

S5L5

LA TRACCIA DI OGGI CONSISTEVA NEL INDIVIDUARE E CORREGGERE SULLA
NOSTRA VIRTUAL BOX MACHINE SU METASPLOITABLE LE VULNERABILITA' E
CORREGGERE NE HO SCELTE 4

The screenshot displays the Metasploit interface with a table of scan results. Four vulnerabilities are highlighted with blue boxes. To the right, the 'Scan Details' and 'Vulnerabilities' sections are visible.

Sev	CVSS	VPR	Name	Family	Count		
CRITICAL	10.0 *	5.9	NFS Exported S...	RPC	1	🔄	✎
CRITICAL	10.0		Unix Operating ...	General	1	🔄	✎
CRITICAL	10.0 *		VNC Server 'pas...	Gain a shell remotely	1	🔄	✎
CRITICAL	9.8		SSL Version 2 a...	Service detection	2	🔄	✎
CRITICAL	9.8	9.0	Apache Tomcat ...	Web Servers	1	🔄	✎
CRITICAL	9.8		Bind Shell Back...	Backdoors	1	🔄	✎
CRITICAL	SSL (Multip...	Gain a shell remotely	3	🔄	✎
HIGH	7.5		NFS Shares Wor...	RPC	1	🔄	✎
HIGH	7.5	6.7	Samba Badlock ...	General	1	🔄	✎

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0 ✎
Scanner: Local Scanner
Start: Today at 4:43 PM
End: Today at 5:12 PM
Elapsed: 29 minutes

Vulnerabilities

Legend: Critical, High, Medium, Low, Info