Information Gathering: Concept, Techniques and Tools explained

Reading time: 12 minutes

"Information is power," as the saying goes. And in most scenarios it's true: having critical information, at the right time, and especially knowing how to use it, can be a great source of power.

Of course, hacking has evolved too: nowadays you can find a lot of automated OSINT Tools that can help anyone with security research and intel reconnaissance in a way that just wasn't possible twenty years ago.

In past decades, ethical hacking and penetration testing were performed by only a few security experts. Now almost anyone can report security incidents. Ethical hacking tools allow you to scan, search and find the flaws and vulnerabilities within any company to help make their systems and applications more secure (as seen in the recent Top CVE's exploited in the wild post published a few weeks ago).

Today we'll explore the best ethical hacking tools used by modern security researchers.

TABLE OF CONTENTS

15 Ethical Hacking Tools You Can’t Miss

We’ve compiled some of the most popular penetration testing tools to help you through the first steps of a security investigation. You’ll find some of the classic tools that seem to have been around forever and some new tools that might not be familiar.

1. John the Ripper

John the Ripper is one of the most popular password crackers of all time. It's also one of the best security tools available to test password strength in your operating system, or for auditing one remotely.

This password cracker is able to auto-detect the type of encryption used in almost any password, and will change its password test algorithm accordingly, making it one of the most intelligent password cracking tools ever.

This ethical hacking tool uses brute force technology to decipher passwords and algorithms such as:

- DES, MD5, Blowfish
- Kerberos AFS
- Hash LM (Lan Manager), the system used in Windows NT / 2000 / XP / 2003
- MD4, LDAP, MySQL (using third-party modules)

Another bonus is that JTR is open source, multi-platform and fully available for Mac, Linux, Windows and Android.

2. Metasploit

Metasploit is an open source cyber-security project that allows infosec professionals to use different penetration testing tools to discover remote software vulnerabilities. It also functions as an exploit module development platform.

One of the most famous results of this project is the Metasploit Framework, written in Ruby, which enables you to develop, test and execute exploits easily. The framework includes a set of security tools that can be used to:

- Evade detection systems
- Run security vulnerability scans
- Execute remote attacks
- Enumerate networks and hosts

Metasploit offers three different versions of their software:

- Pro: ideal for penetration testing and IT security teams.

- Community: used by small companies and infosec students.
- Framework: the best for app developers and security researchers.

Supported platforms include:

- Mac OS X
- Linux
- Windows

3. Nmap

Nmap (Network Mapper) is a free open source security tool used by infosec professionals to manage and audit network and OS security for both local and remote hosts. It's one of the most popular tools in the hackers toolkit..

Despite being one of the oldest security tools in existence (launched in 1997), it continues to be actively updated and receives new improvements every year.

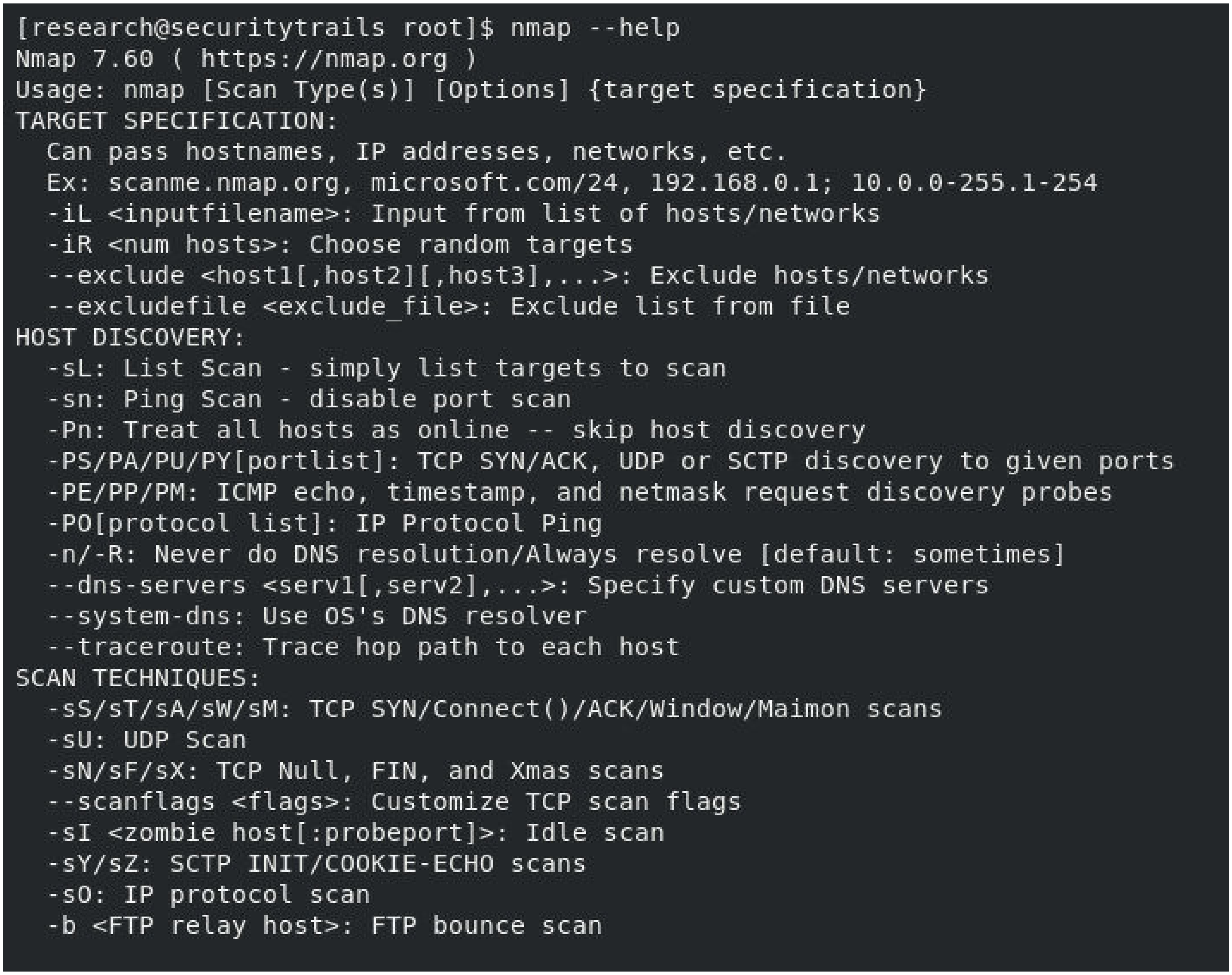
It’s also regarded as one of the most effective network mappers around, known for being fast and for consistently delivering thorough results with any security investigation.

What can you do with Nmap?

- Audit device security
- Detect open ports on remote hosts
- Network mapping and enumeration
- Find vulnerabilities inside any network
- Launch massive DNS queries against domains and subdomains

Supported platforms include:

- Mac OS X
- Linux, OpenBSD and Solaris
- Microsoft Windows



```
[research@securitytrails root]$ nmap --help
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

4. Wireshark

Wiresharkis a free open-source software that allows you to analyze network traffic in real time. Thanks to its sniffing technology, Wireshark is widely known for its ability to detect security problems in any network, as well as for its effectiveness in solving general networking problems.

While sniffing the network, you're able to intercept and read results in human-readable format, which makes it easier to identify potential problems (such as low latency), threats and vulnerabilities.

Main features:

- Saves analysis for offline inspection
- Packet browser
- Powerful GUI

- Rich VoIP analysis
- Inspects and decompresses gzip files
- Reads other capture files formats including: Sniffer Pro, tcpdump (libpcap), Microsoft network monitor, Cisco Secure IDS iplog, etc.
- Supported ports and network devices: Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI.
- Protocol decryption includes but not limited to IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Exports results to XML, PostScript, CSV, or plain text

Wireshark supports up to 2000 different network protocols, and is available on all major operating systems including:

- Linux
- Windows
- Mac OS X
- FreeBSD, NetBSD, OpenBSD

5. OpenVAS

OpenVAS (also known as the old classic “Nessus”) is an open-source network scanner used to detect remote vulnerabilities in any hosts. One of the best-known network vulnerability scanners, it’s very popular among system administrators and DevOps and infosec professionals.

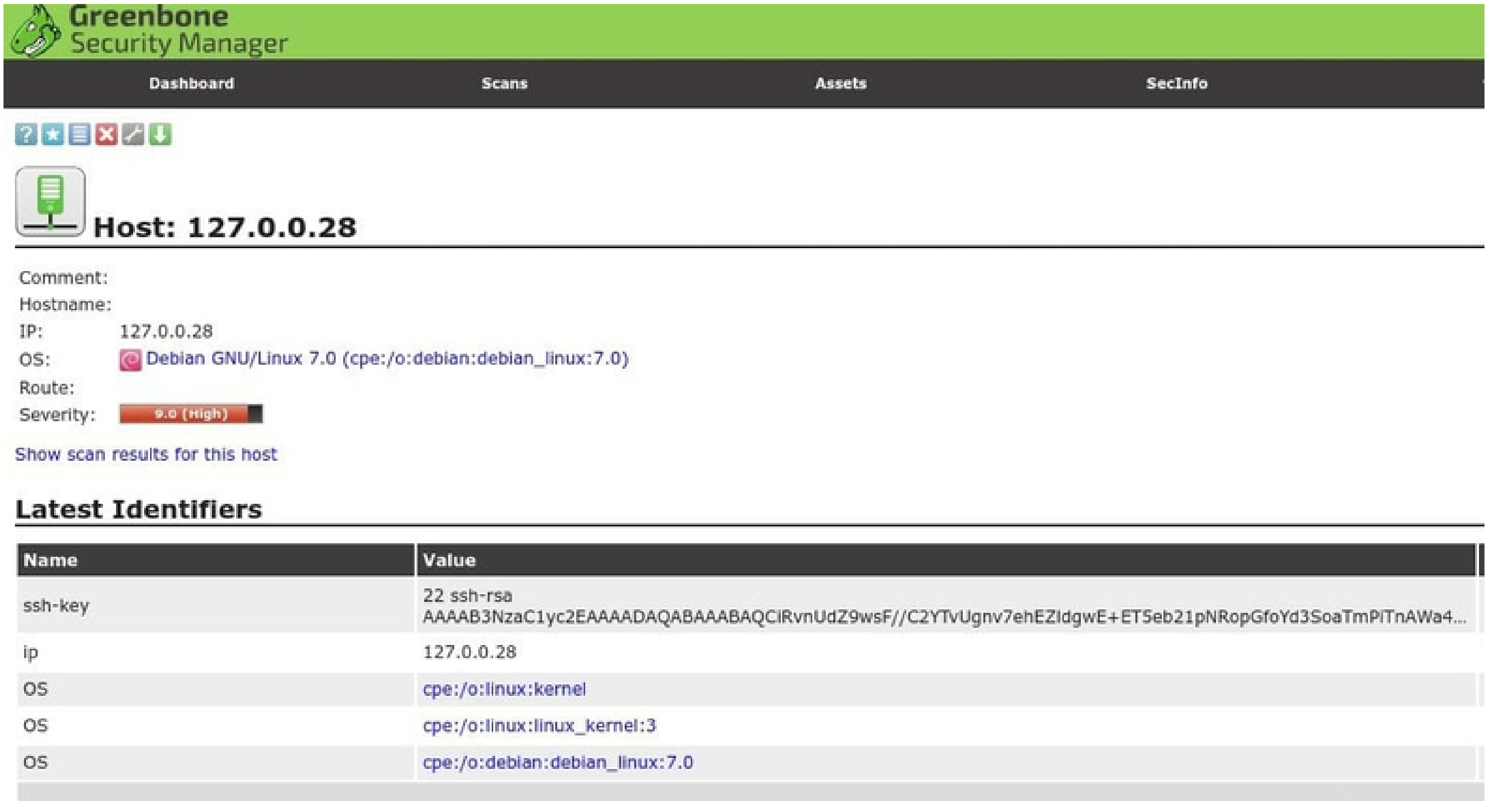
Main features

- Powerful web-based interface
- +50,000 network vulnerability tests
- Simultaneous multiple host scanning
- Able to stop, pause and resume scan tasks
- False positive management
- Scheduled scans
- Graphics and statistics generation

- Exports results to plain text, XML, HTML or LateX
- Powerful CLI available
- Fully integrated with Nagios monitoring software

While its web-based interface allows it to be run from any operating system, a CLI is also available and works well for Linux, Unix and Windows operating systems.

The free version can be downloaded from the OpenVAS website, but there is also a commercial enterprise license available from the Greenbone Security (parent company) website.



Host: 127.0.0.28

Comment:
Hostname:
IP: 127.0.0.28
OS: Debian GNU/Linux 7.0 (cpe:/o:debian:debian_linux:7.0)
Route:
Severity: 9.0 (High)

Show scan results for this host

Latest Identifiers

Name	Value
ssh-key	22 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCiRvnUdZ9wsF//C2YTvUgnv7ehEZIdgwE+ET5eb21pNRopGfoYd3SoaTmPITnAWa4...
ip	127.0.0.28
OS	cpe:/o:linux:kernel
OS	cpe:/o:linux:linux_kernel:3
OS	cpe:/o:debian:debian_linux:7.0

6. IronWASP

If you're going to perform ethical hacking, IronWASP is another great tool. It's free, open source and multi-platform, perfect for those who need to audit their web servers and public applications.

One of the most appealing things about IronWASP is that you don't need to be an expert to manage its main features. It's all GUI-based, and full scans can be performed in only a few clicks. So, if you're just getting started with ethical hacking tools, this is a great way to start.

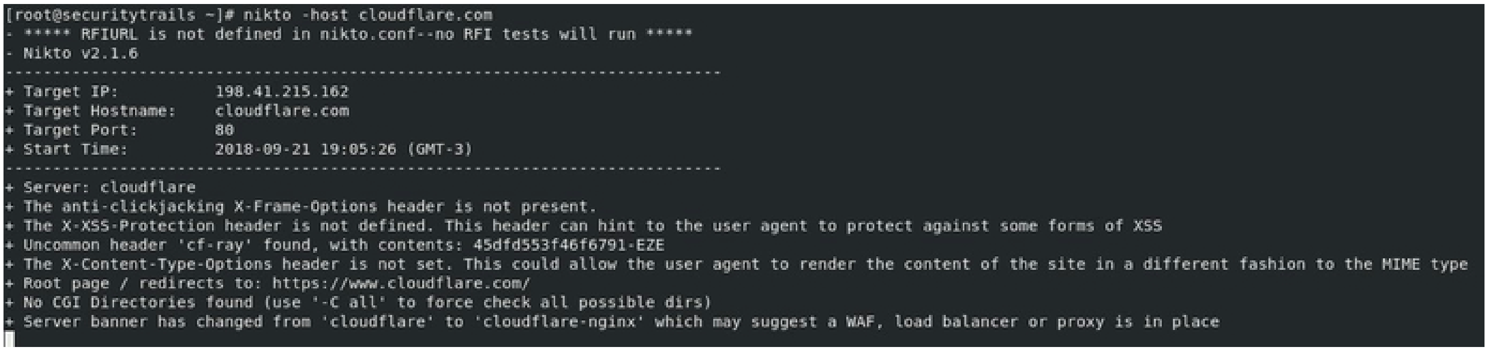
Some of its main features include:

- Powerful GUI-based interface
- Web scan sequence recording
- Exports results into HTML and RTF file format
- 25+ different web vulnerabilities
- False positive and negative management
- Full Python and Ruby support for its scripting engine
- Can be extended by using modules written in C#, Ruby, and Python
- Supported platforms: Windows, Linux with Wine, and MacOS using CrossOver

7. Nikto

Nikto is another favorite in the hackers toolkit, well-known as part of the Kali Linux Distribution. Other popular Linux distributions such as Fedora already come with Nikto available in their software repositories as well.

This security tool is used to scan web servers and perform different types of tests against the specified remote host. Its clean and simple command line interface makes it really easy to launch any vulnerability testing against your target, as you can see in the following screenshot:



```
[root@securitytrails ~]# nikto -host cloudflare.com
- ***** RFIURL is not defined in nikto.conf--no RFI tests will run *****
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          198.41.215.162
+ Target Hostname:    cloudflare.com
+ Target Port:        80
+ Start Time:         2018-09-21 19:05:26 (GMT-3)
---------------------------------------------------------------------------
+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-ray' found, with contents: 45dfd553f46f6791-EZE
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.cloudflare.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'cloudflare' to 'cloudflare-nginx' which may suggest a WAF, load balancer or proxy is in place
```

Nikto's main features include:

- Detects default installation files on any OS
- Detects outdated software applications.
- Runs XSS vulnerability tests
- Launches dictionary-based brute force attacks

- Exports results into plain text, CSV or HTML files
- Intrusion detection system evasion with LibWhisker
- Integration with Metasploit Framework

8. SQLMap

sqlmap is a cool cyber-security tool written in Python that helps security researchers to launch SQL code injection tests against remote hosts. With SQLMap you can detect and test different types of SQL-based vulnerabilities to harden your apps and servers, or to report vulnerabilities to different companies.

Its SQL injection techniques include:

- UNION query-based
- time-based blind
- boolean-based blind
- error-based
- stacked queries
- out-of-band

Main features:

- Multiple database server support: Oracle, PostgreSQL, MySQL and MSSQL, MS Access, DB2 or Informix.
- Automatic code injection capabilities
- Password hash recognition
- Dictionary-based password cracking
- User enumeration
- Get password hashes
- View user privileges and databases
- Database user privilege escalation
- Dump table information
- Executes remote SQL SELECTS

Check out the next video to see the true power of SQLMap using the sqlmap out-of-band injection working with Metasploit integration against Microsoft SQL Server:

Video could not be loaded at this time.

9. SQLNinja

SQLNinja is another SQL vulnerability scanner bundled with Kali Linux distribution. This tool is dedicated to target and exploit web apps that use MS SQL Server as the backend database server. Written in Perl, SQLNinja is available in multiple Unix distros where the Perl interpreter is installed, including:

- Linux
- Mac OS X & iOS
- FreeBSD

SQLninja can be run in different types of modes such as:

- Test mode
- Verbose mode
- Fingerprint remote database mode
- Brute force attack with a word list
- Direct shell & reverse shell
- Scanner for outbound ports
- Reverse ICMP Shell
- DNS tunnelled shell

10. Maltego

Maltego is the perfect tool for intel gathering and data reconnaissance while you're performing the first analysis of your target.

In this case, it can be used to correlate and determine relationships between people, names, phone numbers, email addresses, companies, organizations and social network profiles.

Along with online resources like Whois data, DNS records, social networks, search engines, geolocation services and online API services it can also be used to investigate the correlation between internet-based infrastructures including:

- Domain names
- DNS servers
- Netblocks
- IP addresses
- Files
- Web Pages

Main features include:

- GUI-based interface
- Analyzes up to 10.000 entities per graph
- Extended correlation capabilities
- Data sharing in real time
- Correlated data graphics generator
- Exports graphs to GraphML
- Generates entity lists
- Can copy and paste information

This application is available for Windows, Linux, and Mac OS, and the only software requirement is to have Java 1.8 or greater installed.

11. Burp Suite

Burp Suite may well be one of the most popular platforms used in the security testing and bug bounty hunting industry today. It includes several hacking tools that enable bug bounty hunters and security researchers to detect, map, analyze, and ultimately exploit vulnerabilities within the attack surface of any application.

Its main features include:

- Automated penetration testing
- Manual penetration testing techniques
- Interception of browser-based data
- Fast fuzzing and brute forcing attacks
- Automated vulnerability scanning
- Ability to perform attack analysis
- Productivity tools

12. NetStumbler

NetStumbler (also known as MiniStumbler) is one of the top ethical hacking tools used to analyze IEEE 902.11g, 802, and 802.11b networks on Windows operating systems.

Often called “the Swiss Army knife of wireless network analysis”, this hacking tool is now one of the most popular pieces of software used to find, pivot and cross-relate data from a wireless network, enabling researchers and IT administrators to find, analyze, configure and harden their wireless networks.

Key NetStumbler features and capabilities include:

- Find and explore access points
- Access point filters
- Identify access point network configuration
- Detect illegal/unauthorized access points over the network
- Find root cause of network interferences
- Analysis of signal strength over the network

13. AirCrack-ng

AirCrack-ng is a respected Wifi security suite for home and corporate security investigations. It includes full support for 802.11 WEP and WPA-PSK networks and works by capturing network packets. It then analyzes and uses them to crack Wifi access.

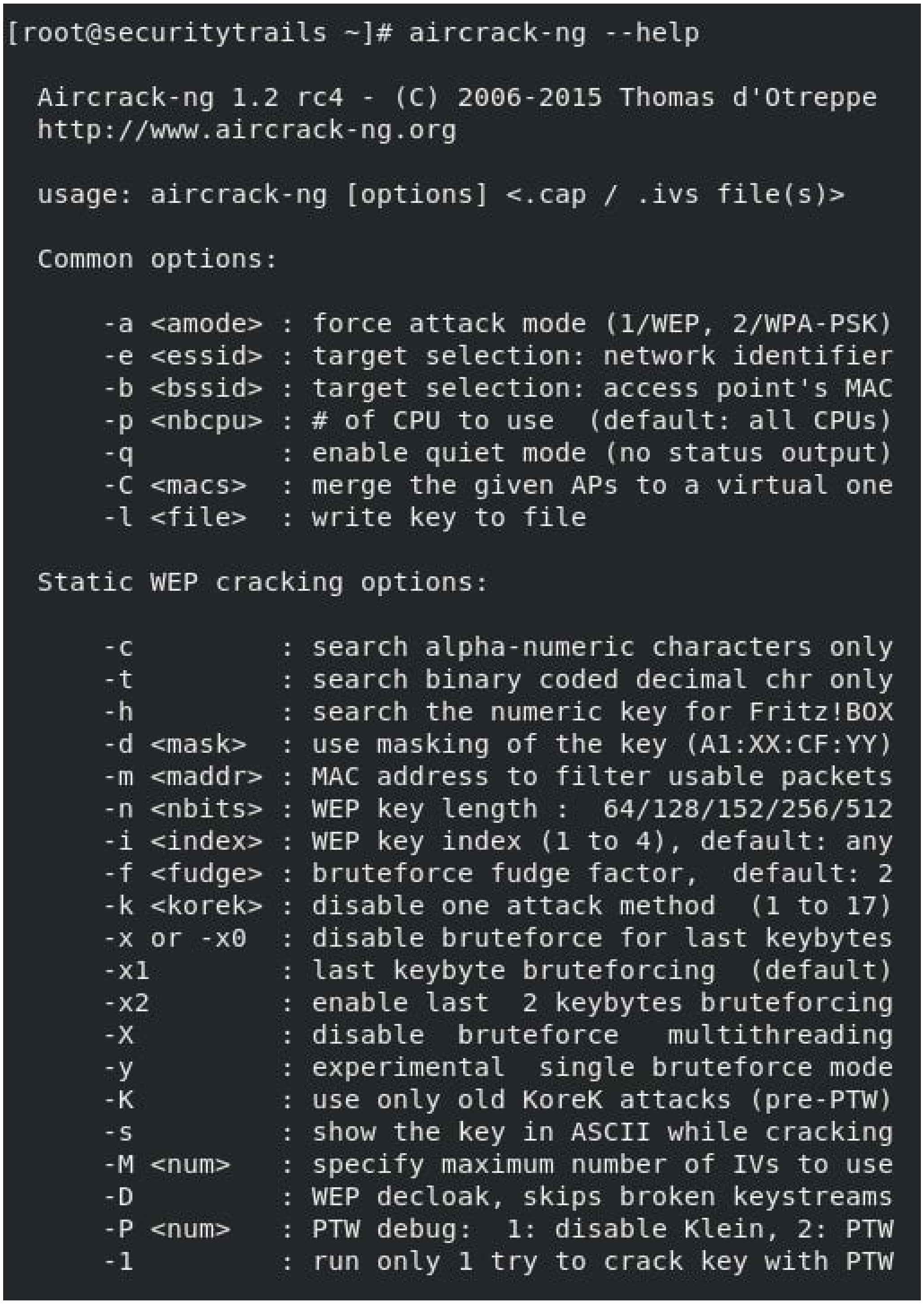
For old-school security professionals, AirCrack-ng includes a fancy terminal-based interface along with a few more interesting features.

Main features:

- Extensive documentation (wiki, manpages)
- Active community (forums and IRC channels)
- Support for Linux, Mac and Windows Wifi detection
- Launches PTW, WEP and Fragmentation attacks
- Supports WPA Migration Mode
- Fast cracking speed
- Multiple Wifi card support
- Integration with 3rd party tools

As a bonus, it comes bundled with a lot of Wifi auditing tools including:

- airbase-ng
- aircrack-ng
- airdecap-ng
- airdecloak-ng
- airdriver-ng
- aireplay-ng
- airmon-ng
- airodump-ng
- airolib-ng
- airserv-ng
- airtun-ng
- easside-ng
- packetforge-ng
- tkiptun-ng
- wesside-ng
- airdecloak-ng



```
[root@securitytrails ~]# aircrack-ng --help

  Aircrack-ng 1.2 rc4 - (C) 2006-2015 Thomas d'Otreppe
  http://www.aircrack-ng.org

  usage: aircrack-ng [options] <.cap / .ivs file(s)>

  Common options:

      -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
      -e <essid> : target selection: network identifier
      -b <bssid> : target selection: access point's MAC
      -p <nbcpu> : # of CPU to use  (default: all CPUs)
      -q         : enable quiet mode (no status output)
      -C <macs>  : merge the given APs to a virtual one
      -l <file>  : write key to file

  Static WEP cracking options:

      -c         : search alpha-numeric characters only
      -t         : search binary coded decimal chr only
      -h         : search the numeric key for Fritz!BOX
      -d <mask>  : use masking of the key (A1:XX:CF:YY)
      -m <maddr> : MAC address to filter usable packets
      -n <nbits> : WEP key length :  64/128/152/256/512
      -i <index> : WEP key index (1 to 4), default: any
      -f <fudge> : bruteforce fudge factor,  default: 2
      -k <korek> : disable one attack method  (1 to 17)
      -x or -x0  : disable bruteforce for last keybytes
      -x1        : last keybyte bruteforcing  (default)
      -x2        : enable last  2 keybytes bruteforcing
      -X         : disable  bruteforce   multithreading
      -y         : experimental  single bruteforce mode
      -K         : use only old KoreK attacks (pre-PTW)
      -s         : show the key in ASCII while cracking
      -M <num>   : specify maximum number of IVs to use
      -D         : WEP decloak, skips broken keystreams
      -P <num>   : PTW debug:  1: disable Klein, 2: PTW
      -1         : run only 1 try to crack key with PTW
```

14. Ettercap

Ettercap is a network interceptor and packet sniffer for LAN networks. It supports active and passive scans as well as various protocols, including encrypted ones such as SSH and HTTPS.

Other capabilities include network and host analysis (like OS fingerprint), as well as network manipulation over established connections -- which makes this tool great for testing man-in-the-middle attacks.

Main features

- Active and passive protocol analysis
- Filters based on IP source and destination, Mac and ARP addresses
- Data injection into established connections
- SSH and HTTPS encryption-based protocols
- Sniffs remote traffic over GRE tunnel
- Extensible with plugins
- Protocol supports include Telnet, FTP, Imap, Smb, MySQL, LDAP, NFS, SNMP, HTTP, etc.
- Determines OS name and version
- Able to kill established LAN connections
- DNS Hijacking

15. Canvas

Canvas is a great alternative to Metasploit, offering more than 800 exploits for testing remote networks.

Main features

- Remote network exploitation
- Targets different kind of systems
- Targets selected geographic regions
- Takes screenshots of remote systems
- Downloads passwords
- Modifies files inside the system
- Escalates privileges to gain administrator access

This tool also lets you use its platform to write new exploits or use its famous shellcode generator. It also integrates an alternative to nmap called scanrand, which is especially useful for port scanning and host discovery over mid to large networks.

Supported platforms include:

- Linux
- MacOSX (requires PyGTK)

- Windows (requires Python and PyGTK)

Summary

Software companies reap the most benefits from the rise of automated ethical hacking tools and penetration testing utilities, giving them more ways to increase system security every day.

Automated tools are changing the way hacking is evolving, making ethical penetration testing easier, faster and more reliable than ever. Penetration testing and reporting activities now play a crucial role in the process of identifying security flaws in remote or local software — enabling company owners to quickly prevent vulnerabilities from running wild all over the Internet.