvato le impostazioni con il comando:

sudo iptables-save

```
msfadmin@metasploitable:~$ sudo iptables-save
# Generated by iptables-save v1.3.8 on Sat May 11 11:56:21 2024
*filter
:INPUT ACCEPT [18984:1978963]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [15883:2510409]
- A INPUT -p tcp -m tcp --dport 1524 -j DROP
- A INPUT -p tcp -m tcp --dport 5900 -j DROP
COMMIT
# Completed on Sat May 11 11:56:21 2024
msfadmin@metasploitable:~$
```

Fix p.'51988' “Bind Shell Backdoor Detection”

Metasploitable / Plugin #51988

[Back to Vulnerabilities](#)

Configure Audit Trail Launch Report Export

Vulnerabilities 64

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	192.168.40.200

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:C/I:C/A:C

Per ‘fixare’ questa vulnerabilità abbiamo proceduto in modo analogo alla chiusura della porta 5900, in questo caso la porta interessata era la **1524**.

Pertanto per la chiusura della porta abbiamo utilizzato il comando:

sudo iptables -A INPUT -p tcp --dport 1524 -j DROP

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
```

Successivamente abbiamo salvato le impostazioni con il comando:

sudo iptables-save

```
msfadmin@metasploitable:~$ sudo iptables-save
# Generated by iptables-save v1.3.8 on Sat May 11 11:56:21 2024
*filter
:INPUT ACCEPT [18984:1978963]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [15883:2510409]
-A INPUT -p tcp -m tcp --dport 1524 -j DROP
-A INPUT -p tcp -m tcp --dport 5900 -j DROP
COMMIT
# Completed on Sat May 11 11:56:21 2024
msfadmin@metasploitable:~$
```

Fix p.'134862' “Apache Tomcat AJP Connector Request Injection (Ghostcat)”

Metasploitable / Plugin #134862

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerabilities](#)

vulnerabilities

critical

Apache Tomcat AJP Connector Request Injection (Ghostcat)

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).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

See Also

<http://www.nessus.org/u/78b6e246>
<http://www.nessus.org/u/78b2734b>
<http://www.nessus.org/u/78c3d54a>
<https://access.redhat.com/security/cve/2020-1745>
<https://access.redhat.com/security/cve/2021-251>
<http://www.nessus.org/u/78d12531>
<http://www.nessus.org/u/78d12531>
<http://www.nessus.org/u/78d12531>
<http://www.nessus.org/u/78d12531>
<http://www.nessus.org/u/78d12531>
<http://www.nessus.org/u/78d12531>

Output

Metasploit was able to exploit the issue using the following request :

0x0000: 02 02 00 08 48 54 54 50 2F 21 2E 31 00 00 0F 2FHTTP/1.1.../
0x0010: 61 73 64 46 2F 78 78 78 78 2E 6A 73 70 00 00 ..add/xxx-xxx-...
0x0020: 09 4C 8F 49 4A 0C 08 08 0F 73 74 00 00 09 8C ..localhost:....
0x0030: 6F 63 61 6C 68 6F 73 74 00 00 00 00 09 8C ..localhost:....
0x0040: 05 0A 68 43 63 70 2D 61 6C 6F 78 65 00 0F 61 ..keep-alive:..A
0x0050: 63 63 65 70 74 2D 4C 61 68 6F 78 61 67 65 00 00 ..compt-1anname...
.....
To see debug logs, please visit individual host

Port

Hosts

8099 / http / http1.1 192.168.40.200

Plugin Details

Severity: Critical

ID: 134862

Version: 1.44

Type: remote

Family: Web Servers

Published: March 24, 2020

Modified: March 19, 2024

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: High

Age of Vuln: 730 days +

Product Coverage: Very High

CVSSv3 Impact Score: 9.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 9.0

Risk Factor: High

CVSS v3.0 Base Score: 9.8

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

CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/R/L/O/R/C

CVSS v3.0 Temporal Score: 9.4

CVSS v2.0 Base Score: 7.5

CVSS v2.0 Temporal Score: 6.5

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

CVSS v2.0 Temporal Vector: CVSS2#E:H/R/L/O/R/C

Vulnerability Information

CPE: cpe:/a:apache:tomcat

Exploit Available: true

Per ‘fixare’ questa vulnerabilità abbiamo proceduto nel seguente modo:

- Abbiamo localizzato il file ‘server.xml’ tramite il comando

find / -name "server.xml"

- Abbiamo modificato il file ‘**server.xml**’ tramite un editor di testo, in questo caso abbiamo utilizzato il comando ‘nano’.

Per modificare il file abbiamo inizialmente individuato nel file la parte relativa alla configurazione del **connetttore AJP**, successivamente abbiamo aggiunto l'attributo ‘**requiredSecret**’ alla configurazione del connettore per **richiedere l'autorizzazione**.

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
            enableLookups="false" redirectPort="8443" protocol="AJP/1.3"
            requiredSecret="msfadmin" />
```

- Infine abbiamo **riavviato** il servizio **Tomcat** tramite i comandi:

sudo /etc/init.d/tomcat5.5 stop

e

sudo /etc/init.d/tomcat5.5 start

```
msfadmin@metasploitable:~$ sudo /etc/init.d/tomcat5.5 stop
* Stopping Tomcat servlet engine tomcat5.5 [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/tomcat5.5 start
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
msfadmin@metasploitable:~$
```

Fix p.'11356' “NFS Exported Share Information Disclosure”

The screenshot shows the Metasploit web interface for vulnerability #11356. The interface is dark-themed and includes a top navigation bar with buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. The main content area is divided into several sections:

- Vulnerabilities**: A tab showing 64 vulnerabilities, with the current one highlighted as 'CRITICAL'.
- Description**: A text block stating that at least one of the NFS shares exported by the remote server could be mounted by the scanning host, allowing an attacker to read (and possibly write) files on the remote host.
- Solution**: A text block suggesting to configure NFS on the remote host so that only authorized hosts can mount its remote shares.
- Output**: A text block showing the results of a scan, indicating that the following NFS shares could be mounted: /, /bin, /boot, and /dev. A 'MORE...' link is provided for additional details.
- Port**: A table showing the port used for the scan, which is 2049 / udp / rpc-nfs.
- Hosts**: A table showing the IP address of the host, which is 192.168.40.200.
- Plugin Details**: A section on the right side of the interface providing detailed information about the vulnerability, including its severity (Critical), ID (11356), version (1.21), type (remote), family (RPC), published date (March 12, 2003), and modified date (August 30, 2023).
- VPR Key Drivers**: A section on the right side of the interface providing key drivers for the vulnerability, including threat recency, threat intensity, exploit code maturity, age of vuln, product coverage, CVSSv3 impact score, and threat sources.
- Risk Information**: A section on the right side of the interface providing risk information, including the vulnerability priority rating (VPR) of 5.9, risk factor of Critical, and CVSS v2.0 base score of 10.0.

Per 'fixare' questa vulnerabilità abbiamo agito in due modi:

- Abbiamo limitato la lista dei volumi condivisibili e abbiamo creato una cartella fittizia tramite i comandi:

sudo nano /etc/exports (lista dei volumi condivisibili)

/_____*(rw,sync,no_root_squash,no_subtree_check) (volumi inizialmente condivisi)

/srv/nfs (creazione cartella fittizia)

/srv/nfs *(rw, sync) (volumi condivisi aggiornati)

```
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)
#
/ *(rw, sync, no_root_squash, no_subtree_check)

[ Read 12 lines ]
^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
```

volumi condivisibili iniziali

```
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)
#
/srv/nfs *(rw, sync)_

[ Wrote 12 lines ]
^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
```

volumi condivisibili aggiornati

- Abbiamo limitato la lista degli host che potevano accedere alle share condivise tramite il comando

sudo nano /etc/hosts.allow

```

GNU nano 2.0.7      File: /etc/hosts.allow      Modified
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
ALL:ALL

```

^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

host autorizzati iniziali

```

GNU nano 2.0.7      File: /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
ALL:ALL EXCEPT 192.168.40.100

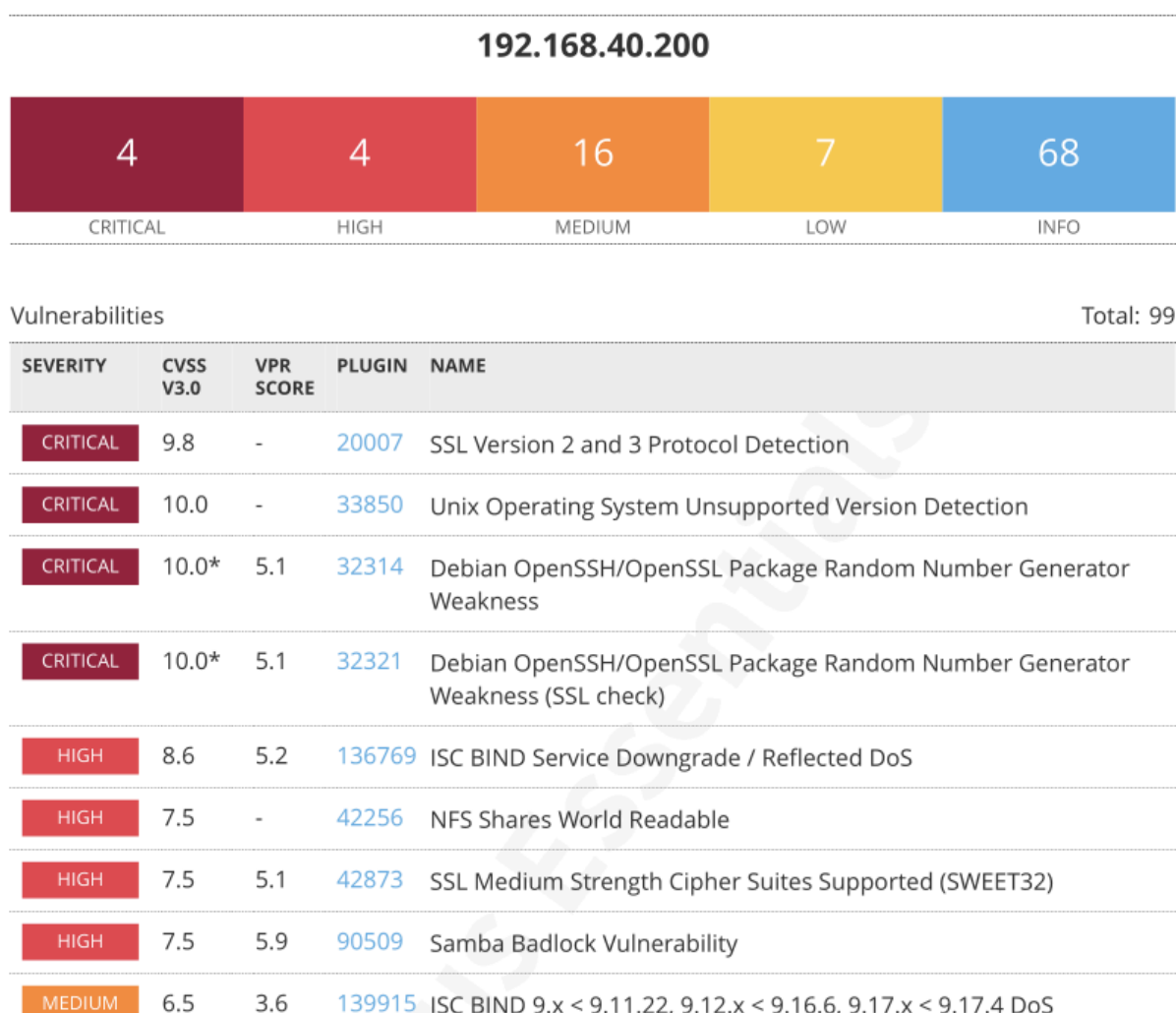
```

[Wrote 14 lines]

^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

Nuova scansione per verificare la reale risoluzione delle vulnerabilità

Abbiamo infine proceduto con una **nuova scansione** con Nessus per verificare il reale **'fixaggio'** delle **vulnerabilità** sopra elencate.



E come previsto le vulnerabilità che abbiamo 'fixato' non sono più presenti.