



PROGETTO S5/L5

Giorgio Trovesi

Vulnerability Scanner

Tramite l'utilizzo di Nessus abbiamo effettuato una scansione completa alla macchina target Metasploitable che ha identificato diverse vulnerabilità.

Dall'immagine a lato possiamo osservare un estratto del report di Nessus.

192.168.1.189				
CRITICAL	HIGH	MEDIUM	LOW	INFO
8	4	18	7	67
Vulnerabilities Total: 104				
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN NAME	
CRITICAL	9.8	9.0	134862 Apache Tomcat AJP Connector Request Injection (Ghostcat)	
CRITICAL	9.8	-	20007 SSL Version 2 and 3 Protocol Detection	
CRITICAL	9.1	6.0	33447 Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	
CRITICAL	10.0	-	33850 Unix Operating System Unsupported Version Detection	
CRITICAL	10.0*	7.4	32314 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	
CRITICAL	10.0*	7.4	32321 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	
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	6.7	90509 Samba Badlock Vulnerability	
MEDIUM	6.5	3.6	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	

Vulnerabilità 1

VNC Server Password

A causa di una password troppo facilmente identificabile (in questo caso “password”) un utente malintenzionato potrebbe prendere controllo del sistema da remoto.

Per risolvere questa vulnerabilità abbiamo dovuto cambiare la password tramite l'utilizzo del comando “vncpasswd”.

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.

```
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#
```

Vulnerabilità 2

Apache Tomcat AJP Connector

A causa di questa vulnerabilità un attaccante potrebbe caricare codice JavaServer Pages (JSP) e ottenere l'esecuzione da remoto.

Per risolvere questo problema bisognava operare sulla porta 8009 nel file "/server.xml".

Si può procedere disattivando il servizio tramite commento della porta o implementando ad essa un'autenticazione tramite password.

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.

```
GNU nano 2.0.7           File: /etc/tomcat5.5/server.xml          Modified

enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />

-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
            enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" address="192.168.1.189" secret="Ep1c0D3!23" />
```

```
GNU nano 2.0.7           File: /etc/tomcat5.5/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" />-$
```

Conclusioni

Possiamo infine osservare con un'ulteriore scansione che grazie alle remediation actions le vulnerabilità sulla nostra macchina target sono diminuite.

