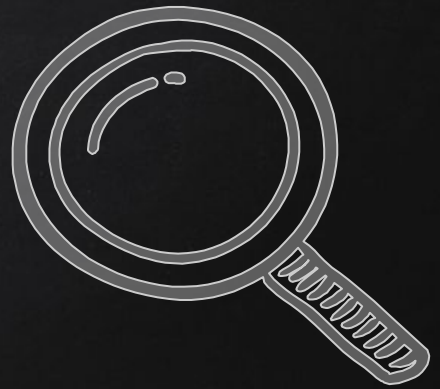
Information Gathering

- IP address.
- Domain name info.
- Technologies used.
- Other websites on the same server.
- DNS records.
- Unlisted files, sub-domains, directories.



Information Gathering

1. Whois Lookup – Find info about the owner of the target.
   → http://whois.domaintools.com/
2. Netcraft Site Report – Shows technologies used on the target.
   → http://toolbar.netcraft.com/site_report?url=
3. Robtex DNS lookup – Shows comprehensive info about the target website.
   → https://www.robtex.com/

Information Gathering

Websites on the same server

- One server can serve a number of websites.
- Gaining access to one can help gaining access to others.

To find websites on the same server:

1. Use Robtex DNS lookup under “names pointing to same IP”.
2. Using bing.com, search for ip: [target ip]

Information Gathering

Subdomains

- Subdomain.target.com
- Ex: beta.facebook.com

Knock can be used to find subdomains of target

1. Download it > git clone https://github.com/guelfoweb/knock.git
2. Navigate to knock.py. > ce knock/knock.py
3. Run it > python knock.py [target]

Information Gathering

Files + Directories

- Find files & directories in target website
- A tool called drib.

```
> dirb [target] [wordlist] [options]
```

For more info run

```
> man dirb
```

Information Gathering

Maltego

Maltego is an information gathering tool that can be used to collect information about ANYTHING.

To run maltego type the following in terminal

```
> maltegoce
```