**ASSIGNMENT 2**

Salavuddin Shaikmothad

UCEN JNTUK

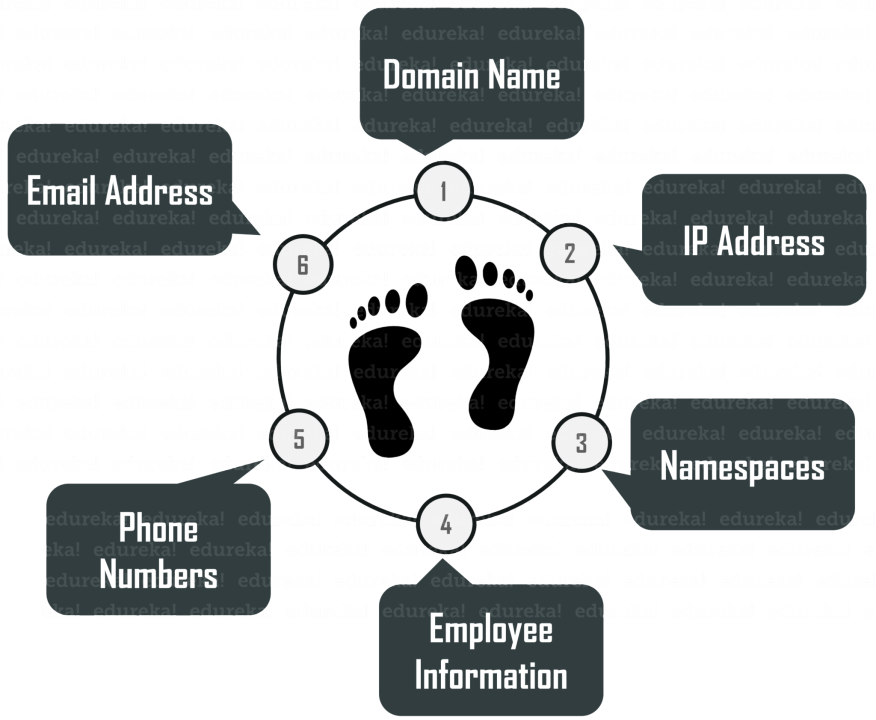
**FOOTPRINTING:**

* [Footprinting](https://www.geeksforgeeks.org/ethical-hacking-footprinting/) refers to the process of collecting data over time in order to make a targeted cyberattack .
* Footprinting involves gathering information about a target—typically related to its network infrastructure, systems, and users—without actually committing an attack.

**Forms of Footprinting**

There are various forms and varieties of Footprinting. Some of them are as follows:

* E-Mail Footprinting
* Google Hacking
* Social Engineering
* Whois Footprinting
* Network Footprinting
* Website Footprinting



* **Steps in Footprinting**
* Several steps need to be followed during footprinting to collect all relevant information.
* **1. Identifying Targets**
* The first step is to identify which systems or organizations to footprint by scanning networks for open ports or performing reconnaissance using Google searches and tools like Shodan.
* **2. Gathering Information**
* After the target has been identified, the next step is to gather as much information about it as possible using tools like Nmap, Netcat, and Whois to identify open ports and services, usernames and passwords, web server information, and more.
* **3. Analyzing Results**
* After all relevant data has been collected, it needs to be analyzed to determine the most vulnerable points. This is done by identifying common weaknesses across multiple systems or comparing results against known exploits.
* **4. Planning Attacks**
* The final step is to use the information gathered during footprinting to plan a successful attack against the target’s systems, networks, and devices. This may involve developing custom exploits or choosing a suitable attack vector based on the data collected.

**TOOLS**

Whois is a renowned Internet record listing tool to identify who owns a domain or who registers for that particular domain along with their contact details. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain registration and ownership details. Whois records have proven extraordinarily beneficial and have developed into an essential resource for maintaining the integrity of domain name registration and website ownership process.

* **Harvester** is also an information-gathering tool that helps you extract a particular target's email address and subdomains. Harvester is coded using a simple python script that searches information from giant search engines like Google, Yahoo, Bing, and much more.
* **Metagoofil** is another information gathering or footprinting tool used for extracting information or data publicly available on the internet belonging to the company.
* **Netifera** is a potent tool that gives a complete platform to gather information regarding the targeted website you want to attack. It is a free tool that comes inbuilt with Backtrack Linux OS. This software will give information such as IP address, the Programming language used for website development, the number of websites hosted, and DNS.

**TECHNIQUES:**

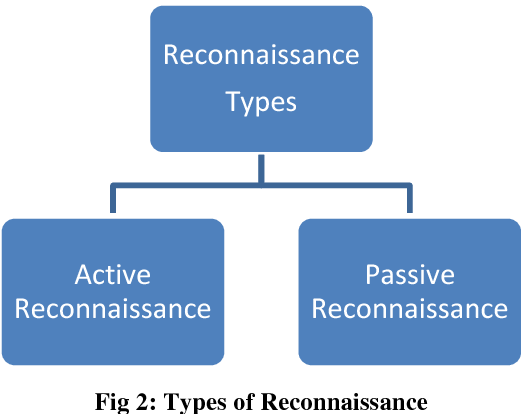
* OS Identification: involves sending illegal TCP (Transmission Control Protocol) or ICMP (Internet Control Message Protocol) packets to the victim's system to identify the OS (Operating system) used by the victim on his server or computer.
* A ping sweep establishes a range of IP addresses that map hackers to live hosts. Fping, Nmap, Zenmap, ICMPEnum, and SuperScan are some of the tools used to ping a large number of IP addresses at a time; to generate lists of hosts for large subnets.

# **Reconnaissance**

[Reconnaissance](https://www.blumira.com/glossary/reconnaissance/) is the practice of covertly discovering and collecting information about a system. This method is often used in ethical hacking or penetration testing.

Like many cybersecurity terms, [reconnaissance](https://www.blumira.com/glossary/reconnaissance/) derives from military language, where it refers to a mission with the goal of obtaining information from enemy territory.

Reconnaissance succeeds in two parts: active reconnaissance and passive reconnaissance.



## Active Reconnaissance

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

Techniques:

1. **Port Scanning:**
   * Port scanning involves sending data packets to target systems to discover which ports are open and which services are running. This information helps attackers identify potential entry points into the system.
2. **Network Scanning:**
   * Network scanning involves mapping out the network architecture, identifying active devices, and determining the relationships between them. Tools like Nmap can be used to perform network scans.
3. **Vulnerability Scanning:**
   * Vulnerability scanning involves searching for weaknesses and vulnerabilities in systems or applications. Automated tools can scan a network for known vulnerabilities and provide a list of potential points of attack.

**4. Man in the middle attack**  
A Man-in-the-Middle (MitM) attack involves an unauthorized third party intercepting and potentially altering communication between two parties without their knowledge. In the context of active reconnaissance, a Man-in-the-Middle attack can be employed to gather information or manipulate data exchanged between the target and other systems.

## Passive Reconnaissance

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Techniques:

1. **Network Scanning:**
   * Passive network scanning involves observing and analyzing network traffic without actively sending packets to the target. This can include monitoring communication patterns, identifying active hosts, and mapping network architecture.
2. **Open Source Intelligence (OSINT) Gathering:**
   * OSINT involves collecting information from publicly available sources. This can include data from websites, social media, public records, and other publicly accessible repositories to gather information about an organization, its employees, or its infrastructure.
3. **Dumpster Diving:**
   * Physical security can be just as important as digital security. Dumpster diving involves searching through an organization's trash to find discarded documents, notes, or other materials that may contain sensitive information.
4. **Shoulder Surfing:**
   * Shoulder surfing is the act of surreptitiously observing someone as they enter passwords, PINs, or other sensitive information. This can be done in person or, in some cases, through the use of surveillance cameras.
5. **Eavesdropping:**
   * Passive eavesdropping involves listening to conversations or monitoring communication channels without actively participating. This can be done through wiretapping, intercepting radio signals, or other methods to gather information.