Foot printing and Reconnaissance

What is Foot Printing?

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

Why Foot Printing?

Footprinting is necessary to systematically and methodically ensure that all pieces of information related to the aforementioned technologies are identified. Without a sound methodology for performing this type of reconnaissance, you are likely to miss key pieces of information related to a specific technology or organization. Footprinting is often the most arduous task of trying to determine the security posture of an entity; however, it is one of the most important. Footprinting must be performed accurately and in a controlled fashion.

Know Security Posture:

Footprinting allows attacker to know about the complete security posture of an organization.

Reduce Attack Area:

It reduces attacker's attack area to specific range of IP address, networks, domain name, remote access, etc.

Build Information Database:

It allows attacker to build their own information database about target organization's security weakness to take appropriate actions.

Draw Network Map:

It allows attacker to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break.

What we do in Footprinting?

- Collect basic information about the target and its network
- Determine the operating system used, platforms running, web server versions, etc.;
- Perform techniques such as Whois, DNS, network and Organizational queries
- Find vulnerabilities and exploits for launching attacks

Foot Printing Terminology

Open Source or Passive Information Gathering:
Collect information about a target from the publicly accessible resources

Active Information Gathering:
Gather information through social engineering on-site visit's, interviews, and questionaries'

What We Need To Collect?

Network Information:

- Domain name
- Network blocks
- IP address of the reachable systems
- Rogue websites/private websites
- TCP and UDP services running
- IDSes Running

System Information:

- User and Group Names
- System Banners
- Routing Tables
- System Architecture
- Remote System Type
- System Names

Organization Information:

- Employee Details
- Organization Website
- Location Details
- Address and Phone Numbers
- Comments in HTML source code
- Security policies Implemented
- Background of the organization

How We Do Foot Printing?

Through Search Engines

Through Social Networking Sites

Through Official Web Sites

Through Directly Communicating To Target

Through Job Portals

What if We Skip Footprinting?

Basically You shouldn’t Skip Footprinting. A hacker or a penetration tester success will not always depends on foot printing, but sometimes these tiny bits of information can rule Your success ratio. Want to know how?

Scenario 1: You found the vulnerabilities in a target and you are trying to hack. But at the last step there was an authentication, and the password for that is the victims DOB. As you don’t know anything about the victim. Of course you are failed.

Scenario 2: you are about to hack a mail, you are thinking to send a phishing mail to the victim telling you are the bank official of some XYZ bank and you are seeking some information about the account details of the victim. But your victim is not the account holder of XYZ bank. So definitely he’ll get doubt on you. If he is aware he may report to cyber crime department also against the fraudulent email.

Conclusion: launching attacks without the proper knowledge about the target is injurious to health.

References:

Some Definitions in this Presentation are taken from EC-Council Official Course Curriculum.
And others are from internet sources