Passive Reconnaissance

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Have a Questions?

Software University

sli.do

#Cyber_Security

Table of Contents

Passive Reconnaissance Theory

Passive Reconnaissance in a Nutshell

- **Passive Reconnaissance** is the art of gathering information about a target, without them even realizing
- **Passive Reconnaissance** is also called OSINT(Open Source INTelligence), since it relies on open sources for the whole process
  - Open Sources is not used in context of coding, but rather view it as publicly accessible resources, which by itself, can include code repositories
  - More about that later

Passive Reconnaissance in a Nutshell

Software University

- **Passive Reconnaissance** is usually the very first step of the real engagements and operations
  - This is used for building up target context (domains, DNS map, live hosts, whois records, publicly available files, code and more)
- **Passive Reconnaissance** is requiring thinking outside of the box
  It is extremely safe, since if done right, the target is unaware

Passive Reconnaissance Techniques

Prepare your notes

Scanning DNS

- Scanning DNS is one of the first things to do while performing **OSINT**
- DNS enumeration is essential, since it returns useful information about the target's Live hosts and it's **DNS records**
- This most usually include information about the target's mail servers, custom dns servers, workstations, web servers and more
- By peeking at the **DNS**, we can obtain information about the target's infrastructure context
- There are attacks that relies on **DNS**, but we are focused in enumerating for now

What is DNS?

- **DNS** (**Domain Name Resolution**) is a protocol which is designed to map specific IP address to specific string
- For example: facebook.com -> 157.240.9.35
- Ok, but, Why? Because it is easier for us humans to remember facebook.com instead of it's representative IP address
- There are global **DNS servers**, like 8.8.8.8, but also everyone can implement their own
- Your router acts as a **DNS server** as well
- In most of the organizations using **Windows**, the **Domain Controller** is also DNS server

What is DNS Record?

- This is the building block of the DNS protocol
- You do not need to remember all of them, but the important ones are:
  - **A** (This is used for mapping string to IPv4 address)
  - **AAAA** (This is used for mapping string to IPv6 address)
  - **CNAME** (This is pointer to another domain, instead of an IP)
  - **NS** (This specifies authoritative DNS servers, which servers the browser should request)
  - **MX** (This points to the mail servers of given domain)
  - **TXT** (This records allows the owner of the domain to store text, some C2 frameworks are using that field to exfiltrate commands, evading security controls)

Stalking Social Media

- If the project is phishing related, the very best place to start is to stalk the target on social media (**Facebook**, **Instagram**, **Twitter**, **Tiktok**)
- This can also be applied for pentesting / red teaming, if you can extract something useful from employees social media, you can craft more complex attacks or wordlists
- See if the target's profiles are open

Stalking Social Media

- See if there is useful information inside
- Gather everything:
  - Favorite places
  - Friends
  - Tags
  - Profile Feed
  - Pretty much everything you can

Enumerating Usernames / Emails

- It is always a good idea to have a list of valid (if possible to verify) list of **usernames** / **email addresses**
- This can lead:
  - Password spraying
  - Phishing
  - Privilege Escalation
  - Many more …

Enumerating Publicly Available Resources

Software University

- The idea here is simple, enumerate:
  - Code repositories
  - Files
  - Pastebins
  - Credentials
  - SSH keys
  - Pretty much everything that can be enumerated

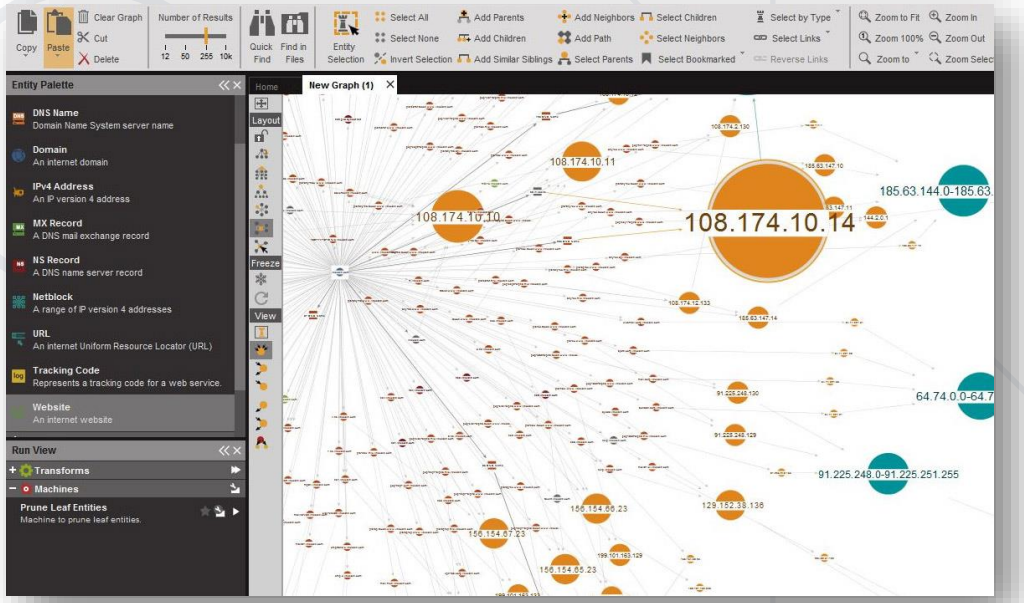
Passive Reconnaissance Tools

Discover (All in one)

- Discover (*https://github.com/leebaird/discover*) is combining tools like recon-ng, amass and DNSdumbster in one, outputting .html report
- It is preoptimized and I recommend using it. It has access to various of tools, most of them requires an API key, which can be paid

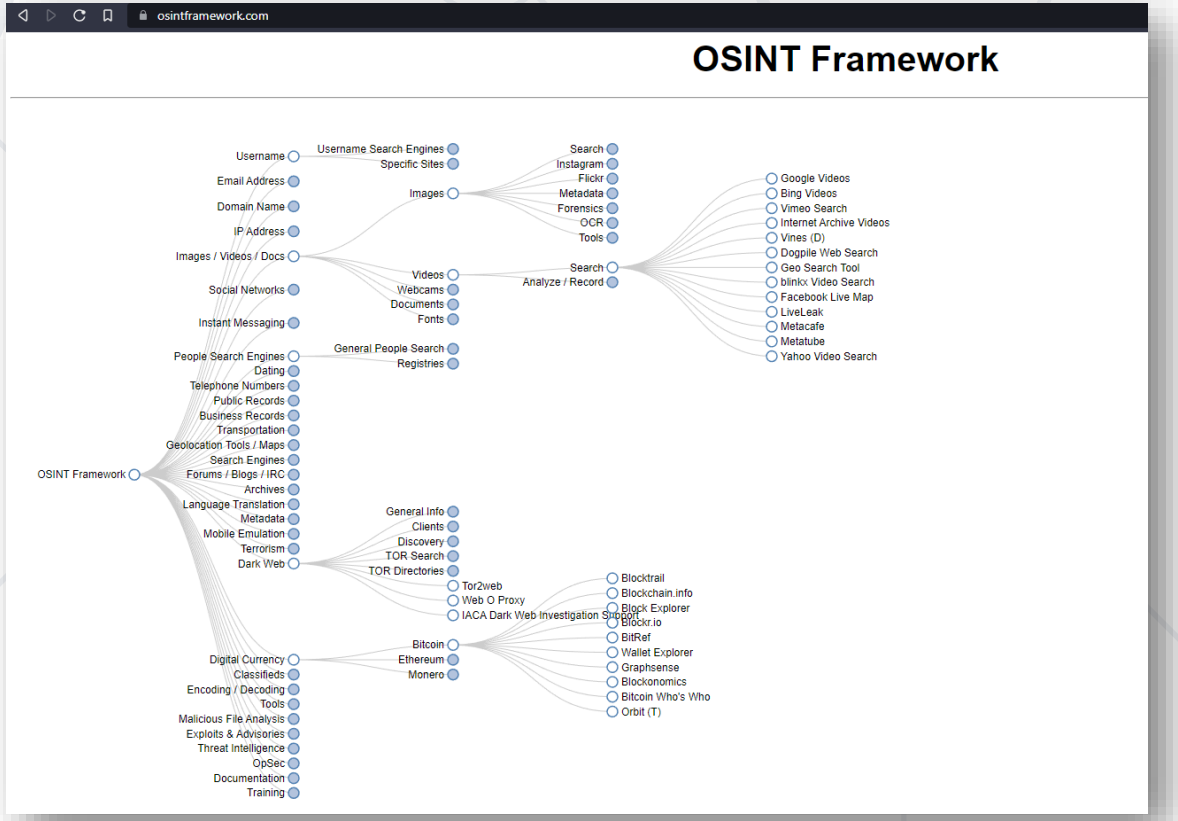
Maltego

- Maltego (*https://www.maltego.com/*) is software for data collection and visualization
- It can perform BOTH passive and active scans, so you must be careful with it
- It can be used as a context or investigation map
- It uses GUI and is easy to use
- It is OS independent



OSINT Framework

- OSINT Framework (*https://osintframework.com/*) can be used for completely anything
- From third party IP scanners, to news parsers
- Better dedicate time to play with it



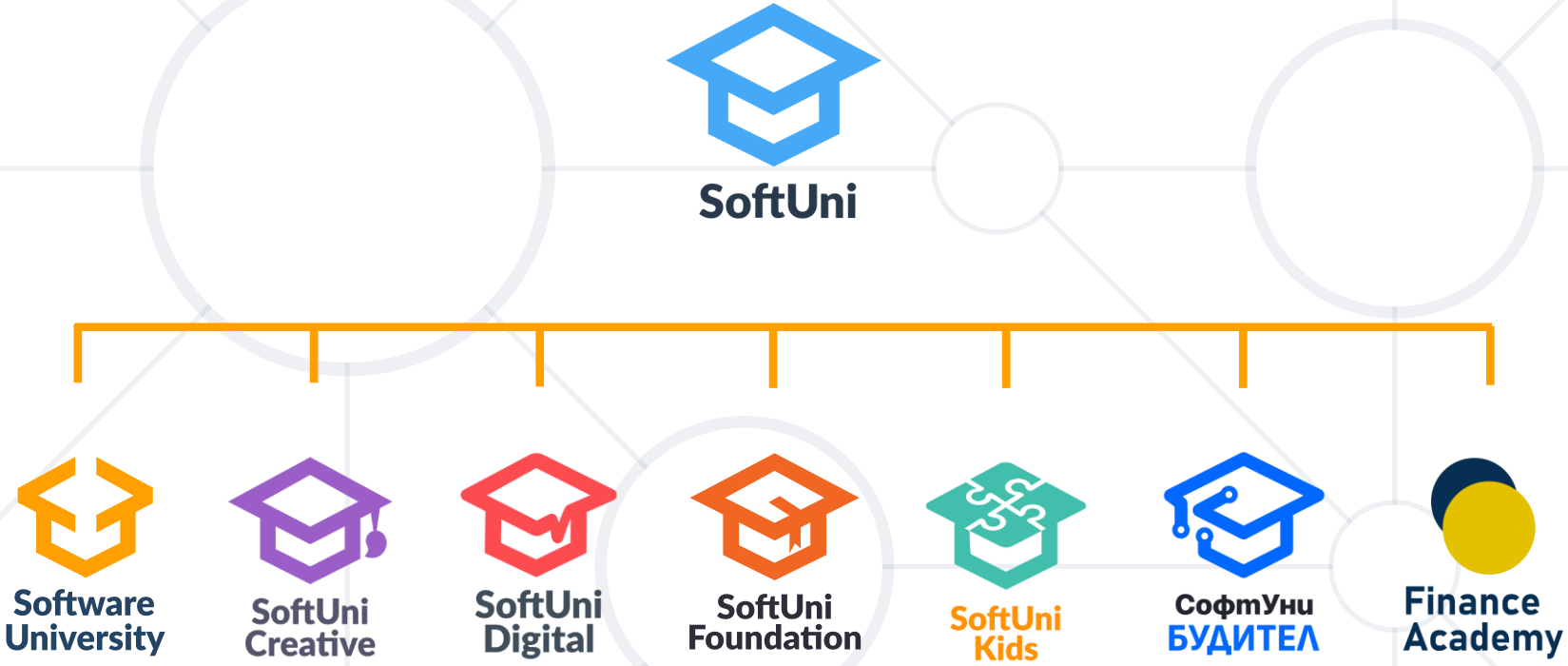
Search Engines

- Their intentional purpose is to help people find what they need, for example a website or image
- What if someone needs information about someone else?
- Search engines can query amazingly high numbers of results
- They can filter files, specific web titles, specific body strings and pretty much anything else
- There is a term for such activities, known as "google hacking"
- Google hacking is a database of google (most usually) queries, allowing you to grep detailed information about the target (*https://www.exploit-db.com/google-hacking-database*)

Summary

- What is DNS?
  - Scanning DNS
  - DNS Record
- Passive Reconnaissance in a Nutshell
  - Discover
  - Maltego
  - OSINT Framework
  - Search Engines

Questions?



SoftUni Diamond Partners

Software University

SmartIT

Coca-Cola HBC Bulgaria

SUPER HOSTING .BG

createX

Postbank

Решения за твоето утре

DRAFT KINGS

THE CROWN IS YOURS

VIVACOM

AMBITIONED

INDEAVR

Serving the high achievers

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity

License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – https://about.softuni.bg/
- © Software University – https://softuni.bg