BENCHMARK W12D4 - Domenico Vecchio

Scansione Iniziale delle Vulnerabilità su Metasploitable2

1. Introduzione

In questa fase iniziale del lavoro è stata effettuata una scansione delle vulnerabilità sulla macchina virtuale **Metasploitable2**, un sistema deliberatamente vulnerabile usato a scopo didattico e per test di sicurezza.

La scansione è stata eseguita utilizzando lo strumento **Nessus**, installato e configurato sulla macchina Kali Linux.

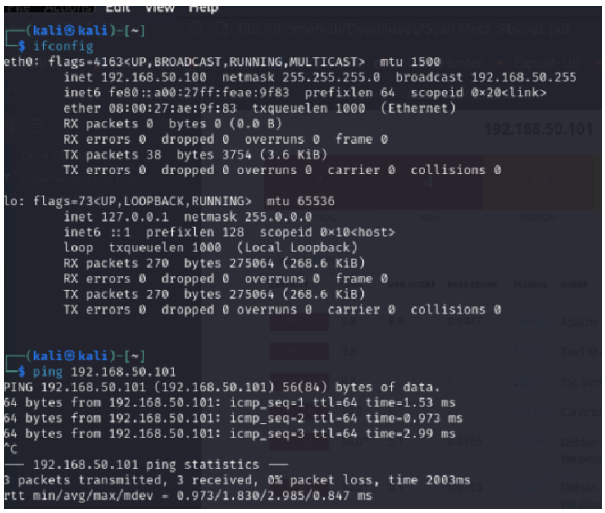
L'obiettivo è:

- Identificare tutti i servizi attivi su Metasploitable
- Rilevare le vulnerabilità critiche
- Selezionarne alcune per l'analisi e la correzione

2. Configurazione della scansione

Ambiente di rete:

- **Kali Linux** e **Metasploitable2** sono collegate tramite **rete interna (Internal Network)** su VirtualBox
- La connettività tra le due è stata verificata con il comando ping:



Parametri della scansione:

- Tipo: **Advanced Scan**
- Nome scansione: ScanMeta
- Target: **Indirizzo IP di Metasploitable** (192.168.50.101)

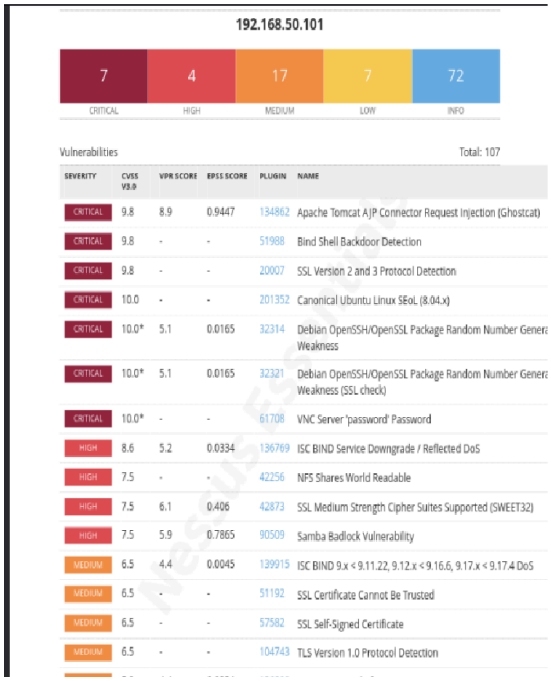
La scansione è stata avviata dalla sezione **My Scans → New Scan → Advanced Scan**, e poi lanciata cliccando su **Launch**.

.

3. Risultato della scansione

Dopo alcuni minuti, Nessus ha completato la scansione restituendo un report dettagliato. I risultati mostrano:

- Numerose vulnerabilità critiche, molte delle quali derivano da servizi attivi obsoleti o mal configurati
- Un grafico a torta che classifica le vulnerabilità in base al livello di gravità e la lista delle vulnerabilità:

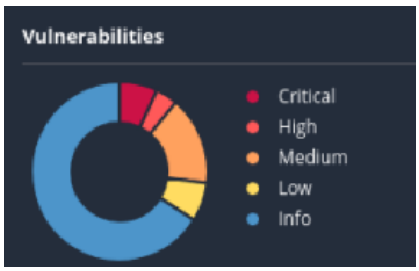


192.168.50.101

7	4	17	7	72
CRITICAL	HIGH	MEDIUM	LOW	INFO

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 Generator Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Generator 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



4. Vulnerabilità critiche selezionate

Dalla lista delle vulnerabilità rilevate, sono state selezionate 4 criticità tra le più pericolose (in linea con quelle evidenziate nella traccia) da correggere nella fase successiva.

Nome vulnerabilità	Porta / Servizio	Descrizione sintetica
NFS Share Disclosure	2049/tcp (NFS)	Consente la condivisione remota di file senza restrizioni; chiunque può accedere a dati sensibili.
rexec Remote Execution	512/tcp (rexec)	Permette l'esecuzione di comandi remoti senza autenticazione.
VNC Weak Authentication	5900/tcp (VNC)	Il server VNC accetta connessioni con password debole o nulla, permettendo il controllo remoto.
Bind Shell Backdoor	1524/tcp (bind shell)	Backdoor attiva che fornisce accesso remoto diretto come utente root tramite shell.

5. Conclusione

La scansione iniziale ha confermato che la macchina Metasploitable presenta **un'ampia superficie d'attacco**, con diversi servizi obsoleti o configurati in modo insicuro.

Le vulnerabilità selezionate sono potenzialmente **sfruttabili da remoto** per ottenere l'accesso al sistema, eseguire comandi o compromettere dati sensibili.

Nella prossima fase si procederà con la **correzione (remediation)** di queste criticità.