S5-L3
Vulnerability scanning

Emanuele Benedetti

9 gennaio 2025

Consegna

Lo studente effettuerà 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:

- Configurazione della Scansione:
    - Target: Metasploitable
    - Porte: Solo le porte comuni (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.
- Esecuzione della scansione:
    - Avvia la scansione configurata su Nessus.

    - Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.
- Analisi del Report:
    - Una volta completata la scansione, scarica e analizza il report generato da Nessus.
    - Per ogni vulnerabilità riportata:
        - Leggi attentamente la descrizione fornita nel report.
        - Approfondisci ulteriormente utilizzando i link e le risorse suggerite nel report.
        - Cerca ulteriori informazioni sul Web, se necessario.

Obiettivi dell'Esercizio:

1. Pratica con Nessus:
    a. Imparare a configurare e avviare scansioni con Nessus.
    b. Capire come restringere le scansioni a porte specifiche.
2. Familiarizzazione con le Vulnerabilità:
    a. Conoscere alcune delle vulnerabilità comuni che si possono incontrare.
    b. Imparare a interpretare i risultati dei report di Nessus.
    c. Sviluppare la capacità di approfondire e comprendere le vulnerabilità utilizzando risorse aggiuntive.

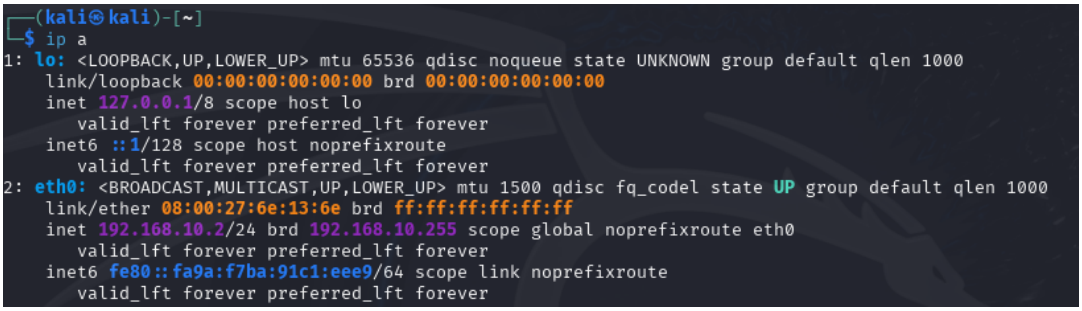
Risultato Atteso:

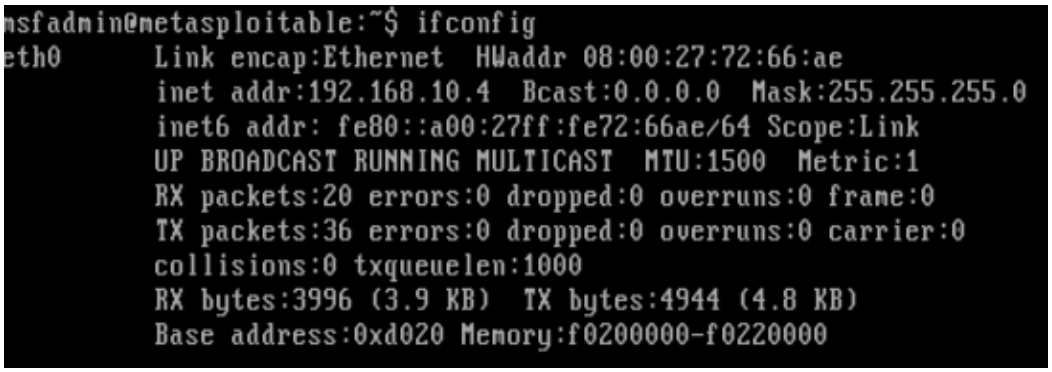
- Configurare e avviare scansioni di vulnerabilità con Nessus.
- Analizzare i report di vulnerabilità e comprendere le informazioni fornite.

Svolgimento

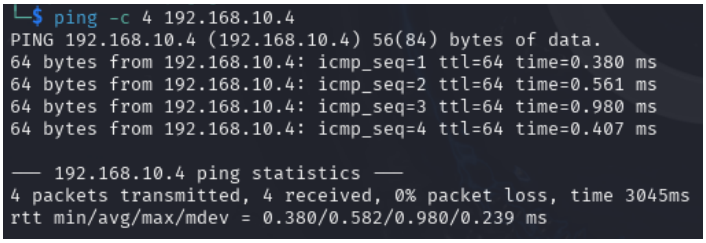
Configurazione delle macchine

Per eseguire l'esercizio, per prima cosa configuriamo le macchine virtuali. Ho eseguito i passaggi per impostare le macchine Kali Linux e Metasploitable2 su "rete interna" in modo tale che possano comunicare tra di loro in un ambiente sicuro. Ho impostato manualmente gli indirizzi IP delle macchine attribuendo a Kali 192.168.10.2 e 192.168.10.4 a Metasploitable.



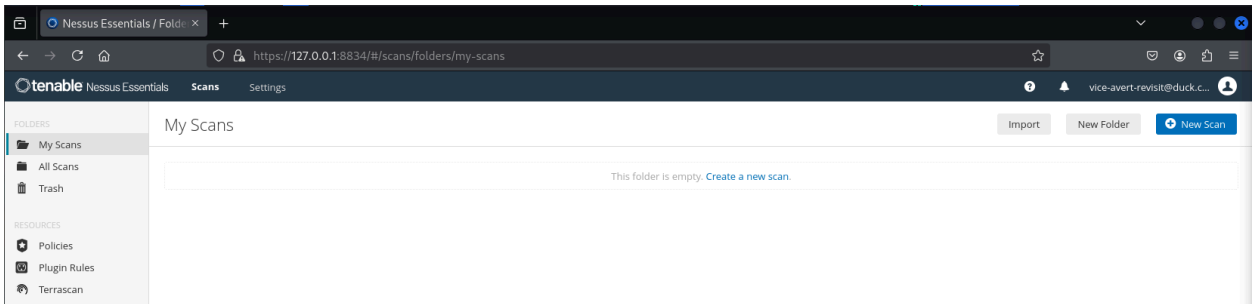


Ho quindi verificato da Kali la corretta configurazione e il dialogo tra le macchine eseguendo un comando di ping verso Metasploitable2 (**ping -c 4 192.168.10.4**).



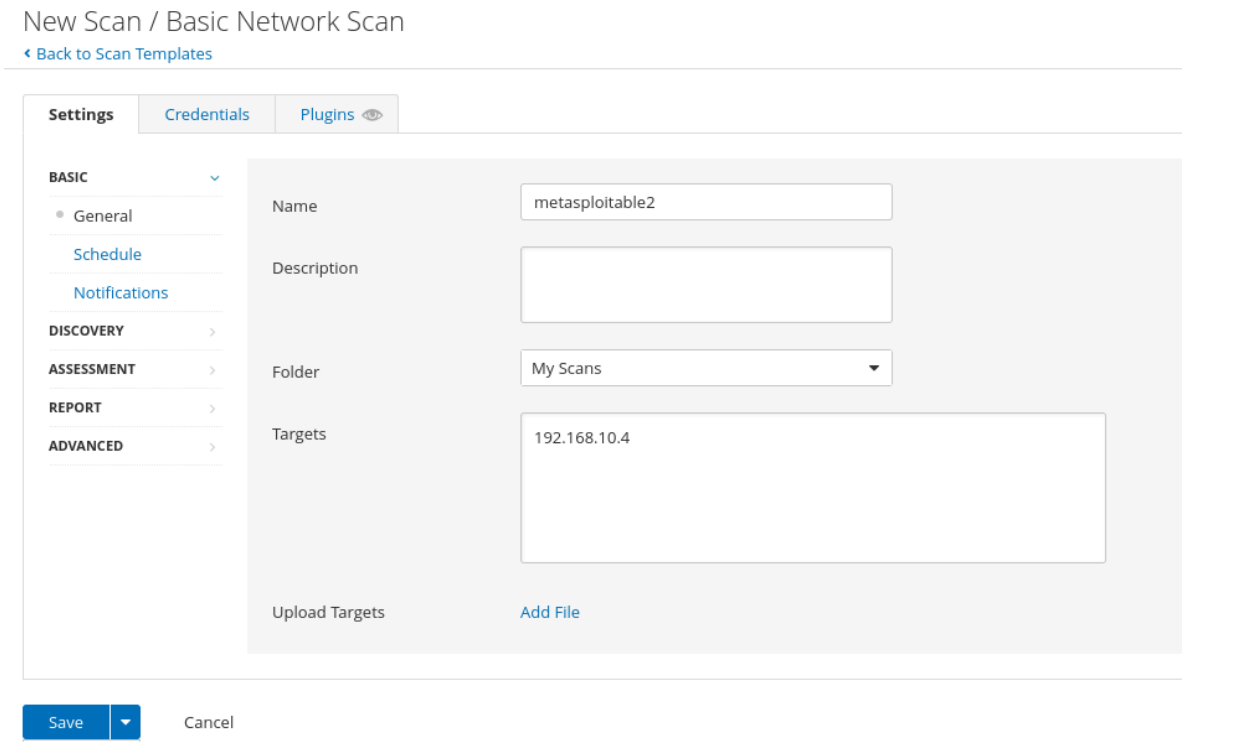
Configurazione Nessus e avvio scansione

Dopo aver configurato le macchine, ho acceduto al client Nessus (tramite l'indirizzo della macchina ospitante il server Nessus in ascolto sulla porta di default 8834)

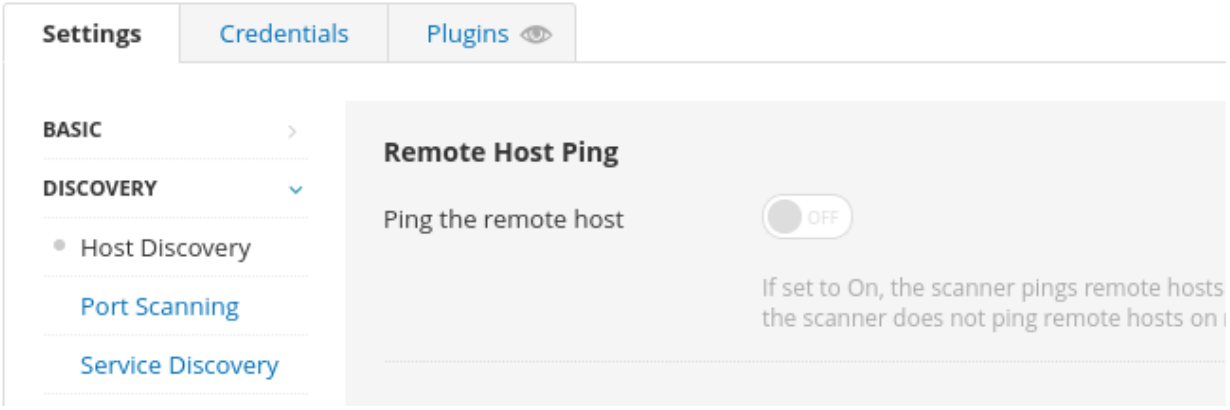


Tramite l'apposito bottone ho creato una nuova scansione, in particolare ho scelto una "**Basic Network Scan**".

Nella sezione seguente ho indicato le impostazioni generali per eseguire la scansione, impostando ad esempio l'IP della macchina target.

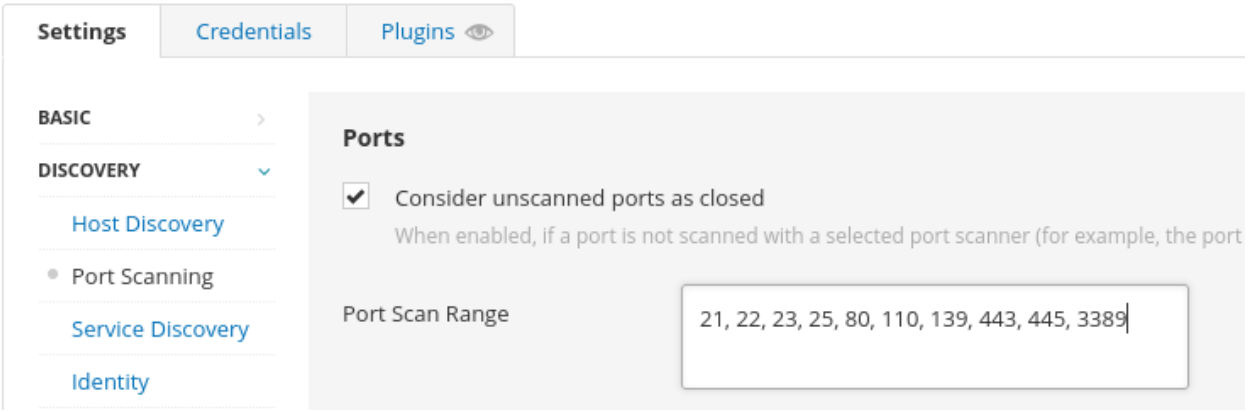


Nella sezione **discovery** ho selezionato la modalità di scansione *custom.* In questo modo ho scelto di disattivare il ping sull'host remoto, per accorciare i tempi di esecuzione della scansione



Poiché era richiesta solamente la scansione delle porte più comuni, ho modificato la sezione *port scanning* indicando solamente le porte 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389 come richiesto dalla consegna.

Ho spuntato la casella *consider unscanned port as closed* per far si che non vengano scansionate le porte non richieste nel range indicato.



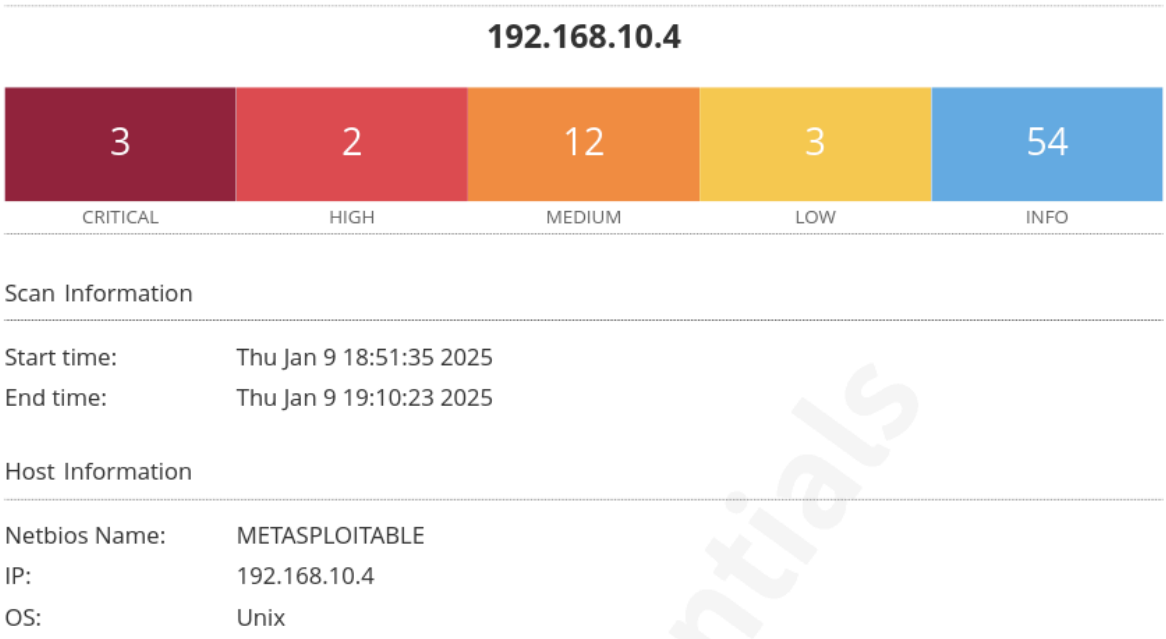
Ho infine selezionando SYN come modalità di port scanner.

Ho quindi lanciato la scansione ed atteso il completamento dei risultati.

Analisi vulnerabilità

Al termine della scansione, Nessus fornisce un'analisi dei risultati e la lista delle vulnerabilità trovate. Il programma inoltre genera un report dettagliato, esportabile in vari formati per l'analisi completa.

Il report mostra inizialmente un interessante riassunto della scansione effettuata, indicando l'indirizzo IP del target, alcune caratteristiche della macchina acquisite tramite la scansione (sistema operativo, indirizzo MAC), orari di inizio e fine scansione ed un grafico che riassume la tipologia di vulnerabilità riscontrate, classificate per livello di criticità.



Come mostrato, Nessus ha rilevato 3 vulnerabilità critiche, che richiedono massima e urgente attenzione.

La classificazione del livello di criticità avviene tramite il **CVSS v3.0** (Common Vulnerability Scoring System), un sistema di valutazione del rischio utilizzato per determinare la gravità delle vulnerabilità di sicurezza di un sistema informatico.

Di seguito riporto le vulnerabilità che richiedono la maggiore attenzione e per ognuna fornisco la descrizione, la soluzione consigliata e la valutazione del rischio:

1. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (porta 22)**
    a. **Descrizione**: La chiave SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
    Il problema è dovuto al fatto che un pacchettizzatore Debian ha rimosso quasi tutte le fonti di entropia dalla versione remota di OpenSSL.
    Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o per configurare un attacco man-in-the-middle.
        i. **Soluzione**: Considera tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutte le chiavi SSH, SSL e OpenVPN dovrebbero essere rigenerate.
        ii. **Criticità CVSS v2.0 base score**: 10

2. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) (porta 25)**
    a. **Descrizione**: Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto al fatto che un pacchettizzatore Debian ha rimosso quasi tutte le fonti di entropia dalla versione remota di OpenSSL. Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o per configurare un attacco man-in-the-middle.
        i. **Soluzione**: Considera tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutte le chiavi SSH, SSL e OpenVPN dovrebbero essere rigenerate.
        ii. **CVSS v2.0 base score**: 10

3. **SSL Version 2 and 3 Protocol Detection (porta 25)**
    a. **Descrizione**: Il servizio remoto accetta connessioni criptate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:
    -Uno schema di padding insicuro con i cifrari CBC.
    -Schemi di negoziazione e ripristino della sessione insicuri.
    Un attaccante può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decifrare le comunicazioni tra il servizio affetto e i client. Sebbene SSL/TLS abbia un metodo sicuro per scegliere la versione più alta supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano versioni migliori), molti browser web implementano questa funzionalità in modo insicuro, consentendo a un attaccante di ridurre il livello di sicurezza della connessione (come nel caso del POODLE). Pertanto, si raccomanda di disabilitare completamente questi protocolli.
    Il NIST ha stabilito che SSL 3.0 non è più accettabile per comunicazioni sicure. A partire dalla data di applicazione stabilita nella PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia forte" del PCI SSC.
        i. **Soluzione**: Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.
        Utilizza invece TLS 1.2 (con suite di cifratura approvate) o versioni superiori.
        ii. **Criticità CVSS v3.0 base score**: 9.8

Si segnala inoltre che queste sono solamente le vulnerabilità critiche riscontrate dalla scansione ma, come mostrato dal riassunto del report, vi sono ulteriori vulnerabilità da risolvere per mettere in sicurezza la macchina target.

Va tenuto in considerazione inoltre, che per attenersi alla richiesta, sono state scansionate solamente le porte più comuni (nello specifico le porte 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389) e dunque c'è motivo di credere che vi possano essere ulteriori criticità nelle altre porte non scansionate ed attive sulla macchina target.

Nota: Il rischio di alcune delle vulnerabilità elencate, è valutato tramite CVSS v2.0 e non 3.0 poiché tali vulnerabilità sono molto vecchie e non sono state valutate con il nuovo standard