REPORT TECNICO

VULNERABILITY SCANNING

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 07/01/2026

1. Introduzione

1.1 Obiettivo dell'Attività

Effettuare un **Vulnerability Scanning** su una macchina Metasploitable tramite l'utilizzo di **Nessus** concentrandoci solo sulle porte comuni (21, 22, 23, 25, 80, 110, 139, 443, 445, 3389) ed analizzarne i risultati.

1.2 Scopo

I traguardi da raggiungere sono i seguenti:

- Imparare a configurare e avviare scansioni con Nessus;
- capire come limitare la scansione a porte specifiche;
- apprendere come analizzare i risultati ottenuti;
- riconoscere eventuali vulnerabilita riscontrate nella macchina target.

2. Ambiente di Lavoro e Strumenti

2.1 Configurazione del Laboratorio

- **Macchina Attaccante:** Kali Linux 2025.3 – IP: 192.168.50.10/24
- **Macchina Vittima:** Metasploitable 2 – IP: 192.168.60.12/24
- **Rete:** Rete Interna con pfSense VirtualBox

2.2 Strumenti Utilizzati

- **Nmap**: Usato per il comando `sudo nmap -sn [IP]` per verificare gli host vivi nella rete ed accertarmi che è presente la Metasploitable tra questi.
- **Nessus**: Usato per lanciare una scansione sulle vulnerabilità di un target.

3. Attività Tecnica e Metodologia

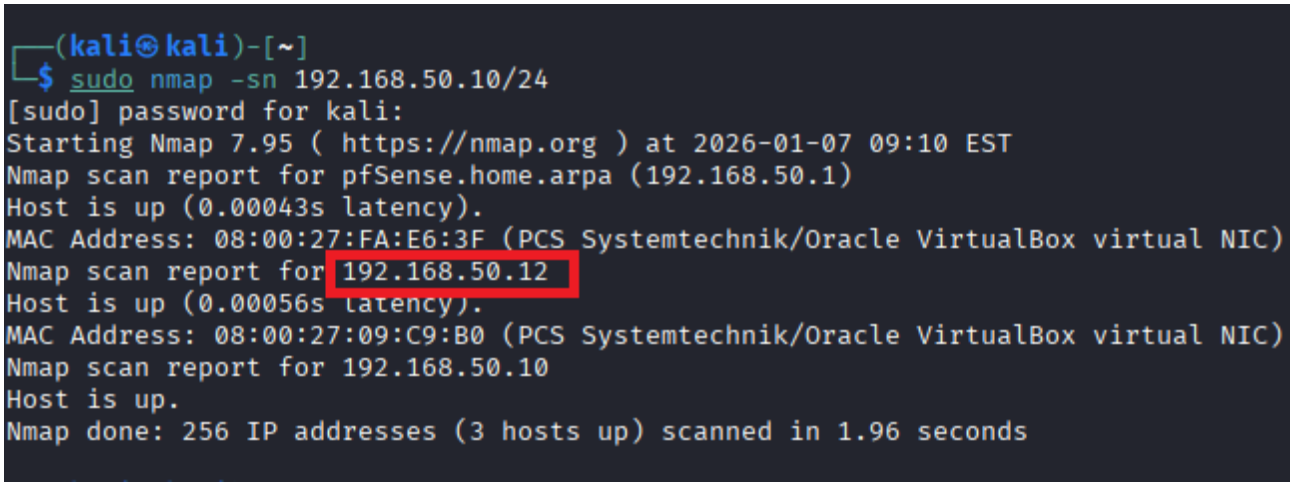
3.1 Fase di *Preparazione*

Prima di cominciare la scansione vera e propria verifichiamo che la macchina Metasploitable sia connessa alla nostra rete ed assicuriamoci che la macchina target sia raggiungibile dalla nostra Kali.

Per fare ciò eseguiamo i seguenti passaggi:

- Eseguire il comando “ip a” sul terminale della Metasploitable per ottenere il suo indirizzo IPv4 (nel mio caso l’IP è 192.168.50.12)
- spostandoci sul terminale della Kali eseguiamo il seguente comando al fine di andare a visualizzare tutti gli host presenti nella nostra rete:

`sudo nmap -sn [IP della Kali]`



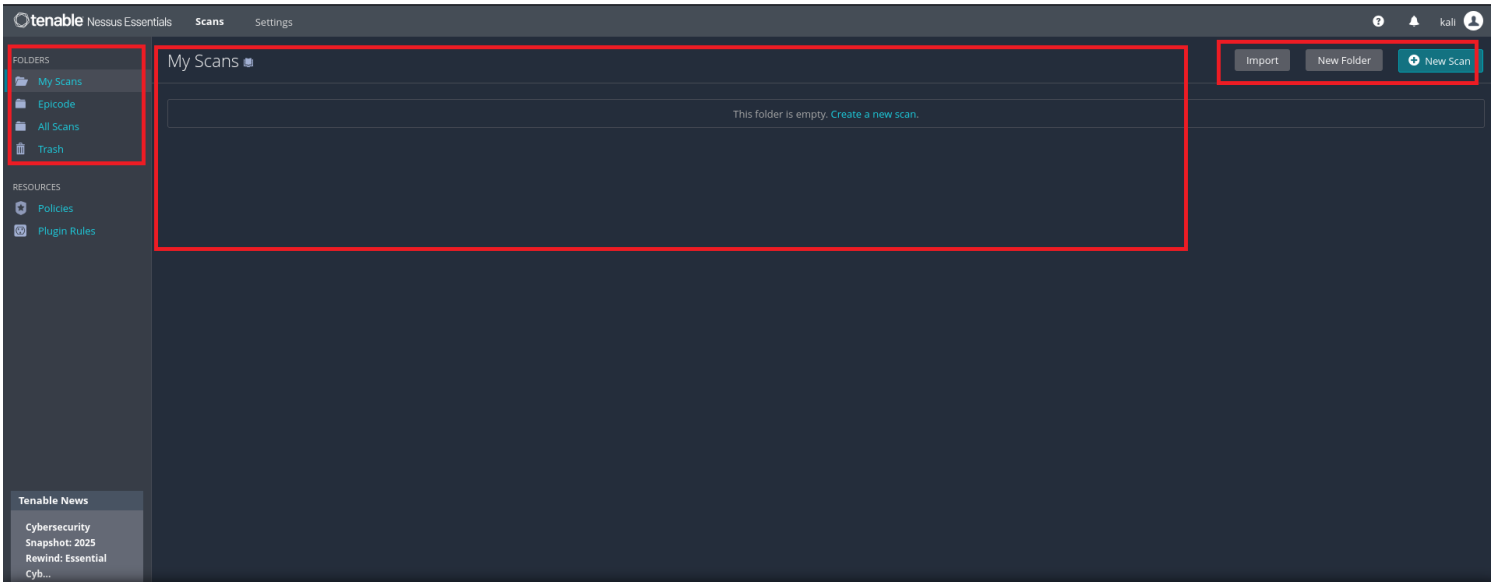
Proprio come ci aspettavamo sulla stessa rete della nostra Kali è presente anche Metasploitable; possiamo dunque procedere con la scansione su Nessus.

3.2 Accesso a *Nessus*

Procediamo ad avviare sul nostro browser Nessus ricordandoci prima di lanciare il seguente comando dal nostro terminale per poter avviare il servizio.

`sudo service nessusd start`

Non appena avremo avviato correttamente il servizio ed effettuato il login ecco come si presenta l’interfaccia di Nessus.



Nella schermata principale di Nessus potremo:

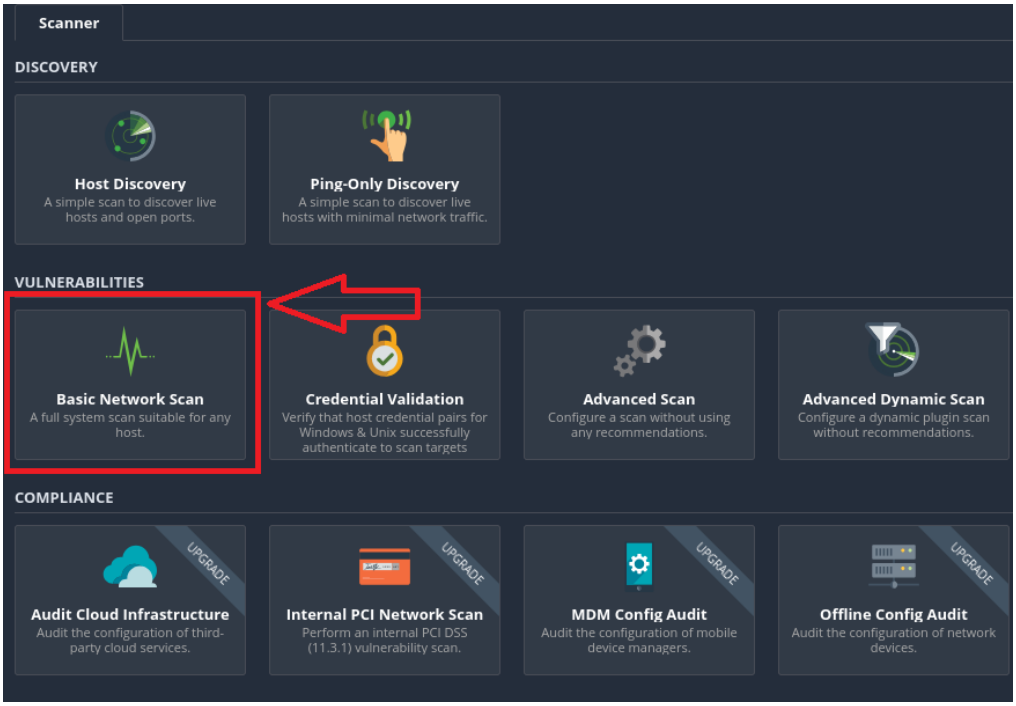
- Visualizzare l'elenco delle cartelle create (in alto a sinistra)
- Visualizzare l'elenco delle scansioni effettuate (in alto al centro)
- Importare/Creare cartelle o avviare scansioni (in alto a destra)

3.3 *Configurazione ed Avvio della scansione*

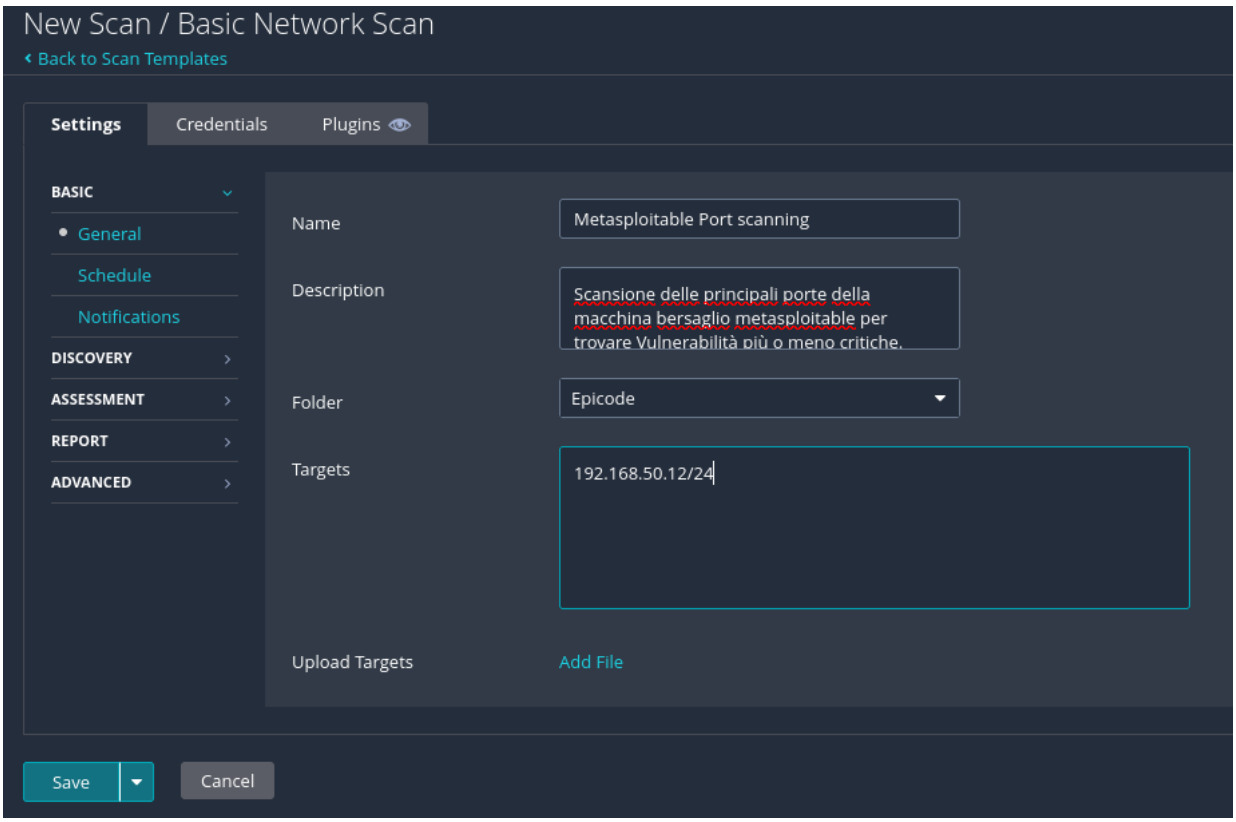
Per creare una nuova scansione spostiamoci su una cartella a nostra scelta (nel mio caso ho creato una cartella "Epicode") e clicchiamo su "New Scan".

Fatto ciò si aprirà un menù in cui potremo selezionare il tipo di scansione che vogliamo effettuare sul nostro Target.

Nel mio caso andrò a selezionare "Basic Network Scan" sotto la voce "vulnerabilities".



Nella schermata successiva potremo iniziare a configurare alcuni dettagli della nostra scansione:

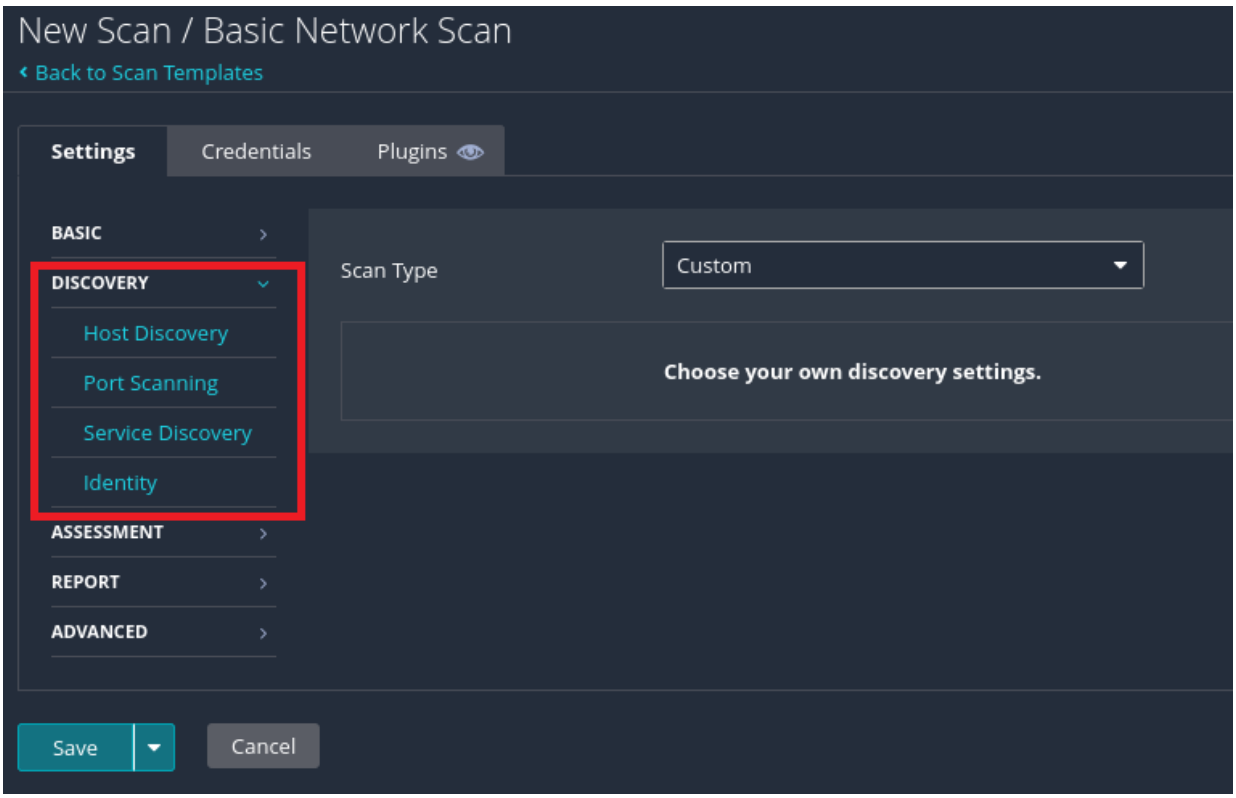


Qui andrò a compilare rispettivamente:

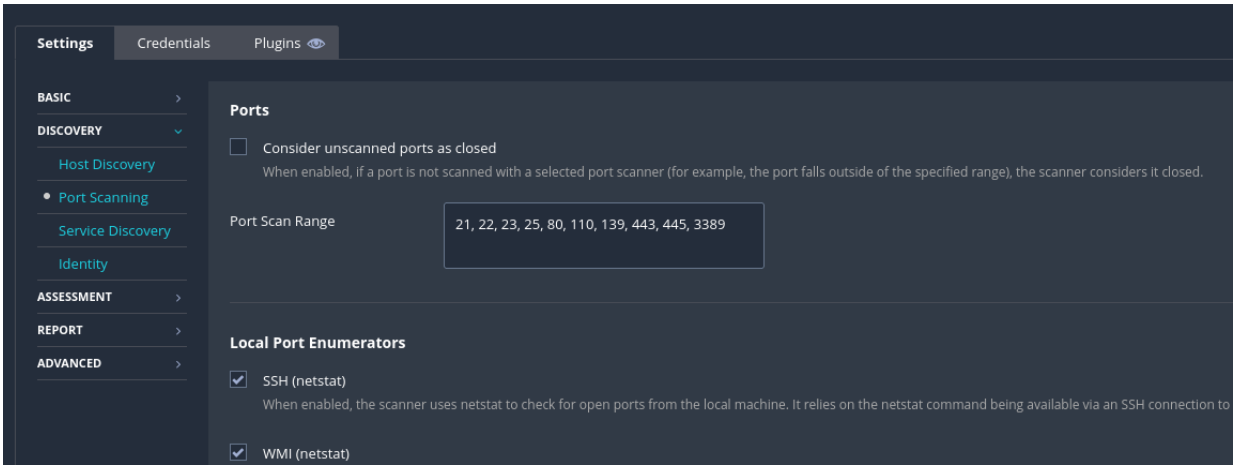
- **Name**: il nome da dare alla scansione (es. Metasploitable Scan)
- **Description**: breve descrizione di cosa andremo a scansionare
- **Folder**: la cartella in cui verra salvata la scansione una volta effettuata
- **Targets**: indirizzi IP di uno o più Target

Per configurare correttamente le porte che andremo a scansionare clicchiamo sulla voce “Discovery” a sinistra della schermata ed impostiamo lo **Scan Type** su **Custom**.

Una volta effettuato questo passaggio ci dovrebbero essere apparsi dei nuovi sotto menu immediatamente sotto la voce “Discovery”:



Clicchiamo su “Port Scanning” ed andiamo ad elencare nella voce “Port Scan Range” tutte le porte che ci interessa analizzare:



Inserite le porte che ci interessano abbiamo praticamente terminato con la configurazione, procediamo cliccando sul tasto “Save” situato in basso a sinistra dopo di che avviamo la scansione premendo sul pulsante “Play”.

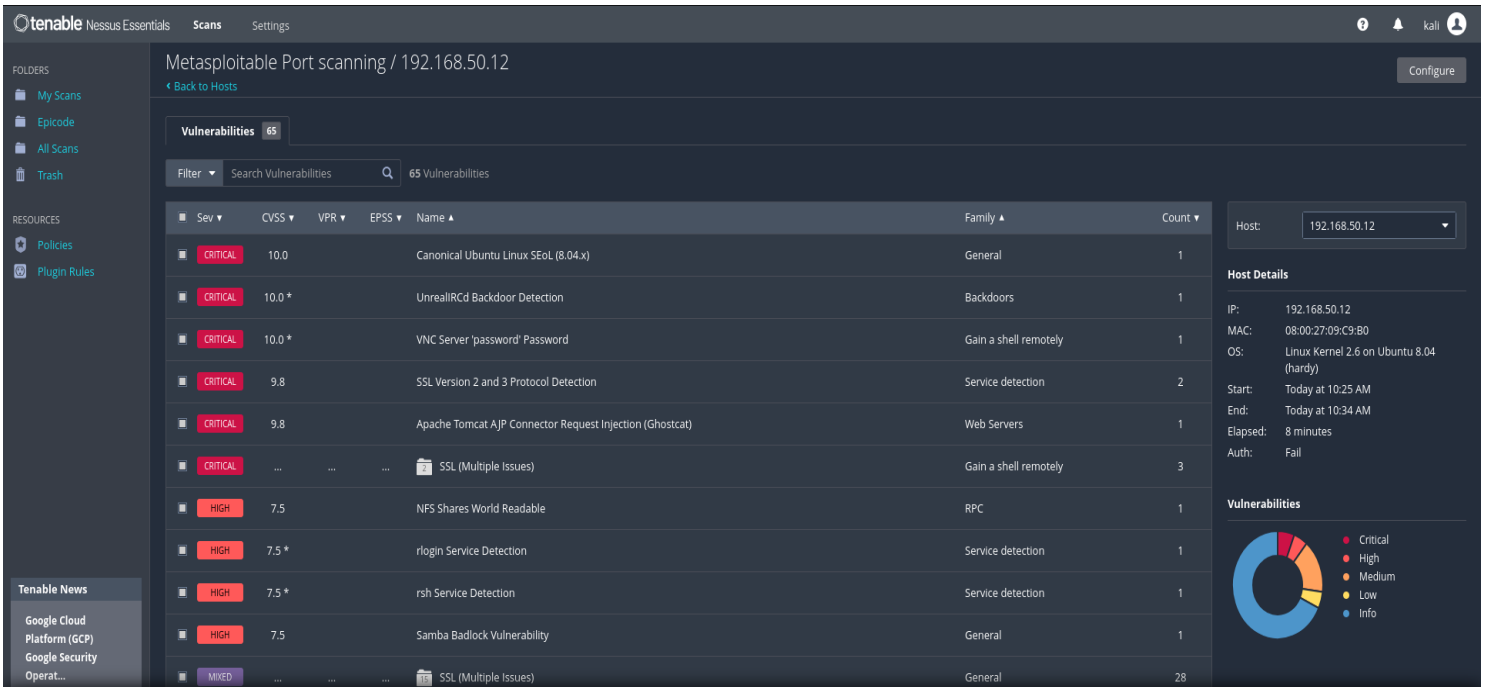
La nostra scansione è stata avviata, occorre solo aspettare che venga completata dopo di che potremo analizzare l'output che ci ha fornito Nessus.

4. Risultati e Analisi

4.1 Vulnerabilità o Criticità Rilevate

Una volta completata la scansione saremo in grado di vedere un elenco molto dettagliato di tutte le vulnerabilità che sono state trovate sulla macchina Target.

Questa lista si presenta in modo ordinato e schematico, suddivisa in ordine di "Criticità" della vulnerability riscontrata; questa organizzazione gerarchizzata ci aiuta ad individuare in modo rapido ed efficiente le criticità più gravi che verranno posizionate ad una posizione più alta rispetto a criticità più lievi.



Nella lista che la scansione ha prodotto notiamo alcuni dettagli come:

- ***Sev**: "Severity" ossia quanto è grave una vulnerabilità individuata (Es. Critical, High, Mixed, Medium e così via.)*
- ***Name**: il nome della criticità rilevata*
- ***Family**: la categoria a cui quella vulnerabilità appartiene (Es. Backdoors, Web Servers, Gain a Shell Remotely, Service detection e così via…)*

4.2 Interpretazione dei Dati

Possiamo cliccare su un elemento della lista per visualizzare in modo più dettagliato tutte le caratteristiche principali di quella particolare criticità individuata:

Questa particolare criticità ci fa capire che il sistema operativo installato è troppo vecchio (fuori supporto dal 2013) e non riceve più aggiornamenti di sicurezza.

In pratica, è estremamente vulnerabile perché non ha protezioni contro i virus o gli attacchi scoperti negli ultimi 12 anni.

5. Conclusioni

5.1 Riepilogo

Possiamo affermare che l'obiettivo dell'attività è stato pienamente raggiunto. Configurando una policy di scansione personalizzata ("Custom") su **Nessus**, sono riuscito a isolare l'analisi esclusivamente sulle porte di interesse, ottenendo un output mirato e privo di 'rumore' di fondo. I risultati hanno evidenziato come la macchina Metasploitable sia esposta a rischi elevati, dovuti principalmente all'utilizzo di un sistema operativo ormai obsoleto (**End of Life**). Questo test pratico mi ha permesso di comprendere concretamente come la mancata manutenzione e l'assenza di patch di sicurezza rendano un sistema estremamente vulnerabile, anche di fronte a scansioni di base.