Discovering Email Addresses

Email addresses are not just mere contact points; they can reveal valuable insights into an organization's structure, personnel, and communication patterns. By identifying key individuals and their roles within an organization, we can target sensitive accounts of high ranking officials in our further attacks.

So, lets get started with the email discovery.

1. Find Email address of target domain/organization

- Hunter.io - https://hunter.io/
- Phonebook.cz - https://phonebook.cz/
- Voilanorbert - https://www.voilanorbert.com/
- Skymem - http://www.skymem.info/
- Email Permutator (Generates possible email address based on target's name) - http://metricsparrow.com/toolkit/email-permutator/
- Clearbit - Google Chrome extension (works only with Chrome)
- Contact Out - Google Chrome extension works on Linkedin profile to find emails
- The Harvester

```
python3 theHarvester.py -d domain.com -l 500 -b google
```

- Email Provider of a domain - https://mxtoolbox.com/
- Email Assumptions - Assume email address of a user based on username.
- Email Format: https://email-format.com
- Gravatar: https://gravatar.com

--> https://en.gravatar.com/site/check/test@gmail.com

--> [Could later be use for Reverse Image Search.]

- Refer All email provider list from github to unravels potential bussiness email accounts.

---

2. Search the email address with google dorks on search engines & verify email

- Search on the search engine - "emailaddress@domain.com" OR "emailaddress" OR site:twitter.com "emailaddress@domain.com"
- Verify Email - https://email-checker.net/
- Verify Email 1 - https://emailable.com/email-verifier/
- Verify Emaill 2 - https://emailrep.io/

---

3. Gathering info on target email

- Epios - https://epieos.com/
- Holehe (Finds accounts assosciated with email address)

```
# Download Holehe

git clone https://github.com/megadose/holehe.git

cd holehe/

# Install the dependencies

sudo python3 setup.py install

# Perform email enum with Holehe

holehe test@gmail.com
```

- MOSINT

```

# Download MOSINT

git clone https://github.com/alpkeskin/mosint.git

cd mosint/v3/cmd/mosint

# Perform email enum with MOSINT

go run main.go test@gmail.com
```

- GHUNT (Gmail address enumeration)

```
# Download Ghunt

git clone https://github.com/mxrch/GHunt.git

cd GHunt

# Install the dependencies

pip3 install -r requirements.txt

# Launch GHunt with login argument

python3 main.py login

choose 1

# Login to a Gmail account and Install the Ghunt companion browser
extension in Firefox.

# Perform email enum with Ghunt

python3 main.py email ltest@gmail.com
```
