

Vulnerability Assessment Report

Target: Metasploitable2

Durata temporale dell'attività:
7 ore

Attività eseguita da:
Leonzio Emanuele

Report Conclusivo: Analisi e Mitigazione delle Vulnerabilità su Metasploitable2

Indice generale Sommario

Premessa.....	3
Approccio alla mitigazione.....	4
Risultati con il nuovo scan.....	5
Analisi grafica.....	5
Conclusioni.....	6

Premessa

L'obiettivo iniziale di questo progetto è stato identificare e mitigare le vulnerabilità presenti sul sistema **Metasploitable2**. Per fare ciò, è stato eseguito uno scan iniziale utilizzando **Nessus**, un noto strumento per il Vulnerability Assessment, che ha evidenziato una serie di vulnerabilità critiche e ad alto rischio.

Tra le vulnerabilità più rilevanti individuate vi erano:

1. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**
2. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness/**
(SSL check)
3. **Bind Shell Backdoor Detection**
4. **Secure the VNC Service**

Tutte queste vulnerabilità rappresentavano potenziali vettori di compromissione per il sistema, con un rischio elevato per l'integrità e la sicurezza delle risorse.

Approccio alla Mitigazione

Dopo l'analisi dei risultati dello scan, sono state applicate le seguenti contromisure per mitigare le vulnerabilità:

1. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness:

- Aggiornamento dei pacchetti OpenSSL e OpenSSH a versioni sicure.
- Rigenerazione delle chiavi crittografiche compromesse.

2. Bind Shell Backdoor Detection:

- Individuazione e terminazione dei processi malevoli con ps e kill.
- Modifica delle configurazioni del sistema per impedire il binding di shell non autorizzate.
- Esecuzione di un audit per garantire che non vi fossero altre backdoor.

3. Secure the VNC Service:

- Configurazione di una password forte per il servizio VNC utilizzando vncpasswd.
- Blocco dell'accesso non autorizzato configurando regole di firewall per il traffico su porte utilizzate dal VNC.

Risultati del Nuovo Scan Nessus

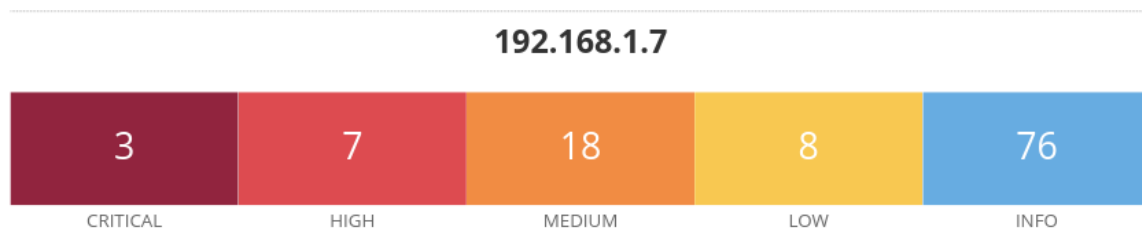
Dopo l'implementazione delle misure di mitigazione, è stato effettuato un nuovo scan del sistema utilizzando **Nessus**. I risultati mostrano un **miglioramento significativo** rispetto alla scansione iniziale.

Analisi Grafica

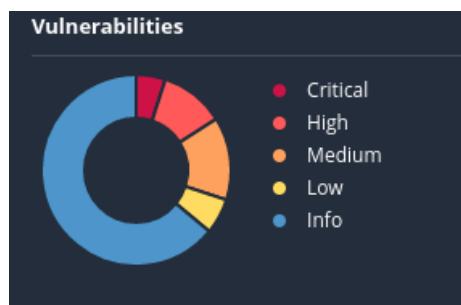
Di seguito, sono riportati i grafici comparativi che illustrano il miglioramento del livello di sicurezza del sistema:

1. Distribuzione delle vulnerabilità per livello di rischio Critical:

- Prima della mitigazione: 8.
- Dopo la mitigazione: 3.



Filter	Search Vulnerabilities		64 Vulnerabilities				
<input type="checkbox"/> Sev	CVSS	VPR	EPSS	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0 *		0.6661	UnrealIRCd Backdoor Detection	Backdoors	1	
<input type="checkbox"/> CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	
<input type="checkbox"/> MIXED	Apache Tomcat (Multiple Issues)	Web Servers	3	
<input type="checkbox"/> HIGH	7.5		0.0358	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/> HIGH	7.5 *		0.015	rlogin Service Detection	Service detection	1	
<input type="checkbox"/> HIGH	7.5 *		0.015	rsh Service Detection	Service detection	1	
<input type="checkbox"/> HIGH	7.5		0.0111	SSL Certificate Signed Using Weak Hashing Algorithm	General	2	
<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC	1	
<input type="checkbox"/> MIXED	SSL (Multiple Issues)	General	30	
<input type="checkbox"/> MIXED	ISC Bind (Multiple Issues)	DNS	5	
<input type="checkbox"/> MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2	



Conclusioni

Grazie all'identificazione e alla mitigazione delle vulnerabilità critiche rilevate durante il primo scan con Nessus, il livello di sicurezza del sistema **Metasploitable2** è migliorato in modo significativo. Le contromisure applicate hanno permesso di eliminare i rischi principali, riducendo drasticamente la superficie di attacco del sistema.

Questo dimostra come un processo strutturato di Vulnerability Assessment e di gestione delle vulnerabilità sia essenziale per proteggere i sistemi esposti. Consigliamo di continuare a monitorare il sistema regolarmente e di applicare aggiornamenti di sicurezza non appena disponibili.