Auditing, Intrusion Detection, Forensics, and Logging

1. Auditing (Code, Host, Network & Password Audit Tools)
   Utilities for checking and verifying security measures
   a. AirDefense (Wireless scanner and rogue detection)

      http://www.airdefense.net/education/index.shtm

   b. Cerberus Internet Scanner (WinNT/Win2K scanner)

      http://www.cerberus-infosec.co.uk/cis.shtml

   c. BSD Airtools (Wireless Network Auditing)

      http://www.dachb0den.com/projects/bsd-airtools.html

   d. Check for Rootkit (chkrootkit.org)

      http://www/crkrootkit.org/

   e. Crack (Password auditor)

      http://www.crypticide.org/users/alecm/

   f. Default Logins for Networked Devices

      http://www.phenoelit.de/dpl/

   g. Dsniff (Tools for network auditing and penetration testing)

      http://www.monkey.org/~dugsong/dsniff/

   h. Ethereal (A network protocol analyzer for Unix and Windows)

      http://www/ethereal.com/download.html

   i. Fenris (Simplifies auditing & forensic work)

      http://razor.bindview.com/tools/fenris/

   j. Fragroute (by Dug Song)

      http://www.monkey.org/~dugsong/fragroute/

k. GFI (Landguard network scanner)

   http://www.gfi.com/lannetscan.index.htm

l. Icon (SNMP Packet Viewer)

   http://www.icon-labs.com/product_sniffer.html

m. Incident-Response.Org (Static binaries for auditing)

   http://www.incident-response.org/

n. Iris (Packet Sniffer)

   http://www.firewall.cx/download-s01-ns.php

o. John The Ripper (Password auditing)

   http://www.openwall.com/john/

p. Lost password (Password cracking/recovery)

   http://www.lostpassword.com/index.htm

q. Nessus (Robust network scanner)

   http://www.nessus.org/

r. Netcat (Feature-rich network debugging & exploration tool)

   http://www.atstake.com/research/tools/network_utilities

s. Network Configuration Calculator

   http://www.treachery.net/~jdyson/netmask.html

t. SAINT (Enhanced version of SATAN)

   http://www.saintcorporation.com/products/saint_engine.html

u. Sam Spade (General Tools)

   http://www.samspade.org/

v. Security Administrator's Tool for Analyzing Networks (SATAN)

http://www.fish.com/~zen/satan/satan.html

w. Security Auditor's Research Assistant (SARA)

http://www.arc.com/sara

x. SuperScan3.0 (Network scanner)

http://www.webattack.com/get/superscan.shtml

y. Tiger Analytical Research Assistant (TARA)

http://www-arc.com/tara/

z. Whisker Utility (Web/CGI auditing)

http://sourceforge.net/projects/whisker/

2. Intrusion Detection & Forensics
   Host- and network-based systems for monitoring attacks and unauthorized system modifications
   a. Autopsy (Forensics tools)

      http://www.sleuthkit.org/autopsy/index.php

   b. Cheops (Network Swiss-knife)

      http://www.marko.net/cheops/

   c. COAST (Computer Operations, Audit, and Security Technology)

      http://www.cerias.purdue.edu/coast/coast-tools.html

   d. Computer Forensics – NTI (Training and tools)

      http://www.forensics-intl.com/

   e. Early Bird (Real-time HTTP worm intrusion detection)

      http://www.treachery.net/~jdyson/earlybird/

   f. File System Saint (FSS)

      http://insecure.dk/fss/

   g. GFI (Landguard network scanner)

      http://www.gfi.com/lannetscan/index.htm

   h. Guidance Software (ENCAS Forensic Software)

      http://www.guidancesoftware.com/

   i. Grave-Robber (captures information)

      http://www.porcupine.org/forensics/tct.html

   j. HoneyNet Project (IDS/Forensics data)

      http://project.honeynet.org/

k. IANA (Port Numbers)

   http://www.iana.org/assignments/port-numbers

l. Key Computer Service (Training and software)

   http://www.keycomputer.net/

m. Lazarus (A tool that recover deleted files)

   http://www.porcupine.org/forensics/tct.html

n. Linux Intrusion Detection System (LIDS)

   http://www.lids.org/

o. Nagios (Network/system monitoring application; formerly known as NetSaint.)

   http://www.nagios.org/

p. NCSA (Network system/monitoring Snooping tools)

   http://archive.ncsa.uiuc.edu/People/vwelch/net_perf_tools.htm

q. Opus one (Trace route tool)

   http://www.opus1.com/www/traceroute.html

r. Samhain File System Integrity Checker

   http://samhain.sourceforge.net/surround.html?main_q.html&2

s. Scanlogd (PortScan detection)

   http://www.openwall.com/scanlogd/

t. Snort (Real-time traffic analysis & logging)

   http://www.snort.org/

u. Snort IDScenter (Win32 Interface)

   http://www.packx.net/

v. The Coroner's Toolkit (TCT)

http://www.porcupine.org/forensics/tct.html

w. TCTUTILs (Forensics toolkit suite for TCT)

http://www.cerias.purdue.edu/homes/carrier/forensics/

x. Tripwire (MD5sum-based file modification monitor)

http://www.tripwire.org/

y. Unrm (recovers deleted files)

http://www.porcupine.org/forensics/tct.html

3. Logging
   Utilities for enhancing and verifying system logs
   a. COAST (Computer Operations, Audit, and Security Technology)

      http://www.cerias.purdue.edu/coast/coast-tools.html

   b. FWanalog (Summarizes IPF & IP tables firewall logs)

      http://tud.at/programm/fwanalog/

   c. FWlogsum (Summarizes Checkpoint FW1 logs)

      http://fwlogsum.sourceforge.net/

   d. FWlogwatch (Summarizes firewall & IDS logs)

      http://www.kyb.uni-stuttgart.de/boris/software.shtml

   e. KLogger (WinNT/Win2K keystroke logger)

      http://ntsecurity.nu/toolbox/klogger/

   f. Linux Event Logger (For Enterprise-Class Systems)

      http://evlog.sourceforge.net/

   g. Logsurfer (Monitors logs in real-time)

      http://www.cert.dfn.de/eng/logsurf/

   h. Swatch (Monitors syslog messages)

      http://swatch.sourceforge.net/

   i. Secure Remote Syslogger (Encrypted streaming syslog)

      http://www.w00w00.org/files/sectools/SRS/

   j. SecureNet Pro (monitoring and analyzing)

      http://www.mimestar.com/products/index.html

k. SnortSnarf (HTMLized Snort Log Reviewer)

   http://www.silicondefense.com/software/snortsnarf/

l. Spector (Monitoring and spy software)

   http://www.computer-spy-software.net/spectorpro_windows/

m. Syslog.Org (Vast info on sys logging)

   http://www.syslog.org/

n. Throughput Monitor (An event counter per timeframe log analyzer)

   http://home.uninet.ee/~ragnar/throughput_monitor/

o. WinZapper (WinNT/Win2K log modifier)

   http://www.ntsecurity.nu/toolbox/winzapper/