

An abstract graphic on the left side of the slide. It features a dark purple background with various colorful geometric shapes, including circles, ovals, and elongated rectangles in shades of blue, orange, red, green, and yellow. Some shapes are solid, while others are outlined or have a slight transparency effect. The shapes are arranged in a dynamic, overlapping pattern that suggests movement and modern design.

Consegna S5-L4

Utilizzo di Nessus

TRACCIA

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:

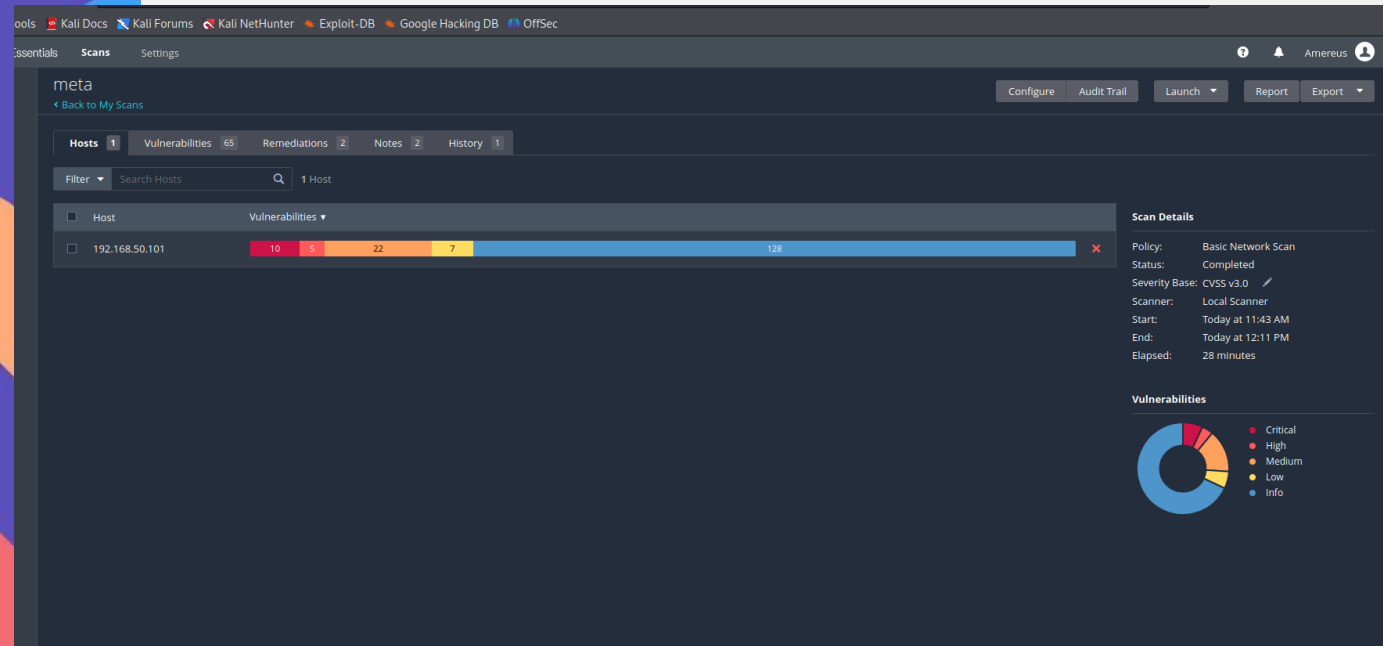
**Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni
Familiarizzare con alcune delle vulnerabilità note che troverete spesso.**

Come ho agito

Dopo aver installato e configurato correttamente la versione di Nessus Essentials ho messo sulla stessa rete interna sia il mio kali che meta. Da Nessus ho fatto partire la scannerizzazione dell'indirizzo di meta e ho riscontrato diverse vulnerabilità

Esiti

Da come si può notare la scannerizzazione ha portato a diverse vulnerabilità anche critiche le quali riportavano tutte le informazioni disponibili una volta selezionate



The screenshot shows the MetaScan web interface with the 'Vulnerabilities' tab selected. It displays a table of 65 vulnerabilities. The table includes columns for severity, CVSS score, VPR, name, family, and count. A 'Scan Details' panel is visible on the right side of the interface.

Sev	CVSS	VPR	Name	Family	Count
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	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	SSL (Multiple Issues)	General	28
MIXED	ISC Bind (Multiple Issues)	DNS	5

Scan Details

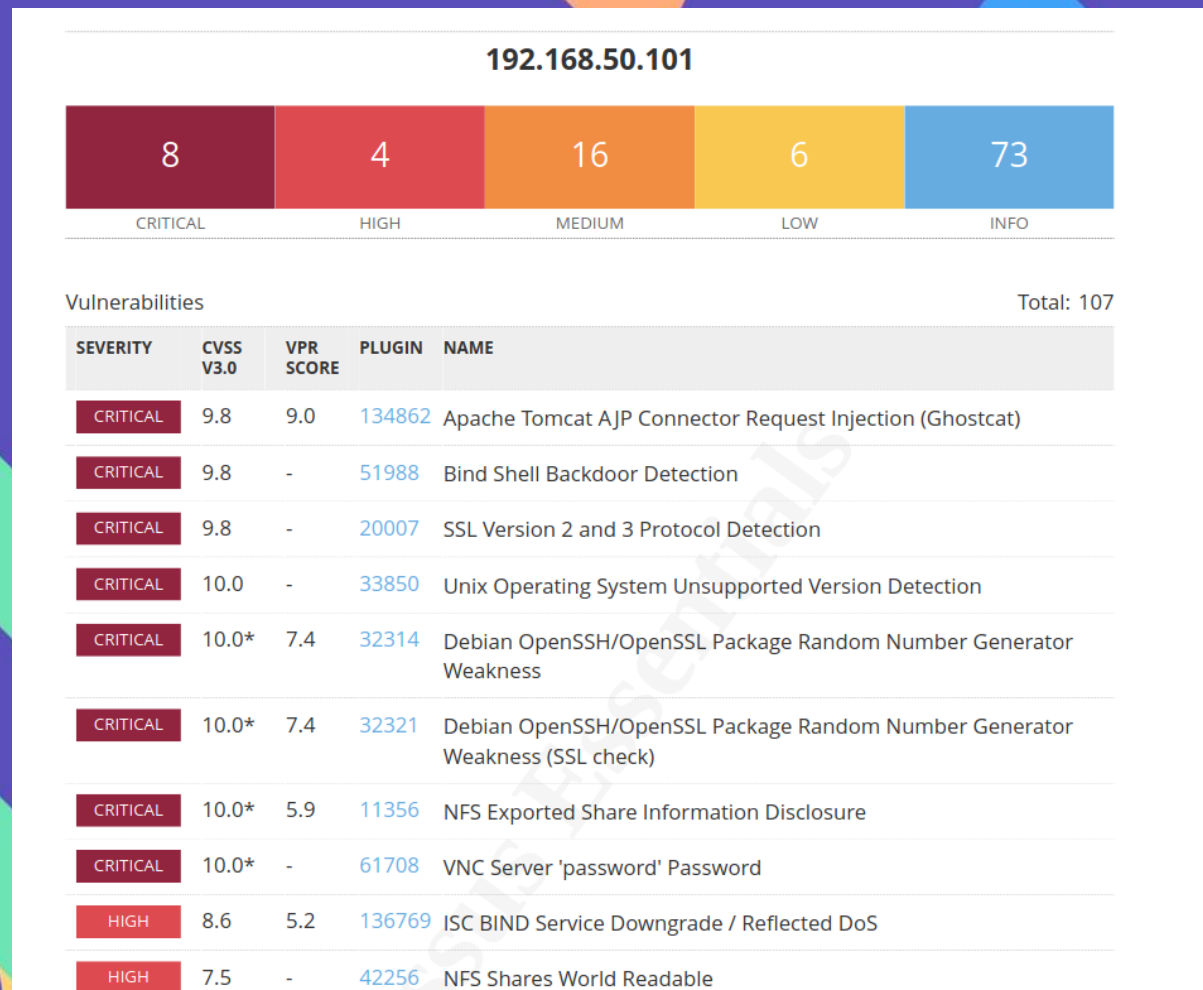
- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 11:43 AM
- End: Today at 12:11 PM
- Elapsed: 28 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Report

Nessus ci permette di stampare il report di tutte le vulnerabilità e ci suggerisce anche eventuali soluzioni a determinate vulnerabilità



Amedeo
Natalizi



FINE

