Consegna S5-L3

Consegna: Scansione Vulnerabilità con Nessus

⚜️ **Tag:** #pentesting #nessus #scansione

Obiettivo:
Lo studente dovrà effettuare un Vulnerability Scanning sulla macchina **Metasploitable** utilizzando **Nessus**, concentrandosi sulle porte comuni. Questo esercizio è finalizzato a:

- Fare pratica con lo strumento Nessus.
- Configurare correttamente le scansioni.
- Familiarizzarsi con alcune 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:**
        - Basic Network Scan: Configurazione predefinita.
        - Advanced Scan: Configurabile in base alle esigenze specifiche.
2. **Esecuzione della Scansione**
    - Avvia la scansione configurata su Nessus.
    - Assicurati che tutte le porte specificate siano state analizzate.
3. **Analisi del Report**
    - Scarica e analizza il report generato da Nessus.
    - Per ogni vulnerabilità riportata:

- Leggi attentamente la descrizione fornita.
- Approfondisci ulteriormente con i link e risorse suggerite.
- Cerca ulteriori informazioni sul Web, se necessario.

Obiettivi dell’Esercizio

1. **Pratica con Nessus:**
   - Imparare a configurare e avviare scansioni.
   - Comprendere come restringere le scansioni a porte specifiche.
2. **Familiarizzazione con le Vulnerabilità:**
   - Conoscere alcune vulnerabilità comuni.
   - Imparare a interpretare i risultati dei report.
   - Approfondire le vulnerabilità utilizzando risorse aggiuntive.

Risultato Atteso

Al termine dell'esercizio, lo studente dovrebbe essere in grado di:

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

🔑 Chiavi:

[pentesting, nessus, scansione, vulnerabilità, analisi]