

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 sceglio 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.

The screenshot shows the Tenable Nessus Essentials web interface. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans' (selected), 'All Scans', and 'Trash'. Under 'RESOURCES', there are 'Policies' and 'Plugin Rules'. A 'Tenable News' section on the right lists 'F5 BIG-IP Breach: 44 CVEs That Need Your Attention...' with a 'Read More' link. The main area is titled 'My Scans' and shows a table with two rows of scan details:

Name	Scan Type	Schedule	Last Scanned	Action
MetaspitablePorteCustom	Vulnerability	On Demand	✓ Today at 3:35 PM	▶ X
Metasploitable	Vulnerability	On Demand	✓ Today at 3:01 PM	▶ X

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:

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:

Eseguiremo 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 Tenable Nessus Essentials web interface. At the top, there's a navigation bar with 'tenable' logo, 'Nessus Essentials', 'Scans', and 'Settings'. On the left, there's a sidebar with 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules), and a 'Tenable News' section. The main area is titled 'New Scan / Basic Network Scan' with a 'Back to Scan Templates' link. It has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', there are sections for 'BASIC' (General, Schedule, Notifications), 'DISCOVERY' (with a dropdown menu), 'ASSESSMENT' (with a dropdown menu), 'REPORT' (with a dropdown menu), and 'ADVANCED' (with a dropdown menu). The 'GENERAL' tab is selected under 'BASIC'. The 'Targets' field is highlighted with a red box and contains the placeholder 'Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'. Below the targets field are 'Upload Targets' and 'Add File' buttons. At the bottom 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

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings [Credentials](#) [Plugins](#)

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

- Port scan (common ports)
- Port scan (common ports)**
- Port scan (all ports)
- Custom

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)

Save **Cancel**

The screenshot shows the 'Basic Network Scan' configuration page. The 'Scan Type' dropdown is set to 'Port scan (common ports)'. Under 'Port Scanner Settings', it's configured to scan common ports, use netstat if credentials are provided, and use SYN scanner if necessary. For 'Ping hosts using', it's set to TCP. At the bottom are 'Save' and 'Cancel' buttons.

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.

My Scans

[Import](#) [New Folder](#) [+ New Scan](#)

Search Scans

Name	Scan Type	Schedule	Last Scanned ▾	Launch
MetasplicablePorteCustom	Vulnerability	On Demand	Today at 3:35 PM	▶ X
Metasploitable	Vulnerability	On Demand	Today at 3:01 PM	▶ X

The screenshot shows the 'My Scans' interface with two entries: 'MetasplicablePorteCustom' and 'Metasploitable'. Both are listed as 'Vulnerability' scans with 'On Demand' schedules. The last scan times are 'Today at 3:35 PM' and 'Today at 3:01 PM' respectively. There are 'Launch' buttons next to each entry.

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:

MetasploitablePorteCustom

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to My Scans](#)

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

Critical: 100% (Red)
High: 0% (Orange)
Medium: 0% (Yellow)
Low: 0% (Blue)

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 serever 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:

MetasploitablePorteCustom / Plugin #46882

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerabilities](#)

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.

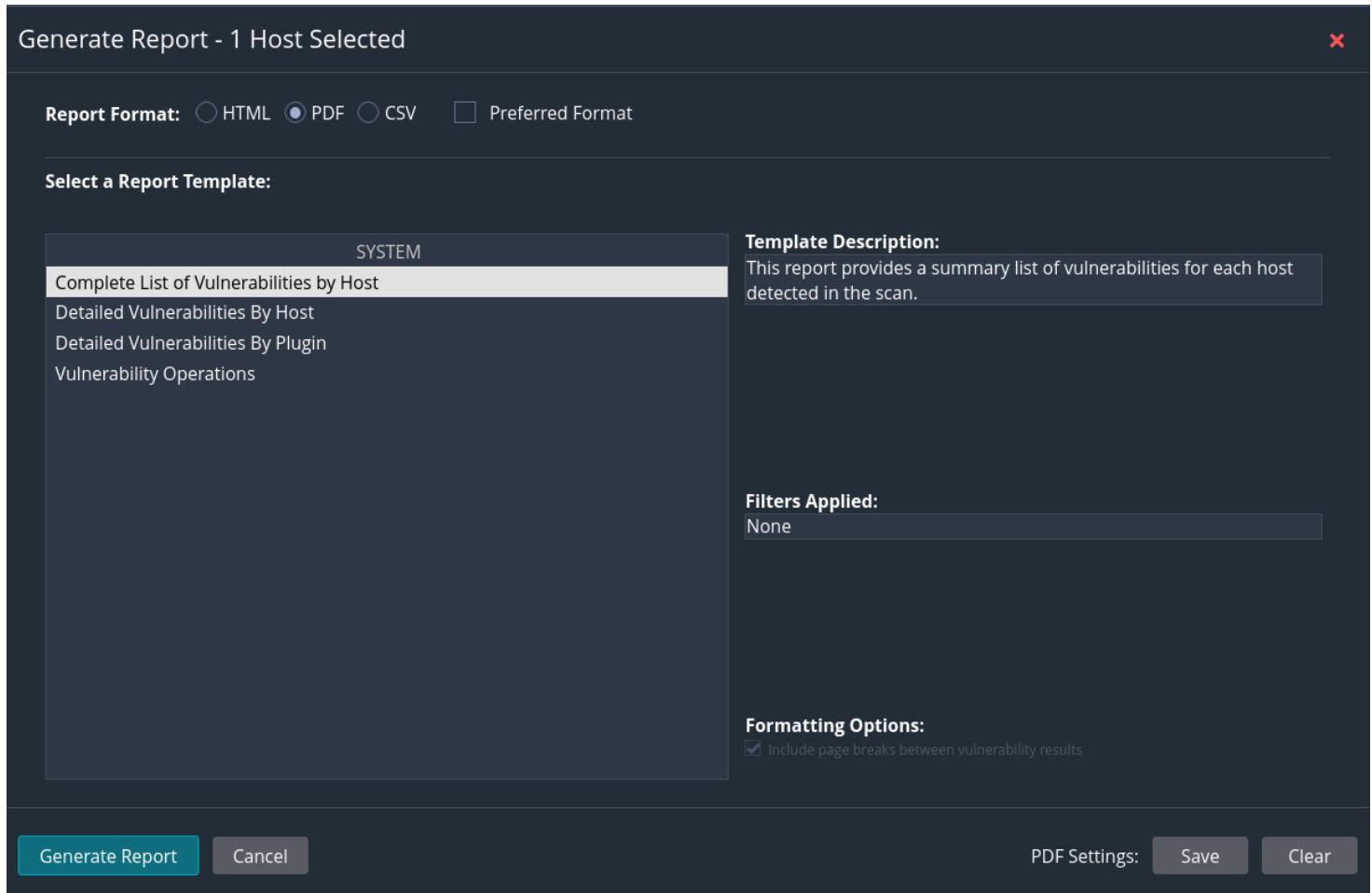
Cosa facciamo adesso?

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:



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



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**.