The hacking tools that terrorise the internet

March 6 2015, by James H. Hamlyn-Harris

These days anyone can download the tools used for cyber crime. Credit: Ivan David Gomez Arce/Flickr, CC BY-SA

Hacking is a state of mind. Traditionally, hackers like to discover, understand and share the secrets they expose. They like to laugh at the dumb things they find. They're not necessarily in it for the money, more so for the glory of mastering the arcane technicalities of computing. Hackers form a community where the most "l33t" (pron. "leet", short for "elite") hackers gain the most respect.

But these days any "noob" (short for "newbie") can download software tools from the internet that take the hard work out of hacking. These tools are often written by malicious hackers, professional security testers or enthusiasts to increase productivity. For example, it's hard work

typing in three million IP addresses. Much easier to write a program that does it for you.

Add some features, such as automatic port scanning, banner grabbing and footprinting, and share it with fellow hackers and your "cred" (credibility) goes up. If it's a really good tool, then you can sell the rights to a commercial cyber security company and retire (or work as a consultant). It's a career path.

Here are some of the easiest and most potent tools being used by hackers, l33t and noob for both good and ill.

NMAP

Port scanning is a process of finding all of the computers on a network, and finding out all about them. It is a precursor to a malicious hacker (or a penetration tester) launching an attack. It's like a lion finding the slowest gazelle in the herd. Find all of the gazelles, test their weaknesses, pick the slowest.

Fydor wrote the NMAP port scanner in 1997 and has been adding functionality ever since. NMAP finds responding computers (by scanning IP addresses), finds services running on them (by scanning ports) and identifies operating systems.

It runs from the command line. Something as simple as "nmap 192.168.1.0/24" will scan your local network and find your router, PC, game console and phone (if they are connected) and tell you all about them.

There is a GUI version called Zenmap if you don't like typing. It also has visualisation tools which display the network.

NMAP is an essential tool for network maintenance, and I use it all the time when setting up computers, to diagnose networking problems and to find out just what my DHCP server has been doing.

SQLMap

Daniele Bellucci and Bernardo Damele A. G. wrote SQLMap in 2006, using the Python programming language. This tool takes all of the hard work out of SQL injection attacks.

SQL injection normally requires considerable knowledge of how web sites and programs like MySQL store and retrieve information from databases. SQLMap systematically scans for errors while injecting portions of SQL scripts into the target web site.

It collates the results and by brute force (trial and error) and finds the names of the databases, tables, fields in the tables and even the passwords stored in the database.

The user has to run the program from a command line (by running a Python script) and has to progressively enter longer, and more specific, commands to get the entire contents of the database, but there are handy YouTube videos which illustrate the process.

SQLMap really lowered the bar for random hacker groups, hacktivists, cyberpunks and LulzSec. It has arguably facilitated massive disclosures of private information, including names, addresses, credit card numbers and medical records. Everybody with a website should run this on their own web applications before they go live on the internet.

PUNKSpider

A small group of hackers started Hyperion Gray in 2013, demonstrating PunkSPIDER, a web application (a web site) vulnerability search tool and scanner, which allows the user to check for common vulnerabilities without having to conduct noisy and potentially illegal port-scans on a target.

PunkSPIDER does not attack or exploit web sites, but it does make it easy for web site owners to test their sites for many of the most obvious vulnerabilities. Unlike port-scanners, scans are launched from the punkSPIDER servers, so it's less likely to get you into trouble.

Wikto

This tool *will* get you into trouble. Wikto is an enhanced Windows version of Nikto –- a web application (a web site) vulnerability scanner which blasts HTTP requests at a target web site relentlessly.

It is a brute-force tool that tries to access admin pages, configuration scripts, misconfigured password files (281,000 of them) just in case they are present. After that it tests for 3,000 known web site vulnerabilities, followed by 1,500 GoogleHacks, which lists web site vulnerabilities identifiable by Google search strings.

This tool will produce so much traffic and log entries –- at the victim's server, your ISP and the NSA -– that everybody will know what you are up to. Wikto is a great tool for automatically checking for vulnerabilities on a complex web site, particularly if you don't know it's history and you need to maintain it.

LOIC

No discussion of entry-level script-kiddie tools would be complete

without the Low Orbit Ion Cannon, a "stress testing" (denial of service, or DOS) tool.

Many versions exist, written in C#, Java, Javascript, and all should be identified by your anti-virus software as malware.

LOIC blasts a web site with traffic, overwhelming it and making it unavailable to legitimate users (hence the "denial of service"). Some versions allow thousands of users to simultaneously attack a single target, where the target is chosen by just one of them. Just type in the domain name or IP address, and click on "IMMA CHARGIN MA LAZER").

LOIC and its variants (LOWC, HOIC) have been used by hacktivist members of Anonymous and 4Chan to attack (or as they might say, "exercise civil disobedience" against) businesses and governments in response to unpopular decisions, policies, laws or actions. Like any DOS tool, LOIC can have legitimate uses. Stress testing tools allow a web site developer to verify that their site can handle real-world traffic.

Don't try this at home

A word of warning: these tools (with the possible exception of PUNKSpider) should not be used on the internet.

There are criminal laws about using these improperly. They should not be used to scan/profile/attack ("test") web sites or networks that you do not own or have no legal authority to "test".

However, they are great fun to play with and great for testing your own locally-hosted or pretend web sites. Just turn off your internet connection (your router, cable modem or WiFi) before unleashing them -– to be sure.

Source: The Conversation