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*.

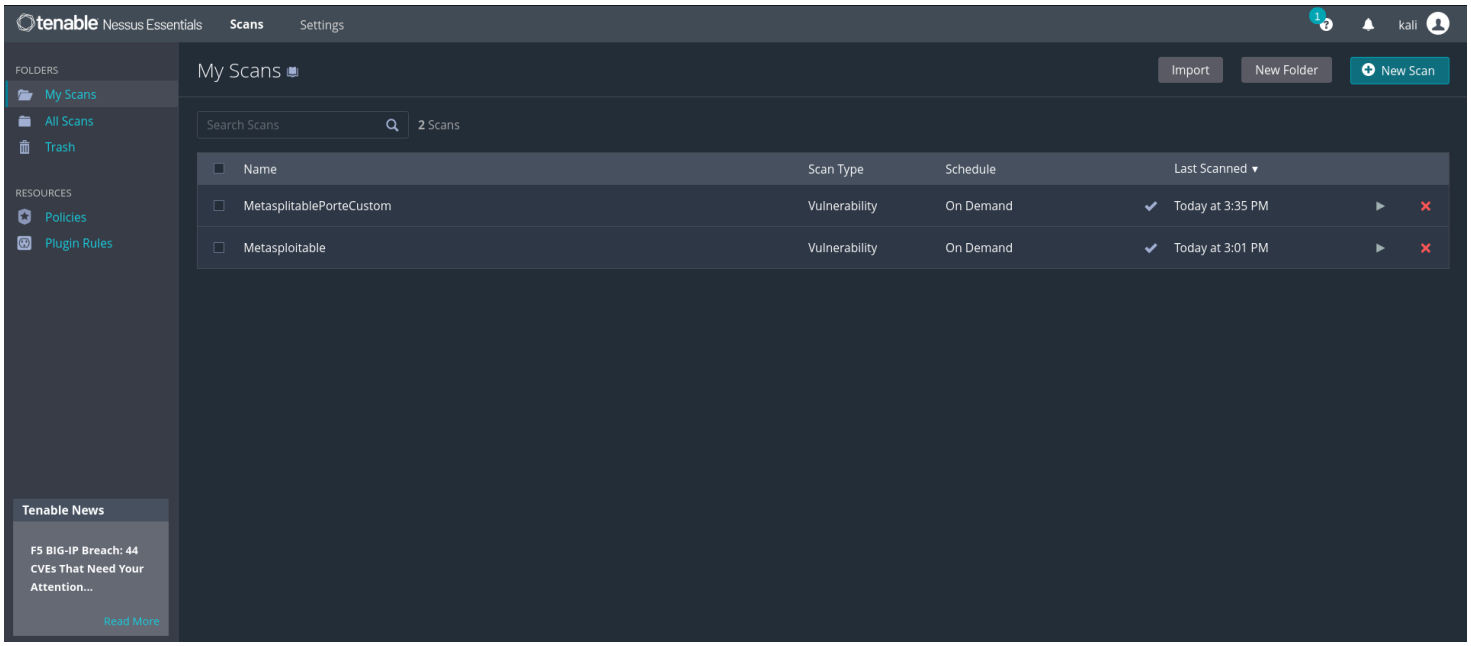
Questo lo possiamo fare in diversi modi:

- 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

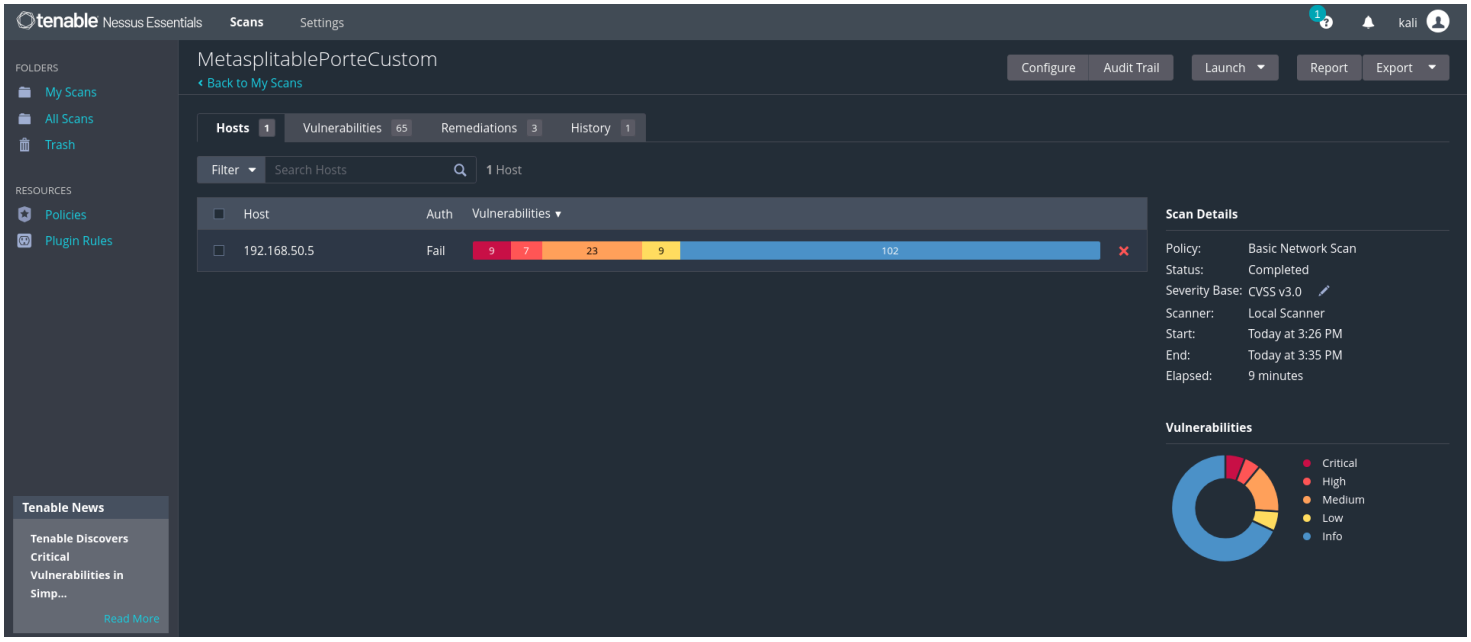
Una volta individuato l'indirizzo IP della Metasploitable, andremo ad usare Nessus per fare la scansione delle porte.



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:

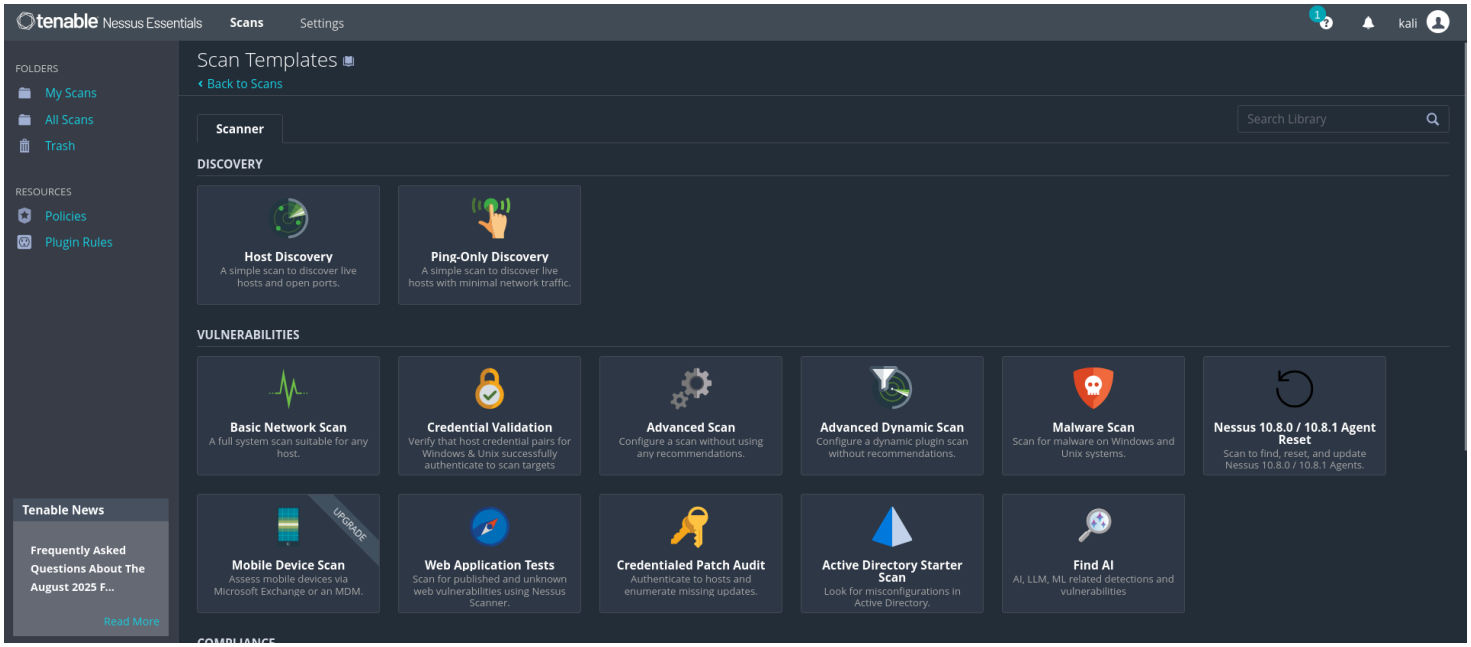


Cosa vediamo?

- 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**".

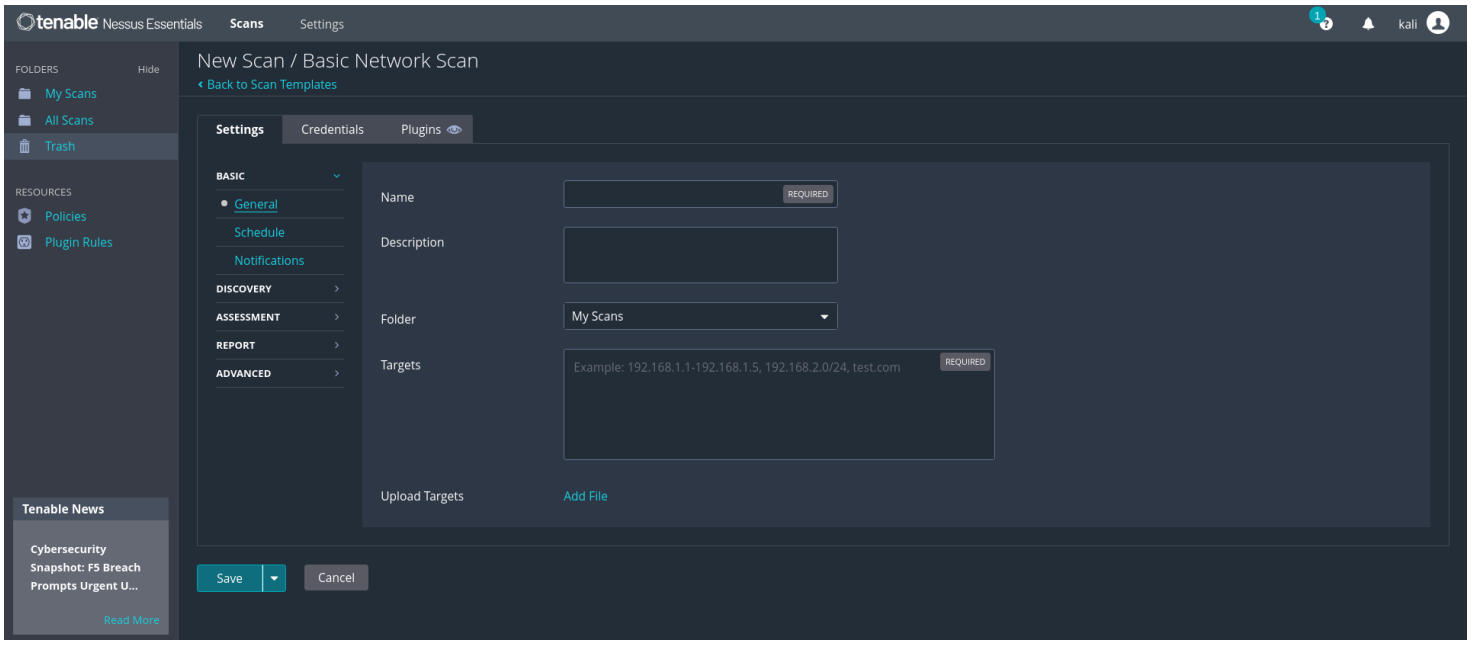
Si aprirà la seguente schermata:



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

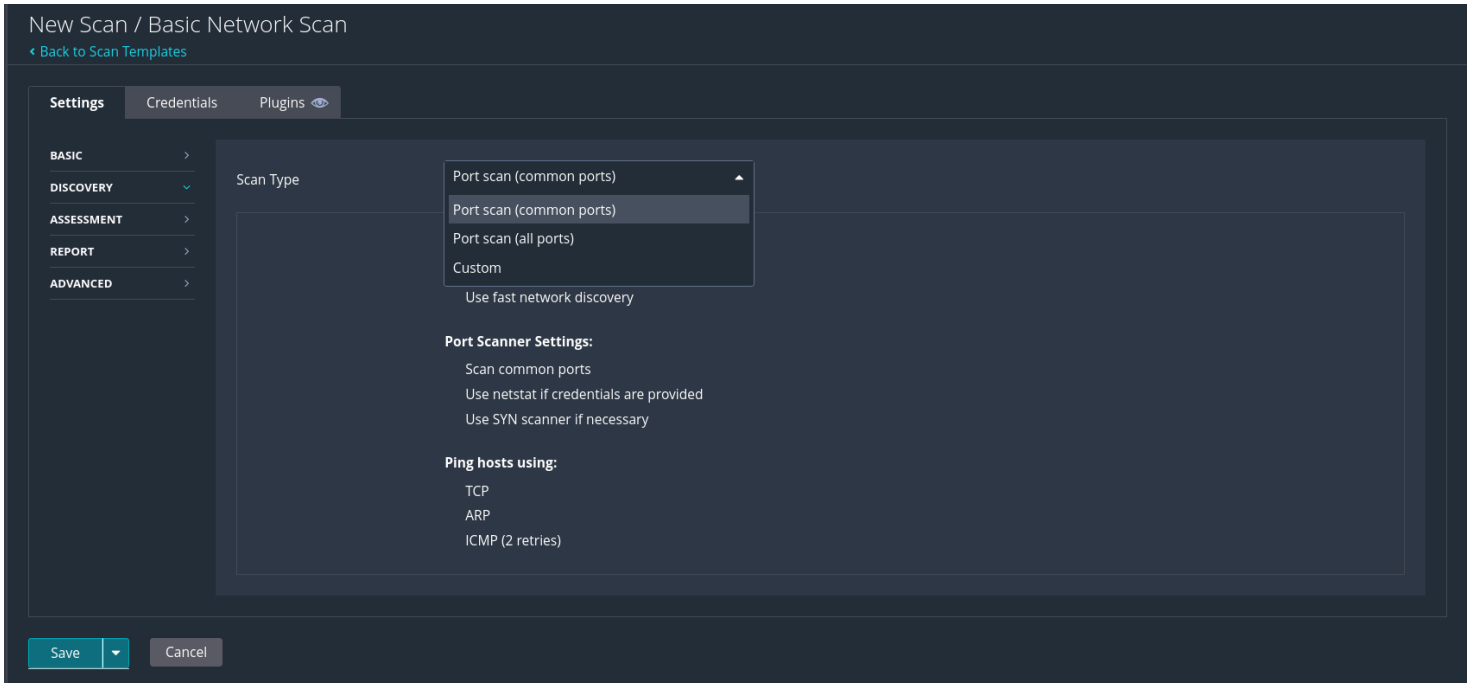
Dopodiché si avvierà una pagina in cui ci chiederà di inserire:

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



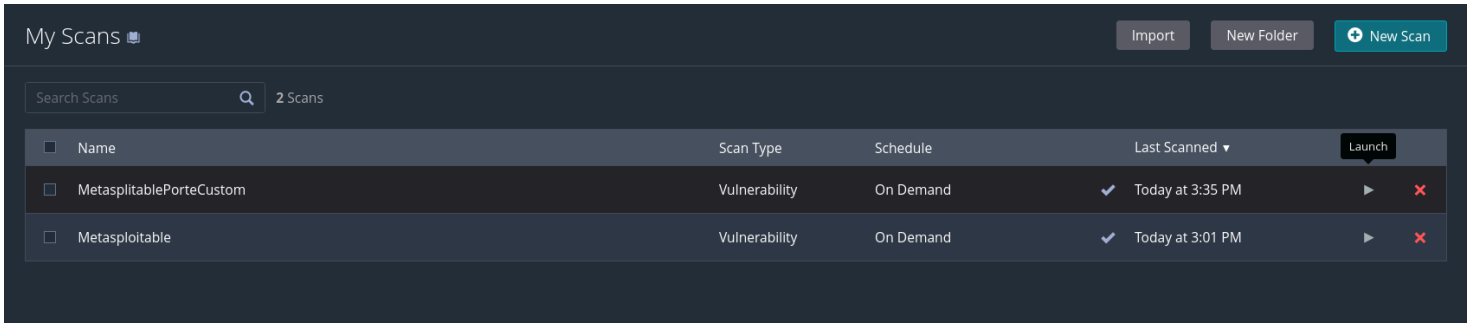
Se andiamo nella sezione Discovery possiamo scegliere il tipo di scansione:

- **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.

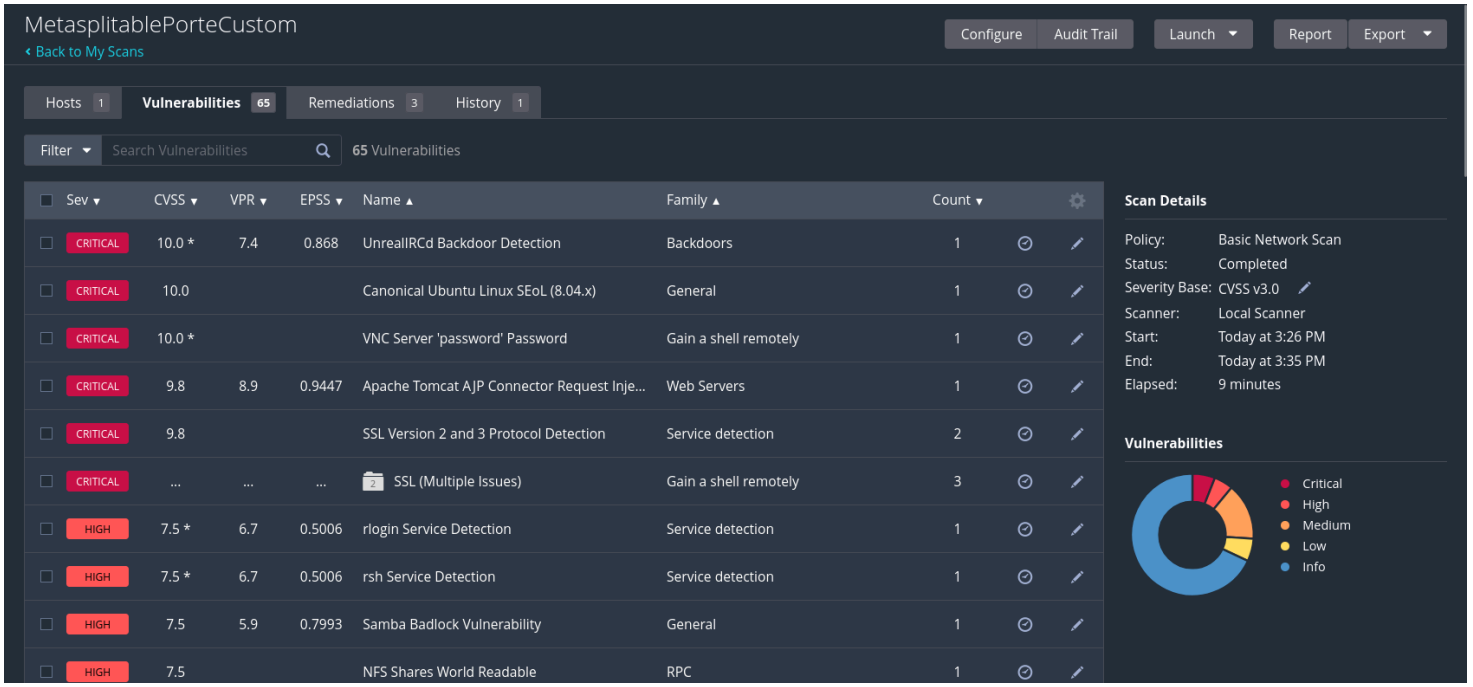


Per effettuare la scansione, potrebbe volerci un po' di tempo, soprattutto a seconda di quante porte si sono scelte per essere analizzate.

Terzo passo

La scansione è terminata. E ora?

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

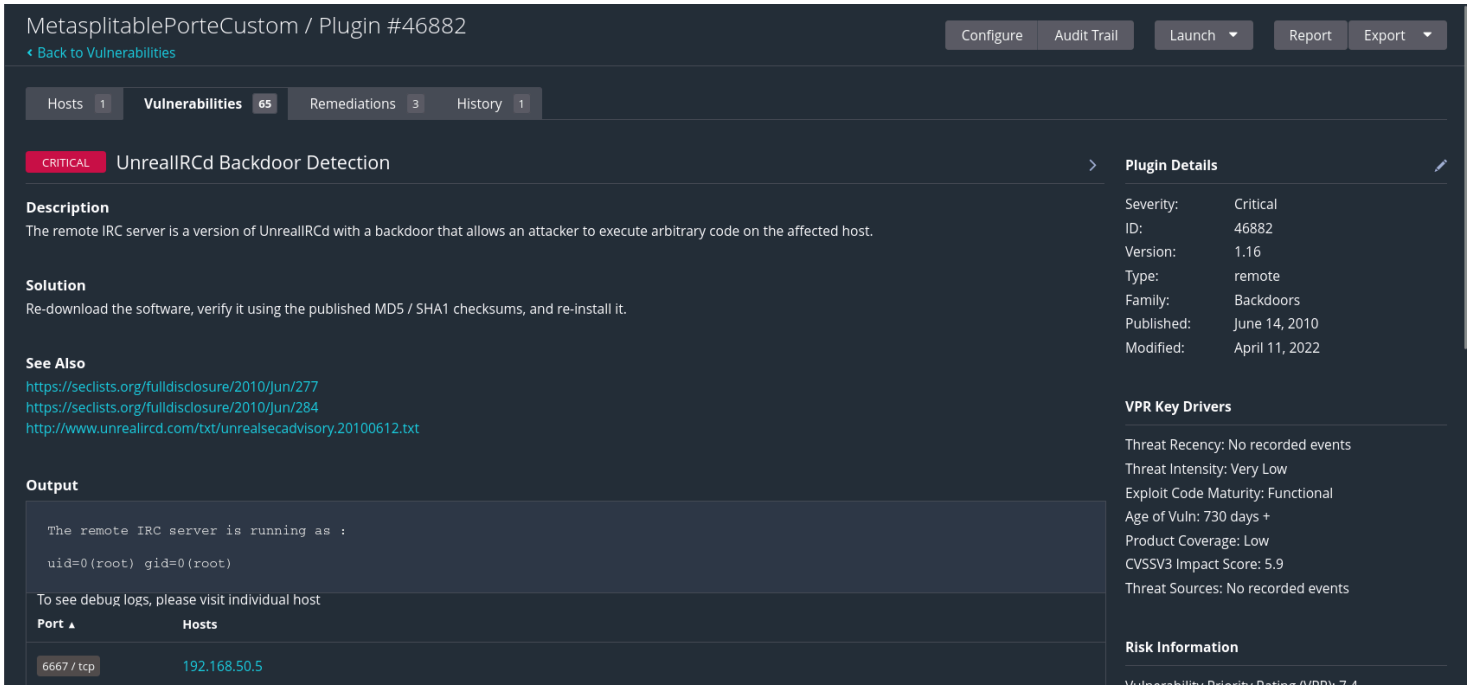


Come possiamo vedere dalle immagini, ci viene proposta una lista di vulnerabilità che vengono classificate dalla più critica alla meno critica.

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:



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

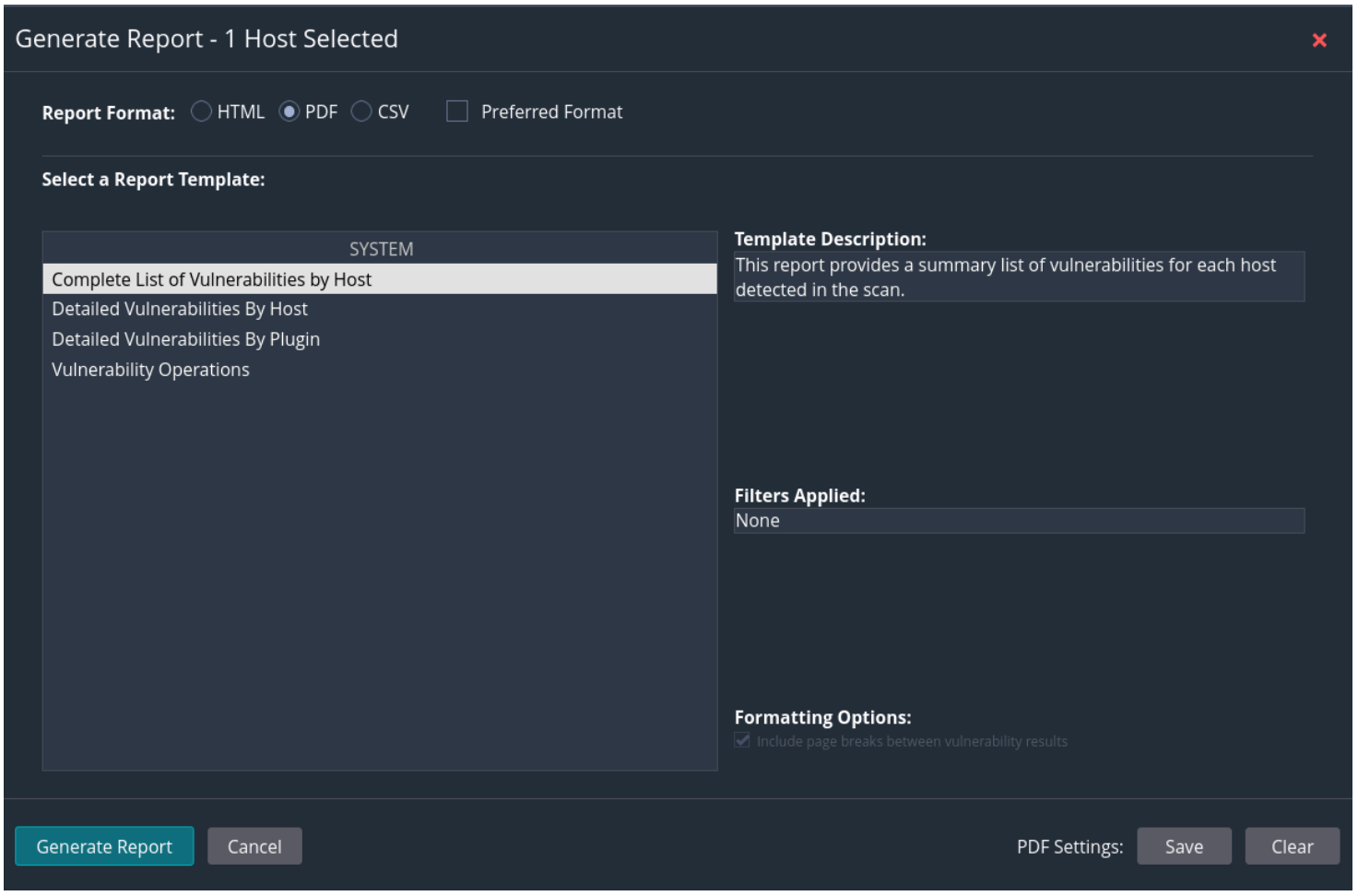
Cosa facciamo adesso?

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:

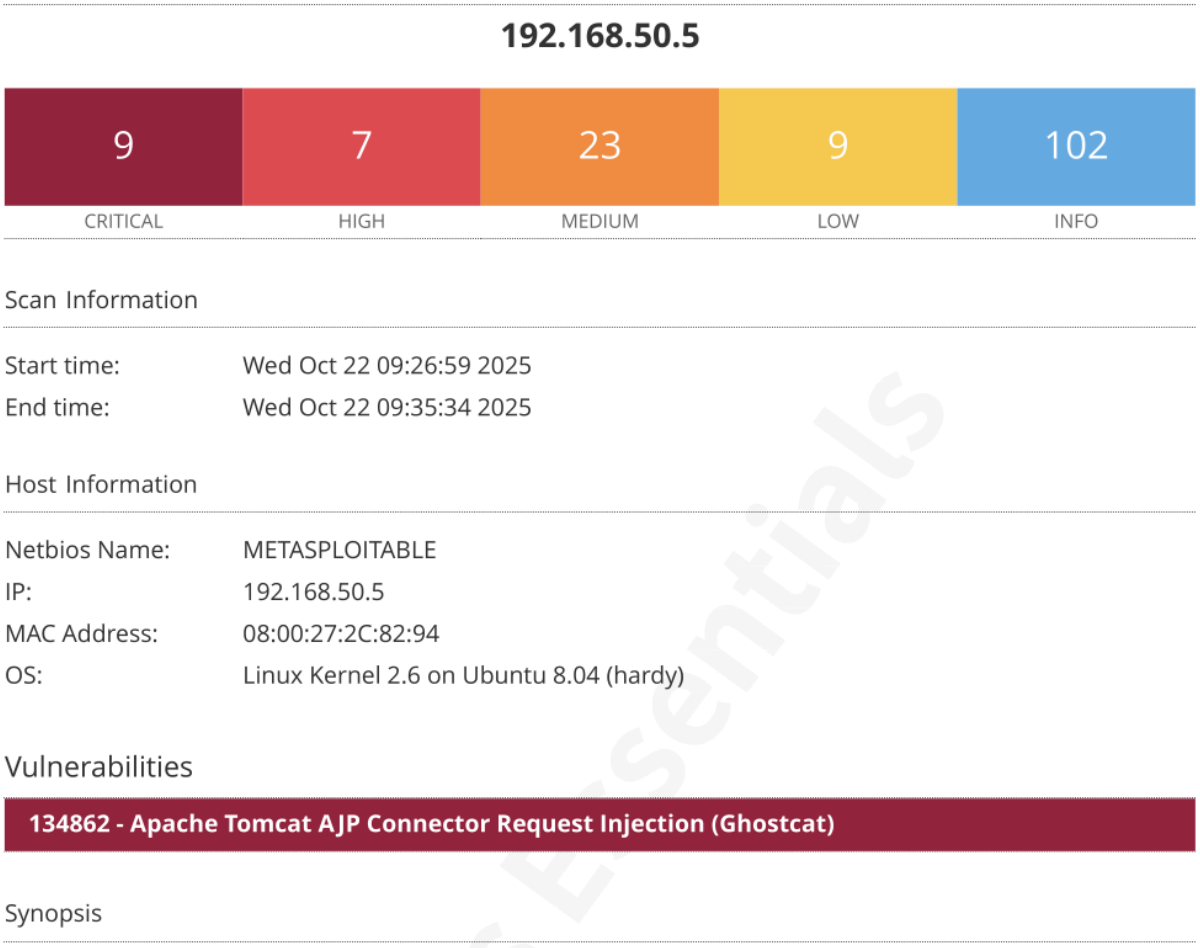


Scegliamo il tipo di report che vogliamo scaricare, scegliamo il formato e clicchiamo su "**Generate Report**". Aspettiamo qualche secondo e subito dopo verrà avviato il download del file.

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:



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**.