

Amedeo Natalizi

PROGETTO S5/L5

Scansione iniziale delle vulnerabilità

TRACCIA

EFFETTUARE UNA SCANSIONE COMPLETA SUL TARGET METASPLOITABLE.

SCEGLIETE DA UN MINIMO DI 2 FINO AD UN MASSIMO DI 4 VULNERABILITÀ CRITICHE / HIGH E PROVATE AD IMPLEMENTARE DELLE AZIONI DI RIMEDIO.

N.B. LE AZIONI DI RIMEDIO, IN QUESTA FASE, POTREBBERO ANCHE ESSERE DELLE REGOLE FIREWALL BEN CONFIGURATE IN MODO DA LIMITARE EVENTUALMENTE LE ESPOSIZIONI DEI SERVIZI VULNERABILI. VI CONSIGLIAMO TUTTAVIA DI UTILIZZARE MAGARI QUESTO APPROCCIO PER NON PIÙ DI UNA VULNERABILITÀ.

PER DIMOSTRARE L'EFFICACIA DELLE AZIONI DI RIMEDIO, ESEGUITE NUOVAMENTE LA SCANSIONE SUL TARGET E CONFRONTATE I RISULTATI CON QUELLI PRECEDENTEMENTE OTTENUTI.

COME HO AGITO

UNA VOLTA CONFIGURATO NESSUS, HO FATTO PARTIRE UNA SCANSIONE PER LA RICERCA DELLE VULNERABILITÀ ALL'INDIRIZZO DI METASPLOITABLE. IL RISULTATO DELLA SCANSIONE HA RIPORTATO NUMEROSE CRITICITÀ SULLE QUALI POI HO LAVORATO PER TENTARE DI RISOLVERLE.

RISULTATO SCANSIONE INIZIALE

meta

[Back to All Scans](#)

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities65Remediations2Notes2History1

FilterSearch Vulnerabilities65 Vulnerabilities

<input type="checkbox"/>	Sev▼	CVSS▼	VPR▼	Name▲	Family▲	Count▼	
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	28	
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5	

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:43 AM
End: Today at 12:11 PM
Elapsed: 28 minutes

Vulnerabilities

Critical

High

Medium

Low

Info