



# 40 Top Security Tools



**Author: Dr. Eric Cole**  
**Chief Security Strategist**  
**Secure Anchor Consulting**

## 40 Top Security Tools

This document contains a list and brief description of the top 40 security tools. Obviously, the ranking of these tools is simply my opinion, and I am sure that my rankings do not align with all security experts in the field. All or part of the description of these tools might be directly taken from the works listed on the references page.

1. **Nessus** – Nessus is a remote security scanner for Linux, BSD, Solaris, and other version of UNIX. It is plugin-based, has a user interface, and performs over 1200 remote security checks. It allows for reports to be generated in HTML, XML, LaTeX, and ASCII text, and suggests solutions for security problems.
2. **Ethereal** – Ethereal is a free network protocol analyzer for UNIX and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.
3. **Snort** – Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts and much more. Snort uses a flexible rule based language to describe traffic that it should collect or pass and a modular detection engine.
4. **OpenSSH / SSH** – SSH (Secure Shell) is a program for logging into or executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel.
5. **GnuPG & PGP** – PGP is the famous encryption program by Phil Zimmerman which helps secure your data from eavesdroppers and other risks. GnuPG is a very well-regarded open source implantation of the PGP standard. While GnuPG is always free, PGP costs money.
6. **Netcat** – A simple UNIX utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be



a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool; since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

7. **Tripwire** – A file and directory integrity checker. Tripwire is a tool that aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner. An Open Source Linux version is freely available at [Tripwire.org](http://Tripwire.org).
8. **Netfilter** – Netfilter is a powerful packet filter which is implemented in the standard Linux kernel. The userspace iptables tool is used for configuration. It now supports packet filtering (stateless or stateful), all different kinds of NAT (Network Address Translation) and packet mangling.
9. **OpenSSL** – The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library.
10. **TCPDump & WinDump** – TCPDump is a well-known and widely-used text-based network packet sniffer. It can be used to print out the headers of packets on a network interface that match a given expression. You can use this tool to track down network problems or to monitor network activities. There is a separate Windows port named WinDump. TCPDump is also the source of the Libpcap/WinPcap packet capture library, which is used by many other utilities.
11. **Hping2** – Hping2 assembles and sends custom ICMP/UDP/TCP packets and displays any replies. It was inspired by the ping command but offers far more control over the probes sent. It also has a handy traceroute mode and supports IP fragmentation. This tool is particularly useful when trying to traceroute/ping/probe hosts behind a firewall that block attempts using the standard utilities.
12. **DSniff** – This popular suite by Dug Song includes many tools. Dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspay passively monitor a network for interesting data (passwords, email, files, etc.). Arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker. Sshmitm and webmitm implement



active man-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI. A separately maintained partial Windows port is available.

- 13. GFI LANguard** – LANguard scans networks and reports information such as service pack level of each machine, missing security patches, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups, and more. Scan results are outputted to an HTML report, which can be customized and queried.
- 14. Ettercap** – Ettercap is a terminal-based network sniffer for Ethernet LANs. It supports active and passive dissection of many protocols. Data injection in an established connection and filtering on the fly is also possible, keeping the connection synchronized. Many sniffing modes were implemented to give you a powerful and complete sniffing suite. It has the ability to check whether you are in a switched LAN or not, and to use OS fingerprints to let you know the geometry of the LAN.
- 15. Whisker/Libwhisker** - Whisker is a scanner which allows you to test HTTP servers for many known security holes, particularly the presence of dangerous CGIs. Libwhisker is a Perl library which allows for the creation of custom HTTP scanners.
- 16. John the Ripper** – John the Ripper is a fast password cracker, currently available for many flavors of UNIX, DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak UNIX passwords. It supports several crypt(3) password hash types which are most commonly found on various Unix flavors, as well as Kerberos AFS and Windows NT/2000/XP LM hashes. Several other hash types are added with contributed patches.
- 17. Sam Spade** – SamSpade provides a consistent GUI and implementation for many handy network query tasks. It was designed with tracking down spammers in mind, but can be useful for many other network exploration, administration, and security tasks. It includes tools such as ping, nslookup, whois, dig, traceroute, finger, raw HTTP web browser, DNS zone transfer, SMTP relay check, website search, and more.
- 18. ISS Internet Scanner** – ISS is an application-level vulnerability assessment tool. ISS Internet Scanner is pretty good, but is not cheap.



- 19. Nikto** – Nikto is a web server scanner which looks for over 2000 potentially dangerous files, CGIs and problems on over 200 servers. It uses LibWhisker but is generally updated more frequently than Whisker itself.
- 20. Kismet** – Kismet is an 802.11b network sniffer and network dissector. It is capable of sniffing most wireless cards, automatic network IP block detection via UDP, ARP and DHCP packets, Cisco equipment lists via Cisco Discovery Protocol, weak cryptographic packet logging and Ethereal and tcpdump compatible packet dump files. It also includes the ability to plot detected networks and estimated network ranges on downloaded maps or user-supplied image files.
- 21. SuperScan** – A connect-based TCP port scanner, pinger and hostname resolver. It can handle ping scans and port scans using specified IP ranges. It can also connect to any discovered open port using user-specified "helper" applications.
- 22. L0phtCrack** – L0phtCrack attempts to crack Windows passwords from hashes which it can obtain from stand-alone Windows NT/2000 workstations, networked servers, primary domain controllers, or Active Directory. In some cases it can sniff the hashes off the wire. It also has numerous methods of generating password guesses (dictionary, brute force, etc).
- 23. Retina** – Retina's function is to scan all the hosts on a network and report on any vulnerabilities found.
- 24. Traceroute** – Everyone should be very familiar with this tool as it comes with most operating systems. It can be very handy in a pinch, although for more advanced usage you may be better off with other tools.
- 25. Fport** – Fport reports all open TCP/IP and UDP ports on the machine you run it on and shows what application opened each port. So it can be used to quickly identify unknown open ports and their associated applications. It only runs on Windows, but many UNIX systems are now provided this information via netstat.
- 26. SAINT** – SAINT is another commercial vulnerability assessment tool. Unlike Windows-only tools, SAINT runs exclusively on UNIX. SAINT used to be free and open source, but is now a commercial product.
- 27. Network Stumbler** – Netstumbler is the best known Windows tool for finding open wireless access points. The tool is currently free but



Windows-only and no source code is provided. They note that "the author reserves the right to change this license agreement as he sees fit, without notice."

28. **SARA** – SARA is a vulnerability assessment tool that was derived from the infamous SATAN scanner. They try to release updates twice a month and try to leverage other software created by the open source community (such as Nmap and Samba).
29. **N-Stealth** – N-Stealth is a commercial web server security scanner. Also note that essentially all general VA tools such as nessus, ISS, Retina, SAINT, and SARA include web scanning components. They may not all be as up-to-date or flexible though.
30. **AirSnort** – AirSnort is a wireless LAN (WLAN) tool that recovers encryption keys. It was developed by the Shmoo Group and operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.
31. **NBTScan** – NBTscan is a program for scanning IP networks for NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address.
32. **Firewalk** – Firewalk employs traceroute-like techniques to analyze IP packet responses to determine gateway ACL filters and map networks. This classic tool was rewritten from scratch. Note that much or all of this functionality can also be performed by the Hping2.
33. **Cain & Abel** – Cain & Abel is a free password recovery tool for Windows. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary and Brute-Force attacks, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.
34. **XProbe2** – XProbe2 is a tool for determining the operating system of a remote host. They do this using some of the same techniques as Nmap as well as many different ideas. XProbe2 has always emphasized the ICMP protocol in their fingerprinting approach.
35. **SolarWinds Toolsets** – SolarWinds has created and sells dozens of special-purpose tools targeted at systems administrators. Security



related tools include many network discovery scanners and an SNMP brute-force cracker. These tools are Windows only.

- 36. NGrep** – NGrep strives to provide most of GNU grep's common features, applying them to the network layer. NGrep is a pcap-aware tool that will allow you to specify extended regular or hexadecimal expressions to match against data payloads of packets. It currently recognizes TCP, UDP and ICMP across Ethernet, PPP, SLIP, FDDI, Token Ring and null interfaces and understands bpf filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop.
- 37. THC-Amap** – Amap is a new but powerful scanner which probes each port to identify applications and services rather than relying on static port mapping.
- 38. NTop** – NTop shows network usage in a way similar to what Yop does for processes. In interactive mode, it displays the network status on the user's terminal. In web mode, it acts as a web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating NTop-centric monitoring applications, and RRD for persistently storing traffic statistics.
- 39. Nemesis** – The Nemesis Project is designed to be a command line based, portable human IP stack for UNIX/Linux and Windows. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts. If you enjoy Nemesis, you might also want to look at hping2. They complement each other well.
- 40. Honeyd** – Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their TCP personality can be adapted so that they appear to be running certain versions of operating systems. Honeyd enables a single host to claim multiple addresses on a LAN for network simulation. It is possible to ping the virtual machines, or to traceroute them. Any type of service on the virtual machine can be simulated according to a simple configuration file. It is also possible to proxy services to another machine rather than simulating them.



## References

- [http://www.techsupportalert.com/best\\_46\\_free\\_utilities.htm](http://www.techsupportalert.com/best_46_free_utilities.htm)
- <http://netsecurity.about.com/cs/hackertools/a/aafreewifi.htm>
- <http://www.progenic.com/>
- <http://www.insecure.org/tools.html>
- <http://www.tucows.com/downloads/Windows/IS-IT/Security/SecurityTools/>

## About Secure Anchor Consulting

Secure Anchor Consulting provides information protection services to a great number of Fortune 500 industries, as well as government, military, energy, IT and legal industries. We have coalesced the expertise of well-known and widely-respected security professionals, many of whom are respected authors and frequent speakers at venues around the globe, including the SANS Institute and BlackHat conferences.

### For More Information:

**Visit our website:**

[www.secure-anchor.com](http://www.secure-anchor.com)

**Email us:**

[info@secure-anchor.com](mailto:info@secure-anchor.com)

