

Free Security Software

Full document at

<http://www.gcasda.org/tech/index.asp?id=118>

Cross-platform

- Analog
- AWStats
- BOU
- Ethereal
- GnuPG
- John the Ripper
- Mapper
- Qualys
- Report Magic
- Webalizer

Windows

- Achilles
- Cain & Abel
- Disk Investigator
- Fport
- HackerWacker
- ITR
- MD5sums
- Network Stumbler
- NTFS Reader

DOS

- Outpost
- PuTTY
- Restoration
- Sam Spade
- Scramdisk / E4m
- Securit-e-

PortControl

- SHA verify
- SpyBot
- SuperScan
- UrlScan
- WinDump
- xorpack

Linux/UNIX

- Adzapper
- AirSnort
- Dsniff
- Ettercap
- Firewalk
- FLAG
- hping
- HUNT
- Mcrypt
- Nessus
- NetCat
- Nikto
- Nmap
- ntop
- OpenSSH
- Packit
- SARA
- SATAN
- Sniffit
- Snort
- SpamAssassin
- Squid
- ssldump
- TCP Wrappers
- TCPdump
- tcpflow
- TCT
- The Packet Master
- Wellenreiter
- Whisker

Free Security Software

Full document at

<http://www.gcasda.org/tech/index.asp?id=118>

Cross Platform

Analog

Analog shows you the usage patterns on your web server. It's Ultra-fast, Scalable, Highly configurable, Reports in 31 languages, Works on any operating system, and it's Free software. Combined with Report Magic, you can generate even prettier reports.

AWStats

AWStats is a short for Advanced Web Statistics. It's a free tool that generates advanced web (but also ftp or mail) server access statistics graphically. This log analyzer works as a CGI or from command line and shows you all possible information your log contains, in few graphical web pages. It uses a partial information file to be able to process large log files, often and quickly. It can analyze log files from IIS (W3C log format), Apache log files (NCSA combined/XLF/ELF log format or common/CLF log format), WebStar and most of all web, proxy, wap, streaming servers (and ftp servers or mail logs).

BOU

BOU (Buffer Overflow Utility) is a command-line utility that enables the user to check for buffer overflows on Web Server Applications. Written in Java, BOU quickly uncovers suspected buffer overflow problems in HTTP requests, and supports both the GET and POST methods.

Ethereal

Ethereal is a network traffic analyzer, or "sniffer", for Unix and Unix-like operating systems. It uses GTK+, a graphical user interface library, and libpcap, a packet capture and filtering library.

GnuPG

GnuPG is open-source software used to replace PGP.

John the Ripper

An active password cracking tool, john, normally called john the ripper, is a tool to find weak passwords of your users.

Mapper

Mapper helps you map the files, file parameters and values of any site you wish to test. Simply browse the site as a normal user while recording your session with Achilles (Mapper supports other proxies as well), and run Mapper on the resulting log file. Mapper will create an Excel CSV file that will

allow you to study the directory and file structure of the site, the parameter names of every dynamic page encountered (such as ASP/JSP/CGI), and their values for every time you requested them. This tool helps you to quickly locate design errors and parameters that may be prone to SQL Injection or parameter tampering problems. Mapper also supports non-standard parameter delimiters and MVC-based web sites.

Qualys

Qualys provides a free online service to scan your IP for the SANS top 20 vulnerabilities.

Report Magic

Report Magic is an add-on for Analog, a Web site logfile analysis program. Generated reports include a description with tabulated, graphed, and summarized results. All colors, fonts, and background images are completely customizable to help make resulting reports fit the theme of your Web site. Report Magic has translations for several languages. It runs on any platform that will run Perl and pre-compiled versions are available for Win32 and Mac.

Webalizer

Webalizer is a fast, free web server log file analysis program. It produces highly detailed, easily configurable usage reports in HTML format, for viewing with a standard web browser.

Linux/UNIX

Adzapper

Adzapper is a tool that works with the Squid proxy server to intercept advertising (banners, popup windows, flash animations, etc), page counters and some web bugs (as found). This has both aesthetic and bandwidth benefits. It's also easy to install.

AirSnort

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

Dsniff

By naughty.monkey.org. A suite of powerful tools for sniffing networks for passwords and other information. Includes sophisticated techniques for defeating the sniffing "protection" of network switches

Ettercap

Ettercap is a flexible tool used to sniff/log/intercept packets on a switched network.

Firewalk

Firewalking is a technique developed by MDS and DHG that employs traceroute-like techniques to analyze IP packet responses to determine gateway ACL filters and map networks. This tool employs the technique to determine the filter rules in place on a packet forwarding device. The tool also includes the option of a GTK-based graphical user interface and a few bug fixes.

FLAG

FLAG was designed to simplify the process of log file analysis and forensic investigations. Often, when investigating a large case, a great deal of data needs to be analysed and correlated. Flag uses a database as a backend to assist in managing the large volumes of data. This allows flag to remain responsive and expedite data manipulation operations. Since FLAG is web based, it is able to be deployed on a central server and shared with a number of users at the same time. Data is loaded into cases which keeps information separated. Flag also has a system for reporting the findings of the analysis by extensively using bookmarks.

hping

hping is a security tool that does TCP/IP packet assembly and analysis. hping is also capable of providing methods for testing networks and hosts.

HUNT

Advanced packet sniffer and connection intrusion. Hunt is a program for intruding into a connection, watching it and resetting it. . Note that hunt is operating on Ethernet and is best used for connections which can be watched through it. However, it is possible to do something even for hosts on another segments or hosts that are on switched ports.

Mcrypt

Mcrypt is a GPL'd tool designed to replace the old unix crypt command. Mcrypt is broken down into a library that can be used by other programs and languages and a command-line tool that can be used to encrypt and decrypt files.

Nessus

Remote network security auditor. The Nessus Security Scanner is a security auditing tool. It makes it possible to test security modules in an attempt to find vulnerable spots that should be fixed. It is made up of two parts: a server and a client. The server/daemon, nessusd, is in charge of the attacks, whereas the client, nessus, interferes with the user through nice X11/GTK+ interface. This package contains the GTK+ 1.2 client, which exists in other forms and on other platforms too.

NetCat

TCP/IP swiss army knife. 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.

Nikto

Nikto is a web server scanner which performs comprehensive tests against web servers for multiple items, including over 2200 potentially dangerous files/CGIs, versions on over 140 servers, and problems on over 210 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).

Nmap

NMap is free, open-source software that uses IP packets to explore networks and help identify vulnerabilities.

ntop

Display network usage in top-like format. Ntop is a Network Top program. It displays a summary of network usage by machines on your network in a format reminiscent of the unix top utility. It can also be run in web mode, which allows the display to be browsed with a web browser.

OpenSSH

Secure rlogin/rsh/rcp replacement (OpenSSH) OpenSSH is derived from OpenBSD's version of ssh, which was in turn derived from ssh code from before the time when ssh's license was changed to be non-free. Ssh (Secure Shell) is a program for logging into a remote machine and for 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. It is intended as a replacement for rlogin, rsh and rcp, and can be used to provide rdist, and rsync with a secure communication channel.

Packit

Packit (Packet toolkit) is a network auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic. By allowing you to define (spoof) nearly all TCP, UDP, ICMP, IP, ARP, RARP, and Ethernet header options, Packit can be useful in testing firewalls, intrusion detection/prevention systems, port scanning, simulating network traffic, and general TCP/IP auditing. Packit is also an excellent tool for learning TCP/IP.

SARA

The Security Auditor's Research Assistant. Open Source (Free) Downloadable Scanners by Advanced Research Corporation.

SATAN

SATAN (Security Auditing Tool for Analysing Networks) is a powerful tool for analyzing networks for vulnerabilities created for sysadmins that cannot keep a constant look at bugtraq, rootshell and the like.

Sniffit

A packet sniffer and monitoring tool. Sniffit is a packet sniffer for TCP/UDP/ICMP packets. Sniffit is able to give you very detailed technical info on these packets (SEC, ACK, TTL, Window, ...) but also packet contents in different formats (hex or plain text, etc.).

Snort

Snort is an open source 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.

SpamAssassin

SpamAssassin(tm) is a mail filter to identify spam. Using its rule base, it uses a wide range of heuristic tests on mail headers and body text to identify "spam", also known as unsolicited commercial email.

Squid

Squid is a high performance Web proxy cache that can be arranged hierarchically for an improvement in response times and a reduction in bandwidth usage. Squid can also be configured with URL filtering tools to reduce banner ads and popups. Squid is derived from the ARPA-funded Harvest project.

ssldump

ssldump is an SSLv3/TLS network protocol analyzer. It identifies TCP connections on the chosen network interface and attempts to interpret them as SSLv3/TLS traffic. When it identifies SSLv3/TLS traffic, it decodes the records and displays them in a textual form to stdout. If provided with the appropriate keying material, it will also decrypt the connections and display the application data traffic.

TCP Wrappers

By Cloud 9 Consulting Inc. Wietse Venema's TCP wrappers library. Wietse Venema's network logger is also known as TCPD or LOG_TCP. These programs log the client host name of incoming telnet, ftp, rsh, rlogin, finger etc. requests. Security options are: access control per host, domain and/or service; detection of host name spoofing or host address spoofing; booby traps to implement an early-warning system.

TCPdump

A powerful tool for network monitoring and data acquisition. This program allows you to dump the traffic on a network. 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, to detect "ping attacks" or to monitor the network activities.

tcpflow

tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging. A program like tcpdump shows a summary of packets seen on the wire, but usually doesn't store the data that's actually being transmitted. In contrast, tcpflow reconstructs the actual data streams and stores each flow in a separate file for later analysis. tcpflow understands TCP sequence numbers and will correctly reconstruct data streams regardless of retransmissions or out-of-order delivery.

TCT

TCT (The Coroner's Toolkit) is a collection of forensics programs and utilities by Dan Farmer and Wietse Venema for a post-mortem analysis of a UNIX system after break-in.

ThePacketMaster

ThePacketMaster is a Linux distribution intended to be run from a bootable CD-ROM. It includes a good assortment of security and forensics related utilities. There is currently one type of CD image available, "ThePacketMaster Linux Security Server" with three more in planning.

Wellenreiter

Wellenreiter is a wireless network discovery and auditing tool. Prism2, Lucent, and Cisco based cards are supported. It is the easiest to use Linux scanning tool. No card configuration has to be done anymore. The whole look and feel is pretty self-explaining. It can discover networks (BSS/IBSS), and detects ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer automatically.

Whisker

Whisker is used to scan for vulnerabilities in CGI scripts.

Windows

Achilles

Achilles is a free general-purpose web application security assessment tool. Achilles acts as a HTTP/HTTPS proxy that allows a user to intercept, log, and modify web traffic on the fly. The concept for Achilles was via David Rhoades of Maven Security.

Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary & Brute-Force attacks, decoding scrambled passwords, revealing password boxes, uncovering

cached passwords and analyzing routing protocols. The program comes in two versions (Win9x and WinNT/2000/XP) because of the differences and limitations of some API. The Windows 9x version is no longer being updated.

Disk Investigator

Disk Investigator helps you to discover all that is hidden on your computer hard disk. It can also help you to recover lost data. Display the true drive contents by bypassing the operating system and directly reading the raw drive sectors. View and search raw directories, files, clusters, and system sectors. Verify the effectiveness of file and disk wiping programs. Undelete previously deleted files.

Fport

Fport is a Windows utility that reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the 'netstat -an' command, but it also maps those ports to running processes with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications. Visit the web site below to download this utility.

HackerWacker

HackerWacker FreeWack offers simple monitoring and logging capabilities of all windows activity and URLs browsed. Recommended for use to monitor children on the Internet, where price and simplicity are a concern. For more advanced capabilities, including keystroke logging, you may wish to check out HWPE or HWAE. HWFW is a good companion for use with Internet Filtering Software.

ITR

The ITR (Interactive TCP Relay) tool provides a security-testing environment for non-HTTP Client/Server applications, similar to that provided by interactive HTTP proxies. When started, ITR operates as a simple TCP tunnel, listening on a specific port, and forwarding all the traffic to the remote host and port. By configuring the client to treat the ITR as its server, all traffic between a client and a server can be tunneled and logged. The true power of ITR, however, lies in its ability to intercept and edit the traffic passing through it. When invoking intercept mode, the ITR stops every message sent through it (client to server and/or server to client). The traffic can then be edited freely, providing a comfortable environment for testing Client/Server applications. The editing of messages is performed using a built-in comfortable HEXA Editor. To provide support and compatibility for various systems, the ITR can operate both its logs and HEXA editor using different types of character encodings, such as ASCII or EBCDIC.

MD5sums

MD5Sums calculates the MD5 message digest for one or more files (includes a percent done display for large files). By comparing the MD5 digest of a file to a value supplied by the original sender, you can make sure that files you

download are free from damage and tampering. MD5 values are frequently supplied along with downloadable files.

Network Stumbler

Network Stumbler is a free tool for discovering the presence of wireless (802.11) access points - a technique called "war driving". The tool is currently free but no source code is provided.

NTFS Reader DOS

NTFS Reader DOS Boot Disk provides read access to NTFS drives from the MS DOS environment. It supports long filenames as well as compressed and fragmented files. NTFS Reader for DOS allows you to preview the files on NTFS and copy them from NTFS to FAT volumes or network drives. In order to use the software you need to copy the readntfs.exe file to a bootable floppy disk and boot from it.

Outpost

The FREE version of Outpost firewall is setting new standards in the firewall industry, yet it looks and acts like any Office application! It starts protecting your system as soon as it's installed without requiring tricky settings or configuration.

PuTTY

PuTTY is a collection of free SSH client tools. It includes the SSH terminal client (PuTTY), command-line client (Plink), secure file transfer (PSCP and PSFTP), and the authentication agent (Pageant).

Restoration

Restoration restores files that were deleted or deleted from the recycle bin by mistake. It includes an option to scan for all recoverable deleted files. It supports FAT and NTFS as well as digital cameras cards.

Sam Spade

Sam Spade is a network query utility for Windows that implements many of the common network utilities found on UNIX machines. It includes utilities such as ping, nslookup, whois, dig, traceroute, finger, raw HTTP web browser, DNS zone transfer, SMTP relay check, website search, and more.

Scramdisk / E4m

Scramdisk and E4m (Encryption for the Masses) are on-the-fly drive encryption packages. Scramdisk is currently unmaintained but is still available for Windows 95, Windows 98 and Windows ME as a free download from the web site below. The Windows NT v4, Windows 2000 and Windows XP versions have been withdrawn from sale and are now superseded by Drivecrypt. Anyone wanting free on-the-fly encryption for Win2k or WinXP should try E4m, also hosted on the web site below.

Securit-e-PortControl

Securit-e-PortControl allows you to quickly view your current network activity and manage your TCP/IP properties per NIC through an easy to use Windows interface, without having to deal with the numerous cumbersome Network Properties dialog windows or the command line.

Securit-e-PortControl allows an administrator to:

- Easily and quickly set the permitted inbound TCP and UDP ports per NIC
- Easily and quickly set the permitted IP protocols per NIC
- Set the NetBIOS settings per NIC
- View the current network activity
- Change the MAC address of a selected NIC
- Enable/Disable LMHOSTS

SHA verify

SHA verify is a command-line program which will calculate the MD5 (128 bit), SHA1 (160 bit), SHA2 (256 bit), SHA2 (384 bit), and SHA2 (512 bit) hashes of files.

SpyBot

Spybot - Search & Destroy can detect and remove spyware of different kinds from your computer. Spyware is a relatively new kind of threat that common anti-virus applications do not yet cover. If you see new toolbars in your Internet Explorer that you didn't intentionally install, if your browser crashes, or if your browser start page has changed without your knowing, you most probably have spyware. But even if you don't see anything, you may be infected, because more and more spyware is emerging that is silently tracking your surfing behaviour to create a marketing profile of you that will be sold to advertisement companies. Visit the SpyBot web site for more information and the free download.

SuperScan

SuperScan is a free TCP port scanner, pinger, and resolver from Foundstone. Please visit the web site below to download directly from Foundstone.

UrIScan

UrIScan version 2.5 is a security tool that restricts the types of HTTP requests that Internet Information Services (IIS) will process. By blocking specific HTTP requests, the UrIScan security tool helps prevent potentially harmful requests from reaching the server. UrIScan 2.5 will now install as a clean installation on servers running IIS 4.0 and later.

WinDump

WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX. Porting is currently based on version 3.5.2. WinDump is fully compatible with tcpdump and can be used to watch

and diagnose network traffic according to various complex rules. It can run under Windows 95/98/ME, and under Windows NT/2000/XP.

xorpack

QX-Mat's Lil'XORer encrypter and decrypter programs. Scramble data in a way that is not obviously it's original content, and unscramble again. Uses an 8 bit random number as the key.