CONSEGNA W12D4

TRACCIA:

Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche 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.

Lo svolgimento sarà eseguito suddividendo l'esercitazione in 3 fasi:

1. Scansione iniziale
2. Remediation
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità

FASE 1

1.1 REPORT INFORMATIVO

Report – Scansione dei Servizi – Target Metasploitable 192.168.50.101

Francesco D'Amora

Data della scansione: 01/10/2025
Strumento utilizzato: Nessus Vulnerability Scanner
Ambiente analizzato: Macchina virtuale Metasploitable 2
Obiettivo: Valutare il livello di esposizione e rischio associato ai servizi attivi sull'host interno 192.168.50.101

Sintesi dei risultati

GRAVITA'	***NUMERO DI VULNERABILITA'***
CRITICO	7
ALTO	4
MEDIO	16
BASSO	2

Principali minacce rilevate

1. **Accesso remoto non autorizzato:** Diverse vulnerabilità critiche permettono l'ottenimento di una shell remota.
2. **Servizi esposti:** Porte aperte su servizi sensibili (FTP, SSH, Telnet, SMTP, HTTP, SMB, MySQL).
3. **Crittografia debole:** Presenza di vulnerabilità SSL (es. DROWN) che espongono il sistema ad attacchi man-in-the-middle.
4. **Configurazioni errate:** Problemi DNS e HTTP che potrebbero facilitare attacchi di enumerazione o spoofing.

Soluzioni

- Disabilitare servizi non necessari (es. Telnet)
- Rivedere configurazioni DNS e HTTP.
- Aggiornare certificati SSL e disabilitare protocolli obsoleti.
- Filtrare ICMP timestamp a livello di firewall.
- Monitorare costantemente i servizi esposti.
- Eseguire scansioni periodiche per rilevare nuove vulnerabilità.

Conclusioni

Il sistema presenta vulnerabilità critiche e medie che potrebbero compromettere la sicurezza dell'infrastruttura. È fondamentale intervenire con urgenza per mitigare i rischi più elevati e rafforzare la sicurezza generale

VULNERABILITA CRITICHE

CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1	
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	
CRITICAL	9.8	8.9	0.9448	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1	
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	

IP:	192.168.50.101
MAC:	08:00:27:6F:33:5E
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	September 29 at 10:21 PM
End:	September 29 at 10:45 PM
Elapsed:	24 minutes
KB:	Download
Auth:	Fail

Vulnerabilities

VULNERABILITA ALTE

HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5

VULNERABILITA MEDIE

MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	3.6	0.9015	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MIXED	...	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	3
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2
MIXED	...	...	...	TLS (Multiple Issues)	Misc.	2
MIXED	...	...	...	TLS (Multiple Issues)	SMTP problems	2

VULNERABILITA BASSE

LOW	2.6 *			X Server Detection	Service detection	1
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1

FASE 1.2 SCANSIONE CON NESSUS

Metasplotable 2

Report generated by Tenable Nessus™ Mon, 29 Sep 2025 22:45:55 CEST

192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
7	4	16	7	74

Vulnerabilities Total: 108

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.9448	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	-	-	201352	Canonical Ubuntu Linux SEoL (8.04.x)
CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0334	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	0.3085	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.7865	90509	Samba Badlock Vulnerability
MEDIUM	6.5	4.4	0.0045	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.9228	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.027	31705	SSL Anonymous Cipher Suites Supported

MEDIUM	5.9	3.6	0.9015	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsole and Weakened eNcryption)
MEDIUM	5.9	7.3	0.9032	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	0.5885	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	7.3	0.6945	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	1.4	0.9191	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	0.9391	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Suppor (Logjam)
LOW	3.4	5.1	0.9377	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	-	10407	X Server Detection
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	21186	AJP Connector Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)

INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11156	IRC Daemon Version Detection
INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosu
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (rem check)
INFO	N/A	-	-	10437	NFS Share Export List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available

INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites

INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	19288	VNC Server Security Type Detection
INFO	N/A	-	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	10342	VNC Software Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

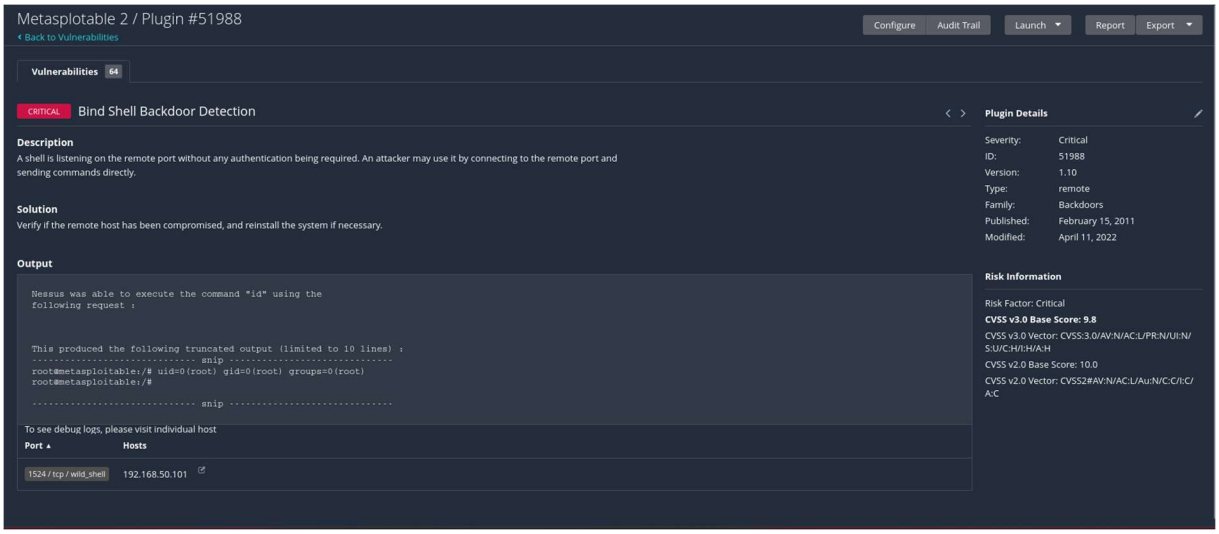
FASE 2 REMEDIATION

2.1 Analisi personale

Vulnerabilità nel dettaglio

Andiamo ad analizzare e a risolvere nello specifico qualche problema/vulnerabilità in modo da rendere più sicura la metasploitable.

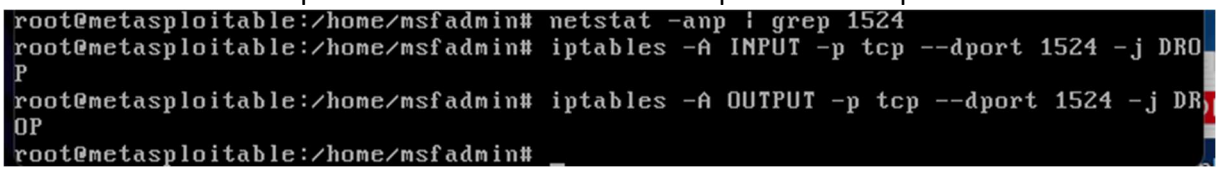
1.Bind Shell Backdoor Detection



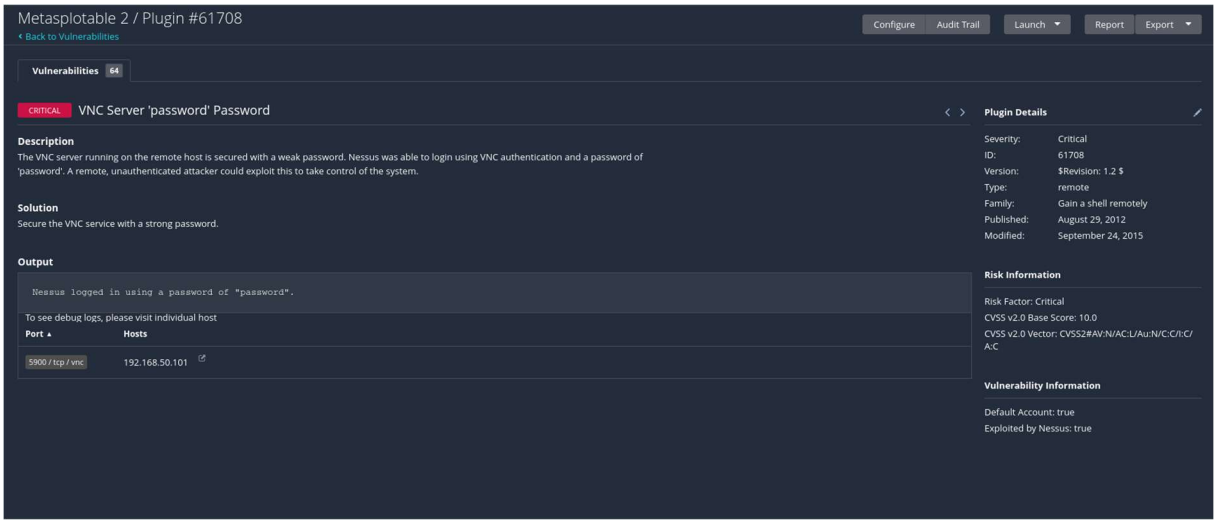
- **Descrizione:** Rilevamento di una backdoor che consente l'accesso remoto tramite shell bind.
- **Soluzioni**: Isolare il sistema, eseguire scansioni approfondite, rimuovere la backdoor e reinstallare da backup sicuro.

Usando il comando “netstat -anp | grep 1524” notiamo come ci restituisce una riga con LISTEN, mostrando come la porta sia in ascolto indice che la bind shell è attiva come confermato dal comando seguente “telnet localhost 1524”.

Andiamo dunque a vedere nello specifico il servizio attivo con il comando “ps aux | grep ‘[i]netd’ “, per poi usare il comando “kill -9 4411 && xinetd &”. Come verifichiamo nella figura seguente andiamo a fare prima una verifica finale e poi rafforzare la sicurezza bloccando la porta a livello di firewall sia in input che in output.



2.VNC Server Password / Password

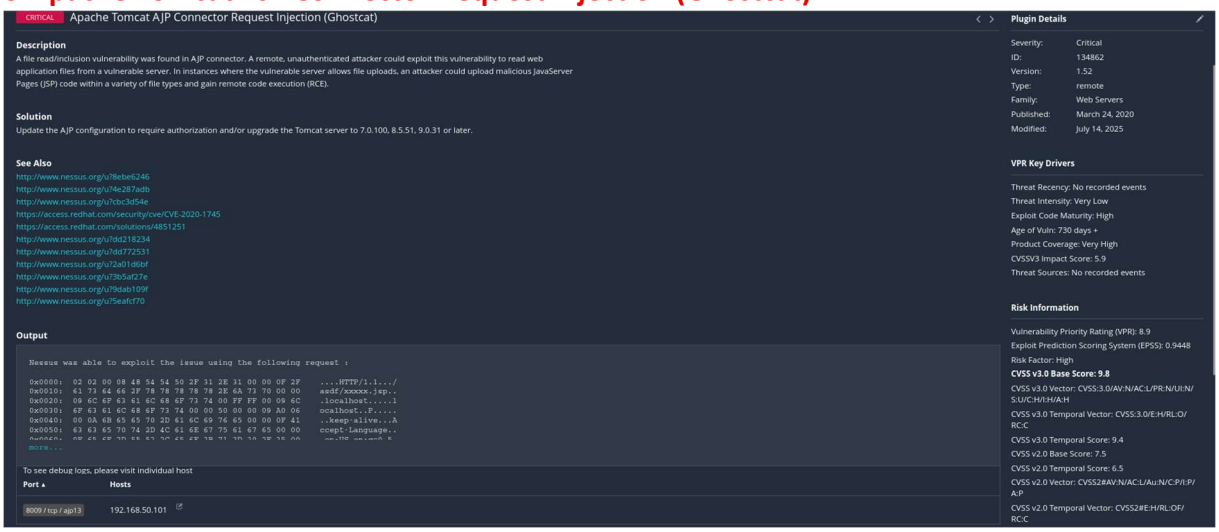


- **Descrizione:** Un VNC configurato con password semplici e di facile lettura da parte di Nessus può comportare ad un accesso da remoto non autorizzato con annesso controllo completo del sistema da parte dell'attaccante
- **Soluzioni**: Rendere sicuro il servizio VNC attraverso l'utilizzo di password sicure

Come impostato in precedenza il server VNC accettava connessioni remote con la password predefinita, permettendo dunque molto semplicemente accessi non autorizzati. Nello specifico abbiamo iniziato eseguendo il comando "ps aux | grep vnc" con lo scopo di cercare i processi attivi filtrando solo quelli contenti la parola vnc.
Dopo aver identificato il processo in questione (/rootf/.vnc/passwd) lo modifichiamo impostando una nuova password molto più sicura pur restando nel range di 8 caratteri (usando il comando "vncpasswd"), per poi verificare che i permessi siano di lettura e scrittura del comando sia sono del root per garantirne la sicurezza.

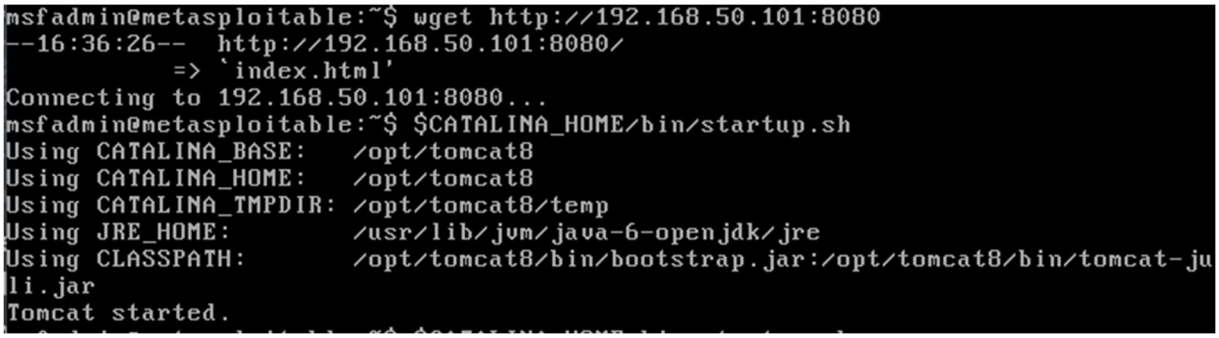
```
root@metasploitable:~# ps aux | grep vnc
root      4610  0.0  0.5  13928 12012 ?        S    06:28   0:00 Xtightvnc :0 -d
esktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -r
fbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fo
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/shar
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
root      4614  0.0  0.0   2724  1188 ?        S    06:28   0:00 /bin/sh /root/.
vnc/xstartup
root      4737  0.0  0.0   3004   752 tty1     R+   06:38   0:00 grep vnc
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~#
```

3.Apache Tomcat AJP Connector Request Injection (Ghostcat)



- **Descrizione:** Permette ad un attaccante remoto di accedere ai file sensibili o eseguire codice arbitrario tramite il protocollo AJP.
- **Soluzioni**: Aggiornare Tomcat server a una delle seguenti versioni 7.0.100, 8.5.51, 9.0.31 o più recente.

La versione di Tomcat adottata dal sistema è piena di vulnerabilità note di conseguenza è stata aggiornata ad una versione più recente e sicura (la v.8.5.51) tramite il comando “wget http://archive.apache.org/dist/tomcat/tomcat-8/v8.5.51/bin/apache-tomcat-8.5.51.tar.gz”. In seguito è stata installata manualmente la versione partendo dall’estrazione (con il comando “tar -xvzf apache-tomcat-8.5.51.tar.gz”) e poi spostata in una posizione permanente del filesystem (ovvero /opt/tomcat8). Successivamente è stata configurata al fine di rimuovere il connettore AJP ed infine avviato.



2.2 REMEDIATION ANALISI NESSUS

192.168.50.101

9	5	22	8	129
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Sep 29 22:21:54 2025
End time:	Mon Sep 29 22:45:55 2025

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.101
MAC Address:	08:00:27:6F:33:5E
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

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).

See Also

http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531

http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70

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.

Risk Factor

High

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)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

8.9

EPSS Score

0.9448

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2020-1745
CVE	CVE-2020-1938
XREF	CISA-KNOWN-EXPLOITED:2022/03/17
XREF	CEA-ID:CEA-2020-0021

Plugin Information

Published: 2020/03/24, Modified: 2025/07/14

Plugin Output

tcp/8009/ajp13

```
Nessus was able to exploit the issue using the following request :

0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
0x0060:  0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00    .en-US,en;q=0.5.
0x0070:  A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45    ....0...Accept-E
0x0080:  6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20    ncoding...gzip,
0x0090:  64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D    deflate, sdch...
0x00A0:  43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09    Cache-Control...
0x00B0:  6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F    max-age=0.....Mo
0x00C0:  7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D    zilla...Upgrade-
0x00D0:  49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74    Insecure-Request
0x00E0:  73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68    s...1.....text/h
0x00F0:  74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73    tml.....localhos
0x0100:  74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C    t...!javax.servl
0x0110:  65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65    et.include.reque
0x0120:  73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61    st_uri...1....ja
0x0130:  76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C    vax.servlet.incl
0x0140:  75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10    ude.path_info...
0x0150:  2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C    /WEB-INF/web.xml
0x0160:  00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65    ...*javax.servle
0x0170:  74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65    t.include.servle
0x0180:  74 5F 70 61 74 68 00 00 00 00 FF                   t_path.....


This produced the following truncated output (limite [...]
```

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)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

```
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 ------------------------------
```

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:C/I:C/A:C)

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc

```
Nessus logged in using a password of "password".
```

3.3 SCANSIONE FATTA DOPO LE CORREZIONI

192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
4	4	15	7	63

Vulnerabilities — Total: 93

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	201352	Canonical Ubuntu Linux SEoL (8.04.x)
CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
HIGH	8.6	5.2	0.0334	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	0.3085	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.7865	90509	Samba Badlock Vulnerability
MEDIUM	6.5	4.4	0.0045	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.9228	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.027	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	3.6	0.9015	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsole and Weakened eNcryption)
MEDIUM	5.9	7.3	0.9032	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	57608	SMB Signing not required

MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	7.3	0.6945	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	1.4	0.9191	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	0.9391	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Suppor (Logjam)
LOW	3.4	5.1	0.9377	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	-	10407	X Server Detection
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses

INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosur
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	10437	NFS Share Export List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted

INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	19288	VNC Server Security Type Detection
INFO	N/A	-	-	65792	VNC Server Unencrypted Communication Detection

INFO	N/A	-	-	10342	VNC Software Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Confrontando le due scansioni notiamo come le 3 vulnerabilità prese in esame siano state risolte e come di conseguenza non compaiono nella nuova scansione con nessus.

CONCLUSIONI

Aggiornare il Sistema Operativo: Oltre ad aggiornare il SO bisogna anche aggiornare tutte le versioni dei servizi attivi installando inoltre anche le patch di sicurezza disponibili.
Disabilitare i servizi superflui: Disattivare i protocolli obsoleti e limitare l'accesso ai servizi solo agli utenti autorizzati.
Segmentazione della rete: Implementare firewall interni per limitare la comunicazione in entrata.
Monitoraggio e Logging: Monitorare costantemente i log di sistema per eventuali attività sospette.
Formazione sulla sicurezza del personale: insegnando al personale tutte le pratiche preventive per la sicurezza come ad esempio l'uso di password di sicurezza più forti e cambi periodici di queste ultime.
Infine programmare e pianificare test di sicurezza periodici per identificare eventuali nuove vulnerabilità.