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

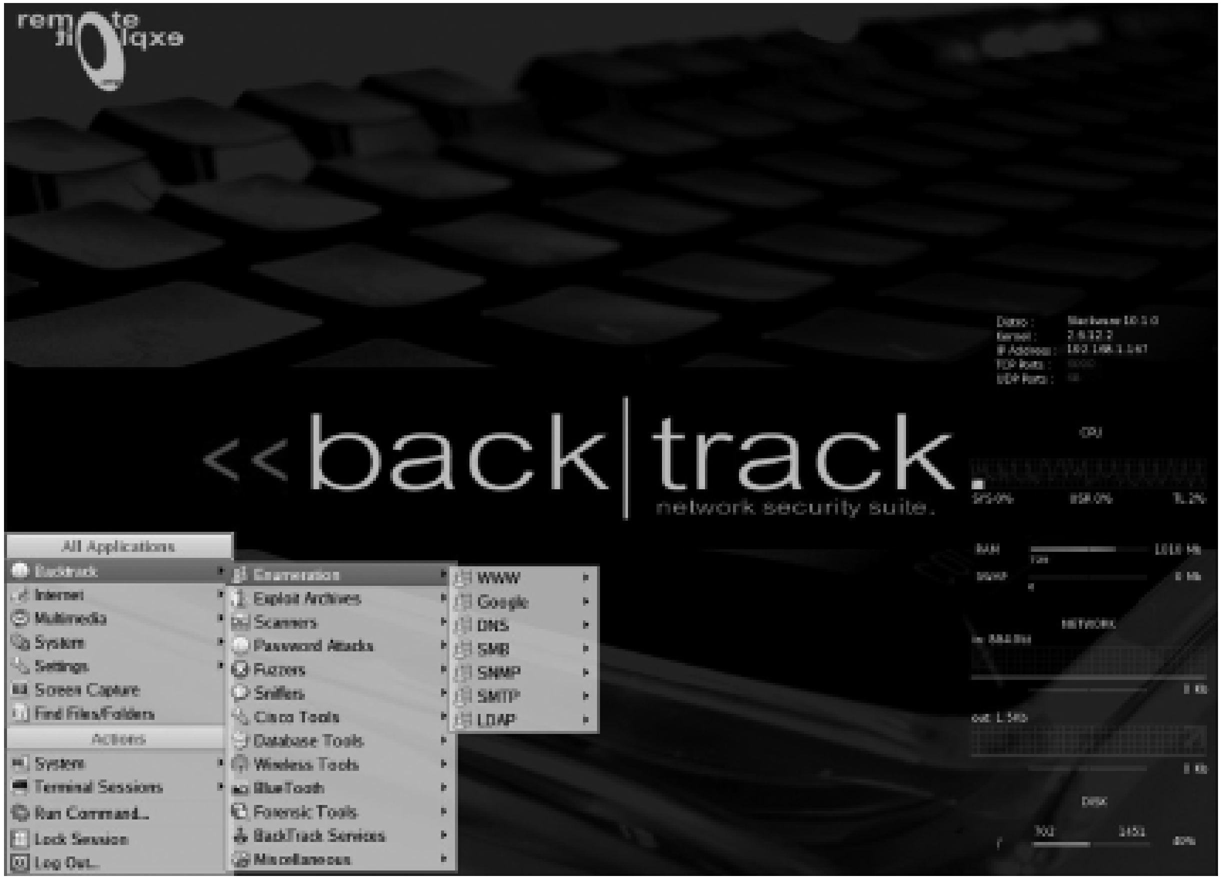


Figure 11-3 Some of the tools available in BackTrack

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

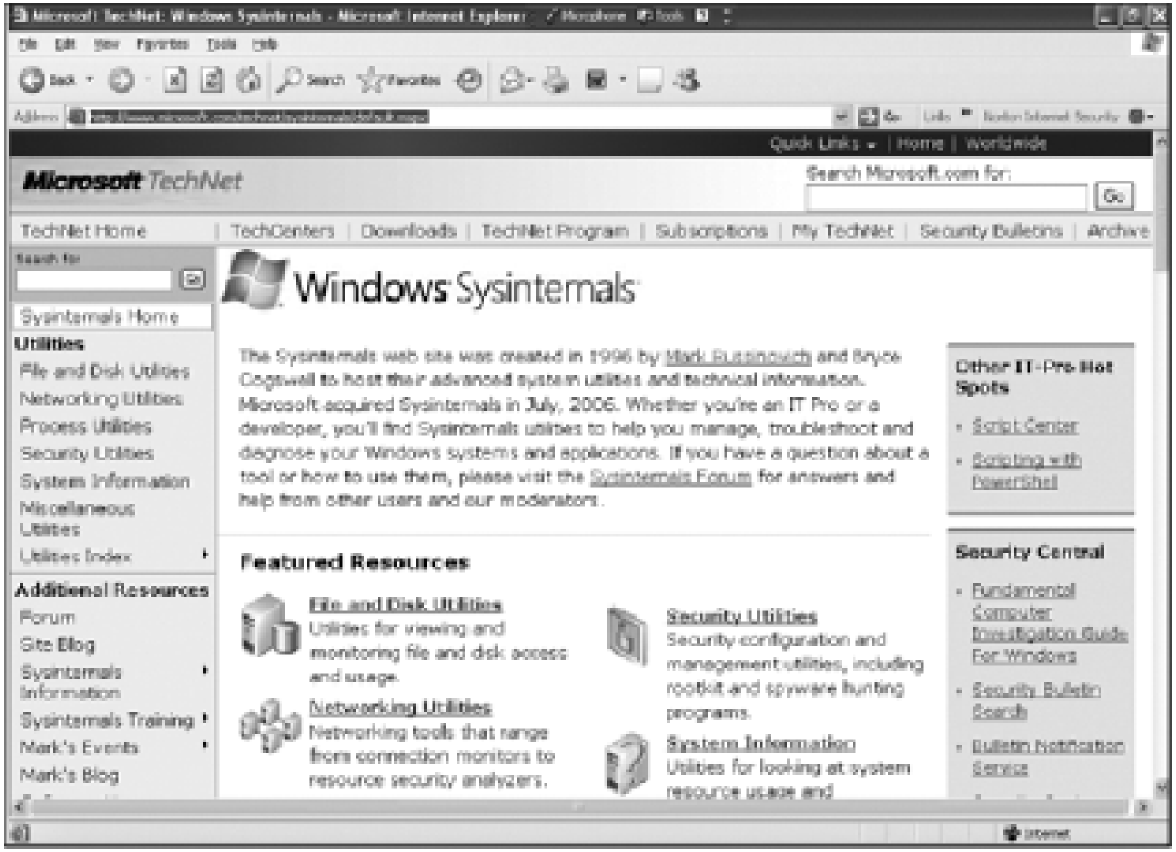
Reviewing Network Logs

- 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)



The Sysinternals web site was created in 1996 by Mark Russinovich and Bryce Cogswell to host their advanced system utilities and technical information. Microsoft acquired Sysinternals in July, 2006. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications. If you have a question about a tool or how to use them, please visit the Sysinternals Forum for answers and help from other users and our moderators.

Featured Resources

File and Disk Utilities
Utilities for viewing and monitoring file and disk access and usage.

Networking Utilities
Networking tools that range from connection monitors to resource security analyzers.

Security Utilities
Security configuration and management utilities, including rootkit and spyware hunting programs.

System Information
Utilities for looking at system resource usage and

Figure 11-4 Opening page of Sysinternals

Using Network Tools (continued)

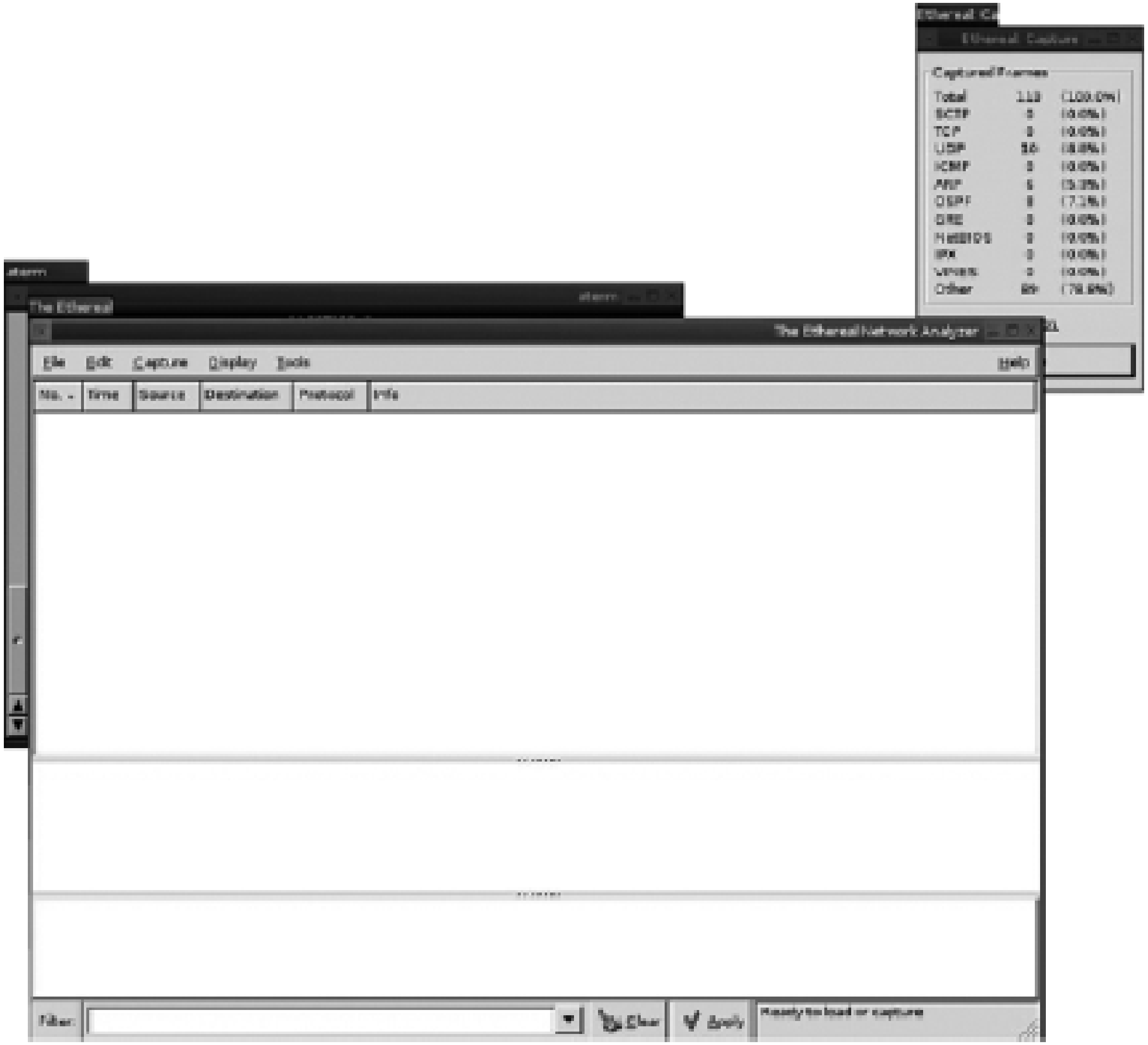
- Tools from PsTools suite created by Sysinternals
  - PsExec runs processes remotely
  - PsGetSid displays security identifier (SID)
  - PsKill kills process by name or ID
  - PsList lists details about a process
  - PsLoggedOn shows who's logged locally
  - PsPasswd changes account passwords
  - PsService 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



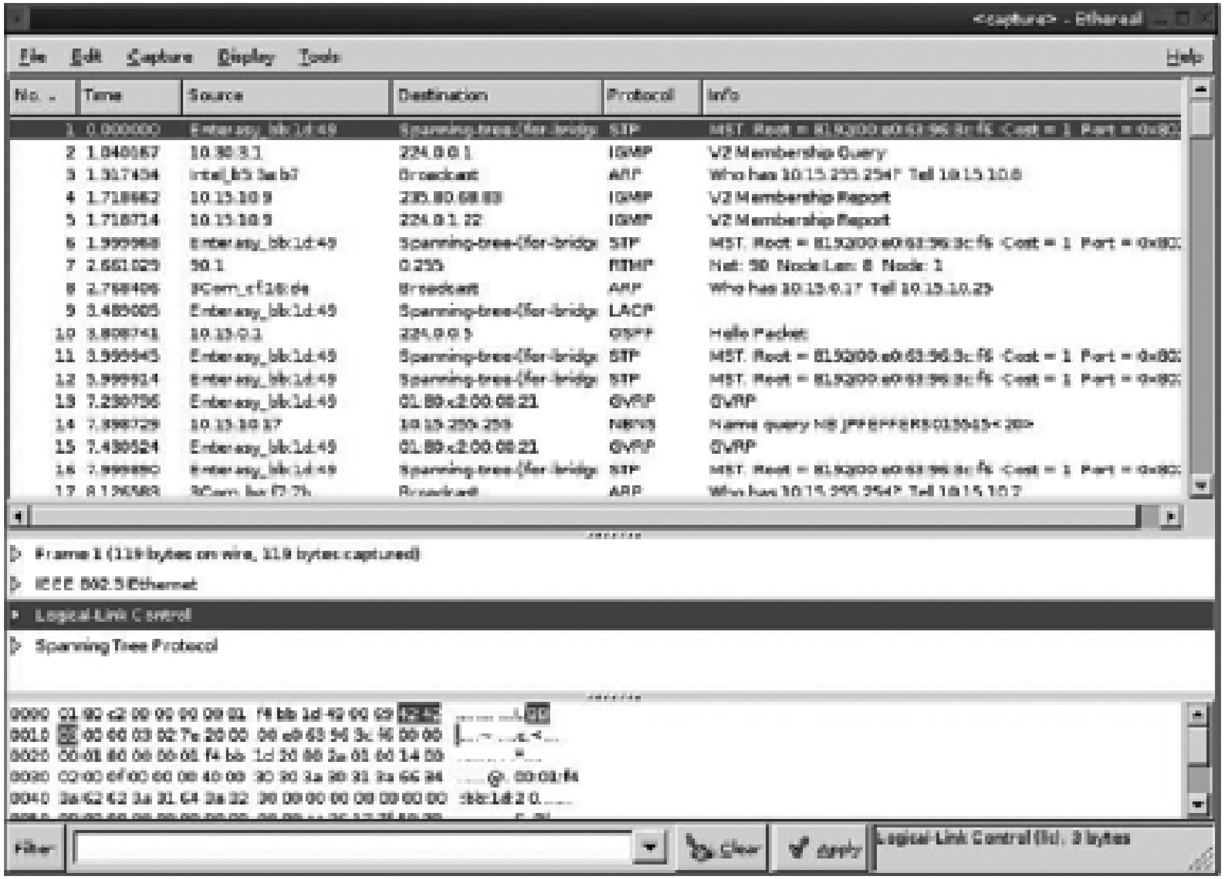
Captured Frames

Total	113	(100.0%)
SCTP	0	(0.0%)
TCP	0	(0.0%)
UDP	10	(8.8%)
ICMP	0	(0.0%)
ARP	6	(5.3%)
OSPF	8	(7.1%)
GRE	0	(0.0%)
NetBIOS	0	(0.0%)
IPX	0	(0.0%)
VINES	0	(0.0%)
Other	89	(78.8%)

Ready to load or capture

Figure 11-6 Capturing frames in Ethereal

Using UNIX/Linux Tools (continued)



```
No. .  Time       Source              Destination              Protocol  Info
  1 0.000000   Enterasy_bb:1d:49   Spanning-tree-(for-bridg STP   MST. Root = 8192/00:e0:63:96:3c:f6 Cost = 1 Port = 0x80
  2 1.040167   10.90.3.1           224.0.0.1                IGMP  V2 Membership Query
  3 1.317434   Intel_b5:3a:b7      Broadcast                ARP   Who has 10.15.255.254? Tell 10.15.10.8
  4 1.718662   10.15.10.9          235.80.68.83             IGMP  V2 Membership Report
  5 1.718714   10.15.10.9          224.0.1.22               IGMP  V2 Membership Report
  6 1.999968   Enterasy_bb:1d:49   Spanning-tree-(for-bridg STP   MST. Root = 8192/00:e0:63:96:3c:f6 Cost = 1 Port = 0x80
  7 2.661025   50.1                0.255                    RTMP  Net: 50 Node Len: 8 Node: 1
  8 2.768409   3Com_cf:18:de       Broadcast                ARP   Who has 10.15.0.1? Tell 10.15.10.23
  9 3.489005   Enterasy_bb:1d:49   Spanning-tree-(for-bridg LACP
 10 3.808741   10.15.0.1           224.0.0.5                OSPF  Hello Packet
 11 3.999945   Enterasy_bb:1d:49   Spanning-tree-(for-bridg STP   MST. Root = 8192/00:e0:63:96:3c:f6 Cost = 1 Port = 0x80
 12 5.999914   Enterasy_bb:1d:49   Spanning-tree-(for-bridg STP   MST. Root = 8192/00:e0:63:96:3c:f6 Cost = 1 Port = 0x80
 13 7.230756   Enterasy_bb:1d:49   01:80:c2:00:00:21        GVRP  GVRP
 14 7.398729   10.15.10.17         10.15.255.255            NBNS  Name query NB JPFEFFER5013045<20>
 15 7.430524   Enterasy_bb:1d:49   01:80:c2:00:00:21        GVRP  GVRP
 16 7.999890   Enterasy_bb:1d:49   Spanning-tree-(for-bridg STP   MST. Root = 8192/00:e0:63:96:3c:f6 Cost = 1 Port = 0x80
 17 8.126589   3Com_ba:f2:7b       Broadcast                ARP   Who has 10.15.255.254? Tell 10.15.10.7
```

```
▷ Frame 1 (119 bytes on wire, 119 bytes captured)
▷ IEEE 802.3 Ethernet
▸ Logical-Link Control
▷ Spanning Tree Protocol
```

```
0000  01 80 c2 00 00 00 00 01  f4 bb 1d 49 00 69 42 42   .........I.iBB
0010  03 00 00 03 02 7e 20 00  00 e0 63 96 3c f6 00 00   .....~ ...c.<...
0020  00 01 80 00 00 01 f4 bb  1d 20 80 2a 01 00 14 00   ......... .*....
0030  02 00 0f 00 00 00 40 00  30 30 3a 30 31 3a 66 34   ......@.00:01:f4
0040  3a 62 62 3a 31 64 3a 32  30 00 00 00 00 00 00 00   :bb:1d:20.......
```

Logical-Link Control (llc), 3 bytes

Figure 11-7 Ethereal displaying frame information

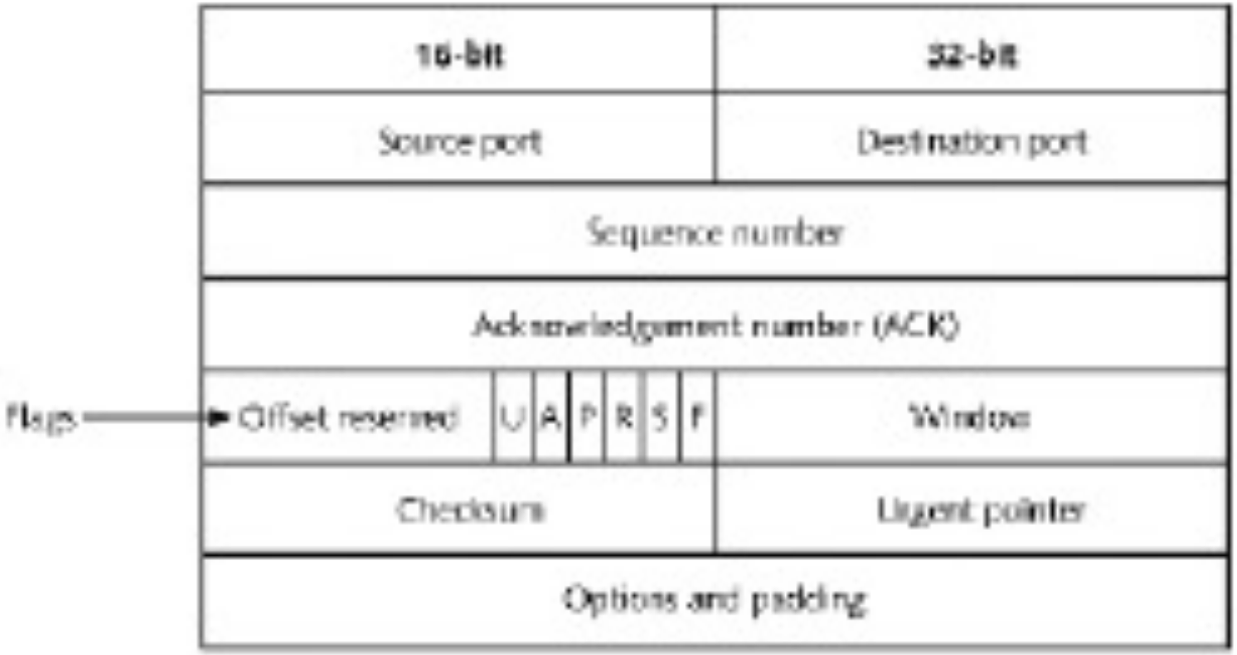
Using UNIX/Linux Tools (continued)

- 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)



Flags

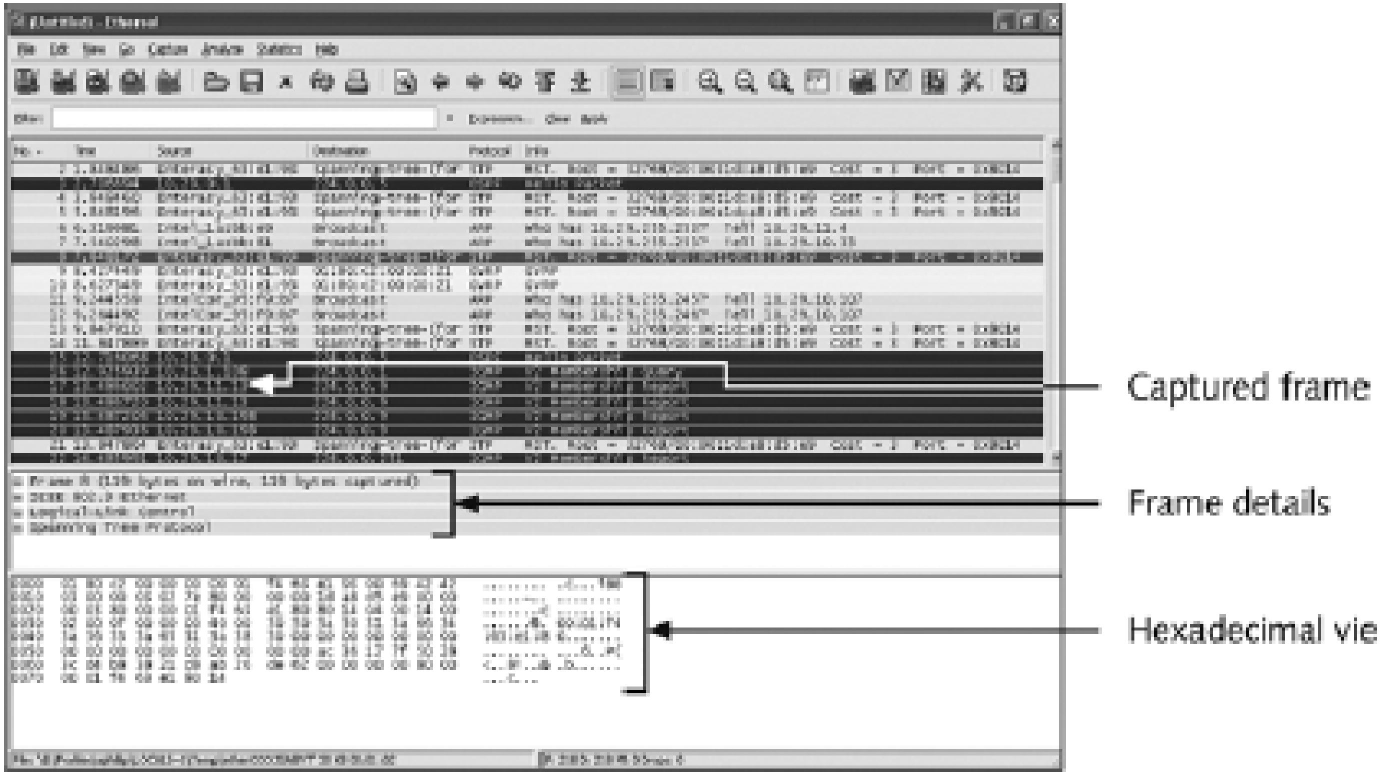
16-bit	32-bit
Source port	Destination port
Sequence number	
Acknowledgment number (ACK)	
Offset reserved | U | A | P | R | S | F	Window
Checksum	Urgent pointer
Options and padding	

Figure 11-8 A TCP header

Using Packet Sniffers (continued)

- Tools (continued)
  - Snort
  - Tcpslice
  - Tcpreplay
  - Tcpdstat
  - Ngrep
  - Etherape
  - Netdude
  - Argus
  - Ethereal

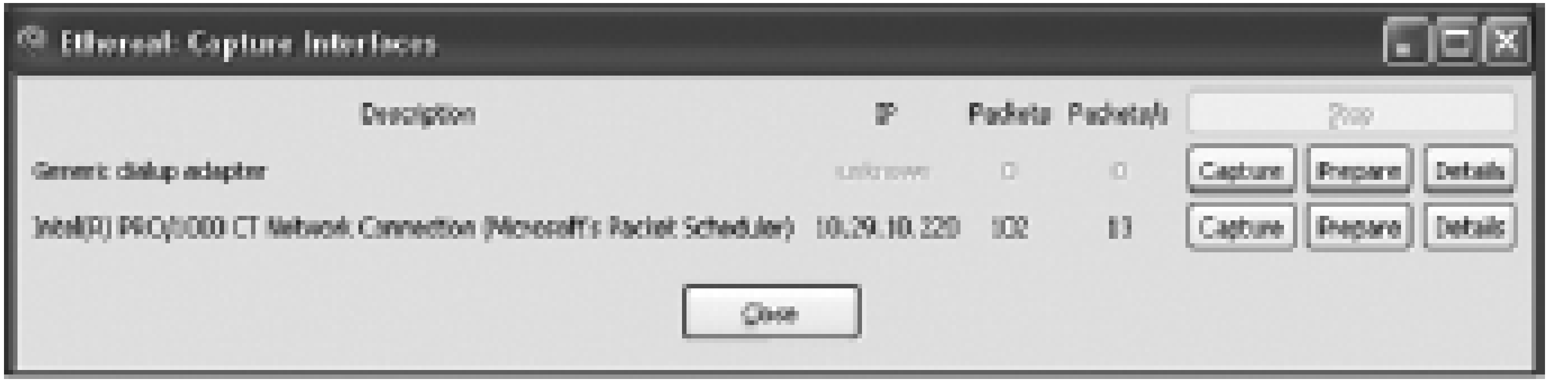
Using Packet Sniffers (continued)


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
Captured frame
Frame details
Hexadecimal view

```
Frame 8 (119 bytes on wire, 119 bytes captured)
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol
```

Figure 11-9 Ethereal in a Windows environment

Using Packet Sniffers (continued)

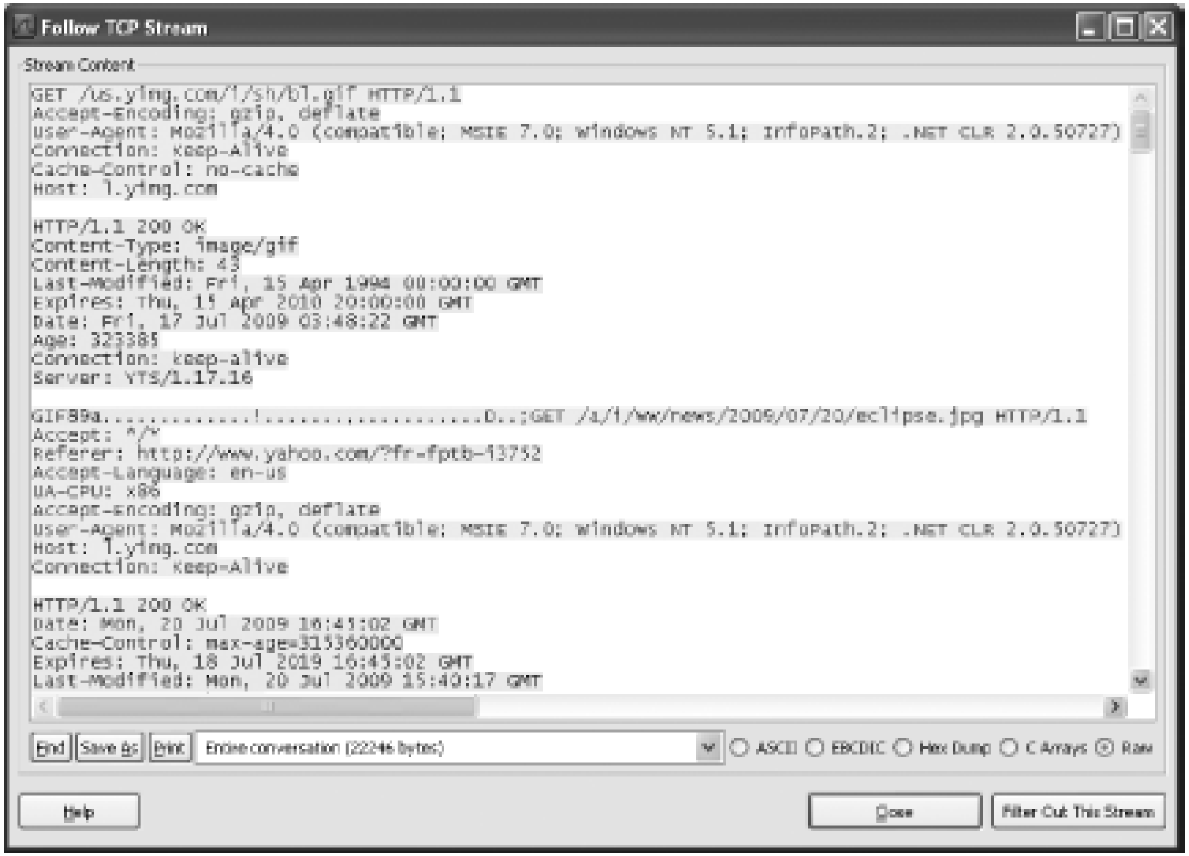


Ethereal: Capture Interfaces

Description	IP	Packets	Packets/s
Generic dialup adapter	unknown	0	0
Intel(R) PRO/1000 CT Network Connection (Microsoft's Packet Scheduler)	10.29.10.220	102	13

Figure 11-10 The Capture Interfaces dialog box

Using Packet Sniffers (continued)



```
GET /us.yimg.com/i/sh/bl.gif HTTP/1.1
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.2; .NET CLR 2.0.50727)
Connection: Keep-Alive
Cache-Control: no-cache
Host: l.yimg.com

HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 43
Last-Modified: Fri, 15 Apr 1994 00:00:00 GMT
Expires: Thu, 15 Apr 2010 20:00:00 GMT
Date: Fri, 17 Jul 2009 03:48:22 GMT
Age: 323385
Connection: keep-alive
Server: YTS/1.17.16

GIF89a..............!.....................D..;GET /a/i/ww/news/2009/07/20/eclipse.jpg HTTP/1.1
Accept: */*
Referer: http://www.yahoo.com/?fr=fptb-13752
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.2; .NET CLR 2.0.50727)
Host: l.yimg.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 20 Jul 2009 16:43:02 GMT
Cache-Control: max-age=315360000
Expires: Thu, 18 Jul 2019 16:43:02 GMT
Last-Modified: Mon, 20 Jul 2009 15:40:17 GMT
```

Entire conversation (22246 bytes)

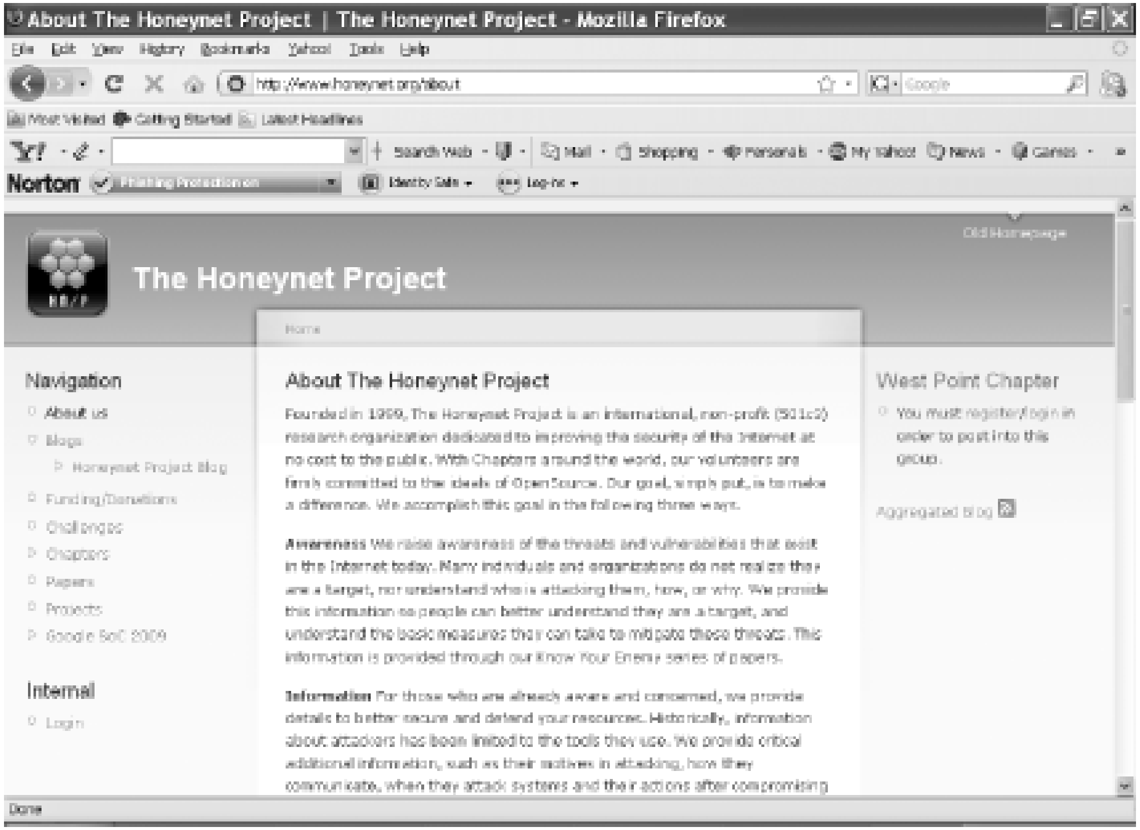
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 11-11 Following a TCP stream

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)


About The Honeynet Project | The Honeynet Project - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://www.honeynet.org/about
Google
Most Visited Getting Started Latest Headlines
Search Web Mail Shopping Personals My Yahoo! News Games
Norton Phishing Protection on Identity Safe Log-in
Old Homepage
The Honeynet Project
Home
Navigation
About us
Blogs
Honeynet Project Blog
Funding/Donations
Challenges
Chapters
Papers
Projects
Google SoC 2009
Internal
Login
West Point Chapter
You must register/login in order to post into this group.
Aggregated blog
Done

About The Honeynet Project

Founded in 1999, The Honeynet Project is an international, non-profit (501c3) research organization dedicated to improving the security of the Internet at no cost to the public. With Chapters around the world, our volunteers are firmly committed to the ideals of OpenSource. Our goal, simply put, is to make a difference. We accomplish this goal in the following three ways.

Awareness We raise awareness of the threats and vulnerabilities that exist in the Internet today. Many individuals and organizations do not realize they are a target, nor understand who is attacking them, how, or why. We provide this information so people can better understand they are a target, and understand the basic measures they can take to mitigate these threats. This information is provided through our Know Your Enemy series of papers.

Information For those who are already aware and concerned, we provide details to better secure and defend your resources. Historically, information about attackers has been limited to the tools they use. We provide critical additional information, such as their motives in attacking, how they communicate, when they attack systems and their actions after compromising

Figure 11-12 The Honeynet Project

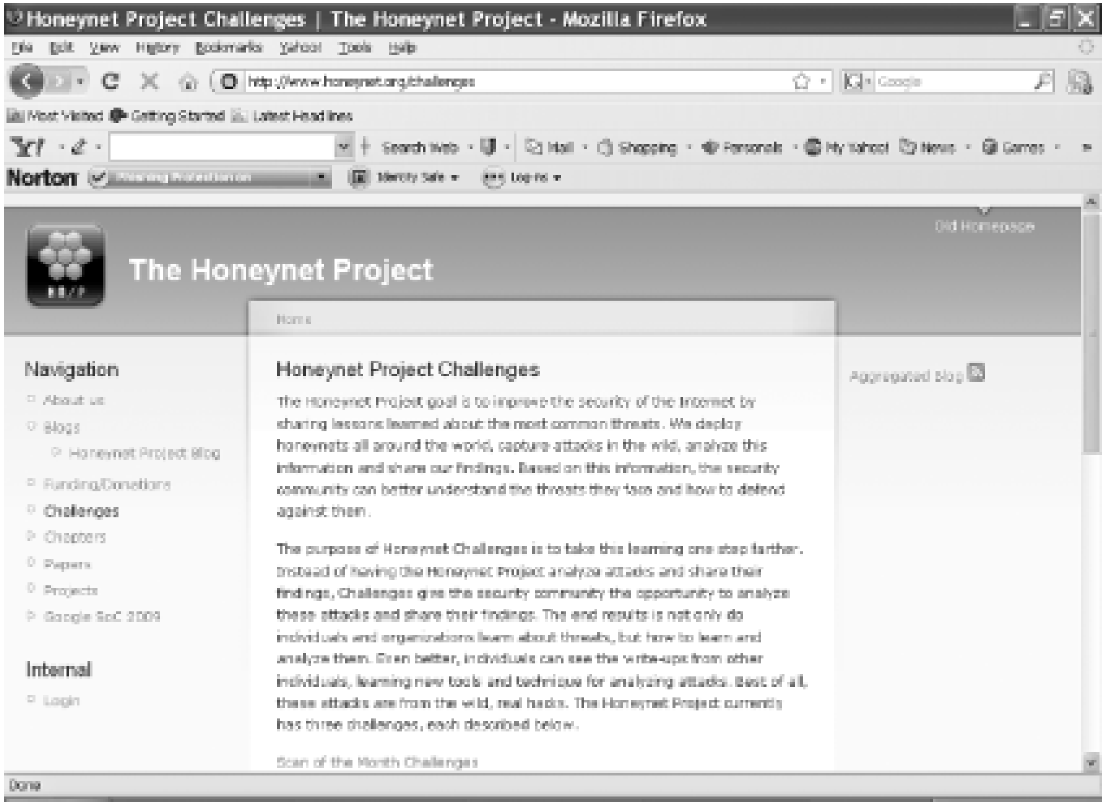
Examining the Honeynet Project (continued)

- **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)


Honeynet Project Challenges | The Honeynet Project - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://www.honeynet.org/challenges
Most Visited Getting Started Latest Headlines
Search Web Mail Shopping Personals My Yahoo! News Games
Norton Identity Safe Log-in
Old Homepage
The Honeynet Project
Home
Navigation
About us
Blogs
Honeynet Project Blog
Funding/Donations
Challenges
Chapters
Papers
Projects
Google SoC 2009
Internal
Login
Aggregated blog
Done

Honeynet Project Challenges

The Honeynet Project goal is to improve the security of the Internet by sharing lessons learned about the most common threats. We deploy honeynets all around the world, capture attacks in the wild, analyze this information and share our findings. Based on this information, the security community can better understand the threats they face and how to defend against them.

The purpose of Honeynet Challenges is to take this learning one step farther. Instead of having the Honeynet Project analyze attacks and share their findings, Challenges give the security community the opportunity to analyze these attacks and share their findings. The end results is not only do individuals and organizations learn about threats, but how to learn and analyze them. Even better, individuals can see the write-ups from other individuals, learning new tools and technique for analyzing attacks. Best of all, these attacks are from the wild, real hacks. The Honeynet Project currently has three challenges, each described below.

Scan of the Month Challenges

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