

nmap

tool multi uso per scansione
porte , determinare OS (Operative system) ,
enumeration grabbing ecc

CERCARE VULNERABILITÀ
SU UN TARGET

nmap --script=vuln
TARGET

PER BANNER GRABBING
nmap -sV TARGET

TIMING

a scelta del livello di timing in Nmap dipende dall'obiettivo della scansione e dalle condizioni della rete. Se si desidera essere discreti e non attirare l'attenzione, è meglio utilizzare i livelli più bassi. Se si ha bisogno di una scansione rapida e si è in un ambiente controllato, i livelli più alti possono essere appropriati.

- T0 (Paranoid): Questo livello è estremamente lento e progettato per evitare il rilevamento da parte di sistemi di intrusion detection. Utilizza un intervallo di attesa molto lungo tra i pacchetti e può richiedere molto tempo per completare la scansione.
- T1 (Sneaky): Ancora più lento di T0, questo livello è utile per scansioni furtive. Riduce ulteriormente la velocità per minimizzare il rischio di essere rilevati.
- T2 (Polite): Questo livello è più equilibrato. Riduce la velocità della scansione per non sovraccaricare la rete e per ridurre il rischio di essere notati. È utile in ambienti in cui è necessario essere discreti.
- T3 (Normal): Questo è il livello di default di Nmap. Fornisce un buon equilibrio tra velocità e discrezione. È adatto per la maggior parte delle scansioni.
- T4 (Aggressive): Questo livello è più veloce e adatto per reti affidabili e veloci. Aumenta la velocità della scansione, ma potrebbe essere più facilmente rilevabile.
- T5 (Insane): Questo è il livello più veloce e può essere utilizzato solo su reti molto veloci e affidabili. È altamente probabile che venga rilevato e può causare congestione sulla rete.

TCP Connect Scans (-sT)
SYN "Half-open" Scans (-sS)
UDP Scans (-sU)

TCP Null Scans (-sN)
TCP FIN Scans (-sF)
TCP Xmas Scans (-sX)

PER SCANSIONARE INTERVALLI USO :

nmap -sn 192.168.0.0/24
NOTA :
posso usare /8 /16 /24