Mirko LAPI

OSINT Italia

OSINT – Domain information Gathering

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

This presentation is licensed under the Creative Commons BY-NC License

To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Prerequisites

- Lectures:
- OSINT: What is open source intelligence and how is it used? | The Daily Swig (portswigger.net)
- OSINT without APIs - SpiderFoot
- Concepts:
- Basic knowledge of networking, linux command line and web infrastructure (whois, dns, ip, hostnames…)

Outline

The scope of this guide is to collect and present some useful tools that can aid in the initial phase of a website domain analysis:

- Identify the current and past owner(s) of a website
- Recognize the thechnology used for building the website
- Enumerate the infrastructure hosting the website and all the assets correlated
- Collect e-mail addresses related to the domain

Outline

- Information gathering using public websites
- Information gathering using linux cli tools
- Mapping of the relevant results in Maltego

Outline

- Information gathering using public websites
- Information gathering using linux cli tools
- Mapping of the relevant results in Maltego

Information gathering using public websites

- https://community.riskiq.com/
  - WHOIS, passive dns, reverse hostname from ssl certificates, reverse ip for domains in same host
- https://viewdns.info/reversewhois
  - Reverse whois from owner name or email addres
- https://domainbigdata.com/
  - Whois history, identify the previous owners of the website

Information gathering using public websites

- http://dnshistory.org/
  - Past DNS records
- https://search.censys.io/
  - Reverse whois from owner name or email addres
- https://www.whoxy.com/
  - Reverse analysis of domain name in https certificates

Information gathering using public websites

- http://dnshistory.org/
  - Past DNS records
- https://dnsdumpster.com/
  - Analyze the DNS records of the website and graphically map them
- https://builtwith.com/
  - Identify the technology used for building the website

Information gathering using public websites

- https://archive.org/
  - Search for old saved snapshots of the website
- https://analyzeid.com/
  - Identify websites with the same google analytics id

Outline

- Information gathering using public websites
- Information gathering using linux cli tools
- Mapping of the relevant results in Maltego

Information gathering using linux cli tools

- https://github.com/OWASP/Amass
  - Perform reverse DNS recognition
  - Usage: amass enum -passive -d domain.com -src
- https://github.com/s0md3v/Photon
  - Url, files and mail crawler
  - Usage: docker run -it --name photon photon:latest -u domain.com
- https://github.com/elceef/dnstwist
  - Typosquatting domain analysis (similar registered domain that can be used in malicious activities)
  - Usage: dnstwist -r domain.com

Information gathering using linux cli tools

- https://github.com/evyatarmeged/Raccoon
  - Automated whois, subdomain mapping and export
  - Usage: raccoon domain.com
- https://github.com/laramies/theHarvester
  - Gathers emails, names, subdomains, IPs and URLs
  - Usage: python3 theHarvester.py -d domain.com -b all -l 300
- https://github.com/smicallef/spiderfoot
  - All in one information gathering tool
  - Usage: python3 sf.py -l 0.0.0.0:80

Information gathering using linux cli tools

- https://github.com/lanmaster53/recon-ng
  - OSINT reconnaissance framework similar to Metasploit
  - Usage with hackertarget module (subdomain enumeration)

```
recon-ng
 workspaces create test
 marketplace install hackertarget
 modules load hackertarget
 show options
 options set SOURCE domain.com
 run
```

Outline

- Information gathering using public websites
- Information gathering using linux cli tools
- Mapping of the relevant results in Maltego

Information gathering using linux cli tools

- https://www.maltego.com/downloads/
  - Tool for graphical link analyses, used to find correlations between entities found in the gathering phase.

    Could be used for sharing and collaborating in real time between multiple users on the same report.

Mirko LAPI

OSINT Italia

OSINT – Domain information Gathering

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it