Øvelse 40 - Nmap Basic Port Scans

Information

NMAP er et netværksscanningsværktøj skrevet af Gordon Lyon (Fyodor). NMAP kan anvendes til at afdække hvilke enheder og services der findes på et netværk. Værktøjet anvendes af både netværksprofessionelle og trusselsaktører til at teste et netværk med henblik på at afdække eventuelle svagheder der kan udnyttes i et angreb. NMAP hører under Mitre Attack taktikken T1595 Active Scanning. Vi har ikke berørt Mitre Attack frameworket endnu men prøv at klikke på linket og find ud af hvad der står om T1595 teknikken og under teknikker (sub-techniques).

NMAP anvender primært TCP, UDP og ping til at udføre sine scanninger men kan også eksekvere scripts der i yderste tilfælde kan lave deciderede angreb på netværksenheder. Derfor er det muligt at overtræde lovgivning og politikker hos for eksempel datacentre og hosting virksomheder. Det betyder at NMAP bør anvendes med forsigtighed, især når i er i gang med at lære det. En god måde at sikre sig at anvendelsen ikke overtræder lovgovning etc. er at anvende NMAP på lukkede netværk, det kan være på tjenester som TryhackMe eller Hackthebox men også på det netværk i har bag jeres opnsense (f.eks 192.168.1.0/24). NMAP er installeret på Kali Linux og det er fra Kali i skal lave denne øvelse.

Formålet med øvelsen er at lære NMAP at kende og samtidig bruge wireshark til at observere hvordan netværkstrafikken som NMAP laver ser ud.

Instruktioner

1. Alle medlemmer i gruppen logger på THM fra deres Kali maskine i virtual box og finder rummet Nmap Basic Port Scans
2. Gennemfør rummet i samme tempo, brug hinanden når i arbejder til at besvare spørgsmål og lave fejlfindign og problemløsning.
3. Lav en samlet dokumentation på jeres gruppes gitlab over havd i har lært om NAMP og hvad det kan bruges til.

Denne kan findes gruppens Gitlab side: Cryptic

Ressourcer

- Cryptic
- Gitlab: UCL

- Nmap.org
- TryHackMe: Nmap Basic Port Scans

2026-02-20 08:38:27