**Foot printing:**

**Refers to the process of collecting as much as information as possible about the target system to find ways to penetrate into the system. An Ethical hacker has to spend the majority of his time in profiling an organization, gathering information about the host, network and people related to the organization.**

**Information such as ip address, Whois records, DNS information, an operating system used, employee email id, Phone numbers etc is collected.**

* **Know Security Posture – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.**
* **Reduce Attack Area – Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on.**
* **Identify vulnerabilities – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.**
* **Draw Network map – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.**

**Practical:**

1. <https://www.wappalyzer.com/>
2. https://whois.domaintools.com/
3. <https://www.netcraft.com/>
4. <https://dnsdumpster.com/>
5. <https://archive.org/>
6. <https://www.yougetsignal.com/tools/web-sites-on-web-server/>
7. https://hackertarget.com/reverse-ip-lookup/
8. <https://www.shodan.io/>
9. https://www.whatismyip.com/email-header-analyzer/
10. <https://www.google.com/finance/>
11. <https://www.moneycontrol.com/>
12. <https://www.google.com/maps/>
13. <https://www.flightradar24.com/>
14. <https://osintframework.com/>

**Tools:**

1. HT Track
2. Web site ripper copier
3. Email tracker pro
4. Advance IP scanner
5. Advance Port Scanner

**Basic command:**

1. Ping
2. Tracert
3. Nslookup
4. Pathping

**Parrot OS Tools:**

1. **The harvester: theHarvester –d microsoft –l 200 –b linkedin**
2. **Dnsrecon: dnsrecon –r 162.241.216.0-162.241.216.255**