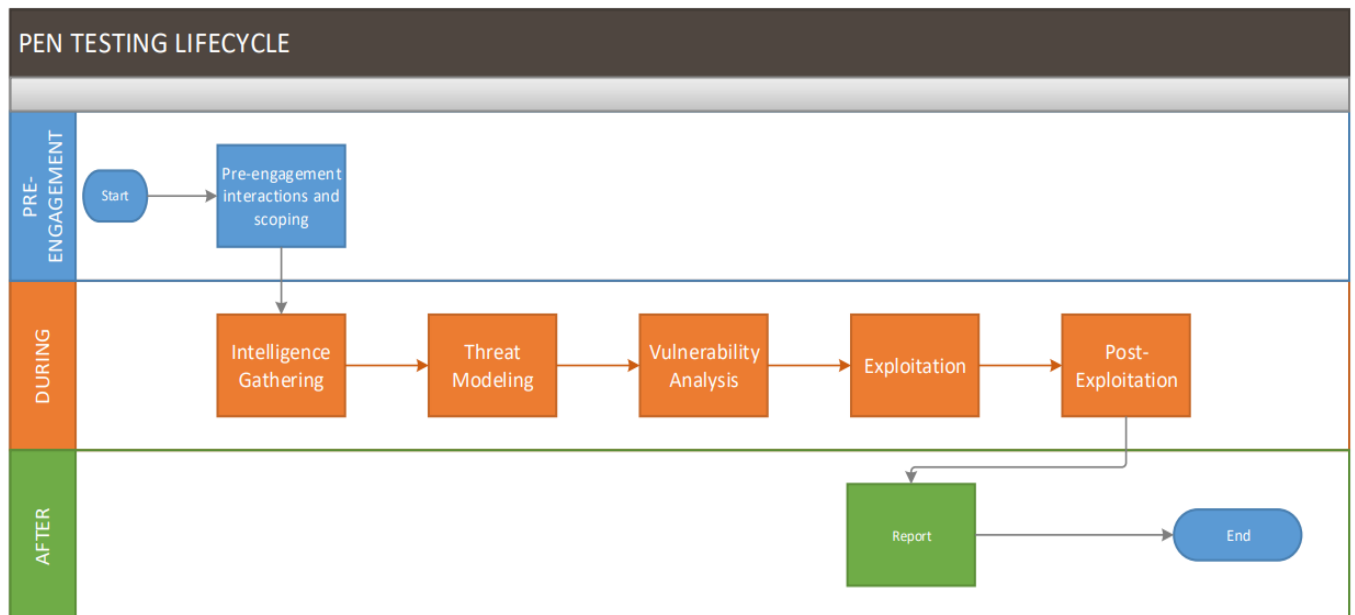


## Pentesting Testing: Passive Recon

### Summary

In this lab we will cover some of the main techniques that are used during penetration testing operations. These techniques are also used by bad actors to gather information about the targets that they are attempting to attack.



## Reconnaissance & Footprinting

In any penetration testing, we start off with information gathering before we do any attempts. The technical terms of this initial step are called 'Enumeration' and/or 'Reconnaissance'. There are two methods of performing enumeration:

- a. Passive - Uses an indirect approach and does not engage the target. This method obtains information that's publicly available from many sources
- b. Active - Uses a direct engaging approach with the target to gather information

**Objective of Reconnaissance:** To gather as much information as we can about the target so we can create a 'Footprint' for it. Footprinting will help create a profile of the target, gathering profiling information such as running services, open ports, and operating systems is a crucial step.

### Recommended Footprinting Techniques:

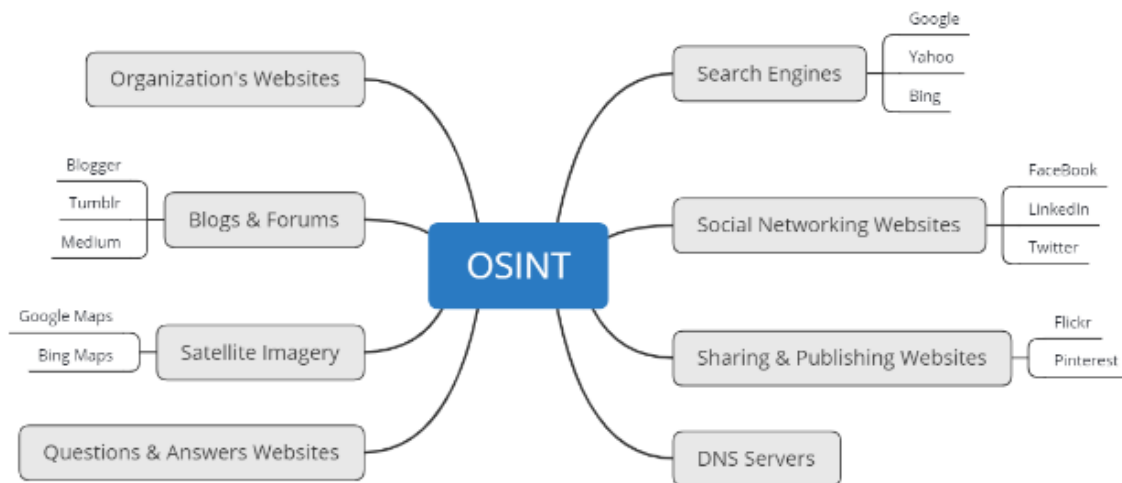
- Checking search engines such as Yahoo, Bing, and Google
- Performing Google hacking techniques (advanced Google searches)
- Information gathering through social media platforms such as Facebook, LinkedIn, Instagram, and Twitter
- Footprinting the company's website Performing email footprinting techniques Using the whois command
- Performing DNS & Network footprinting techniques

## Passive Reconnaissance

We will start off with passive techniques as they are crucial methods to gather information about the targets in scope for pen testing

### Passive - OSINT (Open-source intelligence)

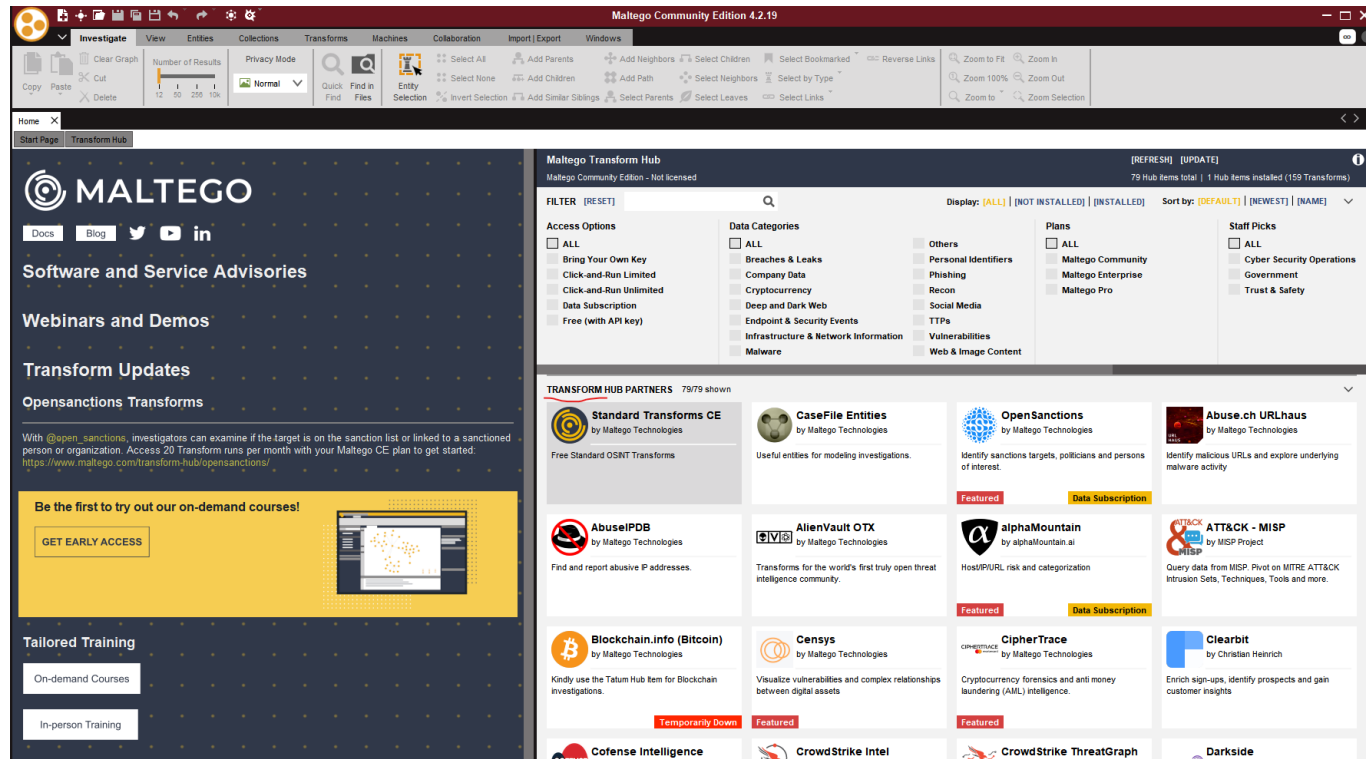
OSINT is a type of passive information gathering where the penetration tester does not make direct contact or a connection with the actual target, but rather asks legitimate and reliable sources about the target. As the internet is so readily available and accessible, it's quite easy for someone to gather information on a target organization simply by using search engines and determining their underlying infrastructure. This technique will help to create a profile about the target.



### **OSINT Passive Recon Tools:**

<ul style="list-style-type: none"> <li>• <a href="#">Google Hacking DB</a></li> <li>• <a href="#">Shodan</a></li> <li>• <a href="#">Recon-NG</a></li> <li>• <a href="#">Maltego</a></li> <li>• <a href="#">Screaming Frog</a></li> <li>• <a href="#">theHarvester</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">SpiderFoot</a></li> <li>• <a href="#">Sublist3r</a></li> <li>• <a href="#">Buscador</a></li> <li>• <a href="#">Censys &amp; Crt.sh</a></li> <li>• <a href="#">Web Data Extractor</a></li> <li>• <a href="#">Xenu</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">AMass</a></li> <li>• <a href="#">Exiftool</a></li> <li>• <a href="#">ExtractMetadata</a></li> <li>• <a href="#">Findsubdomains</a></li> <li>• <a href="#">FOCA</a></li> <li>• <a href="#">IntelTechniques</a></li> <li>• <a href="#">Scrapy</a></li> </ul>
--	--	---

# Maltego Demo



This is a graphical interactive data mining application which is used to query and gather information from various sources on the internet and present data in easy-to-read graphs

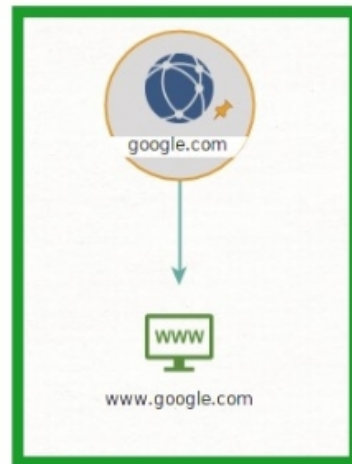
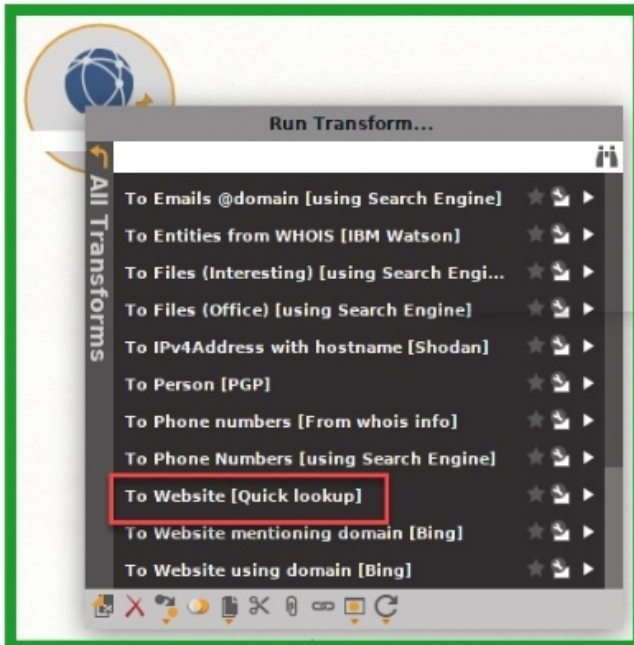
**Transform:** The highlighted option on the image above is an open source resource that Maltego can query for information. As shown, there are many transform sets that Maltego can connect to

## Preparation Steps:

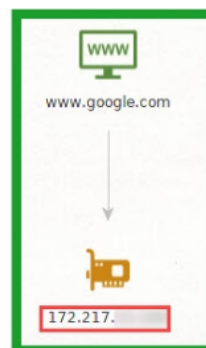
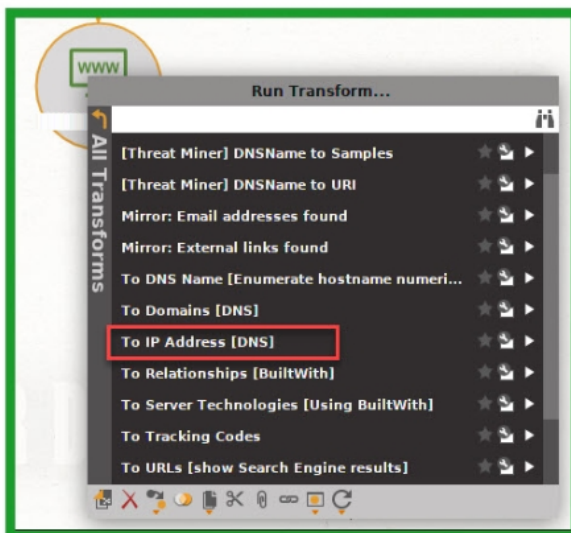
- Creating a free account via [Link](#)
- Installing Maltego in Kali - `sudo apt install maltego`


## Maltego Demo - [Link](#)

- Website
  - Domain Entity
    - Website [Quick lookup]



- Obtain IP Address



- 
- Top-level domains (TLDs) [[TBD](#)]

- **Person**