

**CYBERSECURITY TOOLS AND HOW TO USE**

**1. Information Gathering:**

These tools are primarily used for reconnaissance to gather data about networks, servers, websites, and devices.

* **Nmap**: A network scanning tool for discovering hosts, open ports, and services.
  + **Tutorial**: Learn to scan networks using Nmap to detect live hosts and open ports Nmap Guide.
* **Shodan**: A search engine for internet-connected devices.
  + **Tutorial**: Search for exposed devices, such as webcams or routers, via Shodan [Shodan Guide](https://www.shodan.io/).
* **Maltego**: A tool for gathering and analyzing publicly available information.
  + **Tutorial**: Learn to visualize connections between entities using Maltego Maltego Tutorial.
* **TheHarvester**: OSINT tool for gathering emails, subdomains, and more.
  + **Tutorial**: Collect information using TheHarvester from different public sources [TheHarvester Guide](https://github.com/laramies/theHarvester).
* **Recon-NG**: A web reconnaissance framework with modules.
  + **Tutorial**: Modular information gathering through Recon-NG Recon-NG Guide.
* **Amass**: Focuses on mapping attack surfaces and asset discovery.
  + **Tutorial**: Learn asset discovery with Amass [Amass Tutorial](https://github.com/OWASP/Amass).
* **Censys**: A search engine for internet-connected devices and infrastructure.
  + **Tutorial**: Explore network scanning with Censys [Censys Guide](https://censys.io).
* **OSINT Framework**: Aggregates publicly available data sources.
  + **Tutorial**: Dive into open-source intelligence gathering using the OSINT Framework [OSINT Framework](https://osintframework.com/).
* **Gobuster**: A tool to brute-force directories and files on web servers.
  + **Tutorial**: Use Gobuster to find hidden files and directories [Gobuster Guide](https://github.com/OJ/gobuster).

**2. Password Cracking:**

Used to crack hashed or encrypted passwords by brute force or dictionary attacks.

* **John the Ripper**: A fast password cracker.
  + **Tutorial**: Perform basic and advanced password cracking John the Ripper Guide.
* **Hydra**: A parallelized login cracker.
  + **Tutorial**: Brute-force online services with Hydra [Hydra Tutorial](https://github.com/vanhauser-thc/thc-hydra).
* **Hashcat**: The world’s fastest password recovery tool.
  + **Tutorial**: Learn password hash cracking with Hashcat Hashcat Guide.
* **Ophcrack**: A tool for Windows password cracking.
  + **Tutorial**: Recover Windows passwords using Ophcrack Ophcrack Guide.
* **Medusa**: A speedy brute-force tool.
  + **Tutorial**: Crack online credentials using Medusa [Medusa Guide](https://github.com/jmk-foofus/medusa).
* **THC-Hydra**: Another powerful network login cracker.
  + **Tutorial**: Learn to brute-force with THC-Hydra [Hydra Guide](https://github.com/vanhauser-thc/thc-hydra).
* **Cain & Abel**: Focuses on Windows password recovery.
  + **Tutorial**: Use Cain & Abel for password recovery Cain & Abel Guide.

**3. Wireless Hacking:**

These tools are used for compromising or auditing wireless networks.

* **Aircrack-NG**: A suite for cracking WEP and WPA/WPA2 keys.
  + **Tutorial**: Crack wireless networks using Aircrack-NG [Aircrack-NG Guide](https://www.aircrack-ng.org/).
* **Wifite**: A tool for automating WiFi hacking.
  + **Tutorial**: Simplify WiFi attacks using Wifite [Wifite Guide](https://github.com/derv82/wifite2).
* **Kismet**: A wireless network detector and packet sniffer.
  + **Tutorial**: Sniff and analyze WiFi traffic using Kismet [Kismet Guide](https://www.kismetwireless.net/).
* **TCPDump**: A network packet analyzer.
  + **Tutorial**: Capture network traffic with TCPDump TCPDump Guide.
* **Airsnort**: A tool for recovering encryption keys from WEP networks.
  + **Tutorial**: Use Airsnort to crack WEP Airsnort Guide.
* **Netstumbler**: A wireless network discovery tool.
  + **Tutorial**: Discover wireless networks with Netstumbler [Netstumbler Guide](http://www.stumbler.net/).
* **Reaver**: A tool for brute-forcing WPA/WPA2 WiFi Protected Setup (WPS).
  + **Tutorial**: Crack WPS-enabled networks with Reaver [Reaver Guide](https://github.com/t6x/reaver-wps-fork-t6x).

**4. Vulnerability Scanning:**

These tools are used to identify vulnerabilities in systems, networks, or web applications.

* **OpenVAS**: A vulnerability scanner for identifying security issues.
  + **Tutorial**: Scan for vulnerabilities using OpenVAS [OpenVAS Guide](https://www.openvas.org/).
* **Nessus**: Another vulnerability assessment tool.
  + **Tutorial**: Perform vulnerability assessments with Nessus Nessus Guide.
* **AppScan**: A tool for application security testing.
  + **Tutorial**: Use AppScan for web application security AppScan Guide.
* **LYNIS**: A security auditing tool for Unix-based systems.
  + **Tutorial**: Audit system security using LYNIS LYNIS Guide.
* **Retina**: A vulnerability scanner.
  + **Tutorial**: Conduct vulnerability assessments with Retina [Retina Guide](https://www.beyondtrust.com/).
* **Nexpose**: A vulnerability management solution.
  + **Tutorial**: Perform vulnerability scans with Nexpose Nexpose Guide.

**5. Exploitation:**

Exploitation tools are used to take advantage of system vulnerabilities for penetration testing.

* **Burp Suite**: A web vulnerability scanner.
  + **Tutorial**: Scan and exploit web vulnerabilities with Burp Suite Burp Suite Guide.
* **Metasploit Framework**: A penetration testing framework.
  + **Tutorial**: Perform penetration testing with Metasploit [Metasploit Guide](https://www.metasploit.com/).
* **SQLMap**: A tool for exploiting SQL injection vulnerabilities.
  + **Tutorial**: Automate SQL injection with SQLMap [SQLMap Guide](https://sqlmap.org/).
* **ZAP**: A web application vulnerability scanner.
  + **Tutorial**: Use OWASP ZAP to find security vulnerabilities [ZAP Guide](https://www.zaproxy.org/).
* **ExploitDB**: A collection of public exploits and proof-of-concepts.
  + **Tutorial**: Search for exploits using ExploitDB [ExploitDB Guide](https://www.exploit-db.com/).
* **Core Impact**: A commercial penetration testing tool.
  + **Tutorial**: Conduct professional penetration tests with Core Impact Core Impact Guide.
* **Cobalt Strike**: A tool for advanced adversary simulations.
  + **Tutorial**: Perform red team operations with Cobalt Strike [Cobalt Strike Guide](https://www.cobaltstrike.com/).

**6. Forensics:**

These tools are used for digital forensics investigations, focusing on data recovery and analysis.

* **SleuthKit**: A digital forensics tool for file system analysis.
  + **Tutorial**: Investigate file systems with SleuthKit [SleuthKit Guide](http://www.sleuthkit.org/).
* **Autopsy**: A forensic platform for analyzing data.
  + **Tutorial**: Perform digital forensics using Autopsy [Autopsy Guide](https://www.autopsy.com/).
* **Volatility**: A memory forensics framework.
  + **Tutorial**: Perform memory analysis using Volatility [Volatility Guide](https://www.volatilityfoundation.org/).
* **Guymager**: A forensic imaging tool.
  + **Tutorial**: Capture forensic images using Guymager Guymager Guide.
* **Foremost**: A file carving tool for recovering deleted files.
  + **Tutorial**: Recover files using Foremost Foremost Guide.