

Report Scan delle porte usando Nessus Essential - S5-L3

Introduzione

Nell'esercitazione odierna, andremo a scansionare alcune **porte comuni**, usando il tool *Nessus* installato sulla *Kali*.

Le porte comuni che andremo ad analizzare sono le seguenti:

- `range ports 21-25`
- `port 80`
- `port 110`
- `port 139`
- `port 443`
- `port 445`
- `port 3389`

Prima di iniziare a fare la scansione, dobbiamo scegliere un target su cui effettuare il test. In questo caso scegliamo la macchina *Metasploitable*, sempre installata sulla *Virtualbox*.

Passo primo

Data l'introduzione, dobbiamo procedere con la scansione delle porte.

Prima di entrare nel vivo della questione, dobbiamo innanzitutto trovare l'indirizzo IP della macchina *Metasploitable*.

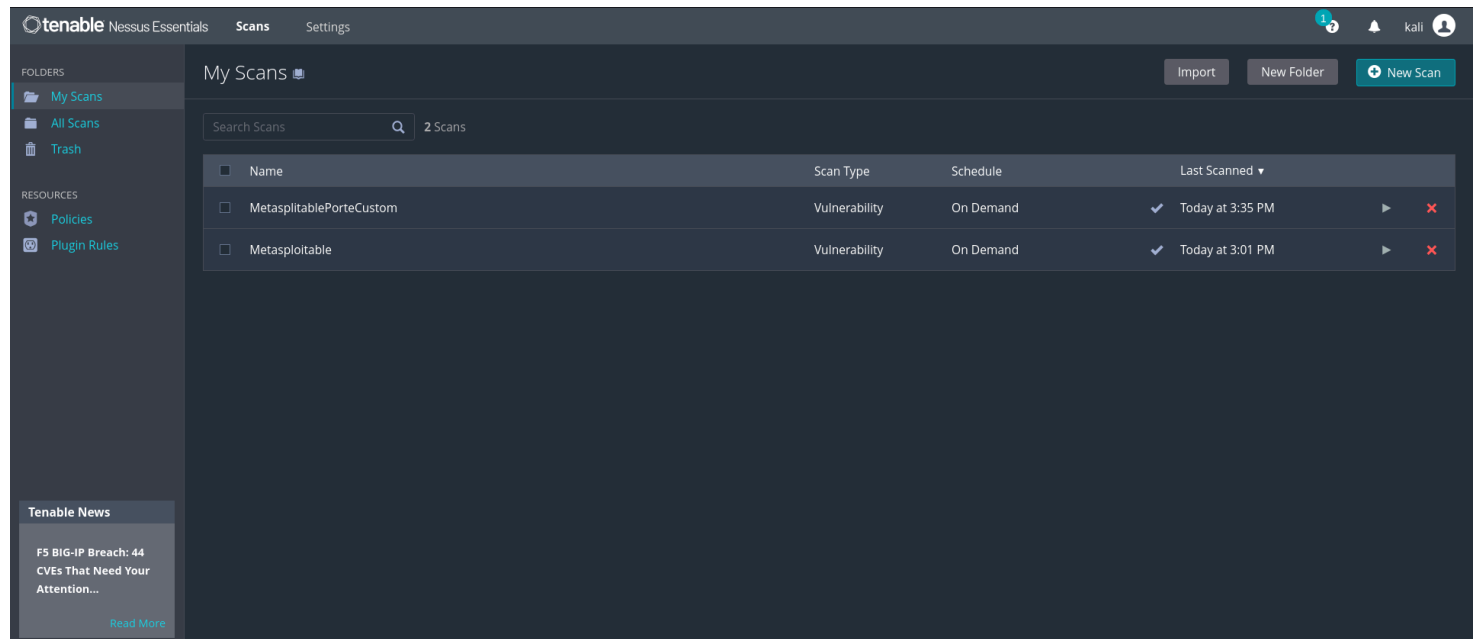
Questo lo possiamo fare in diversi modi:

- Avviando direttamente la macchina *Metasploitable* e con il comando `ifconfig -a` risaliamo all'indirizzo IP della macchina (nel mio caso `192.168.50.5`);
- Su Kali Linux, usando **nmap** da terminale: con il comando `sudo nmap -sn 192.168.50.0/24` possiamo vedere elencati gli host vivi con gli indirizzi IP;
- Andando sulle impostazioni di rete della *Virtualbox* e vedere l'indirizzo IP tramite una GUI.

Io ho usato i primi due metodi contemporaneamente, in tal modo da essere sicura che l'indirizzo IP della *Metasploitable* fosse davvero `192.168.50.5`.

Secondo passo

Una volta individuato l'indirizzo IP della Metasploitable, andremo ad usare Nessus per fare la scansione delle porte.



L'immagine sopra ci mostra la pagina principale di Nessus, che si presenta pulita e semplice da usare.

- sulla sezione **My Scans** troviamo tutte le scansioni che abbiamo eseguito (o che eseguiremo – dipende se abbiamo messo una schedule per l'avvio della scansione).
- in alto a destra possiamo:
 - aggiungere una nuova cartella in cui inserire le scansioni
 - creare una nuova scansione
 - importare una scansione

Cliccando su una scansione, ci si aprirà una finestra in cui vedremo i dettagli della scansione, come nell'immagine sottostante:

tenable Nessus Essentials Scans Settings

MetasploitablePorteCustom
← Back to My Scans

Configure Audit Trail Launch Report Export

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules

Tenable News
Tenable Discovers Critical Vulnerabilities in Simp...
[Read More](#)

Hosts 1 Vulnerabilities 65 Remediations 3 History 1

Filter Search Hosts 1 Host

Host	Auth	Vulnerabilities
192.168.50.5	Fail	9 7 23 9 102

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:26 PM
End: Today at 3:35 PM
Elapsed: 9 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Cosa vediamo?

- vediamo l'indirizzo IP del target che abbiamo scelto per la scansione (192.168.50.5 nel mio caso)
- vediamo le vulnerabilità che sono state rilevate dall'applicativo
- a destra vediamo i dettagli della scansione e il diagramma a torta

Come facciamo ad arrivare fino a qui? Partiamo a fare una nuova scansione, cliccando sul button "**New Scan**".

Si aprirà la seguente schermata:

tenable Nessus Essentials Scans Settings

Scan Templates
← Back to Scans

Scanner Search Library

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Nessus 10.8.0 / 10.8.1 Agent Reset
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Find AI
AI, LLM, ML related detections and vulnerabilities.

Eseguiamo una *Basic Network Scan* in questo caso (se non si vogliono suggerimenti e impostazioni predefinite, scegliere Advanced Scan).

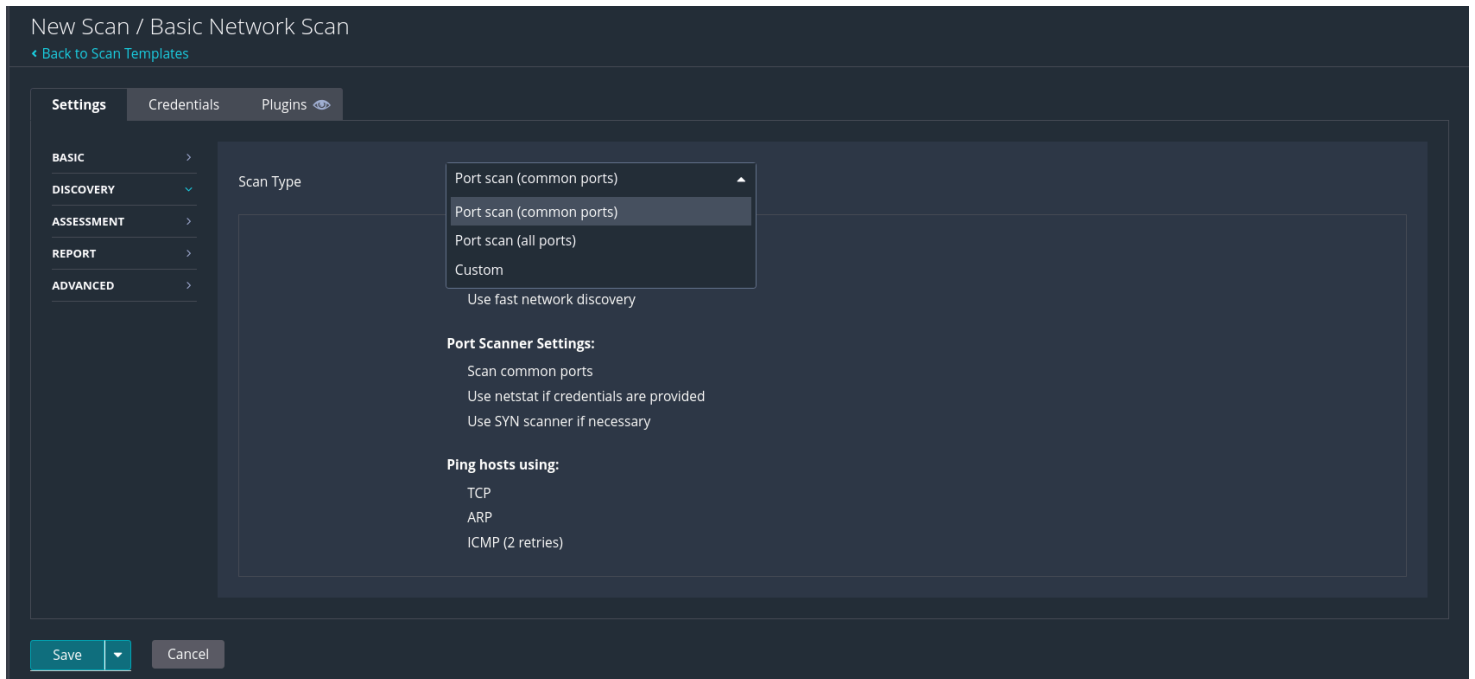
Dopodiché si avvierà una pagina in cui ci chiederà di inserire:

- nome
- descrizione (facoltativa)
- cartella di destinazione
- target (indirizzo IP del target)

The screenshot shows the 'New Scan / Basic Network Scan' configuration page in the Tenable Nessus Essentials interface. The page is divided into a left sidebar and a main content area. The sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules). The main content area has tabs for 'Settings', 'Credentials', and 'Plugins'. Under the 'Settings' tab, there is a 'BASIC' section with a dropdown menu showing 'General' (selected), 'Schedule', and 'Notifications'. Below this are sections for 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'General' settings include: 'Name' (required), 'Description', 'Folder' (set to 'My Scans'), and 'Targets' (required, with an example: '192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'). There is also an 'Upload Targets' button and an 'Add File' link. At the bottom, there are 'Save' and 'Cancel' buttons.

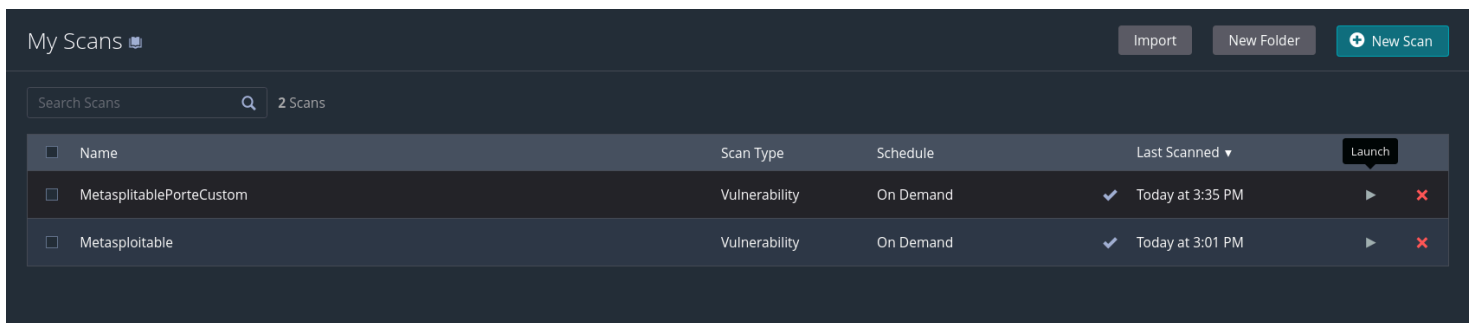
Se andiamo nella sezione Discovery possiamo scegliere il tipo di scansione:

- **port scan (common ports)** → per scegliere lo scan delle porte comuni
- **port scan (all ports)** → per scegliere lo scan di tutte le porte
- **custom** → per scegliere le porte che si vogliono analizzare in autonomia



Una volta settato il tutto facciamo click su **save** e si creerà la scansione che vedremo poi nella pagina iniziale.

Se tutto corrisponde, facciamo click su **Launch** e si avvierà in automatica la scansione.



Per effettuare la scansione, potrebbe volerci un po' di tempo, soprattutto a seconda di quante porte si sono scelte per essere analizzate.

Terzo passo

La scansione è terminata. E ora?

Una volta terminata la scansione, guardiamo un po' quello che ci viene proposto:

MetaspitablePorteCustom

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 65 Remediations 3 History 1

Filter Search Vulnerabilities 65 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
CRITICAL	10.0 *	7.4	0.868	UnrealIRCd Backdoor Detection	Backdoors	1	
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1	
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	
CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Inje...	Web Servers	1	
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1	
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1	
HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1	
HIGH	7.5			NFS Shares World Readable	RPC	1	

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:26 PM
End: Today at 3:35 PM
Elapsed: 9 minutes

Vulnerabilities

Come possiamo vedere dalle immagini, ci viene proposta una lista di vulnerabilità che vengono classificate dalla più critica alla meno critica.

Per ognuna troviamo anche la *family* di vulnerabilità (se è una backdoor, un web server etc.).

Come possiamo vedere, la lista che ci viene proposta è molto dettagliata e chiara.

Per ogni vulnerabilità, possiamo vederne i dettagli, basta cliccarci sopra, come possiamo vedere nella seguente figura:

MetaspitablePorteCustom / Plugin #46882

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 65 Remediations 3 History 1

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

```
The remote IRC server is running as :  
uid=0(root) gid=0(root)
```

To see debug logs, please visit individual host

Port	Hosts
6667 / tcp	192.168.50.5

Plugin Details

Severity: Critical
ID: 46882
Version: 1.16
Type: remote
Family: Backdoors
Published: June 14, 2010
Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Functional
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 7.4

Abbiamo anche diversi link che ci vengono proposti, su cui andare ad approfondire la nostra ricerca.

Cosa facciamo adesso?

Quarto passo

A questo punto siamo pronti a generare un report dettagliato sulla nostra scansione.

Nessus permette appunto di generare un report alla fine di ogni scansione, un report dettagliato e pulito scaricabile in diversi formati (quello consigliato è il formato PDF).

In alto a destra selezioniamo il button "**Report**" e si apre la seguente finestra:

Generate Report - 1 Host Selected

Report Format: ☐ HTML ☒ PDF ☐ CSV ☐ Preferred Format

Select a Report Template:

SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
☒ Include page breaks between vulnerability results

Generate Report Cancel PDF Settings: Save Clear

Scegliamo il tipo di report che vogliamo scaricare, scegliamo il formato e clicchiamo su "**Generate Report**". Aspettiamo qualche secondo e subito dopo verrà avviato il download del file.

Quinto passo

Apriamo il report e vediamo subito come sia ben definito e dettagliato in tutte le sue parti.

Di seguito, un'immagine che rappresenta un'anteprima di uno dei miei report:

192.168.50.5

9	7	23	9	102
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:

Wed Oct 22 09:26:59 2025

End time:

Wed Oct 22 09:35:34 2025

Host Information

Netbios Name:

METASPLOITABLE

IP:

192.168.50.5

MAC Address:

08:00:27:2C:82:94

OS:

Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

Abbiamo sempre la classificazione delle vulnerabilità e tutte le informazioni su ogni tipo di vulnerabilità.

Conclusioni

L'utilizzo del tool **Nessus** rappresenta un passaggio fondamentale per chi aspira a lavorare nel campo della **cybersecurity**. Imparare a eseguire una scansione, interpretare i risultati e comprendere le criticità rilevate significa fare un salto dalla teoria alla pratica, sviluppando quella mentalità analitica indispensabile per individuare e prevenire vulnerabilità reali.

Grazie a Nessus, si acquisisce familiarità con concetti essenziali come l'**enumerazione dei servizi**, l'**analisi delle porte aperte**, la **valutazione del rischio** e la **prioritizzazione delle vulnerabilità**.