

Attachment 5

Recommended List of Tools for Incident Detection and Eradication

Network Vulnerability and Assessment Tools

Proventia/RealSecure - network security application that provides automated network vulnerability assessment across servers, desktops, and infrastructure devices. Performs distributed or event-driven probes of network services, operating systems, routers/switches, servers, firewalls, and application routers to identify potential risks. University of Massachusetts has an enterprise license for this product.
<http://www.iss.net/>

Audit Record Generation and Utilization System (i.e., ARGUS) – a fixed-model Real Time Flow Monitor designed to track and report on the status and performance of network transactions in a data network traffic stream. It can be used to analyze and report on packet capture files or examine data from a live interface for individual end-systems or entire enterprises network activity. This tool pulls tcpdump and SNORT data together for single source of analysis. Argus currently runs on Linux, Solaris, FreeBSD, OpenBSD, NetBSD, and MAC OS X and its client programs have also been ported to Cygwin. <http://www.qosient.com/argus/index.htm>

Center for Internet Security CIS Level-1 Benchmark and Scoring Tool for Linux, Windows and Solaris. http://www.cisecurity.org/bench_linux.html

Dsniff - A suite of powerful for sniffing networks for passwords and other information. Includes sophisticated techniques for defeating the "protection" of network switches. Capable of passively monitor a network for interesting data (passwords, e-mail, etc.), intercepting network traffic and implementing active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions. Runs on OpenBSD (i386), Redhat Linux (i386) and Solars (sparc). <http://naughty.monkey.org/~dugsong/dsniff/>

Ethereal - Network traffic analyzer (also know a Wireshark <http://www.wireshark.org/>)
Ethereal is a network traffic analyzer, or "sniffer". Runs on Windows, Linux Unix and Unix-like operating systems. It uses GTK+, a graphical user interface library, and libpcap, a packet capture and filtering library. <http://www.ethereal.com>

I2 Analyst's Notebook - link analyzer. Link analysis is applied to incident response post mortem. Logs, events and other data feed the link analyzer's analysis process. Analyst's Notebook is part of a suite of products that allow very large, complex logs to be analyzed and subtle connections to be found in extensive distributed enterprises.
<http://www.i2inc.com>

NetStumbler - Wireless network scanning tool that runs on Windows 2k, XP and 2003. A tool that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. Applicable for verifying your network as designed, finding poor coverage areas, detecting overlapping networks, detecting unauthorized access points and WarDriving. <http://www.stumbler.net/>

Attachment 5

Recommended List of Tools for Incident Detection and Eradication

Security Auditing Tool for Analyzing Networks (i.e., SATAN) This is a powerful tool for analyzing networks for vulnerabilities created for sysadmins that cannot keep a constant look at bugtraq, rootshell and the like. SATAN recognizes several common networking-related security problems, and reports the problems without actually exploiting them. For each type or problem found, SATAN offers a tutorial that explains the problem and what its impact could be. The tutorial also explains what can be done about the problem: correct an error in a configuration file, install a bugfix from the vendor, use other means to restrict access, or simply disable service.

<http://www.porcupine.org/satan/>

SNORT - Flexible packet sniffer/logger that detects attacks Snort is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. Snort has a real-time alerting capability, with alerts being sent to syslog, a separate "alert" file, or even to a Windows computer via Samba. <http://www.snort.org>

TCPdump - 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 matches a given expression. You can use this tool to track down network problems, to detect "ping attacks" or to monitor the network activities. A command-line utility that prints, into a terminal window or file, the packet headers on a specified network interface that match an input Boolean expression. This product runs only on Solaris, HP-UX, IRIX., SGI and Win32. <http://www.tcpdump.org>

Host Vulnerability Assessment and Scanning Tools

NESSUS – network security auditing tool capable of remotely scanning network hosts. It makes it possible to test security modules in an attempt to find vulnerable spots that should be fixed. Nessus uses plug-ins that extend the traditional port scanning techniques to include the ability to detect remote flaws of hosts on your network as well as local flaws and missing patches. Runs on Linux-Fedora, Red Hat, SuSE, Debian, FreeBSD, Solaris, MacOS X, Windows 2k, XP & 2003. <http://www.nessus.org/download/>

Network MAPper (i.e., nmap) – a free open source utility for network exploration or security auditing designed to rapidly scan large networks (although it works against single hosts). Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Runs on Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, and Sun Os. Both console and graphical versions are available. Nmap is available with full source code under the terms of the GNU GPL. <http://www.insecure.org/nmap/>

Attachment 5

Recommended List of Tools for Incident Detection and Eradication

Nikto

A comprehensive Open-Source web scanner that tests for over 3200 potentially dangerous files, CGI scripts and version specific problems on a number of server platforms. Makes use of plugins that are updated either automatically or manually. Runs on Win32. <http://www.cirt.net/code/nikto.shtml>

SAINT (Security Administrator's Integrated Network Tool) - a vulnerability scanning tool based on SATAN. Features include scanning through a firewall, updated security checks from CERT & CIAC bulletins, 4 levels of severity (red, yellow, brown, & green) and a feature rich HTML interface. SAINT remotely probes systems for exploitable vulnerabilities via the network and stores its finds in a database. An integration of open sources tools capable of identifying multiple host characteristics and presents thoser findings in an easy to categorize, easy to read format. Runs on Unix, Linux or MAC OS/X. <http://www.saintcorporation.com/saint>

The Security Auditor's Research Assistant (SARA) - a third generation security analysis tool based on the SATAN model which is covered by the GNU GPL-like open license. SARA remotely probes systems for exploitable vulnerabilities via the network and stores its findings in a database. An integration of open sources tools capable of identifying multiple host characteristics and presents those finding in an easily to a categorized, easy to read format. Interfaces with NMAP package for "Operating System fingerprinting" and provides a transparent interface to SAMBA for SMB security analysis. Operates under Unix, Linux, MAC OS/X or Windows 200* and Windows XP platforms. Integrates the National Vulnerability Database. Supports remote self scan and API facilities. <http://www-arc.com/sara/>

Host Based Analysis and Protection

Bastille Hardening System

Bastille is a host-based program that proactively "locks down" an operating system. By default, it interactively asks questions and then builds and applies a policy based on the answers. There is an assessment mode that reports a system's current state of hardening. Runs on Red Hat, Debian, Mandrake, SuSE and TurboLinux Linux, HP-UX and Mac OS X. <http://www.bastille-linux.org/>

Center for Internet Security CIS Level-1 Benchmark and Scoring Tool - standalone host-based application that assesses the security level of a workstation based on a recommended configuration. Tool looks for and reports vulnerabilities in the operating system and provides mitigation suggestions. Runs on Linux, Windows and Solaris. http://www.cisecurity.org/bench_linux.html

Attachment 5

Recommended List of Tools for Incident Detection and Eradication

LiStOpen Files (i.e., LSOF) – host-based tool that lists information about files that are opened by processes running on a UNIX system. It's platform specific and required installation of the proper variant. This command gives you a detailed look at every process and open file on your server. Runs on AIX, Apple Darwin 7.x&8.x, FreeBSD, HP-UX, Linux, OpenBSD, and Solaris. <http://people.freebsd.org/~abe/>

Netstat – command line utility that displays TCP ports on which a computer is listening, Ethernet and IPv4 statistics and the hosts IP routing table. Built into pcs and integrated with operating system. Used in Windows NT/2000/XP/2K3 and Windows 9x, Windows Me internals. <http://www.freshsoftware.com/#>

TRIPWIRE - A file and directory integrity checker that monitors system and configuration files for any changes (i.e., what changed, when it changed, how it changed and who changed it). In the event a change was unauthorized; Tripwire can roll servers back to a known and trusted state. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner. <http://www.tripwire.com/>

Password Assessment Tools

Cain and Abel - password recovery tool for MS OSs capable of recovering various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. Runs on Win32. <http://www.oxid.it/cain.html>

John the Ripper - Multi-platform password hash cracker/password capable of detecting 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. Available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. <http://www.openwall.com/john/>

LC5 (previously LophtCrack) - Windows 2000 and Windows NT password auditing and recovery tool that will compute user passwords from the cryptographic hashes that are stored by the Windows operation system. LC5 can obtain the hashes through many sources (file, network sniffing, registry, etc) and it has numerous methods of generating password guesses (dictionary, brute force, etc). <http://www.atstake.com/products/lc/>

Securitystats.com – web site to check password strength. Available for Cisco, Win32 and Unix. <http://www.securitystats.com/tools/password.php>

Attachment 5 Recommended List of Tools for Incident Detection and Eradication

Vulnerability Eradication Tools

Adaware – host based utility that provides protection and removal capabilities for data-mining, aggressive advertising, Trojans, dialers, malware, browser hijackers, and web tracking components. This software is downloadable free of charge for personal use. Runs on Win32. <http://www.lavasoftusa.com/support/download/>

MacAfee Antivirus – detects and removes virus from desktops, mail/file servers, Internet gateways, etc. Part of a suite of products to protect desktops from intruders. Other suite components include anti-spyware, host based firewall and desktop IDS/IPS. Runs on Win32, Linux, and Mac OS X.
<http://www.networkassociates.com/us/products/mcafee/antivirus/category.htm>

MacAfee Stinger – stand-alone utility used to detect and remove specific viruses. Stinger does not protect systems from infection but removes malicious code using McAfee's next generation scan engine technology that includes process scanning, digitally signed DAT files, and scan performance optimizations. Runs on Win32 and Mac OS X. <http://vil.nai.com/vil/stinger/>

NGenFix - utility that detects and removes specific malicious software. Not a substitute for running normal proactive antivirus protection, but as a reactive tool to handle already infected systems. Runs on Win32.
http://www.norman.com/Virus/Virus_removal_tools/en-us

Norton Antivirus – detects and removes viruses, worms, and Trojan horses from desktop, mail/file servers, Internet gateways, etc. Part of a suite of products to protect desktops from intruders. Other suite components include anti-spyware, host based firewall and desktop IDS/IPS. Runs on Win32, Linux and Mac OS X.
<http://www.symantec.com/product/>

Spybot – free utility that can detect and remove spyware of different kinds from a computer. Part of a suite of products that includes a registry scanner and file analyzer. Runs on Win32. <http://www.safer-networking.org/en/index.html>

Computer Forensics Tools

Forensic Toolkit (i.e. FTK) – Includes features such as a registry viewer, in-depth logging; a standalone disk imager; direct email and zip file analysis; password recovery feature for gaining access to protected files to search for evidence; and a Distributed Network Attack feature, which can be used to crack encrypted files over a network - <http://www.accessdata.com/products/ftk/>

Attachment 5

Recommended List of Tools for Incident Detection and Eradication

Coroner's toolkit (i.e., TCT) - Collection of programs for a post-mortem analysis of a UNIX system after break-in. Can be used to recreate incident. A serious knowledge of Unix is a prerequisite for use of this tool, but if you can manage it, this is an extremely powerful set of tools. This is not a GUI-based product. It is a collection of command line tools designed for the experienced Unix engineer.

www.porcupine.org/forensics/tct.html

Honeynet- Collection of tools used to control and contain attacker activity, log and capture attacker activity and analyze the data collected by honeynets. Can be used to recreate incident. **<http://www.honeynet.org>**

Honeytrap –low interaction honeypot that dynamically creates port listeners based on TCP connection attempts. <http://honeytrap.sourceforge.net/>

Netcat – Free network debugging and exploration tool which reads and writes data across TCP/IP network connections. Designed to used directly or easily driven by other programs as a network debugging and exploration tool. Provides access outbound and inbound connections, TCP or UDP, to or from any ports; allows special tunneling such as UDP to TCP, with the possibility of specifying all network parameters (source port/interface, listening port/interface, and the remote host allowed to connect to the tunnel; Has built-in port-scanning capabilities, with randomizer; Includes advanced usage options, such as buffered send-mode (one line every N seconds), and hexdump (to stderr or to a specified file) of transmitted and received data. It can create almost any kind of connection you would need and has several interesting built-in capabilities.

<http://netcat.sourceforge.net/>

ProDiscover IR - IT forensic tool that can access computers over the network (with agents installed) to enable media analysis, image acquisition and network behavior analysis. Other capabilities include the remote analysis of running processes, open files, open ports and services, and other network-based functions. Features all the basic IT forensic capabilities – full disk imaging, an ability to find hidden data, file metadata information, and hash-keeping, as well as gather data on disks across an entire network. <http://www.techpathways.com/ProDiscoverIR.htm>

Sleuth Kit and Autopsy Browser - freeware open-source computer forensic tools built on the Coroner's Toolkit. Product will feel familiar to anyone comfortable in Unix file systems, however the products can analyze non-Unix file systems. Both the Sleuth Kit and the browser run in Unix/Linux and the browser can run on any html environment and connect to the Autopsy server. Includes features for analysis and case management. <http://www.sleuthkit.org/>

Guide for First Responders On How To Handle Digital Evidence -
www.ojp.usdoj.gov/nij/pubs-sum/187736.htm

Attachment 5
Recommended List of Tools for Incident Detection and Eradication

Guide for Forensic Examination of Digital Evidence -
<http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm>

Audit Tool

Mandiant First Response – Freeware audit tool. Information gathered includes system information, current processes, services, tasks, files, issues, and registry information. After all the data has been gathered, it can be put into a central report to provide a snapshot of a network before any additional forensic evidence is acquired.
www.mandiant.com