REPORT S5/L3

Effettuare un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Fasi dell'Esercizio:

1. Configurazione della scansione:
    - ○ Target: Metasploitable
    - ○ Porte: Solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389)
    - ○ Tipo di Scansione:
        - ■ Puoi scegliere tra:
        - ■ Basic Network Scan: Configurazione predefinita per una scansione di rete.
        - ■ Advanced Scan: Configurabile in base alle tue esigenze specifiche.
2. Esecuzione della scansione:
    - ○ Avvia la scansione configurata su Nessus.
    - ○ Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.

SVOLGIMENTO

Il primo passo dalla macchina Kali è quello di avviare il servizio nessus, mediante comando "***systemctl start nessud.service***". ***Figura 1***

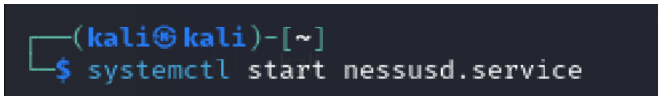

Figura 1.

Il servizio sarà sulla porta 8834 alla quale accederemo direttamente dal browser avendo accesso alla pagina di login per avviare la sessione di Nessus. ***Figura 2***

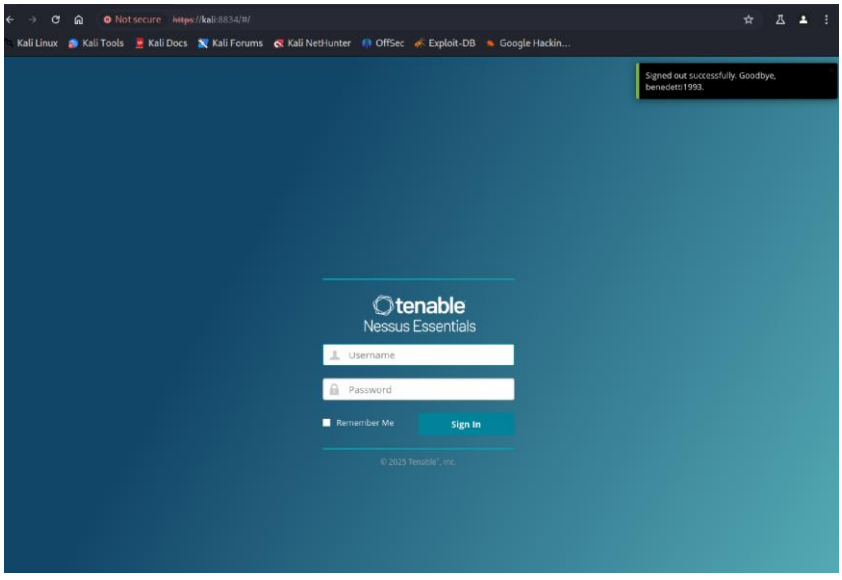

Figura 2, pagina di login sulla porta 8834.

Una volta effettuato il login si procede andando a configurare la scansione sul target Metasploitable in particolare solo sulle porti comuni, come da richiesta. Si procede quindi cliccando su “New Scan”, riempiendo i campi e selezionando la scheda “porte comuni” e si lancia la scansione attendendo il risultato. ***Figura 3***

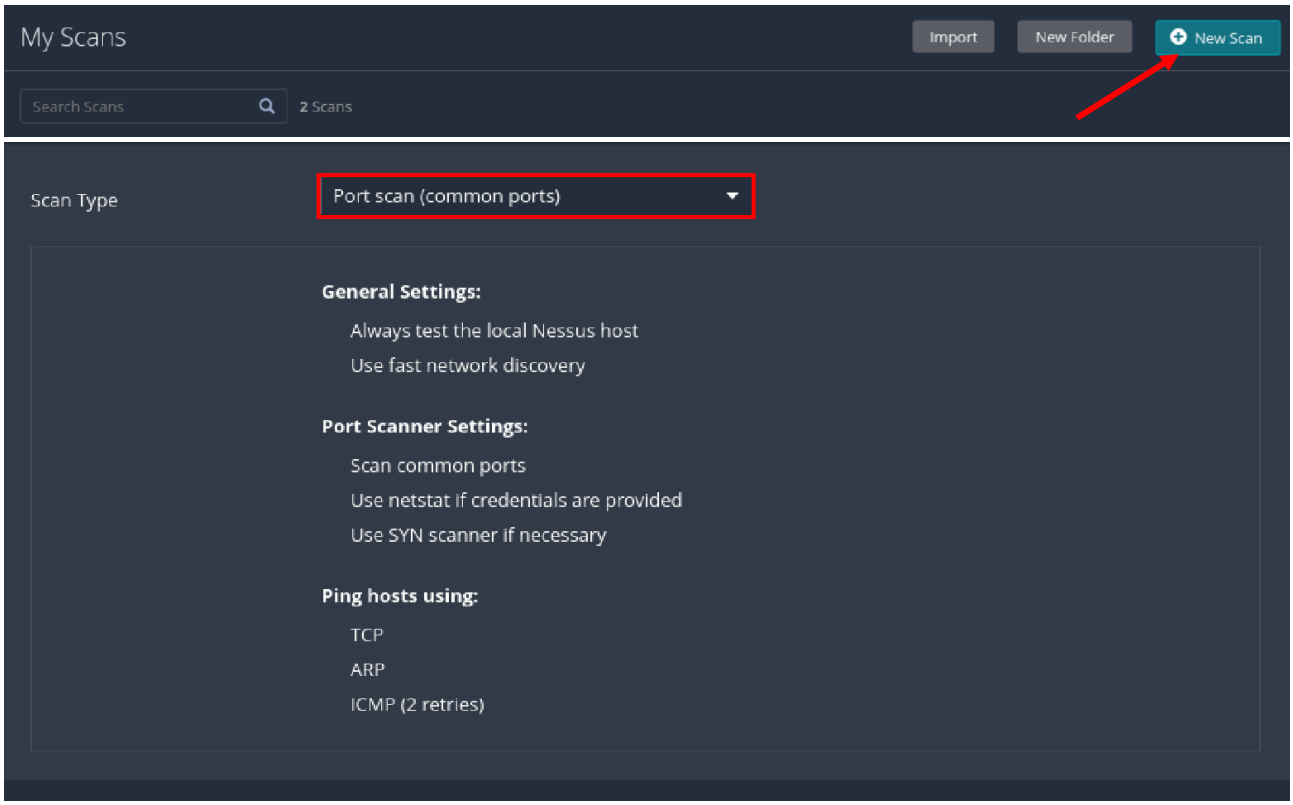

Figura 3, in alto a destra il pulsante “New Scan” per avviare la scansione, in basso la configurazione delle porte da analizzare.

Successivamente si produrrà un report in formato PDF, e si anlizzeranno i risultati prendendo in esame alcune delle vulnerabilità emerse. ***Figura 4***

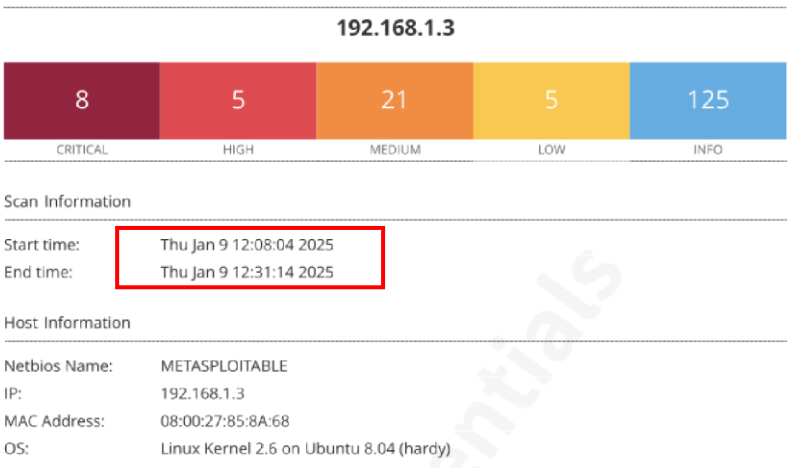

Figura 4

Andando ad analizzare la prima pagina del report, si nota come da subito nella parte alta siano messe in evidenza le vulnerabilità rilevate sulla host target con IP: 192.168.1.3 (Metasploitable), ordinate secondo il relativo CVSS (Common vulnerability scoring system), nello specifico sono presenti:

- 8 vulnerabilità con rischio ***critico***
- 5 vulnerabilità alto ***rischio***
- 21 vulnerablità rischio ***medio***
- 5 vulnerabilità rischio ***basso***

Altro elemento importante da tenere in considerazione immediante sotto al grafico delle vulnerabilità è quello del tempo di inizio e tempo di fine scansione, in questo caso la scansione è iniziata alle ore 12.08 ed è terminata alle ore 12.31. Nel report per ciascuna delle vulnerabilità rilevata oltre ad esserne presente la descrizione vi è anche la relativa soluzione che puo poi essere proposta o meno al cliente, andiamo a prendere in esame per esempio la prima. ***Figura 5***

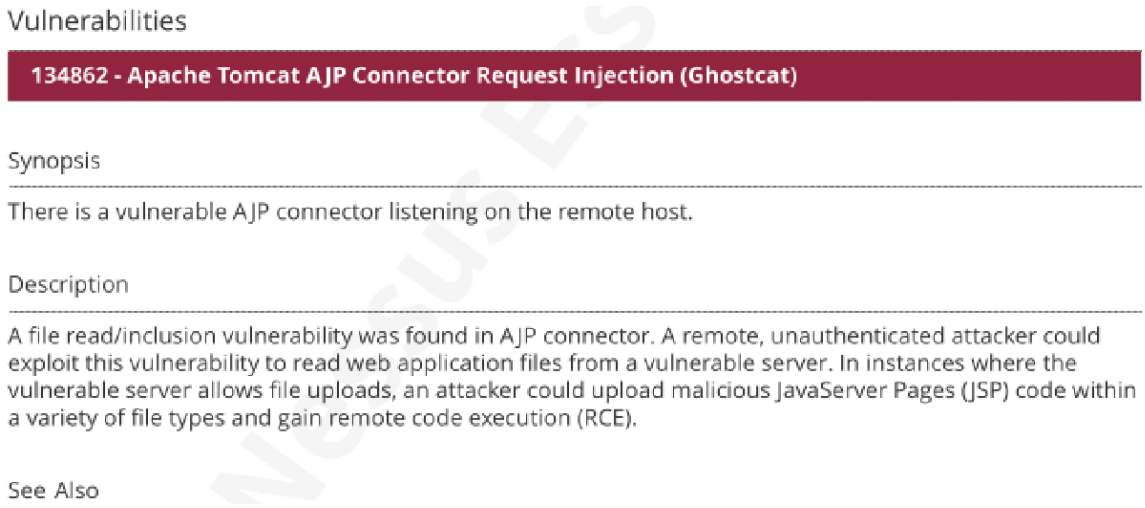

Figura 5

Questa è una vulnerabilità di tipo "***File inclusion***" rilevata su un componente di ***Apache Tomcat*** anche nota come ***GHOSTCAT***, che permette ad un utente remoto di leggere e caricare file su un server vulnerabile. La soluzione proposta dal report è quella di aggiornare la configurazione del componente in questione, visto il rischio critico della vulnerabilità sicuramente questa avrà una priorità elevata.

Andiamo a considerarne un altra. ***Figura 6***

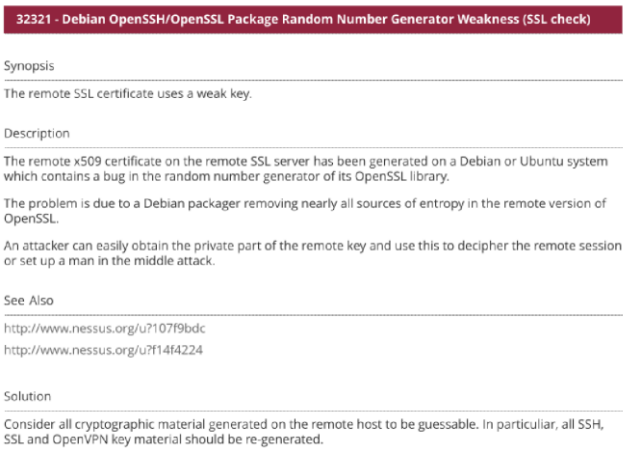

Figura 6.

Nello specifico questa è una vulnerabilità tipica di Debian dovuta ad un bug nella generazione di numeri casuali nelle librerie SSL che a causa di un bug rende predicibili le chiavi crittografiche, la soluzione proposta in questo caso è che tutte le chiavi SSH, SSL e OPeNVPN debbano essere rigenerate. Anche in questo caso il livello di rischio della vulnerabilità in questione è ***critico***.

Un' altra minaccia rilevata sempre con rischio ***critico*** è la "***Bind shell backdoor detection***", in questo caso è presente una porta aperta sull' host che potrebbe essere sfruttata da un eventuale attaccante per connettersi ed inviare comandi in maniera diretta.