# Ethical Hacker 3 – Footprinting, Reconnaissance and Social Engineering

* **Explain why this is an important phase of the pentesting process.**

This is an extremely important phase of the pentesting because this is the part in which the testers gather all the information that they need to create a plan. If this phase is taken seriously and is carried out properly, then the rest of the pentest will be significantly easier and the objectives will be much clearer.

* **Make sure that you can show and explain at least 3 different techniques for searching useful information.**

1. **Google searching** -> Google can be used for hacking. By typing very specific queries, many useful and interesting things can be found and made. This is an easy way to find weaknesses on low security websites.
2. **Network information discovery** -> this technique is gathering private information from online databases and is mainly used to discover more about people or entities.
3. **Social network analysis** -> it involves manual searching on social media networks, but this process can also be facilitated by automated tools, such as Social Mapper or Maltego.

* **Find how frontpage of nu.nl looked like 10 years ago using waybackmachine.org**

Graphical user interface, website

Description automatically generated

* **Discover what URLs are hidden from search robots in robots.txt files of Pentagon and Whitehouse.**

If the domain contains a robots.txt file, the administrator of the domain can specify the URLs that should not be taken into consideration by search bots. As a consequence, the search engines will not check these URLs.

The robots.txt file of the Pentagon:

Text

Description automatically generated

The robots.txt file of the White House:

Graphical user interface, text, application, chat or text message

Description automatically generated

* **Find at least 3 people including email adress (not management) that work within a large International Company, for example using social networks like Linkedin**

1. Amanda Yaw – senior visual designer at Zappos family of companiesamandayaw@justsayyaw.com (Zappos)
2. Georgios Gousios - g.gousios@tudelft.nl (Facebook)
3. Jessie Xu - jessieunc@gmail.com (Google)

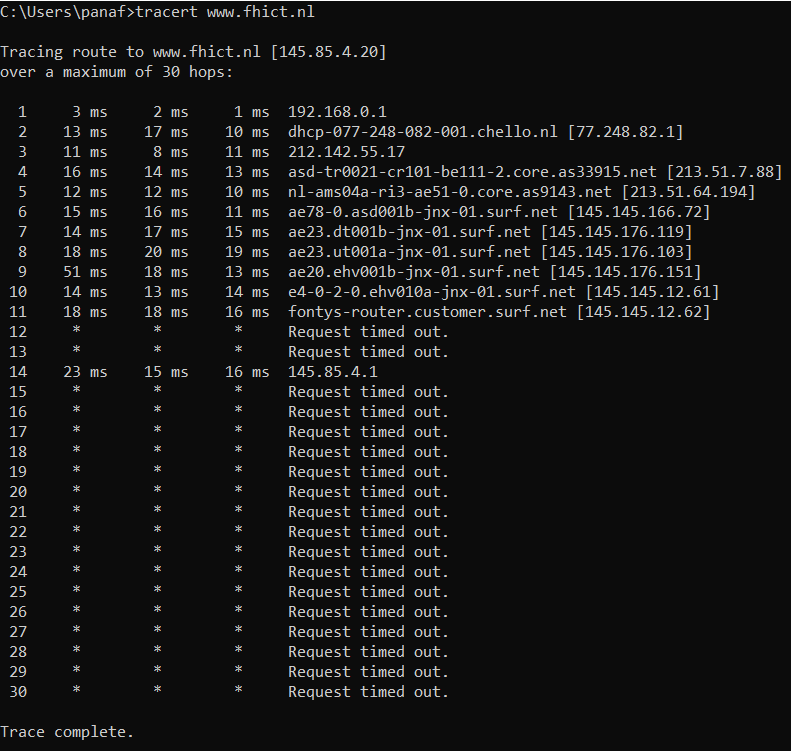
* **Use tooling for:**
* **Traceroute to determine path to fontys.nl, fhict.nl**

Traceroute to fontys.nl: using the command tracert followed by a URL you can display possible routes and measure the transit delays of packets across an IP.

Text

Description automatically generated

Traceroute to fhict.nl: applying the same principles to a different website this time:



* **determine which DNS and email servers are used by fontys and fhict:**

DNS and email servers used by fontys: in order to find out this information, the nslookup instruction is required. After that, I wrote fontys.nl after the generated text.

Text

Description automatically generated

DNS and email servers used by fhict: I have done the same thing, but typed fhict.nl at the end instead:

Text

Description automatically generated

* **determine which ip-adressess are used by fhict by whois utility and non whois tool**

IP addresses used by fhict:

**Whois utility:**

I have searched whois on google to find the website whois.com. I have searched for fontys and the result is this:

Table

Description automatically generated

Table

Description automatically generated with low confidence

**Non whois utility:**

IP adress of fontys.nl:

Text

Description automatically generated

* **run the harvester utility for domain fontys.nl**

Running the Harvester utility by typing the command “theHarvester” in the kali machine terminal:

-d represents the domain, -l represents the limit of the number of results, and -b represents the search engine:

Text

Description automatically generated

Text

Description automatically generated

References:

* <https://www.gohacking.com/use-google-for-hacking/>
* <https://web.archive.org/web/20110225155609/http://www.nu.nl/>
* <https://www.whois.com/whois/fontys.nl>
* <https://www.defense.gov/robots.txt>
* <https://www.whitehouse.gov/robots.txt>