# Cybersecurity

Linde Nouwen

KdG Karel de Grote Hogeschool

# CyberSecurity Footprinting

Karel de Grote Hogeschool

# Footprinting

- "Reconnaissance"
- Information discovery on client/organization (victim)
- 2 types:
  - Active
    - Direct interaction with target
  - Passive
    - No direct interaction with target

# Footprinting

- Active Reconnaissance
  - Direct interaction with target
    - Ping sweeps (active ips)
    - Service port connection (= software version)
    - Network mapping (network diagram/sw)
    - Social engineering
    - …

# Footprinting

- Passive Reconnaissance
  - No direct interaction with target
    - Adverts/Job openings → technology
    - Who-IS (domain/contact info)
    - Social networks
    - Trash
    - …

# CyberSecurity Footprinting

Basic Tools

Karel de Grote Hogeschool

# Footprinting

- Basic tools:
  - Google (Google Dorks)
  - NSLookup (dig)
  - WHOIS

# Google Dorks

- See:
  - https://en.wikipedia.org/wiki/Googlehacking
  - https://www.cybrary.it/0p3n/google-dorks-easy-way-of-hacking/
  - https://jarnobaselier.nl/google-dorks/
  - https://jarnobaselier.nl/google-dorks-google-hacken-en-beveiligen/
  - https://sansorg.egnyte.com/dl/f4TCYNMgN6

# Google Operators

- **+ (plus symbol):** is used to include words that because they are very common are not included on Google searchresults.
  - For example, say that you want to look for company The X, given that the article "the" is very common, it is usually excluded from the search. If we want this word to be included, then we write our search text like this: Company +The X
- **- (minus symbol):** is used to exclude a term from results that otherwise could include it.
  - For example, if we are looking for banking institutions, we could write: banks - furniture
- **"" (double quotes):** if we need to find a text literally, we framed it in double quotes.
  - Example: "Company X"
- **~ (tilde):** placing this prefix to a word will include synonyms thereof.
  - For example, search by ~company X willalso include results for organization X
- **OR:** This allows you to include results that meet one or both criteria.
  - For example, "Company X General Manager" OR "Company X Systems Manager"
- **site:** allow to limit searches to a particular Internet site. Example: General Manager site:companyX.com
- **link:** list of pages that contain links to the url.
  - For example, searching for link:companyX.com gets pages that contain links to company X website.
- **filetype:** or **ext:** allows you to search by file types.
  - Example: Payment roles + ext:pdf site:empresax.com
- **allintext:** get pages that contain the search words within the text or body thereof.
  - Example: allintext: Company X
- **inurl:** shows results that contain the search words in the web address (URL).
  - Example: inurl: Company X

# Google Operators

- https://www.exploit-db.com/google-hacking-database

# Google Operators

- Specific Defense:
  - Cleanup your stuff (old logs, comments,…)
  - Use Robots.txt
    - User-agent: *
    - Disallow: /
  - Disallow directory listing
    - Apache: .htaccess file

      Options section: indexes
  - GHH (Google Hack Honeypot)
    - Logs bots
    - Configure firewall to disallow

# Nslookup

- DNS-tool
- DNS = FQDN domainname to IP
- Usefull options
  - Open nslookup
  - Type “help”
  - Check options
    - “Server” points tool to specific DNS-server
    - “Set” allows to query DNS for specific types
      - Check DNS documentation for types (MX, NS, …)
    - “ls” to check domain-addresses
- Prepare for IP scan

# WHOIS

- Domain ownership → registrars
  - domain name
  - Registrant: (administrant/billing)
    - name
    - email address
    - physical address
    - contact phone number
    - term
    - payment information…
- Belgium?
  - https://www.dnsbelgium.be
- Others?
  - http://www.iana.org/domains/root/db

# WHOIS

- Links:
  - https://www.betterwhois.com
  - https://geektools.com
  - https://www.all-nettools.com
  - https://www.smartwhois.com
  - https://www.dnsstuff.com
  - https://whois.domaintools.com

# WHOIS

- Database to retrieve information:
  - **http://whois.arin.net**
- Suggestion: pay to keep whois information private.

# CyberSecurity Footprinting

Advanced Tools

Karel de Grote Hogeschool

# Footprinting

- Advanced Tools:
  - Maltego
  - Visual Traceroute
  - E-mail tracker (pro)

# Footprinting

- Maltego:
  - Stand-alone or included in Kali
  - Graphical
  - Overview of internet-information:
  - Network information
  - Resource information
  - Java based
  - https://www.paterva.com/web7/buy/mal tego-clients.php

# Footprinting

- Maltego:
  - "Linked" information on:
    - People
    - Groups of people (social networks)
    - Companies
    - Organizations
    - Web sites
    - Internet infrastructure such as:
    - Domains
    - DNS names
    - Netblocks
    - IP addresses
    - Phrases
    - Affiliations
    - Documents and files

# Footprinting

- Visual Traceroute
  - ❖ Get geographical location of target
    - Client premises
    - Hosted premises (less/not interesting)
  - ❖ Several tools:
    - Client-based
      - Visual IP Trace
      - Visual Route
        - » OK for Reporting
    - Web-based
      - YouGetSignal.com
        - » No reporting

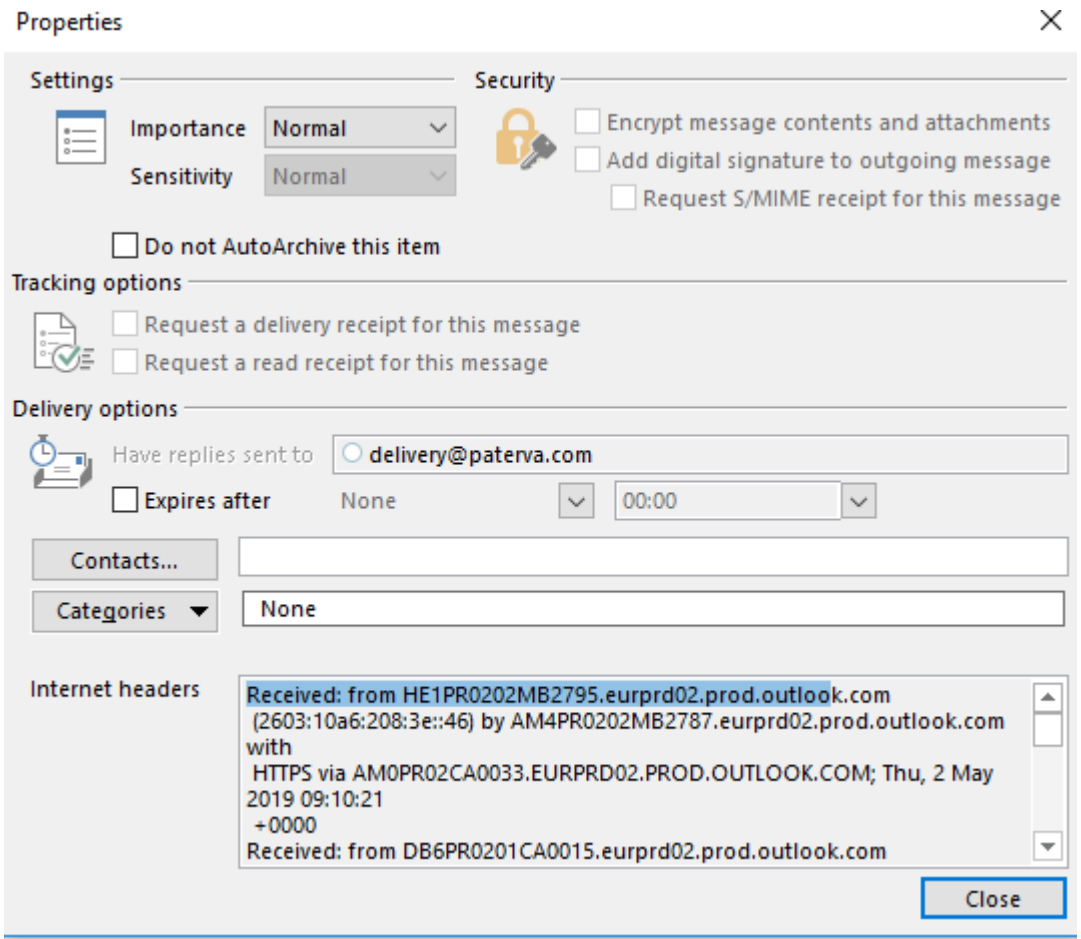
Also: wigle.net

# Footprinting

- E-mail tracker
  - Target has hosted mail infrastructure
  - Try to obtain router-information from mail-chain information:
    - ISP provides public ip to client
    - Mail is sent from client to provider via the ISP’s router infrastructure
    - Mail-header investigation could provide usefull information.

# Footprinting

- E-mail tracker
  - Get E-mail header
    - Different mail-programs = different steps



# Footprinting

- Usefull E-mail header-info
  - Reverse chronological order (low = first)
  - Sending instance:
    - Client
    - Script
  - Route from sending to receiving server

# CyberSecurity
# Footprinting
# The human factor…

KdG Karel de Grote Hogeschool

# Employees

Different strategies:

- Social engineering
  - Phone
  - Mail
- Access to company HW (backdoor)
  - Dropped USB…
- Social media
  - Search blogs:
  - Search Facebook:
    - http://www.spock.com
- Disgruntled (former) employees
  - https://get.sucks/

These domains are volatile
Try to search for examples yourself…

# CyberSecurity Footprinting Defense

Karel de Grote Hogeschool

# Footprinting

- Defense:
  - Difficult
  - Internet = Public
    - Publish only what's needed
    - Also: see "Google Dork" defense
  - Use VPN if possible to access internal information
  - Use a DMZ
  - Use intelligent FWs, IDS/IPS systems
  - Don't post system, app, hw, personal data through social media
  - Train staff (e.g. social engineering)
  - Implement encryption