Report Esercitazione: Vulnerability Scanning con Nessus

1. Obiettivo dell'Esercitazione

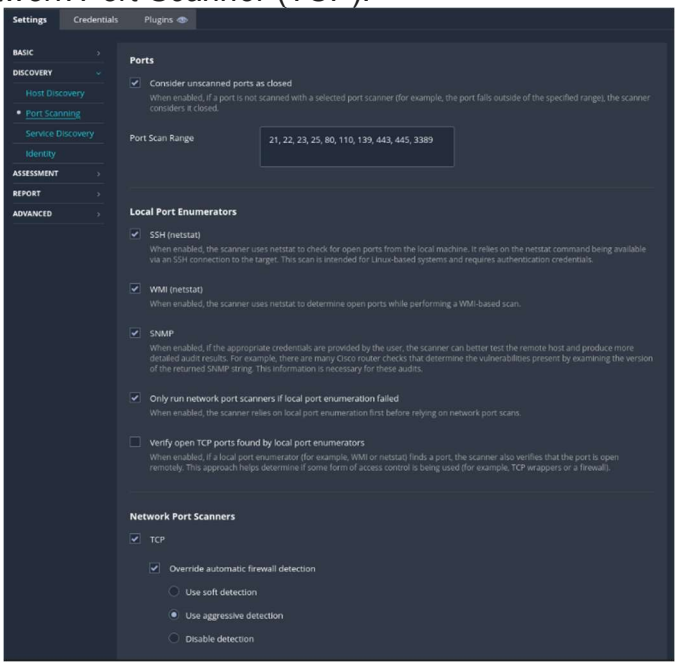
L'obiettivo di questa attività è effettuare un Vulnerability Scanning sulla macchina target **Metasploitable** (IP: 192.168.50.10) utilizzando il tool **Nessus**. L'analisi si concentra specificamente sulle **porte comuni** per identificare servizi attivi, configurare correttamente i parametri di scansione e interpretare i risultati ottenuti.

---

2. Configurazione della Scansione

Come richiesto dalla traccia, è stata configurata una nuova scansione su Nessus. Nella sezione **Discovery > Port Scanning**, è stato definito manualmente il range di porte da analizzare.
I parametri impostati sono i seguenti:

- **Port Scan Range:** 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389.
- **Impostazioni aggiuntive:** Sono stati abilitati i *Local Port Enumerators* (SSH, WMI, SNMP) e il *Network Port Scanner* (TCP).



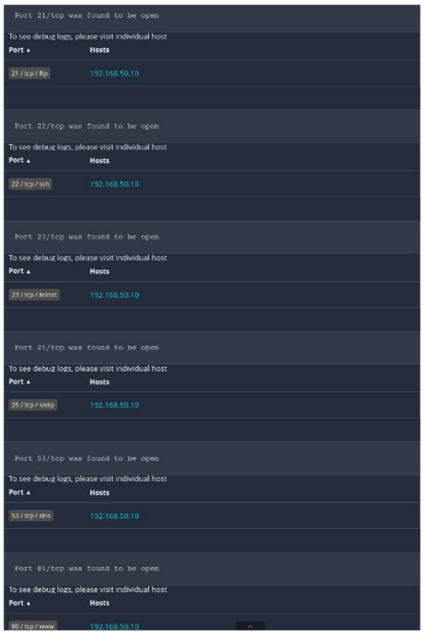
(Descrizione: Configurazione del "Port Scan Range" nelle impostazioni di Nessus).

---

3. Esecuzione e Risultati della Scansione

La scansione è stata lanciata verso l'indirizzo IP target **192.168.50.10**. Il tool ha completato l'analisi rilevando che le porte specificate risultano "Open" (aperte), confermando la presenza di servizi attivi potenzialmente vulnerabili.
Dai risultati è emerso che i seguenti servizi sono attivi e rispondono alle richieste:

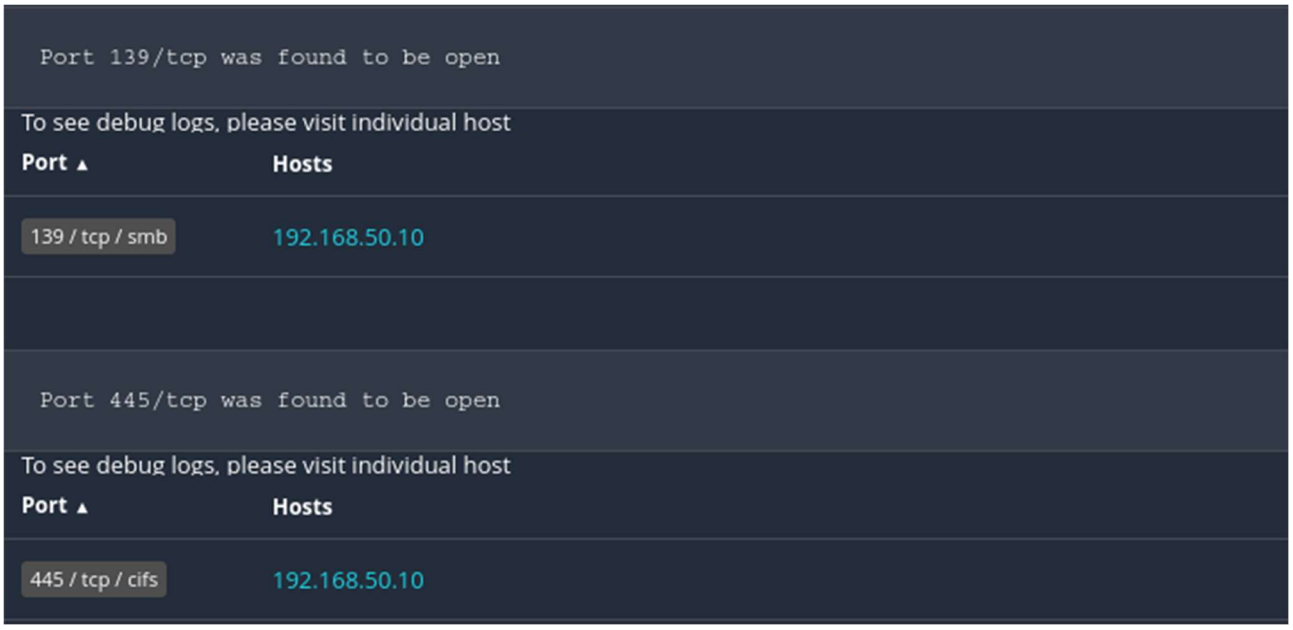
- **Porta 21 (FTP) & 22 (SSH):** Servizi di trasferimento file e accesso remoto.
- **Porta 23 (Telnet):** Protocollo non cifrato, critico per la sicurezza.
- **Porta 25 (SMTP):** Servizio di posta elettronica.
- **Porta 80 (HTTP):** Server web.



(Descrizione: Log dei risultati che mostra le porte 21, 22, 23, 25 e 80 aperte sull'host 192.168.50.10).

Inoltre, la scansione ha identificato servizi relativi alla condivisione file e reti Windows:

- **Porta 139 (SMB):** Session Service.
- **Porta 445 (CIFS):** Microsoft-DS, spesso soggetto a vulnerabilità critiche (es. EternalBlue).



(Descrizione: Log dei risultati che evidenzia le porte 139 e 445 aperte).

---

4. Analisi e Conclusioni

L'esercitazione ha permesso di verificare con successo la configurazione di una scansione mirata su Nessus, restringendo il campo d'azione alle sole porte di interesse.
L'analisi del report conferma che la macchina Metasploitable espone numerosi servizi su porte standard senza adeguate protezioni (come evidenziato dalla presenza di Telnet sulla porta 23). Questo tipo di scansione è fondamentale per mappare la superficie di attacco di un sistema e procedere successivamente con l'analisi approfondita delle vulnerabilità (CVE) associate a ciascun servizio rilevato.

Studente: Caccamo Rocco Paolo

Corso Epicode: Cybersecurity specialist

Data:07/01/2026