Reconnaissance Methodology Checklist

Eyad Islam El-Taher

November 24, 2025

Scope Clarification

- ☐ Identify target domain(s)
- ☐ Check allowed TLD and subdomains
- ☐ Determine in-scope IP ranges
- ☐ Read program rules and restrictions
- ☐ Note rate limiting and automation policies

Passive Reconnaissance

Subdomain Enumeration

- ☐ Subdomains Enum ⇒ DNS & VHOST
- ☐ Certificate Transparency (crt.sh)
- ☐ DNS archives (SecurityTrails, DNSDumpster)
- ☐ favicon.ico hash search (Shodan)
- ☐ Search engine dorks (Google dorks)
- ☐ GitHub/Leaks search (GitHub dorks)
- ☐ Wayback & web Archive

Note: Best OSINT + dorks reference: `https://www.lopseg.com.br/`

Public Footprinting

- ☐ WHOIS info review
- ☐ ASN mapping
- ☐ Technology fingerprinting & Identify outdated technologies
- ☐ Telegram data bots
- ☐ Linked systems discovery

Active Reconnaissance

Service Discovery

- ☐ Port scanning
- ☐ Banner grabbing
- ☐ WAF detection
- ☐ Bbot Tool

Web Asset Mapping

- ☐ sitemap.xml & robots.txt
- ☐ Crawl site structure
- ☐ Hidden directories
- ☐ Parameter discovery
- ☐ Identify exposed development endpoints