



consegna S5-L4

vulnerability scan via Nessus

l'esercizio di oggi richiedeva di utilizzare il tool Nessus su kali per effettuare un vulnerability test su metasploitable, una volta avviato il servizio ed eseguito uno scan possiamo notare che le vulnerabilità sono tante ed alcune critiche

metasploit

[Back to My Scans](#)

ConfigureAudit TrailLaunchReportExport

Hosts 1Vulnerabilities 65Remediations 2Notes 2History 1

FilterSearch Vulnerabilities65 Vulnerabilities

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		
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2		

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:27 AM
End: Today at 11:55 AM
Elapsed: 28 minutes

Vulnerabilities

Critical

High

Medium

Low

Info