**INFROMATION GATHERING:**

Information gathering (also known as reconnaissance or recon) is the first phase of ethical hacking or penetration testing, where the goal is to collect as much relevant data as possible about a target system, organization, or individual. This phase helps attackers (or ethical hackers) understand their target's digital footprint and potential weaknesses before attempting any kind of intrusion.

**Here Tools:**

| **Tool** | **Use** |
| --- | --- |
| Nmap | Port scan, service/OS detection |
| Netcat | Network testing, backdoor, banner grabbing |
| Hping3 | Packet crafting, firewall testing |
| Xprobe2 | OS detection |
| Telnet | Banner grabbing |
| Unicornscan | Fast scanning |
| Amap | Application detection on ports |
| WhatWeb | Web tech detection |
| Dig | DNS info |
| Masscan | Fastest port scanner |
| Traceroute | Find network path |
| Enum4linux | Windows SMB enumeration |
| Curl/Wget | Get HTTP headers or page content |
| Metasploit | Full penetration toolkit including scanning |

**Advance tools:**

| **Tool** | **Use** | **Notes** |
| --- | --- | --- |
| 🔸 **ZMap** | Internet-wide high-speed scanning | 1M packets/sec |
| 🔸 **Scanless** | Port scan using online scanners (hides your IP) | Very stealthy |
| 🔸 **Nessus** | Vulnerability & service detection | Advanced GUI scanner |
| 🔸 **OpenVAS** | Enterprise-level vulnerability scanner | Open-source Nessus alternative |
| 🔸 **RustScan** | Blazing fast port scanner + Nmap integration | Rust-based, lightweight |
| 🔸 **Nmap NSE Scripts** | Advanced service & vuln scanning via scripting | nmap --script vuln |
| 🔸 **EyeWitness** | Captures screenshots of live web services | For web recon |
| 🔸 **Aquatone** | Web screenshot tool + port scanner | Good for subdomain scanning |
| 🔸 **Censys CLI** | Search internet-exposed services & SSL certs | OSINT + active |
| 🔸 **Shodan CLI/API** | Active service data from Shodan database | Needs API key |
| 🔸 **ARP-Scan** | Local network live host discovery | Better than ping sweep |
| 🔸 **Sn1per** | Automatic recon + vulnerability scanner | All-in-one toolkit |
| 🔸 **Recon-ng** | Recon framework with modules (also active modules available) | Terminal interface |
|  |  |  |
|  |  |  |
| 🔸 **Metasploit Scanner Modules** | Built-in modules for services like FTP, SSH, SMB | Use auxiliary/scanner/... |
| 🔸 **Netdiscover** | Active network discovery on LAN | Used in internal testing |

**AI-Powered Tools:**

| **Tool/Platform** | **Type** | **Use Case / Features** |
| --- | --- | --- |
| 🔸 **ReconAI** | AI Recon Bot | Automated reconnaissance using AI-driven decisions |
| 🔸 **Sn1per AI Mode** | Auto recon + AI logic | Uses basic AI logic for prioritizing vulnerabilities |
| 🔸 **Intrigue.io** | Recon platform | Uses ML to track assets, services, CVEs automatically |
| 🔸 **Darktrace** | Network AI | Learns network behavior, flags anomalies (used in blue team too) |
| 🔸 **Maltego with NLP plugins** | Graph recon + AI NLP | Maps relationships, uses NLP to extract entities from text |
| 🔸 **ChatGPT / LLMs** | AI Assistant | Helps generate commands, analyze results, write scripts |
| 🔸 **ReconFTW + GPT** | Recon Framework | Can be customized to include GPT to parse recon data |
| 🔸 **Eyewitness + AI OCR** | Screenshot analysis | Use OCR (Optical Character Recognition) to auto-analyze screenshots |
| 🔸 **Shodan AI Filters** | Cloud-based Recon | Uses AI to tag devices, guess usage, filter by service risk |
| 🔸 **Amass (with AI plugin)** | Subdomain Discovery | Can be extended using AI/NLP for smarter DNS logic |

**AI Tools with Links:**

| **Tool / Platform** | **Description** | **Link / Source** |
| --- | --- | --- |
| **ReconAI** | AI-based recon bot for automated reconnaissance | (Experimental GitHub repos, search “ReconAI” on GitHub) |
| **Sn1per AI Mode** | Automated recon with AI prioritization | <https://github.com/1N3/Sn1per> |
| **Intrigue.io** | Asset discovery and CVE tracking with ML | <https://intrigue.io/> |
| **Darktrace** | Enterprise AI for network anomaly detection | <https://www.darktrace.com/> |
| **Maltego + NLP Plugins** | Graph recon with AI-powered natural language processing | <https://www.paterva.com/web7/> |
| **ChatGPT / LLMs** | General AI assistant for command generation and analysis | <https://chat.openai.com/> (ChatGPT) |
| **ReconFTW + GPT** | Recon framework with GPT integration | <https://github.com/six2dez/reconftw> |
| **EyeWitness + AI OCR** | Screenshots + OCR for web recon | <https://github.com/FortyNorthSecurity/EyeWitness> |
| **Shodan AI Filters** | AI-driven filtering for Shodan data | <https://www.shodan.io/> |
| **Amass (AI Plugin)** | Subdomain enumeration with AI enhancements | <https://github.com/OWASP/Amass> |

**My Top Recommended:**

| **Tool** | **Why Use It** | **When to Use** |
| --- | --- | --- |
| **Nmap** | Most powerful, versatile scanner | Basic to advanced port and service scanning, OS detection, scripts |
| **Masscan** | Ultra-fast port scanning | When you need to scan large IP ranges quickly |
| **Sn1per** | Automated recon + vulnerability scan | Quick, comprehensive recon with some AI logic |
| **EyeWitness** | Visual reconnaissance (screenshots) | When you want to identify login pages, admin panels, or phishing sites |
| **Amass** | Deep subdomain enumeration | Discovering hidden subdomains and DNS info |
| **Recon-ng** | Modular recon framework | Structured recon with scripts and automation |
| **Netcat** | Banner grabbing and basic connectivity tests | Manual probing, testing open ports |
| **Hping3** | Packet crafting and firewall testing | Advanced network testing and evasion |
| **WhatWeb** | Web technology detection | Quickly identify web servers, frameworks, CMS |
| **Shodan** | Internet-wide device discovery | Discover exposed devices and services online |

**Top Tor Browser & Tor-Based Tools:**

| **Tool** | **Use Case / Features** | **Notes** |
| --- | --- | --- |
| **Tor Browser** | Browse .onion websites anonymously | <https://www.torproject.org/> |
| **Torsocks** | Force command-line tools to route traffic through Tor | Use with Nmap, Curl, Netcat, etc. |
| **OnionScan** | Scan and analyze Tor hidden services (.onion) | <https://github.com/s-rah/onionscan> |
| **Ahmia** | Search engine for Tor (.onion) websites | <https://ahmia.fi/> |
| **TorBot** | Crawl and index .onion websites automatically | <https://github.com/Ph055a/TorBot> |
| **DarkSearch.io** | Dark web search engine (free API) | <https://darksearch.io/> |
| **Recon-ng + Tor Proxy** | Automate recon via Tor routing | Set up SOCKS proxy with Tor |
| **Metasploit over Tor** | Run scans through Tor using proxies | Configure proxychains + Tor |
| **Onioff** | Monitor the status of .onion services | <https://github.com/k4m4/onioff> |
| **TorGhost** | Routes all your system traffic through Tor | <https://github.com/susmithHCK/TorGhost> |
| **CrawlTor** | Crawl .onion links recursively | <https://github.com/kingtuna/CrawlTor> |
| **Kali + Tor Setup** | Full Tor environment setup on Kali Linux | Proxychains, torsocks, tor installed |