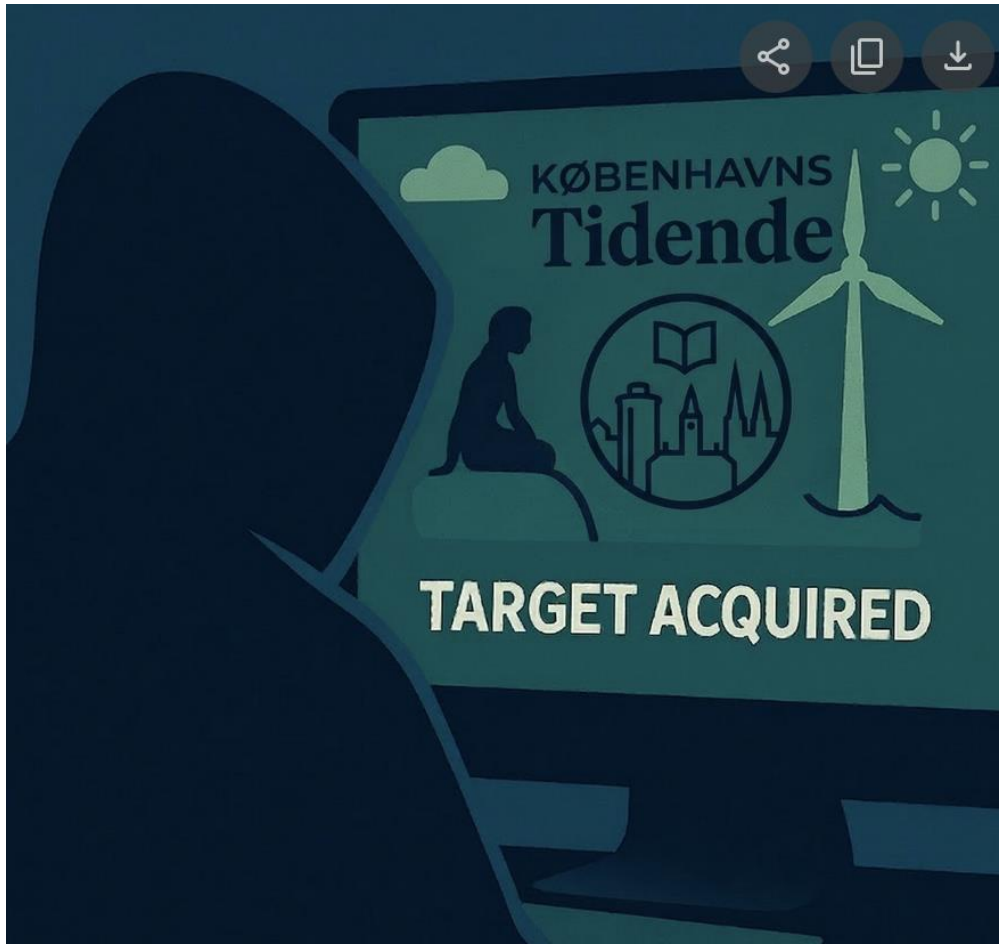
defend Denmark

LIVE HACKING

En moderne dusørjæger



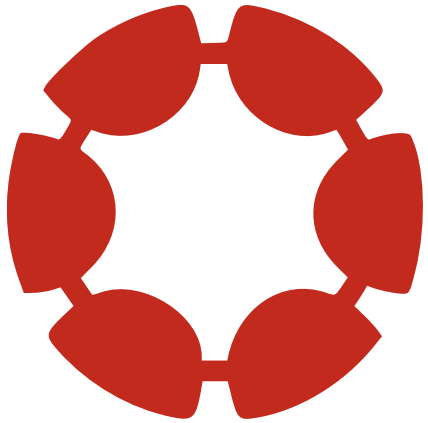
BUG BOUNTY HUNTING OG EN HACKERS VÆRKTØJSKASSE

HVEM ER HACKEREN ?

- ***Emil Christian Hørning***
- Uddannet inden for cybersikkerhed
- White-hat hacker med 10 års erfaring
- Moderne dusørjæger – Finder fejl og bliver betalt for at finde dem
- CEO i Defend Denmark – Startup virksomhed der forbinder danske virksomheder med danske etiske hackere

Dansk platform til at arbejde med danske freelance etiske hackere

1. Danske freelance etiske hackere finder sårbarheder I vores kunder
2. Rapporterer det til Defend Denmark
3. Defend Denmark verificererer og er I kontakt med kunden
4. Kunden får information om sårbarheden
5. Kunden betaler en ***dusør*** alt efter hvor slem sårbarheden er
6. Systemet kaldes bug-bounty



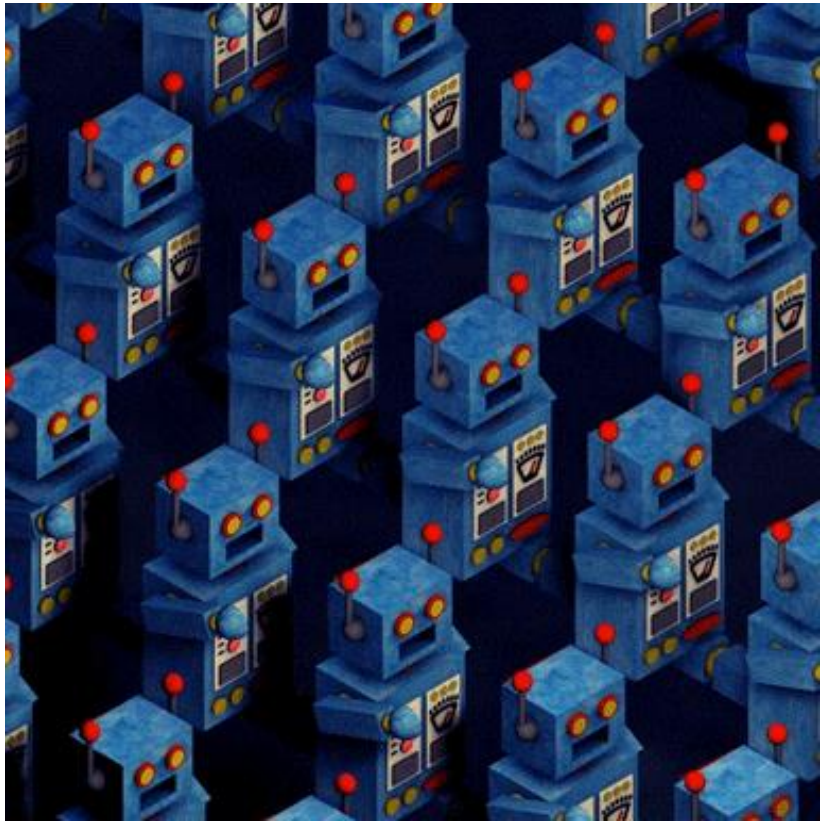
defend Denmark

Hvem er målet?

- Københavns Tidende
- Stor mediekoncern i København
- 500+ medarbejdere
- Tager sikkerhed seriøst, men har også en del legacy
- Hjemmeside: kobenhavns-tidende.dk

Men! Før vi går i gang

- Det ville ikke være en tech talk uden AI
- I Defend Denmark har vi udviklet vores egen **AI Defender**
- En automatisk hack-bot som hjælper med at identificere sårbarheder
- Vi giver den samme opgave, hack *kobenhavns-tidende.dk*



1. Reconnaisance

- **Mål:** Kortlægge hovedstadsenergi.dk’s angrebsflade

Src: palo alto - https://www.paloaltonetworks.ca/cyberpedia/attack-surface-ass

1. Reconnaisance - demo

- **Værktøjer:** Projectdiscoverys **httpx** og **subfinder**

Projectdiscovery.io

Tip 1 til beskyttelse - Recon

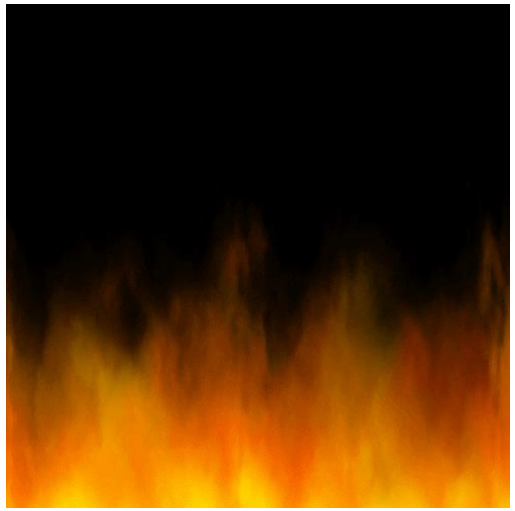
- **Kend din angrebsflade før trusselsaktørerne gør**
- Hold styr på hvad I eksponerer:
  - Subdomains
  - IP ranges som I ejer
  - Cloud / SaaS løsninger som I køber
- Brug firewall til at fjerne offentlig adgang
- Nedlæg services som ikke aktivt bruges

2. Angreb - Demo

- **Mål:** At bryde ind i et admin portal og se hvad vi kan finde
- **Værktøjer:** Hackerens schweizerkniv: web proxy

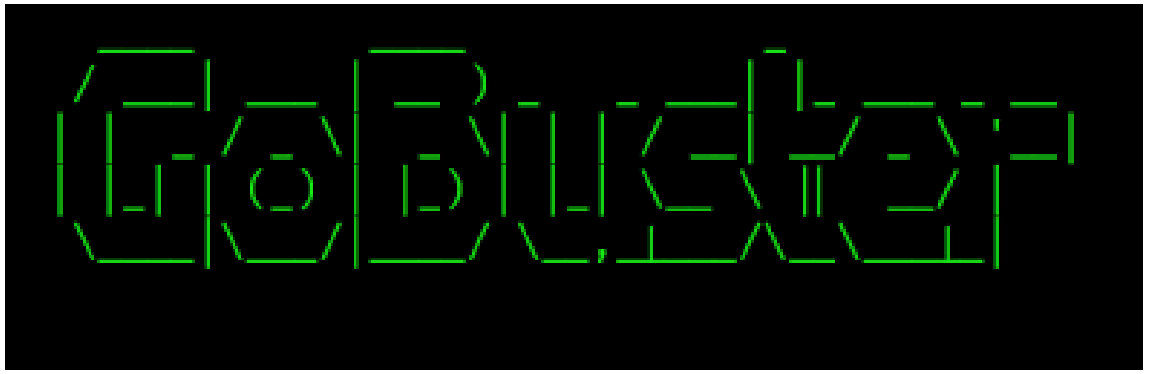
Tip 2 til beskyttelse – Patching / Default creds

- **Antag Alt er Under Angreb**
  - Default credentials ses over alt – skift dem
  - Sørg for at alt er opdateret – unpatched software BLIVER hacket
  - Etablér MFA hvor I kan
- Brug firewall til at fjerne offentlig adgang



3. Eskalering - Demo

- **Mål:** At udnytte admin panelet til at bevæge os videre
- **Værktøjer:** Videre scanning med FFUF eller gobuster



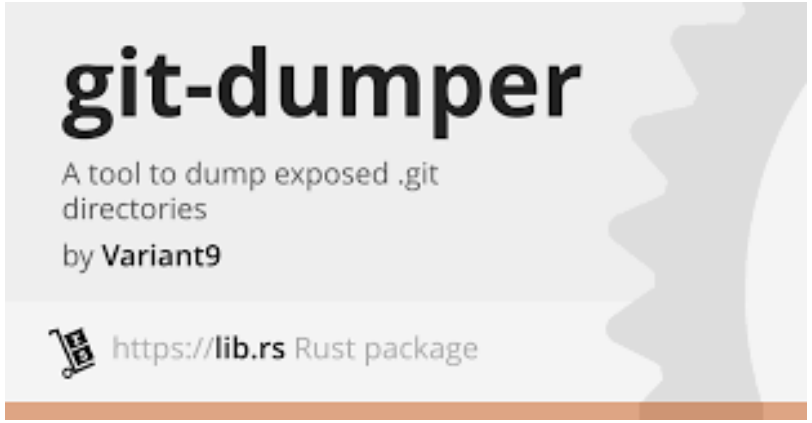
Tip 3 til beskyttelse – uventet og unormal traffik

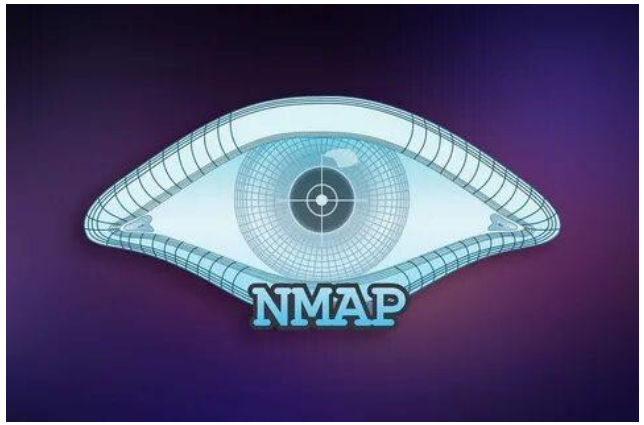
- **Spot ikke-forventet netværkstraffik og luk ned for det**
  - Kommer der lige pludselig mange login forsøg
  - Kommer der lige pludselig mange 404 responses
  - Er trafikken isoleret til en enkelt bruger / IP addresse ? – **Udeluk**

- **Brug Web Application Firewalls**
  - Hjælper med at blokere mange forsøg / ondsindede forsøg
  - Ikke en skudsikker løsning, men hjælper

4. Eksfiltrering - Demo

- **Mål:** At udnytte sårbarhederne til at eksfiltrere sensitive information og vise **impact**
- **Værktøjer:** git-dumper, nmap og mysqldump





Tip 4 til beskyttelse – DevSecOps + separation af miljøer

- **Hav gode rutiner for at håndtere secrets**
  - Brug DevOps værktøjer med fokus på sikkerhed til at håndtere passwords / api keys
  - Aldrig opbevar secrets direkte I koden
  - Følg moderne best practices
- **Lav separation af miljøer**
  - At kompromittere ét system bør ikke påvirke et andet
  - Hav separate miljøer hvor det giver mening


Lad os
tjekke vores
AI Defender

Konklusion

- **Trusselsaktørene er i gang hver dag**
  - De bruger de samme værktøjer som jeg har vist i dag
  - Alle små sprækker er en potentiel åbning til jeres infrastruktur

- **Lav tests og audits**
  - Hjælper jer med at identificere huller og sprækkerne
  - Meget federe at betale for konsulenttimer/dusører frem for en ransom

- **Uautoriseret test er ulovligt i Danmark**
  - Selvom det er gjort med gode intentioner

En opfordring

- **Interessen for cybersikkerhed er stor i dag**
  - Især fra unge mennesker på uddannelser
  - Tak til Industriens Fond for Cybermesterskaberne
- **AI Værktøjer gør det nemmere at identificere sårbarheder**
  - De, ofte, unge folk finder sårbarheder med ai værktøjer
- **Hjælp venlige hackere med at kunne kontakte jer om sårbarheder**
  - Security.txt og en VDP

defend Denmark

Emil Hørning

Fremmer Bugbounty i 🇩🇰 med Defend Denmark | OSCP, OSCE3