1. -O (OS Fingerprinting)

Il parametro -O di Nmap serve per identificare il sistema operativo del target. Nmap utilizza un metodo di fingerprinting, ovvero invia pacchetti al target e analizza le risposte per determinare quale sistema operativo potrebbe essere in uso. Questa tecnica è molto utile per raccogliere informazioni durante un attacco, poiché la conoscenza del sistema operativo può aiutare a identificare vulnerabilità specifiche.

2. -sS (SYN Scan)

Il parametro -sS attiva la scansione SYN, che è una delle modalità di scansione più comuni e veloci. In questo tipo di scansione, Nmap invia un pacchetto SYN (che è il primo passo nel processo di handshake TCP) al target senza completare la connessione. Se il target risponde con un pacchetto SYN-ACK, significa che la porta è aperta. Questo tipo di scansione è considerato relativamente furtivo, poiché non stabilisce mai una connessione completa evitando così di registrare una connessione completa nel log del target.

3. -sT (TCP Connect Scan)

Il parametro -sT attiva una scansione TCP Connect, che è un tipo di scansione più semplice rispetto alla scansione SYN. In questo caso, Nmap cerca di stabilire una connessione TCP completa con il target, completando il processo di handshake (SYN, SYN-ACK, ACK). Questa scansione è più facile da rilevare rispetto alla SYN scan, poiché completa il processo di connessione, ma fornisce risultati affidabili e viene usata quando non si dispone di privilegi di root (necessari per il -sS).

4. -sV (Version Detection)

Il parametro -sV è utilizzato per rilevare le versioni dei servizi in esecuzione sulle porte aperte. Nmap invia pacchetti speciali a queste porte per determinare quali servizi (e le relative versioni) sono in ascolto. Questo è fondamentale per identificare vulnerabilità specifiche legate a versioni di software conosciute. Ad esempio, se un servizio come Apache o SSH è vulnerabile in una determinata versione, Nmap può rilevare questa versione e aiutare a concentrarsi su potenziali exploit.

Quindi in conclusione:  
  
La scansione -O è utile per identificare il sistema operativo e può fornire informazioni vitali per ulteriori attacchi.

La scansione -sS è veloce e furtiva, utile per identificare le porte aperte senza stabilire una connessione completa.

La scansione -sT è più affidabile ma meno furtiva, in quanto completa il processo di connessione TCP.

La scansione -sV è cruciale per identificare le versioni dei servizi in esecuzione sulle porte aperte, permettendo di identificare vulnerabilità specifiche.