Social Media Recon

Social Media Reconnaissance is a key part of the information gathering phase, often using Open-Source Intelligence (OSINT) to collect data about a target company or their employees from publicly available social media profiles.

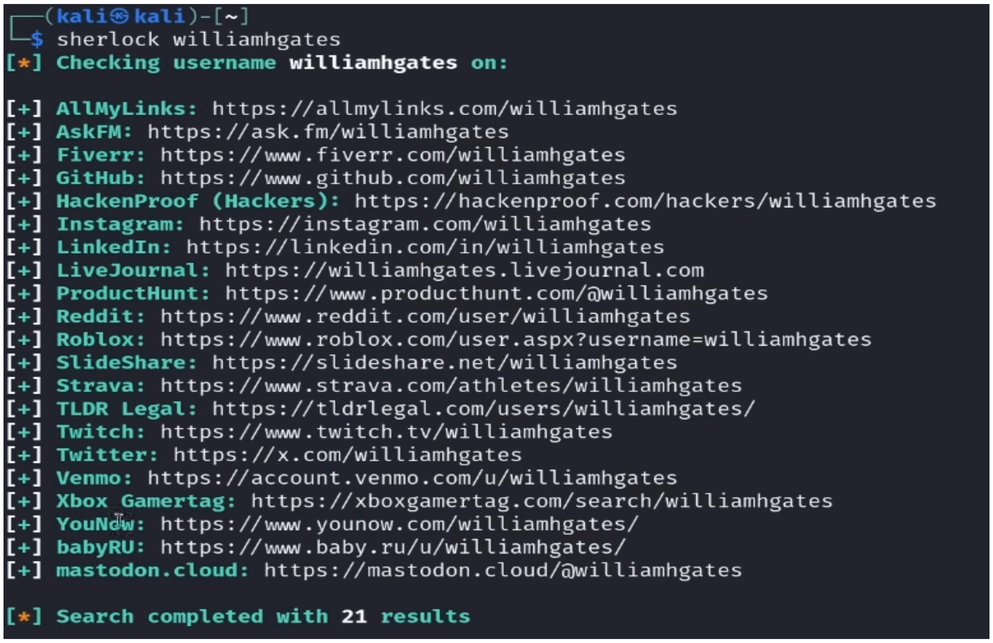
Platform	**Type of Information**	**Potential Use in Attack/Assessment**
LinkedIn	Job titles, employee names, reporting structure, company size, technology stack (from job descriptions), office locations.	Identifying key personnel (executives, IT staff), crafting highly specific phishing emails (spear phishing).
Facebook/Instagram	Personal interests, friends/family names, location data (from check-ins, geotagged photos), birthday, travel plans.	Developing a rapport for social engineering, guessing passwords (pet names, family names), timing physical intrusions (when target is away).
Twitter/X	Complaints, company-related issues, opinions on software/tech, communication style, current events/activities.	Identifying potential insider threats, discovering forgotten third-party vendor connections.
YouTube	Videos related to the company, home office setup (revealing hardware/software), internal events, training videos.	Visual reconnaissance, understanding internal culture/processes.

Commands and Tools

1. Username Searching (Tool-Based)

This technique uses an automated tool to check if a specific username is registered across hundreds of social media platforms simultaneously.

Tool	Type	Installation Command (Kali/Linux)	Execution Command Example	Link
Sherlock	Python Script (Recommended)	pip install sherlock (or clone the repository for Kali)	sherlock username_to_search	GitHub: Sherlock
Namechk	Online Tool	N/A (Web-based)	N/A (Enter username on the website)	Namechk Website



```
┌──(kali㉿kali)-[~]
└─$ sherlock williamhgates
[*] Checking username williamhgates on:

[+] AllMyLinks: https://allmylinks.com/williamhgates
[+] AskFM: https://ask.fm/williamhgates
[+] Fiverr: https://www.fiverr.com/williamhgates
[+] GitHub: https://www.github.com/williamhgates
[+] HackenProof (Hackers): https://hackenproof.com/hackers/williamhgates
[+] Instagram: https://instagram.com/williamhgates
[+] LinkedIn: https://linkedin.com/in/williamhgates
[+] LiveJournal: https://williamhgates.livejournal.com
[+] ProductHunt: https://www.producthunt.com/@williamhgates
[+] Reddit: https://www.reddit.com/user/williamhgates
[+] Roblox: https://www.roblox.com/user.aspx?username=williamhgates
[+] SlideShare: https://slideshare.net/williamhgates
[+] Strava: https://www.strava.com/athletes/williamhgates
[+] TLDR Legal: https://tldrlegal.com/users/williamhgates/
[+] Twitch: https://www.twitch.tv/williamhgates
[+] Twitter: https://x.com/williamhgates
[+] Venmo: https://account.venmo.com/u/williamhgates
[+] Xbox Gamertag: https://xboxgamertag.com/search/williamhgates
[+] YouNow: https://www.younow.com/williamhgates/
[+] babyRU: https://www.baby.ru/u/williamhgates/
[+] mastodon.cloud: https://mastodon.cloud/@williamhgates

[*] Search completed with 21 results
```

2. Reverse Image Search

This is used to find where an image (like a profile picture) appears on the web to uncover linked accounts.

Tool/Engine	Type	Primary Use Case	Link
Google Images	Search Engine	Broad search sometimes finds older/cached results.	Google Images (Use the camera icon)
Yandex Image Search	Search Engine	Often superior for finding similar faces and regional results (especially Russian-language sites).	Yandex Images
TinEye	Search Engine	Excellent for finding an image's first appearance and original source.	TinEye Website
PimEyes	Search Engine	Advanced facial recognition search engine (use with caution and respect privacy).	PimEyes Website

3. Metadata Analysis (EXIF Data)

This technique extracts hidden information (like GPS coordinates, camera model, and time stamp) from image and document files.

Tool	Type	Installation Command (Kali/Linux)	Execution Command Example	Link
ExifTool	Command Line Utility (Recommended)	`sudo apt-get install libimage-exiftool-perl`	`exiftool /path/to/image.jpg`	ExifTool Website
Jeffrey's EXIF Viewer	Online Tool	N/A (Web-based)	N/A (Upload file on the website)	Jeffrey's EXIF Viewer

Metapicz	Online Tool	N/A (Web-based)	N/A (Upload file or provide URL)	Metapicz Website

4. Google Dorking/Advanced Search

Google Dorking (or Google Hacking) uses special operators to filter search results for specific, often sensitive, information.

Operator	Action	Social Media Recon Example
site:	Restricts the search to a specific domain.	site:linkedin.com "John Doe" "Company Name" "VP of IT"
intitle:	Searches for the keyword in the page's title.	intitle:"index of" site:targetcompany.com (Searching for exposed directories)
filetype:	Searches for a specific file extension.	site:targetcompany.com filetype:pdf "employee list"
inurl:	Searches for a keyword in the URL.	inurl:resume filetype:doc site:targetcompany.com
"	Forces an exact match for a phrase.	site:facebook.com "I hate my job at Target Company"