Guide to Computer Forensics and Investigations
Fourth Edition

Chapter 11
Virtual Machines, Network Forensics, and Live Acquisitions
Objectives

- Describe primary concerns in conducting forensic examinations of virtual machines
- Describe the importance of network forensics
- Explain standard procedures for performing a live acquisition
- Explain standard procedures for network forensics
- Describe the use of network tools
Virtual Machines Overview

- Virtual machines are important in today’s networks.
- Investigators must know how to detect a virtual machine installed on a host, acquire an image of a virtual machine, and use virtual machines to examine malware.
Virtual Machines Overview (cont.)

• Check whether virtual machines are loaded on a host computer.
• Check Registry for clues that virtual machines have been installed or uninstalled.
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
    • Technology
    • Operations
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

• 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 bootable 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
  – Copy the physical memory (RAM)
  – The next step varies, depending on the incident you’re investigating
  – 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 3
Performing a Live Acquisition in Windows

Figure 11-3  Some of the tools available in BackTrack
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

• 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
Using Network Tools (continued)

Figure 11-4 Opening page of Sysinternals
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
Figure 11-6 Capturing frames in Ethereal
Using UNIX/Linux Tools (continued)
Using UNIX/Linux Tools (continued)

• The Auditor
  – Robust security tool whose logo is a Trojan warrior
  – Based on Knoppix and 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
  – 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
• Tools
  – Tcpdump
  – Tethereal
Using Packet Sniffers (continued)

<table>
<thead>
<tr>
<th>16-bit</th>
<th>32-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source port</td>
<td>Destination port</td>
</tr>
<tr>
<td>Sequence number</td>
<td></td>
</tr>
<tr>
<td>Acknowledgement number (ACK)</td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>Offset reserved</td>
</tr>
<tr>
<td></td>
<td>Checksum</td>
</tr>
<tr>
<td>Options and padding</td>
<td></td>
</tr>
</tbody>
</table>

Figure 11-8  A TCP header
Using Packet Sniffers (continued)

• Tools (continued)
  – Snort
  – Tcpslice
  – Tcpreplay
  – Tcpdstat
  – Ngrep
  – Etherape
  – Netdude
  – Argus
  – Ethereal
Using Packet Sniffers (continued)

Figure 11-9 Ethereal in a Windows environment
Using Packet Sniffers (continued)

Figure 11-10  The Capture Interfaces dialog box
Using Packet Sniffers (continued)
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)

Figure 11-12 The Honeynet Project
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
Examining the Honeynet Project (continued)

Figure 11-13 The Honeynet Challenges
Summary

• Virtual machines are important in today’s networks, and investigators must know how to detect a virtual machine installed on a host, acquire an image of a virtual machine, and use virtual machines to examine malware
• Network forensics tracks down internal and external network intrusions
• Networks must be hardened by applying layered defense strategies to the network architecture
• Live acquisitions are necessary to retrieve volatile items
Summary (continued)

• Standard procedures need to be established for how to proceed after a network security event has occurred
• By tracking network logs, you can become familiar with the normal traffic pattern on your network
• Network tools can monitor traffic on your network, but they can also be used by intruders
• Bootable Linux CDs, such as Knoppix STD and Helix, can be used to examine Linux and Windows systems
Summary (continued)

- The Honeynet Project is designed to help people learn the latest intrusion techniques that attackers are using.