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:

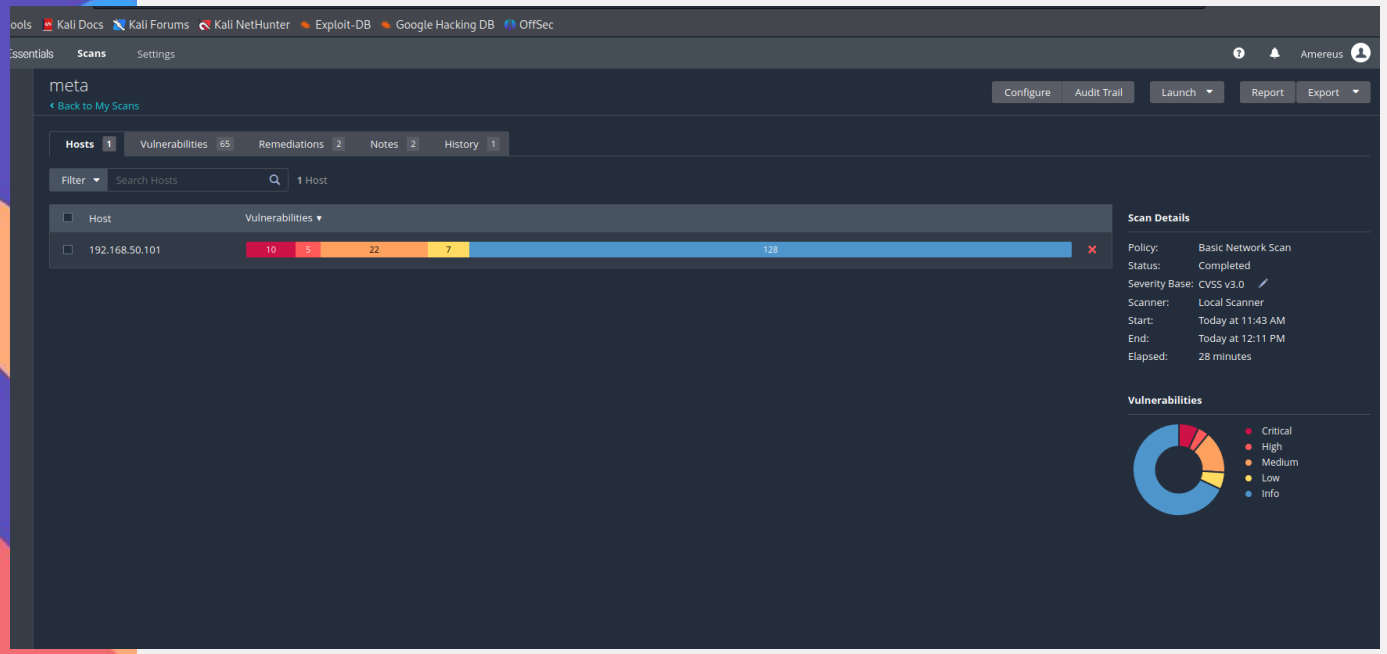
Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni
Familiarizzare con alcune delle vulnerabilità note che troverete spesso.

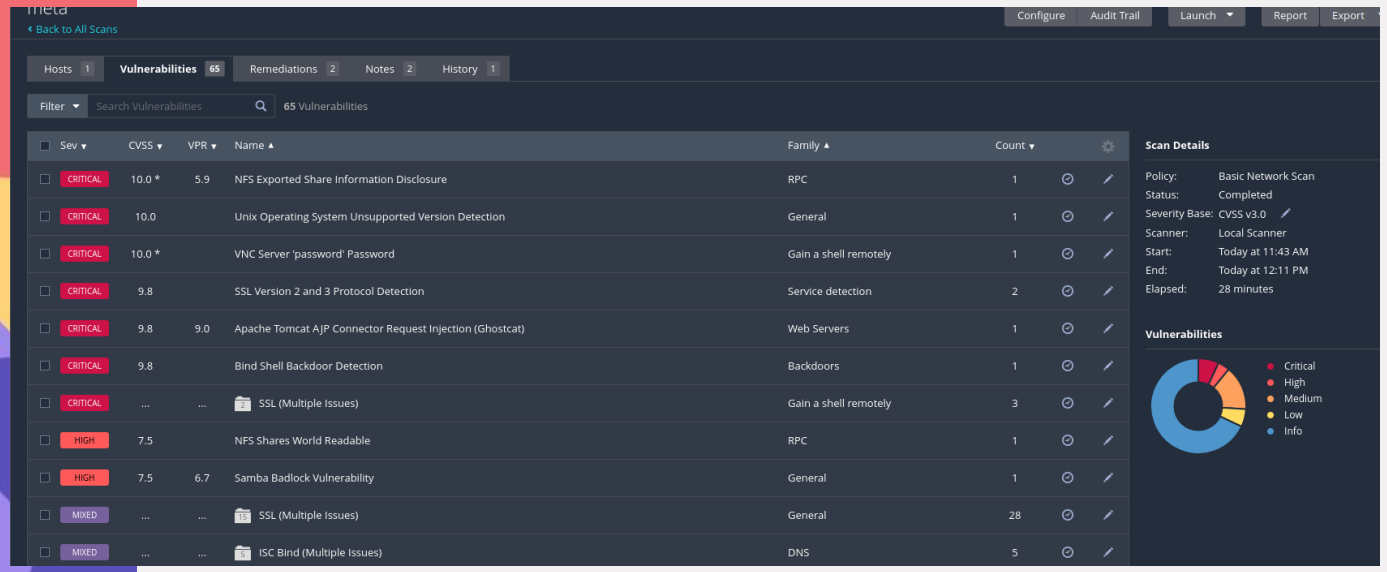
Come ho agito

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

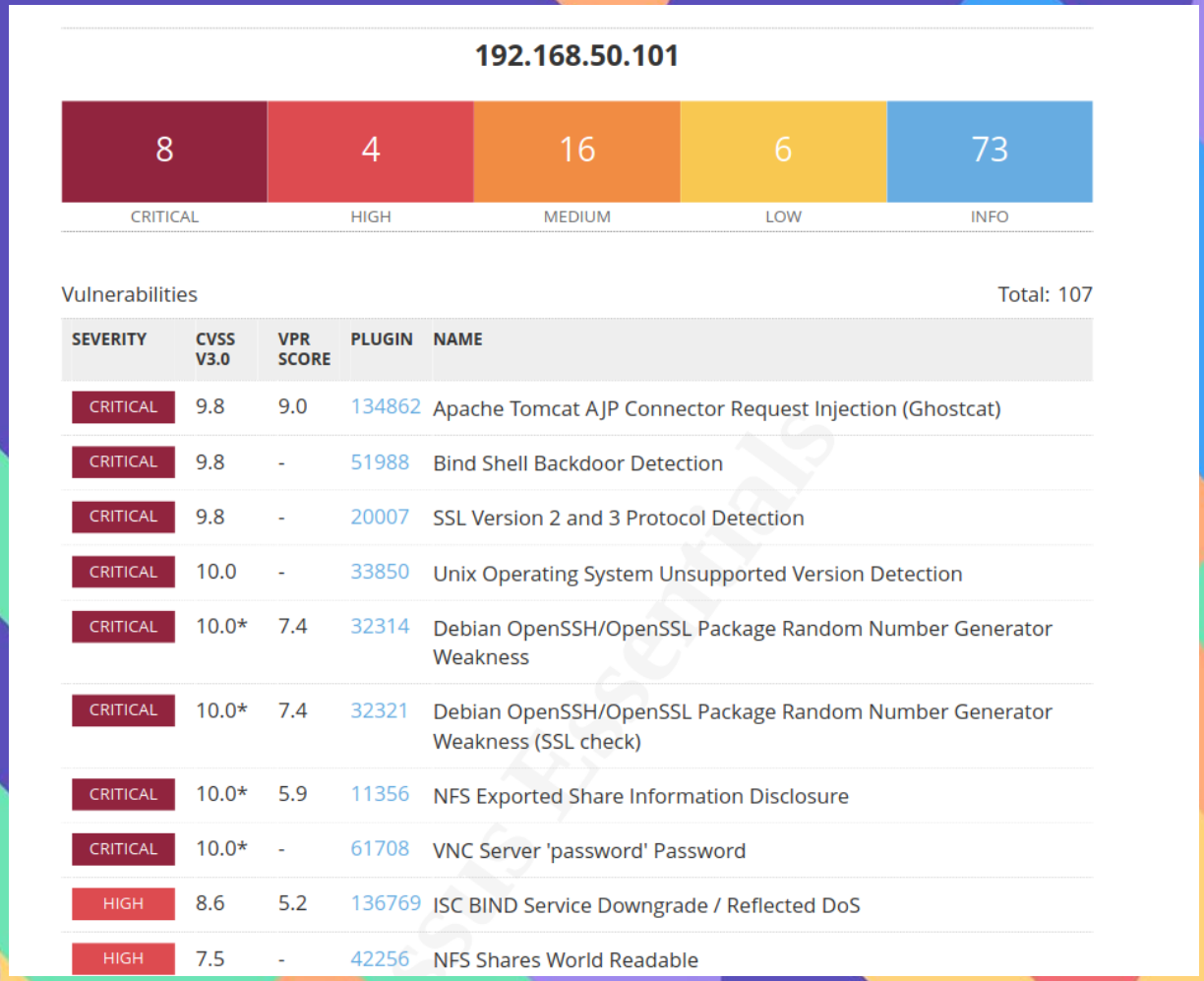
Da come si può notare la scannerizzazione ha portato a diverse vulnerabilità anche critiche le quali riportavano tutte le informazioni disponibili una volta selezionate





Report

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



192.168.50.101

8	4	16	6	73
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 107

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable

Amedeo Natalizi

FINE