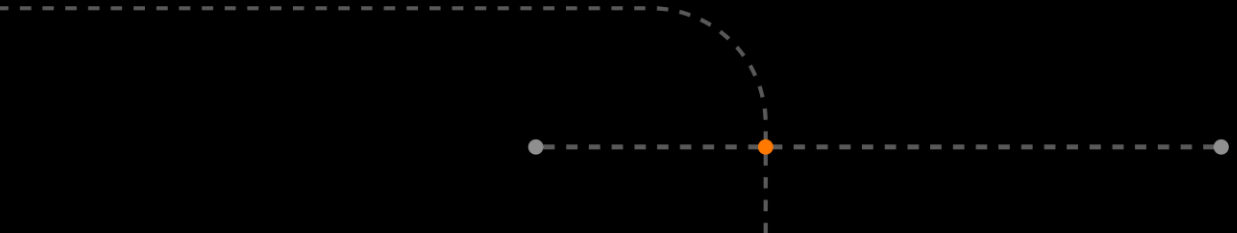
Orange
Cyberdefense

Hvorfor bryte seg inn når man kan gå gjennom døren...

Ragnhild Sageng

20.09.2022



orange™

Hei!

- Ragnhild Sageng, Etisk hacker spesialisering innen social engineering
- IT fylkeskommunalsektor
- Speaker DEFCON og Sikkerhetsfestivalen
- Orange Cyberdefense Red Team: spesialisert på inntrengningstester, adversary simulation, red og purple teaming
- Typiske oppdrag: Ransomware simulering, assumed breach, eksterne til interne inntrengningstester og TIBER-NO/EU

Dagens prat...

- Hva er social engineering?
- Angrepstyper
- Hvordan jobber en angriper, og en pentester?
- Historie fra virkeligheten
- Hvordan man kan beskytte seg

Hva er social engineering?

Social engineering, kalles ofte sosial manipulasjon på norsk:

- Teknikker som brukes for å få et menneske til å utføre en handling eller utgi informasjon, uavhengig av om det er til deres beste eller ikke.

Phishing og Smishing

- **Phishing**
  - Når angripere sender en epost for å få noen til å trykke på en lenke, eller gi ut informasjon.
- **Smishing**
  - Når angripere sender ut SMS med lenker, eller prøver å få ut informasjon fra deg via SMS.
- **Sosiale medier og chatter**
  - Meldinger på sosiale medier og i chatter kan og være phish.

Spearphishing og Whaling

- **Spearphishing**
  - Når angripere går ett er bestemte arbeidsgrupper, et firma, eller individer
- **Whaling**
  - Når angripere går etter sjefer og folk i nøkkelposisjoner

Disse angrepene er veldig skreddersydde og kan være vanskelig å oppdage.

Vishing

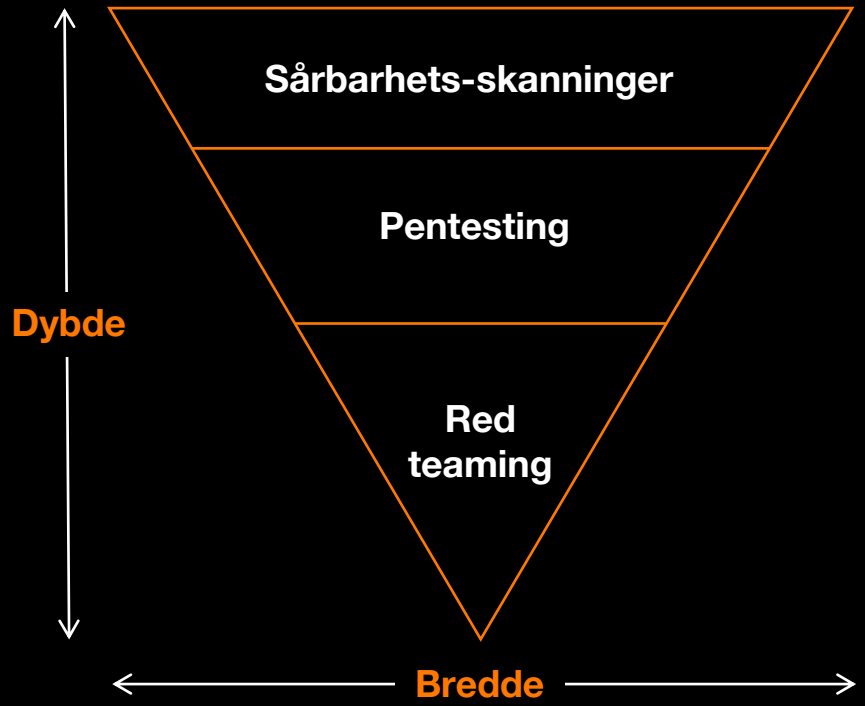
- Telefonsamtaler hvor noen prøver å få ut informasjon
- Microsoft scam
- Utgir seg for å være bank eller politi
- Oppringing fra utlandet
- Spoofing av norske numre

Hva kan skje når man trykker på lenken eller svarer?

- Ransomware
- Keyloggere
- Bli lurt til å oppgi informasjon
  - Kortinformasjon
  - Firmainformasjon
  - Personlig informasjon

Hvordan sjekker man at system er sikre?

- Sikkerhetstest avhengig av modenhet og ønsket scope
- Det er lurt å teste både bredt og smalt, samt overfladisk og dypt i systemer



Slik jobber en social engineer pentester

- Fokus på mennesket
- Informasjonsinnhenting
- Pretext
- Debrief
- Etisk forsvarlighet
- Kan være en del av en større red team pentest

Fysiske tester

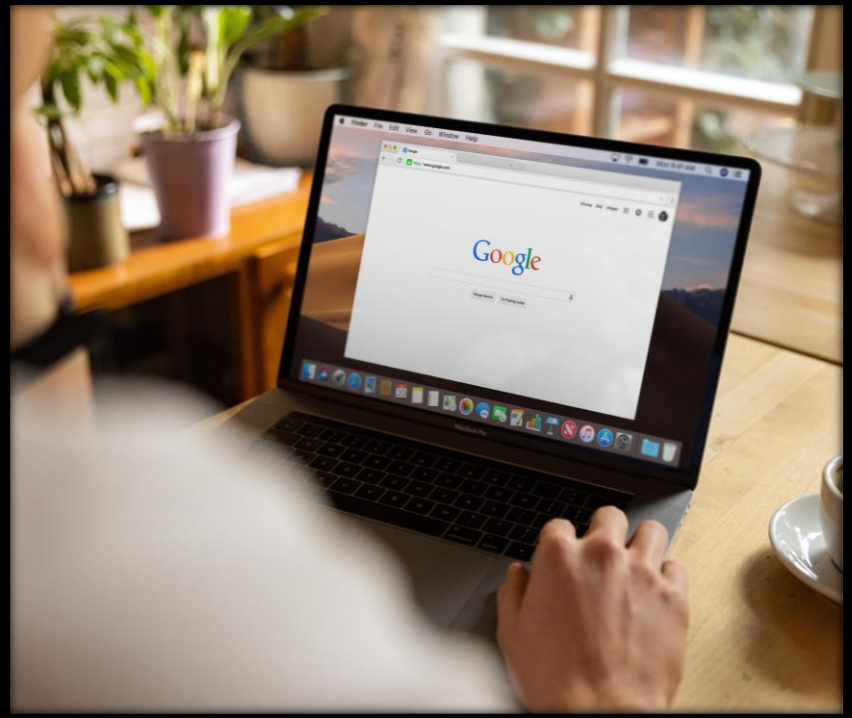
- Prøver å komme seg inn på steder man ikke skal ha tilgang
- Utgir seg for å være noen andre
- Dumpster-diving
- USB penn på gata
- Dokumentere sikkerhetshull

OSINT (Open-Source Intelligence)

- All informasjon man finner åpent på nett

- Eksempler:
  - Sosiale medier
  - Google søk
  - Andre kontoer
  - Google maps
  - Sertifikat informasjon

- OSINT kan gjøres både på individer og på bedrift



Historie fra virkeligheten

- Historien er anonymisert og forhåndsgodkjent for deling.
- Test hos offentlig sektor sin IT avdeling og ekstern lokasjon.
- Navn er fiktive, og presentasjonen inneholder ikke bilder fra lokasjonene.

Hva skulle testes?

Serverrom på en ungdomsskole

Hovedkontoret for IKT-avdelingen

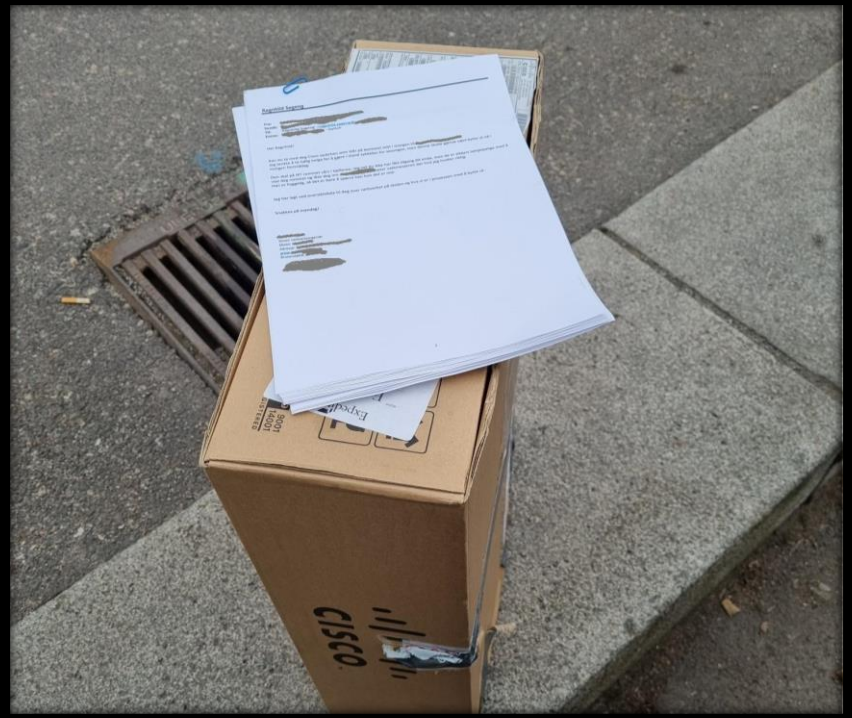
Mål: komme seg inn på serverrom, og se etter andre angrepsvektorer.

I forkant av testen

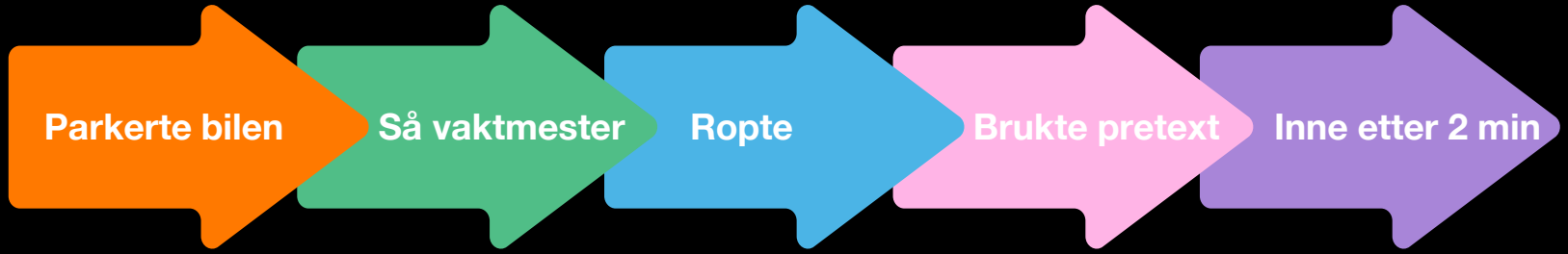
- Samlet informasjon
- Avtalte tidspunkt for testen
- Laget pretexter

Mål 1: Serverrom på skole

- Leste byggeartikler og offentlige dokumenter
- Sjekket kart og sosiale medier for bilder
- Søkte på ansatte i nøkkelroller
  - Vaktmester
  - Rektor
  - IKT
- Plantegninger
  - Inneholdt infrastruktur informasjon



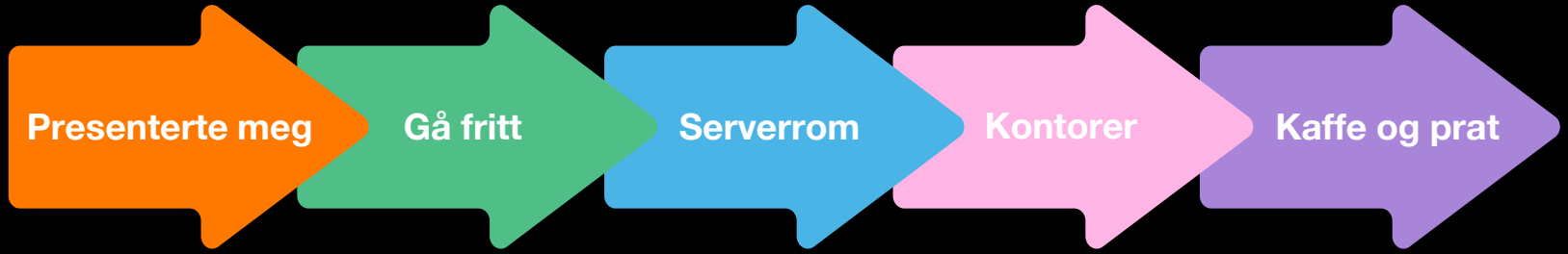
Resultat


Parkerte bilen
Så vaktmester
Ropte
Brukte pretext
Inne etter 2 min

Mål 2: IKT sitt hovedkontor

- Leste byggeartikler og offentlige dokumenter
- Sjekket kart og sosiale medier for bilder
- Søkte på ansatte
- Fant en pretext

Resultat



Hvordan unngå å bli Sosialt manipulert?

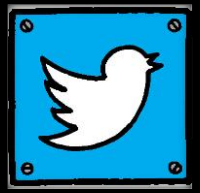
- Opplysning og kursing
- Trening
- Sikkerhetskultur

Vi alle kan bli lurt, det viktigste er å ikke skjule det hvis det skjer.

Orange
Cyberdefense

Takk for meg!

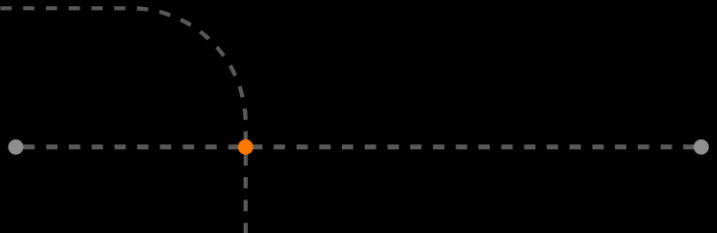
Ragnhild Sageng



@ragnhild_bss

linkedin.com/in/ragnhildsageng

orangecyberdefense.com



orange™