Reconnaissance

- Reconnaissance is the first phase of an attack and is the process of gathering information about the target host or network.

Types of reconnaissance:

- Passive
  - It means gathering information about the target without sending any packet to the target.
  - Tools: netdiscover, Google Dorks, Shodan, OSINT.
- Active
  - It means directly interacting with the target host or network to gain information.
  - Tools: hping, netdetect, arp-scan, routersploit, nmap

The process of reconnaissance is carried out by **Footprinting**, **Scanning**, and **Enumeration**.