FireCompass

SaaS platform for Continuous Recon (Attack Surface Management) &
Automated Pen Testing & Red Teaming

Top 10 Tools for Reconnaissance

As the digital landscape evolves, the threat of data breaches grows, with over 4.5 billion records compromised in recent years. Reconnaissance, the initial step in a cyber-kill chain according to Lockheed-Martin Corporation, involves the research, identification, and selection of targets, aiming to pinpoint vulnerabilities within a network. This document outlines the top tools for reconnaissance that are essential for understanding and securing digital perimeters in 2024.

Understanding Reconnaissance in Cyber Security

Reconnaissance, or recon, is a critical strategy used by hackers to gather information about their target before launching an attack. This preparatory step is crucial as it allows the attacker to identify potential vulnerabilities and plan their attack accordingly. The process of reconnaissance involves thorough research, identification of potential targets, and attempts to uncover weaknesses in the target's defenses.

1. FireCompass RECON

FireCompass RECON employs sophisticated techniques akin to those used by nation-state actors. This platform automatically discovers an organization's dynamic digital attack surface, including unknown exposed databases, cloud buckets, code leaks, exposed credentials, risky cloud assets, and open ports among others. It enables continuous reconnaissance for a dynamic perimeter to discover external attack surfaces, shadow risks, and complete asset inventory, identifying all possible vulnerabilities from known and unknown assets.

➢ Learn about AI powered FireCompass Continuous Recon assets

2. Maltego CE

Maltego CE is an interactive data mining tool that renders data in graph form for analysis. It is primarily used for online investigations to uncover connections between information from various sources. Maltego saves time for security professionals by providing a powerful search that yields smarter results. It is especially useful when access to hidden information is critical to success, aiding in the visualization of interconnected links between searched items.

3. Google

Google, along with other search engines like Bing, is an indispensable tool for continuous cyber reconnaissance. These search engines provide vital data about individuals, companies, and leaked content. The information is freely available and can significantly influence the direction a penetration tester will take during their investigation.

4. Recon-Ng

Recon-Ng is a web-based reconnaissance tool written in Python, favored by penetration testers for its intuitive functionalities that allow for the rapid collection of web-based information.

Shodan, one of the first search engines for internet-connected devices, offers real-time intelligence on the latest technological trends and supports other recon tools like Nmap, Metasploit, Maltego, and FOCA with its APIs.

5. Shodan

Shodan, one of the first search engines for internet-connected devices, offers real-time intelligence on the latest technological trends and supports other recon tools like Nmap, Metasploit, Maltego, and FOCA with its APIs.

➢ Get a free demo: Hacker’s view of your attack surface

6. Censys

Censys provides an avenue to gather data regarding all your assets to help you prevent target attacks. This tool provides actionable insights and helps you track changes in all your assets and identify potential vulnerabilities. Click here to access the user guide.

7. nMap

nMap is among the best **network recon tools** used by both hackers and pen testers. nMap scans networks to determine available hosts, running services and operating systems, and whether the network is using network filters like a firewall.

8. Spiderfoot

Spiderfoot is a **continuous cyber recon tool** that automatically queries over 100 public data sources. This tool gathers intelligence on IP addresses, domain names, and emails among others. During recon, you specify which modules to activate based on the information that you need. Find more details here.

9. Dataspoilt

An #OSINT Framework to perform various recon techniques on Companies, People, Phone Number, Bitcoin Addresses, etc., aggregate all the raw data, and give data in multiple formats.

Datasploit is useful to collect relevant information about a target in order to expand your attack and defense surface very quickly. The feature list includes:

- Automated OSINT on domain/email/username/phone for relevant information from different sources.
- Useful for penetration testers, cyber investigators, defensive security professionals, etc.
- Correlates and collaborative results show them in a consolidated manner.
- Tries to find out credentials, API keys, tokens, subdomains, domain history, legacy portals, and more as related to the target.
- Available as a single consolidating tool as well as standalone scripts.
- Performs Active Scans on collected data.
- Generates HTML and JSON reports along with text files.
- More details here and here

10. Aquatone

A Tool for Domain Flyovers. AQUATONE is a set of tools for performing reconnaissance on domain names. It can discover subdomains on a given domain by using open sources as well as the more common subdomain dictionary brute force approach

More details here and here.

With FireCompass, eliminate the need for repetitive manual effort!

"Traditional Recon involves multiple tools and manual effort. FireCompass eliminates the need for repetitive manual effort and significantly helps to improve delivery speed.”

See it for yourself!