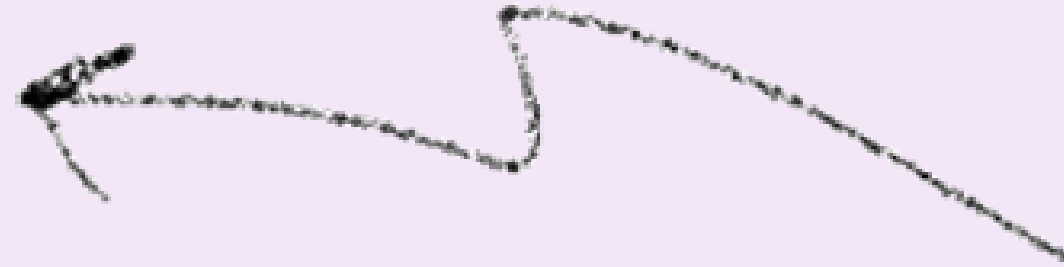


Session 1



Footprinting and Reconnaissance

Footprinting and Reconnaissance



What is Footprinting

Footprinting is the first step of any attack on information systems in which an attacker **collects information about a target network** to identify various ways to intrude into the system

Types of Footprinting

Passive Footprinting

Gathering information about the target **without direct interaction**

Active Footprinting

Gathering information about the target **with direct interaction**

Information Obtained in Footprinting



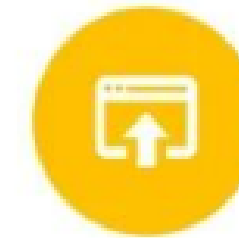
Organization information

- Employee details
- Telephone numbers
- Branch and location details
- Background of the organization
- Web technologies
- News articles, press releases, and related documents



Network information

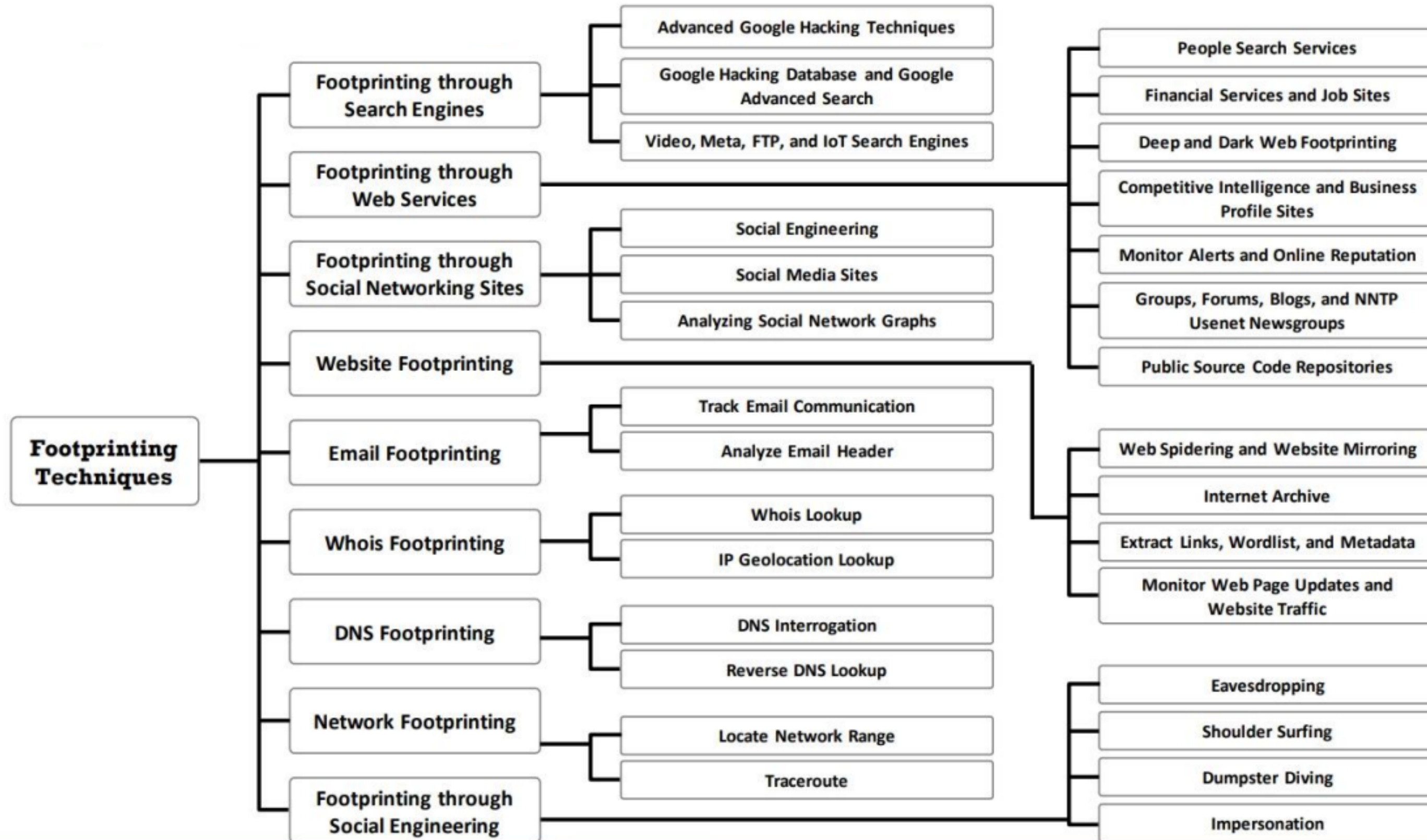
- Domain and sub-domains
- Network blocks
- Network topology, trusted routers, and firewalls
- IP addresses of the reachable systems
- Whois records
- DNS records



System information

- Web server OS
- Location of web servers
- Publicly available email addresses
- Usernames and passwords

Footprinting Techniques



Footprinting Through Search Engines

- Attackers use search engines to **extract information about a target**, such as employed technology platforms, employee details, login pages, and intranet portals, which help the attacker to perform social engineering and other types of advanced system attacks

- Major search engines:

Google

Bing

YAHOO!

Ask.com

Aol.

Baidu 百度

DuckDuckGo

- Attackers can use **advanced search operators** available with these search engines and create complex queries to find, filter, and sort specific information about the target

- Search engines are also used to find other sources of **publically accessible information resources**, e.g., you can type “top job portals” to find major job portals that provide critical information about the target organization

Footprinting Through Search Engines

- 1. Gather information using advanced Google hacking techniques**
- 2. Gather information from IoT search engine**

Google Hacking

- Google hacking refers to the use of advanced Google search operators for **creating complex search queries** to extract sensitive or hidden information that helps attackers **find vulnerable targets**

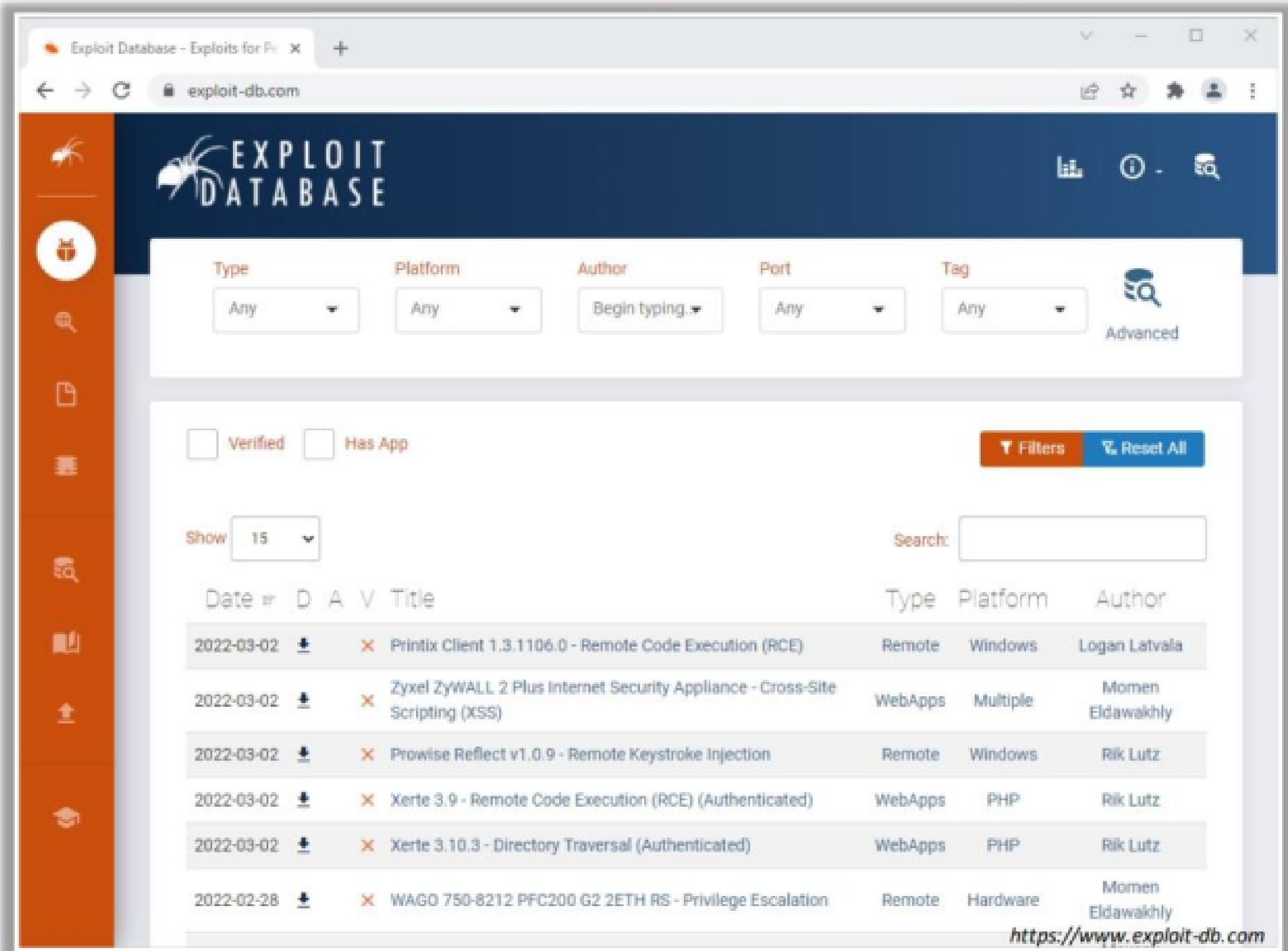
Popular Google advanced search operators

Search Operator	Purpose	Search Operator	Purpose
[cache:]	Displays the web pages stored in the Google cache	[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[link:]	Lists web pages that have links to the specified web page	[intitle:]	Restricts the results to documents containing the search keyword in the title
[related:]	Lists web pages that are similar to the specified web page	[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[info:]	Presents some information that Google has about a particular web page	[inurl:]	Restricts the results to documents containing the search keyword in the URL
[site:]	Restricts the results to those websites in the given domain	[location:]	Finds information for a specific location

Exploit Database

- The Google Hacking Database (GHDB) is an authoritative source for **querying the ever-widening reach of the Google search engine**
- Attackers use **Google dorks** in Google advanced search operators to extract sensitive information about their target, such as vulnerable servers, error messages, sensitive files, login pages, and websites

**EXPLOIT
DATABASE**



The screenshot shows the Exploit Database website interface. At the top, there's a navigation bar with the site logo and search icons. Below this is a filter section with dropdown menus for Type, Platform, Author, Port, and Tag, along with an 'Advanced' search icon. A 'Verified' checkbox and 'Has App' checkbox are also present. A 'Show 15' dropdown and a 'Search:' input field are located above the exploit list. The list itself has columns for Date, D (Download), A (Add), V (Vote), Title, Type, Platform, and Author. The first few entries are:

Date	D	A	V	Title	Type	Platform	Author
2022-03-02	+	+	+	Printix Client 1.3.1106.0 - Remote Code Execution (RCE)	Remote	Windows	Logan Latvala
2022-03-02	+	+	+	Zyxel ZyWALL 2 Plus Internet Security Appliance - Cross-Site Scripting (XSS)	WebApps	Multiple	Momen Eldawakhly
2022-03-02	+	+	+	Prowise Reflect v1.0.9 - Remote Keystroke Injection	Remote	Windows	Rik Lutz
2022-03-02	+	+	+	Xerte 3.9 - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	Rik Lutz
2022-03-02	+	+	+	Xerte 3.10.3 - Directory Traversal (Authenticated)	WebApps	PHP	Rik Lutz
2022-02-28	+	+	+	WAGO 750-8212 PFC200 G2 2ETH RS - Privilege Escalation	Remote	Hardware	Momen Eldawakhly

The URL <https://www.exploit-db.com> is visible in the bottom right corner of the browser window.

Why Google Hacking ?

- Information Gathering
- Finding Vulnerable Systems
- Exploiting Misconfigurations
- Identifying Targets
- Gathering Email Addresses
- Enumerating Subdomains
- Gathering Intelligence
- Finding Exploitable IoT Devices
- Identifying Weak Passwords
- Locating Vulnerable Webcams or Cameras

Other Techniques

Footprinting Technique	Description	Information Gathered	Tools Used
Google Advanced Search	Provides the same precision as that achieved with advanced operators but without typing or remembering the operators	List of sites that may link back to the target organization's website	Google Advanced Search
Advanced Image Search			Google Advance Image Search
Reverse Image Search	Uses an image as a search query	Original source and details of images, such as photographs, profile pictures, and memes	Google Image Search, TinEye Reverse Image Search, and Yahoo Image Search
Video Search Engines	Search for video content related to the target	Hidden information such as time/date and thumbnails	YouTube Metadata, YouTube DataViewer, and EZGif
Meta Search Engines	Use other search engines (Google, Bing, Ask.com, etc.) to produce their own results from the Internet	Detailed information about the target, such as images, videos, blogs, and news articles, from different sources	Startpage and MetaGer
FTP Search Engines	Search for files located on FTP servers	Critical files and directories that reveal valuable information, such as business strategy, tax documents, and employees' personal records	NAPALM FTP Indexer and FreewareWeb FTP File Search
IoT Search Engines	Crawl the Internet for IoT devices that are publicly accessible	Manufacturer details, geographical location, IP address, hostname, and open ports of IoT devices	Shodan, Censys, and Thingful

Other Techniques

- IOT Search Engines
- Find the company's domains and sub-domains using Netcraft
- Gather an email list using theHarvester
- Determine target OS through passive footprinting (Censys)
- Gather personal information from various social networking sites using Sherlock
- Perform Whois lookup