

EPICODE-CS0124

S5/L4 - Pratica

Flaviano Sedici

Pratica

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).

A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono:

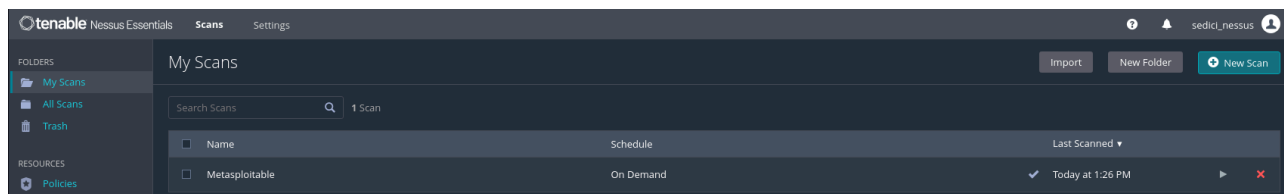
Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.

Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

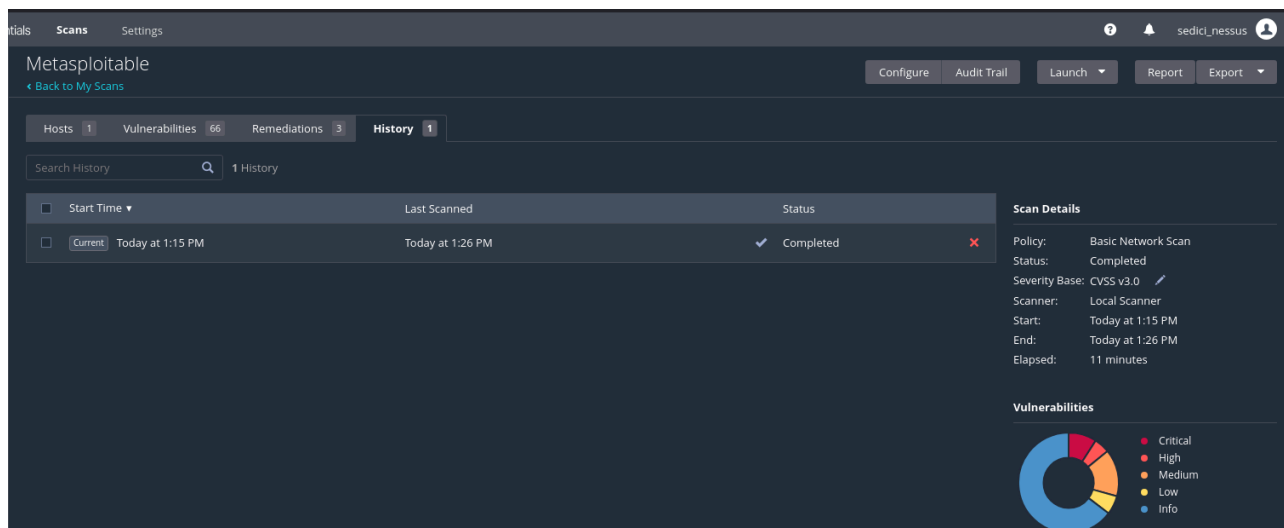
1. Configurazione Nessus scan su Metasploitable

Per configurare la scansione delle vulnerabilità di Metasploitable, con IP 192.168.60.101, sono state utilizzate le impostazioni di default con la funzionalità «basic network scan».

La scansione ha richiesto circa 11 minuti.



Riepilogo Scan



Tempistiche di Scan

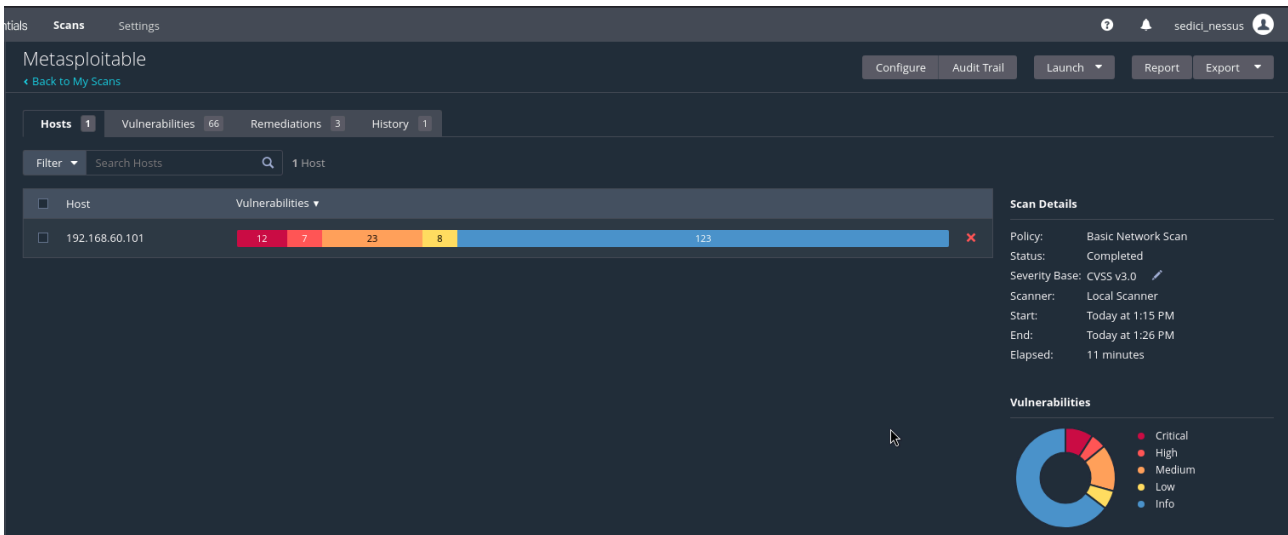
2. Risultati dell'analisi

L'analisi ha rilevato 12 vulnerabilità critiche tra cui ad esempio:

2 backdoors

2 possibili accessi da shell remota

2 sui web servers



Risultati generali della scansione

The screenshot shows the Metasploitable interface with the 'Vulnerabilities' tab active. It displays a detailed list of 66 vulnerabilities. The table includes columns for severity, CVSS, VPR, name, family, and count. A 'Scan Details' panel on the right shows the scan policy, status, and a 'Vulnerabilities' donut chart.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	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	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1
HIGH	7.5		NFS Shares World Readable	RPC	1
MIXED	SSL (Multiple Issues)	General	28
MIXED	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2

Dettaglio dei risultati di scansione

Metasploitable

Back to My Scans

Configure

Audit Trail

Launch

Report

Export

Hosts1

Vulnerabilities66

Remediations3

History1

Search Actions

3 Actions

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 1:15 PM

End:

Today at 1:26 PM

Elapsed:

11 minutes

Dettaglio delle possibili remediations

Nessus restituisce anche dei possibili consigli sulle remediations di alcune vulnerabilità.