FOOTPRINTING AND RECONNAISSANCE :

FOOTPRINTING :

Footprinting, in the context of cybersecurity, refers to the process of gathering information about a target system or network to identify vulnerabilities and gain access to it. There are several types of footprinting:

1. **Passive Footprinting:** This involves collecting information without directly interacting with the target system. It includes gathering data from public sources, such as websites, social media, and public records.

2. **Active Footprinting:** This type involves directly interacting with the target system to gather information. It can include techniques like port scanning, network scanning, and reconnaissance.

3. **Open Source Footprinting:** This involves using publicly available information from sources like search engines, social media, and public databases to gather information about the target.

4. **DNS Footprinting:** This involves gathering information about the target's domain names, such as the domain name system (DNS) records, subdomains, and associated IP addresses.

5. **Social Engineering Footprinting:** This involves gathering information through social engineering techniques, such as phishing emails, to trick individuals into revealing sensitive information about the target.

RECONNAISSANCE :

Reconnaissance, also known as "recon," is the process of gathering information about a target system or network to identify vulnerabilities and gather intelligence. It is a crucial phase in the process of a cyberattack. There are several types of reconnaissance:

1. **Network Reconnaissance:** This involves scanning the target network to gather information about active hosts, open ports, and services running on those ports. Techniques include ping sweeps, port scans, and service identification.

2. **Footprinting:** As mentioned earlier, this involves gathering information about the target from publicly available sources, such as websites, social media, and public records.

3. **OSINT (Open-Source Intelligence):** This involves using publicly available information to gather intelligence about the target, including information from social media, forums, and other online sources.

4. **Scanning:** This involves actively probing the target system or network to gather more detailed information, such as the operating system, running services, and potential vulnerabilities.

5. **Enumeration:** This involves actively querying the target system to gather information about users, shares, and other resources available on the system.

6. **Social Engineering:** This involves using psychological manipulation to trick individuals into revealing sensitive information about the target, such as passwords or system configurations.