Introduction to Footprinting

Concepts: Process of collecting information on the target.

Objectives:

●Know Security Posture: Footprinting allows attackers to know the external security posture of the target organization.

●Reduce Focus Area: It reduces the attacker's focus area to a specific range of IP addresses, networks, domain names, remote access, etc.

●Identify Vulnerabilities: It allows attackers to identify vulnerabilities in the target systems in order to select appropriate exploits.

●Draw Network Map: It allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break

Footprinting Technology :

- Through Search Engines
- Through Google Hacking & Dorking
- Through Social Media
- Through Websites
- Through Emails
- Through Competitive Intelligence
- Through WHOIS
- Through DNS
- Through Network
- Through Social Engineering

Tools Used :

- Search Engines :
- Google Dorks & GHDB :
- Social Media :
- Website Footprinting: Netcraft | HTTrack | Wayback
- Email: Email Tracker | Analyzing Email Headers
- Competitive Intelligence : Jobs/Agents/Alerts
- WHOIS: Whois.com
- DNS Footprinting: Dnsstuff.com
- Network Footprinting: Traceroute | Pingsweep
- Social Engineering: Maltego | SE Toolkit

Footprinting Countermeasures :

● Restrict the employees to access social networking sites from the organization's network

● Configure web servers to avoid information leakage

● Educate employees to use pseudonyms on blogs, groups, and forums

● Do not reveal critical information in press releases, annual reports, product catalogs, etc.

● Limit the amount of information that you are publishing on the website/Internet

● Use footprinting techniques to discover and remove any sensitive information publicly available

● Prevent search engines from caching a web page and use anonymous registration services

● Enforce security policies to regulate the information that employees can reveal to third parties

● Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers

● Disable directory listings in the web servers

● Educate employees about various social engineering tricks and risks

● Opt for privacy services on the Whois Lookup database

● Avoid domain-level cross-linking for the critical assets

● Encrypt and password-protect sensitive information