

VULNERABILITY ASSESSMENT

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.

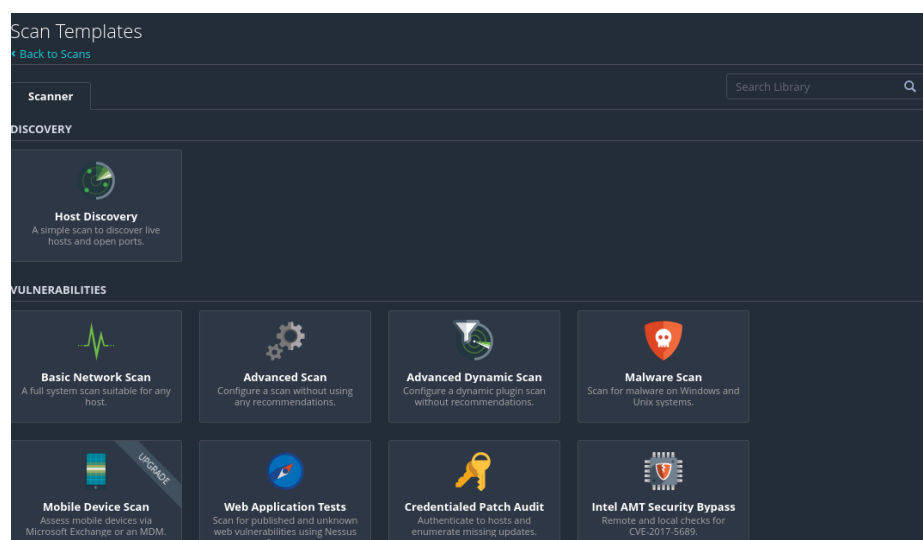
Gli obiettivi dell'esercizio sono:

- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

Nessus è un vulnerability scanner molto potente che ci offre una vasta gamma di funzionalità come scansioni automatiche, valutazioni della vulnerabilità e generazione di report.

I vscanner usano dei database per confrontare ciò che trovano con quello presente nei database che contengono informazioni sulle vulnerabilità note e così facendo possiamo rilevare quelle note. Utilizzare i database noti ci permette di essere sicuri al 100% che le vulnerabilità conosciute possano essere fixate.

Iniziamo con il configurare una basic scan sulla macchina metasploitable.



Useremo la basic network scan per lo scopo di questo esercizio: una scansione di base con tanti parametri e policy preimpostate, così da facilitare l'uso del software. Con questa scansione andremo a scansionare le porte che offrono i servizi più comuni sulla macchina target.

New Scan / Basic Network Scan
[← Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC

- General
 - Name: Metasploitable
 - Description: Virtual machine running linux 2.6
 - Folder: My Scans
 - Targets: 192.168.50.101
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Upload Targets [Add File](#)

[Save](#) [Cancel](#)

In questa schermata inseriremo il nome che vogliamo dare alla scan, una descrizione, dove salvarla e infine nella sezione target inseriremo gli indirizzi IP del target che vogliamo scansionare. Possiamo inserire IP singoli, un range di IP o un network intero.

New Scan / Basic Network Scan
[← Back to Scan Templates](#)

Settings | Credentials | Plugins

DISCOVERY

Scan Type: Port scan (common ports)

General Settings:

- Always test the local Nessus host
- Use fast network discovery

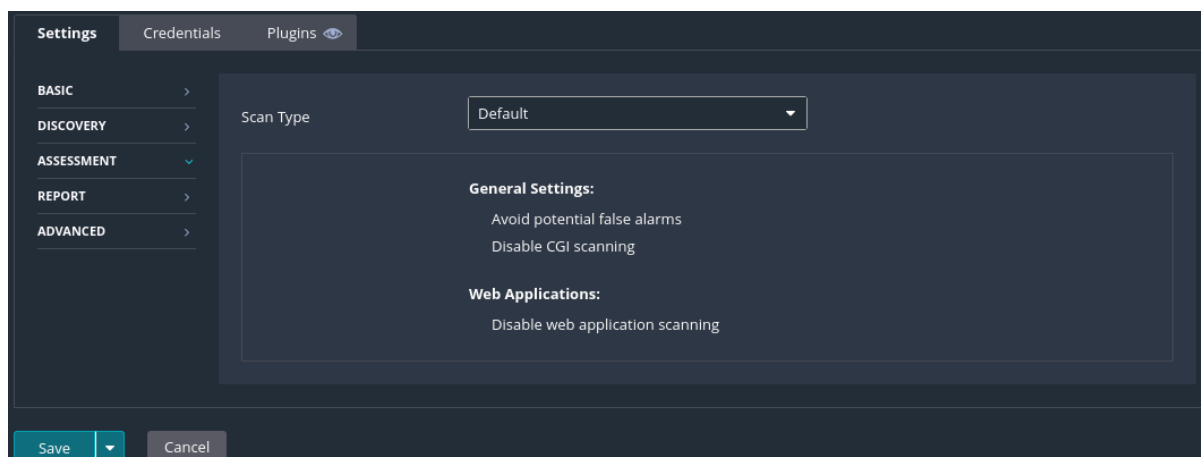
Port Scanner Settings:

- Scan common ports
- Use netstat if credentials are provided
- Use SYN scanner if necessary

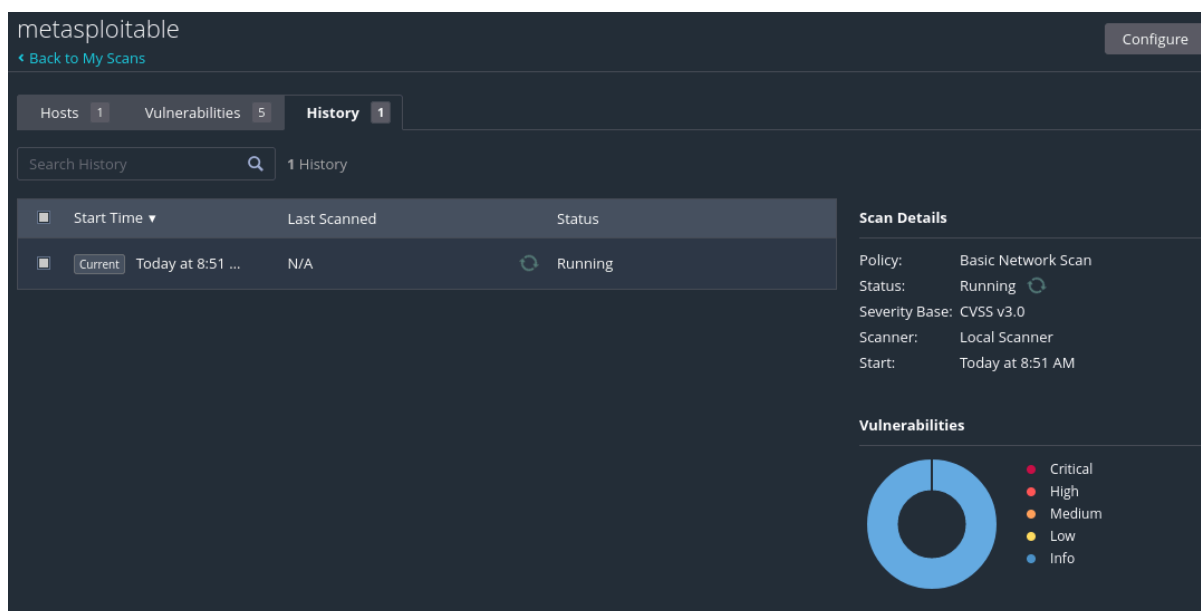
Ping hosts using:

- TCP
- ARP
- ICMP (2 retries)

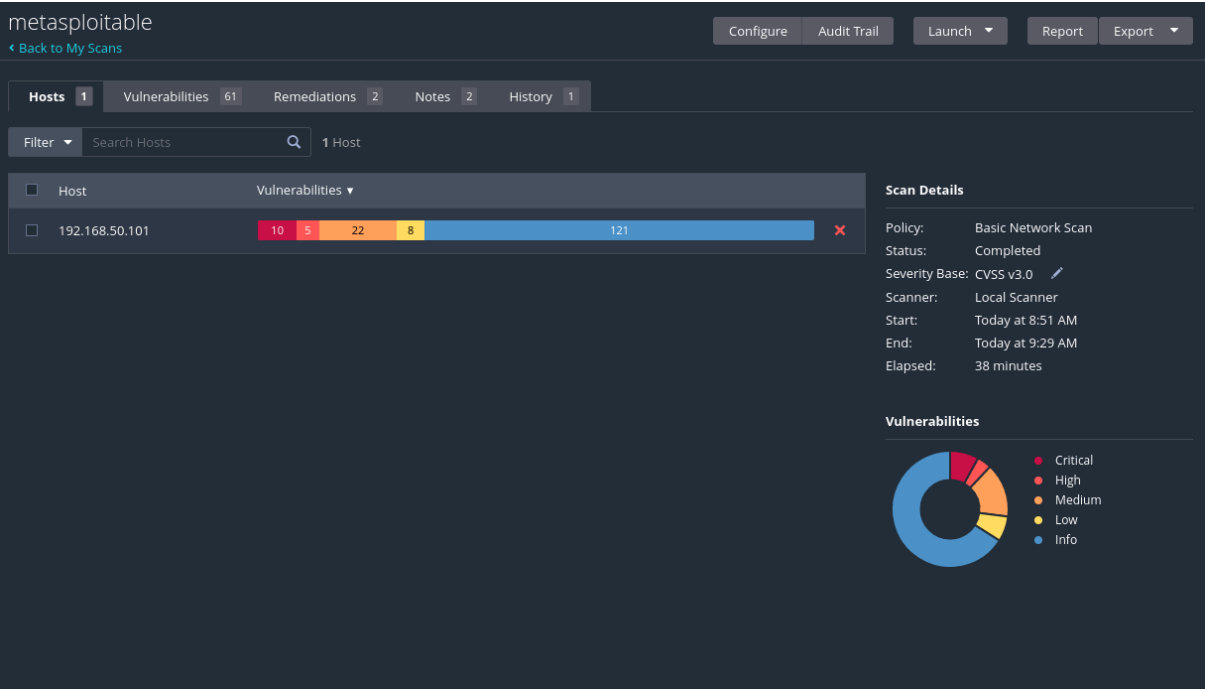
Nella sezione discovery, andremo ad impostare il tipo di scan, in questo caso faremo una scan per le porte comuni. Possiamo anche vedere le impostazioni generali, quelle dello scanning delle porte e quali protocolli verranno usati per pingare gli host. Per questo esercizio useremo lo scan type Port scan (common ports) che è già configurato per la scansione delle porte comuni ma se aprissimo la tendina, potremmo scegliere altri tipi di scan già preimpostate o crearne una che soddisfi i nostri parametri personalizzati.



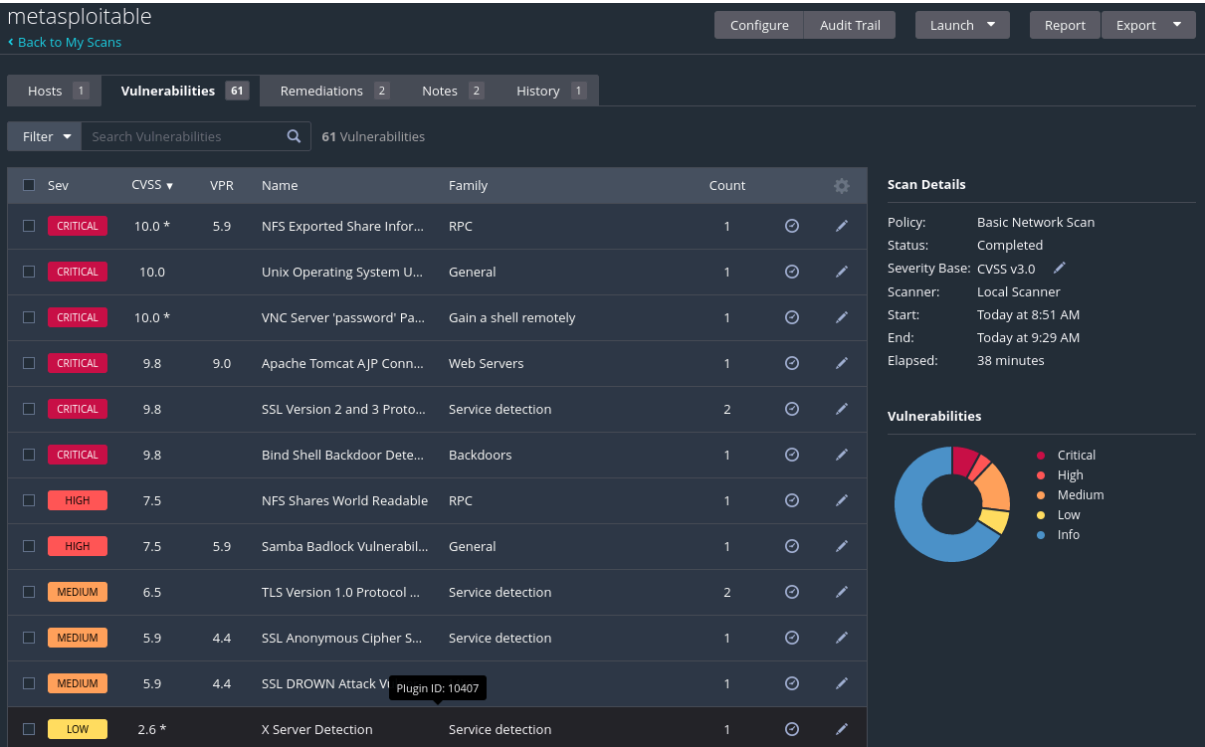
Nella sezione di assesment, imposteremo l'assessment di default ai fini dell'esercizio, ma ricordiamoci che possiamo modificare i parametri. Lascieremo anche gli altri parametri di default in questo caso.




Come si può vedere, Nessus ha iniziato la scannerizzazione della macchina target. In basso a destra, nel grafico, verranno indicate le vulnerabilità note scannerizzate e trovate nei database di riferimento in tempo reale. Queste vulnerabilità verranno già classificate con il Common Vulnerabilities Scoring System (CVSS) così che ad ogni vulnerabilità venga associato un livello di rischio tra Critical, High, Medium, Low, Info.



Finita la scansione, sarà possibile vedere tutte le vulnerabilità note trovate dal programma.



Nessus ci indicherà anche dei rimedi possibili per le vulnerabilità che ha trovato nella tab remediations.

Hosts	1	Vulnerabilities	61	Remediations	2	Notes	2	History	1
Search Actions  2 Actions									
Action	Vulns ▼		Hosts						
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3		1						
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	0		1						

Sarà anche possibile generare un report che mette in evidenza tutte le vulnerabilità note riscontrate, sia per quanto riguarda la versione del servizio, sia per quanto riguarda la porta su cui si trova il servizio stesso. E' possibile scaricare il report in vari formati tra cui PDF.

Alcune delle vulnerabilità più critiche individuate sono:

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*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	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
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability

Bind Shell Backdoor è una vulnerabilità che utilizza una Bash shell collegata (bind) alla porta in questione, quindi poi accessibile con un tool come netcat o telnet. Eseguirà tutti i comandi inviati tramite bash su quella porta. NFS Exported Share Information Disclosure è una vulnerabilità che permette di connettersi in remoto al Network File Sahring della macchina e quindi avere accesso ai dati in essa contenuta. Il VNC Server 'password' Password sta ad indicare che la password del Virtual Network Computing non è abbastanza affidabile e che va modificata. Apache Tomcat AJP Connector Request Injection (Ghostcat) è una vulnerabilità del protocollo AJP Connector, che non è sicuro e può dare accesso di esecuzione di codice da remoto ad un attaccante.

Samba Badlock Vulnerability è una vulnerabilità del servizio SMB che è principalmente utilizzato per lo scambio di file per esempio con dispositivi come stampanti.