REPORT S5/L3

Vulnerability Scanning

L’esercitazione di oggi prevede di effettuare un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandoci sulle porte comuni. Questo per fare pratica con lo strumento Nessus.

Cos’è Nessus?

Nessus è un **vulnerability scanner** semplice da utilizzare e molto potente, che è molto utilizzato dalle compagnie per coprire reti piuttosto estese.

FASI VULNERABILITY SCANNER:

- **Port Scanning**: In questa fase lo scanner cerca di capire se i target sono attivi e quali porte sono aperte)
- **Service Detection**: Per ogni porta aperta che è stata trovata, lo scanner spedisce del traffico di test per capire che tipo di applicazione è in ascolto su quella determinata porta)
- **Ricerca nel Vulnerability Database**: Per ogni servizio rilevato, lo scanner esegue una ricerca nel proprio database. Cosa cerca? Vulnerabilità note per quella particolare versione
- **Test**: Questa fase conclusiva effettua dei test target per verificare se sono affetti dalla vulnerabilità in esame. Inoltre Nessus consente di esportare i risultati con i report delle vulnerabilità per ogni macchina obiettivo)

Caratteristiche principali:

- **Database enorme:** Contiene migliaia di "Plugin" (*piccoli script che verificano una specifica vulnerabilità*).
- **Multipiattaforma:** Funziona su Windows, Linux e macOS.
- **Aggiornamento costante:** Tenable (piattaforma da dove abbiamo scaricato il nostro Nessus) aggiorna i plugin quasi quotidianamente per coprire le nuove minacce ***(Zero-Day***).

  Dalla interfaccia generale il tool ci mette a disposizione una quantità notevole di scansioni predefinite, ovvero per le quali sono già definite una serie di policy di scansione

  (Es. Basic Network Scan)

Per la nostra esercitazione ci affideremo ai seguenti punti:

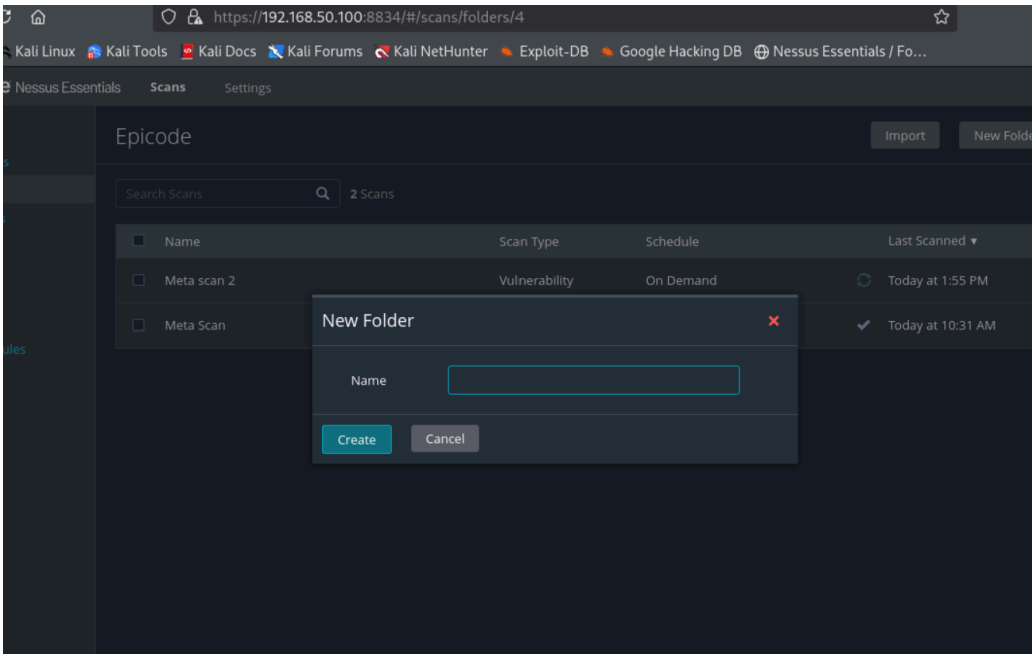
Target: Metasploitable:

Porte: Porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389)

Tipo di scansione: Basic Network Scan (Configurazione per scansione di rete)

1 - Partiamo nel creare una cartella per aiutarci a lavorare in maniera ordinata

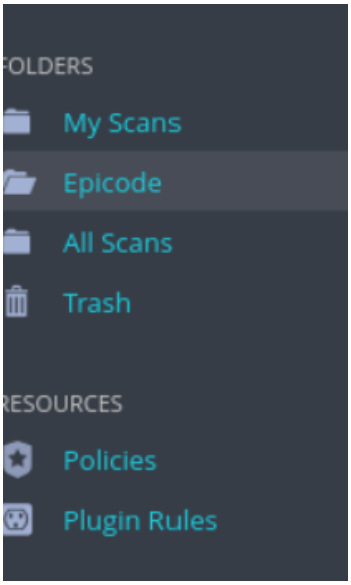
---



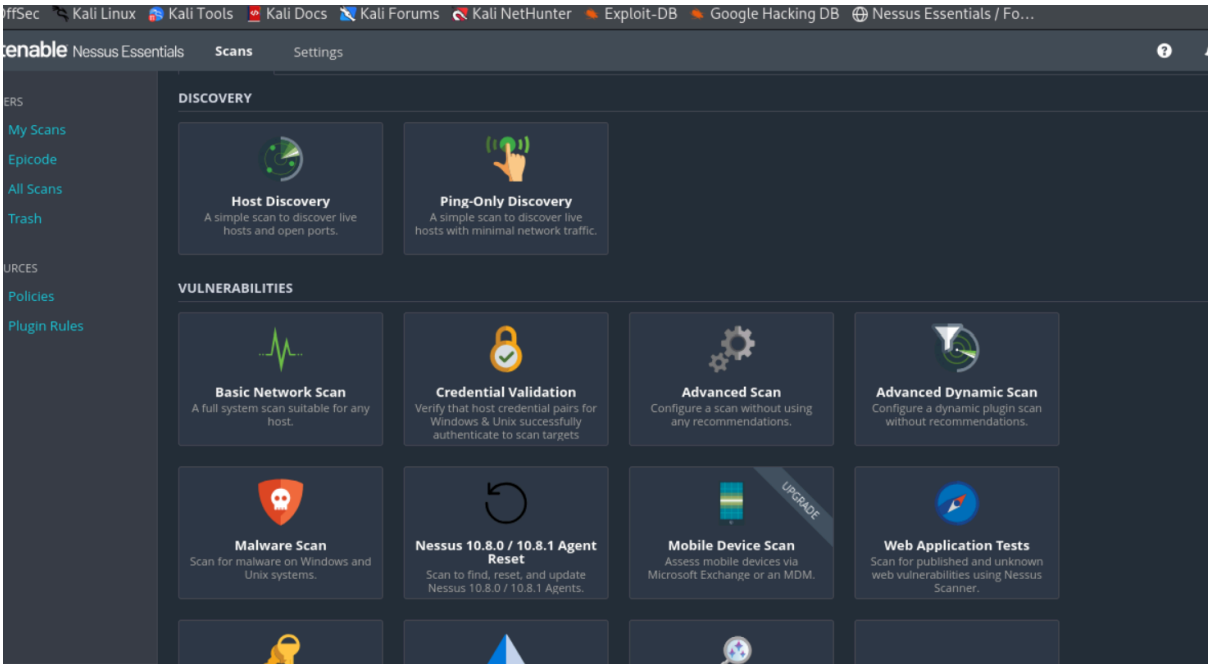
Clicchiamo “**New Folder**” e decidiamo un nome per avviare il nostro lavoro.

In questo caso abbiamo deciso di rinominare la cartella “**Epicode**”. Ma la scelta del nome è libera e si basa sulle proprie esigenze di lavoro o di esercitazioni.

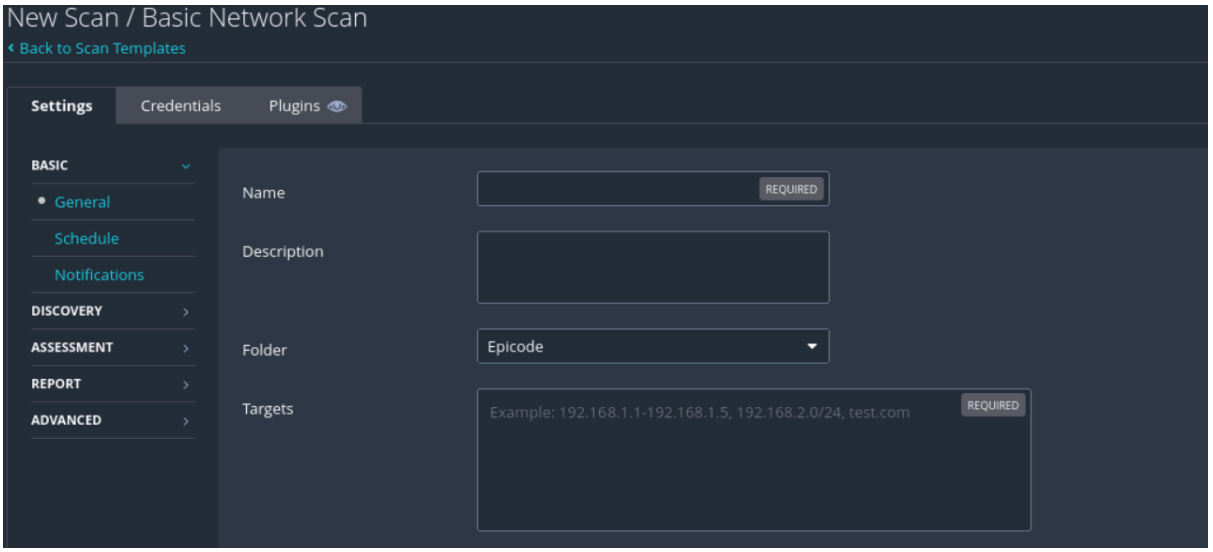
2 - Selezioniamo la nostra cartella rinominata “Epicode”



3 - Selezioniamo dalla cartella Epicode “New Scan” e impostiamo il tipo di scan:
Utilizziamo ***Basic Network Scan*** (*Plugin* Progettato per una scansione generale della sicurezza adatto a quasi ogni tipo di Host)

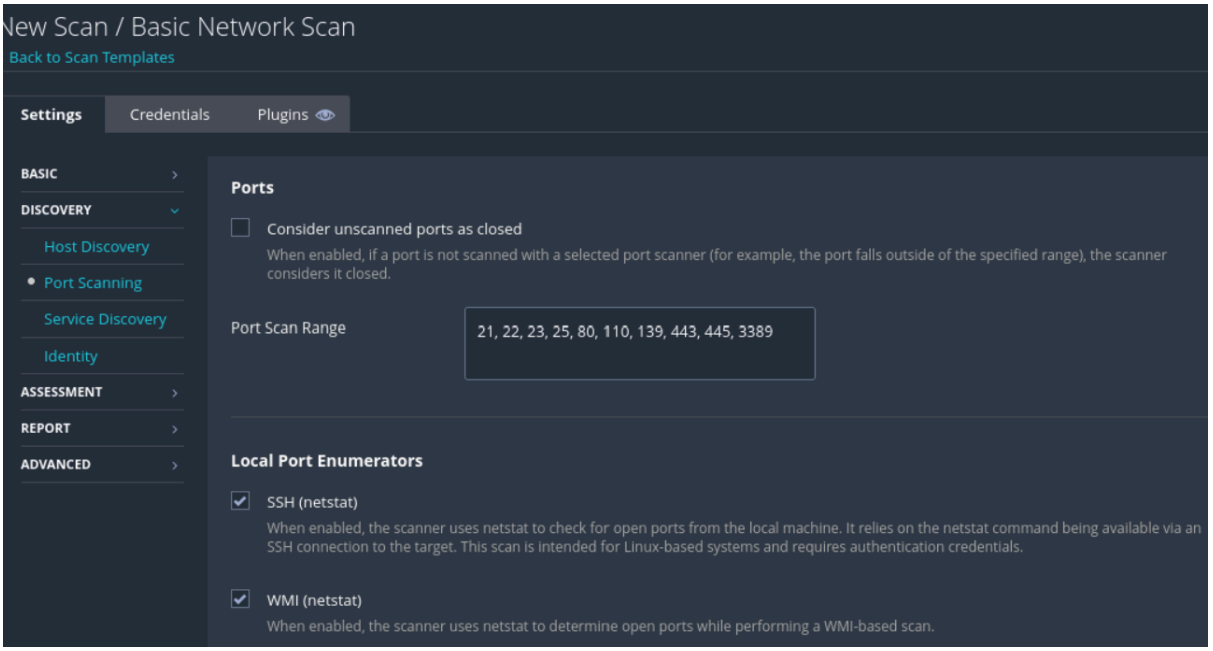


4- Aggiungiamo un nome e l'host su cui desideriamo operare



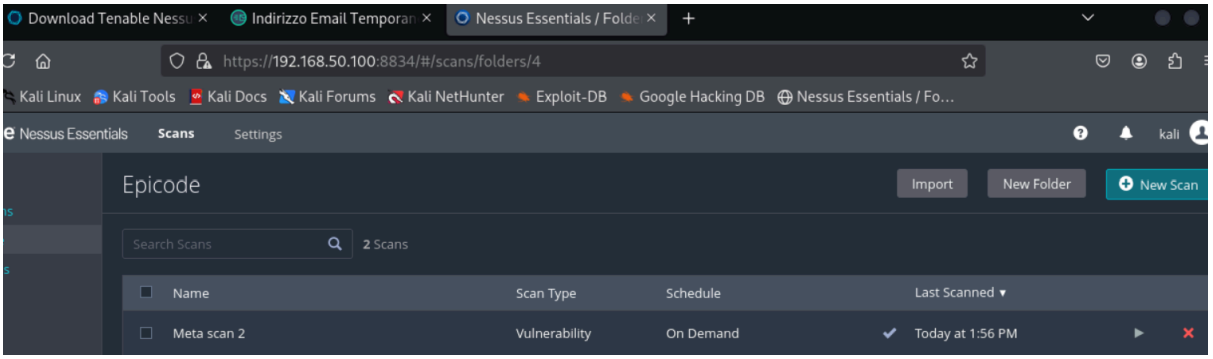
Nella sezione Name scriveremo il nome "**Meta Scan**" mentre nel target andremo a inserire **l'indirizzo IP** della nostra macchina Target, ovvero la **Metasploitable.**

5 - Specifichiamo le porte che vogliamo analizzare su cui vogliamo concentrarci
Come richiesto dalla traccia dell'esercizio



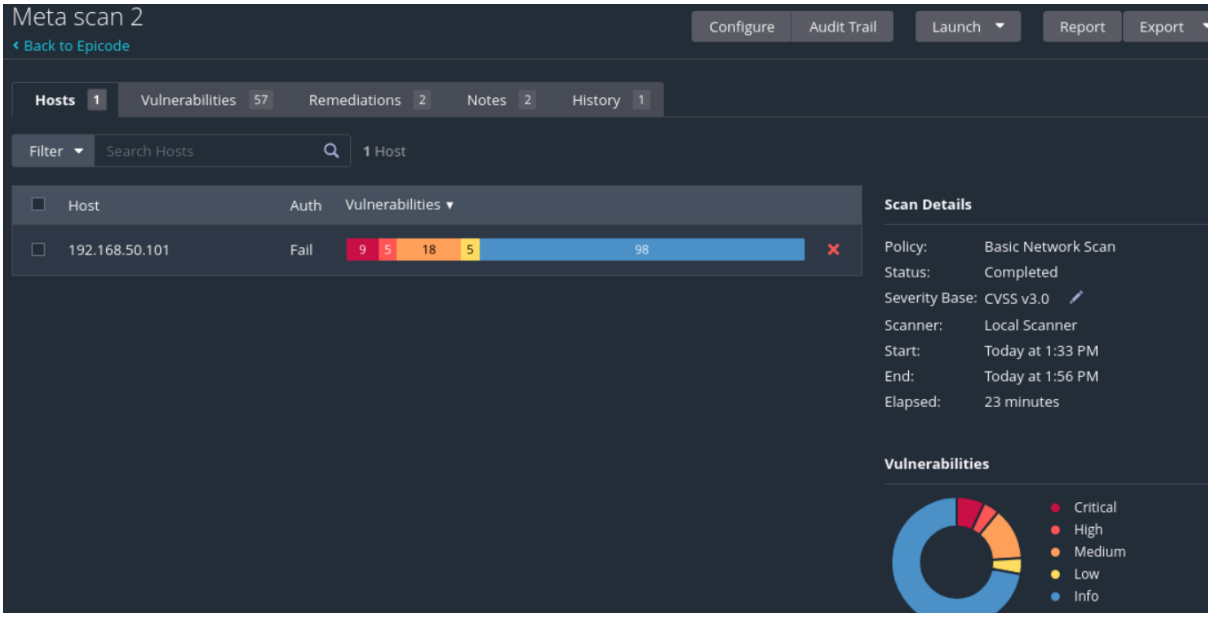
Sotto "***Basic***" andiamo a selezionare "**Discovery**" selezionando "**Custom**" dopodiché vedremo che si aprirà sotto una tabella con **4** sezioni: Andiamo su "**Port Scanning**" e nel "**Port Scan Range**" impostiamo le porti comuni che ci sono state richieste

6- Per far partire il nostro scan clicchiamo il tasto play e aspettiamo che il lavoro finisca



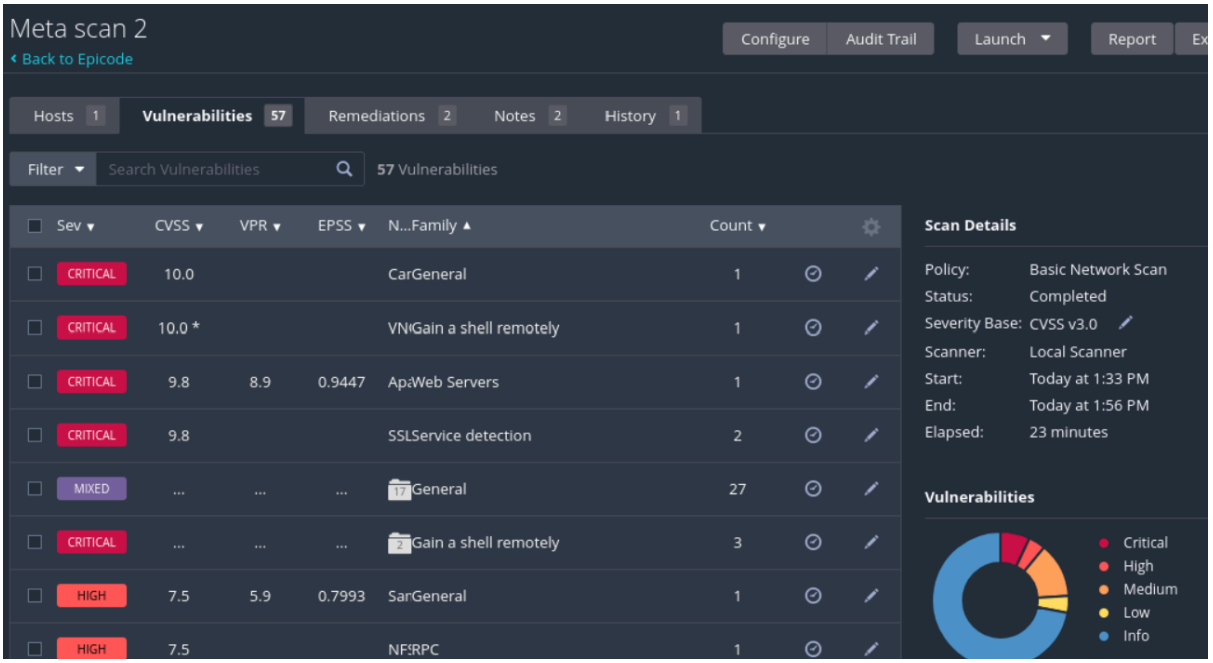
Ritorniamo sulla cartella che abbiamo creato prima "***Epicode***" e ci apparirà il settaggio per far partire la nostra scansione. Clicchiamo sul tasto ***play*** e attendiamo i risultati.

7- Interfaccia generale del completamento dello scanner

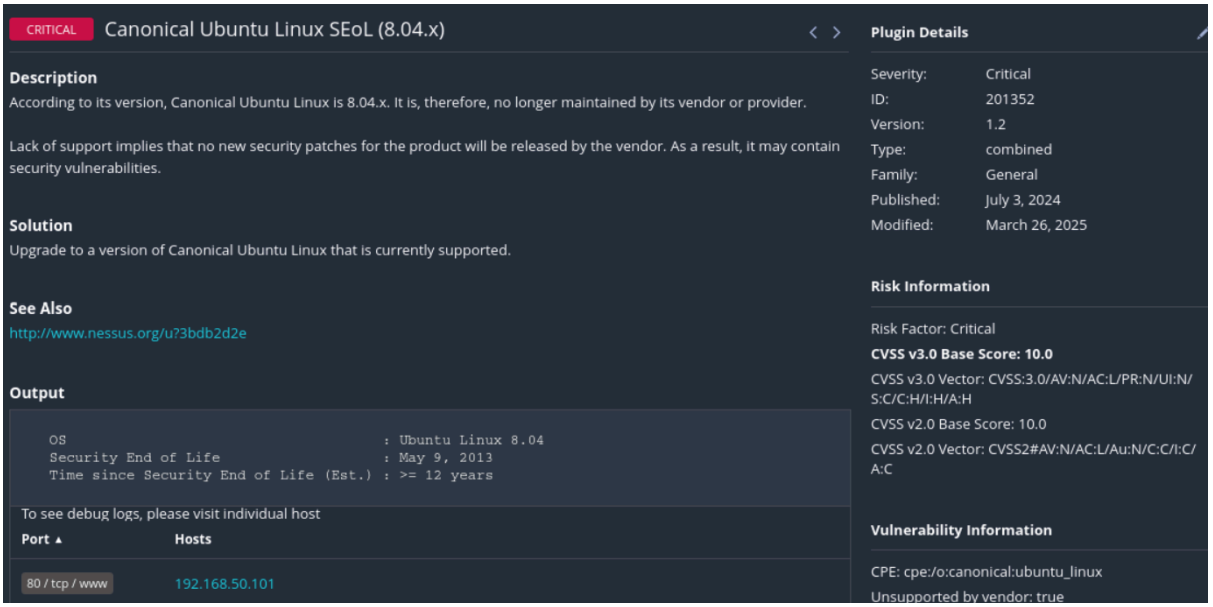


A fine scansione possiamo entrare sulla nostra scansione e ci appariranno le seguenti schede:
Host: Il target utilizzato per la nostra scansione
Vulnerabilities: Le vulnerabilità che la nostra scansione ha rilevato
Remediations: La scansione genera anche dei "Rimedi" per sanificare un qualche tipo di vulnerabilità (*Potrebbe essere un aggiornamento di una versione*)
Notes: Lo scanner in questa sezione ci comunica se ci sono eventi particolari o errori tecnici che sono stati rilevati durante la scansione
History: Ci mostra le nostre attività

8- Andiamo sulle vulnerabilità e analizziamole una



9- Spiegazione della vulnerabilità (*critica*)



Analizziamo prima di tutto **l'output**: Ci restituisce dalla ricerca effettuata che l'host sta utilizzando *Ubuntu Linux 8. 04 ;* mentre la "***Security End of Life***" ci dice che la sicurezza non è aggiornata dal **2013**, pertanto possiamo dedurre che non vengono più rilasciate *patch* di sicurezza. Questa *falla* è stata identificata analizzando la porta **80/tcp**. Lo *scanner* in questo caso è riuscito a determinare la versione esatta del sistema operativo. Come accennavamo anche prima i risultati dello scanner ci consentono anche di visualizzare l'eventuale soluzione (**Solution**). In questo caso specifico ci dice di aggiornare ad una versione successiva. **See Also** una volta aperto il link ci consente di visualizzare le prove documentali che classificano questo tipo di *vulnerabilità* e che tipo di rischi potremmo incontrare se non andiamo a risolvere queste ultime.

Conclusione:

Dopo aver terminato questa esercitazione possiamo affermare di aver iniziato a familiarizzare con il *tool* “**Nessus**” da vicino in quanto ci dà modo di testare le vulnerabilità dei nostri target e scoprirne i vari errori. Inoltre testando Nessus abbiamo anche potuto ampliare il nostro sapere su uno dei ***nodi cardini*** del penetration testing.