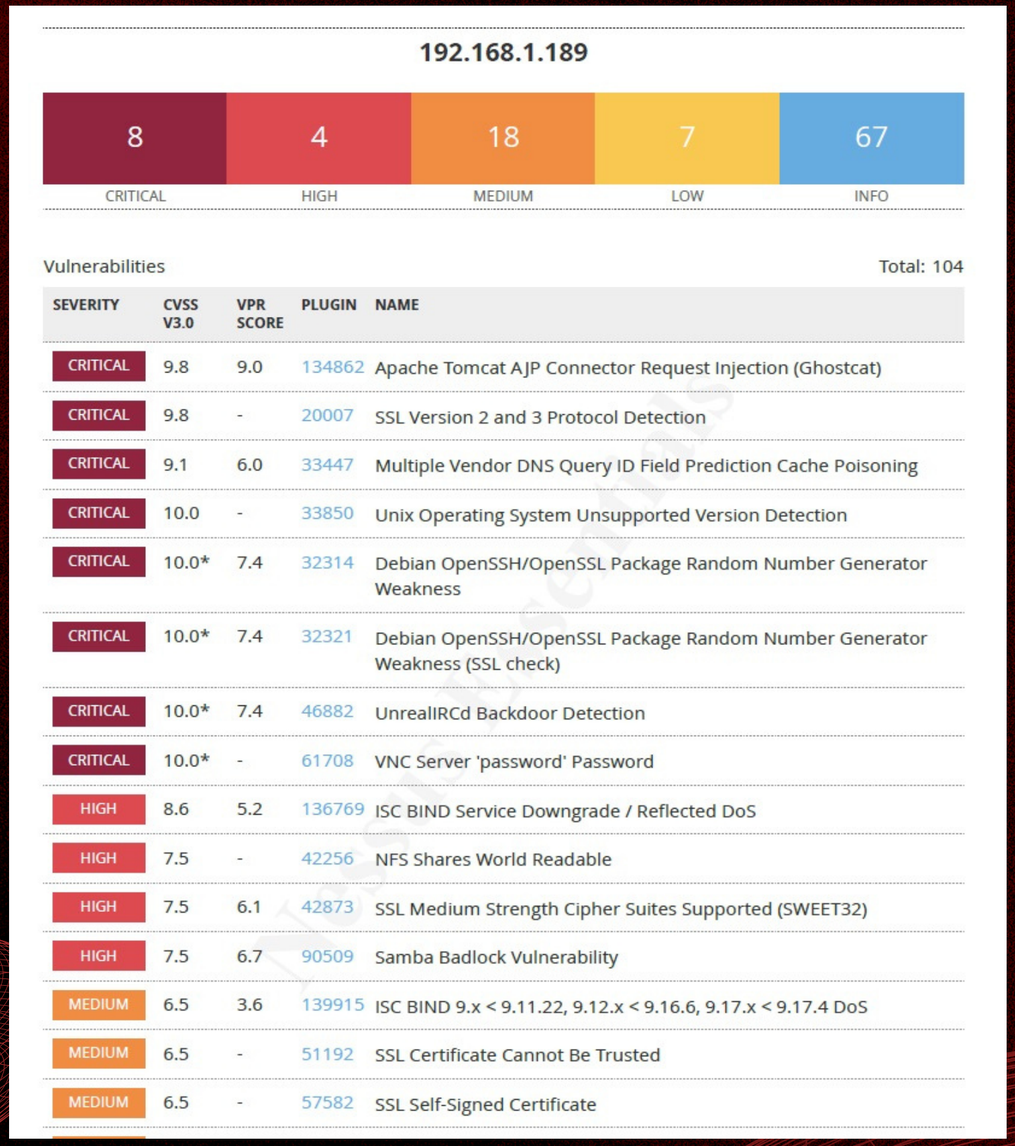
PROGETTO S5/L5

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

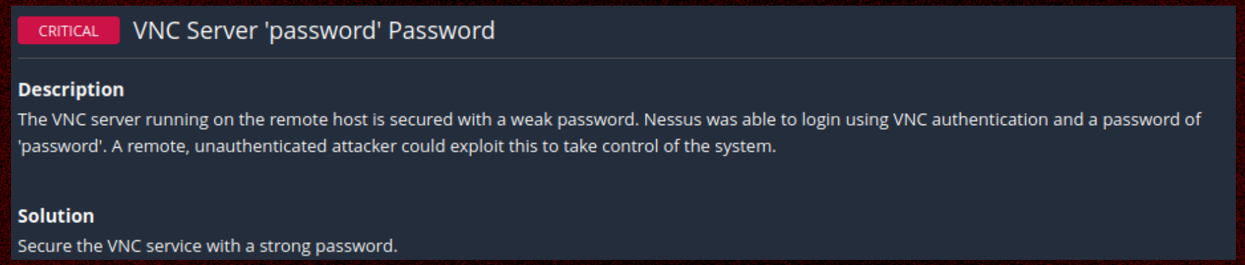
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating 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”.



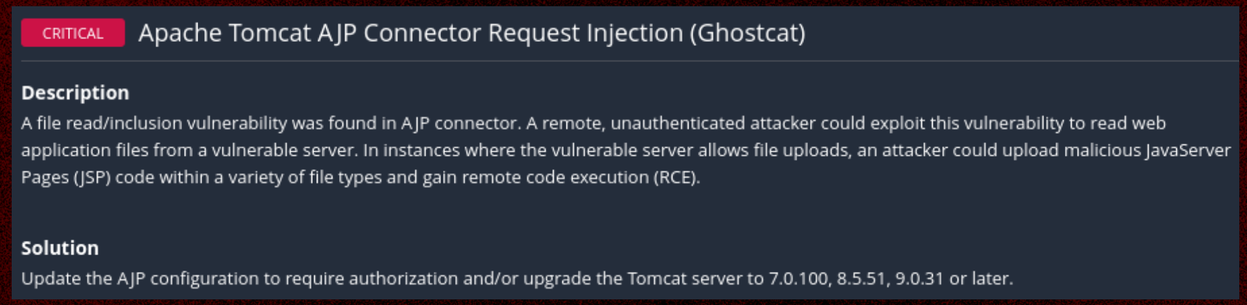

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

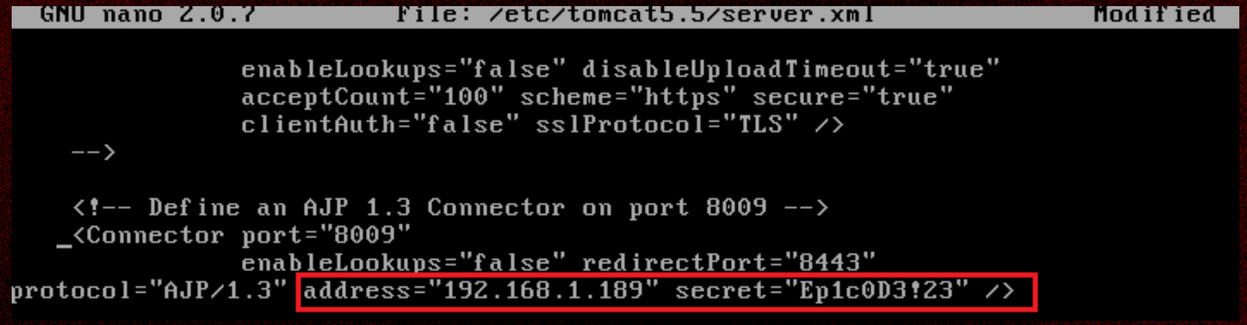
Vulnerabilità 2

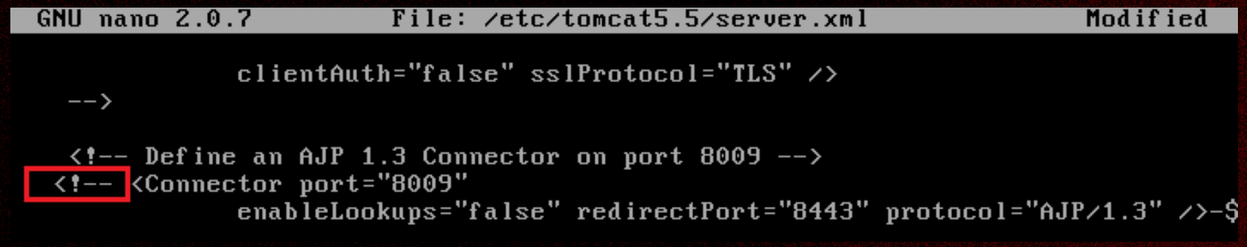
Apache Tomcat AJP Connector

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.

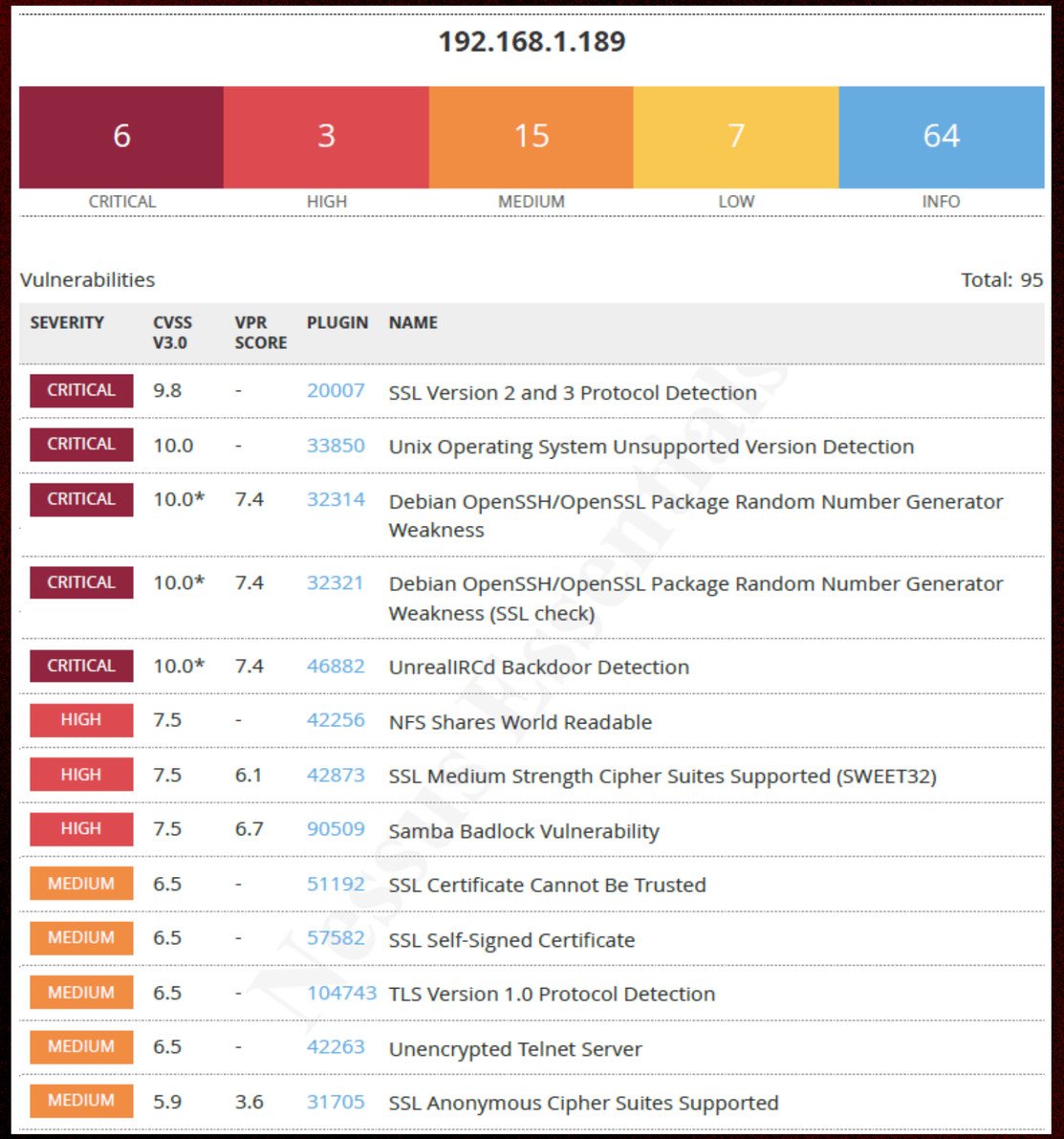






Conclusioni

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



192.168.1.189

6	3	15	7	64
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 95

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
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
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	-	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	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported