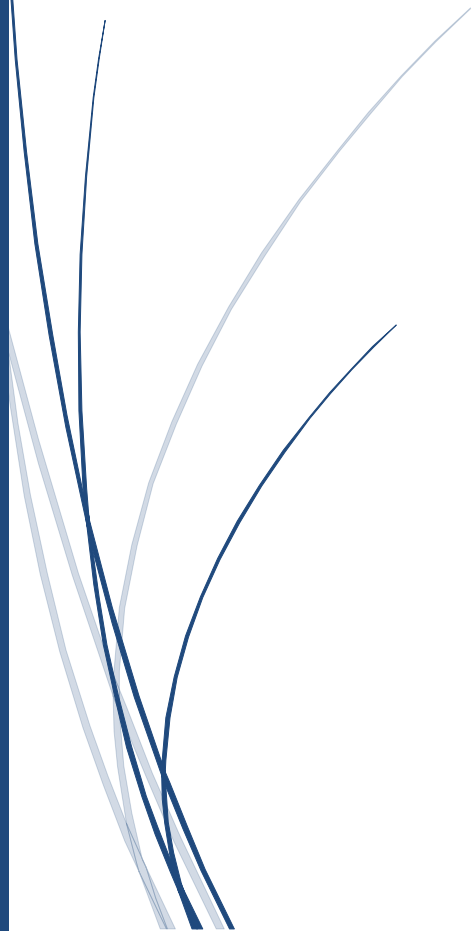
Chapter 2

Footprinting And Reconnaissance

Theory



Ethical Hacking

Footprinting

Footprinting is the process of collecting information related to the target network. Footprinting helps in identifying Various ways to intrude into an Organization's network system.

In this step attacker tries to gather publicly available sensitive information, using which he/she can carry out social engineering, perform system or network level attacks, that can cause substantial financial loss or damage the reputation of an individual or organization. This step helps an attacker in gaining a basic idea of network structure and organization's infrastructure details.

Why perform Footprinting

- Footprinting is the first step of the attacking process. Hackers use to gather information about the target environment, usually to find ways to break into that environment.
- Footprinting allows an attacker to know about the security posture of an organization.
- It helps in reducing attacker's attack surface to a specific range of IP address, networks, domain name, remote access, etc.
- It allows an attacker to build their information database about the target's organization security weakness and plan attacks accordingly.

Terminology

Passive Information Gathering: Is the process of collecting information about the target from the publicly accessible resources

Active Information Gathering: Is the process of gather information about the target by using techniques likes social engineering, grabbing information by visiting personal blogs or websites, or through direct interaction with the individual or employees of the organization.

What kind of information is needed

Network Information:

Domain name, Network blocks, IP address of computers in the target network, TCP and UDP services running, details related to IDS running.

System Information:

User and group names, system banners, routing tables information, system architecture, remote system names.

Organization Information:

Employee details, organization website details, location details, address and phone numbers, information related to security policies implemented, and any non-technical information about the organization.

How to perform Footprinting

- Through search engines
- Through social networking sites
- Through official websites
- Direct communication with the target
- Through job portals
- Through DNS enumeration

Google Hacking

Google is a vast resource where millions of pages are available for an average user to search. But getting useful information out of those results is a challenging task, to extract the desired information (information that is useful to attack target individual or network) we can take help of Google search operators also known as google dorks. This technique is called Google Hacking.

By using these google dorks, we query Google to reveal sensitive data, useful for the reconnaissance stage of an attack, sensitive data such as emails associated with an individual or an organization, database files with usernames and passwords, unprotected directories with confidential documents, URLs to login portals, different types of system logs such as firewall and access logs etc.,

whois lookup

While purchasing a domain, the user (registrant) has to provide their contact details, like address, phone number, email id, etc., those registration details along with domain validity information is usually stored in a publicly available database called whois database.

Domain registrars will protect this information from not to be published on the internet based on the request made by users, at extra cost. Domain registration details will not be available on the internet if they opt domain privacy, of course, domain registrar information will be available, whoever wants to get that domain information should contact the registrar, and if the registrar finds the query is legitimate, they will provide the Domain registrant details. By using the free online and offline tools, we extract domain registrant Information from publicly available Whois database. This process is known as whois lookup.

Traceroute

While the data packet is in transit, it passes through multiple network nodes to reach the destination. If the data packet fails to reach the destination, the user will not know the reason behind the failure; network administrators use traceroute program to trace the packet from source to destination to identify the actual cause of the problem so that they can investigate and resolve the issue.

Traceroute tool is used to extract details about the path that a packet takes from the source to a specific destination.

IP Tracing

The IP address is one of the most critical pieces of information. To attack the target computer, attackers need to identify the IP address of the target computer. Attackers use different techniques to grab the IP address. Sending tracking emails, or SMS, or some malicious links to grab the IP address of the target computer is called as IP Tracing. In other words, extracting user details (like location) based on IP address is known as IP Tracing or IP Lookup.

What if We Skip Footprinting?

We should not skip Footprinting. Hacker or penetration tester's success will not always depend on sophisticated tools used to perform attacks, but information gathered at Footprinting plays a crucial role in gaining access to the target. Want to know how?

Scenario: Information gathered in this step can help us bypass some security controls for example login credentials for one of the computers in the network may be DOB or first name of the employee. As we know some necessary information about an employee, we can try to guess the username or password by observing hint.

Conclusion: launching attacks without proper knowledge about the target may affect the success of the attack.

Countermeasures

- Revise the information before publishing on blogs, social networking sites, and websites.
- Never upload highly classified documents online.
- Privatize the who is lookup registration details by applying for anonymous registration with the web hosting service provider.
- Never click the link in emails or mobiles, if received from an unknown sender.
- Use pseudo-names in blogs and social networking sites to not leak personal information.
- Avoid opening third-party social networking sites or websites from office premises.
- Use IDS in corporate networks to detect Footprinting attacks done by hackers.