Information Gathering and OSINT

What is OSINT?

The term “open source” refers specifically to information that is available for public consumption. If any specialist skills, tools, or techniques are required to access a piece of information, it can’t reasonably be considered open source.

Open-source intelligence (OSINT) is a multi-methods (qualitative, quantitative) methodology for collecting, analyzing and making decision about data accessible in publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or collective intelligence.

OSINT under one name or another has been around for hundreds of years. With the advent of instant communications and rapid information transfer, a great deal of actionable and predictive intelligence can now be obtained from public, unclassified sources.

FULL FORM OF OSINT: Open Source Intelligence

Who use OSINT and Why we should learn it?

Fields and Sectors where OSINT is mostly required:

Government, Finance, Telecom, Critical Infrastructure, Cyber Security Advisory Firms, Cyber Threat Intelligence Teams, Law, Cyber Forensic Teams and etc.

Benefits of learning OSINT:

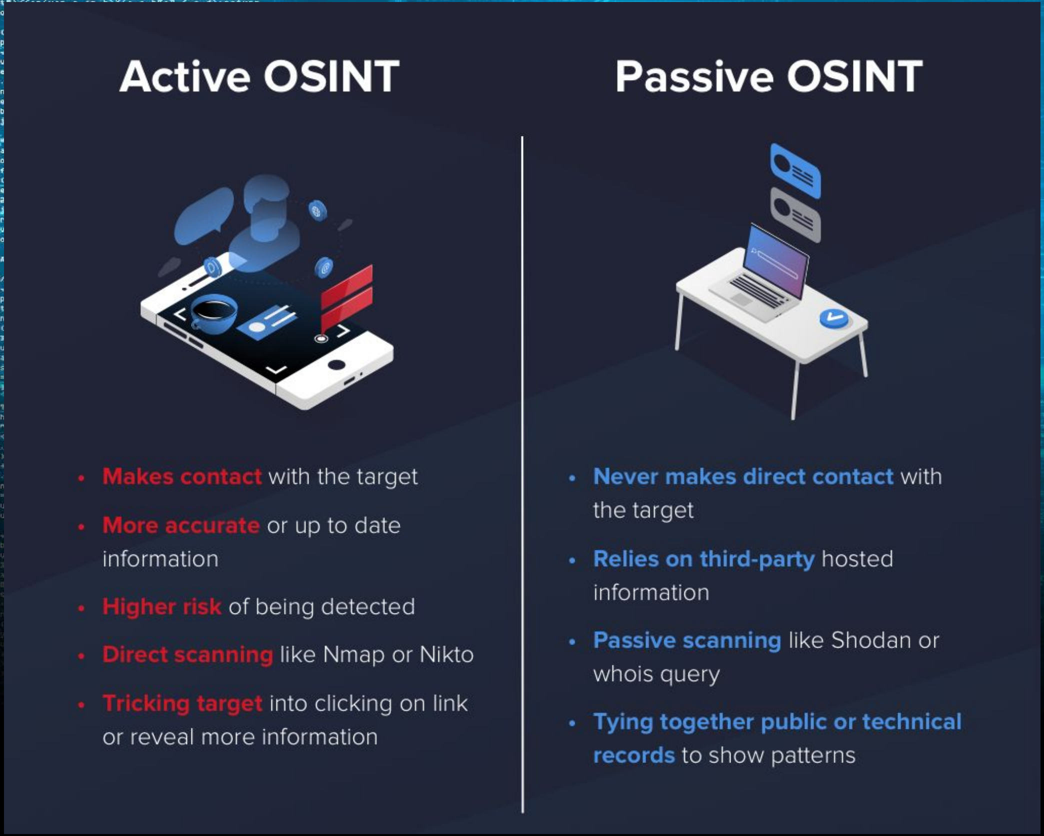
OSINT is a major part in hacking. Because learning about the target is the first part in hacking which is easily achieved through this.Gathering OSINT info is not restricted or illegal. It is totally legal, In this webinar,we’ll focus on the major OSINT tools which are used in Kali.

Types of OSINT:

Passive Collection - This is the most used type when collecting OSINT intelligence, by default most OSINT gathering methods should use passive collection because the main aim of OSINT gathering is to collect information about the target via publicly available resources.

Active Collection - In this type, you interact directly with the system to gather intelligence about it, but The target can become aware of the reconnaissance process since the person/entity collecting information will use advanced techniques to harvest technical data about the target IT infrastructure such as accessing open ports, scanning vulnerabilities (unpatched Windows systems), scanning web server applications, and more. This traffic will look like suspicious behaviour and will more than likely leave traces on the target’s intrusion detection system (IDS) or intrusion prevention system (IPS).

Types of OSINT:



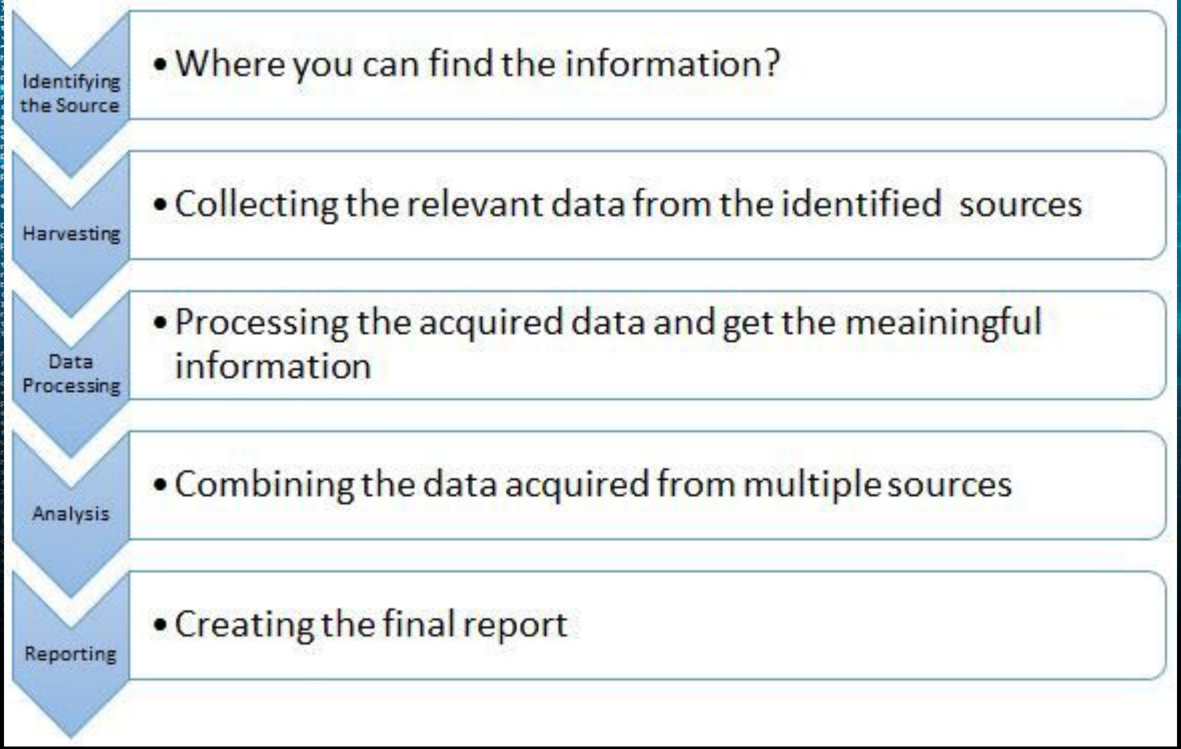
Active OSINT

- **Makes contact** with the target
- **More accurate** or up to date information
- **Higher risk** of being detected
- **Direct scanning** like Nmap or Nikto
- **Tricking target** into clicking on link or reveal more information

Passive OSINT

- **Never makes direct contact** with the target
- **Relies on third-party** hosted information
- **Passive scanning** like Shodan or whois query
- **Tying together public or technical records** to show patterns

Process carried out in OSINT:



Identifying the Source

- Where you can find the information?

Harvesting

- Collecting the relevant data from the identified sources

Data Processing

- Processing the acquired data and get the meainingful information

Analysis

- Combining the data acquired from multiple sources

Reporting

- Creating the final report

What you can find via OSINT?

1. Technology infrastructure like IP, Hostname, Services, Networks, Software / hardware versions and OS information, Geo-location and Network diagrams.

2. Database: Documents, papers, presentations, spreadsheets and configuration files.

3. Metadata:Information like Email and employee search (name and other personal information).

Digital Footprint of an Organization :

Technical footprinting is the main task done by penetration testers and attackers before launching an attack. Your goal as a hacker is to gather as much information as possible about your target website or a system, such as
Exposed ports,
Running network services,
DNS names and IP addresses,
Remote access capabilities,
Unpatched Vulnerabilities in applications and operating systems, or the type of security mechanisms in place.

Footprinting is also a part of OSINT.

Source for learning OSINT:

Major tools used worldwide

- Google Hacking Database by exploitdb

-https://www.exploit-db.com/google-hacking-database

- Shodan - https://shodan.io
- Censys - https://censys.io
- Archives - https://archive.org/

WHOIS - https://who.is/

OSINT framework - https://osintframework.com/

Maltego,TheHarvester,Recon-ng,EXIF tool,Reverse Image lookup,Domain Name finder,Nmap and some alike scanners.