

Forum:[Hack Forums](#)

Thread: [Recon & Information Gathering](#)

W1NK1LL3RX - August 21, 2025, 7:38 am

RECONNAISSANCE & INFORMATION GATHERING

WHAT IS RECON

Recon is the first step in any engagement. Before you ever think about exploiting something you need to learn as much as you can about the target. This includes domains, emails, open ports, technologies, employees, social media, and even small breadcrumbs like document metadata. Good recon can take hours or even days but it always pays off. The more you know the more precise and effective your actions will be later.

TOOLS FOR RECON

Here are some useful programs and services you can start with. Mix and match them depending on what type of target you are analyzing.

- [Nmap](#) – Network scanner for open ports and services.
- [Shodan](#) – Search engine for devices and networks exposed to the internet.
- [OSINT Framework](#) – Organized index of recon tools.
- [Maltego](#) – Visual link analysis, connects people, domains, emails, IPs.
- [Sublist3r](#) – Subdomain enumeration tool.
- [Google Hacking DB](#) – Search queries for finding exposed files, directories, or logins.
- [Recon-NG](#) – Full-featured reconnaissance framework.
- [Nirsoft Utilities](#) – Windows-based tools for network and forensic recon.
- [SpiderFoot](#) – OSINT automation with over 200 modules.
- [Shodan Explore](#) – Browse existing indexed data instead of scanning yourself.

These tools let you collect technical data (ports, domains, IP ranges) as well as personal data (emails, employee profiles, exposed documents).

METHODS OF INFORMATION GATHERING

Recon is split into two main categories.

Passive Recon:

This means gathering information without directly interacting with the target. Examples: searching WHOIS records, scanning through LinkedIn employees, using Shodan, running Google Dorks, checking DNS history.

Active Recon:

This means probing the target directly. Examples: scanning ports with Nmap, enumerating subdomains, fingerprinting web servers, grabbing banners. This is more likely to be detected and logged so take precautions.

Other useful approaches:

- Document Metadata – Tools like [FOCA](#) extract metadata from PDFs, Word docs, and images.
- Social Media Recon – Collect public info from Twitter, Instagram, LinkedIn.
- DNS Enumeration – Find hidden domains with [DNSRecon](#) or Sublist3r.
- Breach Data – Search if target emails are in leaks at [Have I Been Pwned](#).

The goal is to paint a complete picture of the target environment before moving forward.

BEST PRACTICES

Do not rush recon. The more patient you are the more you will find. Always verify results from multiple tools instead of trusting one scan. Keep detailed notes and organize your findings otherwise you will lose track fast. Never run scans from your personal IP always through VPN or a VPS. Rotate tools if one gets flagged. Think like a detective you are piecing together a puzzle one small detail at a time.

FINAL THOUGHT

Reconnaissance is where hacking actually begins. The more you know about a target the easier the rest becomes. Weak points are almost always revealed during careful information gathering. Tools are important but mindset is more important be curious, thorough, and methodical. In hacking information is power and recon is how you collect it.