Verifica Finale delle Vulnerabilità - Metasploitable2

1. Introduzione

Questa relazione documenta la scansione finale effettuata con Nessus sulla macchina vulnerabile Metasploitable2, dopo l'esecuzione di tutte le azioni di remediation relative alle vulnerabilità critiche individuate nella prima analisi.

Obiettivo della scansione è verificare che i servizi vulnerabili siano stati disattivati, corretti o resi inaccessibili, e che le vulnerabilità precedentemente rilevate non siano più presenti nel sistema.

2. Metodo

- È stata utilizzata una scansione **Advanced** di Nessus
- Target: **192.168.50.101** (IP di Metasploitable2)

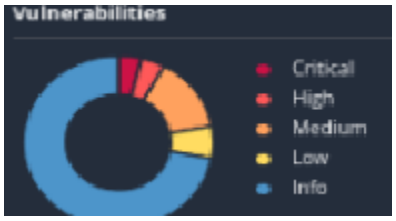
3. Risultati

La scansione Nessus non ha più rilevato le seguenti vulnerabilità critiche, presenti nella prima analisi:

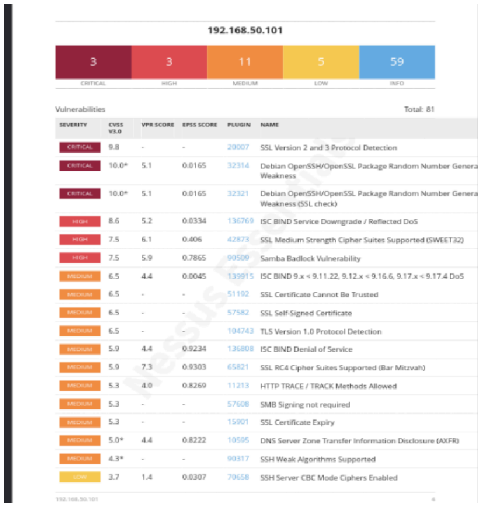
Porta	Servizio	Vulnerabilità	Stato finale
2049	NFS	NFS Share Disclosure	Non rilevata
512	rexec	Remote Execution	Non rilevata
5900	VNC	Weak Authentication	Non rilevata
1524	Bind Shell	Backdoor con shell root attiva	Non rilevata

4. Screenshot

📊 **Grafico riepilogativo** delle vulnerabilità finali :

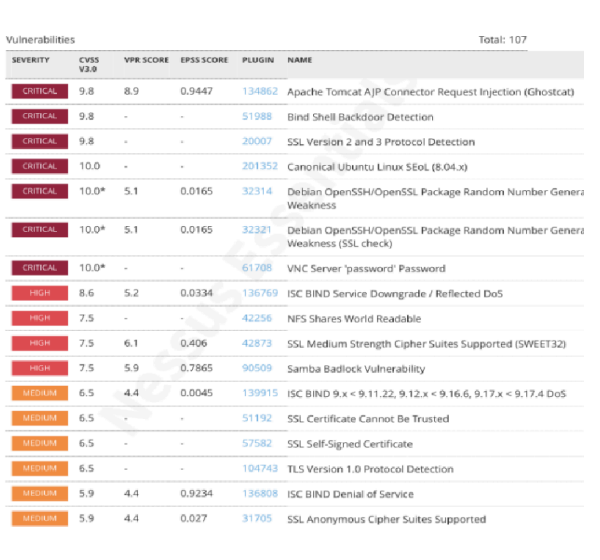


📋 **Lista delle vulnerabilità:**



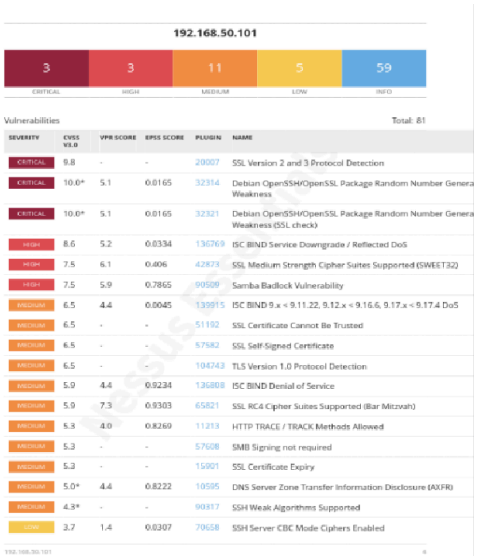
Confronto con la prima scansione:

PRIMA: **DOPO:**



Vulnerabilities Total: 107

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.9447	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	0.406	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	0.9234	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.027	31705	SSL Anonymous Cipher Suites Supported



192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	3	11	5	59

Vulnerabilities Total: 81

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
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	6.1	0.406	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	0.9234	136808	ISC BIND Denial of Service
MEDIUM	5.9	7.3	0.9303	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	0.8260	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.0*	4.4	0.8222	10595	DNS Server Zone Transfer Information Disclosure (AXFR)
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled

5. Conclusione

La scansione finale conferma che le vulnerabilità selezionate sono state efficacemente corrette. Le porte vulnerabili sono risultate chiuse o filtrate e Nessus non le riporta più tra i problemi di sicurezza.

Questo dimostra che gli interventi tecnici (disattivazione servizi, firewall, rimozione processi) hanno raggiunto l'obiettivo di mitigare le criticità presenti nel sistema.