recon-ng

context

dit document beschrijft installatie en werking van Recon-ng, een reconnaissence tool.

installatie

rpm

`apt-get install recon-ng` (check vooraf de versie via `apt changelog recon-ng`)

source

- clone de Github repo: `cd /tmp/ && git clone https://github.com/lanmaster53/recon-ng.git`
- install via pip installer: `cd recon-ng && pip3 install -r REQUIREMENTS`
- verplaats de files: `mv /tmp/recon-ng /usr/local/bin`
- start recon-ng: `cd /usr/local/bin/recon-ng/recon-ng`

☐ opruimen van onnodige files en symlink maken

werking

Note: zet recon-ng in debug mode: ideale manier om werking te zien

Zodra je het een beetje kent, zet het uit, want het is wel vervelend 🙂

bestandsstructuur

- $HOME/.recon-ng
  - .cid
  - keys.db: api keys
  - modules: directory met geinstalleerde modules

    - modules.yml: overzicht van alle beschikbare modules
    - workspaces: workspaces van gebruiker
        - <naam>:
            - data.db: sqlite database
            - snapshot_<timestamp>.db: snapshot van de databank

nuttige modules

- recon/domains-hosts/certificate_transparency: vindt op basis van domain naam alle gekende certificaten.
- recon/hosts-hosts/ipstack: vindt geolocatie van ip adres
- recon/hosts-hosts/resolve: vindt ip adressen ahv dns-lookup
- recon/hosts-hosts/virustotal: vindt heel wat (historische) informatie over ip adressen.
- recon/domains-hosts/shodan_hostname: vindt heel wat domain info ahv shodan lookups.

meer info

- SecurityTrails
- Recon-ng website

digital forensics, RAM, volatility

From:
https://www.louslab.be/ - **Lou's lab**

Permanent link:
https://www.louslab.be/doku.php?id=digital_forensics:recon-ng

Last update: **2024/11/16 18:14**