1. **Fingerprint del Sistema Operativo**: Questo passo riguarda l'identificazione del sistema operativo in esecuzione sul target. Per Metasploitable2, solitamente è un sistema operativo basato su Linux.
2. **Scansione SYN**: Questa scansione identifica le porte aperte inviando pacchetti SYN e notando quali risposte indicano porte aperte.
3. **Scansione TCP Connect**: Simile alla scansione SYN, ma stabilisce connessioni TCP complete. Le differenze tra le scansioni SYN e TCP Connect riguardano

principalmente la velocità e la furtività; le scansioni SYN sono più veloci e più discrete poiché non completano la stretta di mano TCP.

4. **Rilevamento delle Versioni**: Questo passo riguarda il rilevamento delle versioni dei servizi in esecuzione sulle porte aperte identificate.

Informazioni Richieste nel Report:

- **Indirizzo IP**: L'indirizzo IP del target Metasploitable2 identificato nella scansione è 192.168.50.101.
- **Sistema Operativo**: Il sistema operativo rilevato è probabilmente una versione di

Linux, come comunemente utilizzato da Metasploitable2.

- **Porte Aperte**: Dalle scansioni, dovresti identificare l'elenco delle porte aperte. Le immagini fornite includono varie porte utilizzate da Apache, SSH, Telnet, FTP, ecc.
- **Servizi e Versioni**: I risultati della scansione mostrano servizi come Apache Tomcat, Bind Shell, SSL, e altri, insieme alle loro versioni specifiche.

In base agli screenshot del report Nessus:

- **Vulnerabilità Critiche**: Sono presenti 8 vulnerabilità critiche, tra cui Apache Tomcat AJP

Connector Request Injection, problemi di rilevamento del protocollo SSL, e altre.

- **Vulnerabilità Alte**: Ci sono 6 vulnerabilità di alta gravità, come ISC BIND Service Downgrade e Samba Badlock Vulnerability.
- **Medio, Basso e Info**: Un elenco completo include vulnerabilità di livello medio, basso e informativo, che indicano varie configurazioni errate e potenziali esposizioni, come suite di cifratura deboli e protocolli deprecati.