Guide to Computer Forensics and Investigations Fourth Edition

Network Forensics, and Live Acquisitions

Syllabus

- Introduction to Network Forensics and tracking network traffic
- Reviewing Network Logs
- Network Forensics Tools
- Performing Live Acquisitions
- Order of Volatility
- Standard Procedure

Network Forensics Overview

Network Forensics Overview

- **Network forensics**
  - Systematic tracking of incoming and outgoing traffic
    - To ascertain how an attack was carried out or how an event occurred on a network
- Intruders leave trail behind
- Determine the cause of the abnormal traffic
  - Internal bug
  - Attackers

Securing a Network

- **Layered network defense strategy**
  - Sets up layers of protection to hide the most valuable data at the innermost part of the network
- **Defense in depth (DiD)**
  - Similar approach developed by the NSA
  - Modes of protection
    - People (hiring and treatment)
    - Technology (firewalls, IDSs, etc.)
    - Operations (patches, updates)

Securing a Network (continued)

- Testing networks is as important as testing servers
- You need to be up to date on the latest methods intruders use to infiltrate networks
  - As well as methods internal employees use to sabotage networks

Performing Live Acquisitions

Performing Live Acquisitions

- Live acquisitions are especially useful when you're dealing with active network intrusions or attacks
- Live acquisitions done before taking a system offline are also becoming a necessity
  - Because attacks might leave footprints only in running processes or RAM
- Live acquisitions don't follow typical forensics procedures
- **Order of volatility (OOV)**
  - How long a piece of information lasts on a system

Performing Live Acquisitions (continued)

- Steps
  - Create or download a live-acquisition forensic CD
  - Make sure you keep a log of all your actions
  - A network drive is ideal as a place to send the information you collect; an alternative is a USB disk
  - Copy the physical memory (RAM)
  - The next step varies: search for rootkits, check firmware, image the drive over the network, or shut down for later static acquisition
  - Be sure to get a forensic hash value of all files you recover during the live acquisition

Performing a Live Acquisition in Windows

- Several tools are available to capture the RAM.
  - Mantech Memory DD
  - Win32dd
  - winen.exe from Guidance Software
  - BackTrack

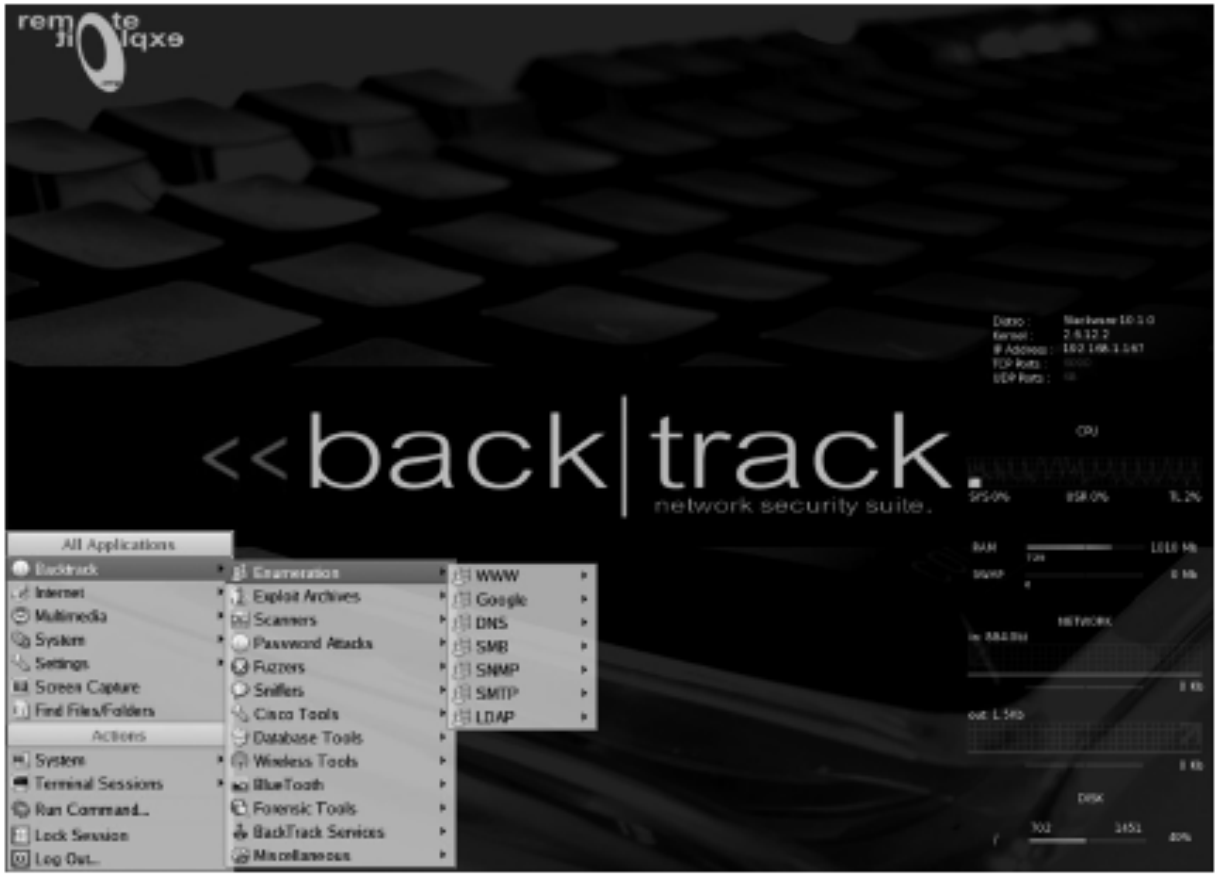


Figure 11-3 Some of the tools available in BackTrack

Developing Standard Procedures for Network Forensics

Developing Standard Procedures for Network Forensics

- Long, tedious process
- Standard procedure
  - Always use a standard installation image for systems on a network
  - Close any way in after an attack
  - Attempt to retrieve all volatile data
  - Acquire all compromised drives
  - Compare files on the forensic image to the original installation image

Developing Standard Procedures for Network Forensics (continued)

- Computer forensics
  - Work from the image to find what has changed
- Network forensics
  - Restore drives to understand attack
- Work on an isolated system
  - Prevents **malware** from affecting other systems

Reviewing Network Logs

- Record ingoing and outgoing traffic
  - Network servers
  - Routers
  - Firewalls
- Tcpdump tool for examining network traffic
  - Can generate top 10 lists
  - Can identify patterns
- Attacks might include other companies
  - Do not reveal information discovered about other companies

Using Network Tools

Using Network Tools

- Sysinternals
  - A collection of free tools for examining Windows products
- Examples of the Sysinternals tools:
  - RegMon shows Registry data in real time
  - Process Explorer shows what is loaded
  - Handle shows open files and processes using them
  - Filemon shows file system activity

SysInternals

- Link Ch 11b

Sysinternals Suite

technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Internet Explorer 8 - faster, safer, easier

Windows Sysinternals

Search TechNet with Bing

Home | Learn | Downloads | Community

Windows Sysinternals > Downloads > **Sysinternals Suite**

Utilities

- Sysinternals Suite
- Utilities Index

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

Additional Resources

- Forum
- Site Blog
- Sysinternals Learning
- Mark's Webcasts
- Mark's Events
- Mark's Blog
- Software License
- Licensing FAQ

Sysinternals Suite

By Mark Russinovich

Updated: November 1, 2010

Download Sysinternals Suite (12.6 MB)

Rate:

Introduction

The Sysinternals Troubleshooting Utilities have been rolled up into a single Suite of tools. This file contains the individual troubleshooting tools and help files. It does not contain non-troubleshooting tools like the BSOD Screen Saver or NotMyFault.

The Suite is a bundling of the following selected Sysinternals Utilities:

AccessChk	Junction	PsLogList
AccessEnum	LDMDump	PsPasswd
AdExplorer	ListDLLs	PsService
AdRestore	LiveKd	PsShutdown
Autologon	LoadOrder	PsSuspend
Autoruns	LogonSessions	RAMMap

Using Network Tools (continued)

- Tools from PsTools suite created by Sysinternals
  - PsExec runs processes remotely
  - PsGetSid displays security identifier (SID)
  - PsKill kills process by name or ID
  - PsList lists details about a process
  - PsLoggedOn shows who’s logged locally
  - PsPasswd changes account passwords
  - PsService controls and views services
  - PsShutdown shuts down and restarts PCs
  - PsSuspend suspends processes

Using UNIX/Linux Tools

- Knoppix Security Tools Distribution (STD)
  - Bootable Linux CD intended for computer and network forensics
- Knoppix-STD tools
  - Dcfldd, the U.S. DoD dd version
  - memfetch forces a memory dump
  - photorec grabs files from a digital camera
  - snort, an intrusion detection system
  - oinkmaster helps manage your snort rules

Using UNIX/Linux Tools (continued)

- Knoppix-STD tools (continued)
  - john
  - chntpw resets passwords on a Windows PC
  - tcpdump and ethereal are packet sniffers
- With the Knoppix STD tools on a portable CD
  - You can examine almost any network system

Using UNIX/Linux Tools (continued)

- BackTrack
  - Contains more than 300 tools for network scanning, brute-force attacks, Bluetooth and wireless networks, and more
  - Includes forensics tools, such as Autopsy and Sleuth Kit
  - Easy to use and frequently updated

Using Packet Sniffers

- Packet sniffers
  - Devices or software that monitor network traffic
  - Most work at layer 2 or 3 of the OSI model
- Most tools follow the PCAP format
- Some packets can be identified by examining the flags in their TCP headers

TCP Header

TCP Header

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number																															
96	Data offset				Reserved				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
128	Checksum																Urgent pointer															
160 ...	Options (if Data Offset > 5) ...																															

- From Wikipedia

Tools

- Tcpdump (command-line packet capture)
- Tethereal (command-line version of Ethereal)
- Wireshark (formerly Ethereal)
  - Graphical packet capture analysis
- Snort (intrusion detection)
- Tcpslice
  - Extracts information from one or more tcpdump files by time frame

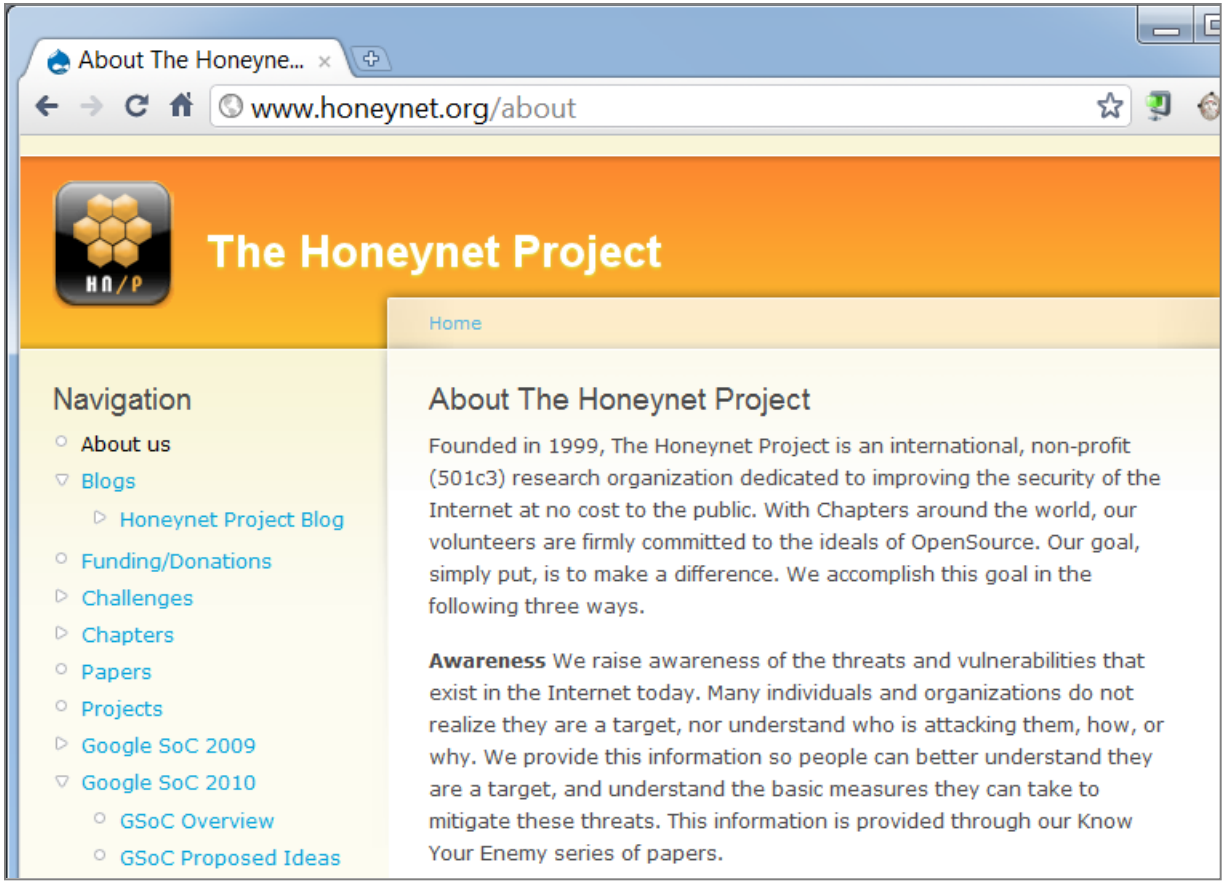
Tools

- Tcpreplay (replays packets)
- Tcpdstat (near-realtime traffic statistics)
- Ngrep (pattern-matching for pcap captures)
- Etherape (views network traffic graphically)
- Netdude (GUI tool to analyze pcap files)
- Argus (analyzes packet flows)

Examining the Honeynet Project

- Attempt to thwart Internet and network hackers
  - Provides information about attacks methods
- Objectives are awareness, information, and tools
- **Distributed denial-of-service (DDoS) attacks**
  - A recent major threat
  - Hundreds or even thousands of machines (**zombies**) can be used

Examining the Honeynet Project (continued)



Examining the Honeynet Project (continued)

- **Zero day attacks**
  - Another major threat
  - Attackers look for holes in networks and OSs and exploit these weaknesses before patches are available
- Honeypot
  - Normal looking computer that lures attackers to it
- Honeywalls
  - Monitor what's happening to honeypots on your network and record what attackers are doing

Examining the Honeynet Project (continued)

- Its legality has been questioned
  - Cannot be used in court
  - Can be used to learn about attacks
- Manuka Project
  - Used the Honeynet Project's principles
    - To create a usable database for students to examine compromised honeypots
- Honeynet Challenges
  - You can try to ascertain what an attacker did and then post your results online