

HUMAN-BASED SOCIAL ENGINEERING

- Impersonating
- Posing as Important User
- Using Third Party Approach
- Calling Tech Support
- Shoulder Surfing
- Dumpster Diving

COMPUTER BASED SOCIAL ENGINEERING

- Phishing
- Email Attachment
- Fake Website

Start your engines!

Exercise for Basic Level

- Explain why this is an important phase of the pentesting proces.
- Make sure that you can show and explain at least 3 different techniques for searching usefull informat
- Find at least 3 people including email adress (not management) that work within a large International LinkedIn
- Find how frontpage of nu.nl looked like 10 years ago using waybackmachine.org
- Discover what URLs are hidden from search robots in robots.txt files of Pentagon and Whitehouse.
- Use tooling for:
 - traceroute to determine path to fontys.nl, fhict.nl
 - determine which DNS and email servers are used by fontys and fhict
 - determine which ip-adressess are used by fhict by whois utility and non whois tool
 - run theharvester utility for domain fontys.nl

Additional Challenges for Advanced level

- Discover contents of Google Hacking database and use following operators:
 - "" and "site" - find all pages containing phrase "geheim" on site defensie/aivd/mivd
 - "inurl" - find login pages on domain whitehouse.gov
 - "filetype" - find all docx files on .gov domains containing phrase "top secret".
- Find 2 different visual trace route tools and discover why its usefull to use
- Discover Maltego (GUI) to collect information regarding from domain philips.com. Can you find:
 - email addresses
 - DNS names
 - Documents and files
- Use the tool social mapper to identify the person on a picture