Øvelse 10 – Aktiv Rekognoscering

Information

I denne øvelse skal du arbejde med **aktiv rekognoscering** – altså direkte og målorienteret indsamling af tekniske oplysninger om et system.

Du skal bruge værktøjer som:

- **Nmap** til port- og service-scanning
- **Gobuster** til path-enumeration via wordlists

Øvelserne fokuserer på at lære praktiske teknikker og værktøjsbrug – men også på at kunne analysere og dokumentere resultaterne.

> **Husk:** Gem og genbrug de wordlister, du udarbejder til crAPI – de skal bruges i senere øvelser og som dokumentation.

Instruktioner

1. **Installer nødvendige værktøjer**
   - Følg afsnittet **Prerequisites**
   - Du skal sikre, at `nmap`, `gobuster`, og `OWASP ZAP` virker korrekt.
2. **Øvelse 1 – Nmap all ports**
   - Udfør en fuld portscanning
   - Dokumentér hvilke porte der er åbne
3. **Øvelse 2 – Nmap service scan**
   - Udfør en service detection (`-sV`) for at identificere hvilke services der kører
   - Sammenlign resultaterne med din portscan
4. **Øvelse 3 – Gobuster med `common.txt`**
   - Brug `gobuster` til at brute-force paths på crAPI
   - Gem resultaterne og notér relevante endpoints
5. **Øvelse 4 – Mere i dybden med `common.txt`**
   - Tilføj evt. nye paths til din samlede wordlist
6. **Øvelse 5 – Mere i dybden med `api-endpoints.txt`**

- Tilføj evt. nye paths til din samlede wordlist

7. **Test dine egne wordlister**
   - Du har undervejs bygget dine egne wordlists (crAPI)
   - Brug `gobuster`, `browser` eller `Burpsuite` til at teste dem

Links og ressourcer

- Nmap man page
- Gobuster - Github page

Last update: 2026-09-13 18:26:38