Vulnerability Assessment con Nessus

Introduzione

La relazione descrive l'esecuzione di un'attività di vulnerability assessment sulla macchina virtuale Metasploitable utilizzando Nessus Essential, uno strumento professionale per l'identificazione e l'analisi delle vulnerabilità di sicurezza informatica.

Obiettivi

L'obiettivo principale dell'esercitazione è stato effettuare un vulnerability scanning sulla macchina Metasploitable, concentrandosi sulle seguenti porte comuni:

- Range porte 21-23 (FTP, Telnet, SSH)
- Porta 25 (SMTP)
- Porta 53 (DNS)
- Porta 80 (HTTP)
- Porta 110 (POP3)
- Porta 139 (NetBIOS)
- Porta 443 (HTTPS)
- Porta 445 (SMB)
- Porta 3389 (RDP)

L'analisi ha permesso di identificare vulnerabilità critiche, valutarne il rischio attraverso lo score CVSS (Common Vulnerability Scoring System) e proporre mitigazioni adeguate.

Configurazione della Scansione

La scansione è stata configurata in Nessus Essential con le seguenti impostazioni:

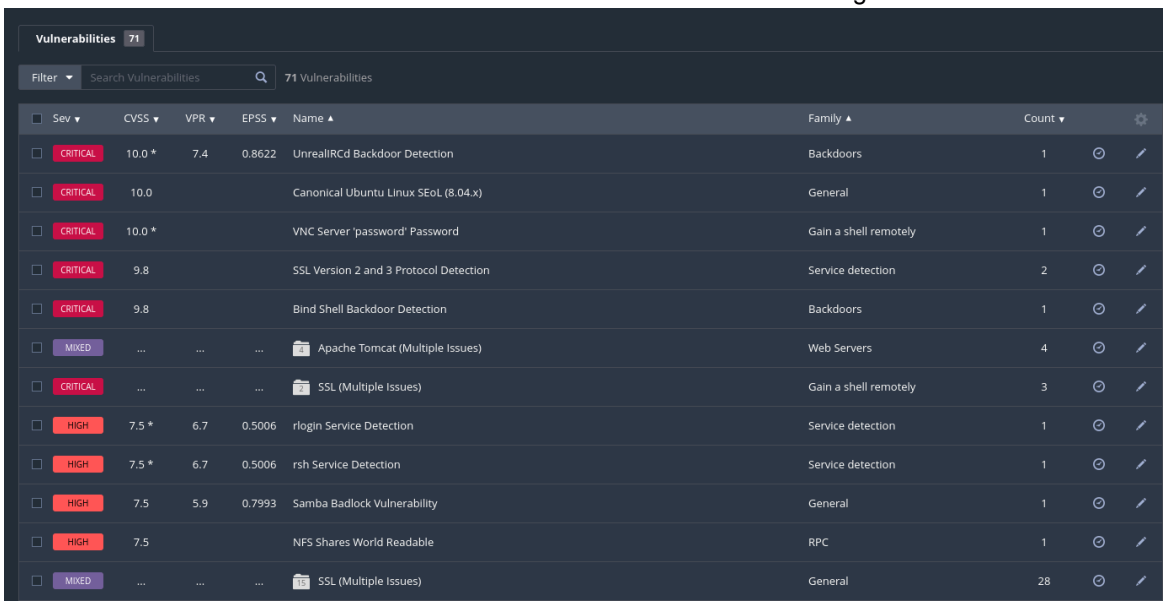
- **Tipo di scansione**: Basic Network Scan
- **Modalità porte**: Port scan (common ports)

Esecuzione della Scansione

Una volta configurata correttamente la scansione, è stata avviata tramite il pulsante Launch in Nessus. Durante l'esecuzione, è stato possibile osservare in tempo reale le vulnerabilità identificate, con relativi dettagli e link per approfondimenti.

Risultati della Scansione

La scansione ha identificato un totale di **71 vulnerabilità** distribuite come segue:



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.8622	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	SSL (Multiple Issues)	General	28

(Le 71 vulnerabilità scansionate)

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.8622	UnrealIRCd Backdoor Detection	Backdoors	1
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1

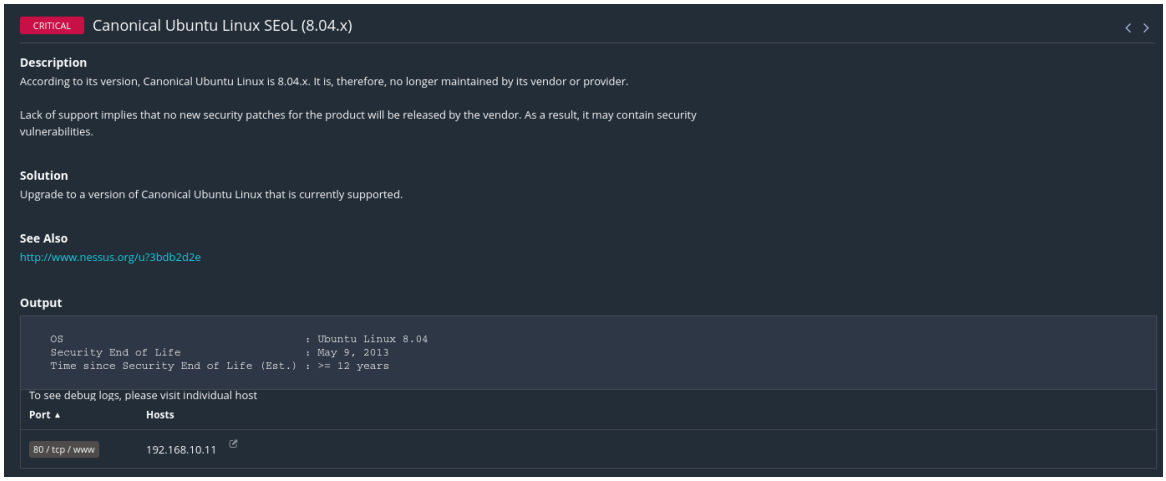
(Vulnerabilità riordinate per Vulnerability Priority Rating)

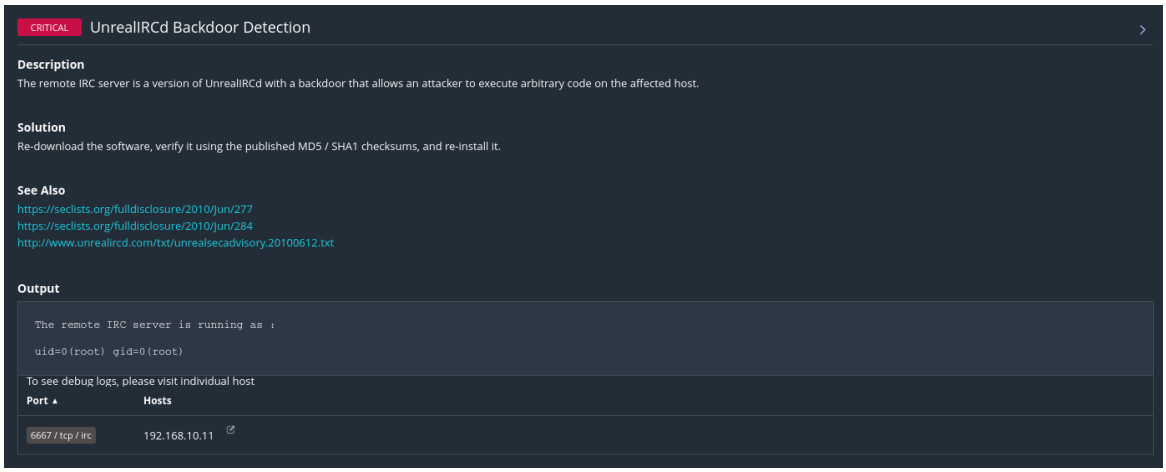
Livello di Severità	**Numero di Vulnerabilità**
Critical	11
High	7
Medium	23
Low	7
Info	137
Totale	**185**

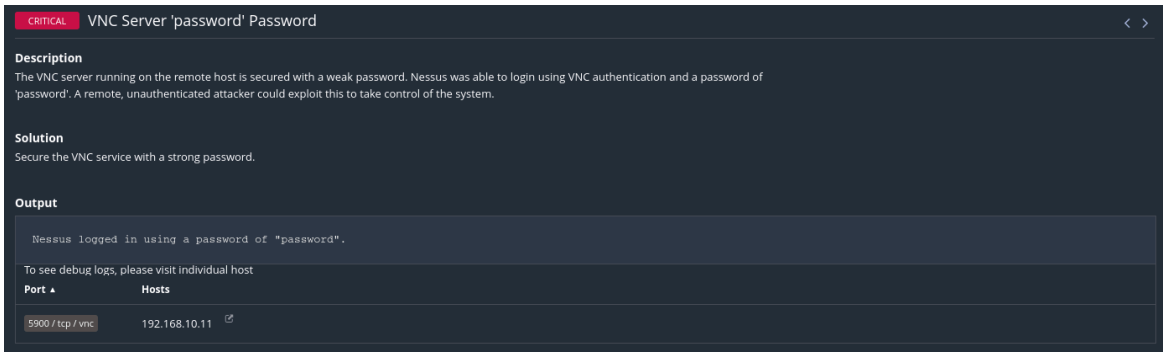
(Distribuzione delle vulnerabilità per livello di severità)

Il report Nessus ha presentato una chiara classificazione delle vulnerabilità dalla più critica alla meno critica, con indicazione della famiglia di appartenenza (backdoor, web server, servizi, etc.).

Vulnerabilità Critiche Identificate







Analisi del Report

Nessus ha consentito di generare un report dettagliato e professionale in formato PDF con le seguenti caratteristiche:

- Riepilogo delle vulnerabilità per host

- Classificazione per livello di severità (Critical, High, Medium, Low, Info)
- Score CVSS per ogni vulnerabilità
- Descrizione dettagliata di ogni vulnerabilità
- Link e risorse per approfondimenti
- Informazioni sull'host scansionato (indirizzo IP, nome NetBIOS, indirizzo MAC, sistema operativo)
- Timeline della scansione (data/ora inizio, fine, tempo totale)

Conclusioni

L'utilizzo del tool Nessus rappresenta un passaggio fondamentale per chi aspira a lavorare nel campo della cybersecurity. L'esercitazione ha dimostrato come:

1. **L'identificazione delle vulnerabilità** è il primo step indispensabile per la sicurezza di un sistema
2. **La valutazione del rischio** tramite CVSS consente di prioritizzare gli interventi di remediation
3. **L'acquisizione di competenze pratiche** con strumenti come Nessus sviluppa la mentalità analitica necessaria per il lavoro nel settore
4. **L'interpretazione dei risultati** è critica per implementare soluzioni di sicurezza efficaci

I risultati evidenziano che il sistema Metasploitable contiene numerose vulnerabilità critiche, molte delle quali sono dovute all'utilizzo di versioni obsolete e non supportate di software fondamentale (OpenSSH, PHP, Apache, Samba). L'aggiornamento di questi componenti e l'implementazione delle soluzioni proposte rappresenterebbero un miglioramento significativo della postura di sicurezza del sistema.