02 Footprinting and Reconnaissance

What is Footprinting?

Footprinting is the process of collecting as much information as possible about a target network, for finding various ways to intrude into an organisation’s network system.

Once you begin the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of target organisation. The term “blueprint” is used here because result gathered at the end refers to unique system profile of target organisation.

Why do Footprinting?

- Know security posture
- Reduce attack area
- Build information database
- Draw network map

So what we actually do in footprinting

- Collect basic information about the target and its network
- Determine the OS used, platforms running, determine web server versions etc
- Perform DNS techniques such as whois, DNS, Network and Organizational queries

Footprinting Terminology

- Open Source or Passive Information Gathering

  Collect information about the target from publicly available sources

- Active Information Gathering

  Gather information through social engineering, on-site visits, interviews and questionnaires

What do we need to collect

Network Information

- Domain name(s)
- Network blocks
- IP Address of the reachable systems
- Rogue websites/ private websites
- TCP and UDP services running
- IDS running

System Information

- User and group names
- System banners
- Routing tables
- System architecture
- Remote system types
- System names

Organization Information

- Employee Details
- Organizational website
- Location details
- Address and Phone numbers
- Comments in HTML source code
- Security policies implemented
- Background of the organization

How do we perform footprinting

- Through search engines
- Through social networking sites
- Through official websites
- Through directly communicating to target
- Through job portals

What if we skip Footprinting

- Scenario

You need to hack a mail account as you see no other available option to get access to your client's system. You manage to create a phishing mail for some XYZ Bank and send him a mai alerting about some unusual activity in his bank account, hence asking for some security checkup. But you didn't know that your client doesn't have an account in XYZ Bank. He gets aware that someone is trying to hack him and reports the mail to cybercrime department and gets extra careful of any other attempts you make take to hack the system.

Conclusion:

Launching attacks directly without understanding the security posture of the organization/ individual may lead to fail