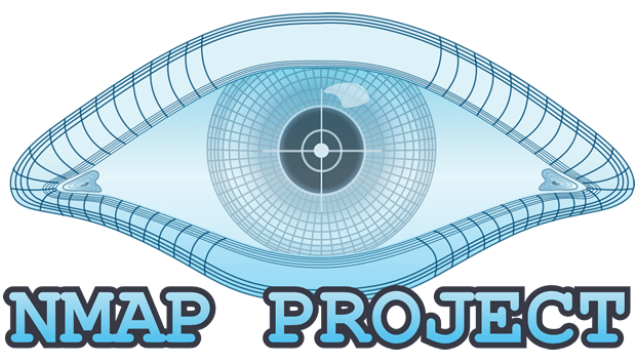
Hacker Tools Top Ten Our recommended pentesting tools for 2017

Welcome to our Hacker Tools list of 2017...

Since 2014 we've listed the web's favorite hacking/ pentesting tools as used by hackers, geeks and security engineers. This list sprung to life when we organized an online poll that was very well received and the below recommended tools are a result of what our community voted as the 'Top Ten List of Hacking Tools'. We've organized this list by including information and links to training courses for each of these tools as well as books, training course and additional information that we think will help you learn!

Our more extensive list of hacking tools is located here (https://www.concise-courses.com/hacking-tools/) that include tools from the following hacking/ pentesting categories: Application Specific Scanners, Debuggers, Encryption Tools, Firewalls, Forensics, Fuzzers, Intrusion Detection Systems, Multi Purpose Tools, Packet Crafting Tools, Packet Sniffers, Password Crackers, Port Scanners, Linux Hacking Distros, Rootkit Detectors, Traffic Monitoring Tools, Vulnerability Exploitation Tools, Vulnerability Scanners, Web Browser Related Tools, Web Proxies, Web Vulnerability Scanners and Wireless Hacking Tools.

Also....remember!
All these tools come bundled in pentesting Linux distro's (https://www.concise-courses.com/linux-distros/) such as Kali Linux (https://www.kali.org/) or BackBox, (https://backbox.org/) so we'd certainly recommend that you install an appropriate Linux hacking box to make your life easier – not least because repositories are (automatically) updated.



(https://www.concise-courses.com/hacking-tools/port-scanners/nmap/)

Recommended Nmap Courses For Beginners (https://www.concise-courses.com/nmap-courses-for-beginners/)

Learn More About Nmap (https://www.concise-courses.com/hacking-tools/port-scanners/nmap/)

Similar Tools To Nmap (https://www.concise-courses.com/hacking-tools/port-scanners/)

Nmap (Network Mapper) | Free

Used to Scan Ports and Map Networks - and a whole bunch more!

Nmap is an abbreviation of 'Network Mapper', and it's very well known free open source hackers tool. Nmap is mainly used for network discovery and security auditing. Literally, thousands of system admins all around the world will use nmap for network inventory, check for open ports, manage service upgrade schedules, and monitor host or service uptime. Nmap, as a tool uses raw IP packets in creative ways to determine what hosts are available on the network, what services (application name and version) those hosts are providing information about, what operating systems (fingerprinting) and what type and version of packet filters/ firewalls are being used by the target. There are dozens of benefits of using nmap, one of which is that fact that the admin user is able to determine whether the network (and associated nodes) need patching. Nmap's been featured in literally every hacker movie out there, not least the recent Mr. Robot series. It's also worth mentioning that there's a GUI version of Nmap called 'Zenmap'. We'd advise you to learn using Nmap (i.e. the 'command line') then rotate into Zenmap when you are feeling all confident.

(https://www.concise-courses.com/hacking-tools/multi-purpose-tools/metasploit/)

Recommended Metasploit Books (https://www.concise-courses.com/books/metasploit/)

Recommended Metasploit Courses For Beginners (https://www.concise-courses.com/metasploit-courses-for-beginners/)

Learn More About Metasploit (https://www.concise-courses.com/hacking-tools/multi-purpose-tools/metasploit/)

Similar Tools To Metasploit (https://www.concise-courses.com/hacking-tools/vulnerability-exploitation-tools/)

Metasploit Penetration Testing Software | Free & Paid

Vulnerability Exploitation Tool

The Metasploit Project is a hugely popular pentesting or hacking framework. If you are new to Metasploit think of it as a 'collection of hacking tools and frameworks' that can be used to execute various tasks. Widely used by cybersecurity professionals and ethical hackers this is a tool that you have to learn. Metasploit is essentially a computer security project (framework) that provides the user with vital information regarding known security vulnerabilities and helps to formulate penetration testing and IDS testing plans, strategies and methodologies for exploitation. There's a ton of incredibly useful Metasploit information out there and we hope that the books that we've chosen go someway to help you on your journey, not least if you are a beginner just starting out and looking for beginners tutorials in how to use Metasploit.

(https://www.concise-courses.com/hacking-tools/password-crackers/john-the-ripper/)

Recommended JTR Books (https://www.concise-courses.com/books/)

Learn More About JTR (https://www.concise-courses.com/hacking-tools/password-crackers/john-the-ripper/)

Similar Tools To JTR (https://www.concise-courses.com/hacking-tools/password-crackers/)

John The Ripper | Free

Password Cracking Tool

John the Ripper (often you'll see abbreviated as 'JTR') wins the award for having the coolest name. John the Ripper, mostly just referred to as simply, 'John' is a popular password cracking pentesting tool that is most commonly used to perform dictionary attacks. John the Ripper takes text string samples (from a text file, referred to as a 'wordlist', containing popular and complex words found in a dictionary or real passwords cracked before), encrypting it in the same way as the password being cracked (including both the encryption algorithm and key), and comparing the output to the encrypted string. This tool can also be used to perform a variety of alterations to dictionary attacks. If you are somewhat confused between John the Ripper and THC Hydra then think of John the Ripper as an 'offline' password cracker whilst THC Hydra is an "online" cracker.

(https://www.concise-courses.com/hacking-tools/password-crackers/thc-hydra/)

Recommended Hydra Books (https://www.concise-courses.com/books/)

Learn More About Hydra (https://www.concise-courses.com/books/)

Similar Tools To Hydra (https://www.concise-courses.com/hacking-tools/password-crackers/)

We Interviewed The Developer! (https://www.concise-courses.com/interview-thc-hydra/)

THC Hydra | Free

Password Cracking Tool

We've purposely placed THC Hydra underneath John The Ripper because they often go 'hand-in'hand'. THC Hydra (we've abbreviated to simply 'Hydra' throughout our site) is a hugely popular password cracker and has a very active and experienced development team. Essentially THC Hydra is a fast and stable Network Login Hacking Tool that will use dictionary or brute-force attacks to try various password and login combinations against an log in page. This hacking tool supports a wide set of protocols including Mail (POP3, IMAP, etc.), Databases, LDAP, SMB, VNC, and SSH. Take a look at John the Ripper as well.

(https://www.concise-courses.com/hacking-tools/web-vulnerability-scanners/)

Recommended OWASP Zed Books (https://www.concise-courses.com/books/)

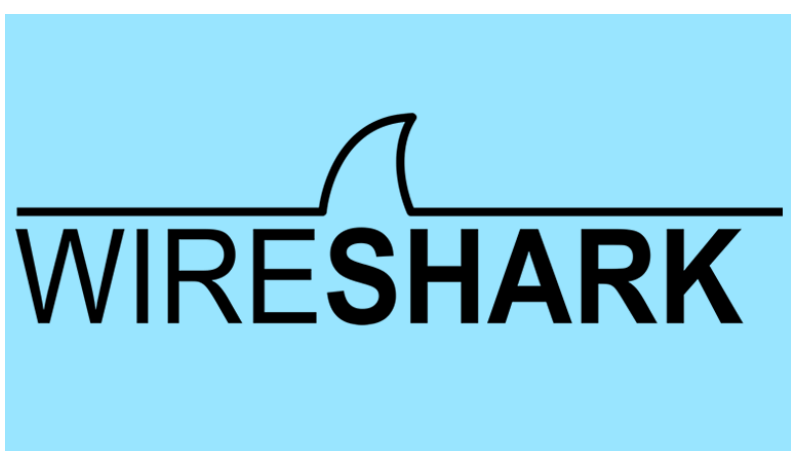
Learn More About OWASP Zed (https://www.concise-courses.com/hacking-tools/web-vulnerability-scanners/)

Similar Tools To OWASP Zed (https://www.concise-courses.com/hacking-tools/password-crackers/)

OWASP Zed | Free

Web Vulnerability Scanner

The Zed Attack Proxy (ZAP) is now one of the most popular OWASP projects. The fact that you've reached this page means that you are likely already a relatively seasoned cybersecurity professional so it's highly likely that you are very familiar with OWASP, not least the OWASP Top Ten Threats listing which is considered as being the 'guide-book' of web application security. This hacking and pentesting tool is a very efficient as well as being an 'easy to use' program that finds vulnerabilities in web applications. ZAP is a popular tool because it does have a lot of support and the OWASP community is really an excellent resource for those that work within Cyber Security. ZAP provides automated scanners as well as various tools that allow you the cyber pro to discover security vulnerabilities manually. Understanding and being able to master this tool would also be advantageous to your career as a penetration tester. If you are a developer then you have it's obviously highly recommended that you learn how to become very proficient with this 'hacker tool!'



(https://www.concise-courses.com/hacking-tools/packet-crafting-tools/wireshark/)

Recommended Wireshark Books (https://www.concise-courses.com/books/wireshark/)

Recommended Wireshark Courses For Beginners (https://www.concise-courses.com/wireshark-courses-for-beginners/)

Learn More About Wireshark (https://www.concise-courses.com/hacking-tools/packet-crafting-tools/wireshark/)

Similar Tools To Wireshark (https://www.concise-courses.com/hacking-tools/packet-crafting-tools/)

Wireshark | Free

Web Vulnerability Scanners

Wireshark is a very popular pentesting tool and for over a year it was not included on our list, however, by popular demand we added it in late June 2016. Wireshark essentially captures data packets in a network in real time and then displays the data in human-readable format (verbose). The tool (platform) has been highly developed and it includes filters, color-coding and other features that lets the user dig deep into network traffic and inspect individual packets. If you'd like to become a penetration tester or work as a Cyber Security practioner, then learning how to use Wireshark is a must. There are a ton of resources out there to learn Wireshark, and, of particular interest, there's also a Wireshark Certification which you can achieve and place on your LinkedIn profile.

(https://www.concise-courses.com/hacking-tools/password-crackers/aircrack/)

Recommended Aircrack-ng Books (https://www.concise-courses.com/books/aircrack-ng/)

Learn More About Aircrack-ng (https://www.concise-courses.com/hacking-tools/password-crackers/aircrack/)

Similar Tools To Aircrack-ng (https://www.concise-courses.com/hacking-tools/password-crackers/)

Aircrack-ng | Free

Password Cracking Tool

The Aircrack suite of Wifi (Wireless) hacking tools are legendary because they are very effectively when used in the right hands. For those new to this wireless-specific hacking program, Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking hacking tool that can recover keys when sufficient data packets have been captured (in monitor mode). For those tasked with penetrating and auditing wireless networks Aircrack-ng will become your best friend. It's useful to know that Aircrack-ng implements standard FMS attacks along with some optimizations like KoreK attacks, as well as the PTW attacks to make their attacks more potent. If you are a mediocre hacker then youll be able to crack WEP in a few minutes and you ought to be pretty proficient at being able to crack WPA/ WPA2. For those interested in Wireless Hacking we'd also highly recommend taking a look at the very awesome Reaver, another very popular hacking tool that alas we couldn't add to our list.

(https://www.concise-courses.com/hacking-tools/forensics/maltego/)

Learn More About Maltego (https://www.concise-courses.com/hacking-tools/forensics/maltego/)

Maltego Books (https://www.concise-courses.com/books/)

Similar Tools To Maltego (https://www.concise-courses.com/hacking-tools/forensics/)

Maltego | Free & Paid

Digital Forensics

Maltego is different in that it works within a digital forensics sphere. Maltego is a platform that was designed to deliver an overall cyber threat picture to the

enterprise or local environment in which an organization operates. One of the awesome things about Maltego which likely makes it so popular (and included in the Kali Linux Top Ten) is its's unique perspective in offering both network and resource based entities is the aggregation of information sourced throughout the web - whether it's the current configuration of a vulnerable router within a network or the current whereabouts of your staff members on their international visits, Maltego can locate, aggregate and visualize this data! For those interested in learning how to use Maltego we'd also recommend learning about OSINT cybersecurity data procurement.

(https://www.concise-courses.com/hacking-tools/packet-sniffers/cain-abel/)

Learn More About Cain and Abel (https://www.concise-courses.com/hacking-tools/packet-sniffers/cain-abel/)

Cain and Abel Books (https://www.concise-courses.com/books/)

Similar Tools To Cain and Abel (https://www.concise-courses.com/hacking-tools/packet-sniffers/)

Cain and Abel Hacking Tool | Free

Password Cracker/ Password Hacking

Cain and Abel (often simply abbreviated to Cain) is a hugely popular hacking tool and one that is very often mentioned online in a variety of 'hacking tutorials'. At its' heart, Cain and Abel is a password recovery tool for Microsoft Windows but it can be used off-label in a variety of uses, for example, white and black hat hackers use Cain to recover (i.e. 'crack') many types of passwords using methods such as network packet sniffing and by using the tool to crack password hashes. Cain, for example, when used to crack password hashes would use methods such as dictionary attacks, brute force, rainbow table attacks and cryptanalysis attacks.

(https://www.concise-courses.com/hacking-tools/web-vulnerability-scanners/nikto/)

Learn More About Nikto (https://www.concise-courses.com/hacking-tools/web-vulnerability-scanners/nikto/)

Nikto Books (https://www.concise-courses.com/books/)

Similar Tools To Nikto (https://www.concise-courses.com/hacking-tools/web-vulnerability-scanners/)

Nikto Website Vulnerability Scanner | Free

Website Vulnerability Scanner Hacking Tool

Nikto is another classic 'Hacking Tool' that a lot of pentesters like to use. Worth mentioning that Nickto is sponsored by Netsparker (which is yet another Hacking Tool that we have also listed in our directory). Nikto is an Open Source (GPL) web server scanner which is able to scan and detect web servers for vulnerabilities. The system searches against a database of over 6800 potentially dangerous files/ programs when scanning software stacks. Nikto, like other scanners out there, also scans for outdated (up to date) versions of over 1300 servers, and version specific problems on over 275 servers. Interestingly, Nikto can also check server configuration items such as the presence of multiple index files, HTTP server options, and the platform will also try to identify

installed web servers and web applications. Nikto will get picked up by any semi-decent IDS tool so its' really useful when conducting a white-hat/ white-box pentest. Certainly a great tool to learn your skills on when attacking an open box for training.
