Mattia Coffetti

Mattia (Mzkk) Coffetti 🔍 | LinkedIn

ROAD TO NO HAT

COMPUTER SECURITY CONFERENCE

30 SETTEMBRE 2022

AULA EX SOFTEL - VIA CLAUDIO 21, EDIFICIO 3/A, I PIANO

L'OSINT APPLICATO ALL'ANALISI DELLE INFRASTRUTTURE

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
- Cybersquatting in office365

Outline

- Information gathering using public websites
- Information gathering using linux cli tools
- Mapping of the relevant results in Maltego
- Cybersquatting in office365

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

- https://osintframework.com/
  - Collection of useful online osint tool
- https://search.censys.io/
  - Find subdomains and mail addresses in ssl certificates
- https://www.whoxy.com/
  - Find past whois records

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

Information gathering using public websites

- Shodan Search
  - Search Favicon hash search (used for finding spoofed websites, leak website behind tor network

- https://crt.sh/
  - Gather info on certificates emitted to the certificate transparency logs

Outline

- Information gathering using public websites
- Information gathering using linux cli tools
- Mapping of the relevant results in Maltego
- Cybersquatting in office365

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
```

- https://github.com/opsdisk/metagoofil
  - Document downloader and automatic metadata extractor
  - Usage python3 metagoofil.py -d domain.com -t pdf,xls,xlsx,doc,docx,jpg
  - exiftool -r *.doc,*.pdf,*.xls,*.xlsx,*.doc,*.docx,*.jpg | egrep -i "Author|Creator|Email|Producer|Template" | sort -u

Outline

- Information gathering using public websites
- Information gathering using linux cli tools
- Mapping of the relevant results in Maltego
- Cybersquatting in office365

Mapping of the relevant results in Maltego

- 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.

Outline

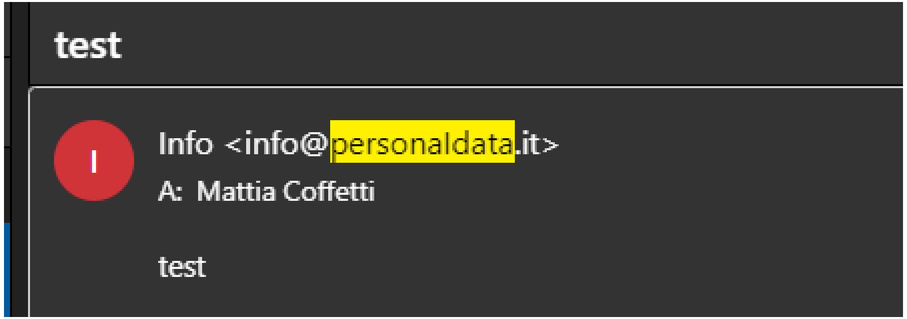
- Information gathering using public websites
- Information gathering using linux cli tools
- Mapping of the relevant results in Maltego
- Cybersquatting in office365

Cybersquatting in office365

- Mail received in office365 are case sensitive
  - You can spoof a domain that has a lowercase L in the name, by registering a domain

that has a I in the domain name, and send the mail writing the I in capital, so in the received mail, the sender is graphically the same as the targeted domain

PersonalData.it   PersonAidata.it



test

Info <info@personaldata.it>

A: Mattia Coffetti

test

Mattia Coffetti

Mattia (Mzkk_) Coffetti 🔍 | LinkedIn

COMPUTER SECURITY CONFERENCE

30 SETTEMBRE 2022

AULA EX SOFTEL - VIA CLAUDIO 21, EDIFICIO 3/A, I PIANO

L'OSINT APPLICATO ALL'ANALISI DELLE INFRASTRUTTURE