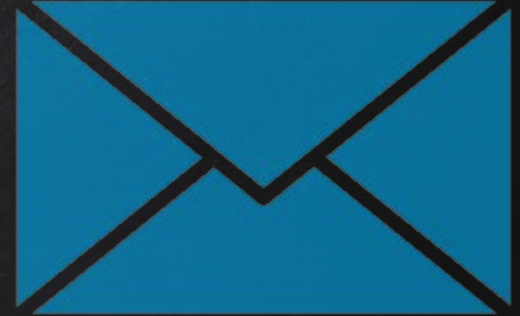# ① Information Gathering

- Gather information about target (company/website/person).
- Discover associated websites, links, companies.
- Associated people, names, emails, phone numbers, social networks, friends.
- Associated social networking accounts.
- Display all info on a graph and build attack strategies.

Fake Emails

- Send fake emails.
- Looks like it's sent from any address !
- Pretend t o be a friend, company, boss ...etc.
- Friend → Ask to open a file (image, pdf ..etc).
- Support member → ask to login to control panel using fake login page.
- Support member → ask to run a command on server.
- Ask to visit a normal web page.
- ....etc

BeEF Framework

- Browser Exploitation Framework.
- Allows us to launch a number of attacks on a hooked target.
- Targets are hooked once they load Javascript code.
- Hook code can be placed in a HTML page and share it with target.
- Or host page online and send URL to target.

INDIRECT DELIVERY

- Google Analytics is used on most websites and youtube accounts.
- Shows visitors.
- Exploit Google Analytics by generating fake traffic.
- Traffic looks as if its coming from our evil URL
- Admin feels curious about where all of this traffic is coming from.
  - → They click on the evil url & We never make direct contact with them!