CYBERMCBEAN PODCAST

GUIDE TO FOOTPRINTING / RECONNAISSANCE

PRESENTATION - 2025

Footprinting (also known as reconnaissance) is gathering information about the victim, the word reconnaissance is a military word meaning the process of obtaining information about enemy forces or mission into enemy territory to obtain information.

Presented By: Gordon Melvin McBean (CEH)
Cybersecurity Engineer Consultant.

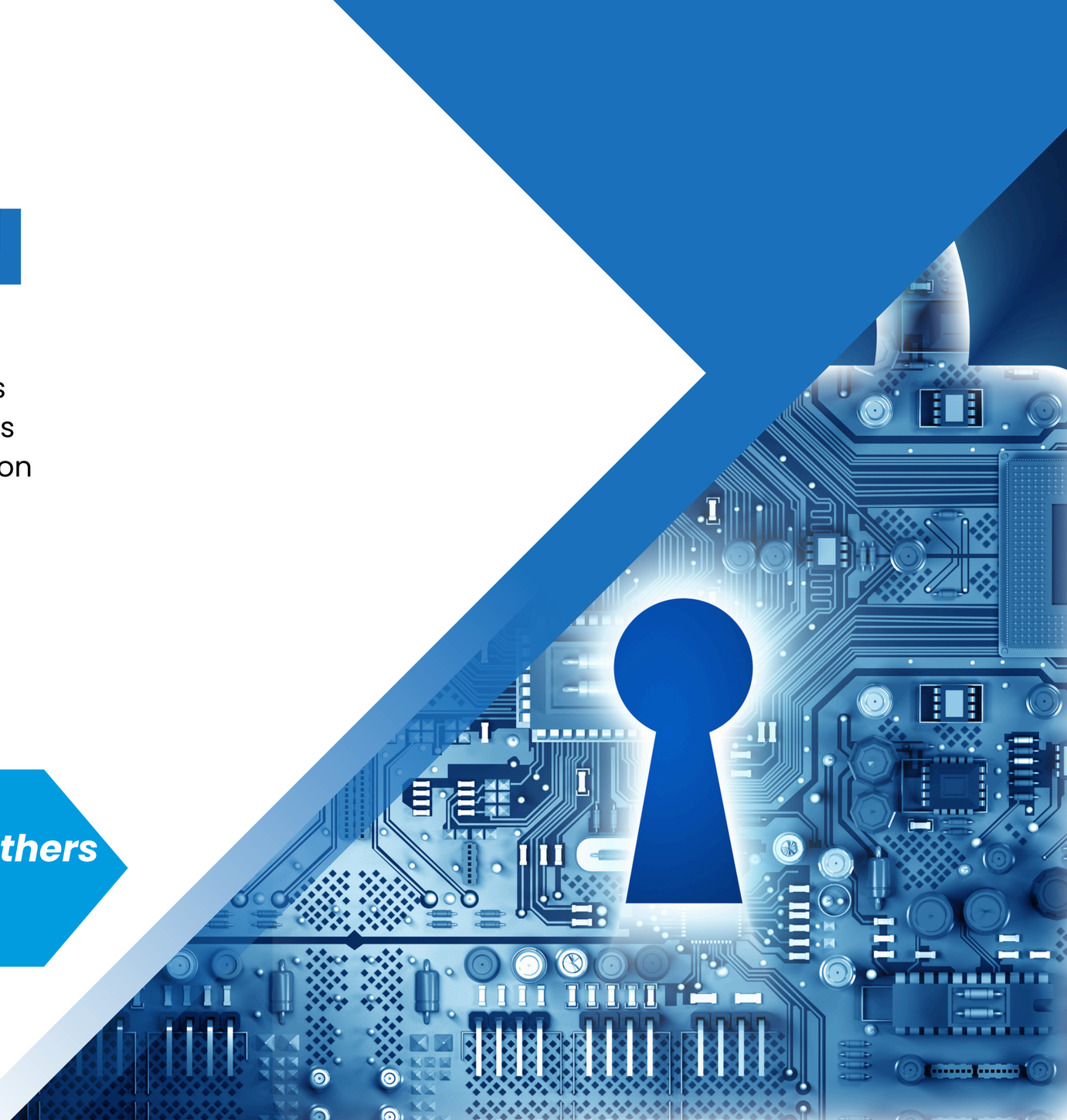
INTRODUCTION

Reconnaissance is also known as Footprinting and information gathering phase, in this phase hacker gathers information about a target before launching an attack. It is during this phase that the hacker finds valuable information such as old passwords, names of important employees.

These data include important areas such as:

– Finding out specific IP addresses
– TCP and UDP services
– Identifies vulnerabilities

This phase the Hacker identifies and gathers information about critical assets



ELEMENTS OF INFORMATION SECURITY

Confidentiality

Assurance that the information is accessible only to those authorized to have access

Integrity

The trustworthiness of data or resources in terms of preventing improper or unauthorized changes

Availability

Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users

Authenticity

Refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine

Non-Repudiation

A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

ELEMENTS OF INFORMATION SECURITY

Information security relies on five major elements: **confidentiality**, integrity, availability, authenticity, and non-repudiation.

Confidentiality

Confidentiality is the assurance that the information is accessible only to authorized individual.

Confidentiality breaches may occur due to improper data handling or a hacking attempt.

Confidentiality controls include data classification, data encryption, and proper disposal of equipment (such as DVDs, USB drives, computers,cell phones etc.).

ELEMENTS OF INFORMATION SECURITY

Information security relies on five major elements: confidentiality, **integrity**, availability, authenticity, and non-repudiation.

Integrity

Integrity:

Data integrity is the accuracy, completeness, consistency, and reliability of data throughout its entire lifecycle. It involves using processes and rules to ensure data is not corrupted, altered, or lost, making it trustworthy for decision-making and protecting against security risks.

ELEMENTS OF INFORMATION SECURITY

Information security relies on five major elements: confidentiality, integrity, **availability**, authenticity, and non-repudiation.

Availability

Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include disk arrays for redundant systems and clustered machines, antivirus software to combat malware, and distributed denial-of-service (DDoS) prevention systems.

ELEMENTS OF INFORMATION SECURITY

Information security relies on five major elements: confidentiality, integrity, availability, **authenticity**, and non-repudiation.

Authenticity

The major role of authentication is to confirm that a user is genuine. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, and documents.

ELEMENTS OF INFORMATION SECURITY

Information security relies on five major elements: confidentiality, integrity, availability, authenticity, and **non-repudiation.**

Non-Repudiation

Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.

RECONNAISSANCE TECHNIQUES:

Footprinting (also known as reconnaissance) is gathering information about the victim, the word reconnaissance is a military word meaning the process of obtaining information about enemy forces or mission into enemy territory to obtain information.
In information security, reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities.
The attacker first discovers any vulnerable ports by using software like **port scanning**. After a port scan, an attacker usually exploits known vulnerabilities of services associated with open ports that were detected during the footprinting phase.

Footprinting is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools. This information is very useful to a hacker who is trying to crack a whole system.

RECONNAISSANCE TECHNIQUES:

There are two types of Footprinting that can be used:

Active Footprinting:
Passive Footprinting:

Active Footprinting is the process of using tools and techniques, such as performing a ping sweep or using the traceroute command, to gather information on a target. Active Footprinting can trigger a target ‘s Intrusion Detection System (IDS) and may be logged and thus requires a level of stealth to do successfully.

Passive Footprinting is the process of gathering information on a target by passive means. Browsing the target ‘s website, visiting social media profiles of employees, searching for the website on **WHOIS**, and performing a **Google search** of the target are all ways of passive Footprinting. **Passive Footprinting** is the stealthier method since it will not trigger a target ‘s IDS or otherwise alert the target of information being gathered.
WHOIS s a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The current refinement of the **WHOIS protocol** was drafted by the **Internet Society** and is documented in **RFC 3912.**

RECONNAISSANCE TECHNIQUES:

Reconnaissance Using Advanced Google Hacking Techniques:

Google hacking refers to the use of **advanced Google search operators** for creating complex search queries to extract sensitive or hidden information. The accessed information is then used by attackers to find vulnerable targets. **Footprinting using advanced Google hacking techniques** involve locating specific strings of text within search results using advanced operators in the Google search engine.

Advanced Google hacking refers to the art of creating complex search engine queries. Queries can retrieve valuable data about a target company from Google search results. Through Google hacking, an attacker tries to find websites that are vulnerable to exploitation. Attackers can use the **Google Hacking Database (GHDB),** a database of queries, to identify sensitive data. Google operators help in finding the required text and avoiding irrelevant data. Using advanced Google operators, attackers can locate specific strings of text such as specific versions of **vulnerable web applications.** When a query without advanced search operators is specified, Google traces the search terms in any part of the webpage, including the title, text, URL, digital files, and so on. To confine a search, Google offers **advanced search operators**. These search operators help to narrow down the search query and obtain the most relevant and accurate output.

RECONNAISSANCE TECHNIQUES:

Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

RECONNAISSANCE TECHNIQUES:

1. Reconnaissance:

This is the first step of Hacking. It is also called as Footprinting and information gathering Phase. This is the preparatory phase where Hacker collect as much information as possible about the target. Hackers usually collect information about three groups:

· Network, finding out specific IP addresses.
· Host, TCP and UDP services.
· People involved, identifies vulnerabilities.

2. Scanning:

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools.

Network Mapping: Finding the topology of network, routers, firewalls servers, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

RECONNAISSANCE TECHNIQUES:

3 Gaining Access:

This phase is where an attacker breaks into the system/network using various tools and methods. After entering into a system, Hacker has to increase his/her privilege to Administrator level so he can install an application he/she needs or modify data or hide data. At this point, the Hacker has the information he needs. So first he designs the network map and then he/she has to decide how to carry out the attack? There are many attack options, such as:

Phishing attack - Phishing refers to the practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information.

Man in the middle attack - An attacker pretends to be a legitimate sender who intercepts all the communication between the sender and receiver and hijacks the communication.

Brute Force attack - In a brute-force attack, attackers try every combination of characters until the password is broken**.**

Session hijacking - Session hijacking refers to an attack in which an attacker seizes control of a valid TCP communication session between two computers.

RECONNAISSANCE TECHNIQUES:

3 Gaining Access:

Spoofing attack - In a spoofing attack, an attacker pretends to be another user or machine (victim) to gain access. Instead of taking over an existing active session, the attacker initiates a new session using the victim's stolen credentials. Simple IP spoofing is easy to perform and is useful in various attack methods. To create new raw packets, the attacker must have root access on the machine. However, to establish a spoofed connection using this session hijacking technique, an attacker must know the sequence numbers used by a target machine.

DOS attack – an overwhelming volume of malicious traffic is sent, which results in a DoS attack to authorized users, thus obstructing legitimate traffic and making the endpoints unable to communicate with each other. **(Denial Of Service) attack**.

DDoS Attack: An attacker converts the devices into an army of **botnets** to target a specific system or server, making it unavailable to provide services.

Buffer overflow attack - The attacker exploits various buffer overflow vulnerabilities that exist in ICS software, such as HMI web interface, ICS web client, communications interfaces, etc., to inject malicious data and commands to modify the normal behavior and operations of the systems. (**Industrial Control Systems** software).

Attacker uses Shodan (https://www.shodan.io) and searches for vulnerable in **Industrial Control Systems (ICSs)**
After gaining access to the ICS, the attacker attempts to gain access to the HVAC system remotely through the ICS

RECONNAISSANCE TECHNIQUES:

4. Maintaining Access:

Hacker may just hack the system to show it was vulnerable or he/she can be so mischievous that he/she wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using **Trojans, Rootkits** or other malicious files. The aim is to maintain access to the target until he finishes the tasks he planned to accomplish in that target.

5. Clearing Track:

No Hacker wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him/her. Hacker does this by:

. Clearing the cache and cookies
. Modifying registry values
. Modifying/corrupting/deleting the values of logs
. Clearing out sent emails
. Closing all the open ports
. Uninstalling all applications that he/she used

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

1.Perform footprinting through search engines:

. Information gathering using advance Google hacking techniques.
. information gathering from **video search engines**.
. Information gathering from **FTP search engines.**
. Information gathering from **IoT search engines**

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

2.Perform footprinting through web services:

. Locate a company’s domains and sub-domains using **Netcraft**.
. Gather personal information by using **PeekYou** online people search service
. Gather an email list using **theHarvester**
. Gather information using deep and dark web searching
. Determine target **OS** through **passive footprinting**

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

3.Perform footprinting through social networking sites:

. Gather employee information from Linkedin using **theHarvester**
. Gather personal information from various social networking sites using **Sherlock**

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

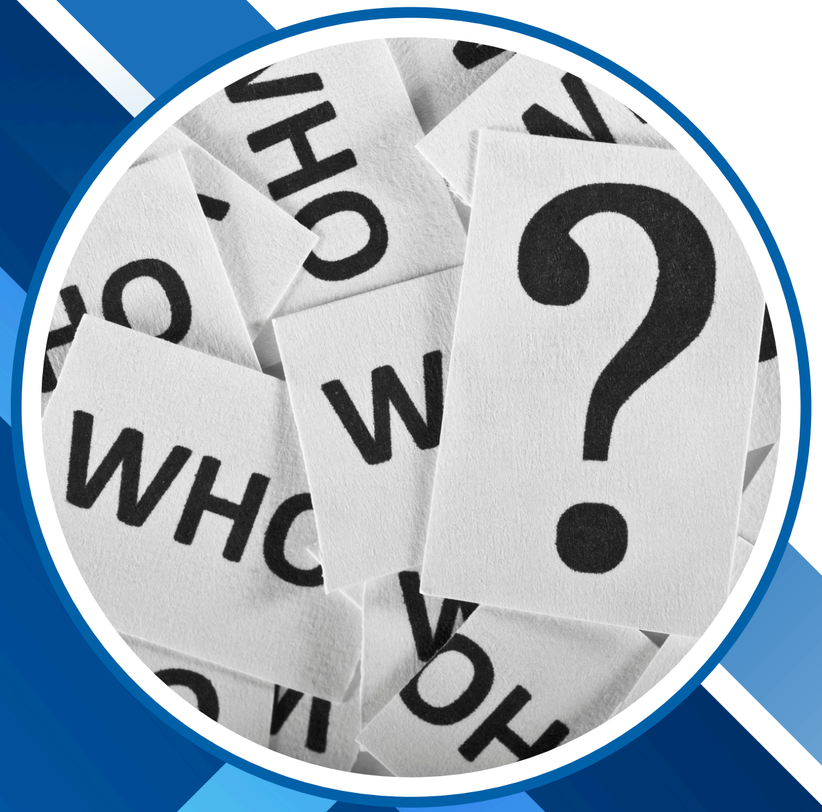
4.Perform website footprinting:

. Gather information about a target website using **ping command line utility, Photon, Central Ops, GRecon.**
. Extract a company's data using **Web Data Extractor**
. Mirror a target website using **HTTrack Web Site Copier.**
. Gather a wordlist from the target website using **CeWL**

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

5. Perform email footprinting:

. Gather information about a target by tracking email using **eMailTrackerPro**



FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

6.Perform Whois footprinting:

. Perform Whois lookup using **DomainTools**

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

7. Perform DNS footprinting:

. Gather DNS information using **nslookup** command line utility and online tool
. Perform reverse DNS lookup using reverse **IP domain check and DNSRecon**
. Gather information of subdomain and DNS records using **SecurityTrails**

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

8 .Perform Network footprinting:

. Locate the network range
. Perform network tracerouting in Windows and Linux Machines

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER INCLUDE:

9. Perform footprinting using various footprinting tools:

. Footprinting a target using **Recon-ng**
. Footprinting a target using **Maltego**
. Footprinting a target using **OSRFramework**
. Footprinting a target using **FOCA**
. Footprinting a target using **BillCipher**
. Footprinting a target using **OSINT Framework**

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER SUMMARY:

Performing footprinting through Search Engines:

Search engines are used to gather as much information about the target organization by performing footprinting using search engines. Examples of major search engines include **Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.**

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER SUMMARY:

Footprint Using Advanced Google Hacking Techniques:

- **Query String:** Google hacking refers to creating complex search queries in order to extract sensitive or hidden information.
- **Vulnerable Targets:** It helps attackers to find vulnerable targets.
- **Google Operators:** It uses advanced Google search operators to locate specific strings of text within the search results.
-

Google Advance Search Operators:

Launch any browser such as Mozilla Firefox. In the address bar type https://www.google.com and press Enter.

You can use the following to perform an advance search to gather more information about the target organization from publicly available sources. Advance Google Search operator can help attackers and pen testers to extract login pages of the target organization’s website.

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER SUMMARY:

Google supports several advanced operators:

- **[cache:]** Displays the web pages stored in the Google cache. This operator allows you to view cached version of the web page. **[cache: www.abababbab.org]**
- **[link:]** Lists web pages that have links to the specified web page. This operator searches websites or pages that contain link to the specified website or page. **[link: www.abababbab.org]**
- **[related:]** Lists web pages that are similar to a specified web page. **[related: www.abababbab.org]**
- **[info:]** Presents some information that Google has about a particular web page. [info: eccouncil.org]
- **[site:]** Restricts the results to those websites in the given domain
- **[allintitile:]** Restricts the results to those websites with all of the search keywords in the title
- **[intitle:]** Restricts the results to documents containing the search keyword in the title
- **[allinurl:]** Restricts the results to those with all of the search keywords in the URL
- **[inurl:]** Restricts the results to documents containing the search keyword in the URL

FOOTPRINTING TECHNIQUES USED BY ETHICAL HACKER SUMMARY:

Cleaning Tracks or Covering Tracks:

The finale of ethical hacking revolves around ensuring the hacker remains under the radar. This implies wiping logs, concealing files, and manipulating timestamps to eliminate evidence or proof of any attack. The intention is to ensure that attackers can never be detected or traced via their attack methodology.

Hacker Tools Used:

- CCleaner
- Stealth Rootkit
- Timestomp

Standard Methods for Covering Tracks:

- **Log Tampering:** Deleting or modifying logs to erase evidence of hacking activities.
- Steganography: Hiding malicious files or data within legitimate files to avoid detection.
- **File Timestamp Alteration:** Changing the timestamps of modified files to mislead investigators.
- **Clearing Command Histories:** Deleting or altering shell command histories to prevent detection.
- **Encryption:** Encrypting communication and files to obscure activities makes forensic analysis more difficult.

FOOTPRINTING TECHNIQUES FOOTNOTES:

Footnote Source:
https://ktflash.gitbooks.io/ceh_v9/content/222_footprinting_using_advanced_google_hacking_tec.html

Footnote Source:
EC-Council:
https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking

Footnote Source:
Palo Alto Networks:
https://www.paloaltonetworks.com/resources

FOOTPRINT CONCLUSION

The primary goal of footprinting in ethical hacking is to gather as much information as possible about a target to identify potential attack vectors. This includes collecting data on network infrastructure, employee contact details, security policies, and host information to build a comprehensive picture of the target's digital and physical assets

Key objectives of footprinting:

Identify Attack Surface
Map the target’s infrastructure
Collect sensitive information
Plan the attack

cybermcbean@cybermcbean.com

www.cybermcbean.com

_https://www.youtube.com/@gmmcdigital1976

THANK YOU

FOR YOUR ATTENTION AND PARTICIPATION

PRESENTATION - 2025

Presented By: Gordon Mcbean (CEH)