11 penetration testing tools the pros use

JM Porup, Josh Fruhlinger

ABSTRACT (ENGLISH)

Top penetration testing tools* Kali Linux * nmap * Metasploit * Wireshark * John the Ripper * Hashcat * Hydra * Burp Suite * Zed Attack Proxy * sqlmap * aircrack-ng Kali LinuxIf you're not using Kali Linux as your base pentesting operating system, you either have bleeding-edge knowledge and a specialized use case or you're doing it wrong. Many legitimate organizations such as insurance agencies, internet cartographers like Shodan and Censys, and risk scorers like BitSight scan the entire IPv4 range regularly with specialized port-scanning software (usually nmap competitors masscan or zmap) to map the public security posture of enterprises both large and small. Sqlmap supports all the usual targets, including MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, HSQLDB and H2. Types of penetration testing tools Some of the tools we've discussed here are virtual Swiss Army knives that can help you conduct a number of different kinds of pen tests, whereas others are more specialized.

FULL TEXT

A penetration tester, sometimes called an ethical hacker, is a security pro who launches simulated attacks against a client's network or systems in order to seek out vulnerabilities. Their goal is to demonstrate where and how a malicious attacker might exploit the target network, which allows their clients to mitigate any weaknesses before a real attack occurs.

For an in-depth look at what penetration testing entails, you'll want to read our explainer on the subject. In this article, we're going to look at one specific aspect of the pen tester's trade: the tools they use to defeat their clients' defenses. As you might expect, these are largely the same tools and techniques employed by malicious hackers.

Back in ye olde days of yore, hacking was hard and required a lot of manual bit fiddling. Today, though, a full suite of automated testing tools turn hackers into cyborgs, computer-enhanced humans who can test far more than ever before. After all, why use a horse and buggy to cross the country when you can fly in a jet plane? Here are the supersonic tools that make a modern pen tester's job faster, better, and smarter.

Top penetration testing tools* Kali Linux

* nmap
* Metasploit
* Wireshark
* John the Ripper
* Hashcat
* Hydra
* Burp Suite
* Zed Attack Proxy
* sqlmap
* aircrack-ng

Kali LinuxIf you're not using Kali Linux as your base pentesting operating system, you either have bleeding-edge knowledge and a specialized use case or you're doing it wrong. Formerly known as BackTrack Linux and maintained by the good folks at Offensive Security (OffSec, the same folks who run the OSCP certification), Kali is optimized in every way for offensive use as a penetration tester.

While you can run Kali on its own hardware, it's far more common to see pen testers using Kali virtual machines on OS X or Windows.

Kali ships with most of the tools mentioned here and is the default pentesting operating system for most use cases. Be warned, though—Kali is optimized for offense, not defense, and is easily exploited in turn. Don't keep your super-duper extra secret files in your Kali VM.

nmapThe granddaddy of port scanners, nmap—short for network mapper—is a tried-and-true pen testing tool few can live without. What ports are open? What's running on those ports? This is indispensable information for the pen tester during recon phase, and nmap is often the best tool for the job.

Despite the occasional hysteria from a non-technical C-suite exec that some unknown party is port scanning the enterprise, nmap by itself is completely legal to use, and is akin to knocking on the front door of everyone in the neighborhood to see if someone is home.

Many legitimate organizations such as insurance agencies, internet cartographers like Shodan and Censys, and risk scorers like BitSight scan the entire IPv4 range regularly with specialized port-scanning software (usually nmap competitors masscan or zmap) to map the public security posture of enterprises both large and small. That said, attackers who mean malice also port scan, so it's something to log for future reference.

MetasploitWhy exploit when you can meta-sploit? This appropriately named meta-software is like a crossbow: Aim at your target, pick your exploit, select a payload, and fire. Indispensable for most pen testers, Metasploit automates vast amounts of previously tedious effort and is truly "the world's most used penetration testing framework," as its website trumpets. An open-source project with commercial support from Rapid7, Metasploit is a must-have for defenders to secure their systems from attackers.

WiresharkWireshark doo doo doo doo doo doo... now that we've hacked your brain to hum that tune (see how easy that engagement was?), this network protocol analyzer will be more memorable. Wireshark is the ubiquitous tool to understand the traffic passing across your network. While commonly used to drill down into your everyday TCP/IP connection issues, Wireshark supports analysis of hundreds of protocols including real-time analysis and decryption support for many of those protocols. If you're new to pen testing, Wireshark is a must-learn tool.

John the RipperUnlike the software's namesake, John the Ripper doesn't serially kill people in Victorian London, but instead will happily crack encryption as fast as your GPU can go. This password cracker is open source and is meant for offline password cracking. John can use a word list of likely passwords and mutate them to replace “a” with “@” and “s” with “5” and so forth, or it can run for an infinity with muscular hardware until a password is found. Considering that the vast majority of people use short passwords of little complexity, John is frequently successful at breaking encryption.

HashcatThe self-proclaimed "world's fastest and most advanced password recovery utility" may not be modest, but the hashcat folks certainly know their worth. Hashcat gives John the Ripper a run for its money. It is the go-to pen testing tool to crack hashes, and hashcat supports many kinds of password-guessing brute force attacks, including dictionary and mask attacks.

Pen testing commonly involves exfiltration of hashed passwords, and exploiting those credentials means turning a program like hashcat loose on them offline in the hope of guessing or brute-forcing at least some of those passwords.

Hashcat runs best on a modern GPU (sorry, Kali VM users). Legacy hashcat still supports hash cracking on the CPU, but warns users it is significantly slower than harnessing your graphics card's processing power.

HydraJohn the Ripper's companion, Hydra, comes into play when you need to crack a password online, such as an SSH or FTP login, IMAP, IRC, RDP and many more. Point Hydra at the service you want to crack, pass it a word list if you like, and pull the trigger. Tools like Hydra are a reminder why rate-limiting password attempts and disconnecting users after a handful of login attempts can be successful defensive mitigations against attackers.

Burp SuiteNo discussion of pentesting tools is complete without mentioning web vulnerability scanner Burp Suite, which, unlike other tools mentioned so far, is neither free nor libre, but an expensive tool used by the pros. While there is a Burp Suite community edition, it lacks much of the functionality, and the Burp Suite enterprise edition goes

for a cool $3,999 a year (that psychological pricing doesn't make it seem that much cheaper, guys).
There's a reason they can get away with those kind of nosebleed prices, though. Burp Suite is an incredibly effective web vulnerability scanner. Point it at the web property you want to test and fire when ready. Burp competitor Nessus offers a similarly effective (and similarly priced) product.
Zed Attack ProxyThose without the cash to pay for a copy of Burp Suite will find OWASP's Zed Attack Proxy (ZAP) to be almost as effective, and it is both free and libre software. Like the name suggests, ZAP sits between your browser and the website you're testing and allows you to intercept (aka man in the middle) the traffic to inspect and modify. It lacks many of Burp's bells and whistles, but its open-source license makes it easier and cheaper to deploy at scale, and it makes a fine beginner's tool to learn how vulnerable web traffic really is. ZAP competitor Nikto offers a similar open-source tool.
sqlmapDid somebody say SQL injection? Well hello, sqlmap. This incredibly effective SQL injection tool is open-source and "automates the process of detecting and exploiting SQL injection flaws and taking over of database servers," just like its website says. Sqlmap supports all the usual targets, including MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, HSQLDB and H2. Old-timers used to have to craft their SQL injection with a hot needle to their hard drive. These days sqlmap will take the squinty-eyed work out of your pen testing gig.
aircrack-ngJust how secure is your client's Wi-Fi (or your home Wi-Fi)? Find out with aircrack-ng. This wifi security auditing tool is free/libre, but the Pringles can you'll have to acquire on your own. (We hear the darknet market at 7-11 can give you one on the down low.) Cracking Wi-Fi today is often possible because of poor configuration, bad passwords, or outdated encryption protocols. Aircrack-ng is the go-to choice for many—with or without a Pringles cantenna.
Types of penetration testing tools
Some of the tools we've discussed here are virtual Swiss Army knives that can help you conduct a number of different kinds of pen tests, whereas others are more specialized. We'll look at the categories our chosen tools fall into, and also showcase some of the best of the rest of penetration tools out there available to download.
Network penetration testing tools. The stereotypical hacker spends their days breaking into networks where they don't belong, and so a pen tester needs tools that can help them gain access to their targets' network infrastructure. Of our top picks, Kali Linux, nmap, Metasploit, Wireshark, John the Ripper, and Burp Suite all fall into this category. Other popular network pen testing tools include the packet manipulating program Scapy; w3af, an attack and audit framework; and the vulnerability scanners Nessus, Netsparker, and Acunetix.
Web application penetration testing tools. Web-facing applications are one of the primary attack surfaces that any organization needs to secure, so a pen tester will want to focus a good amount of energy there to really assess their target's security. Nmap, Metasploit, Wireshark, Jon the Ripper, Burp Suite, ZAP, sqlmap, w3af, Nessus, Netsparker, and Acunetix can all help with this task, as can BeEF, a tool that focuses on web browsers; web application vulnerability scanners Wapiti, Arachni, Vega, and Ratproxy; diresearch, a command-line tool designed to brute force directories and files on webservers; and Sn1per, an "all in one" pen testing framework.
Database penetration testing tools. If a hacker's goal is to exfiltrate valuable data, those crown jewels are generally lurking in a database somewhere, so it's important for a pen tester to have tools to pry open the locks. nmap and sqlmap are important tools for this purpose. So are SQL Recon, an active and passive scanner that specifically targets and tries to identify all Microsoft SQL Server on a network, and BSQL Hacker, an automated SQL injection tool.
Automated penetration testing tools. Finding every possible vulnerability in a target system by hand could take years. Many pen testing tools have automation features built in to speed up the process. Metasploit, John the Ripper, Hydra, Sn1per, and BSQL Hacker stand out in this regard.
Open source penetration testing tools. Pen testing has its roots in a hacking world that is deeply invested in the open source movement. All of our top tool picks other than Burp Suite are open source, as are Scapy, BeEF, w3af, Wapiti, Arachni, Vega, Ratproxy, and Sn1per.

DETAILS

Subject:	Software; Automation; Cutlery; Linux; Knives; Penetration; Tools; Cartography; Websites; Operating systems; Hackers; Network security; Passwords; Cybercrime
Business indexing term:	Subject: Automation
Publication title:	CSO (Online); Framingham
Publication year:	2021
Publication date:	Dec 13, 2021
Publisher:	Foundry
Place of publication:	Framingham
Country of publication:	United States, Framingham
Publication subject:	COMPUTERS--COMPUTER SECURITY, Criminology And Law Enforcement--Security
Source type:	Trade Journal
Language of publication:	English
Document type:	News
ProQuest document ID:	2609526331
Document URL:	https://ezproxy.semo.edu:2443/login?url=https://www.proquest.com/trade-journals/11-penetration-testing-tools-pros-use/docview/2609526331/se-2?accountid=38003
Copyright:	Copyright CXO Media, Inc. Dec 13, 2021
Last updated:	2024-01-03
Database:	ProQuest Central

LINKS

Check Full Text Finder for Full Text