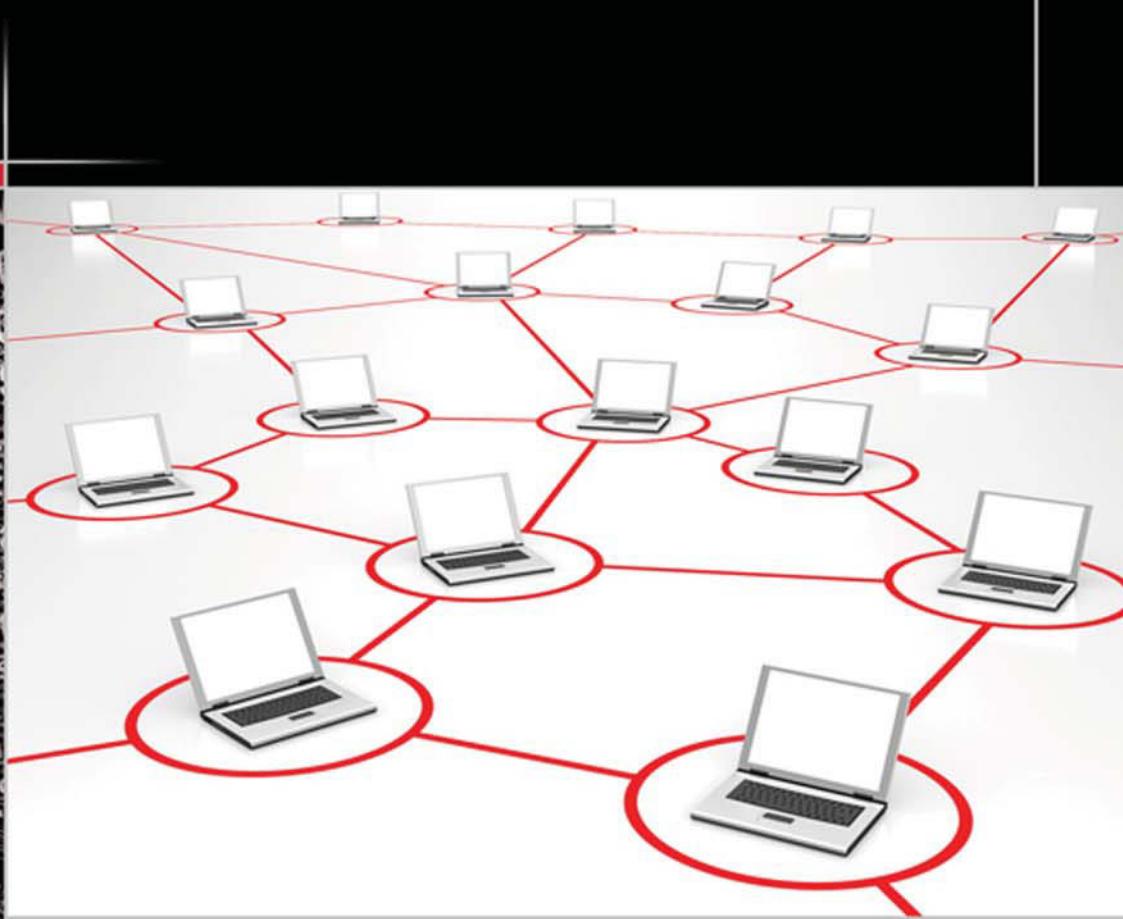


# Ethical Hacking & Countermeasures

## Secure Network Infrastructures



This title maps to

TM



## 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|EH – Certified Ethical Hacker

Certified Ethical Hacker is a certification designed to immerse the learner in an interactive environment where they will learn how to scan, test, hack and secure information systems. Ideal candidates for the C|EH program are security professionals, site administrators, security officers, auditors or anyone who is concerned with the integrity of a network infrastructure. The goal of the Ethical Hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits.

## Additional Certifications Covered By EC-Council Press:

### 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.

### 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|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.

### 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.

### 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.

# Secure Network Infrastructures

EC-Council | Press

Volume 5 of 5 mapping to



**Secure Network Infrastructures:**  
**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](http://www.cengage.com/permissions).

Further permissions questions can be e-mailed to  
[permissionrequest@cengage.com](mailto:permissionrequest@cengage.com)

Library of Congress Control Number: 2009933546

ISBN-13: 978-1-4354-8365-1

ISBN-10: 1-4354-8365-0

**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](http://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](http://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.

# Brief Table of Contents

TABLE OF CONTENTS .....	v
PREFACE .....	ix
CHAPTER 1 <b>Hacking Wireless Networks</b> .....	1-1
CHAPTER 2 <b>Physical Security</b> .....	2-1
CHAPTER 3 <b>Evading IDS, Firewalls and Detecting Honeypots</b> .....	3-1
CHAPTER 4 <b>Cryptography</b> .....	4-1
INDEX .....	I-1

*This page intentionally left blank*

# Table of Contents

PREFACE .....	ix
CHAPTER 1	
<b>Hacking Wireless Networks.....</b>	<b>1-1</b>
Objectives .....	1-1
Key Terms .....	1-1
Introduction to Hacking Wireless Networks .....	1-1
Wireless Networking.....	1-2
Wired Network Versus Wireless Network.....	1-2
Effects of Wireless Attacks on Businesses .....	1-2
Types of Wireless Networks .....	1-2
Advantages and Disadvantages of a Wireless Network.....	1-3
Wireless Standards .....	1-3
Wireless Standard: 802.11a.....	1-4
Wireless Standard: 802.11b.....	1-4
Wireless Standard: 802.11g.....	1-4
Wireless Standard: 802.11i .....	1-4
Wireless Standard: 802.11n.....	1-5
Wireless Standard: 802.15.1 (Bluetooth).....	1-5
Wireless Standard: 802.16 (WiMAX).....	1-5
Wireless Concepts.....	1-5
Related Technologies and Carrier Networks.....	1-5
Service Set Identifier (SSID).....	1-6
Authentication and Association.....	1-7
Authentication and (Dis)Association Attacks .....	1-8
MAC Sniffing and AP Spoofing.....	1-8
Wireless Devices .....	1-8
Antennas .....	1-8
Wireless Access Points .....	1-9
Beacon Frames.....	1-9
Phone Jammers .....	1-9
Wired Equivalent Privacy (WEP) .....	1-10
Role of WEP in Wireless Communication.....	1-10
Key Points .....	1-10
WEP Issues.....	1-10
WEP Authentication Phase .....	1-11
WEP Association Phase .....	1-11
WEP Flaws.....	1-12
WPA .....	1-12
WPA Vulnerabilities .....	1-12
WEP, WPA, and WPA2 .....	1-12
WPA2.....	1-12
Attacking WPA-Encrypted Networks .....	1-12
TKIP and LEAP .....	1-13
Temporal Key Integrity Protocol (TKIP).....	1-13
LEAP: The Lightweight Extensible Authentication Protocol .....	1-14
Hacking Methods .....	1-15
Techniques to Detect Open Wireless Networks.....	1-15
Steps for Hacking Wireless Networks .....	1-15
Super Bluetooth Hack .....	1-16
Man-In-The-Middle Attack (MITM) .....	1-17
Denial-Of-Service Attacks.....	1-17
Hijacking and Modifying a Wireless Network .....	1-18
Cracking WEP.....	1-18
Automated WEP Crackers.....	1-19
Pad Collection Attacks .....	1-19
XOR Encryption .....	1-19
Stream Cipher .....	1-20
WEP Cracking Tools .....	1-20

Rogue Access Points .....	1-23
Requesting a Beacon .....	1-23
Sniffing the Air .....	1-23
Tools to Generate Rogue Access Points .....	1-24
Cloaked Access Point.....	1-25
Scanning Tools .....	1-26
Prismstumbler .....	1-26
MacStumbler .....	1-26
Mognet .....	1-26
WaveStumbler .....	1-27
NetChaser .....	1-28
Wavemon .....	1-28
Wireless Security Auditor (WSA).....	1-28
AirTraf .....	1-29
WifiScanner.....	1-29
eEye Retina Network Security Scanner.....	1-29
Wireless Lan Scanner.....	1-29
Sniffing Tools .....	1-31
AiroPeek NX.....	1-31
Wireshark .....	1-31
vxSniffer .....	1-32
EtherPEG .....	1-33
AirMagnet .....	1-33
driftnet.....	1-33
WinDump .....	1-33
THC-RUT .....	1-35
Microsoft Network Monitor .....	1-36
Wireless Security Tools.....	1-36
CommView for WiFi PPC .....	1-36
AirMagnet Handheld Analyzer .....	1-36
AirDefense Guard .....	1-38
Google Secure Access .....	1-38
RogueScanner .....	1-38
Chapter Summary.....	1-40
Review Questions .....	1-40
Hands-On Projects .....	1-41

**CHAPTER 2**

<b>Physical Security .....</b>	<b>2-1</b>
Objectives .....	2-1
Key Terms .....	2-1
Case Example .....	2-2
Introduction to Physical Security .....	2-2
What Is the Need for Physical Security? .....	2-2
Physical Security .....	2-3
Physical Measures .....	2-3
Technical Measures .....	2-4
Operational Measures .....	2-9
Physical Security Personnel .....	2-9
Physical Security Challenges.....	2-10
Physical Security Threats.....	2-10
Personnel Challenges .....	2-11
Security Countermeasures.....	2-11
Physical Security Checklists.....	2-15
Tools .....	2-20
Encryption Tools .....	2-24
Chapter Summary.....	2-25
Review Questions .....	2-26
Hands-On Projects .....	2-27

<b>CHAPTER 3</b>	
<b>Evading IDS, Firewalls and Detecting Honeypots .....</b>	<b>3-1</b>
Objectives .....	3-1
Key Terms .....	3-1
Case Example .....	3-2
Introduction to Evading IDS, Firewalls, and Detecting Honeypots .....	3-2
Introduction to Intrusion Detection Systems .....	3-2
Intrusion Detection System (IDS) .....	3-3
Types of Intrusion Detection Systems .....	3-5
Indications of Intrusion .....	3-7
Steps to Perform after an IDS Detects an Attack .....	3-8
Evading IDS .....	3-8
Intrusion Prevention Systems (IPS) .....	3-10
Firewalls .....	3-13
Firewall Countermeasures .....	3-17
Honeypots .....	3-21
Security Responses to Hacking Attacks .....	3-24
Tools .....	3-25
Logging Tools .....	3-25
Host-Based IDS Tools .....	3-25
Intrusion Detection Tools .....	3-26
Tools to Evade IDS .....	3-31
Packet Generators .....	3-32
Tools to Breach Firewalls .....	3-35
Common Tools for Testing Firewalls and IDS .....	3-36
Honeypot Tools .....	3-46
Tools to Detect Honeypots .....	3-48
Chapter Summary .....	3-49
Review Questions .....	3-50
Hands-On Projects .....	3-51
<b>CHAPTER 4</b>	
<b>Cryptography .....</b>	<b>4-1</b>
Objectives .....	4-1
Key Terms .....	4-1
Introduction to Cryptography .....	4-2
Public-Key Cryptography .....	4-2
Digital Signature .....	4-2
Encryption Algorithms .....	4-3
Message-Digest (Hash) Functions .....	4-6
MD2, MD4, and MD5 .....	4-6
SHA-1 (Secure Hash Algorithm) .....	4-7
SSL (Secure Sockets Layer) .....	4-7
SSL Sessions .....	4-8
SSL Handshake Protocol Flow .....	4-8
Secure Shell (SSH) .....	4-9
Disk Encryption .....	4-10
Encryption-Breaking Initiatives .....	4-10
RSA Factoring Challenge .....	4-10
Distributed.net .....	4-11
Encryption Countermeasures .....	4-11
Code-Breaking Methodologies .....	4-11
Cryptography Attacks .....	4-12
Tools .....	4-13
Encryption-Cracking Tools .....	4-13
Data-Protection Tools .....	4-15
PGP (Pretty Good Privacy) .....	4-15

<b>viii</b>	Table of Contents	
Chapter Summary.....		4-18
Review Questions .....		4-18
Hands-On Projects .....		4-20
INDEX . . . . .		<b>I-1</b>

# Preface

Hacking and electronic crimes sophistication has grown at an exponential rate in recent years. In fact, recent reports have indicated 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.

## 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 CIEH 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
- 

## Secure Network Infrastructures

*Secure Network Infrastructures* discusses hacking wireless networks; physical security, how to evade IDS and Firewalls; how to detect honey pots; and an introduction to cryptography.

## Chapter Contents

Chapter 1, *Hacking Wireless Networks*, discusses wireless networking and the different wireless standards and provides information on SSID, wireless access points, how to crack WEP and much more. Chapter 2, *Physical Security*, focuses on the need to be aware of physical security; challenges in ensuring physical security; and ways to physically secure networks. Chapter 3, *Evading IDS, Firewalls and Detecting Honeypots*, discusses various security features that administrators deploy to protect their networks. Chapter 4, *Cryptography*, explains what cryptography is and discusses the various cryptography attacks and introduces various cracking tools.

## 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](http://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](http://www.cengage.com/community/eccouncil) for a link to the Student Resource Center.

---

## Additional Instructor Resources

Free to all instructors who adopt the *Secure Network Infrastructures* 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](http://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 activities 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 *Secure Network Infrastructures* content.

---

## Cengage Learning Information Security Community Site

This site was created for learners and instructors to find out about the latest in information security news and technology.

Visit [community.cengage.com/infosec](http://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 CIH Certified

The CIH certification focuses on hacking techniques and technology from an offensive perspective. The certification is primarily targeted at security professionals who want to acquire a well-rounded body of knowledge to have better opportunities in this field. Acquiring a CIH certification means the candidate has a minimum baseline knowledge of security threats, risks and countermeasures. An organization can rest assured that they have a candidate who is more than a systems administrator, a security auditor, a hacking tool analyst or a vulnerability tester. The candidate is assured of having both business and technical knowledge.

CIH 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](http://www.cengage.com/community/eccouncil), if one was not purchased with your book.
2. Once you have your exam voucher, visit [www.prometric.com](http://www.prometric.com) and schedule your exam, using the information on your voucher.
3. Take and pass the CIH certification examination with a score of 70% or better.

C|EH 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](http://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|EH certification examination with a score of 70% or better.

---

## About Our Other EC-Council | Press Products

### 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 organization's 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 organization's 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

### 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. The series, when used in its entirety, helps prepare readers to take and succeed on the CHFI, Certified Forensic Investigator certification exam from EC-Council.

#### 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

## 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

*This page intentionally left blank*

# 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 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*

# Hacking Wireless Networks

## Objectives

After completing this chapter, you should be able to:

- Understand wireless networking
- Understand the different types of wireless networks
- Understand the different wireless standards
- Understand SSID
- Understand wireless access points
- Understand Wired Equivalent Privacy
- Understand Wi-Fi Protected Access (WPA)
- Hack wireless networks
- Crack WEP
- Utilize tools for scanning and sniffing
- Secure wireless networks

## Key Terms

**APE** a term sometimes used for a wireless access point

**Roaming** the process of moving seamlessly between wireless access points

**Service set identifier (SSID)** a unique identifier that names a particular WLAN

**Whacker** a hacker on a wireless network

## Introduction to Hacking Wireless Networks

More and more networks are moving away from hard-wiring systems together and are instead communicating wirelessly. This leads to a host of new security concerns that will be addressed in this chapter.

## Wireless Networking

A wireless LAN (WLAN) is a local area network that exchanges data without the use of cables. A wireless LAN offers data connectivity in an existing building where wiring may not be practical due to construction design, location, or expense involved. WLANs are gaining popularity due to their ease of use and potential for mobility.

WLANs do raise the issue of security due to radio waves being easier to intercept than physical wires. However, the user authentication and data encryption system known as Wired Equivalent Privacy, or WEP, helps increase the security of the network. All users accessing the wireless network share the bandwidth available via access points.

The major advantage of wireless networks is mobility, although users should not expect flawless reception between access points.

### Wired Network Versus Wireless Network

Both types of communication have their pros and cons. Wireless networks offer fully mobile, untethered access to the network, allowing users to more easily connect using notebooks or other mobile devices. However, this mobility comes with the following tradeoffs:

- Higher cost
- Lower reliability
- Slower performance
- Lessened security

### Effects of Wireless Attacks on Businesses

As more and more firms adopt wireless networks, security becomes more important. Businesses are at high risk from wireless hackers, sometimes called *whackers*. Whackers do not need physical entry into the business network to hack, but can easily compromise a network with the help of freely available tools. Warchalking, wardriving, and warflying are some of the ways in which a whacker can assess the vulnerability of a wireless network. Many organizations are deploying wireless networks to allow employees to roam the corporate campus without leaving the network. Some airports offer wireless connectivity so travelers can continue working while waiting for flight departures, and many hotels also provide these facilities to their customers. Unfortunately, this ease of use also comes with increased risk, as an attacker who is sitting miles away can sniff the network without being noticed.

Large companies generally make the most use of wireless networks and devices. These networks are generally expensive and troublesome to deploy and manage. They require networking expertise. However, from the whacker's point of view, wireless networks and access points (sometimes called *APes*, WAPs, or APs) are some of the easiest, most inexpensive targets while being some of the hardest to defend.

### Types of Wireless Networks

There are four basic types of wireless networks.

#### Peer-To-Peer Networks

In this type of network, every computer can communicate directly with the other computers on the same network without going through an access point. They can share files and printers in this manner. However, they may not be able to access wired LAN resources unless one of the computers acts as a bridge to the wired LAN using special software.

#### Extension to a Wired Network

An extension to a wired network can be obtained by placing access points between the wired network and the wireless devices. With this type of network, the access point acts like a hub, providing connectivity for the wireless computers on its system. It can connect a wireless LAN to a wired LAN, allowing wireless computer access to LAN resources such as file servers or existing Internet connections.

There are both software and hardware access points. Software access points (SAPs) can be connected to the wired network and run on a computer equipped with a wireless network interface card. Hardware access points (HAPs) provide comprehensive support to most wireless features.

## Multiple Access Points

This type of network consists of computers connected wirelessly by using multiple access points. If a single large area cannot be covered by a single access point, multiple access points or extension points can be established. Although extension point capability has been developed by some manufacturers, it is not defined in the wireless standard.

When using multiple access points, each access point's coverage area needs to overlap another point's coverage area. This provides users the ability to move around seamlessly using a feature called *roaming*. Some manufacturers develop extension points that act as wireless relays, extending the range of a single access point. Multiple extension points can be strung together to provide wireless access to locations far from the central access point.

## LAN-To-LAN Wireless Network

Access points provide wireless connectivity to local computers, and local computers on different networks can be interconnected. All hardware access points have the capability of being interconnected with other hardware access points. However, interconnecting LANs over wireless connections can be a complex task.

## Advantages and Disadvantages of a Wireless Network

Using a wireless network has several key advantages:

- It provides mobility to users accessing the networks.
- Connecting to the network is easier.
- The initial cost to set up the WLAN is low compared to adding Ethernet cables to a large building.
- Data can be transmitted in different ways through cellular networks such as Mobitex, DataTAC, Cellular Digital Packet Data (CDPD), and others.
- Sharing of data is easy among wireless devices.

However, a wireless network also comes with some disadvantages:

- There is no physical protection for wireless networks.
- The risk of data sharing is high. Packets are sent through the airwaves, and an attacker can easily use various wireless sniffing tools.
- Most wireless devices use a broad spectrum, so it is easy to identify the signal, making it more vulnerable to attackers.

---

## Wireless Standards

IEEE (Institute of Electrical and Electronics Engineers) standard 802.11 has grown from a standard of infrared communication to cover most wireless communications used today. It has several issues, such as security, roaming among multiple access points, and quality of service. Therefore, there are many extensions of this standard for different uses. The following are some of the extensions:

- 802.11a: More channels, high speed, less interference
- 802.11b: Protocol in use when Wi-Fi became popular
- 802.11g: Similar to 802.11b, only faster
- 802.11i: Improves WLAN security
- 802.11n: Next-generation Wi-Fi standard with greatly improved throughput

There are also other IEEE standards covering wireless communications, including the following:

- 802.15.1: Bluetooth, a high-speed, short-distance cable replacement option
- 802.16: WiMAX, a long-distance wireless infrastructure

## Wireless Standard: 802.11a

IEEE 802.11a has the following features:

- Works at 40 MHz in the 5-GHz range
- Theoretical transfer rates up to 54 Mbps
- Actual transfer rates of approximately 26.4 Mbps
- Limited in use because it is almost a line-of-sight transmittal that requires multiple WAPs (wireless access points)
- Uses a modulation technique called coded orthogonal frequency-division multiplexing (COFDM)
- Cannot operate in same range as 802.11b/g
- Absorbed more easily than other wireless implementations
- Overcomes the challenge of indoor radio frequencies
- Uses a single-carrier, delay-spread system

## Wireless Standard: 802.11b

IEEE 802.11b was used in most home and office networks before 802.11g. It has the following features:

- Operates at 20 MHz in the 2.4-GHz range
- Theoretical transfer rates up to 11 Mbps
- Actual transfer rates of 5.9 Mbps over TCP, 7.1 Mbps over UDP
- Transmits up to 8 km in a city environment
- Not as easily absorbed as 802.11a
- Can cause or receive interference from the following:
  - Microwave ovens
  - Wireless telephones
  - Other wireless appliances operating in the same frequency

## Wireless Standard: 802.11g

IEEE 802.11g is replacing 802.11b in most applications. Its features include the following:

- Operates at the same frequency range as 802.11b
- Theoretical transfer rates up to 54 Mbps
- Actual transfer rates of approximately 24.7 Mbps
- Backward compatible with 802.11b
- Same limitations as 802.11b
- May suffer significant decrease in network speeds if entire network is not upgraded from 802.11b

## Wireless Standard: 802.11i

IEEE 802.11i uses improved encryption for networks that use the 802.11a, 802.11b, and 802.11g standards. Its security features include the following:

- 802.1x for authentication (EAP and authentication server)
- Robust Security Network (RSN) to keep track of associations
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to provide confidentiality, integrity, and origin authentication

## Wireless Standard: 802.11n

IEEE 802.11n is the next-generation Wi-Fi standard developed by Task Group N of the IEEE. This standard merges the use of multiple antennas, more advanced encoding, and optional spectrum doubling to attain data rates of up to 600 Mbps.

802.11n has the following basic features:

- Based on multiple-in/multiple-out (MIMO) technology
- Expected increase of throughput to potentially well over 100 Mbps
- Specifies improvement to the physical layer and medium access control layer
- Improved radio technology to increase physical data transfer
- New methods to implement effective management of improved physical-layer performance modes
- Improved data transfer efficiency to reduce performance impact of physical-layer headers and radio turnaround delays that adversely affect the physical transfer rate

## Wireless Standard: 802.15.1 (Bluetooth)

IEEE 802.15.1, commonly called Bluetooth, is used for wireless personal area networks, or WPANs. It is used in short-range, low-power, low-cost small networks such as the connection between a cellular phone and headset, or computer and mouse. Bluetooth specifies standards on the physical layer and data-link layer of the OSI model with the following four sublayers:

1. RF layer
2. Baseband layer
3. Link manager
4. Logical Link Control and Adaptation Protocol (L2CAP)

## Wireless Standard: 802.16 (WiMAX)

WiMAX (Worldwide Interoperability for Microwave Access) is a communication system designed to support point-to-multipoint wireless broadband access. It provides high-speed mobile Internet access with ranges of up to 30 miles and speeds of up to 75 Mbps.

There are two types of WiMAX: fixed and mobile. Fixed WiMAX is similar to a cable or DSL modem service and delivers wireless last-mile access (the connection between a communications provider and a customer) for fixed broadband services. Mobile WiMAX supports both fixed and mobile applications.

---

# Wireless Concepts

## Related Technologies and Carrier Networks

The following are some technologies and carrier networks related to wireless networks:

- *CDPD (Cellular Digital Packet Data):* CDPD works over the popular time division multiple access (TDMA) mobile network, which is the most widely deployed mobile network in the United States. CDPD modems use serial port connections or PCMCIA slots and offer speeds of up to 19.2 Kbps. Currently, TDMA operators are moving toward GSM technology.
- *1xRTT on CDMA:* CDMA (Code Division Multiple Access) is the second most popular mobile technology in the United States. The original CDMA data services offered speeds of 9,600 bps to 14.4 kbps. An upgrade called 1xRTT is supposed to achieve a speed of up to 144 kbps, but the actual speed is somewhere between 60 and 80 kbps. 1xRTT is the first phase of the CDMA2000 plan. A technology called EVDO can theoretically achieve 2 Mbps from fixed locations over CDMA.
- *GPRS/GSM:* It is a challenge for network planning engineers to manage the integration of GPRS (General Packet Radio Service) services into GSM (Globile System for Mobile communications) networks. One critical challenge comes from the requirement of providing a certain quality of service (QoS) for GPRS traffic without significantly degrading the performance of existing GSM services. In a GSM/GPRS network, it is important to keep exclusive channels for GPRS in order to offer a baseline QoS for

GPRS users. On the other hand, the exclusive reservation obviously reduces the capacity of GSM traffic. This causes a significant impact on the performance of GSM traffic, especially GSM handover traffic (traffic that occurs in the process of a mobile device moving from one cell carrier to another as the device crosses cell boundaries).

- *FRS and GMRS:* FRS (Family Radio Service) operates around 462 and 467 MHz and is sometimes referred to as UHF citizens' band. FRS radios share some channels with GMRS (General Mobile Radio Service) radios but are restricted to 500 mW maximum power. FRS radios come with fixed antennas and cannot be legally modified to accommodate other antennas or amplifiers. GMRS gear can include removable antennas, making it easy to use a handheld with a car mount or stationary antenna. With the use of repeaters, GMRS can be used to communicate over large distances.
- *HPNA and Powerline Ethernet:* HPNA (Home Phone Networking Alliance) provides networking capabilities over existing CAT3 cable and can share the same wire as a standard telephone line. Powerline Ethernet uses AC power lines as a physical medium for network traffic. The data speed is comparable to 802.11b.
- *802.1x:* The 802.1x protocol is not a wireless protocol, but rather, a method for port authentication that can be applied to nearly any network connection, whether wired or wireless. 802.1x is an IEEE standard that attaches EAP (Extendable Authentication Protocol) over wired or wireless Ethernet, and provides several authentication techniques including token cards, Kerberos, certificates, and public key authentication.
- *BSS and IBSS:* BSS (Basic Service Set) has one station acting as a gateway between a wireless and a wired (Ethernet) network. IBSS (Independent Basic Service Set) does not require an access point.

## Service Set Identifier (SSID)

A *service set identifier (SSID)* is a unique identifier that names a particular WLAN. It is used to establish and maintain wireless connectivity. SSIDs act as a single shared password between access points and clients. Security concerns arise when the default values are not changed since these networks can then be more easily compromised. An unsecure access mode station communicates with access points by broadcasting the configured SSID, a blank SSID, or an SSID configured as "any." Because an SSID is a unique name given to a WLAN, all devices and access points present in the WLAN must use the same SSID. It is necessary for any device that wants to join the WLAN to give the unique SSID. Unfortunately, SSID does not provide security to WLAN, as it can be sniffed in plaintext from packets.

An SSID can be up to 32-characters long. The following are some common default SSIDs:

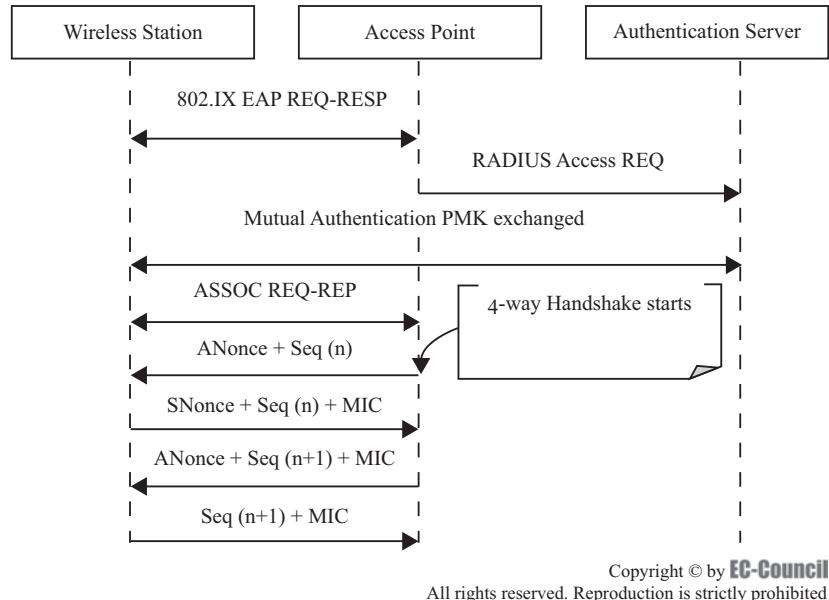
- Comcomcom
- Default SSID
- Intel
- Linksys
- Wireless
- WLAN

### **Is the SSID a Secret?**

The SSID is a key to the network, so it is necessary for every user to choose an SSID that is difficult to guess. The following shows how devices connect to a WLAN using an SSID:

- Stations searching for an access point send the SSID in a probe request.
- Access points reply with a probe reply frame that includes the SSID and BSSID (basic service set identifier) pair.
- Stations that want to be a part of the BSS (basic service set) send an association request frame, which also includes the SSID/BSSID pair in cleartext.

The SSID is secret only on closed networks with no activity. Closed networks are mainly inconvenient to legitimate users.



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

**Figure 1-1** This shows the four-way handshake by which a station authenticates itself.

## Authentication and Association

To become part of a BSS, a station should first authenticate itself on the network. Then it will request association to a specific access point. The access point is responsible for authentication and accepts the association of the stations unless an add-on authentication system such as RADIUS is used. The MAC address is responsible for giving the exact identity of the station or access point. Figure 1-1 is a flowchart showing how this four-way handshake operates.

### Authentication Modes

Authentication can either be performed by a station that gives the correct SSID or through shared key authentication. In shared key authentication, the following occurs:

- The access point and all base stations in a network share a secret encryption key that has the following features:
  - Hard to deploy
  - Hard to change
  - Hard to keep secret
  - Provides no accountability
- It is necessary for the station to encrypt with WEP a challenge text that should be offered by the access point.
- An eavesdropper can determine both the plaintext and the ciphertext by performing a known plaintext attack that in turn helps to crack WEP encryption.

### The 802.1x Authentication Process

For 802.1x authentication to work on a wireless network, the AP must be able to securely identify traffic from a particular wireless client. The identification is accomplished by using authentication keys that are sent to the AP and the wireless client from the Remote Authentication Dial In User Service (RADIUS) server. When a wireless client (802.1x supplicant) comes within range of the AP (802.1x authenticator), the following process occurs:

1. The AP issues a challenge to the wireless client.
2. The wireless client responds with its identity.
3. The AP forwards the identity to the RADIUS server using the uncontrolled port.

4. The RADIUS server sends a request to the wireless station via the AP, specifying the authentication mechanism to be used.
5. The wireless station responds to the RADIUS server with its credentials via the AP.
6. If the credentials are acceptable, the RADIUS server sends an encrypted authentication key to the AP.
7. The AP generates a multicast/global authentication key encrypted with a per-station unicast session key, and transmits it to the wireless station.

### **802.11 Specific Vulnerabilities**

Two common vulnerabilities to the 802.11 standard are default SSIDs and beacon broadcast. Many people fail to change the SSIDs on their networks as set by the manufacturers. Attackers will see this and assume the target has not spent much time securing the network. Also, base stations regularly broadcast their existence for end users to listen and negotiate a session. These signals can be captured by anyone, who can then discover the SSID.

### **Authentication and (Dis)Association Attacks**

Any station can impersonate another station or access point and attack or interfere with the authentication and association mechanisms. Since these frames are not encrypted, the difficulty is trivial. A station receiving disassociation and deauthentication frames must redo the authentication and association process. With a single short frame, an attacker can delay the transmission of the data acquiring the station and real access point to redo these processes. This takes several frames to perform.

### **MAC Sniffing and AP Spoofing**

Most access points have MAC address filtering capabilities, which means a network administrator can create a list of approved MAC addresses that are allowed to connect to the network. This feature has two options: open or closed. In a closed MAC filter, only listed addresses are allowed to access the network. In an open MAC filter, the addresses listed in the filter are prevented from accessing the network.

The MAC address does not offer a good security mechanism because it is both easily observable and reproducible. Even if WEP is enabled, an attacker can easily sniff MAC addresses because they appear in cleartext. Moreover, it is possible to change the MAC address on a wireless card through software.

Each network card has a unique MAC address. But the attacker can easily change the MAC address by using the ifconfig command. All the attacker needs to know is a trusted MAC address. When the attacker tries to login with the spoofed MAC address, the legitimate user with that MAC address is disconnected from the wireless network.

### **Defeating MAC Address Filtering in Windows**

Most commercial-grade and consumer-grade wireless networking equipment sends the MAC address in cleartext even if WEP is enabled. Passively sniffing the traffic on a wireless network using a tool such as Ethereal allows an attacker to determine one or more MAC addresses that are allowed to connect to the network. If MAC address filtering is the only security measure in place, attackers need only to change their MAC addresses to those that are allowed access.

---

## **Wireless Devices**

### **Antennas**

Antennas are needed for sending and receiving radio signals. There are two types of antennas:

- Omnidirectional antennas
- Directional or unidirectional antennas

Omnidirectional antennas radiate electromagnetic energy regularly in all directions. They usually radiate strong waves uniformly in two dimensions, but not as strongly in the third. These antennas are efficient in areas where wireless stations use time division multiple access technology. A good example of an omnidirectional antenna are the ones used by radio stations. These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio will be able to receive a signal regardless of its location.

Directional antennas radiate radio waves in a more constrained area. They are not as versatile as omnidirectional antennas, but are useful for fixed locations. These antennas are used where the distances between the

transmitter and receiver are no more than a few hundred meters. The amount of information to be transferred can be high.

It is not difficult to assemble an antenna out of common materials. For example, the requirements for making a can antenna are a piece of PVC, all-thread, washers, some low-cost copper tubing, a can, and some scrap cardboard.

### **Super Cantenna**

Super Cantenna is a device that can extend the range of a wireless network or connect to other wireless networks nearby. A user connects it to the wireless router, AP, or network card, and points it at the target. Its features include the following:

- Works with most wireless devices
- Compatible with 802.11b and 802.11g wireless networks
- Engineered for maximum signal strength and distance

### **Wireless Access Points**

An access point is a piece of wireless communications hardware that creates a central point of wireless connectivity. Similar to a hub, the access point is a common connection point for devices in a wireless network.

APs are necessary for strong wireless security. They are also used for increasing the physical range of services. The range of the APs is increased with the help of repeaters, which amplify the network's radio signals.

In a corporate setting, wireless access points must be deployed and managed in common areas of the campus. They must also be coordinated with the telecommunications and network managers.

The following points should be kept in mind while positioning access points:

- It is best to choose a location that maximizes the broadcast pattern of the antenna over areas inside the facility where users will be located.
- Wireless devices must be near the antenna to minimize signal degradation.
- It is necessary to keep access points indoors, as they are not waterproof.
- If the antenna is mounted on the roof, then the best access point is in the loft.

### **Beacon Frames**

Beacon frames broadcast the SSID so users can locate available networks. Networks without beacon frames are called closed networks but should not be considered secure based purely on that fact, as the SSID can be easily sniffed.

### **Phone Jammers**

A cell phone jammer spreads low-power radio frequency waves to interrupt the communication between cell phones and base stations. It only interrupts in a specific regulated zone. The cell phones are automatically reestablished when the phone jammer turns off. The range of a cell phone jammer is based on its power and the local environment. The following are areas where phone jammers may be useful:

- Businesses (conferences, board-of-directors rooms, seminars, and meeting rooms)
- Government buildings and complexes
- Police stations
- Drug enforcement facilities
- Prisons
- Courts of law and courthouses
- Embassies
- Military installations, complexes, and training centers

Phone jammers are made up of the following components:

- *Antenna*: Sends the signals
- *Circuitry*: The main components, including:

- *Voltage-controlled oscillator*: Transmits the radio signals
- *Tuning circuit*: Controls the signals by transmitting a specific voltage to the oscillator
- *Noise generator*: Produces the frequency to block the network
- *RF amplification (gain stage)*: Boosts the power of the radio frequency output
- *Power supply*: Can be wired or battery powered

## **Wired Equivalent Privacy (WEP)**

Wired Equivalent Privacy (WEP) is a security protocol designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to that which is usually expected of a wired LAN. WEP is a component of the IEEE 802.11 WLAN standards.

Physical security can be applied in wired LANs to stop unauthorized access to a network. In a wireless LAN, the network can be accessed without physically connecting to the LAN. Therefore, IEEE utilizes an encryption mechanism at the data-link layer for minimizing unauthorized access. This is accomplished by encrypting data with the symmetric RC4 encryption algorithm.

### **Role of WEP in Wireless Communication**

WEP uses a secret key to protect wireless communications from eavesdropping and minimizes unauthorized access to the wireless network. This key is used to encrypt packets before transmission. A mobile station and an access point share this key. An integrity check is performed to ensure that packets are not altered after transmission. 802.11 WEP encrypts data only between 802.11 stations. The following are its main goals:

- Confidentiality
- Access control
- Data integrity
- Efficiency

### **Key Points**

- WEP was developed without academic or public review, or review from cryptologists.
- It has significant vulnerabilities and design flaws.
- Only about one quarter to one third of wireless access points still use WEP.
- WEP is a stream cipher that uses RC4 to produce a stream of bytes that are XORed with plaintext.
  - The input to the stream cipher algorithm is an initialization vector (IV) sent in plaintext and a secret key.
  - The IV size of WEP is 24 bits.
  - The length of the secret key is either 40 or 104 bits, for a total length for the IV and secret key of 64 or 128 bits.

### **WEP Issues**

WEP has the following issues:

- CRC32 is not sufficient to ensure complete cryptographic integrity of a packet.
  - By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
- IVs are 24 bits.
  - An AP broadcasting 1,500-byte packets at 11 Mbps would exhaust the entire IV space in five hours.
- There are known plaintext attacks.
  - When there is an IV collision, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.
- WEP is vulnerable to dictionary attacks.
  - WEP is based on a password.

- The small space of the initialization vector allows the attacker to create a decryption table, which is a dictionary attack.
- WEP can be vulnerable to denial-of-service attacks.
  - Associate and disassociate messages are not authenticated.
- Eventually, an attacker can construct a decryption table of reconstructed keystreams.
  - With about 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.
- A lack of centralized key management makes it difficult to change WEP keys with any regularity.
- IV is a value that is used to randomize the keystream value, and each packet has an IV value.
  - The standard allows only 24 bits, so the range of values can be used up within a matter of hours at a busy AP.
  - IV values will be reused.
- The standard does not dictate that each packet must have a unique IV, so vendors use only a small part of the available 24-bit possibilities.
  - A mechanism that depends on randomness is not random at all, allowing attackers to easily figure out the keystream and decrypt other messages.

Since most companies have configured their stations and APs to use the same shared key, or the default four keys, the randomness of the keystream relies on the uniqueness of the IV value. The use of IV and a key ensures that the keystream for each packet is different, but in most cases the IV changes while the key remains constant. Since there are only two main components to this encryption process where one stays constant, the randomization of the process decreases to an unacceptable level. A busy access point can use all available IV values (224) within hours, which requires the reuse of IV values.

Making the IV issue worse is that the 802.11 standard does not require each packet to have a different IV value. In many implementations, the IV value changes only when the wireless NIC reinitializes, usually during a reboot. The 24 bits for the IV value provide enough possible IV combination values, but most implementations only use a handful of bits.

## **WEP Authentication Phase**

In open system authentication (OSA) all the transactions are clear, enabling an intruder to sniff the traffic and walk through the same steps to be authenticated and associated to an AP.

Shared key authentication (SKA) encrypts most, but not all, encryption components for the authentication process and data transfers. It uses WEP encryption, which can be easily defeated.

The access criteria may include specific MAC addresses of stations, but intruders can easily change their MAC addresses to those that completed the authentication phase.

When a wireless station wants to access a network, it sends a probe request packet on all channels so that any AP in range will respond. The AP responds with packets containing the AP's SSID and other network information. The process of the authentication phase is as follows:

- When an OSA is configured, the station will send an authentication request to the AP. The AP will make an access decision based on its policy.
- When SKA is configured, the AP will send a challenge to the station. The station encrypts it with its WEP key and sends it back to the AP.
- The AP can successfully decrypt and obtain the challenge value that the station has authorized.

## **WEP Shared Key Authentication**

In shared key authentication, the requesting station first sends the challenge text. The receiving station then decrypts the challenge using the same shared key. It compares it to the challenge text sent earlier, sending an acknowledgment if the text matches and a negative authentication notice if it does not. Once acknowledged, the transmission is sent.

## **WEP Association Phase**

After the authentication phase, the station will send an association request packet to the AP. If the AP has a policy to allow this station to access the network, it will associate the station to itself by placing the station in its association table. A wireless device has to be associated with an AP to access network resources and not just be authenticated.

The authentication and association phases authorize the device and not the user. There is no way to know if an unauthorized user has stolen and is using an authorized device.

## **WEP Flaws**

Some basic flaws undermine WEP's ability to protect against a serious attack, including the following:

- No defined method for encryption key distribution.
  - Preshared keys are set once at installation and are rarely (if ever) changed.
  - It is easy to determine the number of plaintext messages encrypted with the same key.
- Use of RC4, which was designed to be a one-time cipher and not intended for multiple message use.
  - The preshared key is rarely changed.
  - An attacker monitors the traffic and determines the different ways to decipher the plaintext message.
  - With knowledge of the ciphertext and the plaintext, an attacker can compute the key.
- Attackers can analyze the traffic from passive data captures and crack the WEP keys with the help of tools such as AirSnort, WEPCrack, and dweputils.
- Key generators that are used by different vendors are vulnerable.
- Key scheduling algorithms are also vulnerable to attack.

## **WPA**

WPA (Wi-Fi Protected Access) is compatible with the 802.11i security standard. It is a software upgrade, but may also require a hardware upgrade. Nearly every Wi-Fi company has decided to employ this standard for increased security called Wi-Fi Protected Access.

The security issue concerning initialization vectors (IVs) is taken care of by WPA. Data encryption security is increased in WPA because messages are passed through Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP) to enhance data encryption. The unicast traffic changes the encryption key after every frame using TKIP.

## **WPA Vulnerabilities**

WPA is vulnerable to denial-of-service attacks if an attacker injects or corrupts packets. The only way around this attack is to switch completely to WEP until it subsides. In addition, WPA is vulnerable to dictionary attacks if the preshared 14-character key is a real word.

## **WEP, WPA, and WPA2**

WEP's primary purpose is to provide for confidentiality of data on wireless networks at a level equivalent to that of wired LANs, but it is weak and fails to meet any of its goals. WPA fixes most of WEP's problems but adds some new vulnerabilities. WPA2 is expected to make wireless networks as secure as wired networks.

## **WPA2**

WPA2 (Wi-Fi Protected Access 2) is compatible with the 802.11i standard. It supports most of the security features that are not supported by WPA. It provides stronger data protection and network access control. WPA2 implements the National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm to provide government-grade security.

WPA2 offers two modes of operation: WPA-Personal, which makes use of a setup password, and WPA-Enterprise, which confirms the network user through a server.

## **Attacking WPA-Encrypted Networks**

WPA utilizes a 256-bit preshared key or a passphrase that can vary in length from 8 to 63 bytes. Short passphrase-based keys (less than 20 bytes) are vulnerable to an offline dictionary attack. The preshared key that is used to set up the WPA encryption can be captured during the initial communication between the access point and the client. Once the preshared key is captured, it can be used to guess the WPA key using a standard dictionary attack. In theory, this type of dictionary attack takes less time and effort than attacking WEP.

## Evil-Twin Attack

An evil-twin is a homemade wireless access point that masquerades as a legitimate access point to gather private information without the end user's knowledge. The attacker positions the evil-twin in the vicinity of a legitimate access point and discovers what name and radio frequency that point uses. The attacker then sends out a radio signal using the same name.

# TKIP and LEAP

## Temporal Key Integrity Protocol (TKIP)

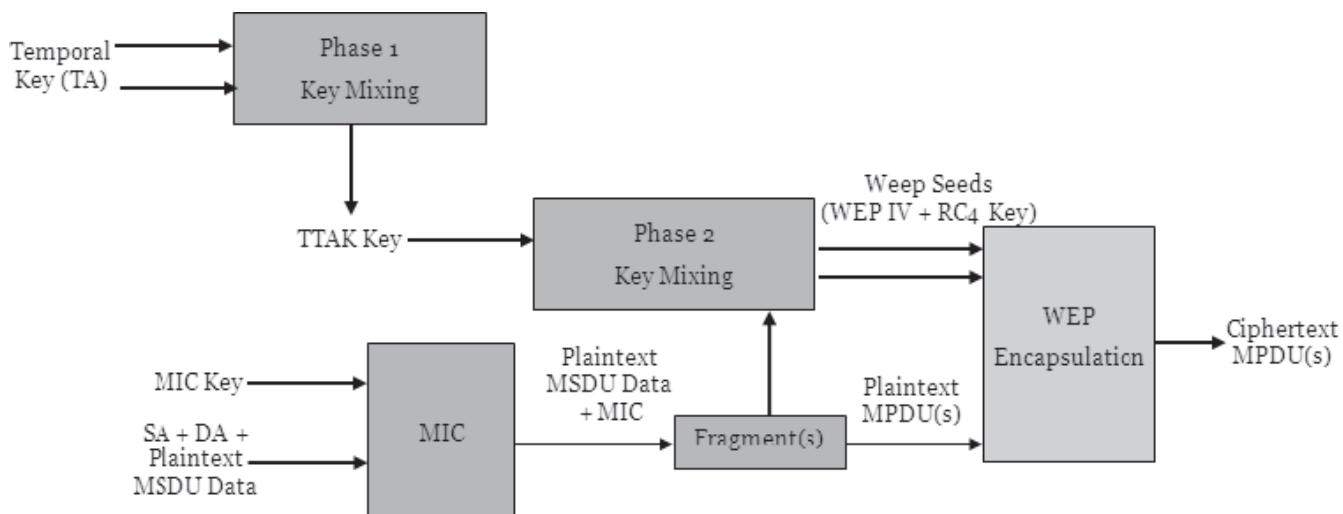
The Temporal Key Integrity Protocol (TKIP) is an element of the IEEE 802.11i encryption standard. TKIP was designed as a successor to WEP. TKIP eliminates the drawbacks of WEP by offering per-packet key mixing, a rekeying mechanism, and a message integrity check. Its key points include the following:

- Secret key created during four-way handshake authentication
- Dynamically changes secret key
- Function used to create new keys based on the original secret key created during authentication
- Initialization vectors increased to 48 bits
- First 4 bits indicate QoS traffic class
- Remaining 44 bits are used as a counter
- Over 500 trillion keystreams possible
- Initialization vectors are hashed
- Harder to detect keystreams with the same initialization vectors

## Functioning of TKIP

TKIP encryption works in a two-phase process. In the first phase, a session key is generated from a temporal key, the TKIP sequence counter (TSC), and the transmitter's MAC address. Once this phase is completed, a value called the TKIP-mixed transmit address and key (TTAK) is created. This value is used as a session-based WEP key in the second phase.

In the second phase, the TTAK and the IV are used to produce a key that encrypts the data. TKIP can be considered more safe than WEP because the key is using a different value. A flowchart of TKIP's encryption can be seen in Figure 1-2.



**Figure 1-2** TKIP is considered more safe than WEP.

## Changes from WEP to TKIP

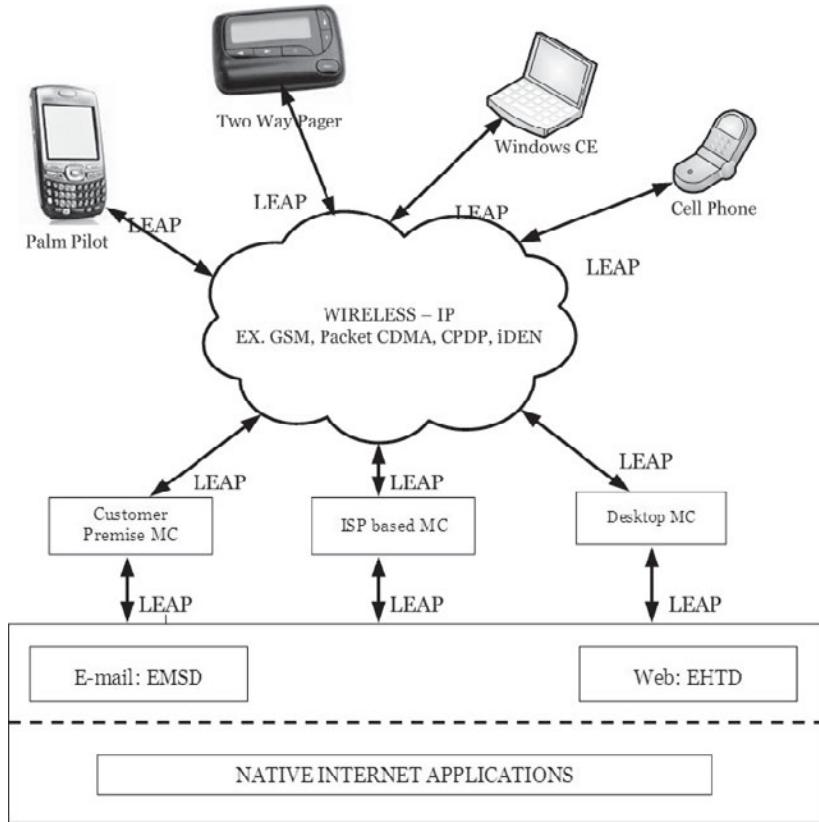
- Message integrity: Added a message integrity protocol to prevent tampering that can be implemented in software
- IV selection and reuse: Changed the rules of IV selection, and IV is reused as a replay counter
- Per-packet key mixing: Changes the encryption key for every frame
- IV size: Increased the size of IV to avoid ever reusing the same IV
- Key management: Added a mechanism to distribute and change the broadcast keys

## LEAP: The Lightweight Extensible Authentication Protocol

The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary, closed solution that offers user-name/password-based authentication between a wireless client and a RADIUS server. LEAP conducts mutual authentication. It is used with the IEEE 802.1x standard for LAN port access control. Its key points include the following:

- It provides assurance to the client that the access point is authorized.
- It employs per-session keys that need to be changed regularly.
  - This makes the collection of pads or weak IVs more difficult.
  - The secret key can be changed before the collection is complete.
- The user is authenticated, instead of the hardware.
  - MAC address access control lists are not needed.
- LEAP requires an authentication server (RADIUS) to support the access points.
- It is still vulnerable to dictionary attacks.

Figure 1-3 is a diagram of LEAP.



**Figure 1-3** LEAP provides higher security than WEP.

### **LEAP Attack Tool: ASLEAP**

ASLEAP, a tool for attacking LEAP networks, features the following:

- Actively deauthenticates users on LEAP networks, forcing them to reauthenticate
- Deauthenticates only users who have not already been seen; does not waste time on users who are not running LEAP
- Can read from stored libpcap files or AiroPeek NX files (1.X or 2.X files)
- Uses a dynamic database table and index to make lookups on large files very quickly
- Reduces the worst-case search time to .0015% as opposed to lookups in a flat file
- Can write the LEAP exchange information to a libpcap file in order to capture LEAP credentials with a device short on disk space (like an iPaq). It can then process the LEAP credentials stored in the libpcap file on a system with more storage resources.

ASLEAP works as follows:

1. Scans the 802.11 packets by putting the wireless interface in RFMON mode
2. Hops channels to look for targets (WLAN networks that use LEAP)
3. Deauthenticates the users on LEAP networks, forcing them to reauthenticate by providing their user-names and passwords
4. Records the LEAP exchange information to a libcap file
5. Analyzes the information captured offline and compares it with values in the dictionary to guess the password

---

## **Hacking Methods**

### **Techniques to Detect Open Wireless Networks**

- Warwalking: walking around to look for open wireless networks.
- Wardriving: driving through a neighborhood with a wireless-enabled notebook computer, mapping houses and businesses that have wireless access points.
- Warflying: involves flying around in an aircraft looking for open wireless networks.
- Warchalking: This term comes from whackers who use chalk to place a special symbol on a sidewalk or another surface to indicate a nearby wireless network that offers Internet access. Some warchalking symbols are shown in Figure 1-4.

### **Steps for Hacking Wireless Networks**

When hacking wireless networks, whackers will usually follow these five steps.

#### **Step 1: Find Networks to Attack**

An attacker first uses a tool like Network Stumbler while driving around to map out active wireless networks. The attacker locates a strong signal for the target WLAN. Network Stumbler not only has the ability to monitor all active networks in the area, but it also integrates with a GPS to map APs.

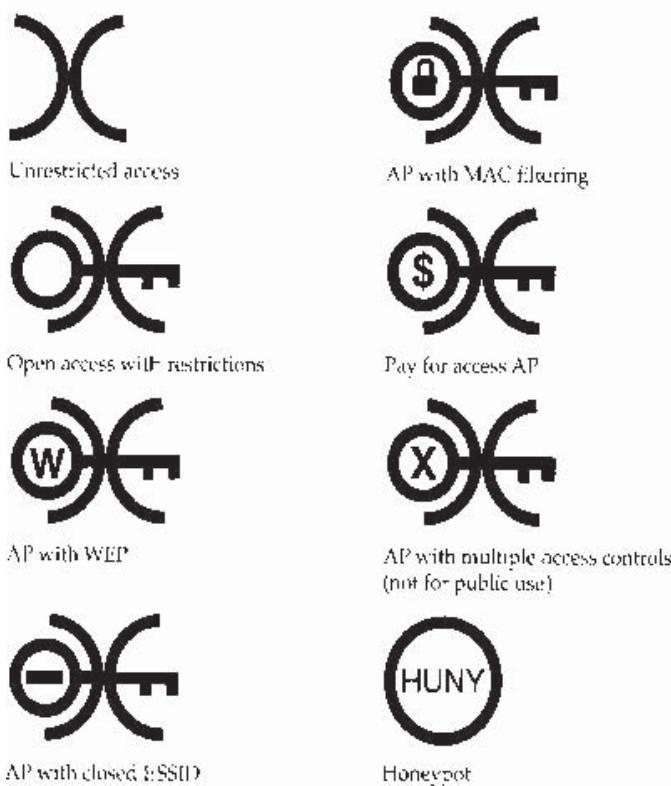
In addition to a notebook PC running Network Stumbler, networks can be found using the following devices:

- Handheld PC running MiniStumbler
- Passive scanners such as Kismet or KisMAC
- Active beacon scanners like MacStumbler or iStumbler

#### **Step 2: Choose the Network to Attack**

Network Stumbler or Kismet will tell the attacker how a network is encrypted, if at all, which will help in determining which network to attack.

### Proposed New Signs



**Figure 1-4** These are some more warchalking symbols.

### Step 3: Analyze the Network

Network Stumbler will tell the attacker various information regarding the network, such as its SSID and authentication method.

### Step 4: Crack the WEP Key

The attacker sets the NIC drivers to monitor mode. The attacker captures packets with the Airodump tool. Airodump quickly lists the available network with their SSIDs and starts capturing packets. After a few hours of the Airodump session, the Aircrack tool can determine the WEP key.

### Step 5: Sniff the Network

Once the WEP key is cracked and the NIC is configured appropriately, the attacker is assigned an IP and can access the WLAN. The attacker can listen to traffic using the Wireshark tool and look for plaintext protocols like FTP, POP, and Telnet.

### Super Bluetooth Hack

Super Bluetooth Hack is a mobile application allowing an attacker to gain access to a victim's phone via Bluetooth. The hack is shown in Figure 1-5. Using the tool, a hacker can do the following:

- Initiate and end voice calls
- Switch off the phone
- Restore factory settings
- Read saved messages
- Read contacts



**Figure 1-5** Using Super Bluetooth Hack, an attacker can gain control of a victim's cell phone.

- Change profiles
- Play ringtones
- Change ringing volume

## Man-In-The-Middle Attack (MITM)

There are two types of man-in-the-middle attacks: eavesdropping and manipulation.

Eavesdropping is easy in a wireless network because there is no physical medium used to communicate. An attacker who is in an area near the wireless network can receive radio waves on the wireless network without much effort. The entire data frame sent across the network can be examined in real time or stored for later assessment.

In order to prevent whackers from getting sensitive information, several layers of encryption should be implemented. If a security mechanism such as IPSec, SSH, or SSL is not used for transmission, the transmitted data is available to anyone.

WEP can be cracked with tools freely available on the Internet. Accessing e-mail using POP or IMAP protocols is risky because these protocols can send e-mail over a wireless network without any form of extra encryption. A determined whacker can potentially log gigabytes of WEP-protected traffic in an effort to postprocess the data and break the protection.

Manipulation is a higher level of attack than eavesdropping. Manipulation occurs on a wireless link when an attacker is able to receive the victim's encrypted data, manipulate it, and retransmit the changed data to the victim. In addition, an attacker can intercept packets with encrypted data and change the destination address in order to forward these packets across the Internet.

## Denial-Of-Service Attacks

Denial-of-service (DoS) attacks at the application and transport layers are primarily the same. The possibility of DoS attacks on wireless networks is greater due to the relationship of the physical, data link, and network layers.

Wireless DoS attacks are divided into three types: physical, data link, and network.

## **Physical DoS Attacks**

To conduct a physical DoS attack on a wired network, close proximity to the victim's network is required. However, this is not the case with a wireless network, since attackers can launch attacks from great distances.

It is easy and inexpensive to construct a device that produces a lot of noise at 2.4 GHz. In fact, there are several commercial devices available today that can bring down a wireless network with ease. Many 2.4 GHz cordless phones available on the market have the capability of disrupting an 802.11b network. A cordless phone can be used to induce a noise that drops the signal-to-noise ratio sufficiently to bring down a wireless LAN.

If there is interference in a particular band due to the crowding of signals, there is a good chance that a wireless network is down somewhere. If the attacker is able to produce sufficient RF noise to reduce the signal-to-noise ratio to a level where it becomes unusable, devices within range of the noise will go offline.

An attacker attempting a physical DoS attack can also use large-scale Bluetooth deployments.

## **Data-Link DoS Attacks**

Since the data-link layer is so accessible, DoS attacks can be carried out easily. The attacker who is preparing for a DoS attack at this layer can ignore WEP being turned on, as it will not prevent the attack.

In addition, with WEP turned off, the attacker has total access to manipulate associations among stations and access points to terminate access to the network. If the victim's network is not using WEP authentication, it is vulnerable to spoofed APs. By spoofing the AP, the attacker can block traffic from the victim's network.

If an AP is improperly using antenna diversity, an attacker can deny access to clients associated with the AP. Antenna diversity is a method in which a single radio utilizes multiple antennas to reduce multipath fade. If these antennas do not cover the same region, an attacker can deny service to associated stations by taking advantage of the improper setup.

## **Network DoS Attacks**

The 802.11 network is a shared medium, allowing an attacker to reject the affected access point that users access by flooding network traffic. If the network allows any unauthorized user on the network, it is more vulnerable to a network-layer DoS attack. For instance, an attacker can generate a ping (ICMP) to flood the base station (BS). Because the speed on 802.11 networks is relatively slow, a network DoS malfunction may accidentally occur due to the transfer of large files or the running of applications that require more than the allotted bandwidth.

## **Hijacking and Modifying a Wireless Network**

Numerous techniques are available for an attacker to hijack a wireless network or session. Unlike some attacks, network and security administrators may be unable to distinguish between the hijacker and a legitimate user. Many tools are available to network hijackers. These tools are based on basic implementation issues within almost every network device available today.

As TCP/IP packets go through switches, routers, and APs, each device looks at the destination IP address and compares it with the IP addresses it knows to be local. If the address is not in the table, the device hands the packet off to its default gateway. This table is used to coordinate the IP address with the MAC addresses that are known to be local to the device. In many situations this list is a dynamic one, built up from traffic passing through the device and through Address Resolution Protocol (ARP) notifications from new devices joining the network.

There is no authentication or verification that the request the device received is valid. Thus, a malicious user is able to send messages to routing devices and APs stating that his or her MAC address is associated with a known IP address. From then on, all traffic that goes through that router destined for the hijacked IP address will be handed off to the hacker's machine. If the attacker spoofs as the default gateway or a specific host on the network, all machines trying to get to the network or the spoofed machine will connect to the attacker's machine instead of their intended target. The attacker can use this information only to identify passwords and other necessary information and then route the rest of the traffic to the intended recipients. The end users will have no idea that this man in the middle has intercepted their communications, compromising their passwords and information.

---

## **Cracking WEP**

WEP can be cracked using either passive attacks or active attacks.

Passive attacks compromise the confidentiality of the network. The semipassive approach makes this more practical, but it needs some time and space to implement. The presence of the attacker does not change traffic until WEP has been cracked.

Active attacks compromise the integrity and availability of the network. They need less time and space compared to passive attacks. Active attacks increase the risk of being detected, but are more effective. If an active attack is reasonable, and the risk of detection is disregarded, the goal is to stimulate traffic to collect more pads (some attacks require only one pad) and use weak IVs.

## Automated WEP Crackers

There are several automated WEP cracking programs, including the following:

- AiroPeek
- WEPCrack
- AirSnort
- Network Stumbler
- iStumbler
- KisMAC
- Kismet

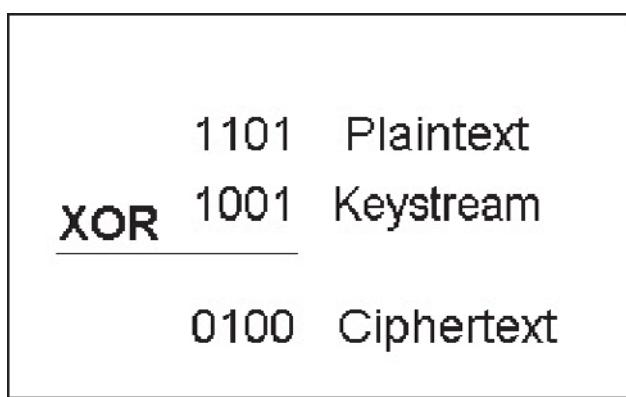
## Pad Collection Attacks

Pads are the numbers used in the WEP encryption sequence. A pad collection attack is a semipassive attack. It collects a set of pads and then decrypts any packet for which a pad is present. It works with 64-bit or 128-bit encryption. It requires traffic flowing across the network. It can spread the attack over time in order to slow down possible detection.

- There should be a separate pad for each encrypted packet that is transferred between the access point and a station.
- It is possible to make a table and skip the RC4 step by mapping pads to IVs.
  - The stream is never longer than 1,500 bytes (the maximum Ethernet frame size).
  - The 24-bit IV provides 16,777,216 ( $256^3$ ) possible streams, so all the pads can fit inside 25,165,824,000 bytes (23.4 GB).
- The WEP key is not needed.
  - Once a table is completed, it is as good as having the WEP key.

## XOR Encryption

In XOR encryption, plaintext is XORed with the keystream. If either the plaintext or keystream bit is a 1, then a 1 is returned. If neither bit is a 1 or both bits are 1, then a 0 is returned. Figure 1-6 depicts XOR encryption.



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

**Figure 1-6** In XOR encryption, the ciphertext is generated by XORing the plaintext with the keystream.

## Stream Cipher

Stream cipher is the process of encrypting text in which the plaintext digits are encrypted one at a time, and the cryptographic key and algorithm are applied to each binary digit in a data stream. The encryption of each digit depends on the current state.

Given an initialization vector (IV) and secret key, the stream of bytes (pad) produced is always the same. Knowing all pads is the same as knowing the key.

The following are the applications of stream cipher to WEP:

- The pad is produced from the combination of the IV and the WEP key passed through RC4.
- If all the pads are known, then it is similar to knowing the 40-bit or 104-bit secret.
- Weak IVs disclose additional information about the secret.

## WEP Cracking Tools

### Aircrack

Aircrack recovers 40-bit to 104-bit WEP keys after the required number of encrypted packets is gathered. It is shown in Figure 1-7.

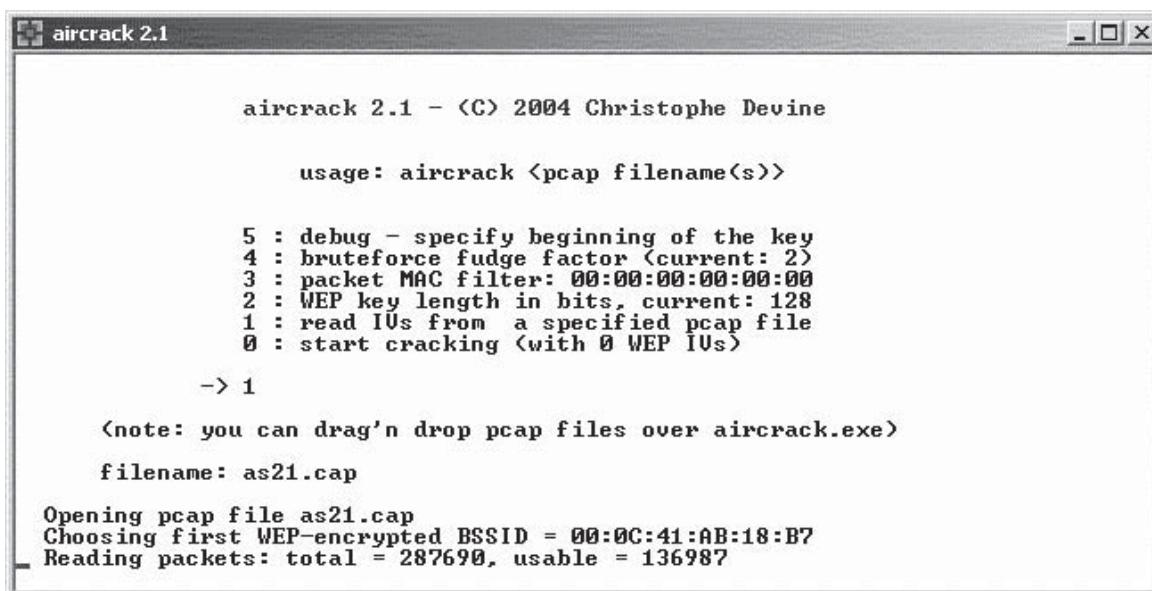
Aircrack traps FMS attacks. In addition, Aircrack has the capability of implementing a new type of attack called Korek.

The Fluhrer Mantin Shamir (FMS) attack can capture encrypted traffic in bulk and, with a little CPU power, crack the key using a probabilistic algorithm. The cracking of keys takes places linearly. A 128-bit key takes a longer time to crack than a 64-bit key.

Aircrack supports all versions of Windows, Linux, and Mac OS.

### AirPcap

AirPcap enables troubleshooting tools like Wireshark (formerly Ethereal) and WinDump to provide information about wireless protocols and radio signals. AirPcap comes as a USB 2.0 adapter and has been fully integrated with WinPcap and Wireshark. It captures and analyzes 802.11b/g wireless traffic including control frames, management frames, and power information. AirPcap's control panel can be seen in Figure 1-8.



```

aircrack 2.1 - <C> 2004 Christophe Devine

usage: aircrack <pcap filename(s)>

      5 : debug - specify beginning of the key
      4 : bruteforce fudge factor (current: 2)
      3 : packet MAC filter: 00:00:00:00:00:00
      2 : WEP key length in bits, current: 128
      1 : read IVs from a specified pcap file
      0 : start cracking (with 0 WEP IVs)

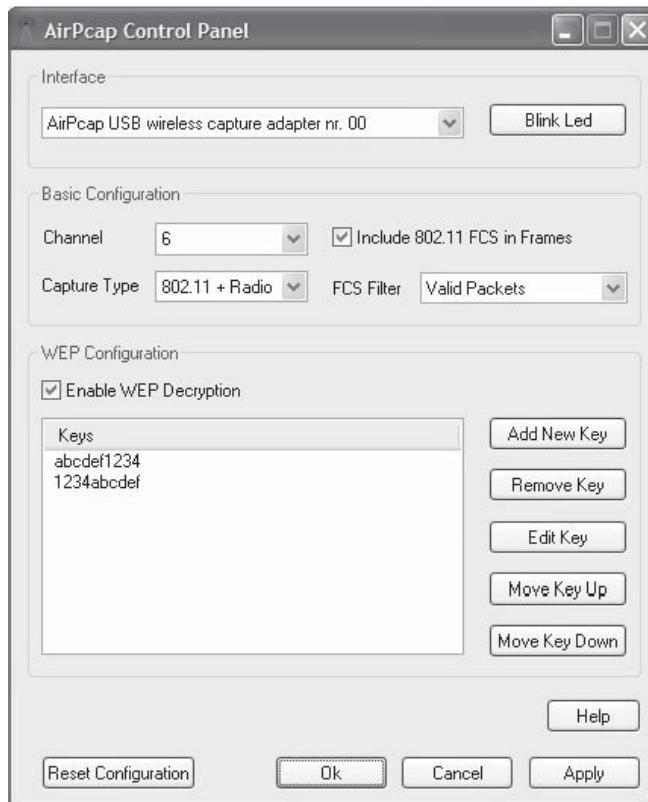
-> 1

<note: you can drag'n drop pcap files over aircrack.exe>
filename: as21.cap

Opening pcap file as21.cap
Choosing first WEP-encrypted BSSID = 00:0C:41:AB:18:B7
Reading packets: total = 287690, usable = 136987

```

**Figure 1-7** Aircrack can crack WEP, WPA, and WPA-2 keys after sniffing enough packets.



**Figure 1-8** AirPcap is a USB wireless capture device.

### Cain & Abel

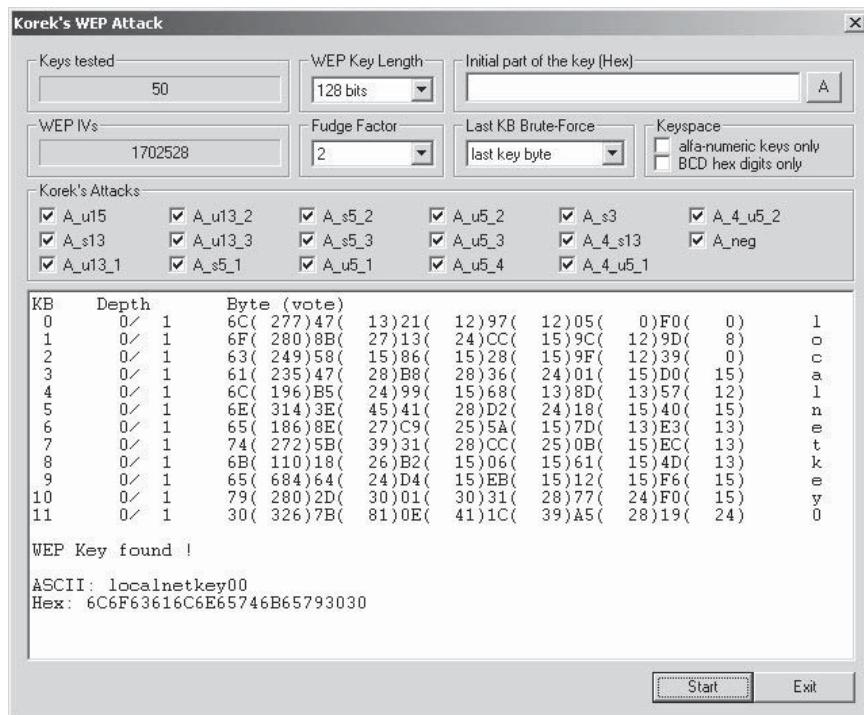
Cain & Abel is a password recovery tool for Windows. It allows easy recovery of several types of passwords through the following methods:

- Sniffing the network
- Cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks
- Recording VoIP conversations
- Decoding scrambled passwords
- Recovering wireless network keys
- Revealing password boxes
- Uncovering cached passwords
- Analyzing routing protocols

It covers some security aspects and weaknesses intrinsic in protocols' standards, authentication methods, and caching mechanisms. Its main purpose is the simplified recovery of passwords and credentials from various sources.

The following are some of the features of Cain & Abel:

- 802.11 Capture Files Decoder can decode wireless capture files from Wireshark and/or Airodump-ng containing WEP or WPA-PSK encrypted 802.11 frames.
- Password decoders can be used to immediately decode encrypted passwords from several sources such as the Windows Protected Store, the Credential Manager, standard edit boxes, LSA secrets, passwords from SQL Enterprise Manager, Windows Mail, dial-up, Remote Desktop profiles, and the Windows Wireless Configuration service.
- WEP Attack, shown in Figure 1-9, covers the same functionality as Aircrack and can quickly recover 64-bit and 128-bit WEP keys if enough unique WEP IVs are available.



**Figure 1-9** Cain & Abel's WEP Attack has the same functionality as Aircrack.

- Wireless Scanner detects Wireless Local Area Networks (WLANS) using 802.11x.
- Wireless Zero Configuration Password Dumper enables the recovery of wireless keys stored by Windows's Wireless Zero Configuration Service.

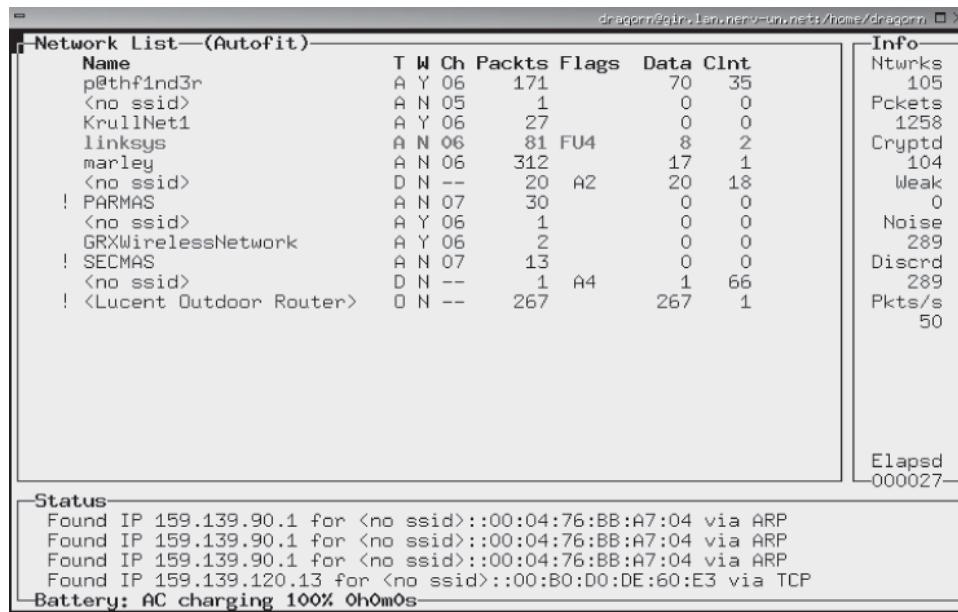
## Kismet

Kismet is a wireless network detector, sniffer, and intrusion detection system. It works with any wireless card that supports raw monitoring (RFMON) mode, and can sniff 802.11b, 802.11a, 802.11n, and 802.11g traffic. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting and decloaking hidden networks, and inferring the presence of nonbeaconing networks via data traffic.

Kismet's features include the following:

- Ethereal/Tcpdump-compatible data logging
- AirSnort-compatible weak-IV packet logging
- Network IP range detection
- Built-in channel hopping and multicard split-channel hopping
- Hidden network SSID decloaking
- Graphical mapping of networks
- Client/server architecture allows multiple clients to view a single Kismet server simultaneously
- Manufacturer and model identification of access points and clients
- Detection of known default access point configurations
- Runtime decoding of WEP packets for known networks
- Named pipe output for integration with other tools, such as an IDS like Snort
- Multiplexing of multiple simultaneous capture sources on a single Kismet instance
- Distributed remote drone sniffing
- XML output

Kismet is shown in Figure 1-10.



**Figure 1-10** Kismet can detect and decloak wireless networks.

## Rogue Access Points

Unauthorized access points can allow anyone with an 802.11-equipped device onto the network. With the help of wireless sniffing tools, access points for the authorized Media Access Control (MAC) address, vendor names, or security configurations can be determined. The attacker can then create a list of the MAC addresses of authorized access points on the LAN and cross-check this list with the list of MAC addresses found by sniffing.

An access point should be considered a rogue if it looks suspicious. It can possibly be located by using a simple technique that involves walking with a wireless-access-point-sniffing device in the direction the signal strength of the access point's beacon increases.

Sometimes a rogue access point may be an active access point that is not connected to the network, but these access points are not security issues. When an access point is found that interfaces with the network, it must be shut off immediately. Using a centralized network-monitoring device attached to the wired network, workstations and individual users that use multiple systems can be tracked easily. Centralized network-monitoring devices are used to monitor networks.

There are two basic methods for locating unauthorized access points: requesting a beacon and sniffing the air.

### Requesting a Beacon

When an 802.11b/g-compliant network card transmits a packet to request a beacon, all the access points in the vicinity broadcast their availability via SSID announcement. This method is effective because current traffic is not required.

The problem with this method is that the access point must be configured to respond to these beacon requests; however, many organizations turn this option off. For this reason, this method is not effective at finding all wireless access points. Some users, however, fail to turn this feature off while deploying access points. Also, some home wireless access points do not have the option to turn off SSID broadcasting.

### Sniffing the Air

Another method of detecting rogue access points is by using wireless sniffing tools. In order to passively capture packets from the air, the receiver on the wireless card has to be turned on in promiscuous mode. The receiver records the information of the sniffed packet, allowing the attacker to deconstruct the packets in order to find a way to access the network.

A precise channel should be selected for sniffing the wireless network. 802.11b operates on 11 channels, and it is difficult to constantly switch between channels to monitor packets. For all practical purposes, because of frequency overlapping, the only effective channels that can be used without interference from other access points are 1, 6, and 11. It should be noted that while there are 11 assigned channels within the United States, most of Europe can use channels 1 through 13, while Japan uses only channel 14.

In order to sniff the wireless network, there must be traffic on the network. Technically, it is feasible to detect an access point by sniffing traffic, but it is not practical. If the network does not have users who use unauthorized access points, there will be no traffic to watch. In addition, if the access point is near but not in use, the sniffer will not find it. Sniffing is a useful method of finding out who is using a wireless access point after it has been identified.

## Tools to Generate Rogue Access Points

### *Fakeap*

Black Alchemy's Fakeap generates thousands of counterfeit 802.11b access points via beaconing in order to confuse attackers. Fakeap runs on Linux and BSD versions of UNIX. It is pictured in Figure 1-11.

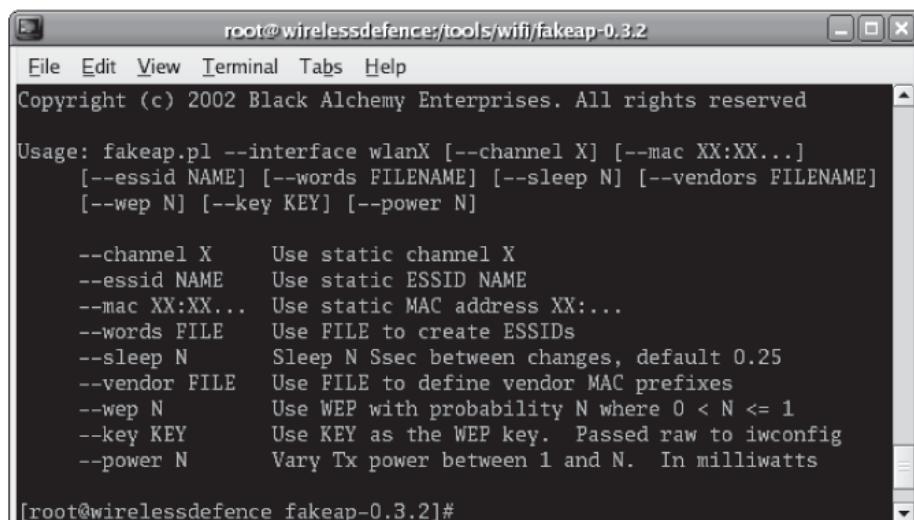
### *Network Stumbler*

Network Stumbler provides an easy method for enumerating wireless networks. It transmits connection requests to all the listening access points with an SSID. The APs respond by sending their own SSID. Note that NetStumbler is not a passive sniffer; this means that the traffic handled by it is visible on the victim's network.

When Network Stumbler is launched, it starts a capture file and starts searching for access points. There are two panes on Network Stumbler's display, shown in Figure 1-12. The top one shows the MAC address of the AP, WEP status, SSID, signal strength, and coordinates in case a GPS unit is attached to the computer. The bottom pane has three views: channels, SSID, and filters.

### *MiniStumbler*

MiniStumbler, shown in Figure 1-13 is a Windows Mobile application that listens for broadcasts and captures network information. It provides important information, including whether or not the network is encrypted, the MAC address of the AP or wireless device, the SSID, the AP name, the channel used, the vendor, whether it is an AP or a peer device, and signal strength. MiniStumbler not only detects the different WLAN networks, but also their longitude and latitude if a GPS device is attached.



```
root@wirelessdefence:/tools/wifi/fakeap-0.3.2
File Edit View Terminal Tabs Help
Copyright (c) 2002 Black Alchemy Enterprises. All rights reserved

Usage: fakeap.pl --interface wlanX [--channel X] [--mac XX:XX...]
      [--essid NAME] [--words FILENAME] [--sleep N] [--vendors FILENAME]
      [--wep N] [--key KEY] [--power N]

      --channel X      Use static channel X
      --essid NAME    Use static ESSID NAME
      --mac XX:XX...   Use static MAC address XX:...
      --words FILE    Use FILE to create ESSIDs
      --sleep N       Sleep N Ssec between changes, default 0.25
      --vendor FILE   Use FILE to define vendor MAC prefixes
      --wep N         Use WEP with probability N where 0 < N <= 1
      --key KEY       Use KEY as the WEP key. Passed raw to iwconfig
      --power N       Vary Tx power between 1 and N. In milliwatts

[root@wirelessdefence fakeap-0.3.2]#
```

Figure 1-11 Fakeap generates fake access points.

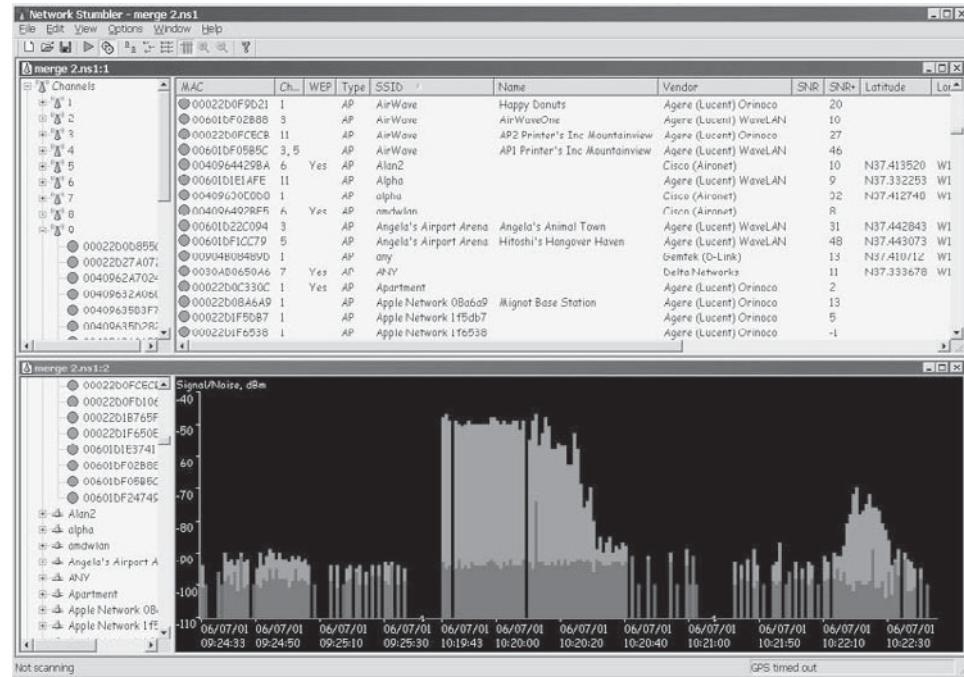


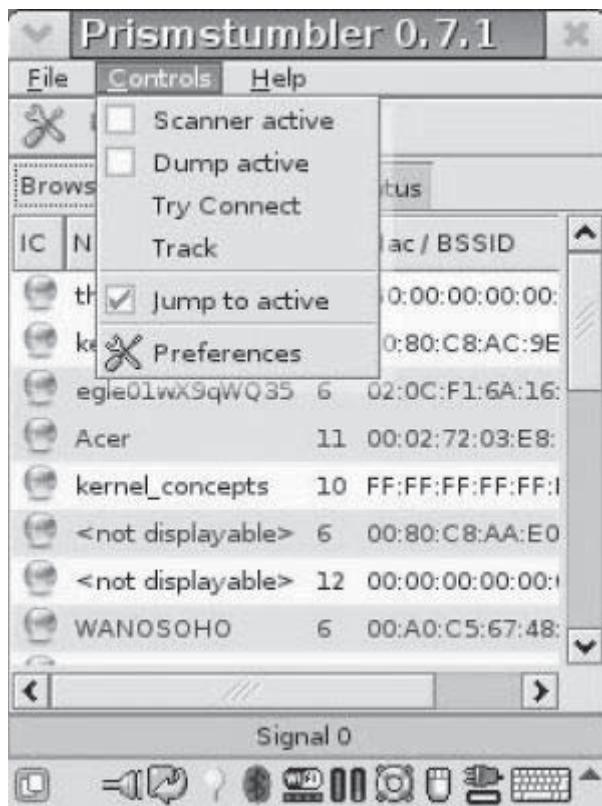
Figure 1-12 Network Stumbler is a high-level WLAN scanner.



Figure 1-13 MiniStumbler provides many of Network Stumbler's features to Windows Mobile.

## Cloaked Access Point

Wireless network administrators cloak their access points by putting them in stealth mode. Cloaked access points are not detected by active scanners like Network Stumbler. The only way to detect a cloaked access point is by using passive scanners like Kismet or AirSnort.



**Figure 1-14** Prismstumbler scans for beacon frames.

## Scanning Tools

### Prismstumbler

Prismstumbler, shown in Figure 1-14, is a wireless LAN (WLAN) tool that scans for beacon frames from access points. It operates by switching channels frequently and monitoring frames received on the selected channel. The auto-homing mode of a Lucent/Orinco card can be used for this application.

For doing security assessments in WLANs, the AirSnort package is required, which in turn requires a Prism2-based card. Prismstumbler was created to simplify the process of having to swap PC Cards.

Prismstumbler also finds private networks. Since the method used is “receive only,” additional networks with weaker signals can also be found by Prismstumbler.

### MacStumbler

MacStumbler, shown in Figure 1-15, is the Mac OS equivalent of Network Stumbler. It requires an Apple Airport Card and Mac OS 10.1 or greater; it does not currently support any kind of PCMCIA or USB wireless device.

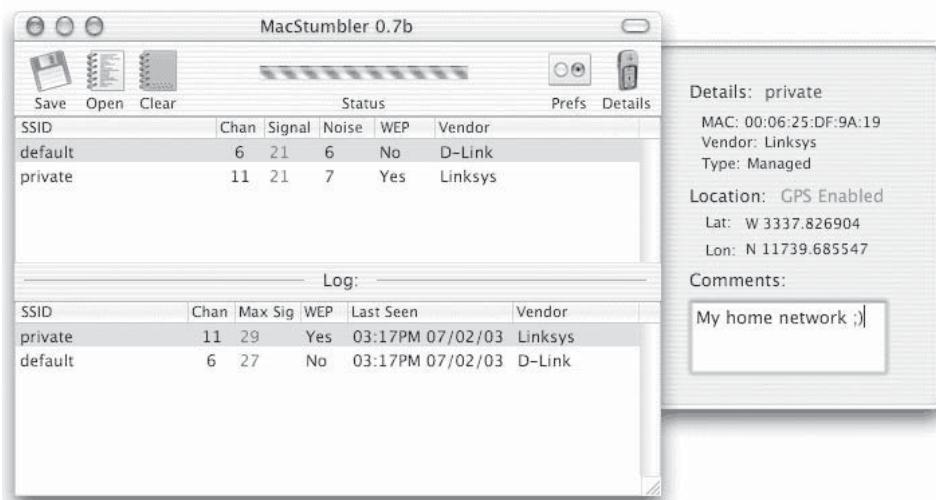
For wardriving, MacStumbler requires a NMEA (National Marine Electronics Association)-compatible GPS device, which means that the GPS must have a serial connection or a USB port. NMEA is the standard protocol used by GPS receivers to transmit data. MacStumbler has a text-to-speech option, so the ESSIDs (extended service set identifiers) of networks are read out as they appear.

### Mognet

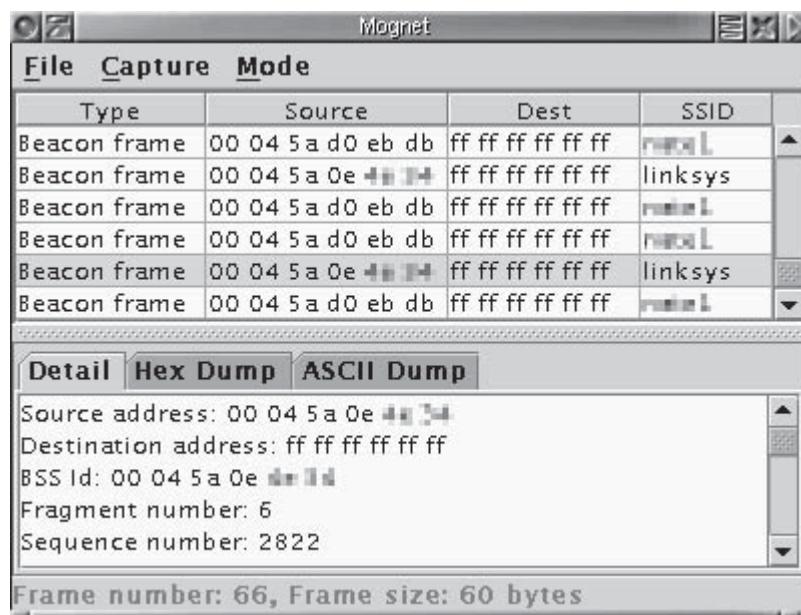
Mognet is an 802.11b protocol analyzer/sniffer written in Java. It is available free under the GNU General Public License. It is a simple, lightweight program, shown in Figure 1-16.

Its features include the following:

- Real-time capture output
- Support for all 802.11 generic and frame-specific headers



**Figure 1-15** MacStumbler is the Mac OS equivalent of Network Stumbler.



**Figure 1-16** Mognet is a free 802.11b analyzer/sniffer.

- Raw/hex/ASCII views for any frame
- Text-mode capture for GUI-less devices
- Loading/saving capture sessions in Ethereal/libpcap/Tcpdump format

## WaveStumbler

WaveStumbler is a console-based 802.11-network mapper for Linux. It reports basic AP information such as channel, WEP, ESSID, and MAC.

WaveStumbler consists of a patch against the kernel driver orinoco.c. This makes it possible to send the output of the scan command to the driver via the /proc/hermes/ethX/cmdu file. The answer is sent back via a netlink socket. WaveStumbler listens to this socket and displays the output data on a console.

## NetChaser

NetChaser requires a Palm Tungsten C handheld computer in order to work. It displays signal strength, access point SSID, WEP status, loss-of-signal time display, current battery voltage, and time.

It also displays access point information including the AP MAC address, AP SSID, signal strength, channel, loss-of-signal time and date display, and latitude and longitude of strongest signal. NetChaser is shown in Figure 1-17.

## Wavemon

Wavemon is a monitor for wireless devices. It monitors the signal and noise levels, packet statistics, device configuration, and network parameters of wireless network hardware. This tool is not designed to assess performance over time. It gives a rolling report on how the wireless connection is functioning.

Its features include the following:

- Overview screen, displaying all important information, such as device configuration, encryption, power management parameters, and network information, at once
- Adaptive-level bar graphs for link quality, signal/noise strength, and signal-to-noise ratio
- Customizable “level alarm” feature that notifies the user of changes in signal-level strength audibly and/or visually
- Full-screen level histogram displaying signal/noise levels and signal-to-noise ratio

## Wireless Security Auditor (WSA)

Wireless Security Advisor, shown in Figure 1-18 is intended for less experienced users who want a way to verify the security configuration of their networks without having to understand any of the details of the 802.11 protocols. It features the following:

- Tracks beacon packets to find all access points
- Determines SSID and AP name
- Tracks probe packets and probe responses
- Tracks data packets

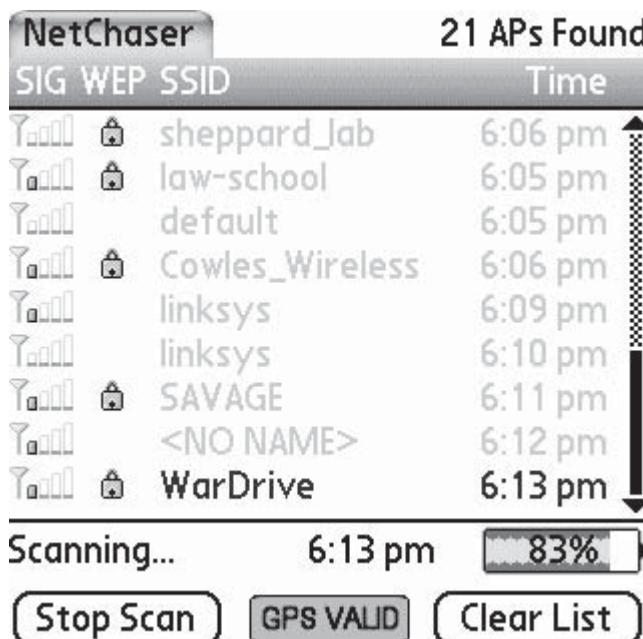


Figure 1-17 NetChaser is a scanning tool for the Palm Tungsten C.

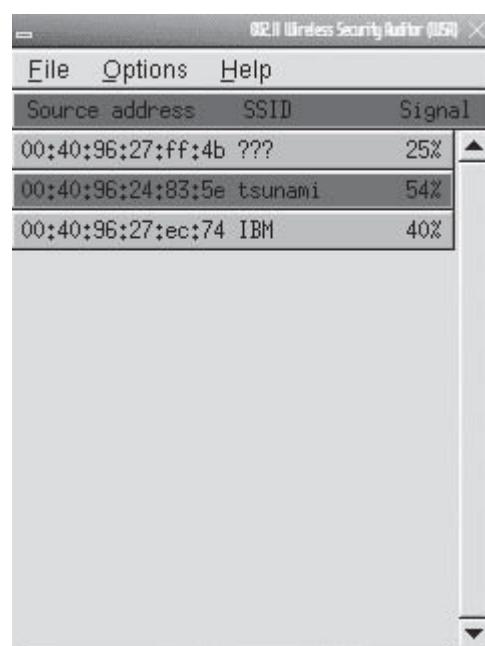


Figure 1-18 WSA is made for the average user.

```

AirTraf: 1.0.0 '02
Channel Scanning: listening using Cisco Aironet (eth1)

Activity Overview -- Detailed Breakdown
Total Networks: 2
Scan Mode: Complete
          CH  TYPE SSID           BSSID      WEP   MGMT  CTRL   DATA   CRYPT   SIGNAL
          01  AP  Command Center  0006257d8777  open   136    0     9    0  0,0
          08  AP  WaveLAN Network 00022d28dc25  open   514    0    23    0  0,0

Channel APs Packets
 01    1    145
 02    0    0
 03    0    0
 04    0    0
 05    0    0
 06    0    0
 07    0    0
 08    1    537
 09    0    0
10    0    0
11    0    0
12    0    0
13    0    0
14    0    0

-- End --

Current Status
Performing Initial Channel Scan...
Detected new network 'Command Center' (0006257d8777) on Channel 01
Detected new network 'WaveLAN Network' (00022d28dc25) on Channel 08
Initial Channel Scan Complete!
Entering Continuous Scan Mode...

Elapsed: 00:00:41

F-force new scan Up/Down/PgUp/PgDn=scroll window X=exit

```

**Figure 1-19** AirTraf is an open-source sniffer.

- Determines link encryption method
- Tracks authentication packets
- Determines authentication method
- Tracks clients
- Determines firmware versions by fingerprinting the access point's detailed behavior

## AirTraf

AirTraf is an open-source wireless sniffer that can detect and determine exactly what is being transmitted over 802.11 wireless networks. It tracks and identifies legitimate and rogue access points, keeps performance statistics on a by-user and by-protocol basis, measures the signal strength of network components, and more. AirTraf is shown in Figure 1-19.

## WifiScanner

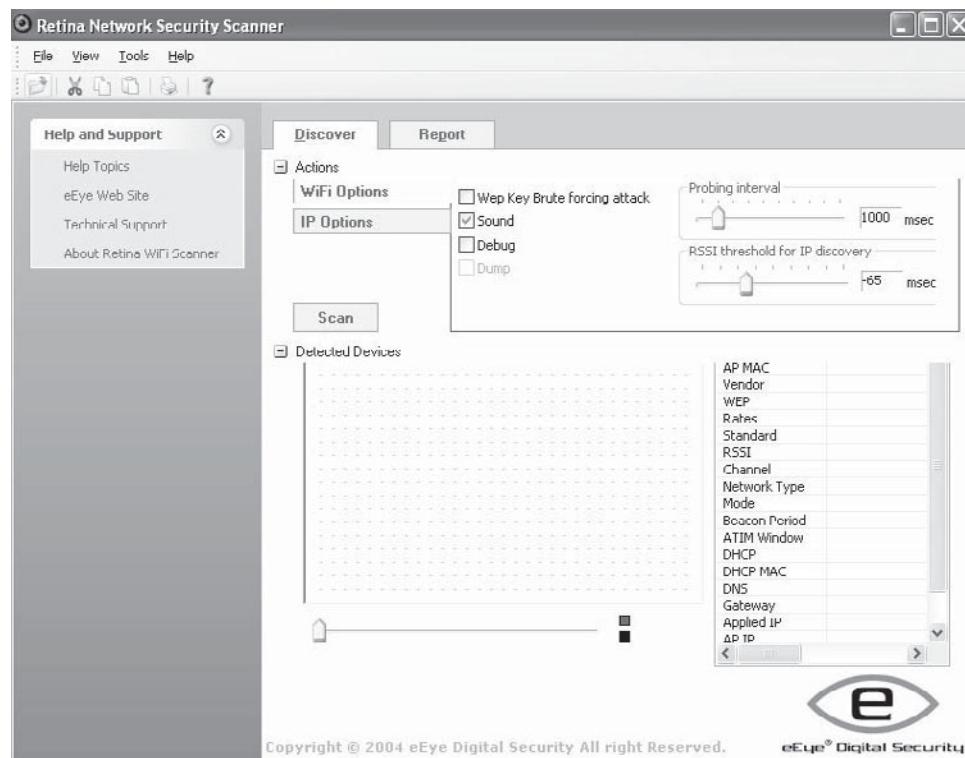
WifiScanner is a tool that has been designed to discover access points and wireless clients. It dumps the traffic in real time, and the sniffed channels can be changed. It is distributed under the GNU General Public License. It works with Cisco, Prism, prism 54g, Hermes/Orinoco, Atheros, and Centrino cards, and with the hostap and wlan-ng Linux drivers. An IDS system is integrated to detect anomalies like MAC usurpation.

## eEye Retina Network Security Scanner

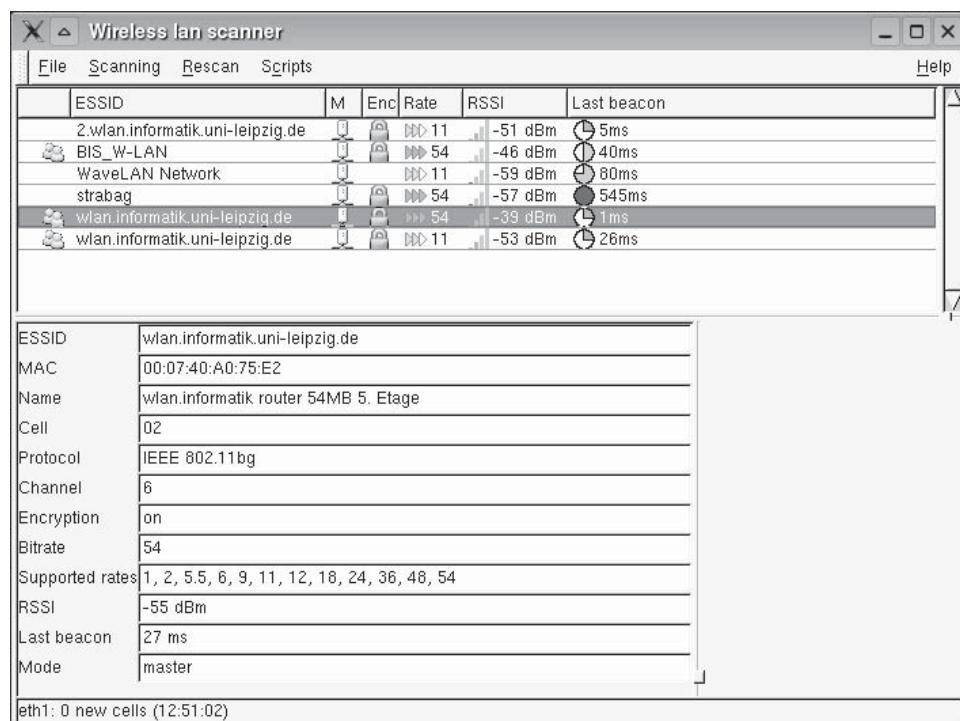
eEye Retina Network Security Scanner scans the area and detects the presence of wireless devices located within a network or connected wirelessly to the network. This tool, shown in Figure 1-20, detects rogue mobile devices and transmitting laptops.

## Wireless Lan Scanner

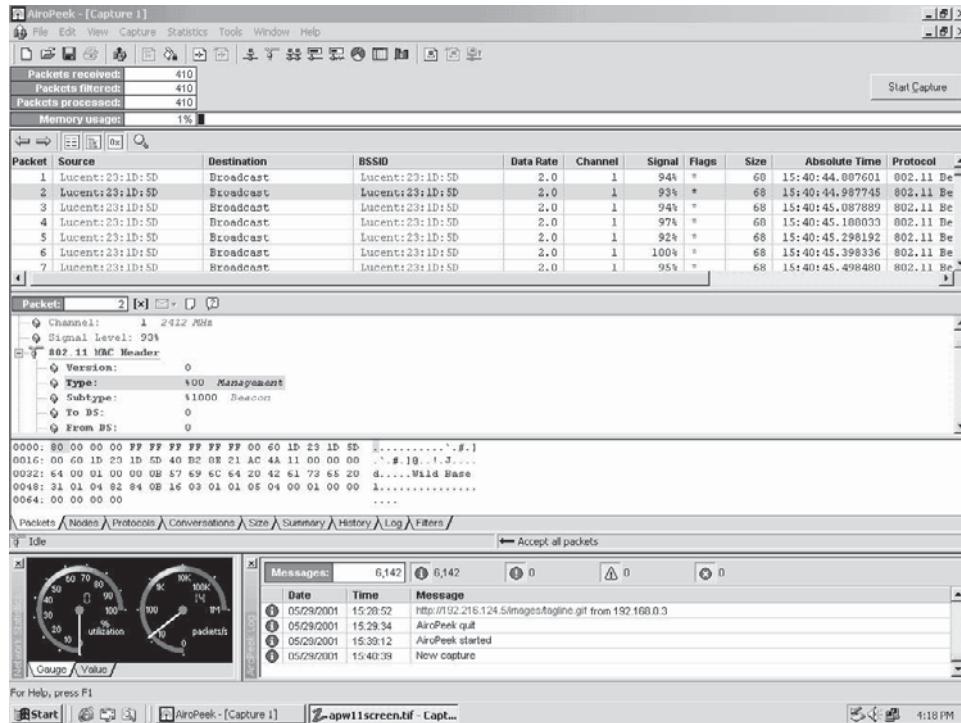
Wireless Lan Scanner, shown in Figure 1-21, lists available networks, with data such as signal strength, encryption status, and connection speed.



**Figure 1-20** eEye Retina Network Security Scanner scans the area for wireless devices.



**Figure 1-21** Wireless Lan Scanner lists available networks.



**Figure 1-22** AiroPeek captures WLAN traffic.

## Sniffing Tools

### AiroPeek NX

AiroPeek NX, shown in Figure 1-22, works by capturing traffic on a wireless LAN. It provides the tools to filter and analyze this traffic by interpreting traffic patterns, data packet contents, statistics, and protocol types.

When AiroPeek is launched the user is prompted for an adapter to use for capturing data. Highlighting the correct card and clicking OK enables AiroPeek for use. The user then selects Capture from the main menu. Most wireless traffic that passes within range of the wireless card can be captured. In case there are multiple wireless networks in the area or there is too much traffic, triggers can be used to narrow down the amount of data collected.

This tool can be used to debug the network if there are communication problems among servers, unresponsive hosts, or interfering traffic. It can also be used to determine what kind of traffic goes across the network.

### Wireshark

Wireshark is a network protocol analyzer. Shown in Figure 1-23, it allows examination of data from a live network or from a capture file on disk. It has several features, including the following:

- Rich display filter language
- Ability to view the reconstructed stream of a TCP session
- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis with rich VoIP analysis
- Captured network data can be browsed via a GUI or via the TTY-mode TShark utility
- Captured files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

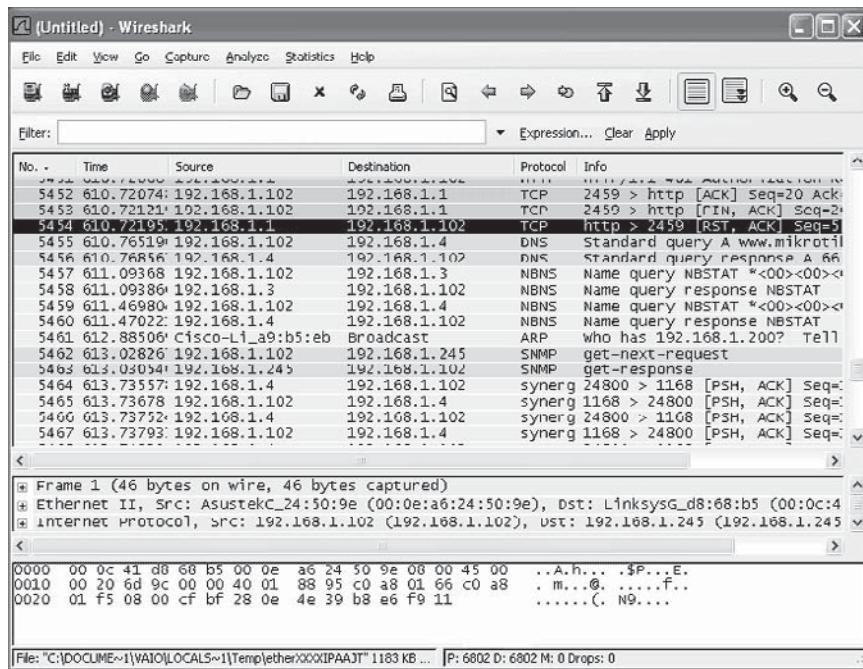


Figure 1-23 Wireshark examines data from hundreds of protocols.

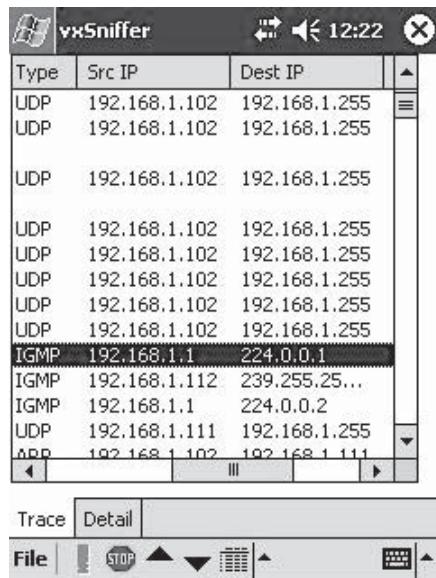


Figure 1-24 vxSniffer is a network-monitoring tool for Windows CE.

## vxSniffer

vxSniffer is a complete network-monitoring tool for Windows CE-based devices. It operates on all handheld HP 2000 HPCs and others. It is licensed software and requires an Ethernet adapter with an NDIS-compatible driver. vxSniffer is shown in Figure 1-24.



**Figure 1-25** EtherPEG creates a collage of images being transferred over the network.

## EtherPEG

EtherPEG is Macintosh software that displays GIF and JPEG images that are being sent over a network. Images that come from visited Web pages on an AirPort wireless network can also be viewed.

It works by capturing unencrypted TCP packets off the local network and collecting packets into groups based on TCP connection (determined from source IP address, destination IP address, source TCP port, and destination TCP port). It reassembles those packets in order based on TCP sequence number, and scans the resulting data for byte sequences that suggest the presence of JPEG or GIF data.

EtherPEG then displays that data in a random fashion in a large window, shown in Figure 1-25. This tool does not make any attempt to display where the images have been downloaded from or who requested them. It does not even save any local data; once the application is closed, the collected data is lost.

EtherPEG will not work if the data is encrypted using IPSec or virtual private network (VPN), products such as PGPNet, or Web Browser SSL encryption.

## AirMagnet

AirMagnet, (shown in Figure 1-26) is similar to MiniStumbler, except without the GPS option.

AirMagnet displays real-time statistics of WLANs in the area with the help of graphics and animations. AirMagnet not only displays unsecured networks, it also provides a list of possible security holes and configuration problems with WLANs in the area.

## driftnet

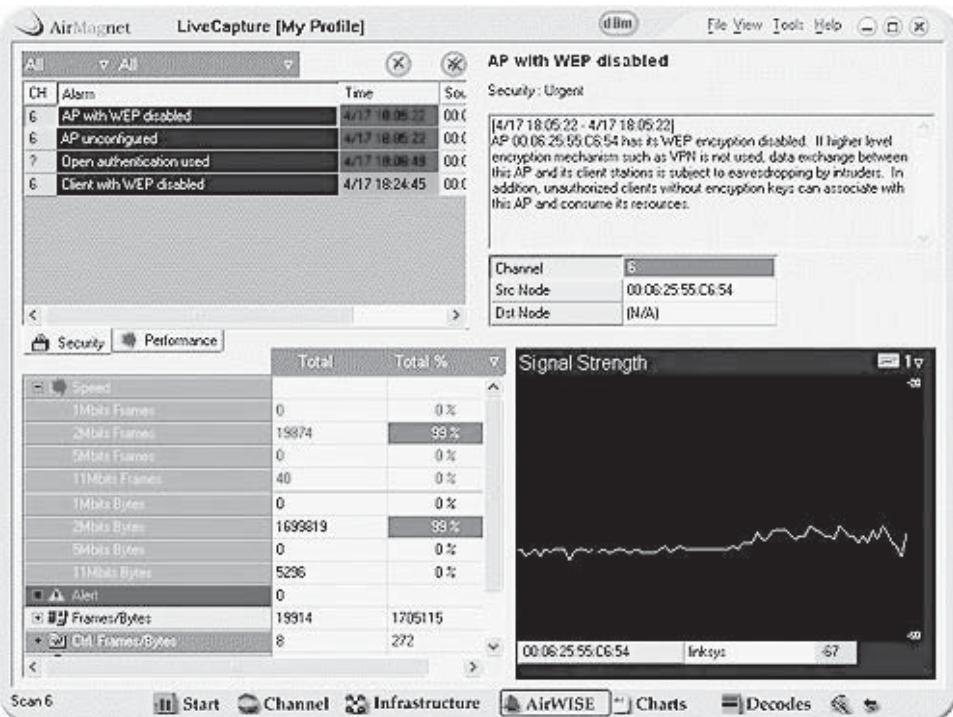
driftnet is similar to EtherPEG. It listens to network traffic, picks out images from the TCP streams it observes, and then shows them in a window, as demonstrated in Figure 1-27. driftnet also picks out MPEG audio streams from network traffic and tries to play them.

Unlike EtherPEG, driftnet can save all decoded images for later processing.

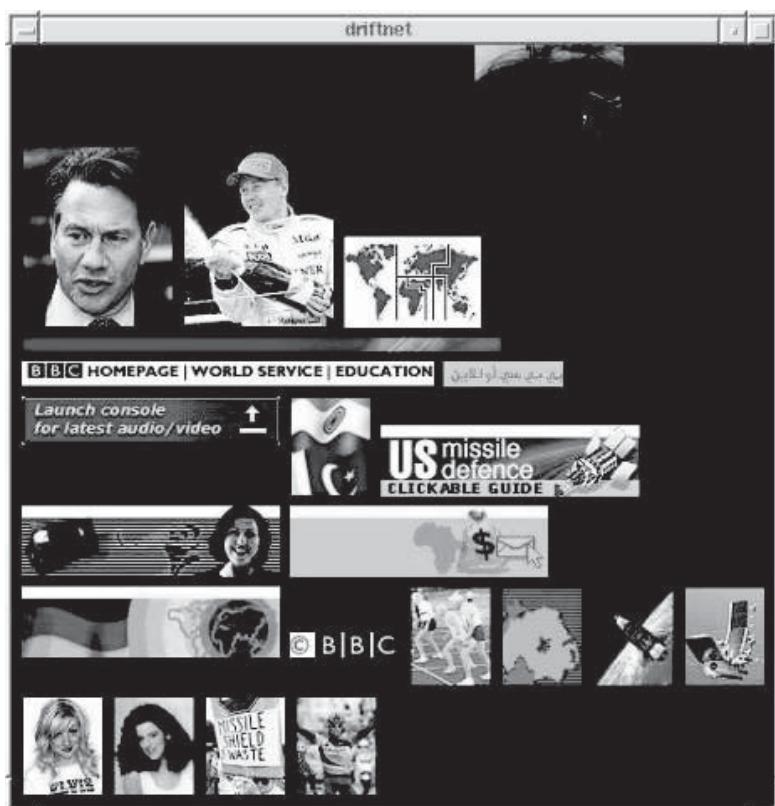
## WinDump

WinDump is a Windows version of Tcpdump, a network sniffer/analyizer for UNIX. WinDump is fully compatible with Tcpdump and can be used to watch and diagnose network traffic according to various complex rules.

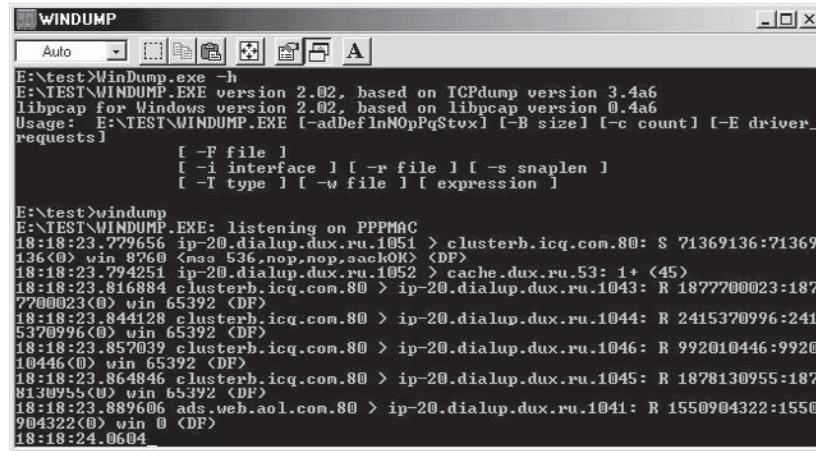
WinDump uses WinPcap, an architecture for packet capture and network analysis for the Win32 platform. It includes a kernel-level packet filter, a low-level dynamic link library (packet.dll), and a high-level and



**Figure 1-26** AirMagnet displays real-time WLAN statistics.



**Figure 1-27** driftnet, like EtherPEG, shows images being transferred over the network.



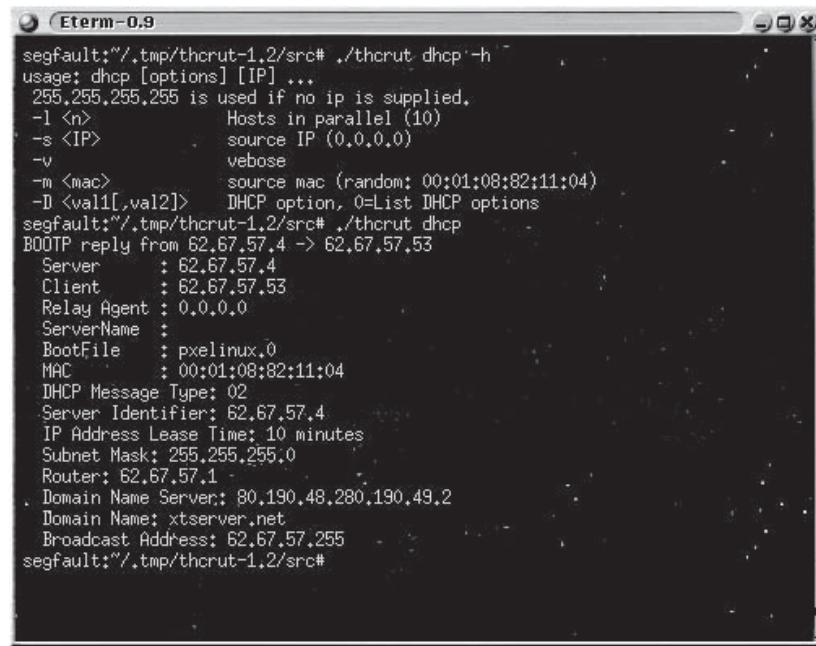
```

WINDUMP
Auto [ ] [ ] [ ] [ ] [ ] [ ] [ ] A
E:\test>WinDump.exe -h
E:\TEST\WINDUMP.EXE version 2.02, based on TCPdump version 3.4a6
libpcap for Windows version 2.02, based on libpcap version 0.4a6
Usage: E:\TEST\WINDUMP.EXE [-adDeflnMOpPgStvx] [-B size] [-c count] [-E driver_
requests]
      [-F file]
      [-i interface] [-r file] [-s snaplen]
      [-T type] [-v file] [-expression]

E:\test>windump
E:\TEST\WINDUMP.EXE: listening on PPPMAC
18:18:23.779656 ip-20.dialup.dux.ru.1051 > clusterb.icq.com.80: S 71369136:71369
136<0> win 8760 <mse 536,nop,nop,sackOK> <DF>
18:18:23.794251 ip-20.dialup.dux.ru.1052 > cache.dux.ru.53: 1+ <45>
18:18:23.816884 clusterb.icq.com.80 > ip-20.dialup.dux.ru.1043: R 1877200023:187
2700023<0> win 65392 <DF>
18:18:23.844128 clusterb.icq.com.80 > ip-20.dialup.dux.ru.1044: R 2415370996:241
5370996<0> win 65392 <DF>
18:18:23.857039 clusterb.icq.com.80 > ip-20.dialup.dux.ru.1046: R 992010446:9920
10446<0> win 65392 <DF>
18:18:23.864846 clusterb.icq.com.80 > ip-20.dialup.dux.ru.1045: R 1878130955:187
8130955<0> win 65392 <DF>
18:18:23.889606 ads.web.aol.com.80 > ip-20.dialup.dux.ru.1041: R 1550904322:1550
904322<0> win 0 <DF>
18:18:24.0604

```

**Figure 1-28** WinDump is a Windows port of Tcpdump.



```

Eterm-0.9
segfault:"/tmp/thcrut-1.2/src# ./thcrut dhcp -h"
usage: dhcp [options] [IP] ...
  255.255.255.255 is used if no ip is supplied.
  -l <n>          Hosts in parallel (10)
  -s <IP>          source IP (0.0.0.0)
  -v               verbose
  -m <mac>         source mac (random: 00:01:08:82:11:04)
  -D <val1[,val2]> DHCP option, 0=List DHCP options
segfault:"/tmp/thcrut-1.2/src# ./thcrut dhcp
BOOTP reply from 62.67.57.4 -> 62.67.57.53
  Server      : 62.67.57.4
  Client      : 62.67.57.53
  Relay Agent : 0.0.0.0
  ServerName  :
  BootFile   : pxelinux.0
  MAC        : 00:01:08:82:11:04
  DHCP Message Type: 02
  Server Identifier: 62.67.57.4
  IP Address Lease Time: 10 minutes
  Subnet Mask: 255.255.255.0
  Router: 62.67.57.1
  Domain Name Server: 80.190.48.280,190.49.2
  Domain Name: xtserver.net
  Broadcast Address: 62.67.57.255
segfault:"/tmp/thcrut-1.2/src#"

```

**Figure 1-29** THC-RUT offers a wide range of network discovery tools.

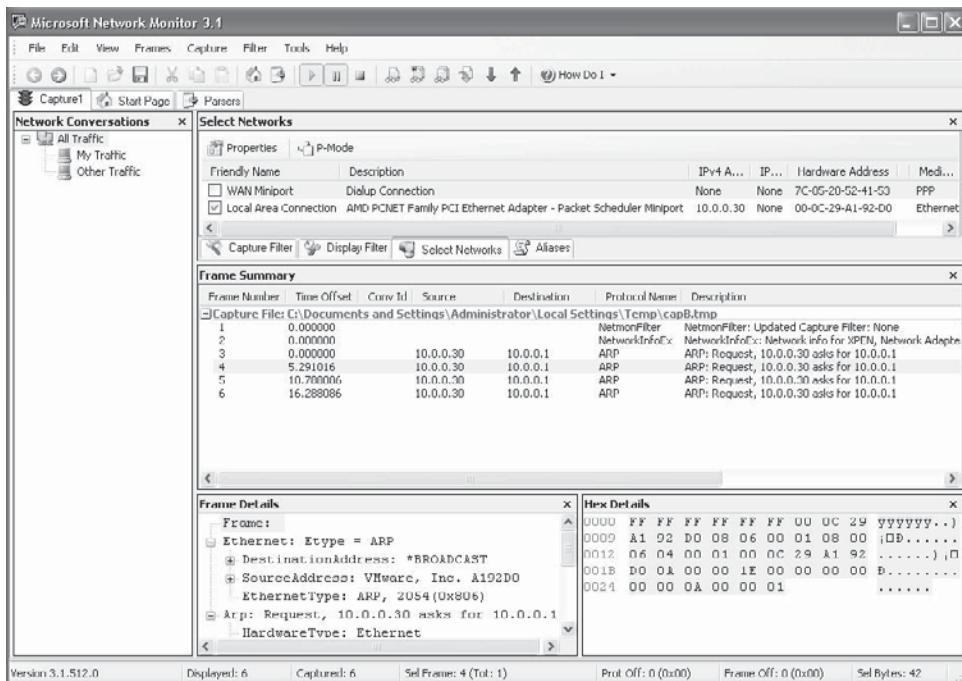
system-independent library. The packet filter is a device driver that adds the ability to capture and send raw data from a network card to Windows 95, 98, NT, 2000, XP, 2003, and ME, with the possibility to filter and store the captured packets in a buffer.

WinDump is shown in Figure 1-28.

## THC-RUT

THC-RUT offers a wide range of network discovery tools, including ARP lookup on an IP range, spoofed DHCP request, RARP, BOOTP, ICMP-ping, ICMP address mask request, OS fingerprinting, and high-speed host discovery. THC-RUT gathers TCP stack information, banners, open/closed port characteristics, and timing values and puts them through a Perl regular expression matrix to determine the OS with the highest accuracy.

The tool (shown in Figure 1-29) is capable of discovering a class B network within 10 minutes.



**Figure 1-30** Microsoft Network Monitor troubleshoots wireless connections in Vista and other Windows platforms.

## Microsoft Network Monitor

Microsoft Network Monitor is a wireless (802.11) capturing and monitoring tool for Windows. It troubleshoots wireless connections. It can trace wireless management packets, and it scans all available channels. It also provides RAS tracing support on Vista (Figure 1-30).

---

## Wireless Security Tools

### CommView for WiFi PPC

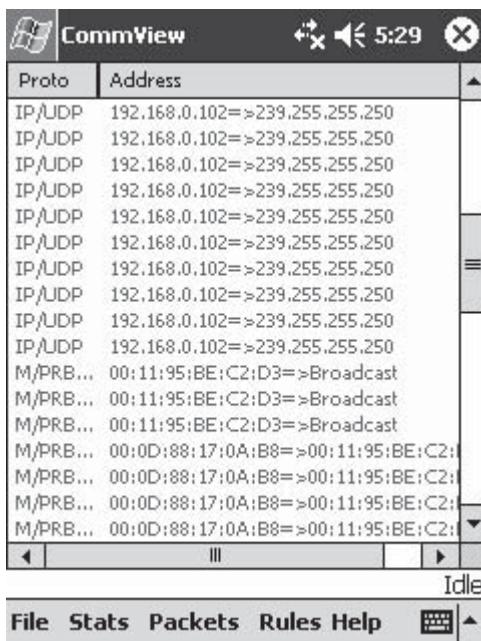
CommView for WiFi PPC is a special, lightweight edition of CommView for WiFi that runs on Pocket PC handheld computers. It is designed for express wireless site surveys, as well as capturing and analyzing network packets on wireless 802.11b/g networks. With CommView for WiFi PPC, shown in Figure 1-31, the user can do the following:

- Scan the air for Wi-Fi signals
- Select channels for monitoring
- Detect access points and wireless stations
- Capture packets
- Measure signal strength
- View the list of network connections
- Examine and filter individual packets

### AirMagnet Handheld Analyzer

AirMagnet's Handheld Analyzer, shown in Figure 1-32, allows the user to do the following:

- *Automatically detect vulnerabilities:* Handheld Analyzer performs a continuous vulnerability assessment of a Wi-Fi network in order to detect weaknesses that often go overlooked. Handheld



**Figure 1-31** CommView analyzes wireless network data.



**Figure 1-32** AirMagnet Handheld Analyzer detects weaknesses in wireless networks.

Analyzer automatically identifies hundreds of vulnerabilities and performance problems, such as 802.11b/g conflicts, 802.11e problems, and QoS. It also watches for dozens of wireless intrusions and hacking strategies, including rogue devices, denial-of-service attacks, dictionary attacks, fake APs, RF jamming, Stumbler tools, and many more.

- **Lockdown security policies:** Handheld Analyzer can set detailed security policies for all devices on the network. It will also validate that the encryption methods themselves function correctly over the WLAN. It can establish an even higher level of organized security by designating a list of approved APs for client access, and monitor for exposed wireless stations, ad-hoc devices, and other vulnerabilities.
- **Perform live, interactive network tests:** In addition to the issues that Handheld Analyzer automatically locates, a suite of active troubleshooting tools are available to help quickly pinpoint network problems, such as RF interference, traffic/infrastructure overloads, hardware failures, connectivity issues, and more. It will test connections with traditional tools such as DHCP, ping, and traceroute. It can also use AirMagnet's Diagnostic Tool to view the step-by-step progress of a connection between a client and AP to pinpoint exactly where the process has broken down.
- **Track down rogues and devices:** Handheld Analyzer offers a zero-tolerance approach to rogue management, detecting and blocking rogues either wirelessly or at the wired port. The Find Tool locks on to a particular AP or station and discovers the physical location of a device. The Find Tool can also be used to align signals between antennas to quickly optimize reception in line-of-sight bridging.
- **Detailed packet and frame analysis:** Handheld Analyzer shows real-time packet flows for any Wi-Fi asset. This allows it to track data and management packets live, and watch CRC errors, utilization, packet speed, media type, and more. It shows a real-time decode page for detailed network analysis. Handheld Analyzer decodes the most popular protocols such as FTP, HTTP, SMTP, POP, and Telnet, with advanced filtering options to focus on particular conversations based on IP address or port number.
- **GPS support:** Handheld Analyzer provides GPS coordinates to help quickly pinpoint the location of security and performance issues in an outdoor 802.11b network.
- **Flexible mobile form factor:** The Handheld Analyzer software works on any hardware platform that supports AirMagnet's Wireless CompactFlash card (Mercury NL\_2511 CF) or the Cisco Aironet 352 (AIR-LMC352 or AIR-PCM352).

## AirDefense Guard

AirDefense Guard is an 802.11a/b/g wireless LAN intrusion detection and security solution that recognizes security risks and attacks, offers real-time network audits, and observes the condition of a wireless LAN.

AirDefense Guard has two components:

- Distributed sensors are located near 802.11 access points to observe all WLAN activities and provide reports to server appliances.
- Server appliances analyze the traffic in real time.

Its features include the following:

- It detects all rogue WLANs.
- It secures a wireless LAN by recognizing and responding to intruders and attacks as they occur.
- It carries out real-time network audits to record all hardware, track all wireless LAN activity, and enforce WLAN policies for security and management.
- It observes the health of the network, identifying and responding to hardware failures, network interferences, and performance degradation.

The remote sensors feature the following:

- Deployed in the proximity of WLAN to cover multiple access points
- Provide 24/7 monitoring of all WLAN activities
- Covers 40,000 square feet of typical office space and can be greatly extended with building antennas
- Capture wireless traffic from APs and stations
- Report to back-end server
- Centrally managed

The server appliance features the following:

- Analyzes traffic in real time
- Enforces wireless LAN security policies
- Multi-Dimensional Detection Engine
- State Analysis Engine
- SNMP integration with network management applications
- Secure Web-based interface
- Comprehensive reporting

## Google Secure Access

Google Secure Access is a downloadable client application that allows users to establish a more secure Wi-Fi connection. It encrypts Internet traffic and sends it through Google's VPN servers to the Internet. The data that is received will be encrypted and sent back through Google servers. It can be downloaded for free, as shown in Figure 1-33.

## RogueScanner

RogueScanner is a network security tool for automatically discovering rogue wireless access points by scanning a wired network. It can also be used for network asset discovery. It can find all network-connected devices such as printers, routers, Web cameras, and PCs, and is shown in Figure 1-34.

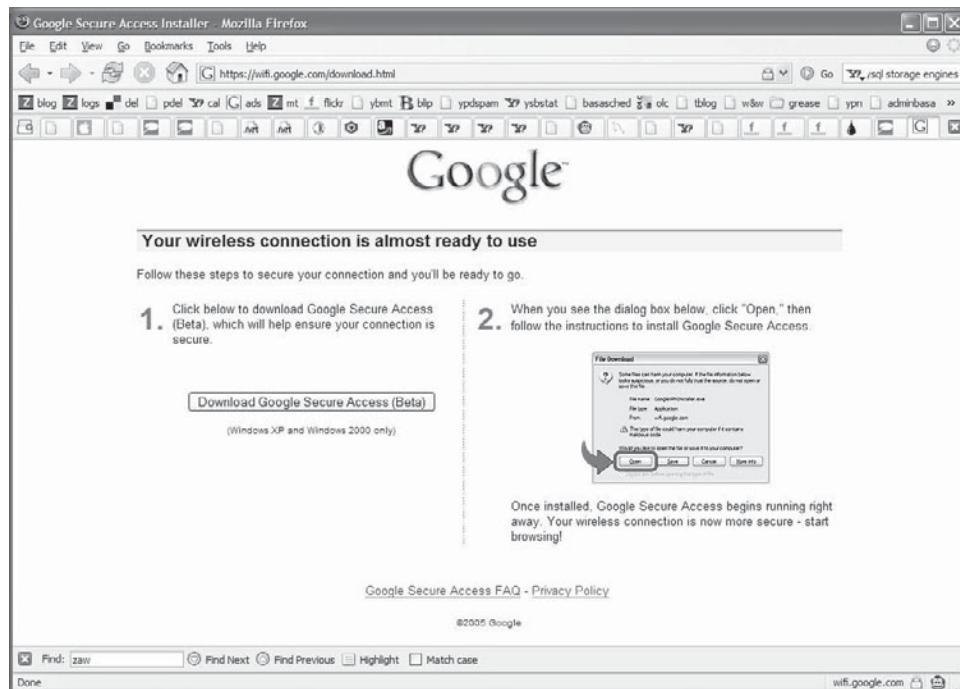


Figure 1-33 Google Secure Access uses Google's VPN to secure wireless transfers.

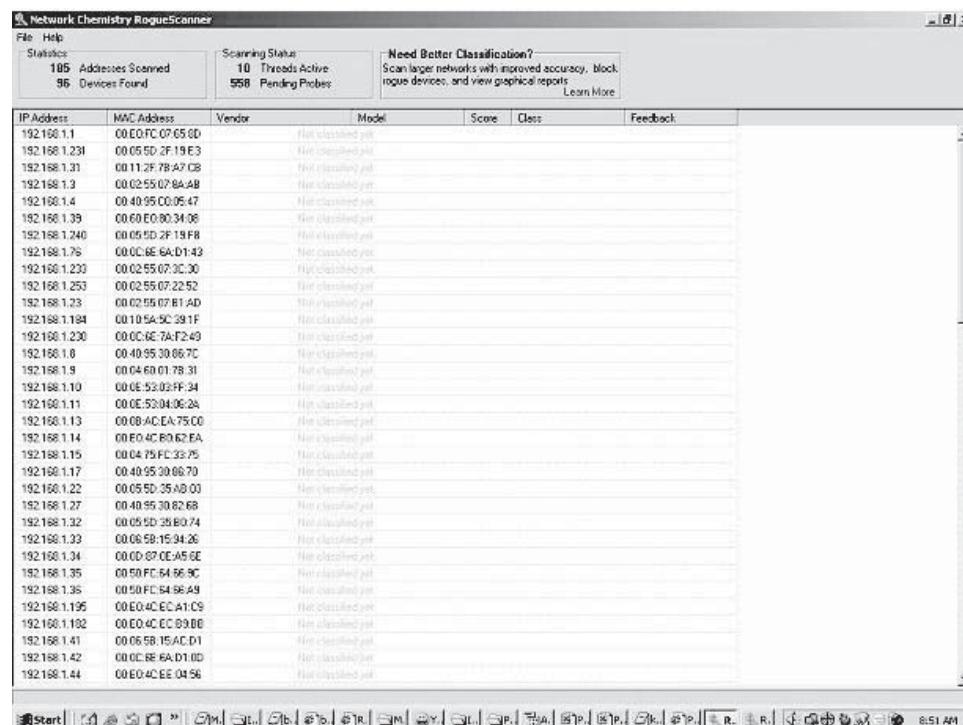


Figure 1-34 RogueScanner discovers rogue wireless access points.

---

## Chapter Summary

- Wireless technology enables a mobile user to connect to a local area network (LAN) through a wireless (radio) connection.
- Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wi-Fi standard. IEEE 802.11b is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.
- WEP is vulnerable because of relatively short IVs and keys that remain static.
- Even if WEP is enabled, an attacker can easily sniff MAC addresses because they appear in cleartext format. Spoofing a MAC address is not difficult.
- If attackers use wireless equipment to scan for a wireless network, they will be able to perform a spoofing attack by setting up an access point (rogue) near the targeted wireless network.
- Wireless networks are vulnerable to DoS attacks.
- A variety of hacking and monitoring tools are available for wireless networks.
- Securing wireless networks includes adopting a suitable strategy for MAC address filtering.

---

## Review Questions

1. List the two basic methods for locating access points.

---

---

---

---

2. List the steps to access a WLAN.

---

---

---

---

3. What is WEP?

---

---

---

---

4. Discuss the differences between WEP and WPA.

---

---

---

---

5. List the steps to hack a wireless network.

---

---

---

---

6. What is LEAP?

---

---

---

7. How does an administrator secure a wireless network?

---

---

---

8. What is a rogue access point?

---

---

---

## Hands-On Projects



1. Use the AiroPeek NX tool to deploy, secure, and troubleshoot a wireless LAN.
  - Navigate to Chapter 1 of the Student Resource Center.
  - Install and run AiroPeek NX.exe, as shown in Figure 1-35.

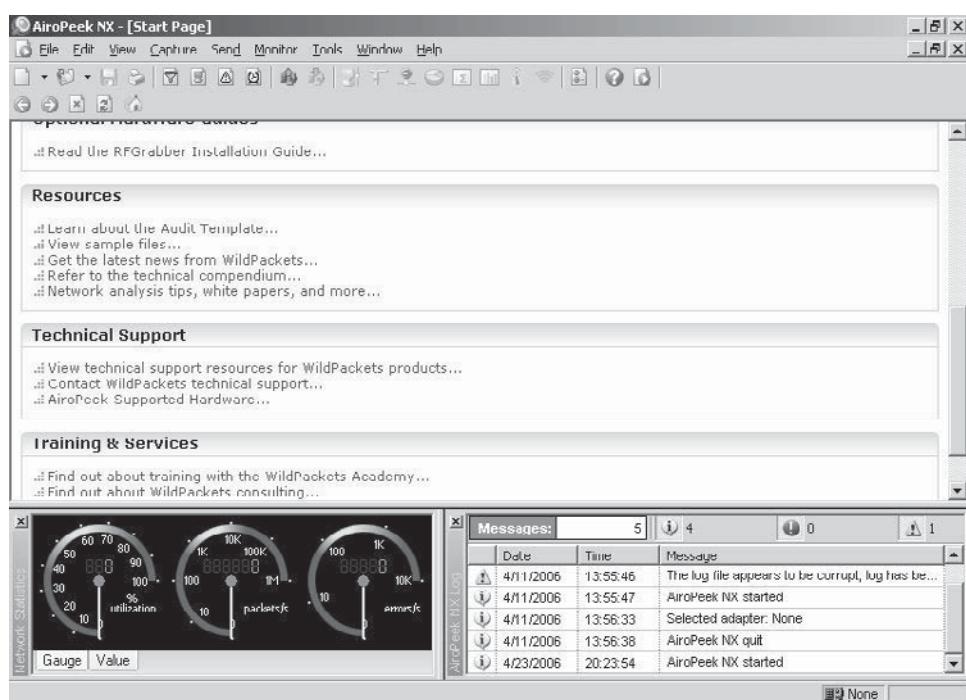


Figure 1-35 Install AiroPeek NX.

- Click View sample files in the Resources section, as shown in Figure 1-36.



Figure 1-36 Click View sample files.

- Click Wireless, as shown in Figure 1-37.

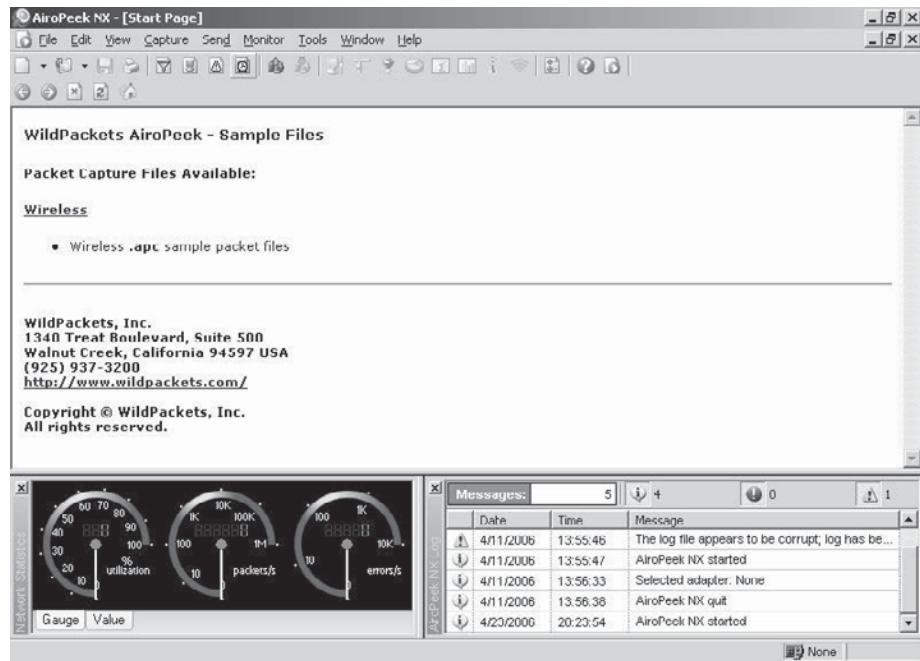


Figure 1-37 Click Wireless.

- Note the Telnet-WEP.APC WEP keys:
  - Telnet using Windows 2000: “Telnet Server Administration”
  - Encryption enabled: key1=“0123456789”, key2=“9876543210”

- Click Telnet-WEP.APC, as shown in Figure 1-38.

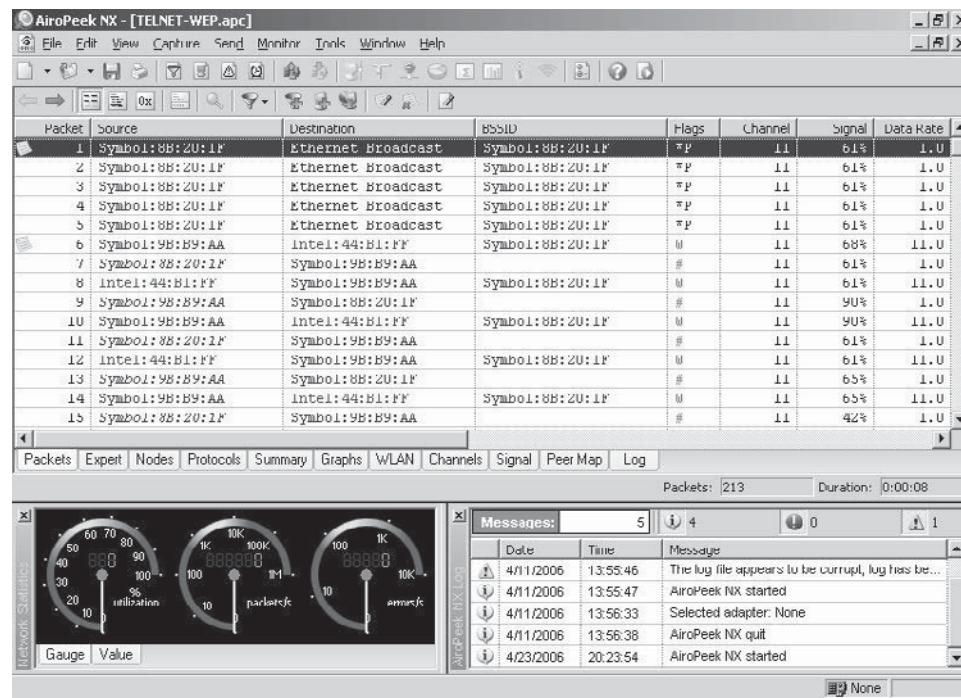


Figure 1-38 Click Telnet-WEP.APC.

- Click a packet and view its details, noting that the data is encrypted, as shown in Figure 1-39.

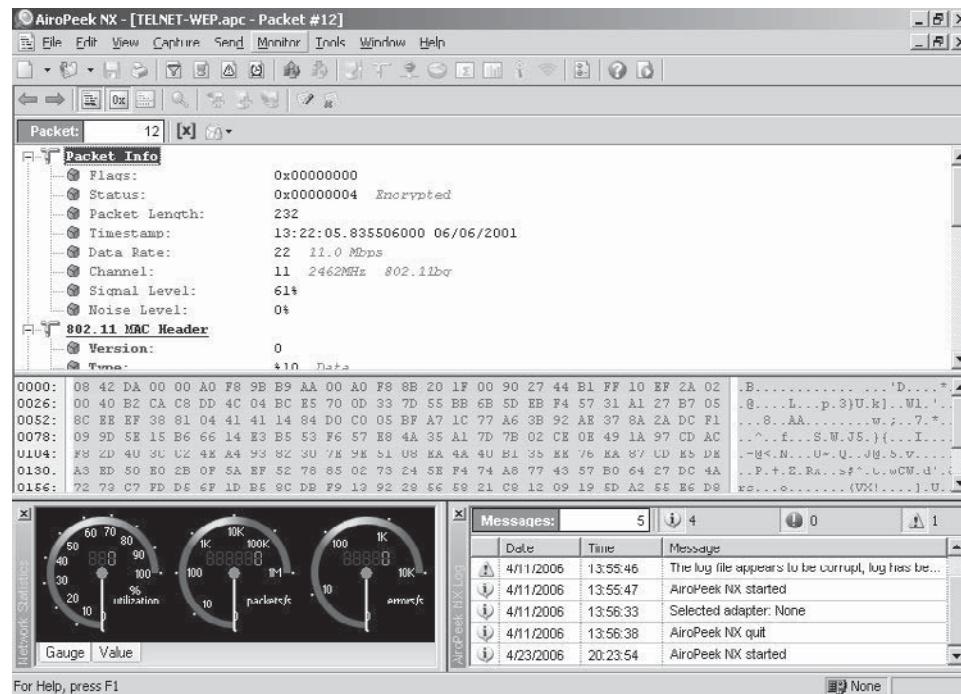


Figure 1-39 Click a packet and view its details.

- Click Tools and then Decrypt WLAN Packets, as shown in Figure 1-40.
- Click the ellipsis (...) button as shown in Figure 1-41.

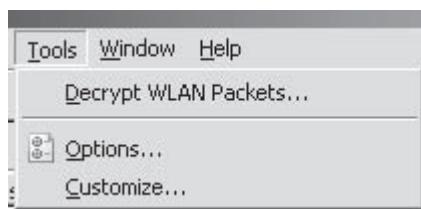


Figure 1-40 Click Tools, then Decrypt WLAN Packets.



Figure 1-41 Click the ellipsis (...) button.

- Click Insert, as shown in Figure 1-42.
- In the Key1 field, type 0123456789.
- In the Key2 field, type 9876543210.

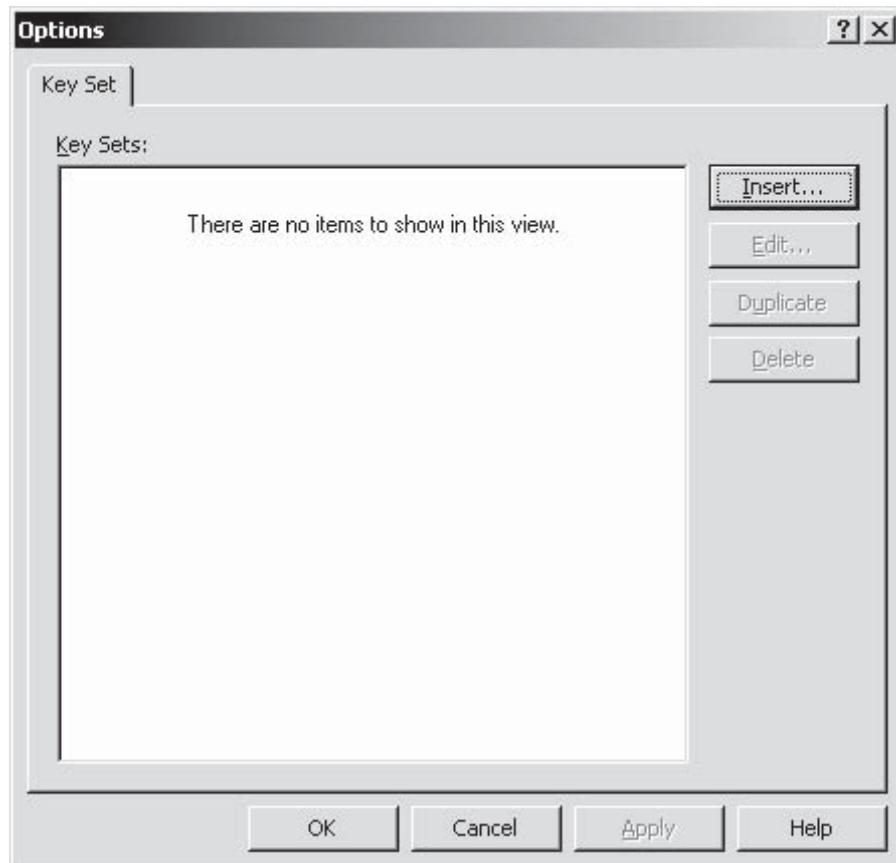
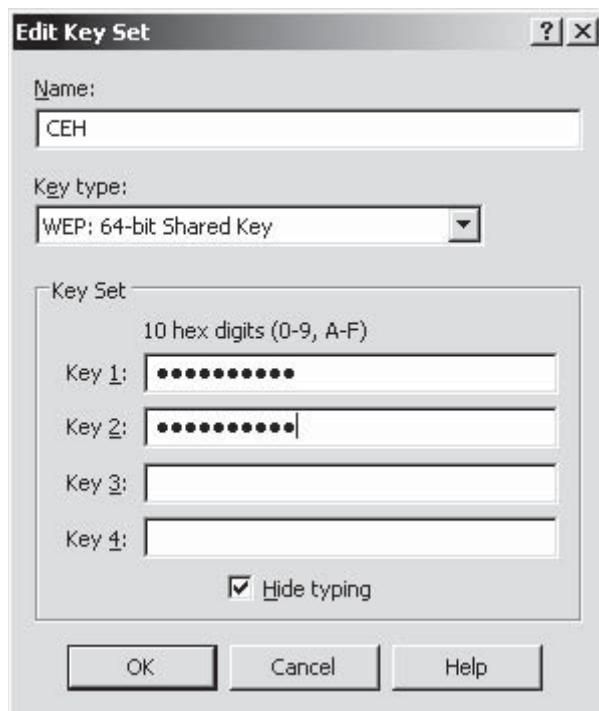


Figure 1-42 Click Insert.

- Click the OK button, as shown in Figure 1-43.
- View the unencrypted packets.



**Figure 1-43** Click the **OK** button.

2. Read *A Guide to Wireless Security*.
  - Navigate to Chapter 1 of the Student Resource Center.
  - Open *A Guide to Wireless Security.pdf* and read it.

*This page intentionally left blank*

# Physical Security

## Objectives

After completing this chapter, you should be able to:

- Understand security statistics
- Understand physical security
- Explain the need for physical security
- List the factors affecting physical security
- Explain the features of various locks
- Understand the challenges in ensuring physical security
- Understand the differences between various spyware technologies
- Create a physical security checklist
- Understand wireless security
- Prevent laptop thefts
- Describe a mantrap

## Key Terms

**Biometric technology** devices that can read and store unique physical traits for authentication purposes

**Compromising emanation (CE)** sensitive information unintentionally leaked from hardware

**Digital certificate** an electronic document that contains a user's identification information

**Encryption** the process of translating information into a code for secure transmission

**Mantrap** a security system that utilizes independently locking doors to ensure visitor authentication

**Smart card** a card containing a microchip that can process and store information for verification purposes

**Virtual private network (VPN)** a network that functions securely by "tunneling" through larger public networks

**Wi-Fi Protected Access (WPA)** a more secure encryption protocol that was designed to replace WEP

**Wired Equivalent Privacy (WEP)** a protocol used to provide encryption for wireless networks

**Wireless access point (WAP)** a device that allows multiple users to access wireless networks

---

## Case Example

A well-known firm had a database of information that was considered its major competitive edge. Although the firm believed its systems were secure, it hired a consultant to perform a security assessment, just to be sure.

On the first day of the assessment, the consultant walked into the lobby and announced that he was there to see the security officer. Company policy did not allow visitors to be unattended, so the receptionist phoned the security officer to meet the consultant in the lobby. The consultant told the receptionist that he had forgotten something in his car and would return shortly.

Before entering the lobby, the consultant had noticed that the parking lot encircled the building completely, and that the loading bays in the rear of the building were quite busy. He walked to the loading bays, walked up the stairs, stopped to chat with a few employees, and walked through the warehouse to what was an obvious entrance to a key card-accessible office area. When someone entered the warehouse from the office area, the consultant walked toward the door, and the employee politely held the door for him.

The consultant already knew the location of the computer room. As he walked toward the door, another polite employee held the door for him. On entering the computer room, the consultant went straight to the tape racks. There, studying the racks as if looking for specific information, he grabbed a tape containing accounting information. He tucked the tape under his arm, exited the room, and took the elevator to the second floor. There, he asked someone for the location of the security officer's office. After being told where it was, the consultant entered the office and waited for the officer to return. The entire event lasted no more than 15 minutes. In that time, the consultant breached the company's physical security by entering the building and taking a tape. He also could have used the security officer's computer to browse the company's internal network, since the computer had been left logged on with no screensaver security.

Not all evaluations begin this way, but most organizations have vulnerabilities as obvious as this one. If it isn't a physical security problem, it is a security management problem.

---

## Introduction to Physical Security

This chapter focuses on physical security. It covers the reasons why companies need to be aware of physical security needs and the ways an organization can go about making its facilities physically secure.

### What Is the Need for Physical Security?

Many companies raise this question. Physical security doesn't just mean securing systems; it also involves securing the entire premises, boundaries, workstations, and any other areas that may be unique to a company. Even though physical security is an added layer for network security, the goal is the same: to prevent unauthorized access.

The scenario in this chapter highlights the need for physical security. The consultant easily walked into a supposedly secure company and stole accounting data from the computer room. Placing security guards at key points does not necessarily make an organization physically secure. Often, other critical areas are left unattended.

The following statistics come from a survey taken of various companies' physical security policies:

- Receive alarm communications—28%
- Access control technology with identification cards—90%
- Require visitors to wear a badge or pass that identifies them as a visitor—93%
- Have explosion-detection devices—9%
- Have emergency telephones in parking areas—9%
- Employ police officers for security—56%
- Use metal detectors to screen employees and visitors—7%

The varying percentages in these statistics reveal that very few companies have all aspects of their physical security covered. Many employees do not realize the role that they must take in securing their company. Hardware

and software security precautions complement each other in keeping hackers at bay, making physical security an essential aspect of any company's security policy.

Physical security is needed for the following reasons:

- Prevents tampering/stealing of data and other valuable information from computer systems
- Protects the integrity of the data stored in a computer
- Prevents loss of data and damage of systems due to natural calamities
- Prevents any unauthorized person from getting into a company's work area, or in other critical areas, such as the server room, R&D room, and labs
- Prevents critical information from being disposed of improperly, thus eliminating the effectiveness of dumpster diving, a way of collecting trash with the intent of finding sensitive information such as credit card receipts, tapes, CDs, phone books, and scribbled papers
- Because prevention is better than a cure

---

## Physical Security

Physical security describes the measures taken to protect personnel, critical assets, and systems against deliberate attacks and accidents. Physical security is intended to prevent attackers from accessing resources and information stored by a company. Physical security measures can be physical, technical, or operational.

### Physical Measures

Physical measures are taken to secure structural assets. They include:

- Deploying security personnel
- Installing access controls
- Installing locks

#### ***Deploying Security Personnel***

Security personnel secure assets from man-made and natural disasters. These assets include physical structures, hardware, and also employees. To guard these assets and prevent unauthorized entry, security guards and/or intruder detection systems should be employed at every access point. It is the responsibility of security personnel to implement appropriate entry controls and confirmation procedures to make sure that only authorized people are allowed to enter a company's critical and sensitive areas.

#### ***Installing Access Controls***

Access controls are devices used to ensure that only authorized personnel can access vital information. Because a company's information must be used on a daily basis by employees, access must not be so restrictive that it hinders a company's performance. Different kinds of access controls should be installed based on the level of security needed in order to maximize the company's efficiency.

The following are several types of access controls:

- Intruder detection systems
- Sensors
- Fences
- Biometric access controls
- CCTV

#### ***Locks***

One of the most basic physical measures that a company can take is installing locks. A lock has two modes: engaged/locked and disengaged/opened. When the lock is engaged, only persons who can disengage it can access the assets protected by the lock. When the lock is disengaged, anyone can access the asset. Some kinds of locks have a provision for engaging or disengaging only from one side, while others can be used from both sides.

Locks are classified into three types, depending on their security level—minimum, medium, or maximum:

1. Minimum security locks can be easily disengaged.
2. Medium security locks take some time to be disengaged.
3. Maximum security locks are the most complex and take the longest to disengage.

The robustness of security provided by a lock depends upon how well it can withstand physical damage, and what its requirements are for operation. The physical design of locks is either mechanical or electrical.

**Mechanical Locks** Mechanical locks contain movable parts and do not require electricity to function.

There are three types of mechanical locks:

- Warded
  - Warded locks operate through the physical insertion of a key into the lock.
  - Warded locks are easy to pick with a stiff piece of wire or thin strip of metal, so these locks are usually used in areas that do not require a high level of security.
- Tumbler
  - Tumbler locks are similar to warded locks except that they have movable metal parts called tumblers that prevent the wrong key from opening the locked tumbler.
- Combination
  - Combination locks use a combination of numbers to lock. The lock opens only when the proper combination of numbers is known and set.

**Electric Locks** Electric locks are electronic devices with scanners that can identify the processing codes of users and computers.

There are four types of electric locks:

- Card access systems
  - These locks are the most common electronic locks and are found in many hotels and buildings.
  - With this type of system, when a person inserts a card into the card reader, the card reader reads the code on the card, and sends the information to a computer that verifies the card. If the code matches, the lock opens.
- Electronic combination locks (cipher locks)
  - With this type of lock, in order to gain entry, a combination of numbers must be entered on a keypad.
  - If the number entered on the keypad matches the information stored in the computer, the door opens.
- Electromagnetic locks
  - With these kinds of locks, a strike-plate is placed on top of a door.
  - A strong electromagnet is fastened to the door in alignment with the strike-plate.
  - Current is passed through the system, causing the electromagnet to be attracted to the strike-plate and preventing the door from opening. To open the door, a key that stops the flow of current is used.
- Biometric entry systems
  - **Biometric technology** uses an individual's unique physical traits to identify a valid user. Biometric entry systems have information stored regarding retinas, fingerprints, and palms of authentic users. Exposing the applicable physical attribute to the biometric reader allows entry.

## Technical Measures

Technical measures are taken to secure the systems, services, and resources that support a company's information technologies. They include:

- Providing security for office, warehouse, and factory space
- Disabling removable media drives
- Installing authentication mechanisms
- Securing laptops

## Disabling Removable Media Drives

It is necessary to secure systems from unauthorized and illegitimate access. The system administrator is responsible for safeguarding the network beyond its firewall. Initially, administrators secure a network by configuring mail filters on the SMTP server or installing antivirus software; however, attackers have various ways to extract sensitive information from a network despite these precautions. For example, information can be extracted by means of a Memory Stick. A 1-GB USB Stick has the capacity to hold all of a company's confidential information. An attacker can extract the data in a fraction of a second, or inject a virus or a Trojan to infect the system.

### Disabling USB Storage Devices

The procedure to disable USB storage devices is as follows:

Check to see whether a USB storage device is installed on a computer. If it is not, assign the user or the group "Deny" permission via the following files:

```
%SystemRoot%\Inf\Usbstor.pnf  
%SystemRoot%\Inf\Usbstor.inf
```

This restricts a user from installing a USB storage device on the system.

The steps followed for Windows-based operating systems are:

1. Start Windows Explorer, and locate the %SystemRoot%\Inf folder.
2. Right-click the Usbstor.pnf file, and then click the **Properties** button.
3. Click the **Security** button.
4. Select the user or group from the list that you want to set Deny permissions for.
5. In the **Permissions for UserName or GroupName** list, click to select the **Deny** check box next to **Full Control**, and then click the **OK** button.



In addition, add the System account to the Deny list.

6. Repeat the same procedure for the Usbstor.inf file.

## Authentication Mechanisms

Authentication mechanisms verify a user's identity and security clearance. They can be classified in three ways: biometric, knowledge-based, and object-based.

**Biometric Authentication** Biometric authentication mechanisms use unique physical traits to identify and validate users. The following are some of the biometric devices used for access control:

- Fingerprint scanner
  - This is the oldest form of identification in biometrics.
  - All individuals have unique, immutable fingerprints.
  - An electronic scanner reads a user's fingerprint, and matches it with the stored fingerprints of authenticated users.
- Face scanner
  - Facial scan technology works well with standard off-the-shelf PC video capture cameras and generally requires 320 × 240 resolution and at least 3–5 frames per second.
  - In biometrics, a facial scan is carried out in four steps: capturing the sample, extracting the feature, comparing the feature with available templates, and then matching the sample.
- Iris scanner
  - The human eye's iris has a unique random pattern of textures and pigments.
  - An iris's pattern can be scanned the same way a fingerprint can.
  - Iris scans are beginning to be implemented in many areas, including for computer logins, passports, ATMs, and credit card authentication.

- Voice recognition device
  - This type of verification can be deployed where voice data is already captured.
  - Voice or speaker verification is a biometric authentication technology well suited for a handful of applications and systems in which other biometric technologies would be difficult to use.
- Retina scanner
  - This technology scans the blood vessels in the eye.
  - Retinal scans use a low-intensity light source and optical coupler to recognize blood vessel patterns with acute accuracy.
  - The user is asked to look through a small opening in the device at a small green light. It takes about 10 to 15 seconds for the device to recognize and verify the patterns in the eye of the user.
- Vein pattern scanner
  - The arrangement, location, and thickness of veins are considered unique biological traits.
  - The hand's vein structure is read with an infrared light source.
  - These traits are compared with stored data, thus authenticating a person if there is a match.
- Palm print scanner: Palm print technology is a new biometric method used to verify a person's identity. There are two types of features in palm prints: structural and statistical.
  - Structural features use the lines that exemplify a palm accurately.
  - Statistical features use the physical features, but they cannot reveal the structural information of the palm print.
- Hand geometry scanner
  - Hand geometry biometric technology scans the hand for 3-D features such as the size and shape of knuckles and fingers. This type of scanning does not consider scars, cuts, etc.
  - The scanner equipment has a light source, a mirror, a camera, and a scanning surface.
  - The hands of the user are placed in a uniform position, and pegs are used to calculate the area between the fingers and the angle between them. During the scanning process, 90 characteristics are recorded.
- Signature dynamics analyzer
  - This type of analysis is used to verify an individual's identification on the basis of their signature.
  - Signature scanning equipment includes an electronic drawing tablet and stylus used to record the direction, speed, and coordinates of a handwritten signature.
- Keyboard dynamics analyzer
  - Keyboard dynamics technology analyzes the user's keystrokes on the keyboard.
  - The various characteristics that are used to verify dynamics are speed, pressure, total time taken to type a specific word, and the amount of time taken to hit certain keys.
  - Keyboard dynamics technology uses two different variables: "dwell time" is the amount of time a particular key is held down, and "flight time" is the time interval between keystrokes.

**Knowledge-Based Authentication** This type of authentication is based on a user's knowledge. A traditional UNIX password system would be an example of this type. Password authentication depends on something the user knows that is hard to guess. To make reliable authentication, the user must have a password that cannot be guessed by others. Many people set weak passwords or have a hard time keeping passwords secret. When creating a password, using short keys makes a password weak; conversely, using long keys makes it strong.

There are two ways to make traditional and memorized passwords nonreusable:

- *Encrypted time stamp:* This method is used by the protocol Kerberos. It prevents payback while modifying time stamps without knowing the password.
- *Challenge-response system:* With this system, the password given is dependent on the prompt given by the server.

**Object-Based Authentication** This type of authentication uses physical objects such as cards or tokens to validate users. These objects function as *digital certificates*, which are essentially access keys containing a user's identity information and digital signature. With electronic cards, it becomes practical to use challenge-response or time-based encryption. **Encryption** is the translation of information into code for secure transmission. For challenge-response, the user encodes the rule in the card itself that converts the challenge to the response. For time-based encryption, the user encodes both the time source and the encryption in the card itself.

**Smart Cards** *Smart cards* are similar to credit cards in shape and size, but their memory capacity is much greater, allowing users to carry digital certificates on them.

- A smart card contains memory and a CPU. It has more information than a magnetic stripe card (memory only), and it can be programmed for different applications.
- Smart cards provide mobility and improved security by allowing users to carry their digital certificates with them. Digital certificates can be used anywhere on the Internet where user identification is required.
- Digital certificates allow users to communicate secretly over the Internet. One needs a personal identification number (PIN) for using a smart card. This makes the smart card more secure, as only the user of the card knows the PIN.
- Personal computers at the office can be protected from unauthorized access using smart cards. Smart cards separate the certificates from the hard drive and ask for a PIN to access the system. Smart cards become disabled if a certain number of attempts to input the right PIN fail.
- Some smart card readers look similar to a 3.5-inch floppy drive which, when connected to laptops or PCs, allow users to safely access the Internet or corporate data.

**Security Token** Security tokens provide an extra level of assurance through a method known as two-factor authentication: Users have a personal identification number (PIN), which authorizes them as the owner of that particular device. The device then displays a number that uniquely identifies users to the service, allowing them to log in.

- Security tokens are physical objects, unlike passwords.
- A smart card is accessible via a PIN, whereas a token is used in tandem with a PIN.
- Validating users on a network is easy when using a security token.
- Tokens improve security, lower the cost per user, centralize the authentication mechanism, reduce administrative costs, and prevent unauthorized access to services.

**Laptop with 5,000 Medical Records Stolen** According to an article in *The Independent* dated February 14, 2008, a laptop was stolen from the outpatient department at Russells Hall Hospital in Dudley, U.K. The laptop contained records of 5,123 patients with a blood disorder. Hospital management sent letters to affected patients about the theft. The data in the stolen laptop was protected by two sets of usernames and passwords. The database contained the names, addresses, and dates of birth of the patients. Paul Farenden, chief executive of Dudley Group of Hospitals NHS Trust, reassured the public that it was unlikely that access could be gained to the database.

## Securing Laptops

The physical security of digital devices is as important as Internet security software. Antivirus, antispyware, and other security software will not protect you from a thief stealing your laptop.

Laptops must be secured because they often contain information about confidential assets. Figure 2-1 illustrates the results of an informal TechRepublic poll for laptop theft.

The high percentage of company laptop thefts makes this area of physical security a high priority. Personal information about a laptop's owner can be discovered through this kind of theft, but information about a company's network can also be gained by tracking IP addresses and finding the mail servers used. Hackers can use this kind of information to discover and exploit vulnerabilities in a company's network. Information concerning business deals, financial arrangements, and company strategies can also be discovered on an employee's laptop. Both the laptop itself and the information it holds must be secured against potential attackers and competitors with malicious intent. Intruders can attack with a number of malicious programs—viruses, Trojans, worms,



Copyright © by EC-Council

All rights reserved. Reproduction is strictly prohibited

**Figure 2-1** This informal TechRepublic poll shows the high rate of company laptop thefts.

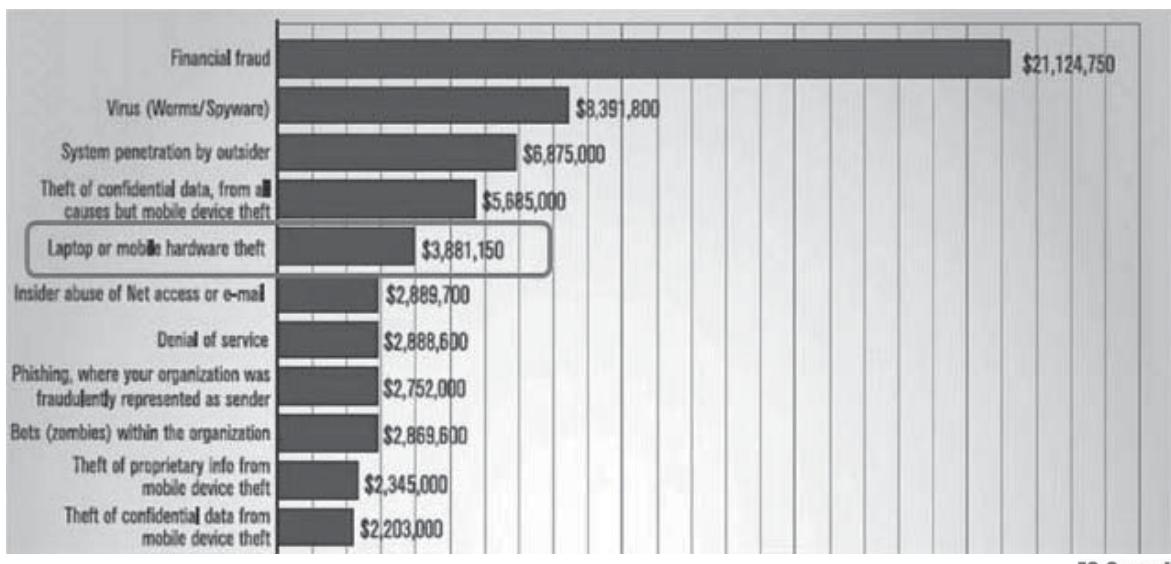
rootkits, dialers, joke, spyware, and spam—which can corrupt stored data. In order to avoid laptop theft or compromise, information in laptops must be secured through the following means:

- *Password protection:* Use a combination of uppercase, lowercase, alphanumeric characters, and special symbols. Changing passwords frequently is another measure to safeguard them. The BIOS of the laptop must be protected with an appropriate password. Also disable the BIOS setting for floppy drives and other devices.
- *Blocking unnecessary ports and devices:* In order to protect the laptop from unwanted, unauthorized access, device-locking software must be installed and all unwanted ports and devices, such as USB drives, must be disabled.
- *Patches and updates:* The operating system should be updated regularly. Patches and updates can be downloaded and installed either manually from the vendor's Web site, or by using automatic updating tools provided by the vendor.
- *Antivirus software, firewalls, and intrusion detection systems:* Antivirus software and spyware detection software must be installed and updated regularly. The firewall rules should also be updated, and the IDS configured to prevent unauthorized access.
- *Encryption:* With the rise in laptop theft, it is advisable to encrypt confidential/important files stored on a laptop.
- *Securing the operating system:* The operating system should be secured by checking the default configurations.
- *Laptop registration:* A laptop must be registered with its manufacturer. This can help in tracking it in case of theft.
- *Laptop engraving:* The laptop is safer if it is marked permanently with the company's logo and other identifying information. Tamper-resistant metal commercial asset tags are also helpful in the recovery of a stolen laptop.

### Other Measures

- Avoid unnecessary user accounts and renaming the administrator account.
- Disable the display of the last logged-in username in the login dialog box.
- Backup data on a regular basis.

According to a computer crime and security survey carried out by CSI, losses, in dollar amounts, of a typical organization due to various types of attacks are shown in Figure 2-2.



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

**Figure 2-2** This chart shows the high cost of laptop thefts to companies.

## Operational Measures

These are taken to ensure the security of organizational resources before and during operations. Operational measures include:

- Identifying possible threats
- Analyzing threats
- Risk assessments

## Physical Security Personnel

Effective measures need to be taken to ensure a company's security. Precautions should include ensuring that there is sufficient physical security to prevent illicit and untraceable access to the data processing facility. Security personnel need to be deployed according to the value and secrecy of the work being carried out. Both physical and intellectual property need to be considered. In large corporations, it is common for different types of security personnel to be deployed according to the sensitivity of the work and/or equipment. Usually a chief security officer trains and supervises security personnel, and monitors the corporation's overall security infrastructure.

With accountability comes responsibility. Most organizations do not have employees who are accountable for security. If compromises occur in a company's security, employees tend to hold others responsible. If a network is compromised, the system administrator is likely to be held accountable, regardless of where the fault took place. To strengthen the physical security of a company, the following personnel should be made accountable for a firm's physical and information security:

- The security officer
  - This officer is responsible for any physical security breach.
  - The security officer is responsible for educating the rest of the employees and guards on duty.
  - The security officer has to manually check every detail of a firm's physical security.
- Safety officer
  - The safety officer assesses the fire protection and safety measures that need to be taken.
  - Educating employees and other staff on fire and safety should be of prime concern for this officer.

- Information systems analyst or security administrator
  - This officer primarily looks into network security and related issues.
- The chief information officer
  - This officer heads the committee that frames security policies.

---

## Physical Security Challenges

Challenges to a company's physical security can be classified as threats, personnel challenges, and security countermeasures.

### Physical Security Threats

#### *Vandalism*

- Disgruntled or former employees may try to compromise the system.
- Systems could be mishandled during civil unrest or a disaster.

#### *Theft*

- Lack of proper security and locks may result in theft of equipment.
- The presence of an alert guard within the premises can help prevent theft.

#### *Natural Calamities*

- Earthquakes
  - Tarpaulins/plastic sheets should be readily available in the system room. Covering computing assets in an emergency may mitigate damage.
  - Magnetic tapes should be covered to prevent wear and tear.
  - Operators should be trained on how to properly cover equipment.
- Fire and smoke
  - Fires are generally caused by human error.
  - Fire alarms and extinguishers should be placed well within reach of employees.
  - Smoke detectors should be placed on the ceiling and in other locations.
  - A separate, secure smoking zone should be available to company employees.
- Flood
  - Periodic inspections under the flooring in the data processing room must be conducted to check for water seepage, especially during times of heavy precipitation.
  - Water detectors should be installed and subjected to periodic checks.
  - Administrators should be aware of proper shutdown procedures, and exercise drills must be performed regularly.
- Lightning and thunder
  - All computer systems should have a UPS (uninterruptible power supply) to protect the systems from voltage fluctuations, sudden power surges, or power outages.
  - Such incidents can damage the hardware of a computer, especially the memory chips.

#### *Dust*

- Dust that accumulates on hardware hinders its performance.
- Dust can seriously hinder a PC's ability to cool down.
- Even if the computer's case has never been opened, dust can still get in through the drive openings. An effective way to remove dust from the inside of a CPU is with compressed air, which can be used to blow dust away from the motherboard and other components.

## Water

- PCs should not be placed near water sources that can splash onto the components or drip down into them.
- PCs should not be placed near windows. During storms, there may be a chance of water getting inside the CPU through the openings meant for cooling.
- PCs should be placed in an environment where humidity is controlled.

## Explosions

- Chemicals should be placed in isolation.

## Terrorist Attacks

- Terrorist actions can often occur regardless of a building's security. These types of attacks can be extremely destructive. The building should be adequately lit at night on all sides.
- Only people with proper security clearance should be permitted into the data processing area. Suspicious parties should be reported to security and/or the concerned authorities.

## Personnel Challenges

The physical security officer may face many challenges while ensuring physical security. These include:

- *Enforcing physical security policy*: Practical problems, such as inconveniences caused by the implementation of physical security policies, may raise security threats.
- *Social engineering attempts*: Social engineering tricks may be attempted on personnel to divulge sensitive information about the security arrangements of a company. Such knowledge may prompt attackers to find ways to compromise security systems. Management should provide enough training to employees to make them aware of social engineering attempts.
- *Restrictions for sharing experience and knowledge*: Access control policies may restrict personnel in one department from sharing their experiences and knowledge with other departments. Physical security ensures data security but may also restrict knowledge and company efficiency.
- *Cost and time*: Installing a physical security department in a company takes both time and money. Costs are incurred in the form of salaries, system installations, and training. Management can outsource security functions to a reliable and efficient firm that specializes in this area.
- *Terrorism*: Terrorists may enter a company through the standard recruiting process and later collect sensitive data needed for designing an attack on the target organization. Background checks on employees are crucial for avoiding this kind of attack.
- *Sophisticated technologies*: Security personnel often encounter problems with sophisticated technologies such as hidden cameras and recorders. Security personnel should be trained regularly on the technologies that can breach the security of an organization.

## Security Countermeasures

Security countermeasures are tools and techniques used by intruders to bypass physical security measures. They include spyware technologies, techniques to bypass biometric authentication devices, lock-picking techniques, and TEMPEST monitoring.

### Spyware Technologies

Spyware has been around since before the Cold War. Intelligence agencies used innovative technologies such as spy cameras and sound recorders to help agents in the field gather information. Current technologies include small pinhole cameras with audio as well as clear black-and-white pictures. Spyware is not only available to government agencies, but also to the general public. One recent camera is the size of a dime, and can be hidden in a wall, under a necktie, underneath jackets, or in any other strategic location. Another camera looks like a calculator and transmits color video and audio up to 1,000 feet. This system comes with a four-channel receiver, and connects to any TV or VCR for portable recording.

Other spyware includes:

- Long-range wireless video recorders
- Color video optical GRII (glasses)
- Smoke alarm video cameras
- Lock pick sets
- Spy cameras
- Night-vision cameras
- GPS tracking systems
- Wiretapping equipment
- Voice recorders
- Voice changers

### **Biometric Authentication Mechanism Challenges**

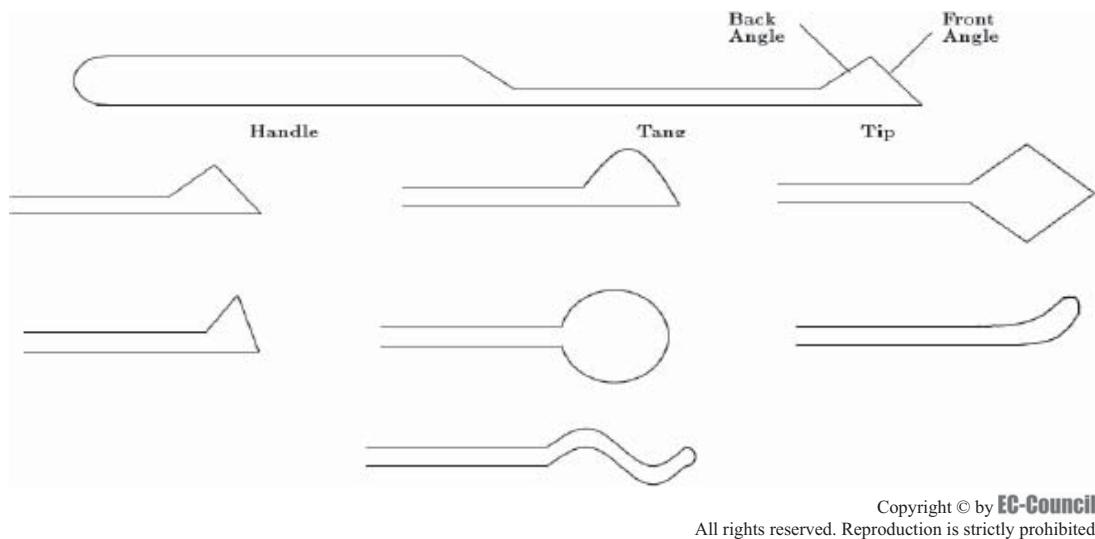
- Fingerprints can be faked easily. Dirty fingers can disturb the matching process. Some scanners need the proper placement of fingers for verification.
- Face recognition systems can be tricked by masquerading techniques such as hats, beards, sunglasses, and facemasks.
- Hand geometry algorithms use a limited number of data points, resulting in a higher level of false negatives and false positives than other types of biometrics.
- Retinal systems can be falsified when there is no beam of light illuminated into the eyeball at a fairly close distance.
- Some users object to vascular pattern technology that uses infrared light.
- Voice dynamics is prone to inaccuracy as it relies on the production of a “voice template” that is compared with a recorded voice.

**Faking Fingerprints** Following are the steps involved in faking fingerprints:

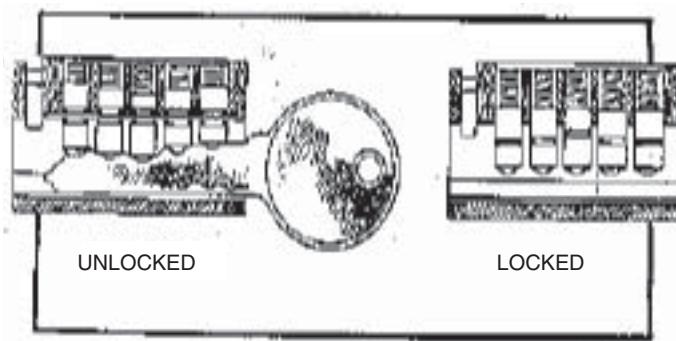
1. Identify the original fingerprints that are going to be forged. Glasses, doorknobs, and glossy paper can be good sources to obtain fingerprints of the target.
2. Sprinkle the fingerprint with colored powder so that it sticks to the fat. Latent fingerprints are nothing but fat and sweat on the surface used by the target.
3. Scan the fingerprint.
4. Use a professional image editor to work on the scanned image. It is necessary to get the exact image of the fingerprint to use as a mold from which a dummy is made.
5. Make a print of the image on a transparency sheet using a laser printer. Add wood glue to one of the prints on the transparency sheet.
6. Add a small drop of glycerin to help in the process of making the dummy. Use a roller for letterpress printing.
7. After the glue dries up, pull it off of the transparency and cut it to finger size.
8. Glue the dummy onto the user’s finger with theatrical glue and use this finger in the biometric scanner.

### **Lock Picking**

Lock picking is the technique of unlocking a lock without the use of its key. An attacker can pick a lock to get direct unauthorized access to an area by using this technique. Tools used for lock picking are called lock picks, and they can include simple tools such as hairpins, safety pins, and blank keys. Lock picks are used to manipulate or operate the internal pins of a lock. A pick is inserted into the key hole and rotated systematically to set the internal pins to the correct position, releasing the lock. With the right set of lock picking tools, every lock can be picked. Lock picks used for releasing pin-tumbler locks include the tools in Figure 2-3.



**Figure 2-3** This illustration shows different kinds of lock picks.



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

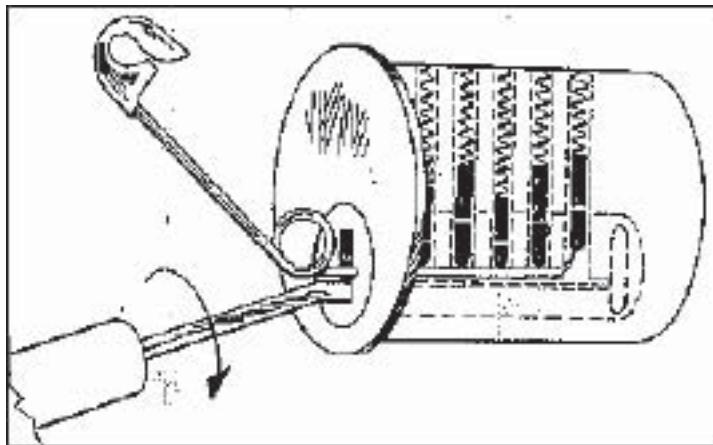
**Figure 2-4** This illustration shows the locked and unlocked positions of a pin-tumbler lock.

**Picking a Pin-Tumbler Lock** The following steps are used for unlocking or releasing a locked pin-tumbler lock, illustrated in Figure 2-4, without using valid keys.

- *Step 1:* Slip into the lock, as shown in Figure 2-5, by using a tension wrench and a safety pin. Bend the pin so that it's straight and can be inserted into the lock. First, insert the safety pin into the lock. When the pin has reached the deepest part of the lock, slowly raise it toward the last tumbler and hold it as shown in Figure 2-5. Insert the tension or torque wrench into the lock and rotate it. A gentle sound will be heard when the tumbler breaks.
- *Step 2:* Keeping the tension wrench with the same pressure, perform the steps explained in step 1 again on the next tumbler. It will be a little easier this time. See Figure 2-6.
- *Step 3:* Apply the same procedure for all the remaining tumblers, holding the tension wrench with even pressure. The lock is released when all the tumblers are broken. See Figure 2-7.

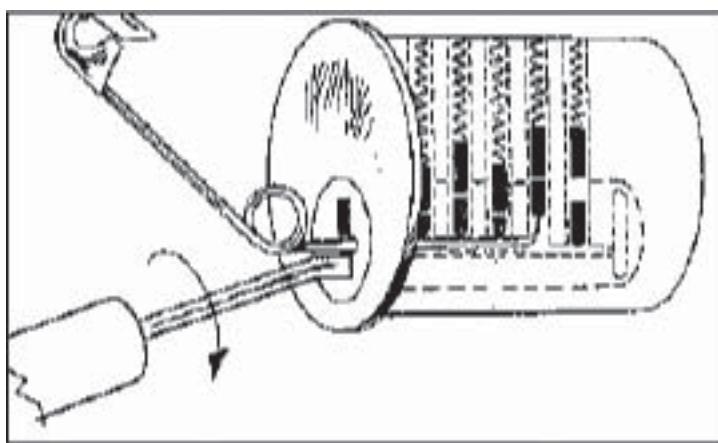
### **TEMPEST Monitoring**

TEMPEST is the abbreviation for Transient Electromagnetic Pulse Emanation Surveillance Technology or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions. This technology deals



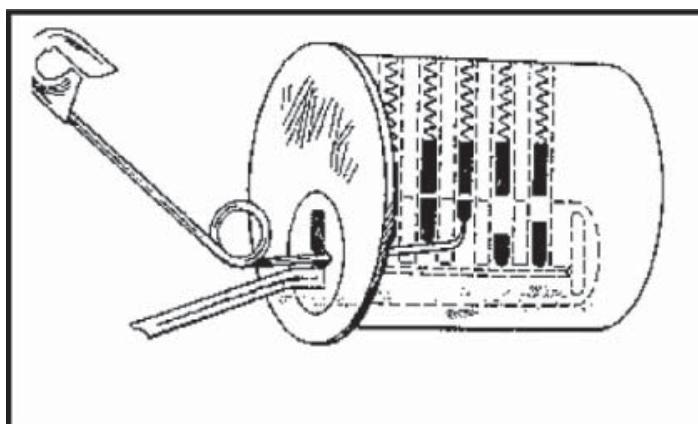
Copyright © by EC-Council  
All rights reserved. Reproduction is strictly prohibited

**Figure 2-5** Step one is to break the first tumbler.



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

**Figure 2-6** Break the second tumbler while keeping the same pressure on the tension wrench as in step one.



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

**Figure 2-7** Continue to keep the same pressure on the tension wrench while the rest of the tumblers are broken.

with information that is unintentionally leaked out of computers through energy emissions. These emissions are known as CE, or *compromising emanations*, and they can occur as:

- Electromagnetic fields set free by elements of plaintext processing equipment
- Text-related signals coupled to cipher, power, signal, control, or other BLACK lines through common circuit elements such as grounds and power supplies or inductive and capacitive coupling
- Sound waves emanating from mechanical or electromechanical devices

### Sources of TEMPEST Signals

- *Functional sources*: Functional sources such as switching transistors, oscillators, signal generators, synchronizers, line drivers, and line relays generate electromagnetic energy.
- *Incidental sources*: Machinery that is not designed to generate electromagnetic energy, such as electro-mechanical switches and brush-type motors, can be an incidental source of CEs.

**Types of Compromising Emanations** The types of CE are RED baseband signals, modulated spurious carriers modulated by RED baseband signals, and impulsive emanations.

RED baseband signals are the most easily recognized CE. This type of CE can be introduced into electrical conductors connected to circuits with the same impedance and power source as circuits processing RED baseband signals. This type can also be introduced into an escape medium by capacitive or inductive coupling.

Modulated spurious carriers are the result of modulation of a carrier by RED data. The carrier could potentially be a parasitic oscillation generated in the equipment.

Impulsive emanations are caused by very fast mark-to-space and space-to-mark transitions of digital signals.

## Physical Security Checklists

It is very important to have a checklist for physical security. Checklists ensure that every aspect of a company's security policy is covered and accounted for. These lists can be given to the appropriate security personnel and to employees who deal with the specific checklist areas.

Checklists are needed for the following common vulnerable aspects of a company's physical security:

- Company surroundings
- Premises
- Reception
- Servers
- Workstation areas
- Wireless access points
- Equipment such as fax machines and removable media
- Access controls
- Computer equipment maintenance
- Wiretapping
- Remote access

### Physical Security Checklist: Company Surroundings

Checklist for securing a company's perimeter:

- Fences
  - Fences can be used as a deterrent.
  - A high-security installation must contain two fences—an outer and inner fence, each between 15- and 30-feet high.
- Gates
  - Gates are an additional level of protection.
  - Gates can be used to filter visitors that are coming in and leaving.
  - Electronic gates add an extra layer of security because they cannot be opened manually.

- Walls
  - Walls are used to separate various areas.
  - Guard dogs behind the walls of a facility can provide additional protection.
- Guards
  - Guards are of two types: in-house (company-paid) guards and contract guards.
  - Contract guards are less secure since they do not work for the company, and if they commit a mistake they may simply be transferred to another site. In-house guards know the facility better and have more to gain by doing a good job, so they are more security conscious.
- Alarms
  - Alarms can be used to indicate a problem with machinery, water levels, chemical spills, tornadoes, or fires.

### ***Physical Security Checklist: Premises***

Checklist for protecting the company's premises:

- AC duct access
  - There is a chance of an intruder getting in through such ducts.
- CCTV cameras with monitored screens and video recorders
  - CCTV cameras help in analyzing the events of the day, in case something suspicious happened.
  - CCTV cameras provide real-time monitoring of the premises. Their presence can act as a deterrent.
  - The only drawback of these cameras is that their usefulness depends on the personnel monitoring them.
- Intruder detection systems
  - Intruder systems can be placed in secure locations such as the server room, laboratory, or testing room.
  - Examples are interior sensors and ultrasonic detectors.
  - Interior motion sensors can be used to detect an intruder inside the premises.
  - Ultrasonic detectors operate at very high frequencies that the human ear cannot hear.
  - The difference between an intruder detection system and other warning systems is that when the alarm for the intruder system is triggered, it means someone unauthorized has gained entry to an area or is trying to get in. When other warning systems are triggered, it sends a warning to people about other types of problems—such as fire or equipment malfunction.
- Panic buttons
  - These buttons/alarms are placed throughout a company to signal various dangers. Two examples include the button a bank teller may have to warn of a robbery, or a button a receptionist might have to warn security of a dangerous person trying to gain admittance.
  - These buttons signal if there is a fire or other type of mishap in the vicinity.
- Burglar alarms
  - Some instruments are fitted with burglar alarms. If anyone tries to remove them physically or touch them, they send a signal in the form of a loud siren, thus alerting security.
- Window and door bars
  - Window and door bars are the most basic method of securing a room.
  - This type of security has been in use for centuries.
- Deadlocks
  - Deadlocks are also called deadbolts. These might have either have a turning knob on one side and a key lock on the other side, or it can have a key lock on both sides depending on the specification.

### **Physical Security Checklist: Reception**

Reception is usually a busy area with a large number of people coming and going. This area often has a seating area for visitors and can be of use to a person who wants to learn about the office staff and the company's activities. A person can be seated in the waiting area on the pretext of meeting someone and eavesdrop on the conversations taking place in the reception area.

Following is the checklist for securing the reception area:

- *Seating arrangement:* The seating arrangement for visitors should be at a safe distance from the reception desk so that a person sitting in the waiting area cannot overhear conversations.
- *Loitering policy:* A person sitting in the waiting area for an unusually long period should be questioned. If the person's response cannot be verified (e.g., the individual is waiting for an employee), the person should be asked to leave for security reasons.
- *Files and media:* Files and documents, removable media, etc., should not be kept on or near the reception desk.
- *Access to administrative area:* Reception desks should be designed to discourage attempts by non-staff members to inappropriately gain access to the administrative area.
- *Computer screen visibility:* Computer screens should be positioned in such a way that people near the reception desk are unable to see them easily.
- *Hardware security:* Computer monitors, keyboards, and other equipment at the reception desk should be locked whenever the receptionist moves away from the desk, and should be logged off after office hours.

### **Physical Security Checklist: Server**

The server is the most important component of any network, so it should be given a high level of security. The server room should be well lit. High-end configurations should be used for servers so that they can sustain the overload due to continuous uptime.

Following is the checklist for securing the server:

- *Acceptable use:* Servers should not be used to perform day-to-day activities.
- *Security enclosure:* Servers should be enclosed and locked to prevent any physical movement.
- *Drive access:* Booting from floppy and CD-ROM drives on the server should be disabled, and if possible these drives should not even be on the server.
- *Label use:* Some system administrators label the server and other systems in the server room. These labels sometimes have the operating system's name and hardware specification written on them. This is not wise, as anyone who passes through the server room can get details about the server and other devices. If an attacker sees this information, they do not have to go through the tiresome process of footprinting.
- *Additional systems:* Unnecessary services and subsystems should be removed.
- *Software updates:* Patches and versions should be kept updated.

### **Physical Security Checklist: Workstation Area**

It is common for both large and small companies to have areas where the majority of employees who use computers work. Often each of these employees has a cubicle for an office. Employees need to be educated on such points as how to secure their desktops to prevent any kind of intrusion. Employees like to personalize their workstations as well as their PCs, but they need to be educated on how to secure this personal space. Many people write their passwords, personal information, IP addresses, or telephone numbers on whiteboards, post-it notes, pads, or pieces of paper. This should be discouraged, since attackers can easily obtain this information—as well as critical information regarding the LAN and the company—by going through dumpsters or by other means. Address books, company policies, reminders, and user IDs should be kept away from the reach of others.

Following is the checklist for securing the workstation:

- *CCTV:* Install CCTV cameras with monitored screens and video recorders to monitor the movements of employees.
- *Terminal screen access:* Unmanned/unattended terminal screens should be locked to prevent unauthorized access.

- *Cubicle design:* Workstation cubicles should be designed in such a way that employees cannot see each other's terminal screens.
- *PC movement:* PCs should be locked down to prevent any physical movement.
- *Removable drives:* Removable media drives should be avoided on workstations, if it is possible. Only one workstation per row should have such drives, and that particular workstation should not be used for any other purpose.

### **Physical Security Checklist: Wireless Access Points**

A *wireless access point (WAP)* is a piece of wireless communications hardware that creates a central point of wireless connectivity. Similar to its hardware counterpart hub, the access point is a common connection point for devices in a wireless network. Access points can be used to connect segments of a LAN, utilizing transmit-and-receive antennas instead of ports for access by multiple users of the wireless network. Similar to standard wired hubs, access points are shared bandwidth devices that can be connected to the wired network via a Network Access Medium (NAM), allowing wireless access to a company's network.

The mobility of a wireless network is its biggest disadvantage. If an intruder successfully connects to a firm's wireless access points, they are virtually inside the LAN, just like any other employee of the firm. To prevent such unauthorized access, the wireless access points should be secured.

### **Wireless Security**

**Enabling WEP and WPA/WPA2 on a Wireless Network** These protocols are used to secure wireless networks from eavesdropping. WEP stands for *Wired Equivalent Privacy*. It provides an encryption standard designed for wireless networks. Although it is widely used, it is considered to be inferior to **WPA (Wi-Fi Protection Access)**. The advantage of the WPA/WPA2 protocol is that the encryption keys can be changed as and when needed.

**MAC Address** A MAC (media access control) address can help prevent unauthorized access by illegitimate users because the MAC addresses of legitimate users are registered with the router. Tools that detect MAC address spoofing should be installed on the network to trap intruders.

**End-to-End Encryption** End-to-end encryption is a process that allows data to be transmitted to one particular recipient, making the data secure from eavesdropping over the Internet. This can be done using protocols such as TLS (Transfer Layer Security) and SSH (Secure Shell).

**VPN (Virtual Private Network)** A VPN can be used to transfer critical/sensitive data/information between two users. VPN is a network that functions securely by “tunneling” through larger public networks. The tunneling technology of VPN ensures that the data is not sniffed and is encrypted.

### **Access Point Evaluation**

- Check for rogue access points.
- Change default configuration.
- Install personal firewalls and intrusion detection systems on laptops.
- Scan the OS for any incorrect security configuration.
- Lock down the system with limited user accounts and limited access.
- Disable broadcast of SSID.

Following is the checklist for wireless access points:

- *Encryption:* Encryption should be employed (WEP for open access, and WPA and VPN for better encryption).
- *Passwords:* Access points should be password protected, and passwords should be robust and hard to crack.

## **Physical Security Checklist: Other Equipment**

Following is the checklist for equipment such as fax machines, removable media, etc.:

- Fax machines
  - Fax machines near the reception area should be locked in the absence of the receptionist.
  - Faxes received should be filed properly.
- Telephones
  - Telephones in the reception area should not be left unattended.
  - Proper checks should be carried out to make sure telephones are not wiretapped.
  - Telephones should be locked, requiring a PIN code to unlock for dialing, as well as physically locked by placing a guard on the keypad.
  - Numbers should not be written on the telephone instrument.
- Instrument labels
  - There should not be any labeling of instruments that don't typically have removable media.
- Device accessibility
  - Multifunctional devices such as scanners, fax machines, printers, and copiers should not be easily accessible.
- Modems
  - Modems should not have autoanswer mode unnecessarily turned on.
- Removable media
  - Removable media should not be openly displayed in public places.
  - Physically destroy corrupted removable media, e.g., by burning or shredding.

## **Physical Security Checklist: Access Control**

Access control must be used to prevent unauthorized access to highly sensitive operational areas. Following is the checklist for access control:

- *Separation of work areas*: Every department must have a separate work area to maintain control over access and follow security policies. This also ensures the easy identification of employees and the departments for which they work.
- *Biometric access control*: Biometric access controls should be in place in any highly sensitive operational area.
- *Entry cards*: Entry cards, also called key or access cards, are used to differentiate visitors from employees.
- *Mantraps*: Mantraps are automatic devices for securing a sensitive location in an organization from trespassers. Mantraps are used for access control to high-security areas.
- *Employee sign-in procedures*: Employee sign-in procedures are used to record information regarding an employee's arrival at a lab, departments they have been to, and their exit times.
- *Identification badges*: These are used for internal verification and identification of employees.

## **Physical Security Checklist: Computer Equipment Maintenance**

- *AMC companies*: Many large firms outsource their computer maintenance to Annual Maintenance Contract (AMC) companies.
  - AMC company personnel are summoned in case of any hardware failure or system complaints.
  - AMC company personnel should not be left alone when they come to the company for maintenance.
  - The toolboxes and baggage of the AMC company personnel should be thoroughly scanned for any suspicious materials that could compromise the security of the firm.
- *Maintenance personnel*: Appoint a person who will be responsible for looking after the maintenance of computer equipment.
- *Equipment storage*: Computer equipment in warehouses should also be accounted for.

## **Physical Security Checklist: Wiretapping**

There are different types of legal means to record conversations. If either party involved in the conversation has knowledge about the recording, it is called a one-party state. If both parties have knowledge about the recording, it is called a two-party state. It is illegal to record a conversation without the consent of either party. This is called wiretapping, and can be performed by listening through a third telephone, or by means of wiretapping technologies that can detect phone conversations through the telephone wires.

Following is the checklist to secure against wiretapping:

- *Inspection:* Inspect all data-carrying wires routinely.
- *Shielding:* Protect wires using shielded cables.
- *Conceal wires:* Never leave wires exposed.

## **Physical Security Checklist: Remote Access**

Remote access is an easy way for an employee to work from any location outside the company's physical boundaries. It is easy for an attacker to access the company's network remotely by compromising the employee's connection. Remote access is more dangerous than physical access, as the attacker is not in the vicinity, and there is less likelihood of catching the culprit. Remote access to the company's networks should be avoided, as much as possible.

Following is the checklist for facilitating remote access:

- *Encryption:* The data flowing during remote access should be encrypted to prevent eavesdropping.
- *Access restrictions:* Remote access should be restricted to top employees who have a higher-than-average level of responsibility within the company.
- *Login procedure:* There should be a separate login for remote access, and the password sent to the server for authentication should be encrypted so that it is not visible to sniffers.

## **Tools**

### **Device Lock**

Device Lock is a device control solution to safeguard network computers against internal and external attacks.

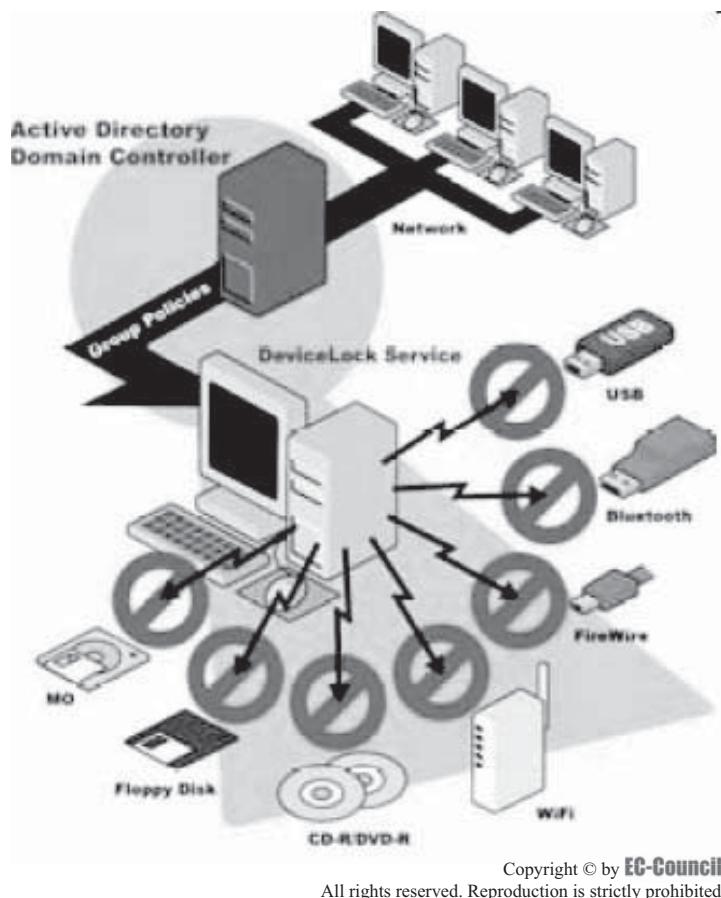
Device Lock will do the following:

- Allow network administrators to lock out unauthorized users from USB ports.
- Allow administrators to control access to devices such as floppies, serial and parallel ports, magneto-optical disks, CD-ROMs, ZIPs, and USBs.
- Generate a report concerning the permissions that have been set.
- Provide a level of precision control over unavailable device resources.
- Grant users temporary access to USB devices when there is no network connection.
- Control the system remotely using the centralized management console.
- Generate a report displaying the USB, Firewire and PCMCIA devices.
- Set devices to read-only mode.
- Give a complete log of port and device activity such as uploading and downloading made by users and filenames in the standard Windows event log.
- Provide a report displaying the USB, Firewire and PCMCIA devices currently connected to computers, as well as those that were previously connected.

Figure 2-8 shows how Device Lock fits into a network.

### **Lock-Picking Tools**

- *Lock-picking set:* These tool sets include a variety of 14 tools made with electroless nickel plating. Sets often contain:
  - Lock picks
  - A broken-key extractor
  - Tension tools



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

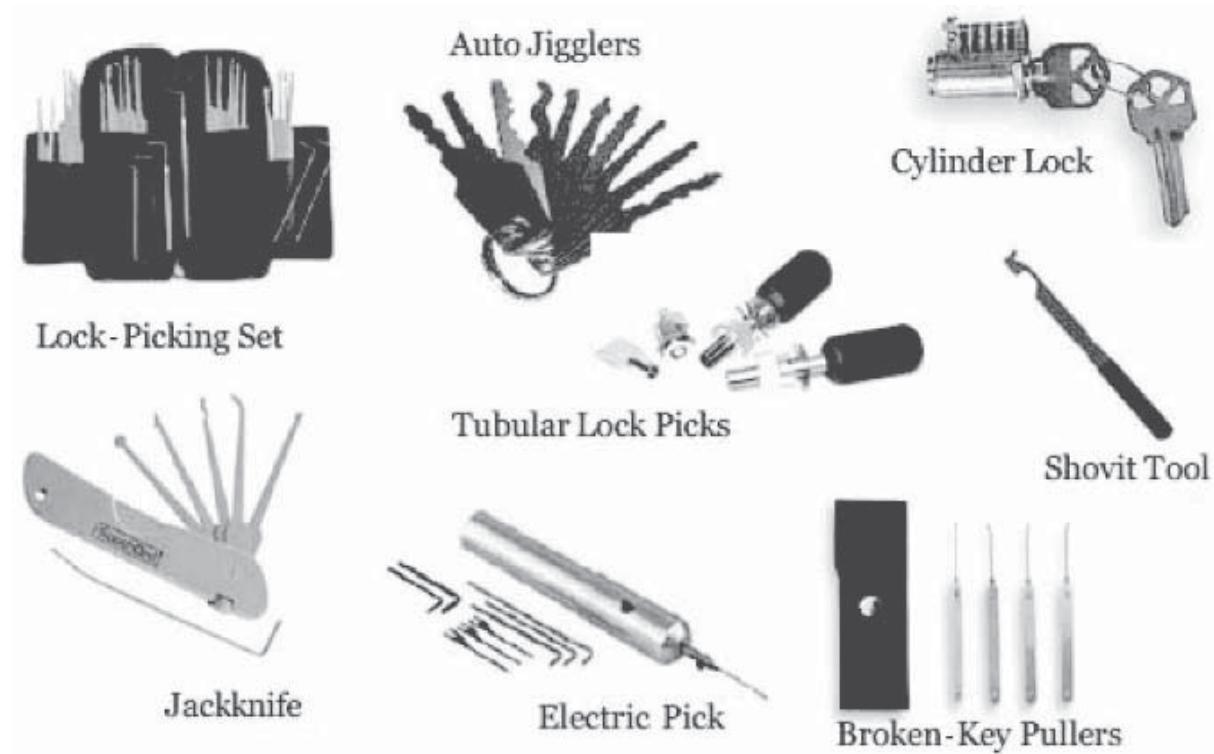
**Figure 2-8** Device Lock protects network computers against attacks.

- *Auto jiggers*: This stainless steel tool is designed for foreign and domestic cars and trucks.
- *Cylinder lock*: If a valid key is inserted in the lock, it can lift the pin tumblers, permitting the cylinder plug to rotate and open the door.
- *Jackknife*: A jackknife is made up of a small handle that can be opened to reveal lock picks and a tension tool.
- *Tubular lock picks*: These tools help to tune the needle pressure of a lock with high spring pressure when attempting to pick it.
- *Shovit tool*: This tool can unlock many door locks. It works by pushing the device and forcing the plunger. It is one of the easiest and cheapest ways of lock picking.
- *Electric pick*: This tool uses a 3-volt electrical system powered by two conventional alkaline or Ni-Cad C-cell batteries. It should contain:
  - Picking needles
  - Tension tools
  - Adjustment wrenches
  - Broken-key pullers

See Figure 2-9 for pictures of these tools.

### Laptop Security Tools

**Laptop Steel Cable Locks** Steel cable locks protect laptops from theft by securing them to something that is not easy to move. The cables do not depend on the built-in security slots that many manufacturers are now



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

**Figure 2-9** This is an assortment of lock-picking tools.

adding to their laptops. The cables can also be used with other devices by using different add-on adapters. Keying options: keyed-alike, keyed-different, or master-keyed are available.

**Laptop Tie-Down Bracelets** Tie-down bracelets secure laptops with a locking post that is secured to a desk or table. It can be locked by turning a key. Keys must be kept in a safe place, away from the computer.

**Portable Laptop Carts** Portable laptop carts provide mobile security for storing multiple laptops. Electrical units allow laptops to be recharged. Various models are designed to secure 30, 24, 18, and 15 laptops, respectively.

### Tracking and Recovery Tools

Lost or stolen laptops are recovered by a variety of tracking and recovery techniques.

**Track Stick GPS Tracking Device** The Track Stick GPS Tracking Device is a 1 MB Memory Stick that can store months of travel information. It has the capability to record the following:

- Its own time
- Its own date
- Its own speed
- Its own direction
- Its own altitude

The Stick keeps track of travel information and records its history. The output comes in the following formats:

- RTF (Detailed text file with .html map links)
- XLS (Microsoft Excel spreadsheets)

- HTML (Web page with graphics and maps)
- KML (Proprietary Google Earth file)

The Track Stick receives signals from 24 satellites orbiting the earth. It can estimate a location anywhere on the planet by using 3-D mapping technology. Each location can be pinpointed to within 15 meters.

**Laptop Tracker—XTool Computer Tracker** XTool Computer Tracker uses a signature software-based transmitter to send a signal to the Signal Control Center by means of telephone or Internet connection. The signal sent from the stolen piece of software enables the user to reboot the system when it starts and when the IP address changes. Every signal holds the telephone number or the IP address that is used by the transmitted signal. Stolen equipment can be reported to the control center, which can then trace the stolen equipment. The user also has the facility to delete files remotely, even if the system is mobilized.

The following are the platforms it supports:

- All Windows platforms including XP
- All Macintosh platforms including OS X

The following are some of the features of XTool Computer Tracker:

- *Undetectability*: Some antivirus programs can detect XTool, but it does not affect the performance of the system.
- *Compatibility*: The tool can be upgraded or downgraded as needed, without affecting the computer's security.
- *Smart adaptability*: The tool is adaptable to a new environment or configuration, simultaneously ensuring a computer signal every time from anywhere.
- *Global monitoring capability*: XTool has the capability of worldwide monitoring coverage.
- *Global recovery capability*: Worldwide monitoring and recovery services help the computer owner search for stolen equipment across the globe by contacting various authorities, phone companies, and Internet service providers. The tool keeps track of the computer's footsteps 24/7.

**Ztrace Gold** Ztrace Gold is a security application that connects with a server (ZSERVER) every time an Internet connection is established. If a laptop equipped with Ztrace Gold has been reported missing, a recovery team identifies its physical location and coordinates with local law enforcement to retrieve it. Ztrace Gold is undetectable and cannot be removed from a laptop's hard drive.

**The CyberAngel** The CyberAngel security application is enabled when a laptop user cannot correctly enter an authentication password. When authentication fails, the application immediately encrypts sensitive data—stored on a separate area of the hard drive—and makes it invisible to the user. The CyberAngel then sends a signal to a security monitoring center that checks to see if the laptop has been reported stolen. The CyberAngel uses Wi-Fi technology to physically locate the computer, and a recovery team coordinates with law enforcement to recover it.

**ComputracePlus** ComputracePlus tracks large numbers of computers, including remote and mobile assets. It provides detailed reports for every computer with an Internet connection. This is useful for:

- Tracking machines as they change hands or move around within an organization
- Reducing and deterring theft problems
- Recovering lost or stolen computers

**STOP (Security Tracking of Office Property) Plate** STOP plates (Figure 2-10) use a barcode and an indelible tattoo to mark laptops and other equipment with an identifier that can be traced anywhere in the world. The barcode is included in an international database that allows a recovery team to quickly trace and recover a stolen laptop. This barcode also allows companies to track their internal inventories with a STOP handheld scanner.

The following are some of the features of STOP plates:

- STOP's patented marking system prevents theft by eliminating resale value.
- The STOP system helps in recovery and boasts a 90% reduction in equipment loss.



**Figure 2-10** STOP plates use a barcode and an indelible tattoo to ensure laptop identification.



**Figure 2-11** TrueCrypt creates encrypted virtual volumes that cannot be detected.

- An identification number on a security plate matches the equipment's serial number for a positive ID.
- They are strongly constructed.

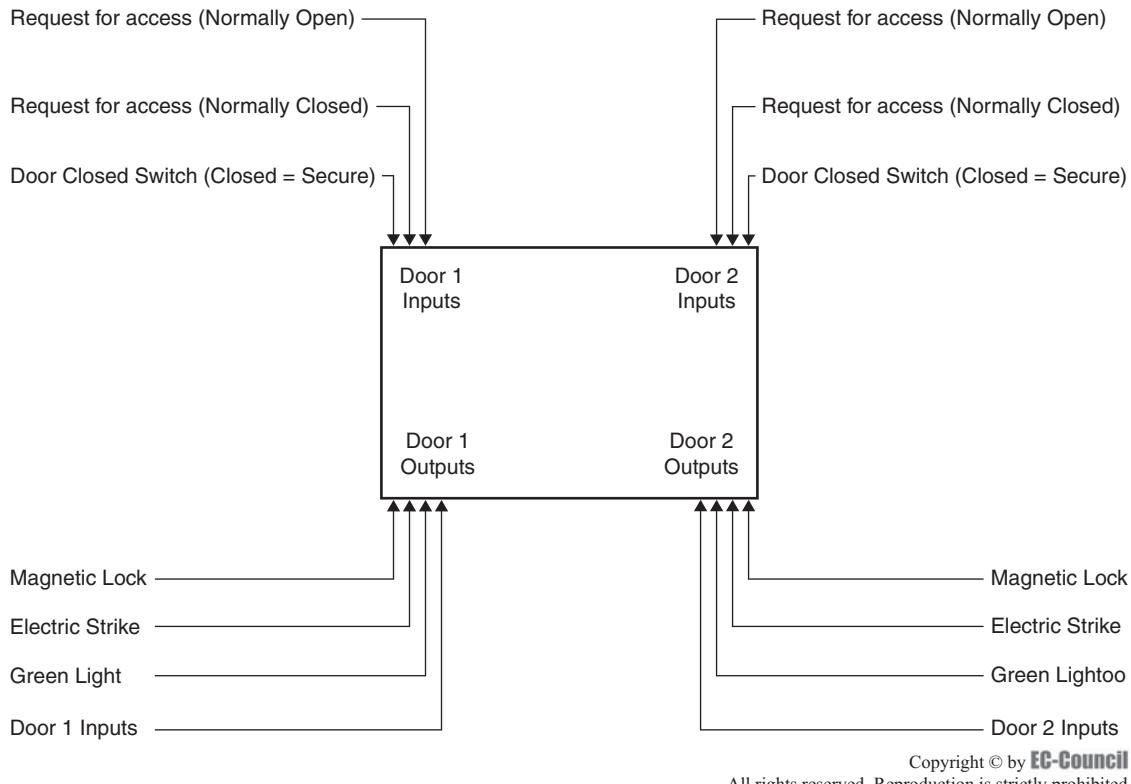
## Encryption Tools

### **TrueCrypt**

TrueCrypt is free open-source disk encryption software for Windows XP/2000/2003 and Linux. Figure 2-11 shows the startup screen for TrueCrypt.

The following are some of the features of TrueCrypt:

- This application provides automatic, real-time encryption of entire hard disks or other storage devices such as USB flash drives.
- TrueCrypt creates encrypted virtual volumes that cannot be detected even if an intruder has the user's password.
- TrueCrypt uses AES-256, Blowfish (448-bit key), CAST5, Serpent, triple DES, and Twofish algorithms.



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

**Figure 2-12** The two doors of a mantrap must be accessed individually.

## Mantrap

A mantrap offers alternate access for materials and people with different levels of security clearance. It has two doors with an airlock between them. A single door can be opened at a time, provided authentication is confirmed for both doors.

Mantraps restrict access to secure areas while providing an effective means to physically detain unauthorized persons until security provides clearance. Once individuals pass through the first door, they are not allowed to go through the second door until the first one is closed. Figure 2-12 illustrates a mantrap.

This system offers protection in three ways:

1. It is difficult to force entry through a single door, let alone two doors.
2. It provides time to assess the person inside the mantrap prior to letting him or her pass through the second door.
3. It permits only one person in at a time.

In huge areas such as government installations and large financial institutions, as many as 99 doors can be installed to form a massive mantrap system. The programmable character of such a massive system allows designers to create a complex space that contains many rooms and safe areas.

---

## Chapter Summary

- Security officers, who would be accountable for any security breach in a firm, should be employees.
- Physical security should be checked for vulnerabilities.
- Device Lock is a device control solution to safeguard network computers against internal and external attacks.
- All organizations should have a checklist for physical security as a part of their security check-ups.

- Natural disasters cannot be prevented, but the loss can be decreased substantially if a security policy is properly implemented.
- Employees need to take responsibility for handling security issues.
- Biometrics can be used as an effective access control to restricted areas.
- Implementation of a good physical security policy and countering social engineering tactics are the two biggest challenges for physical security.

---

## Review Questions

1. Name four physical security threats.

---

---

---

---

2. What are compromising emanations, or CEs?

---

---

---

---

3. What does the checklist for securing the company surroundings include?

---

---

---

---

4. Name three methods for securing servers.

---

---

---

---

5. What is the difference between a smart card and a security token?

---

---

---

---

6. What are the four different types of security personnel?

---

---

---

---

7. Name three different types of biometric authentication devices and explain their operation.

---

---

---

---

8. How can biometric authentication devices be compromised?

---

---

---

---

9. What is a mantrap?

---

---

---

---

10. What is encryption?

---

---

---

---

---

## Hands-On Projects



1. Perform the following steps:
  - Navigate to Chapter 2 of the Student Resource Center.
  - Read MIT Guide to Lock Picking.pdf.
2. Perform the following steps:
  - Navigate to Chapter 2 of the Student Resource Center.
  - Read Physical Security and Operations.pdf.
3. Perform the following steps:
  - Navigate to Chapter 2 of the Student Resource Center.
  - Read PHYSICAL SECURITY.pdf.
4. Perform the following steps:
  - Navigate to Chapter 2 of the Student Resource Center.
  - Read Security Standards Physical Safeguards.pdf.
5. Perform the following steps:
  - Navigate to Chapter 2 of the Student Resource Center.
  - Read secure.pdf.

*This page intentionally left blank*

# Evading IDS, Firewalls and Detecting Honeypots

## Objectives

After completing this chapter, you should be able to:

- Understand intrusion detection systems (IDS)
- Detect an intrusion
- Name the types of IDS
- Detect an attack on an IDS
- Evade an IDS
- List tools to evade an IDS
- Install an intrusion prevention system (IPS)
- Identify a firewall
- Bypass a firewall
- List the tools used to bypass a firewall
- Understand honeypots
- Detect honeypots

## Key Terms

**Anomaly detection** an intrusion detection technique that uses a database of anomalies to detect possible intrusions

**Baseline** a measurement and rating of the performance of a network in real-time situations to establish normal network activity

**Firewall** a software program or hardware device that protects the resources of a private network from users on other networks

**Honeypot** a computer or virtual appliance, set up as a vulnerable system, designed to detect, deflect, or in some manner counteract attempts by unauthorized individuals to penetrate a network system; this preventive measure is used to learn the language of attackers and other intruders, and to adopt security measures in keeping with their intrusion tools and techniques

**Host-based intrusion detection system** an intrusion detection system (IDS) that analyzes a specific system for signs of intrusion on the computer it is installed on

**Intrusion detection system (IDS)** software that inspects all inbound and outbound network activity

**Intrusion prevention system (IPS)** any device that uses access control to guard systems from attacker misuse

**Log file monitor (LFM)** software that monitors log files created by network services

**Network-based intrusion detection system (NIDS)** a system that checks every packet entering a network for the presence of anomalies and incorrect data

**Protocol anomaly detection** an intrusion detection technique that searches for the anomalies specific to a particular protocol

**Signature recognition** a technique that attempts to identify events that indicate an abuse of a system

**System integrity verifier (SIV)** software that monitors system files to determine whether they have been changed by an intruder

---

## Case Example

eGlobal Bank is a reputable bank in New York City with a large number of companies and individuals as customers. In addition to regular banking services, the bank began offering a number of online services that included online bill payment, transaction of money through credit cards, and other online transactions.

Recently, Web hacking attacks on institutions in the financial sector have increased rapidly. These include attacks that access the personal information, credit card details, passwords, and bank account details of bank customers.

Due to the growth of such incidents, eGlobal Bank made the security of its banking operations a top priority. The bank had basic experience in security, so it had a firewall installed by a third party. The bank believed that its banking sector was completely safe from the vulnerabilities of Web attacks.

A few months later, bank officials were taken aback by the news that their servers had been hacked and sensitive information on thousands of customers had been stolen.

How did the attacker access the servers despite the installation of a firewall?

---

## Introduction to Evading IDS, Firewalls, and Detecting Honeypots

This chapter focuses on evading IDS, firewalls, and honeypots, security features that administrators deploy to protect their networks. It covers each of these features and the security issues involved with each.

---

## Introduction to Intrusion Detection Systems

Attackers are always on the prowl to compromise networks. This poses a major threat to a company's internal network.

One of the simplest ways of preventing attackers from compromising a network is to customize its settings. Customization of network settings gives network administrators an efficient means of monitoring network traffic. Administrators can also put restrictions on the data and information exchanges taking place over the network to prevent unknown and unauthenticated users from accessing it.

It is also necessary to understand the importance of continuous monitoring. Having a firewall or intrusion detection system on a network does not make the network secure unless there is continuous monitoring of the exchange of data information and network traffic. System and network administrators must be thoroughly trained to track log files, look for suspicious signatures, and maintain a database of weekly alerts. This allows them to track events that have occurred over a specific span of time. This information gives systems personnel the ability to deal with intrusions, attacks, or threats imposed on the company's network. Attackers always find new ways to elude the defensive mechanisms of a network. Therefore, the victim of a particular attack must be aware of the tools and techniques that the attackers employed to compromise the network. This helps administrators develop techniques and methods of blocking attackers, as well as trace the origin of the attack.

Today, there are many exploits that facilitate the infiltration of computer networks. However, there are several mechanisms that assist administrators in preventing these exploits from materializing. The following are the four main mechanisms for exploit prevention:

- **Intrusion detection system (IDS):** inspects all inbound and outbound network activity. The IDS identifies any suspicious pattern that may indicate an attack that could compromise the system. The IDS acts as a security check on all transactions that take place in and out of the system. This allows the user to keep a close check on the authenticity and reliability of the activity that is taking place on the network.

- **Intrusion prevention system (IPS):** can be any device that uses access control to guard systems from attacker misuse. IPS is treated as an enhancement of IDS because it not only detects an intrusion, but also reacts to prevent it from succeeding.
- **Firewall:** is a software program or hardware device that protects the resources of a private network from users on other networks. A firewall acts as a wall around the network that allows only authenticated users to access network resources. This restricts attackers (unauthenticated users) from entering the network by denying them access. Today, most organizations rely heavily on firewalls for their internal security but there are many ways by which an attacker can bypass them.
- **Honeypots:** are computers or virtual appliances, set up as vulnerable systems, designed to detect, deflect, or in some manner counteract attempts by unauthorized individuals to penetrate a network system. This preventive measure is used to learn the language of attackers and other intruders, and to adopt security measures in keeping with their intrusion tools and techniques. The goal of setting up a honeypot is to divert an attack to a softer target and allow that system to be probed, attacked, and potentially exploited. By having honeypots on the network an administrator can gain enormous amounts of information about how a malicious hacker can gain access to systems. Security improvements can occur by knowing the tools that intruders use. This data allows system administrators to build countermeasures against these activities.

## Intrusion Detection System (IDS)

James Anderson, in his paper published in 1980, “Computer Security Threat Monitoring and Surveillance,” suggested a method to monitor packets passing through computer networks. It was in this paper that he introduced the concept of intrusion detection. Since then, several significant developments in IDS technology have taken place. This paper raised issues regarding misuse and the need to detect misuse in conjunction with the changes that were taking place. Anderson’s work in data auditing has had a great impact on the auditing subsystems of almost all operating systems. Anderson’s hypothesis laid the groundwork for intrusion detection system design and development. His work marked the beginning of host-based intrusion detection and IDS in general.

An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, including both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). An IDS uses vulnerability scans to assess the security of a computer system or network.

### IDS Placement

An IDS plays a key role in monitoring hosts or computer networks. It can target unknown attacks in conjunction with other network devices. It can be placed on the network at a point where it can track shared entry or exit points. At times it comprises more than one installation running on more than one system.

IDS software monitors the requests made by internal or external networks. Figure 3-1 represents a setup of dedicated machines with an IDS. An IDS protects the network by securing it from illegitimate sources.

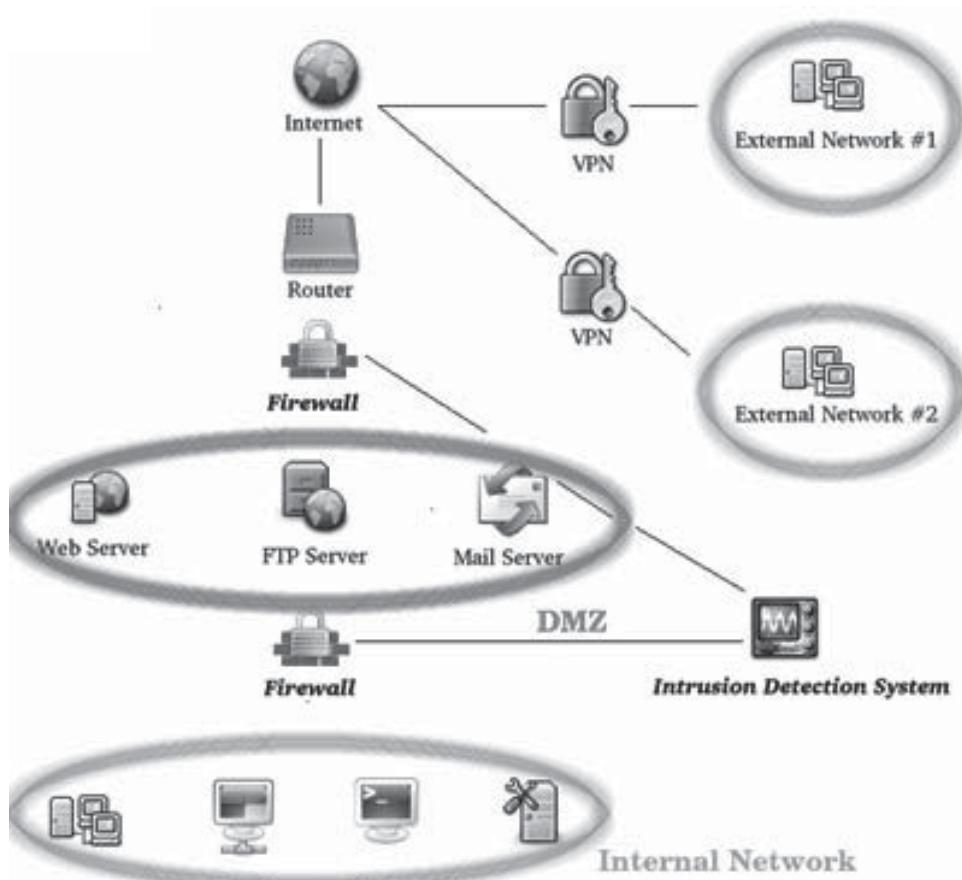
### Intrusion Detection Techniques

The following sections describe some of the ways to detect an intrusion.

**Signature Recognition** *Signature recognition* is also known as misuse detection. It tries to identify events that indicate an abuse of a system. It is achieved by creating models of intrusions. Incoming events are compared with intrusion models to make a detection decision. While creating signatures the model must detect an attack without disturbing the normal traffic on the system. Attacks, and only attacks, should match the model or false alarms will be generated.

The simplest form of signature recognition uses pattern matching to compare the network packets against binary signatures of known attacks. A binary signature may be defined for a specific portion of the packet, such as the TCP flags.

Signature recognition can detect known attacks. However, there is a possibility that other matching packets might represent the signature, triggering bogus signals. Signatures that are formed improperly may also trigger bogus signals. In order to detect misuse, the number of signatures required is huge. The more signatures, the more attacks can be detected. Traffic may incorrectly match with the signatures however, reducing the performance of the system.



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

**Figure 3-1** An IDS protects the network by securing it from illegitimate sources.

Network bandwidth is consumed with the increase in the signature database. As the signatures are compared against those in the database, there is a probability that the maximum number of comparisons cannot be made, resulting in certain packets being dropped.

Virus attacks such as Nimda have created the need for multiple signatures for a single attack. Changing a single bit in some attack strings can invalidate a signature and create the need for an entirely new one.

Despite problems with signature-based intrusion detection, such systems are popular and work well when configured correctly and monitored closely.

**Anomaly Detection** *Anomaly detection* differs from the signature recognition model in that it is based on heuristics or behavioral rules derived from a baseline established during normal network operations. The model consists of a database of anomalies or out of the ordinary activities. Any event that has a match in the database is considered an anomaly. Any deviation from normal use is labeled an attack. Creating a model of normal use, called a baseline, is the most difficult task in creating an anomaly detector. The *baseline* is a measurement of the performance of a network in real-time situations to establish normal network activity.

In the traditional method of anomaly detection, important data are kept for checking variations in network traffic for the model. However, in reality there is less variation in network traffic and too many statistical variations, making these models imprecise; some events labeled as anomalies may only be irregularities in network usage.

These models should be trained on the specific network that is to be policed if they are to be effective.

**Protocol Anomaly Detection** *Protocol anomaly detection* is based on the anomalies specific to a protocol. This model has recently been integrated into the IDS model. It identifies the TCP/IP protocol-specific flaws in a network.

Protocols are created with specifications, known as RFCs, for dictating proper use and communication. New attack methods are being discovered that violate protocol standards.

The pace at which the malicious signature attacker is growing is incredibly fast. Therefore the signature database must be updated frequently to detect attacks. But network protocols, in comparison, are well defined and changing slowly. A protocol anomaly detector can identify new attacks without requiring new signature updates.

Protocol anomaly detectors are different from the traditional IDS in how they present alarms. The best way to present alarms is to explain which part of the state system was compromised. For this, the IDS operators must have a thorough knowledge of the protocol design. Protocol anomaly detectors focus on specific protocols, allowing operators to easily see the compromised area.

## Types of Intrusion Detection Systems

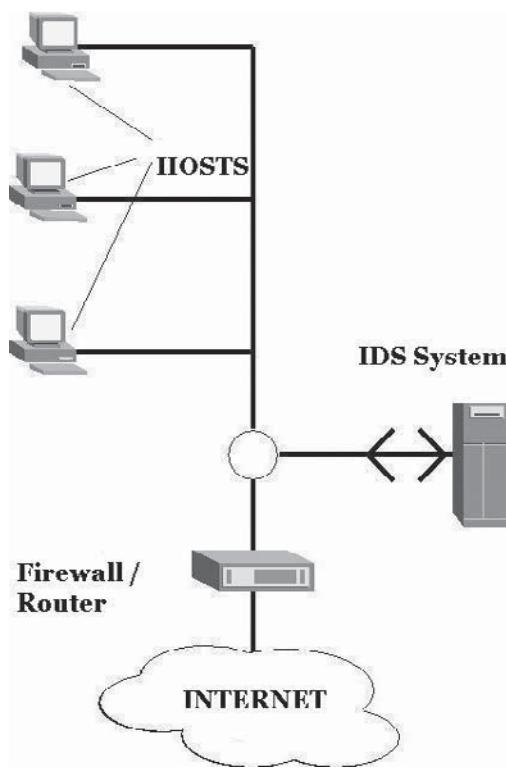
### **Network-Based Intrusion Detection System (NIDS)**

A **network-based intrusion detection system (NIDS)** (Figure 3-2) checks every packet entering the network for the presence of anomalies and incorrect data. Unlike firewalls, which are confined to the filtering of data packets with vivid malicious content, the NIDS checks every packet thoroughly. A NIDS captures and inspects all traffic regardless of whether it is permitted. Based on the content, an alert could be generated at either the IP or application level. Network-based intrusion detection systems tend to be more distributed than host-based IDS.

The NIDS is basically designed to identify the anomalies at the router and host levels. The NIDS audits the information contained in the data packets and logs information on malicious packets. A threat level is assigned to each risk after the data packets are received. The threat level enables the security team to be on alert.

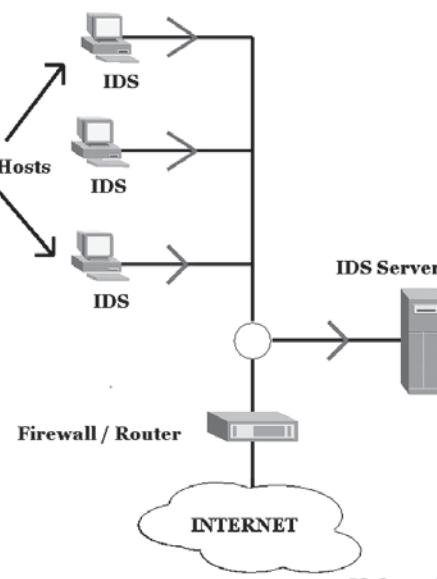
### **Host-Based Intrusion Detection System (HIDS)**

In a **host-based intrusion detection system** (Figure 3-3) the IDS analyzes each system's behavior. The HIDS can be installed on any system, ranging from a desktop PC to a server. The HIDS is more versatile than the NIDS. One example of a host-based system is a program that operates on a system and receives application or operating system audit logs. These programs are highly effective for detecting insider abuses.



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

**Figure 3-2** A NIDS checks every packet for the presence of anomalies.



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

**Figure 3-3** Host-based IDS analyze each system's behavior.

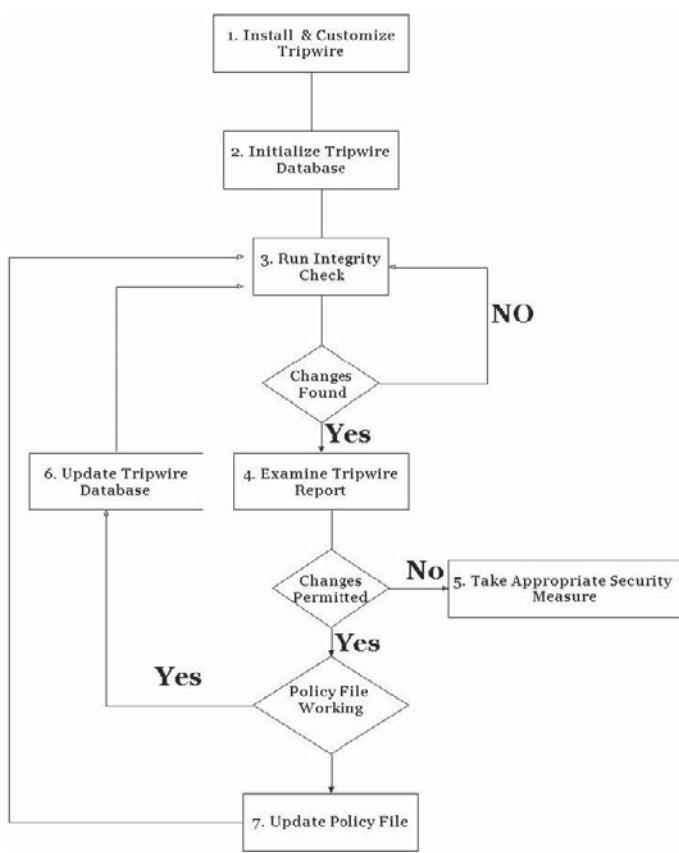
Residing on the trusted network systems themselves they are close to the network's authenticated users. If one of these users attempts unauthorized activity, host-based systems usually detect and collect the most pertinent information promptly. In addition to detecting unauthorized insider activity, host-based systems are also effective at detecting unauthorized file modification. HIDS are more focused on changing aspects of the local systems. HIDS are also more platform-centric. Many focus on the Windows OS, but there are other HIDS for UNIX platforms.

### **System Integrity Verifiers (SIV)**

A *system integrity verifier (SIV)* monitors system files to determine whether an intruder has changed the files. An integrity monitor watches key system objects for changes. For example, a basic integrity monitor uses system files or registry keys to track changes by an intruder. Although they have limited functionality, integrity monitors can add an additional layer of protection to other forms of intrusion detection.

### **Log File Monitors (LFM)**

A *log file monitor (LFM)* (Figure 3-4) monitors log files created by network services. An LFM IDS searches through logs and identifies malicious events. In a manner similar to NIDS, these systems look for patterns in the log files that suggest an intrusion. A typical example are parsers for HTTP server log files that look for intruders who try well-known security holes such as the “phf” attack. An example is the Swatch program.



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

**Figure 3-4** An LFM monitors log files created by network services.

## Indications of Intrusion

### ***System Intrusions***

Certain parameters clearly indicate the presence of an intruder on a system. Attackers modify certain system files and configurations to hide any signs of intrusion. Signs of system intrusion include the following indicators:

- A system fails to identify a valid user
- Active access to unused logins
- Logins during nonworking hours
- New user accounts other than the accounts the administrator has created
- Modifications to system software and configuration files using administrative access, and the presence of hidden files
- Gaps in system audit files, which indicate that the system was idle for that particular time. The gaps may actually indicate that an intruder has attempted to erase the audit tracks.
- The system's performance decreases drastically, consuming CPU time
- System crashes suddenly and reboots without user intervention
- The system logs are too short and incomplete
- Time stamps of system logs are modified to include strange inputs
- Permissions on the logs are changed, including the ownership of the logs
- System logs are deleted
- System performance is abnormal; the system responds in unfamiliar ways
- Unknown processes are identified on the system
- Unusual display of graphics, pop-ups, and text messages observed on the system

### ***File System Intrusions***

By observing the system files, a user can identify the presence of an intruder. System files record the activities of the system. Any modification or deletion of the file attributes or the files themselves is a sign that the system was a target of attack. The following anomalies are indications of file system intrusion:

- New, unknown files or programs on the system
- Changed file permissions: Intruders often attempt to escalate privileges to gain administrative access. Intruders who obtain administrative privileges can change the file permissions.
- Unexplained modifications in file size: All system files should be analyzed
- Presence of rogue suid and sgid files on a Linux system that do not match the master list of suid and sgid files
- Unfamiliar file names in directories, including executable files with strange extensions and double extensions
- Missing files

### ***Network Intrusions***

The following symptoms are general indications of network intrusions:

- Sudden increase in bandwidth consumption
- Repeated probes of a machine's available services
- Connection requests from IPs other than those in the network range
- Repeated attempts to log in from remote machines
- Arbitrary log data in log files, indicating attempts of denial-of-service attacks, bandwidth consumption, and distributed denial-of-service attacks

## Steps to Perform after an IDS Detects an Attack

The following steps should be performed after an IDS detects a possible attack:

- Configure the firewall to filter out the IP address of the intruder. However, this still allows the intruder to attack from other addresses.
- Beep or play a WAV file. This may be anything that draws the attention of the administrator.
- Send an SNMP trap datagram to a management console like HP OpenView or Tivoli
- Send a Windows NT event to the event log
- Send an event to the UNIX syslog event system
- Send e-mail to an administrator to notify him or her of the attack
- Page (using normal pagers) the system administrator
- Save the attack information (time stamp, intruder IP address, victim IP address/port, and protocol information)
- Save a trace file of the raw packets for future analysis
- Launch a separate program to handle the event
- Forge a TCP FIN or RST packet to force a connection to terminate

## Evading IDS

### *IDS Attacks*

IDS are not foolproof. Attackers can spoof from fake addresses to trick the IDS. The attacker can create fake attacks to trigger a reaction from the IDS, making it snap network connectivity for a genuine service. The attacker can attack in a variety of ways.

**Insertion Attacks** Insertion is the process by which an attacker confuses an IDS by forcing it to read invalid packets. In this case, the packets would not be accepted by the system to which they are addressed. If a packet is malformed or if it does not reach its actual destination, the packet is invalid. If the IDS reads an invalid packet, the IDS will become confused.

To understand how insertion becomes a problem for a network IDS, it is important to understand how IDS detect attacks. The IDS employs pattern-matching algorithms to look for specific patterns of data in a packet or stream of packets. For example, IDS might look for the string “phf” in an HTTP request to discover a PHF Common Gateway Interface (CGI) attack. An attacker who can insert packets into the IDS can prevent pattern matching from working. For instance, an attacker can send the string “phf” to a Web server, attempting to exploit the CGI vulnerability, but force the IDS to read “phoneyf” (by inserting the string “oney”) instead. One simple insertion attack involves intentionally corrupting the IP checksum. Every packet transmitted on an IP network has a checksum that is used to verify whether the packet was corrupted in transit. IP checksums are 16-bit numbers that are computed by examining information in the packet. If the checksum on an IP packet does not match the actual packet the host to which it is addressed will not accept it, while the IDS might consider it part of the effective stream.

**Evasion Attacks** An evasion attack occurs when the IDS discards a packet that the host to which it is addressed accepts. Evasion attacks are devastating to the accuracy of the IDS. An evasion attack at the IP layer allows an attacker to attempt arbitrary attacks against hosts on a network, without the IDS ever realizing it. One example of an evasion attack occurs when an attacker opens a TCP connection with a data packet. Before any TCP connection can be used, it must be opened with a handshake between the two endpoints of the connection (a fairly obscure fact about TCP is that the handshake packets can themselves bear data). IDS that do not accept the data in these packets are vulnerable to an evasion attack.

**Denial-Of-Service Attacks** Multiple types of denial-of-service attacks are valid against IDS. The attacker identifies a point of network processing that requires the allocation of a resource, causing a condition to occur that consumes all of that resource. The resources that can be affected by the attacker are CPU cycles, memory, disk space, and network bandwidth. The CPU capabilities of the IDS can also be monitored and affected. This is because the IDS needs half of the CPU cycle to read the packets, detect the purpose of their existence, and then compare them with some location in the saved network state. An attacker can verify the most computationally expensive network processing operations and then compel the IDS to spend all of its time carrying out useless work.

An IDS requires memory for a variety of things. For generating a match for the patterns, the TCP connections should be saved, the reassembly queues should be maintained, and the buffers of the data should be generated. In the initial phase the system requires memory, so that it can read the packets. Memory, which is allocated by the system, is needed for network processing operations. An attacker can verify the processing operations that require the IDS to allocate memory and force the IDS to allocate all of it for meaningless information.

In certain circumstances the IDS stores activity logs on the disk. The stored events occupy most of the disk space. The attackers can occupy a major part of the disk space on the IDS by creating and storing a large number of useless events. This renders the IDS useless in terms of storing real events.

Network IDS record the activity on the networks they monitor. They are competent because networks are hardly ever used to their full capacity; few monitoring systems can cope with an extremely busy network.

Unlike an end system, the IDS must read everyone's packets, not just those sent specifically to it. An attacker can overload the network with meaningless information and prevent the IDS from keeping up with what is actually happening on the network.

**Complex Attacks** Hackers can direct their attacks to bypass IDS through complex procedures. For example, an intruder might send a TCP RST or FIN packet that the NIDS detects but the target system does not. This leads the NIDS to believe that the connection is closed when it is actually open. Because TCP connections are stateful, the intruder could wait a long time before resuming the attack. Although most systems disconnect after a specific amount of time with no activity, the intruder can still cause a wait of several minutes before continuing.

The first attack determines a path so that the packets can be passed as far as the NIDS is concerned. However, it causes the later router to drop the packets, depending on how the router is configured.

If the link is slow for NIDS, the hacker can overload the link with the IP packets having a higher priority and send the TCP FIN as a packet with a low priority. In this case, the queuing process of the router will drop the packets.

Another approach is to consider what the host will or will not accept. For example, different TCP stacks behave differently to slightly invalid input. Typical ways of causing different traffic to be accepted or rejected are to send TCP options, cause timeouts to occur for IP fragments or TCP segments, overlap fragments or segments, or to send slightly wrong values in TCP flags or sequence numbers.

**Obfuscation** A tool called an obfuscator is sometimes used to convert a straightforward program into one that works the same way but is much harder to understand. An IDS may find it difficult to detect a malicious program that has been run through an obfuscator because the IDS compares the malicious program to the signatures in its database.

**Desynchronization** Desynchronization uses SYN packets in two different ways: postconnection and preconnection.

#### Postconnection SYN

Attackers do not try to directly deceive an intelligent sniffer or an IDS because they keep track of the TCP sequence numbers. For this technique to work efficiently, attackers first desynchronize the sniffer or IDS. The attack on the sniffer or IDS can be implemented by sending a postconnection SYN packet in the data stream. The data stream will have all the necessary sequence numbers (all different) and meet the criteria so the target accepts the stream. After transmitting the data stream, the host ignores the SYN packet because the reference of the SYN packet has already established a connection. The motive behind this attack is to resynchronize the sniffer or IDS. If the attacker succeeds in resynchronizing the IDS with a SYN packet, the attacker then sends an RST packet with the new sequence number.

#### Preconnection SYN

This attack is performed by sending an initial SYN before the real connection is established, but with an invalid TCP checksum. The sniffer can ignore or accept subsequent SYNs in a connection. If the sniffer is smart, it does not check the TCP checksum. If the sniffer checks the checksum, the attack is synchronized and a bogus sequence number is sent to the sniffer or IDS before the real connection occurs.

**Fragmentation** These attacks are similar to session splicing. Attackers use different fragmentation methods to evade the IDS.

**Session Splicing** Session splicing is a network-level evasion method that divides the string across several packets. The data in the packets is divided into small portions of bytes, and during delivery the string match

is evaded. To handle these evasion techniques, an IDS needs to watch and understand that the session or IDS has to detect the evasion technique using other methods. The following is the Snort rule to detect an evasion technique:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-MISC
whisker
space splice attack"; content:"|20|"; flags:A+; dsize:1;
reference:arachnids,296; classtype:attempted-recon; reference
```

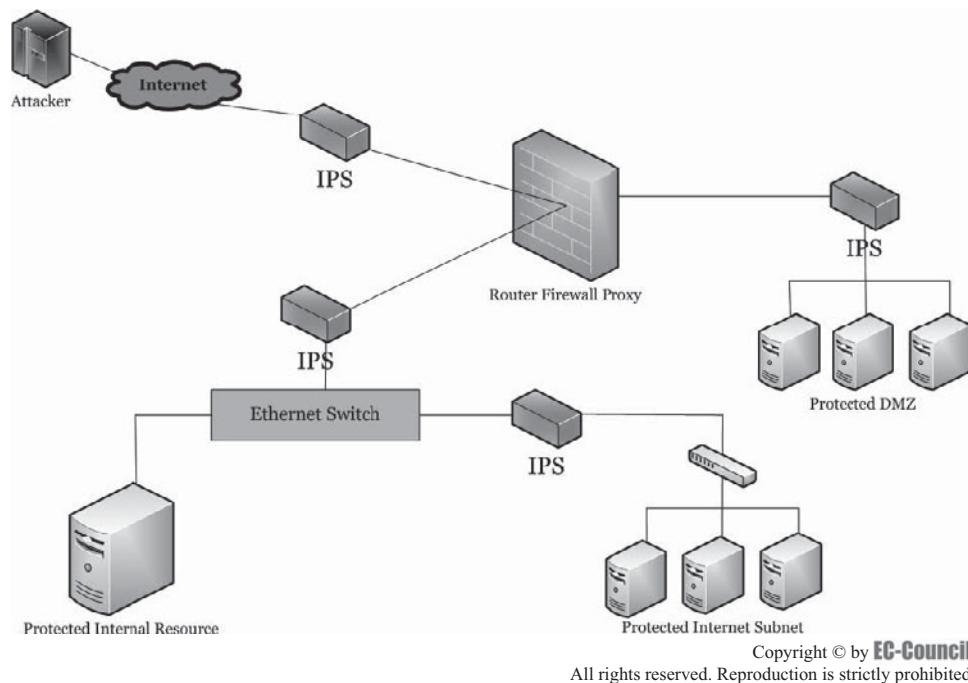
The above code rule identifies the traffic that is intended for port 80 with the ACK flag set, a space (hex 20) in the payload, and a dsize of 1.

## Intrusion Prevention Systems (IPS)

The inadequacies in current security systems have made it necessary to develop a new breed of security products known as intrusion prevention systems (IPS) (Figure 3-5). Intrusion prevention is a preemptive approach to network security, used to identify potential threats and respond to them swiftly.

An intrusion prevention system can be any device that uses access controls to guard systems from attacker misuse. Intrusion prevention is treated as an enhancement of intrusion detection. Primarily, an IPS must display the same output, consistency, and latency characters as other network communications elements such as switches and routers. IPS are designed to detect malicious data packets, stop intrusions, and block malicious traffic automatically prior to any attacks taking place. Network engineers must cautiously design their networks to send traffic from one point to another with precise latency and throughput necessities. These presentation characteristics should not rely on the number of sort-outs that are used or the type of traffic that is being transmitted through the network. An IPS can correct CRCs, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport- and network-layer options.

An IPS is the first step in the union of networking and security. IPS is not just an outer-limit defense element, but presents its maximum value as an invasive security element that is executed at both interior and boundary network segments. To be efficient, an IPS must display unrestricted network performance and tremendous attack-plugging precision. IPS indicate a theoretical shift from conventional security tools like firewalls and intrusion detection systems that require widespread design, modification, and manual protection to an automated safety key.



**Figure 3-5** Intrusion prevention systems entail a preemptive approach to network security.

## Intrusion Prevention Strategies

The following three strategies are used to direct IPS:

- *Host-based memory and process protection*: With this strategy, the IPS monitors the executing processes and disables those that look malicious—for example, processes that try to execute buffer overflows.
- *Session interception*: Terminating a session by sending a reset (RST) packet can be done when a flexible response plug-in is enabled. Snort can automatically terminate TCP sessions using this plug-in response.
- *Gateway intrusion detection*: Snort uses gateway ID to block hostile traffic and, using SnortSam, manipulates the access list of blocked traffic. Alerts are generated if any suspicious traffic is found.

## IPS Deployment Risks

Risks should be considered while deploying an IPS and Snort operating in one of the IPS modes. The following sections discuss those risks.

**Session Interception and IDS Identification** Snort terminates TCP sessions when it detects an attack with the help of an RST packet. This packet may allow the attacker to determine not only the type of IPS responsible for termination but also the type of system that runs the IPS software.

The pOf (Passive OS Fingerprinting) tool is used to identify the type of OS and analyze the flow of packets in an OS. This tool listens to the packets on the network and determines what type of machine is sending the RST packet, allowing an attacker to identify what type of IPS solution is causing the problem.

**Exploiting Time Delays** When there is a time gap between the IPS detecting attacks and ordering a change in access control lists of border devices, attackers can use the target to establish a backdoor connection to another system.

**Self-Inflicted Denial-Of-Service** Modifying the actual source address to become a forged address is called spoofing. If this forged address is a system that the network actually needs, denial-of-service conditions result. Spoofing the address of a DNS server prevents name resolution. Spoofing a mail gateway can stop the flow of e-mail.

**Blocking Legitimate Traffic** An IPS usually blocks traffic if the packet is identified as an attack. If legitimate traffic is incorrectly identified as an attack by an IPS that blocks millions of inbound connections, then the customers using that IPS will lose a great deal of money. Careful considerations should be taken to avoid this kind of situation.

## IPS Types

The two types of IPS are host-based and network-based.

**Host-Based IPS (HIPS)** A host-based IPS (HIPS) installs the intrusion-prevention application directly onto the particular system that is being protected. The intrusion-prevention application binds directly to the operating system and its services to monitor and intercept system calls. The application, by binding to the operating system, prevents attacks and maintains a log file. A HIPS does not need regular updates to stay ahead of new malware as it uses traditional fingerprint-based and heuristic antivirus detection methods. Apart from monitoring and intercepting system calls, a HIPS can also monitor data streams, file locations, and registry settings for a Web server in order to protect it from generic attacks.

Malicious code usually tries to modify the system or other software on the attacked machine. Host-based IPS recognize such changes and either prevent them by default or notify the user for permission. An application binary interface (ABI) is a set of basic binary software conventions that remains constant. HIPS works by enforcing ABI. ABI stays one step beyond the application program interface. For a particular CPU family, ABI can be defined as the application program interface plus the machine language for that particular CPU family. Hence, it is difficult for an attacker to attack the system without violating the ABI.

**Network-Based IPS (NIPS)** NIPS come with the features of an IDS, an IPS, and a firewall. For this reason they are also referred to as in-line or gateway IDS. NIPS come with two interfaces: one is designated as internal and the other as external. All incoming packets are first transferred to the internal interface's detection engine, which examines the packets and checks for any threats. If the packets are found to be legitimate and threat free, they are forwarded to the intended destination. A NIPS is an application or piece of hardware that prevents an intrusion on a specific network host. NIPS are designed to inspect traffic based on the security policy and drop

any malicious traffic. They analyze, detect, and report any security-related events. There is no need to install a NIPS on every computer system as must be done with host-based IPS.

The following are the NIPS types:

- *Content-based NIPS*: inspects the content of network packets for unique sequences. It inspects and blocks any unknown entry into the network. These sequences, called signatures, are analyzed to detect and prevent attacks such as worm infections or hacks.
- *Rate-based NIPS*: depends on the intent of the attack rather than the content. It identifies the threats that are different from the usual traffic. It sets parameters by learning or monitoring the type and behavior of normal traffic. Anything falling outside of these parameters is considered malicious and blocked. These NIPS prevent denial-of-service and distributed denial-of-service attacks.

### **Information Flow in IDS and IPS**

The flow of information is similar in both IDS and IPS. The following sections describe eight methods of information flow illustrating the similarities and differences between IDS and IPS.

**Raw Packet Capture** The information flow starts from raw packet capture in IDS and IPS. This method captures the packets and transfers data to the next intended component of the system. There are two modes of data capturing:

- *Promiscuous mode*: packets are picked up by network interface cards (NICs) at every point that interfaces with the network media.
- *Nonpromiscuous mode*: packets are picked up by NICs that are related to particular MAC addresses. This mode is best suited for host-based detection and prevention.

Network-based detection uses two NICs; one for raw packet capture and the other to allow the host systems to provide remote administration. These captured raw packets should be saved by both IDS and IPS so they can be processed and analyzed for future use.

**Filtering** Filtering is a process of controlling the packets that are captured and can be done in many ways. Network interface cards filter incoming packets. Another method is to use packet filters to capture some configured packets. For example, libpcap offers packet filtering with the help of a BPF interpreter when it decides what packet should be sent to an application. In most operating systems filtering is done in kernel space with the help of a BPF interpreter. In other systems, like Solaris, filtering is done in user space, which is less efficient.

**Packet Decoding** A decoder is used to define the packet structures that are collected through promiscuous monitoring. Decoding is used to determine whether a packet is IPv4, an IP header with no options, or in IPv6. Some IDS, like Snort, use packet encoding that allows a checksum to determine whether the packet header coincides with the checksum value in the header itself or not. This checksum calculation is done for all combinations of protocols.

**Storage** After decoding the packet it should be stored either by saving its data to a file or by placing it in a data structure. Saving data in a file is simple and easy because new data can be appended to an existing file or a new file can be created to store the filtered data. The disadvantage of writing intrusion detection data to a file is that an IDS sorts huge amounts of data in one or more files, making disk space management a challenge. This challenge can be handled by using a data structure.

**Fragment Reassembly** After storing the data, packet fragmentation should be done. This can be accomplished in different ways. One packet fragment can overlap another packet through fragment reassembly. The overlapped fragment can overwrite the first rather than being reassembled in its sequential order. Fragmentation helps to remove wasted size, which is left blank.

**Stream Assembly** The stream assembly method is a complicated storage mechanism as it has to handle many conditions.

**Stateful Inspection of TCP Session** Stateful inspection of network traffic is used to analyze the importance of packets that traverse the network. Both IDS and IPS have difficulty dealing with packets that appear to be a part of the session; an attacker can flood the entire network with such packets, rendering the presence of IDS and IPS useless. Current IDS and IPS perform these stateful inspections of network traffic. Stateful inspection helps IDS and IPS perform signature matching on the contents of the session. Stateful analysis enables IDS and IPS to identify scans in which OS fingerprinting is attempted.

**Firewalling** The main purpose of firewalling is to protect the IDS and IPS from outside attacks such as worms, viruses, Trojan horses, and so on. Attackers can launch attacks on IDS and IPS that disable them. In this situation, the firewall plays a major role in protecting both the IDS and the IPS. The firewall filters proxy data over a network and reduces the traffic. Most IDS and IPS do not have built-in firewalls, as they limit the performance of the system.

### IDS Versus IPS

The subject of IDS versus IPS has become an unnecessary argument in the field of technical security. IDS and IPS are two separate technologies that can complement each other. There are many differences between them. The major ones are listed in Table 3-1.

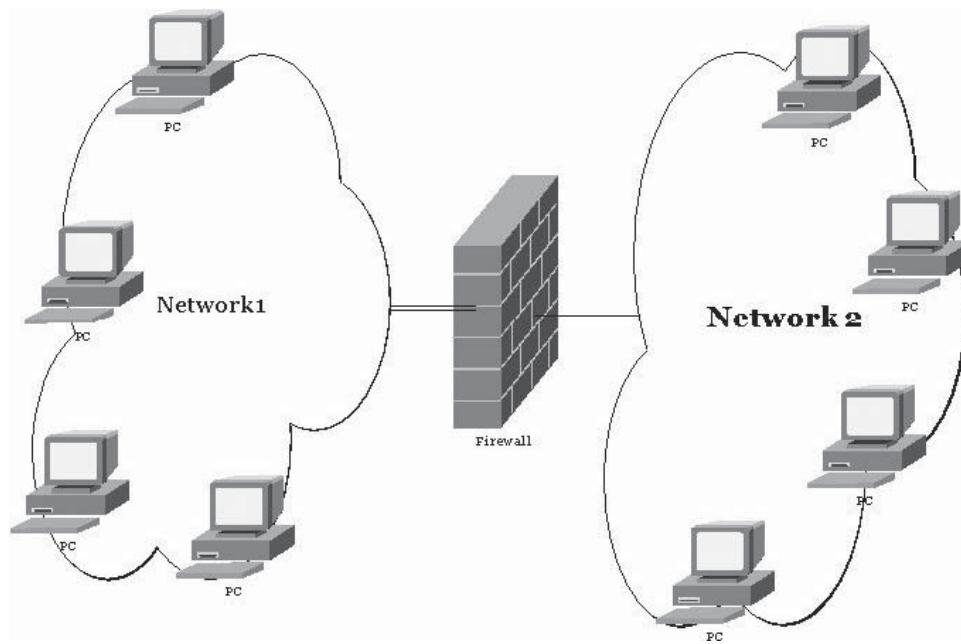
### Firewalls

A firewall (Figure 3-6) is a set of related programs that protect the resources of a private network from users on other networks. Firewalls are a set of tools that monitor the flow of traffic between networks. A firewall, placed at the network level and working closely with a router, filters all network packets to determine whether or not to forward them toward their destinations. A firewall is often installed away from the rest of the network so that no incoming request can get directly to a private network resource. If configured properly, systems on one side of the firewall are protected from systems on the other side of the firewall.

A firewall is an intrusion detection mechanism and is specific to an organization's security policy. The settings of firewalls can be changed to make appropriate changes to its functionality. They can be configured to

IDS	IPS
Placed on network inactively	Placed in-line (actively)
Cannot parse encrypted traffic	Better at defending applications
Installed on network segments (NIDS) and on hosts (HIDS)	Installed on network segments (NIPS) and on hosts (HIPS)
Becomes reactive by providing alerts	Becomes proactive by providing blocking
Ideal for identifying hacking attacks	Better at blocking Web destruction

Table 3-1 IPS and IDS have different strengths



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

Figure 3-6 A firewall protects the resources on a network from users on other networks.

restrict incoming traffic to POP and SNMP and to enable e-mail access. Certain firewalls block e-mail services to secure against spam.

Firewalls can be configured to check inbound traffic at a point called the choke point, where security audits are performed. The firewall can also act as an active phone tap tool by identifying an intruder's attempts to dial into modems within the network. The firewall logs contain information that reports to the administrator on all the attempts to access various incoming services.

The firewall verifies incoming and outgoing traffic against firewall rules. It acts as a router to move data between networks, managing the access of private networks to host applications. All attempts to log in to the network are identified for auditing. Unauthorized attempts can be identified by embedding an alarm that is triggered when an unauthorized user attempts to login.

### **Packet Filtering**

Packet filtering is based on IP address and the type of network layer on which the firewall operates. Firewalls can filter packets based on address and traffic type. They identify the source addresses, destination addresses, and port numbers while address filtering. They also identify types of network traffic when protocol filtering. Firewalls can identify the state and attributes of the data packets.

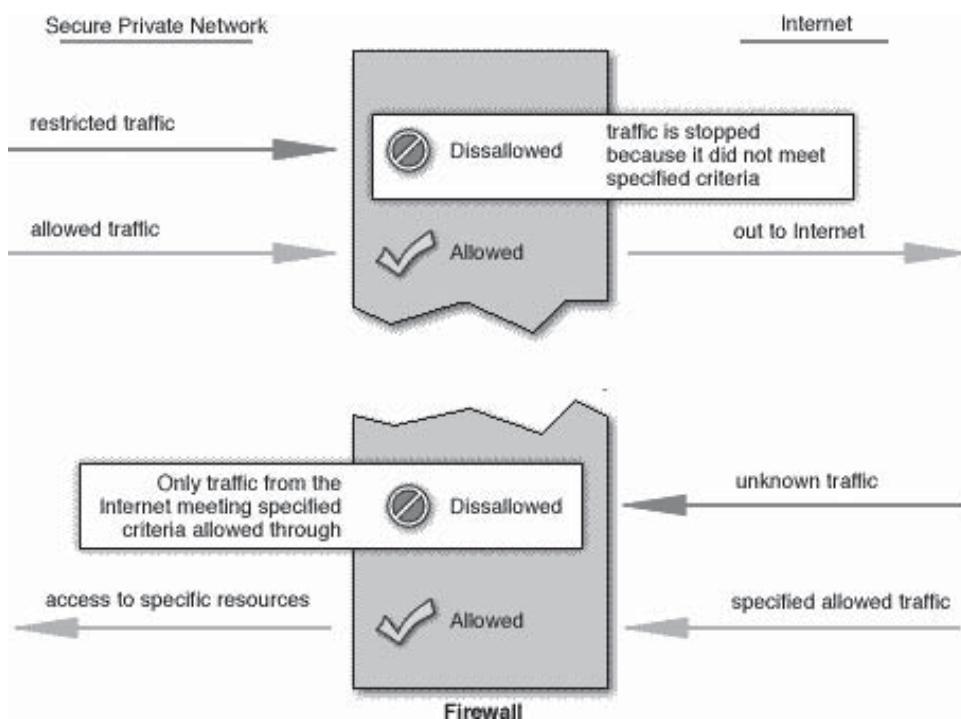
**Address Filtering** Firewalls can filter packets based on their source and destination addresses and port numbers.

**Protocol Filtering** Firewalls can also filter specific types of network traffic. The decision to forward or reject traffic depends on the protocol used—for example, HTTP, FTP, or ICMP. Firewalls can also filter traffic by packet attribute or state.

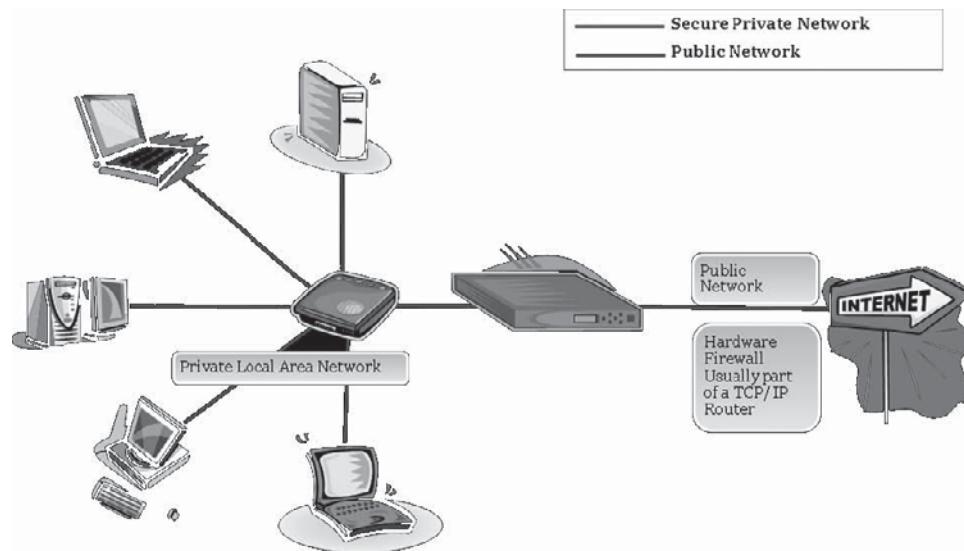
### **Firewall Methodology**

Firewalls generally deny traffic based on the following two methodologies (Figure 3-7):

- A firewall can allow any traffic except that which is specified to be restricted. It depends on the type of firewall used, the source and destination addresses, and the ports.
- A firewall can deny traffic that does not meet the specified criteria based on the network layer on which the firewall operates.



**Figure 3-7** Firewalls use two different methodologies for denying traffic.



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

**Figure 3-8** Hardware firewalls can be used for more than one system.

The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another. Firewalls may be concerned with the type of traffic or with source or destination addresses and ports. A firewall may also use complex rule bases that analyze the application data to determine whether the traffic should be allowed through.

### **Firewall Limitations**

The following are some limitations of firewalls:

- A firewall cannot prevent individual users with modems from dialing into or out of the network, bypassing the firewall altogether.
- A firewall cannot prevent an attacker from getting a user to reveal sensitive information through social engineering. Therefore, employees must be trained to keep confidential information intact. Attackers can socially engineer an employee who is not alert to reveal passwords that allow the intruder to easily dial through the modem into the organization's private network.
- Firewalls cannot secure against tunneling attempts. Applications that are secure can be Trojaned. Tunneling malicious packets over HTTP, SMTP, and other protocols is quite simple and trivially demonstrated.

### **Types of Firewalls**

**Hardware Firewall** A hardware firewall is preferred when a firewall is required on more than one system. Hardware firewalls provide an additional layer of security to the physical network. The disadvantage with this approach is that if one firewall is compromised, all the systems that it serves are vulnerable.

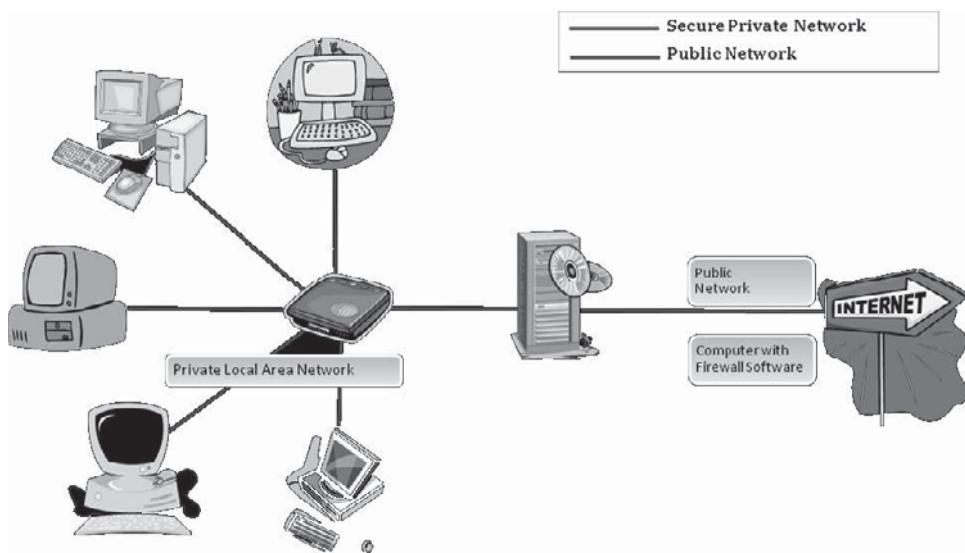
The firewall is plugged into the system just as other terminals are. Most large enterprises use hardware firewalls. Figure 3-8 describes how a hardware firewall is deployed in a network.

**Software Firewall** A software firewall (Figure 3-9) secures the network from malware, worms, viruses, and e-mail attachments. A software firewall looks like any other program and can be customized based on network requirements. A software firewall is a second layer of security for the network. Software firewalls are often coupled with antispam, antivirus, and antiadware programs.

**Packet-Filtering Firewall** Packet-filter-based firewalls (Figure 3-10) concentrate on individual packets, analyzing their header information and which way they are directed. These firewalls investigate each individual packet and make a decision whether to pass or drop the packet.

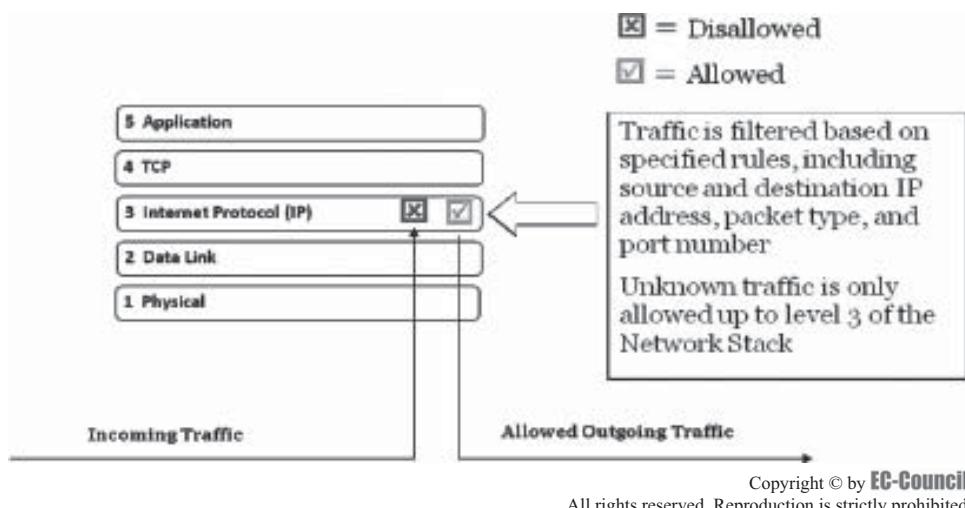
Traditional packet filters make the decision based on the following information:

- **Source IP address:** This is used to check whether or not a packet is coming from a valid source. The information about the source IP address can be found in the IP header of the packet.



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

**Figure 3-9** Software firewalls protect against malware.

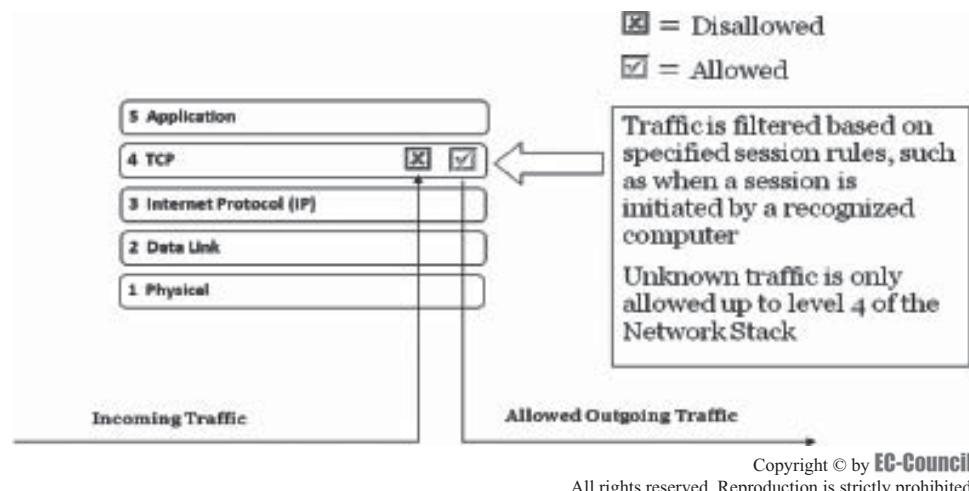


Copyright © by EC-Council  
All rights reserved. Reproduction is strictly prohibited

**Figure 3-10** Packet-filter firewalls analyze packet headers.

- *Destination IP address:* This is used to check if the packet is going to the correct destination and if the destination accepts these types of packets. The information about the destination IP address can be found in the IP header of the packet.
- *Source TCP/UDP port:* This is used to check the source port for the packet.
- *Destination TCP/UDP port:* This is used to check the destination port for the services to be allowed and the services to be denied.
- *TCP code bits:* This is used to check whether the packet has a SYN, ACK, or other bits set.
- *Protocol in use:* This is used to check whether the protocol the packet is carrying should be allowed.
- *Direction:* This is used to check whether the packet is coming from the packet-filter firewall or leaving it.
- *Interface:* This is used to check whether the packet is coming from an unreliable site.

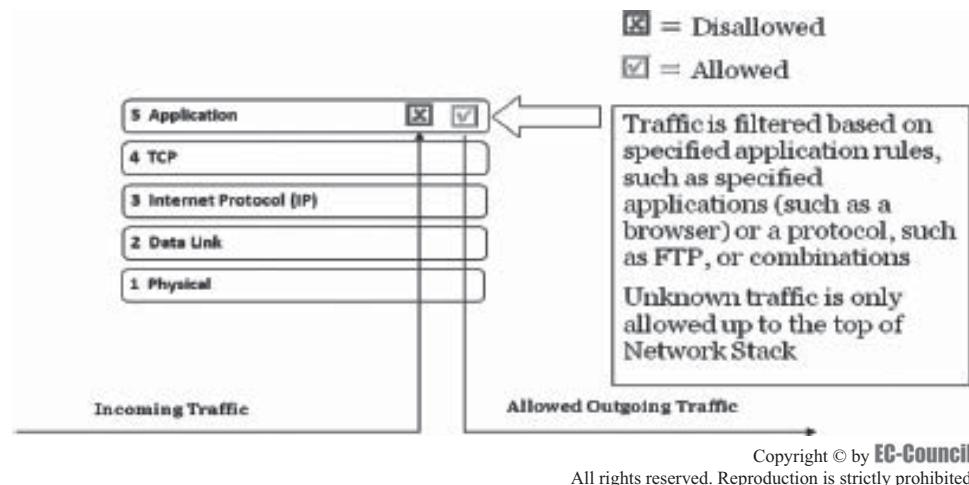
**Circuit-Level Gateway** Circuit-level gateways (Figure 3-11) work at the session layer of the OSI model or the TCP layer of TCP/IP. A circuit-level gateway forwards data between networks without verifying it. It blocks packets from coming into the host but allows the traffic to pass through to the next network. Information passed to remote computers through a circuit-level gateway appears to have originated from the gateway, as the incoming traffic carries the IP address of the proxy (circuit-level gateway).



Copyright © by EC-Council

All rights reserved. Reproduction is strictly prohibited

**Figure 3-11** Circuit-level gateways work at the session layer of the OSI model or the TCP layer of TCP/IP.



Copyright © by EC-Council

All rights reserved. Reproduction is strictly prohibited

**Figure 3-12** Application-level firewalls focus on the application layer.

A circuit-level gateway gives a controlled network connection to the network between the systems internal and external to it. To detect whether or not a requested session is valid, it checks the TCP handshaking between the packets. Circuit-level gateways do not filter individual packets. Circuit-level gateways are relatively inexpensive and hide information about the private networks they protect.

**Application-Level Firewall** Proxy/application-based firewalls (Figure 3-12) concentrate on the application layer rather than just the packets. These firewalls analyze the application information to make decisions about whether or not to transmit the packets. A content-caching proxy optimizes performance by caching frequently accessed information instead of sending new requests for the same data.

**Stateful Multilayer Inspection Firewall** The inability of a packet-filter firewall to check the header of the packets to allow their passing is overcome by stateful packet filtering (Figure 3-13). This type of firewall can remember the packets that passed through it earlier and make decisions about future packets based on memory. These firewalls provide the best aspects of both packet filtering and application-based filtering.

## Firewall Countermeasures

### Firewall Identification

**Port Scanning** This is one of the most popular methods that hackers use for investigating the ports that victims use. Nmap is probably the most popular port-scanning tool available.

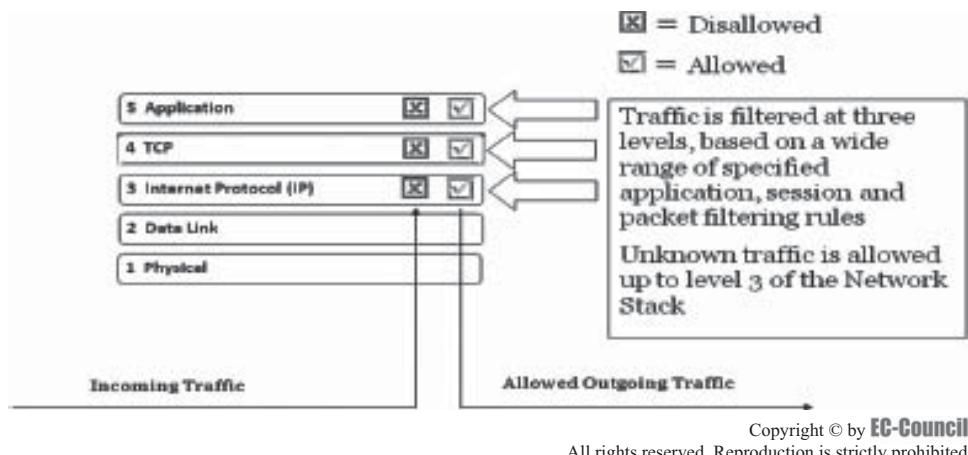


Figure 3-13 Stateful packet filtering allows firewalls to remember packets.

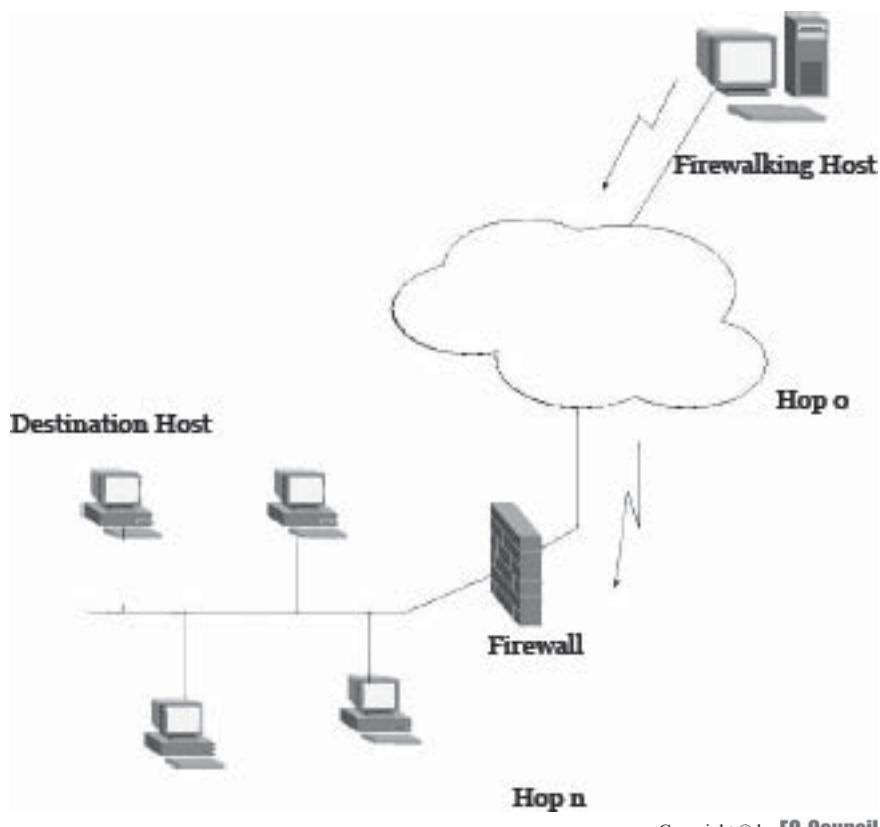


Figure 3-14 Firewalking allows the user to obtain information from behind a firewall.

**Firewalking** Firewalking (Figure 3-14) is a method used to collect information about remote networks that are behind firewalls. It probes ACLs on packet-filtering routers and firewalls. Firewalk is the best-known software used for firewalking. Firewalking has two phases: a network discovery phase and a scanning phase.

Firewalking requires three hosts:

- *Firewalking host*: the system, outside the target network, from which the data packets are sent to the destination host in order to gain more information about the target network
- *Gateway host*: the system on the target network that is connected to the Internet, through which the data packets pass on their way to the target network
- *Destination host*: the target system on the target network that the data packets are addressed to

**Banner Grabbing** Banners are messages sent out by network services during connections to the service. Banners announce which service is running on the system. Banner grabbing is a very simple means of OS detection. Banner grabbing also helps in discovering services run by firewalls.

The three main services that send out banners are FTP, telnet, and Web servers. Ports of services such as FTP, telnet, and Web servers should not be kept open as they are vulnerable to banner grabbing. A firewall does not block banner grabbing by default because the connection between the attacker's system and the target system looks legitimate.

An example of SMTP banner grabbing is the command `telnet mail.targetcompany.org 25`. This command connects to the SMTP port of the mail server at `mail.targetcompany.org`.

The following example shows a user opening a telnet connection to a known port on the target server (in this case the HTTP port):

```
telnet www.corleone.com 80
HTTP/1.0 400 Bad Request
Server: Netscape – Commerce/1.12
```

This system works with many other common applications that respond on a set port. The information generated through banner grabbing can enhance an attacker's efforts to further compromise a system. With information about the version and the vendor of the Web server, the attacker can further concentrate on employing platform-specific exploit techniques.

### Countermeasures

Some of the main countermeasures against banner grabbing include the following:

- Disabling the presentation of the vendor and version in banners. For example, the most popular banner to grab on Windows NT/2000 is the IIS banner. An administrator can change the IIS banner through a hex edit of the DLL that contains the IIS banner, `%systemroot%\system32\inetsrv\w3svc.dll`. Another way to change the IIS banner is to install an ISAPI filter that sets the banner using the `SetHeader()` function call.
- Regular auditing with port scans and raw netcat connections to active ports.

### Breaching Firewalls

When a firewall protects a network, attackers look for ways and means of hacking their way through it. This can be achieved through various methods, including the following:

- *Insider:* The easiest way to circumvent a firewall is if the attacker has an accomplice inside the company who installs a backdoor. Another easy, and common, way for an attacker to slip by a firewall is by installing network software on an internal system that communicates using a port address permitted by the firewall configuration. A popular port to use is port 80 (HTTP). Many firewalls permit all traffic using port 80 by default because it simplifies firewall configuration and reduces support calls.
- *Vulnerable services:* Almost all networks offer a number of services that include incoming e-mail, WWW, and DNS. It may be that these services exist on the firewall host, in the DMZ, or on an internal system. As soon as an attacker finds a hole in any of these services, he or she can access the system.
- *Vulnerable external server:* Sometimes external systems are accessed from within the firewall. If an attacker compromises the external systems, he or she can do serious damage. The attacker could also send fake FTP answers to overflow a buffer in the FTP client software, replace a GIF picture on a Web server with one that crashes the browser, or execute a command. Some firewall configurations allow incoming telnet sessions from certain systems so that anyone can sniff the network and get in.
- *Hijacking connections:* Often, companies consider incoming telnet connections with secure authentication, such as SecureID, safe. However, anyone can hijack these after the authentication has occurred and get in. Hijacked connections can also be used to modify replies in the protocol implementation to generate a buffer overflow.

### Bypassing a Firewall Using HTTPTunnel

HTTPTunnel creates a bidirectional virtual data connection tunneled in HTTP requests and replies. The HTTP requests can be sent via an HTTP proxy, if so desired. This can be useful for users behind restrictive firewalls. If WWW access is allowed through an HTTP proxy, it is possible to use HTTPTunnel and telnet, or PPP, to connect to a computer outside the firewall.

The syntax for HTTPTunnel is `htc [option]...HOST[:PORT]`.

The following are some examples of HTTPTunnel commands and their explanations:

- **htc -h:** This command gives an explanation of HTTPTunnel and its options.
- **htc -A:** This command is for proxy authorization.
- **htc -V:** This command gives information about the versions of the current services running on the system.
- **htc -m:** This command helps determine a minimum time for a connection to stay alive.

### ***Placing Backdoors Through Firewalls***

Written by THC's van Hauser, rwwwshell was released between October 1998 and May 1999 as a proof-of-concept program for the white paper "Placing Backdoors through Firewalls." It was written in Perl, making it portable and flexible. The key strength of rwwwshell lies in the paradigm shift it represented: on the slave/Trojan side, the initial connection is made to the master rather than the reverse. This strategy was designed to circumvent stateful packet inspection devices and proxies that only allow incoming traffic from preexisting, internally initiated connections.

In practice, the rwwwshell slave can be actively used in real time or configured as a passive backdoor to wake up and contact the preconfigured master as a timed event via an outgoing HTTP request. The master side then sends shell commands as HTTP response packets, and output from a command is returned to the slave as CGI script HTTP GETs. Each command-response exchange is a new TCP connection initially connecting from port 1171, and, by default, connecting to port 8080. This allows nonroot use and gives the appearance of being a caching Web server exchange. The commands and responses are encoded to make the conversation incomprehensible. In passive mode, the slave side always fails to establish a connection with the master side. In the meantime, the actual remote control session takes place, and does not appear to be a new or unusual conversation. The master server adds to the authenticity by responding to the usual attempts for the connection by sending 404 error messages. The integrity of the data is also ensured by the reliable transport of the TCP packets. One drawback to this is that the Web traffic trustworthiness is affected, particularly when all the traffic is exposed to /cgi-bin/order. A successful strategy for covert channel establishment is embedded Web traffic.

### ***Hiding Behind a Covert Channel: Loki***

Loki was originally presented in August 1996 in the underground magazine *Phrack*, one of the oldest and best-known "hackzines" on the net. The concept of the Loki Project is possible because arbitrary information tunneling in the data portion of ICMP\_ECHO and ICMP\_ECHOREPLY packets is possible. Loki exploits the covert channel that exists inside of ICMP\_ECHO traffic because network devices usually do not filter the contents of ICMP\_ECHO traffic. The devices simply pass the traffic, drop it, or return it.

The attacker can send Trojan packets by masquerading them as common ICMP\_ECHO traffic. The attacker can then encapsulate any information in the packet. While the author states that Loki is not a compromise tool, attackers use it for various purposes, including breaking into systems. It can be used as a backdoor into a system by providing a covert method of getting commands executed on a target system.

The reverse is also possible, as Loki can be used as a way of secretly retrieving information from a system. In essence, the channel is simply a way to communicate data secretly and confidentially. Authenticity can be added by way of cryptography. Because both symmetric and asymmetric key exchange and Blowfish encryption were available in Loki during the development phase, there was a clear realization that a covert channel was no guarantee. Additionally, while the confidentiality of the commands embedded in the packets certainly reduced the risk of detection, it was not enough. The important point is that routers, firewalls, packet filters, and dual-homed hosts all can serve as conduits for Loki as long as they pass ICMP\_ECHO traffic.

Detection can be difficult, with perhaps the only indication being a surplus of ICMP\_ECHOREPLY packets with a garbled payload. However, if the attacker can keep traffic on the channel down to a minimum and is able to hide the Loki server inside the kernel, chances of detecting Loki are slimmer. The only countermeasure that can be taken is to disallow ICMP\_ECHO and UDP port 53 DNS traffic entirely. Actually, the UDP port 53 traffic could be restricted to the internal DNS server and the designated external DNS forwarder. Restricting ICMP\_ECHO traffic to be accepted from trusted hosts can be overcome by forging packets for "incoming-only" Loki traffic.

### ***ACK Tunneling***

A firewall generally restricts a Trojan client (outside) from connecting to a Trojan server (inside). ICMP tunneling and protocol tunneling have proved that a firewall can be penetrated. However, firewalls would become impenetrable if countermeasures such as blocking all ICMP traffic were adopted.

Ordinary packet filters belong to this class of firewalls, while stateful firewalls do not. It is known that TCP is a protocol that establishes virtual connections on top of IP. When a client sends a SYN (synchronize) part, the session is created and the server replies with the SYN/ACK part. The client makes sure of this with the ACK (acknowledge) segment. All the traffic present in the ensuing session contains the ACK segment.

Typical packet-filtering firewalls consider that a session always starts with a SYN segment from the client. Therefore, rule sets are applied on all SYN segments and it is assumed that any ACK segments detected are part of an established session. More advanced firewalls apply their rule sets on all segments, including ACK segments. However, these firewalls must also track server-side ephemeral port negotiation in the second part of the TCP three-way handshake.

Other firewalls are configurable regarding the two ways to handle ACK segments. Typically, a session may have thousands or even millions of ACK segments, but only one SYN-only segment. Firewalls do not apply the rule set on ACK segments because it increases both the workload and cost of running the firewall.

Consider this scenario: UDP and ICMP traffic is blocked by the firewall, an attacker sends a Trojan server by mail to a user behind the firewall, and the user runs the Trojan. How does the attacker on the outside contact the Trojan on the inside?

This is where ACK tunneling comes into play. The client part of the Trojan employed by the attacker uses only ACK segments to communicate with the server part planted on the victim network and vice versa. Now the segments pass straight through the firewall.

As long as the attacker knows the IP address of the target system, it does not matter if the IP address is dynamic. Additionally, even if the target IP address changes with time, the attacker could use a special scanner to scan for the Trojan straight through the firewall. The Trojan does not have to contain any link to the attacker. Moreover, the person connecting to it might not even know who sent the Trojan to them. It would be like scanning for NetBus over an entire network, hoping it's running on some of the systems.

## Honeypots

A honeypot is a system intended to attract and trap people who try unauthorized or illicit utilization of the host system. Whenever there is any interaction with a honeypot, it is most likely malicious activity. Honeypots are unique; they do not solve a specific problem. Instead, they are highly flexible tools with many different security applications. Some honeypots can be used to help prevent attacks, others can be used to detect attacks, while a few honeypots can be used for information gathering and research. The following examples illustrate some uses of honeypots:

- Installing a system on a network with no particular purpose other than to log all attempted access.
- Installing an older, unpatched operating system on a network. For example, the default installation of Windows NT 4 with IIS 4 can be hacked using several different techniques. A standard intrusion detection system can then be used to log hacks directed against the system and further track what the intruder attempts to do with the system once it is compromised. This has the advantage of making it look like the intruder is successful without really allowing access to the network.

Any existing system can be “honeypot-ized.” For example, on Windows NT it is possible to rename the default administrator account and then create a dummy account called “administrator” with no password. Windows NT allows extensive logging of a person’s activities, so this honeypot tracks users who are attempting to gain administrative access and exploit it.

### ***The Honeynet Project***

The Honeynet Project is a nonprofit research organization of security professionals dedicated to information security. The organization has no products, services, or employees, and all research is carried out on a voluntary basis. Historically, intelligence about attackers has been limited to the tools they use. The Honeypot Project intends to provide additional information such as the attackers’ motives, how they communicate, when they attack systems, and their actions after compromising a system. The Honeynet Project is a four-phased project.

**Phase I** From 1999 to 2001, the Honeynet Project captured and studied a variety of attacks using GenI honeynets. The purpose of Phase I was to be a proof of concept, identifying the most common threats against default installations of operating systems and applications.

**Phase II** From 2002 to 2003, the purpose of this phase was to develop a superior honeynet-one that is easier to deploy, harder to detect, and more efficient in collecting data. These GenII honeynets are deployed to target the more sophisticated attackers, improving the project’s intelligence-gathering capabilities.

**Phase III** Begun in 2003, the goal of Phase III was to develop a bootable CD-ROM that boots into a honeynet gateway or honeywall. Once booted, all the user has to do is place the target systems behind this gateway. This standardizes honeynets, making them easier to deploy. In addition, these bootable devices have the option of logging to a central system, enabling the deployment of distributed honeynets.

**Phase IV** In 2004, the goal of Phase IV was to create a centralized system that could collect and correlate data from distributed honeynets.

### **Types of Honeypots**

**Low-Interaction Honeypot** Honeyd is a low-interaction honeypot. Developed by Niels Provos, Honeyd is open source and designed to run primarily on UNIX systems. Honeyd operates on the concept of monitoring unused IP space. Anytime it sees a connection attempt to an unused IP, it intercepts the connection and then interacts with the attacker, pretending to be the victim.

By default, Honeyd detects and logs connections to any UDP or TCP port. In addition, the user can configure emulated services to monitor specific ports such as an emulated FTP server monitoring port 21 (TCP). When an attacker connects to the emulated service, not only does the honeypot detect and log the activity, but it also captures all of the attacker's interactions with the emulated service.

In the case of the emulated FTP server, an attacker's login and password can be potentially captured; the commands that were issued, what they were looking for, or their identity can be tracked. Most emulated services work the same way. They expect a specific type of behavior and then are programmed to react in a predetermined way.

The limitation of emulated services is that if the attacker does something the emulation does not expect, it does not know how to respond. Most low-interaction honeypots, including Honeyd, generate an error message.

**High-Interaction Honeypot** Honeynets are a prime example of a high-interaction honeypot. A honeynet is neither a product nor a software solution that the user installs. Instead, it is an architecture: an entire network of computers designed to track an attack. The idea is to have an architecture that creates a highly controlled network, one where all activity is controlled and captured. Intended victims are placed within this network and the network has real computers running real applications.

Attackers find, attack, and break into these systems on their own initiative. When they do, they do not realize that they are within a honeynet. All of their activity, from encrypted SSH sessions to e-mail and file uploads, is captured without their knowledge. This is done by inserting kernel modules on the victim's systems, capturing all of the attacker's actions.

At the same time, the honeynet controls the attacker's activity. Honeynets accomplish this by using a honeywall gateway. This gateway allows inbound traffic to the victim's systems but controls the outbound traffic using intrusion prevention technologies. This gives the attacker the flexibility to interact with the victim's systems while preventing the attacker from harming other nonhoneynet computers.

**Medium-Interaction Honeypot** Medium-interaction honeypots inherit the benefits of both the low-interaction and high-interaction honeypot approaches to detect bot and malware attacks. Application layer virtualization is one of the important features of medium-interaction honeypots. Known exploits wait on certain ports for expected responses. A medium-interaction honeypot sends these responses to trick the exploits into sending a payload. The shellcode is extracted and analyzed after the payload is received. The honeypot emulates the shellcode actions to download the malware. After the honeypot downloads the malware, it can either store it locally or submit it for further analysis.

### **Advantages and Disadvantages of a Honeypot**

The following are some of the advantages of using a honeypot:

- **Small data sets:** Honeypots collect small amounts of data, and almost all of this data reveals real attacks or unauthorized activities. Because honeypots collect only malicious activities, they make it much easier for administrators to analyze and react to the information they collect.
- **Reduced false positives:** With most detection technologies (such as IDS sensors), a large percentage of alerts are false warnings, making it difficult to find real attacks. With honeypots, almost everything that is detected or captured is an attack or unauthorized activity, vastly reducing false positives.
- **Reduced false negatives:** Unlike most technologies, it is easy for honeypots to detect and record attacks or behaviors that have not been seen before.

- *Cost effective:* Honeypots only interact with malicious activity and do not need high-performance resources. Most honeypots can easily run on an old Pentium computer with 128 MB of RAM.
- *Simplicity:* Honeypots are simple; there are no advanced algorithms to develop or rule bases to maintain.

Honeypots also have their disadvantages. This is why they do not replace existing technologies. Instead, they work with and complement the existing infrastructure. The two main disadvantages of honeypots are as follows:

- *Limited view:* Honeypots only see activity that they interact with. They do not see or capture any attacks directed against existing systems.
- *Risk:* Any time another resource is added with an IP stack, there is a risk. Different honeypots have different levels of risk, so it is always an issue that needs to be addressed.

Network intrusion detection systems have trouble distinguishing hostile traffic from benign traffic. Isolated honeypots have a much easier time because they are systems that should not normally be accessed. This means that all traffic to a honeypot system is already suspect.

### ***Placing a Honeypot***

If external attacks are the main thrust for setting up a honeypot, the honeypot should be placed in front of the firewall, preferably on the external demilitarized zone (DMZ). The DMZ is a host computer or a network placed as a neutral network between a particular firm's internal (private) and outside (public) network to prevent an outside user from accessing the company's private data. Honeypots can be dispersed throughout the internal network of the firm. Preferably, one honeypot should be placed in every subnet.

The following points should be noted about honeypots:

- Honeypots should be checked to determine whether they are router-addressable. If not, the honeypot will be reachable only by users within the network.
- Honeypots should have a static address. If not, it would be difficult to trap attackers inside the honeypot. If a dynamic address is assigned to the honeypot, the chances of an attacker getting into the same honeypot repeatedly are much smaller.

### ***Available Honeypots***

Honeypots are available in both commercial and open-source formats. Most honeypots are available as free downloads in the wild. The following is a partial list of available commercial and open-source honeypots.

#### ***Commercial Honeypots***

- KFSensor
- NetBait
- ManTrap
- SPECTER

#### ***Open-Source Honeypots***

- Bubblegum Proxypot
- Jackpot
- BackOfficer Friendly
- Bait-n-Switch
- Bigeye
- HoneyWeb
- Deception Toolkit
- LaBrea Tarpit
- Honeyd
- Honeynets
- Sendmail SPAM Trap
- Tiny Honeypot

## Physical and Virtual Honeypots

A physical honeypot is a real system on the network with its own IP address. A virtual honeypot is simulated by another system that responds to network traffic sent to the virtual honeypot.

While gathering information about network attacks or probes, the number of deployed honeypots influences the amount and accuracy of the collected data. A suitable example is measuring the activity of HTTP-based worms. These worms can be identified only after they complete a TCP handshake and send their payload. However, most of their connection requests will go unanswered because they contact randomly chosen IP addresses. A honeypot can capture the worm payload if the honeypot is configured to function as a Web server. If a large number of honeypots are deployed, the worm is more likely to contact them.

Physical honeypots are often high interaction, allowing the system to be compromised completely. They are expensive to install and maintain. For large address spaces, it is impractical or even impossible to deploy a physical honeypot for each IP address. In that case, virtual honeypots should be deployed.

## Security Responses to Hacking Attacks

A good response to hacking attacks requires that there are good defensive policies in place. These include the following measures:

- *Incident response team:* Set up an incident response team. Identify those people who should be called whenever an intrusion is suspected. Not all team members need to be involved with every incident. For example, top management is needed to deal with serious attacks. They may never be called upon, but they do need to be identified and they do need to be prepared for the kinds of decisions they will have to make. The response team needs to be interdepartmental and include the following people:
  - *Top management:* Top management needs to identify somebody with the authority to handle escalated issues. For example, if the company has an online trading service, the company needs to identify an individual with enough power to “pull the plug.” Going offline on such a service will have a major impact, but would still be better than hackers trading away people’s stocks.
  - *Human resources:* Many attacks come from internal employees. This consists of both serious attacks (cracking into systems), as well as nuisance attacks such as browsing servers to look for customer lists that might be left open. Therefore, the human resources department must be aware of such issues and proactively respond immediately to such acts.
  - *Technical staff:* Security is often separate from normal MIS activity. If security personnel detect a compromised system, they need to know who in MIS they need to call.
  - *Outside members:* Identify people outside the company that may be contacted. This may be a local ISP person (for example, helping against smurf attacks), the local police, or the FBI. These aren’t necessarily formal team members. The names of these people should be simply put on a list so that everyone knows whom to call.
  - *Security team:* Of course, the most important team members will be the security personnel themselves.
- *Response procedures:* For example, priorities between network uptime and intrusion detection have to be decided. Can the network plug be pulled whenever a suspected intrusion occurs? Should continued intrusion be allowed in order to gather evidence against the intruder? These questions have to be answered beforehand because there will be no time during an attack.
- *Lines of communication:* Determine guidelines for communication. Is the information propagated up the corporate food chain from the immediate superior up to the CEO, or horizontally to other business units? Does the company take part in incident reporting organizations such as FIRST (Forum for Incident Response and Security Teams)? Are the FBI or the local police informed in the case of an incident? Are partners (vendors/customers) who have a connection to the company network notified? Are intrusions hidden from the press?
- *Logging procedures:* Set up logging/auditing/monitoring procedures. Adequate logging procedures can help the team determine what happened.
- *Training/rehearsal:* Each person involved needs to understand the scope of what he or she needs to do. Also, carry out dry runs. Assume a massive hacker penetration and run a drill based on what happens next. Most hacker penetrations succeed because companies are unprepared for the attacks. Because

computer networks are growing so fast, there are not enough trained people to handle intrusions. Likewise, networks grow in ad-hoc fashion, making logging/auditing haphazard. These conditions lead to people not knowing what to do when under attack, and their networks are not robust enough to recover well from the attack.

## Tools

### Logging Tools

#### *Tripwire*

Tripwire (Figure 3-15) is available for both Windows and UNIX. It can monitor a number of attributes including file additions, deletions, modifications, flags, last access time, last write time, create time, size, hash checking, and so on. An SIV can monitor other components as well—such as the Windows registry and cron configuration—in order to find well-known signatures. It can also detect when a user privilege has been escalated.

### Host-Based IDS Tools

#### *Cisco Security Agent (CSA)*

Cisco Security Agent (CSA) (Figure 3-16) is a software application that secures servers from malicious attacks such as viruses and harmful downloads. CSA prevents attacks before they are deployed, whether they are known or unknown risks. It enables intrusion prevention, firewall capabilities, protection from harmful code, and it guarantees operating system integrity for Windows users.

CSA is a host-based IDS and does not rely on signature matching. It has the capability of preventing new and existing threats. It therefore builds up robust protection, while decreasing the cost of the operations applied. It also helps to integrate the endpoint server and the desktop system that are hooked into the Cisco Self-Defending Network.

Other agents, such as Cisco Network Access Control (NAC) and Cisco Clean Access, as well as Trusted QoS, ensure network security for further advancement of the delivery of mission-critical traffic when the network is heavily loaded.

CSA also produces an alarm warning the user about threats occurring on the server machine that can corrupt the operating system files. It warns if any illegitimate downloads take place. CSA can be installed to secure the network from viral crashes.

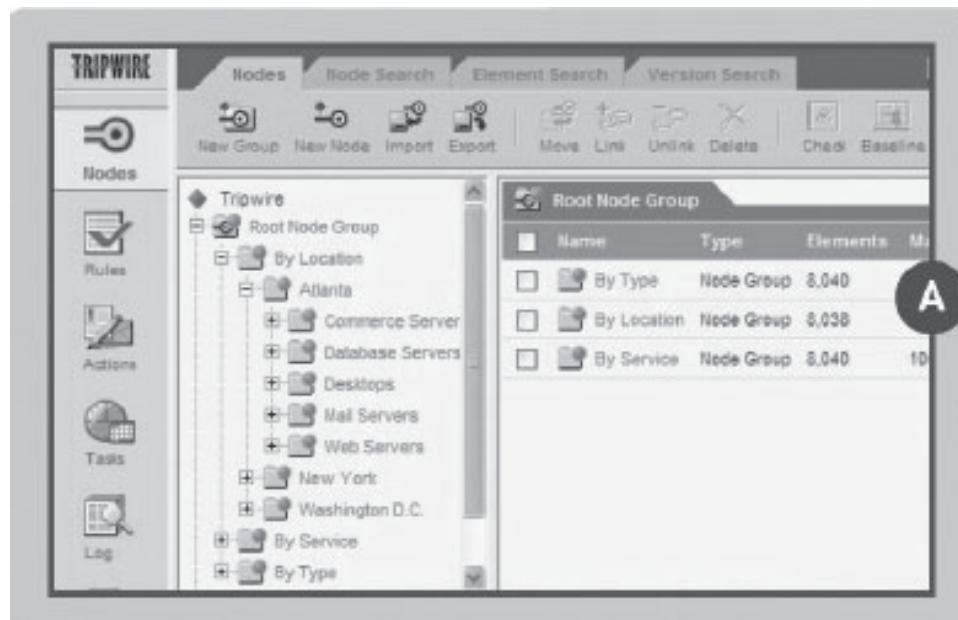
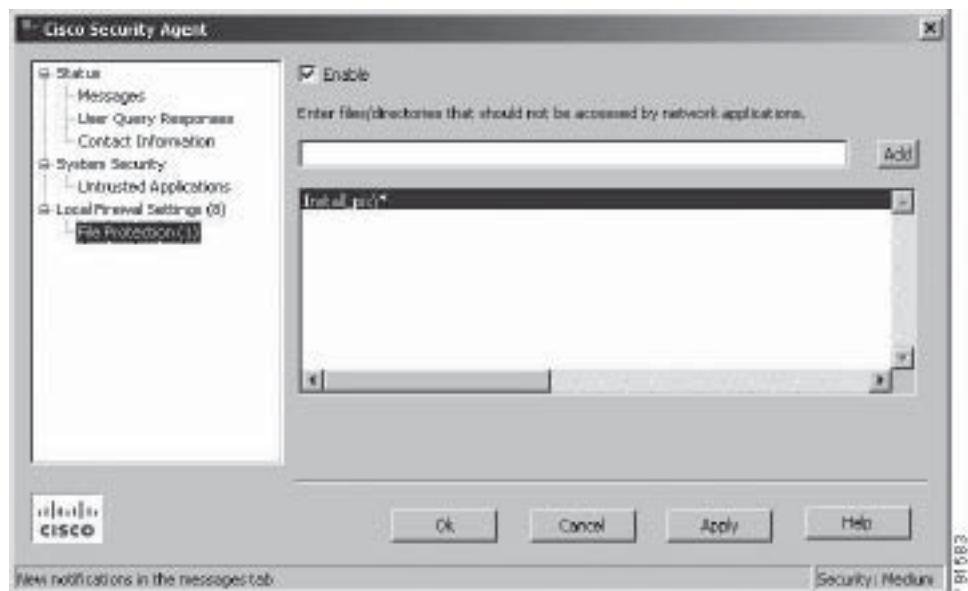


Figure 3-15 Tripwire fulfills a variety of logging functions.



**Figure 3-16** Cisco Security Agent secures servers against malicious attacks.

CSA has the following features:

- It is comprehensive and widens multiple endpoint security functions within a single agent to decrease operating costs.
- It secures against entire classes of attacks.
- It protects against known and unknown attacks without updates or emergency patching.
- It offers a flexible architecture, enforcing security based on a corporate policy.
- It integrates with Cisco Clean Access to provide network access control.

It integrates with Cisco VPN devices to provide endpoint security for IP Security IPsec and Secure Sockets Layer (SSL) VPN deployments.

## Intrusion Detection Tools

### **BlackICE**

BlackICE has multiple versions. The core is built around BlackICE Sentry, a full network-based intrusion detection system. There are also host/hybrid versions that run on Windows desktops with a built-in personal firewall.

BlackICE Sentry includes the following features:

- Full seven-layer stateful protocol analysis
- Antievasion techniques (handles fragmentation, Whisker scans, and a whole suite of signature changing attacks)
- Extremely fast; easily handles a 100-Mbps full-duplex connection

### **CyberCop Monitor**

CyberCop Monitor is a hybrid host/network-based IDS that analyzes network traffic to and from the host, Windows NT Event Log audit trails, and Windows NT authentication activity.

CyberCop Monitor includes the following features:

- Configuration editor allows for custom settings and thresholds to suit every environment, including security profiles, account groups, time, and subnets
- Extensive filtering using ordered filter rules for each signature

- Report coalescing suppresses denial-of-service attacks on the IDS itself
- Report collating of monitoring and scanning information per system with trend analysis options, including 3-D charting and graphing from an SQL database

### ***RealSecure***

RealSecure is an intrusion detection system that comes with over 400 attack signatures and the ability for customers to add or modify their own signatures in both the network and host-based solutions.

### ***Network Flight Recorder (NFR)***

NFR is available in multiple forms. The NFR Intrusion Detection Appliance, a piece of freeware, comes as a bootable CD-ROM and bundles with third-party resellers that add their own features on top of it.

One of the most popular features of NFR is N-code, a fully featured programming language optimized for intrusion detection-style capabilities. It has a full SMTP parser written in N-code. Numerous N-code scripts are downloadable from the Internet from sources such as L0pht. The N-code system allows easy additions into NFR's generic statistical system.

### ***Dragon***

Dragon is UNIX-based and compatible with many current operating systems. It is a host-based intrusion defense tool that monitors individual systems and applications to detect malicious or suspicious activity in real time, and monitors key system logs to detect tampering. Dragon can be deployed either on a protected host or on a dedicated analysis system where logs, aggregated via SNMP or syslog, are forwarded from switches, firewalls, routers, and other IDS aggregated via SNMP or syslog.

### ***NetProwler***

NetProwler identifies, modifies, and terminates unauthorized users. The program listens to the traffic specified by the user and is able to function in invisible mode, preventing hackers from detecting it.

### ***SilentRunner***

SilentRunner is an IDS tool that was developed to locate internal threats. It is referred to as a “passive network discovery LAN engine,” and allows the user to perform the following functions:

- Analyze real-time network topology and activity levels
- Exhibit individual terminal activity
- Develop and execute Boolean logic alerts
- Process network data for further detailed visualization and analysis

### ***Vanguard Enforcer***

Vanguard Enforcer is a tool that secures critical data by using standards and policies that are defined by security experts. It provides a state-of-the-art intrusion management solution for the mainframe environment.

### ***HP OpenView Node Sentry***

HP OpenView Node Sentry is an IDS tool that secures networks from DoS attacks, Web server exploits, e-mail tracks, and so on. It functions by observing data packets and searching for attack signatures. It produces an alarm when an attack is found and eliminates it from the network.

### ***Cisco Secure IDS***

Cisco Secure IDS is a real-time tool that uses a signature database to identify possible intrusions. It provides end-to-end security to the network.

### ***Lucent RealSecure***

Lucent RealSecure produces an immediate response when an illegitimate source enters prior to compromising a network. It determines attacks like DoS before the network becomes compromised. It seizes and reacts to every security breach on both the internal and external network. It then terminates the illegitimate source from the network. This process is carried out by warning a system administrator through an SNMP trap, syslog, or e-mail.

Snort

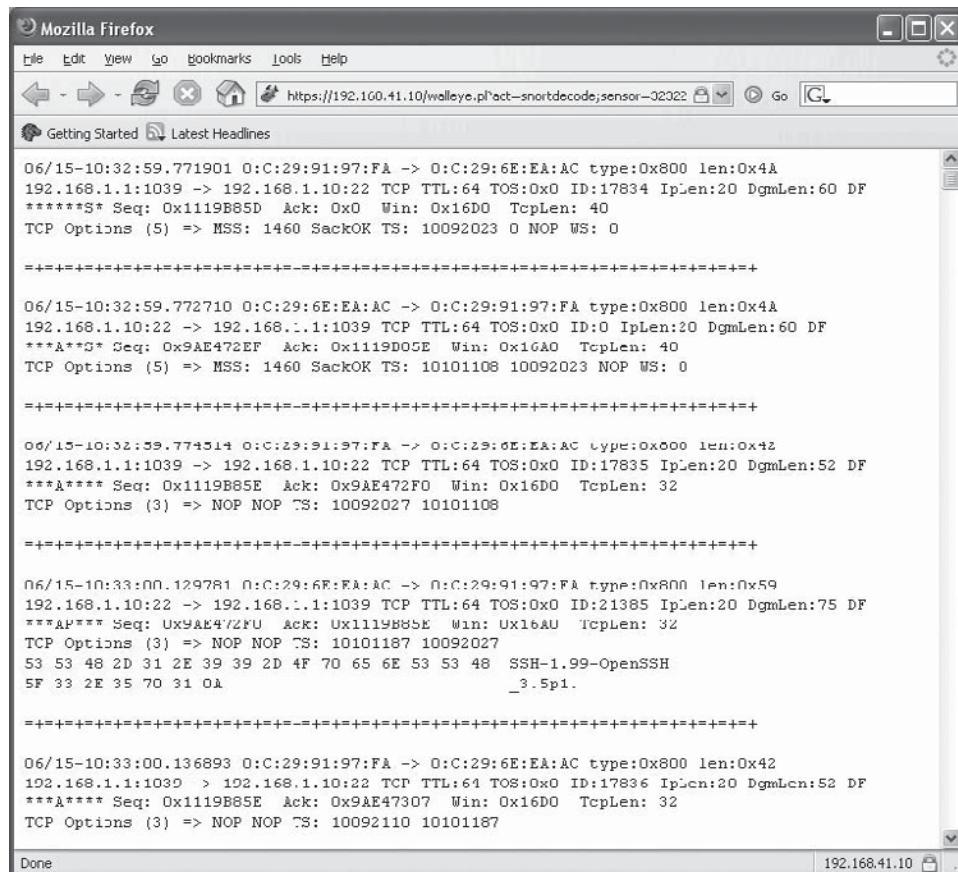
Snort (Figure 3-17) is a software-based, real-time, signature-based network IDS that notifies an administrator of a potential intrusion attempt. It is a lightweight NIDS that utilizes familiar methods for rule development. Snort currently includes the ability to detect more than 1,100 potential attack signatures.

Snort performs the following functions:

- Detects threats, based on pattern matching, including buffer overflows, stealth port scans, CGI attacks, SMB probes, NetBIOS queries, port scanners (e.g., Nmap), well-known backdoor and system vulnerabilities, and DDoS clients, and issues alerts
  - Uses syslog, SMB “WinPopUp” messages, or a file to alert an administrator
  - Develops new rules quickly once the pattern (attack signature) is known for the vulnerability
  - Records packets from the offending IP address in a hierarchical directory structure, in human-readable form
  - Can be used as a “passive trap” to record the presence of traffic that should not be found on the network, such as NFS or Napster connections
  - Can be used on an existing workstation to monitor a home DSL connection or on a dedicated server to monitor a corporate Web site

**Configuring Snort (`snort.conf`)** After installation, Snort needs to be configured on the local network using the following steps:

1. Differentiate internal traffic from external traffic.
    - a. Open snort.conf in Notepad, find the line “var HOME\_NET any,” and replace “any” with the IP range and subnet mask (e.g., 10.0.0.0/24).



**Figure 3-17** Snort can detect more than 1,100 signatures.

- b. If there is more than one internal subnet, they can all be specified by putting them in brackets and separating them with commas.
  - c. Define the external network. Find the line “var EXTERNAL\_NET any,” and replace “any” with the IP address(es) of the external networks, or leave “any” to set all networks not defined in HOME\_NET as external.
2. Define the services on the network. Find the following lines and replace \$HOME\_NET with the IP address(es) of the server(s) running the the following services:
- var DNS\_SERVERS \$HOME\_NET
  - var SMTP\_SERVERS \$HOME\_NET
  - var HTTP\_SERVERS \$HOME\_NET
  - var SQL\_SERVERS \$HOME\_NET

**Snort Console** After installing and configuring Snort, the user must start it with a command such as the following:

```
snort -l C:\Snort\Log -c C:\Snort\etc\snort.conf -A console
```

This command tells Snort to write its log files to C:\Snort\Log. It also points out the location of the snort.conf file.

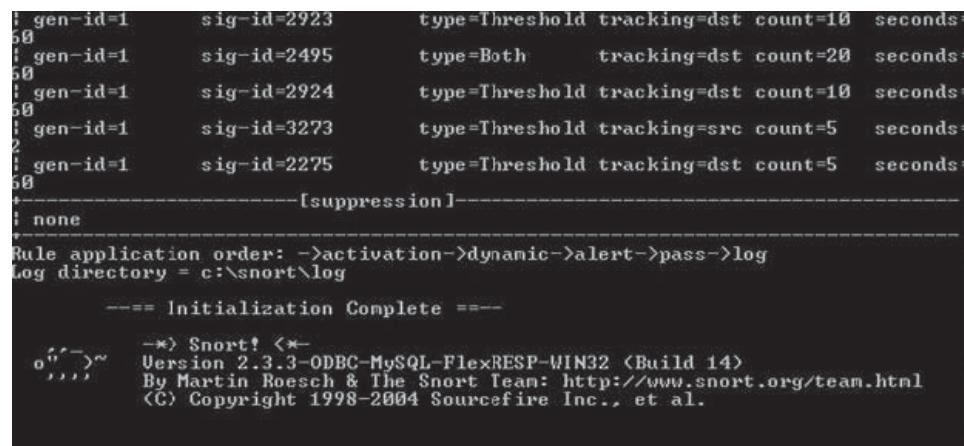
The **-A console** switch sends Snort output alerts to the console window. It notifies the user that an installation was successful (Figure 3-18).

**Snort Rules** Snort uses the popular libpcap library (for UNIX/Linux) or WinPcap (for Windows). Snort decodes all the packets passing through the network media to which it is attached by entering promiscuous mode. Based on the content of the individual packets and rules defined in the configuration file, an alert is generated.

There are a number of rules that Snort allows the user to write. In addition, each of these Snort rules must describe the following aspects:

- Any violation of the company’s security policy 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 by which a user thinks that a network packet is unusual, e.g., if the identity of the packet is not authentic

Snort rules, written for both protocol analysis and content searching and matching, should be robust and flexible. In this case, robust means the system should keep a rigid check on the activities taking place on the network and notify the administrator of any potential intrusion attempt. Flexible means the system must be compatible enough to act immediately and take necessary remedial measures according to the nature of the intrusion.



```

gen-id=1      sig-id=2923      type=Threshold tracking=dst count=10  seconds=
60
gen-id=1      sig-id=2495      type=Both      tracking=dst count=20  seconds=
60
gen-id=1      sig-id=2924      type=Threshold tracking=dst count=10  seconds=
60
gen-id=1      sig-id=3273      type=Threshold tracking=src count=5   seconds=
2
gen-id=1      sig-id=2275      type=Threshold tracking=dst count=5   seconds=
60
+-----[suppression]-----
| none
|
Rule application order: ->activation->dynamic->alert->pass->log
Log directory = c:\snort\log
==== Initialization Complete ====
o^__~  => Snort! <=-
              Version 2.3.3-ODBC-MySQL-FlexRESP-WIN32 (Build 14)
              By Martin Roesch & The Snort Team: http://www.snort.org/team.html
              (C) Copyright 1998-2004 Sourcefire Inc., et al.

```

**Figure 3-18** The **-A console** switch notifies the user that an installation was successful.

Both flexibility and robustness can be achieved using an easy to understand and lightweight rule-description language that aids in writing simple Snort rules. The two following principles must be kept in mind while writing Snort rules:

- Rule 1: No written rule must extend beyond a single line. Rules should be short, precise, and easy to understand.
- Rule 2: Each rule should be divided into two logical sections:
  - The rule header
  - The rule options

The rule header contains the rule's action, the protocol, the source and destination IP addresses, the source and destination port information, and the CIDR (Classless Interdomain Routing) block.

The rule-options section includes alert messages and information about which part of the packet should be inspected in order 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" ; )
```

**SnortSam** SnortSam is a plug-in for Snort. It is an open-source, lightweight IDS and can be compiled on any platform. The plug-in permits automated blocking of IP addresses on the following firewalls:

- Checkpoint Firewall-1
- Cisco PIX firewalls
- Cisco routers (using ACLs or null routes)
- Juniper firewalls
- IP Filter (ipf), available for various UNIX-like OSs such as FreeBSD
- FreeBSD's ipfw2
- OpenBSD's Packet Filter (pf)
- Linux IPchains
- Linux IPtables
- Linux EBtables
- WatchGuard Firebox firewalls
- 8signs firewalls for Windows
- MS ISA Server firewall/proxy for Windows
- CHX packet filter
- Ali Basel's Tracker SNMP

SnortSam is comprised of two pieces:

- The output plug-in within Snort
- An intelligent agent that operates on a firewall

The agent provides the following functions beyond blocking:

- White-list support of IP addresses that will never be blocked
- Time-override list
- Maximum block-time ceiling as well as minimum block-time definition for reporting entities
- Flexible, per-rule blocking specification, including rule-dependent block-time interval
- An SID filter list of allowed or denied SIDs, based on reporting entity
- Misuse/attack detection engine (including rollback support) that attempts to mitigate the risk of a self-inflicted denial of service in the IDS–firewall integration
- Repetitive (same IP) block prevention with customizable window to improve performance

- Twofish encrypted communication between Snort and the SnortSam agent
- True OPSEC support using the Checkpoint SDK
- Block tracking and block expiration for firewalls that do not support timeouts
- Multithreading for faster processing and simultaneous block on multiple devices
- File logging and e-mail notification of events

## Tools to Evade IDS

### **SideStep**

SideStep was written by Robert Graham to demonstrate IDS evasion techniques. The basic premise is that existing network IDS technology is based on a simplistic model of how networks work. In particular, the assumption is made that hackers will be nice and will play by the rules.

The program generates attacks using three modes:

1. *Normal*: This mode executes the attack/scan at the sophistication level of script kiddies. Most IDS should pick up these attacks.
2. *Evasion*: Evasion carries out the same attack, but this time using sophisticated IDS evasion techniques. None of these attacks are fragmented at the IP or TCP layer.
3. *False positive*: This mode does not attack the target, but instead, it does something relatively normal. In this mode, an alarm is generated when no condition is present to warrant one. However, many IDS falsely trigger on this.

### **Mendax**

Mendax is a simple TCP desynchronizer that injects overlapping segments in randomly generated order. It is a standalone TCP client program that can inject a simple attack signature or typed lines.

### **Stick**

Stick uses the Snort rule set and produces a C program via lex (a lexical analyzer that partitions the input text) which, when compiled, produces an IP packet capable of triggering that rule from a spoofed IP range into a target IP range. A function for each rule is produced along with a loop that then executes these rules in a random order. The tool currently produces these at about 250 alarms per second.

### **Fragrouter**

Fragrouter is a program for routing network traffic in such a way as to elude most network intrusion detection systems. It is designed to test the correctness of an NIDS according to specific TCP/IP attacks.

Fragrouter could be used to do the following:

- Obfuscate a “phf” attack against a Web server
- Obfuscate a buffer overflow attack against a DNS server

### **Anzen NIDSbench**

Anzen NIDSbench includes several tools, including Fragrouter. This forces all traffic to fragment and demonstrates how easy it is for hackers/crackers to do the same in order to evade intrusion detection. It accepts incoming traffic and then fragments it according to various rules.

### **ADMutate**

In the case of a purely signature-based IDS, ADMutate takes advantage of its weaknesses. It is able to avoid patterns that the IDS looks for. It can take an attack shellcode and transform it. Therefore, if the application-level data is put through a mutation algorithm, the user can obtain a functionally equivalent yet completely unique code sequence. This technique is quite easy to adapt to the needs of the exploit coder.

The preferred exploit is a buffer overflow as it has sufficient nonoperational code that can be altered to perform a number of other tasks. ADMutate attempts to encode the shellcode with a simple mechanism (XOR) so the shellcode will be unique to any NIDS sensor. This evades any shellcode signature analysis.

Usually, when an attacker tries a buffer overflow attack, an IDS will match a string contained in the data (or shellcode) of the attack and generate an alert. ADMutate generates different strings (or signatures) so that the IDS do not recognize the threat. This means that attackers can gain ground on security experts because it takes time for IDS developers to update their products. This situation is made more difficult because attackers can generate an infinite number of possible random strings.

## **Packet Generators**

### ***Aicmpsend***

*Aicmpsend* is an ICMP packet sender with features including ICMP flooding and spoofing. All ICMP flags and codes are implemented. An attacker can use this program for various DoS attacks, ICMP flooding, and firewall testing.

### ***Apsend***

*Apsend* is a TCP/IP/UDP/ICMP packet sender with the ability to perform SYN flood attacks, LAND attacks, DoS attacks, and spoofing. It also includes socket functions like Netcat. The attacker can specify many other options including time to live (TTL), type of service (ToS), sequence number, ACK number, urgent pointer, SYN/PUSH/ACK/RST/URG/FIN flag, window size, number of packets to send, and so on. This program can be used to test firewall configurations.

### ***Blast***

*Blast* is a small, quick TCP service stress-test tool. *Blast* does a large amount of work very quickly, and it can help spot potential weaknesses in network servers.

### ***CASL***

*CASL* is a high-level scripting language that allows an attacker to write simple scripts to invoke complex vulnerability tests, thereby avoiding hundreds of lines of low-level coding.

### ***Easy TcpIp Library***

*Easy TcpIp Library* is a library of functions to help a user make basic TCP/IP applications quickly and easily.

### ***Ettercap***

*Ettercap* is a network sniffer/interceptor/logger for switched LANs. It uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts. Data injection to an established connection is also possible. The attacker can sniff connections between local and remote hosts through a gateway using the MAC-based sniffing mode.

### ***Hping2***

*Hping2* is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies in much the same way as ping with ICMP replies. *Hping2* handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols. Using *Hping2*, an attacker can perform the following tasks:

- Network performance testing using protocols, packet size, ToS (type of service) and fragmentation
- Path MTU discovery
- File transfers, even between extremely strict firewall rules
- Traceroute functionality under different protocols
- Firewall testing
- Remote OS fingerprinting
- TCP/IP stack inspection

### ***ICMPush***

*ICMPush* is a tool that sends fully customized ICMP packets from the command line. It supports ICMP error types Unreachable, Parameter Problem, Redirect, and Source Quench, as well as the ICMP information types Timestamp, Address Mask Request, Information Request, Router Solicitation, Router Advertisement, and Echo

Request. ICMPPush also supports IP spoofing, broadcasting, and other useful features. It is a powerful program for testing and debugging TCP/IP stacks and networks.

### **Ippacket**

Ippacket is a command-line utility to construct IP/TCP/UDP/ICMP packets on a Linux system.

### **ipsend**

ipsend is a test tool included with the ipfilter package. The ipfilter package is used to provide Network Address Translation (NAT) or firewall services. It can be used to generate arbitrary IP packets on Ethernet-connected systems.

### **ISIC**

ISIC sends randomly generated packets to a target computer. The following are the primary uses of ISIC:

- To stress-test an IP stack
- To find leaks in a firewall
- To test the implementation of IDS and firewalls

The user can specify how often the packets will be fragmented, the IP options, the TCP options, the urgent pointer, and more. Programs for TCP, UDP, ICMP, IP with random protocols, and random Ethernet frames are included.

### **lcrzo**

lcrzo is a network library for network administrators and network hackers. Its main objective is to easily create network test programs. This library provides network functionalities for Ethernet, IP, UDP, TCP, ICMP, ARP, and RARP protocols. It supports spoofing, sniffing, and client and server creation. Furthermore, lcrzo contains high-level functions that deal with data storage and handling. Using all of these functions, the attacker can quickly create a network test program.

### **Libnet**

Libnet is a collection of routines to help with the construction and handling of network packets. It provides a portable framework for low-level network packet writing and handling. Using Libnet, a user can create quick and simple packet assembly applications with minimal programming effort. Libnet features portable packet creation interfaces at the IP layer and link layer, as well as a host of supplementary and complementary functionality.

### **LibnetNT**

LibnetNT is a Win32 port of Libnet. LibnetNT has the exact same functionality and abilities as Libnet, except that LibnetNT can be used to develop low-level packet injection programs on Windows NT 4.0 and Windows 2000. LibnetNT requires WinPcap for its functionality.

### **MGEN Toolset**

The Naval Research Laboratory's (NRL) Multi-Generator (MGEN) Toolset provides programs for sourcing/sinking real-time multicast/unicast UDP/IP traffic flows. It also includes support for scripted generation of packet flows with the IP ToS field set. The MGEN tools transmit and receive time-stamped, sequence-numbered packets. Posttest analysis of the log files can be performed to assess network or network component ability to support the given traffic load in terms of packet loss, delay, delay jitter, and so on. MGEN has been used to evaluate the capability of networks and devices to properly provide IP multicast and RSVP support.

### **Mpac**

Mpac is a Linux tool for creating Ethernet TCP/IP packets with payloads. Packets are built with plaintext configuration files representing each layer (Ethernet, IP, and ICP payload).

### **Nemesis**

The Nemesis Project is a Libnet-based toolset designed to be a command-line-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol and allows for useful scripting of injected packet streams from simple shell scripts.

### **Net::RawIP**

Net::RawIP is a Perl module that allows for the easy manipulation of raw IP packets, with the optional feature of manipulating Ethernet headers. The module has been tested on Linux, FreeBSD, OpenBSD, BSDI, and Solaris.

### **Netcat**

Netcat is a simple UNIX utility that reads and writes data across network connections using TCP or UDP. It is designed to be a reliable back-end tool that can be used directly or easily driven by other programs and scripts. Netcat is a feature-rich network debugging and exploration tool because it can create almost any kind of connection that an attacker would need, and it has several interesting built-in capabilities. Netcat also allows an attacker to specify source ports for arbitrary TCP and UDP connections, bind as a server, and use source routing.

### **Netsh**

Netsh is a tool designed to debug network applications. It enables the user to dump incoming packets and send customized packets in ASCII or hexadecimal format. Netsh is also able to forward the dumped packets. It has been designed to be inserted between a client and a server application, even if it can be used differently.

### **PacketX**

PacketX is a native Windows NT firewall testing tool that allows for complete TCP/IP packet creation and provides a method for verifying the claims of a firewall vendor. Featuring packet spoofing technology and raw packet creation techniques, this tool is essentially a packet cannon. It shoots custom packets at a firewall in order to verify the approval/denial of Internet domain addresses against firewall ACLs.

### **Send Packet**

Send Packet is a small but powerful program to test how a network responds to specific packet content. The attacker can forge (modify the headers of) TCP/UDP/ICMP/IP packets and send them through the network via a configuration file and/or command-line parameters. Its modular philosophy allows for the specification of which modules the attacker wants to include. The attacker can also modify almost all of the parameters in the headers of the TCP/UDP/ICMP/IP set of protocols. This program is useful to test networks, firewalls, and so on.

### **SendIP**

SendIP is a command-line tool for sending arbitrary IP packets. It has a large number of command-line options to specify the content of every header of a TCP, UDP, ICMP, or raw IP packet. It also allows for the addition of any data to the packet. Checksums can be calculated automatically, but sending out incorrect checksums is also supported.

### **SING**

SING stands for Send ICMP Nasty Garbage. SING is a tool that sends fully customized ICMP packets from the command line. Its main purpose is to replace the ping command while adding certain enhancements (fragmentation, spoofing, etc.).

### **Socket Script**

Socket Script is primarily for people who want to create networking-oriented programs but do not want to learn the details of using sockets. It has multiple network commands that enable the attacker to tell the script interpreter where to connect. All the interpreter has to do is focus on the script itself, leaving the connection parts to Socket Script. It is good for both nonprogrammers as well as experienced developers. Socket Script has more than 100 commands and can be compiled as text-only or graphic, using GTK (GIMP Toolkit). The basic concept of GTK is to start a script in binary.

### **Spak**

Spak (Send PAcKet) is a collection of programs that can be used to create and send a packet over a network. Spak is designed to be modular and allows as much control as possible over the design of the packet.

## **TCP/IP Library**

TCP/IP Library is a library for Windows 2000 that allows arbitrary packet creation. It allows the attacker to send raw IP headers, perform IP spoofing, and play with the nuts and bolts of networking protocols.

### **Tcpreplay**

TcpReplay is aimed at testing the performance of an NIDS by replaying real background network traffic to hide attacks. TcpReplay allows the user to control the speed at which the traffic is replayed, and it can replay arbitrary Tcpdump traces. Unlike programmatically generated artificial traffic, which does not exercise the application/protocol inspection that an NIDS performs and does not reproduce the real-world anomalies that appear on production networks (asymmetric routes, traffic bursts/lulls, fragmentation, retransmissions, etc.), TcpReplay allows for exact replication of real traffic on real networks.

### **The Packet Shell**

The Packet Shell tool is provided by Sun and was originally meant for use with Solaris 2.5.1 and above. The Packet Shell is an extensible Tcl/Tk-based software toolset for protocol development and testing. The Packet Shell creates Tcl commands that allow the user to create, modify, send, and receive packets on networks.

### **USI++**

USI++ is a powerful, low-level network library that allows an attacker to send modified/spoofed packets over the network. USI++ runs on Linux and FreeBSD systems and supports 10-MBit, 100-Mbit, and PPP devices.

### **Xipdump**

Xipdump is a protocol analyzer and tester. It's a kind of graphical Tcpdump, which adds the possibility of changing packet values and resending them. The graphical representation of a packet is intended to offer a complete, customizable view at a glance.

## **Tools to Breach Firewalls**

### **007 Shell**

007 Shell is a simple client/server C program used for remotely administering a system over a network using techniques similar to Loki. That is, covert ICMP ECHO\_REPLY packets encapsulate the command and response messages within the packet payload.

The 007 Shell distribution is split into a reusable tunneling library and a shell front end, with the same program serving as either client or server. Data is padded out to multiples of 64 bytes, virtually guaranteeing the appearance of ping packets, as it also employs only ping reply packets.

007 Shell is a backdoor that can either be placed by an attacker after a successful intrusion or deployed as a Trojan if an unsuspecting user executes a malicious program or script.

Unlike Loki, the 007 Shell client sends commands in the ECHO\_REPLY packet payload that the server responds to with a new ECHO\_REPLY packet. The function of ECHO\_REPLY is to return the identical payload received from an ECHO (ICMP TYPE 8) back to the originator, as a connectivity test.

007 Shell requires raw IP network access, which is a way to circumvent the operating system's native IP networking stack in order to listen to and create its own crafted packets. Because root permission is required for ICMP raw socket access, the program makes no attempt to hide itself on the local system. Because data transmission is in plaintext, it is easy to detect.

### **ICMP Shell**

ICMP Shell (ISH) is a telnetlike protocol providing the capability of connecting to a remote host in order to open a shell using only ICMP for input and output. ICMP Shell was written in C for the UNIX environment. It allows the administrator to access the computer remotely using ICMP. The ICMP Shell server is run in daemon mode on the remote server.

When the server receives a request from the client, it strips the header and looks for the ID field. Upon finding a match, the server pipes the data to /bin/sh. It then reads the results from the pipe and sends the results back to the client. The client can then print the results to stdout. By default, the client and server send packets with an ICMP type of 0 (ICMP\_ECHO\_REPLY), but this can be changed on both the client and server sides. ICMP

Shell does not depend on the ICMP type sent from either the client or the server end. Moreover, the types do not have to match.

ICMP Shell doesn't only pipe commands to a server and send back the output. It also works with interactive programs (for example, gdb). However, there is a minor problem. ICMP Shell is unable to display a shell prompt (#), as there is no way to differentiate between a command and interaction with a program. Like 007 Shell, ICMP Shell uses raw sockets on both the client and server side; therefore, root privileges are required to use this program.

### **AckCmd**

AckCmd provides a remote command shell to Windows 2000 systems. AckCmd is a backdoor client/server program that lets an attacker open a remote command prompt to another system (running the server part of AckCmd). It communicates using only TCP ACK segments. This way, in some cases the client component is able to directly contact the server component through a firewall. Although it uses TCP packets for transport like traditional remote shells, there are a number of aspects that make the program particularly covert.

AckCmd was designed to exploit weaknesses in many firewall and IDS rules. AckCmd communicates using only TCP ACK segments rather than more typically examined TCP SYN packets. The data segment of each originating ACK contains buffered command-line data and elicits a TCP RST from the remote side. The response is then presented in a new ACK back to the originator.

While an extremely fast user can produce an abnormally large rate of RST (reset) packets, the traffic pattern looks like an already established (and torn down) connection and is unlikely to raise any flags. In addition, the choice of client-side TCP port 80 and server-side port 1054 increases the likelihood of successful firewall traversal and reduces the risk of detection. However, the packets are not properly formatted for HTTP, the program is plainly visible on the task list, and the command-line transaction in plaintext is easily observable if an administrator knows it is there.

### **Covert\_TCP**

Files are transferred over the network by splitting them into different segments. Each segment has a value attached to it to allow the destination of the respective files to know which segments came and how to rearrange them. The attacker, who has access to various tools available in the wild, can easily manipulate this way of transferring files.

Covert\_TCP is one such tool that manipulates TCP/IP headers to transfer a file, one byte at a time, to a destination host. This technique helps in breaching a firewall from inside as well as exporting data with innocent-looking packets that contain insufficient data for sniffers or firewalls to analyze.

## **Common Tools for Testing Firewalls and IDS**

### **FTester**

Ftester (Figure 3-19) is a tool designed for testing firewalls and intrusion detection systems. It is based on a client/server architecture for generating real TCP/IP connections. The client is a packet generation tool (ftest), while the server (ftestd) is an intelligent network listener capable of processing and replying to ftest-generated packets. All packets generated by ftest have a special signature encoded in the payload that permits identification.

Ftester's ability to simulate real TCP/IP connections allows users to test stateful inspection firewalls and IDS. FTester offers additional features for manipulating the traffic type, timing options, and connection states so that the administrator may fully test the stack of the security device and configure the security policy.

FTester can spoof IP source addresses. Because ftestd, using the payload identifier, can distinguish packets generated by ftest, FTester is able to simulate spoofing of real connections.

**Basic Configuration** All testing is conducted using the packet injector (ftest) on a host placed on one side of the firewall, and the listener (ftestd) on a host placed on the other side of the firewall. The placement depends on which firewall policy (rule) is to be checked. For example, to test inbound filtering, ftest must be used on the external segment and ftestd on an internal one. Testing outbound filtering is equally important. In this case, the tester would reverse the placement of the client and the server.

The definitions of the packets that will be sent are specified in a configuration file called ftest.conf. In all examples the destination address represents either the host where ftestd is listening or a host from which traffic can be captured. The source address can be any host or network. However, while sending and testing spoofed traffic, it is important to verify that any intermediate routers will route the spoofed source. Generally, placing ftest and ftestd close (in terms of hops) to the firewall makes the spoof attempt easier to configure and execute.

To issue a TCP packet to destination 10.1.7.1, port 80 from source 192.168.0.10, port 1024, with the SYN flag and ToS set to 0, use 192.168.0.10:1024:10.1.7.1:80:S:TCP:o. In the previous example, to set the PUSH and ACK flags, use: 192.168.0.10:1024:10.1.7.1:80:TCP:o.

To send a UDP packet to destination 10.1.7.1, port 53, from source 192.168.0.10, port 53 with ToS set to 0, use 192.168.0.10:53:10.1.7.1:53::UDP:o.

Similarly, to send an ICMP packet, type 3 code 5, and use 192.168.0.10::10.1.7.1::ICMP:3:5.

FTester allows one to specify ranges for source address, source port, and destination port. Source address can also be specified in CIDR form (e.g., 192.168.0.1-255:1024:10.1.7.1:80:S:TCP:o, 192.168.0.10:1024:10.1.7.1:1-65535:S:TCP:o).

A stop signal is necessary to tell the ftestd that the test is completed. The stop signal can be a TCP, UDP, or ICMP packet, for example, stop signal=192.168.0.1:666:10.1.7.1:666:S:TCP:o. The arrival of this packet will cause the sniffer to terminate. Any packet specified in the configuration file after the stop signal directive will not be seen by ftestd.

**Figure 3-19** FTester is designed to test firewalls and IDS.

```
- ftest.log -
# ftest started
1 - 192.168.0.10:1025 > 10.1.7.1:1 S TCP 0
2 - 192.168.0.10:1026 > 10.1.7.1:2 S ICMP 0
3 - 192.168.0.10:1025 > 10.1.7.1:3 S TCP 0
... [deleted]
1023 - 192.168.0.10:1025 > 10.1.7.1:1023 S TCP 0
1024 - 192.168.0.10:1025 > 10.1.7.1:1024 S TCP 0
1025 - 192.168.0.10:1025 > 10.1.7.1:1025 S TCP 0
1026 - 192.168.0.10:1025 > 10.1.7.1:3128 S TCP 0
1027 - 192.168.0.10:80 > 10.1.7.1:1025 PA TCP
# ftest stopped
```

**Figure 3-20** The output displays every packet sent.

**Basic Usage in Firewall Testing** First, see how FTester can be used to find some simple firewall filtering policies.

**Step 1:** For testing which privileged services can be reached from the outside, the following simple configuration file can be used.

```
# checking privileged ports
192.168.0.10:1025:10.1.7.1:1-1025:S:TCP:0
# checking proxy port
192.168.0.0:1025:10.1.7.1:3128:S:TCP:0
stop signal=192.168.0.10:80:10.1.7.1:1025:S:TCP:0
```

It is important to be sure the stop signal will reach ftestd. In this case, it has been verified that the firewalled host can surf the Web, so a reply from port 80 should be fine.

**Step 2:** Start ftestd as root on Host B with the command `ftestd -i eth0 -v`. Inject the packets as root on Host A with the command `ftest -f ftest.conf -v -d 0.01`. The output displays every packet sent and the ftest.log file is created (Figure 3-20).

On Host B, ftestd shows the same messages for each packet received and creates the ftestd.log file. It should be noted that each packet is marked with a unique identifier, the first number of the line, which corresponds to the IP packet's ID field. This will help when comparing the different log files.

```

Authorized packets:
-----
21 - 192.168.0.10:1025 > 10.1.7.1:21 S TCP 0
22 - 192.168.0.10:1025 > 10.1.7.1:22 S TCP 0
23 - 192.168.0.10:1025 > 10.1.7.1:23 S TCP 0
25 - 192.168.0.10:1025 > 10.1.7.1:25 S TCP 0
80 - 192.168.0.10:1025 > 10.1.7.1:80 S TCP 0
110 - 192.168.0.10:1025 > 10.1.7.1:110 S TCP 0
113 - 192.168.0.10:1025 > 10.1.7.1:113 S TCP 0
1027 - 192.168.0.10:80 > 10.1.7.1:1025 PA TCP 0
Modified packets (probably NAT):
-----
443 - 192.168.0.10:1025 > 10.1.7.1:443 S TCP 0
        ffffffff>>>>>
443 - 192.168.0.10:1025 > 10.1.7.5:443 S TCP 0
Filtered or dropped packets:
-----
1 - 192.168.0.10:1025 > 10.1.7.1:1 S TCP 0
2 - 192.168.0.10:1025 > 10.1.7.1:2 S TCP 0
3 - 192.168.0.10:1025 > 10.1.7.1:3 S TCP 0
... (deleted)
1026 - 192.168.0.10:1025 > 10.1.7.1:3128 S TCP 0

```

**Figure 3-21** The two log files can be compared using freport.

**Step 3:** For the final step, two log files are copied onto the same host and can be compared with freport using the command `freport ftest.log ftestd.log`. The report generated looks like the one shown in Figure 3-21.

FTP, telnet, SSH, SMTP, HTTP, POP3, and auth are apparently reachable from the outside, HTTPS is forwarded to host 10.1.7.5, and the rest—including the proxy port—are filtered. NAT, with respect to the destination address, can be detected only if the user sniffs on a nonswitched environment; otherwise, only port address translation or source address translation can be detected.

**Testing Stateful Inspection Firewalls** The outcome of sniffing packet 1027 (the PSH/ACK from port 80) in the example displays that the firewall inside the test is just a simple one, unable to perform connection tracking. In the case of stateful examination however, firewalls are more likely to be established in real environments.

Tracking of a connection is usually done by stateful inspection firewalls. They do not forward and pass packets that do not match. A real connection should be established with proper SYN, SYN/ACK, and ACK handshakes. It should be connected for the purpose of testing the filtering policies related to TCP PSH, ACK, URG, RST, and FIN packets. This should be done prior to sending the packets with correct sequence numbers so the tested process returns the correct replies. The stack of the destination host replies with the spoofed packets during the simulation of the connection with the spoofed source address. The real host resets the connection because it has not received responses.

Two things must be done in this case:

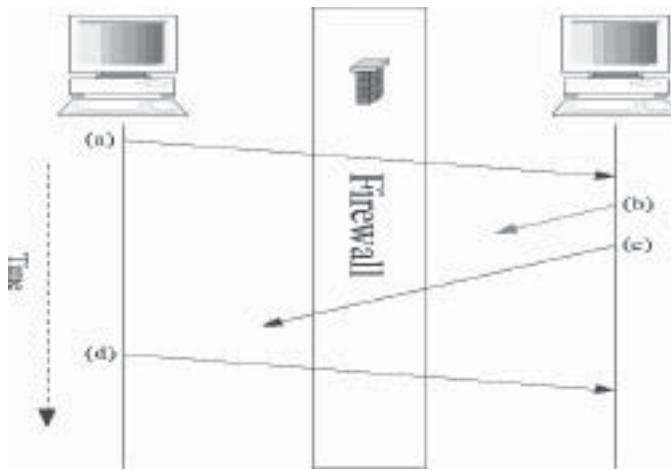
- Prevent the tested host stack reply from reaching the firewall and the spoofed host itself
- Make sure that the ftestd reply will traverse the firewall but will not reach the spoofed host

Setting a very low default hides the tested host stack reply. Setting the TTL to a low value equal to the hop delay between ftestd and the firewall hides the ftestd reply from the spoofed host.

Refer to the diagram in Figure 3-22 to see how this works.

- Packet (a) is the first connection request.
- Packet (b) is the destination host stack reply forced to have a low TTL value.
- Packet (c) is the ftestd reply with enough TTL to make it through the firewall.
- Finally, packet (d) completes the three-way handshake.

In this way the firewall is fooled without involving the real host, whose address has been spoofed.



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

**Figure 3-22** Setting a very low default hides the tested host stack reply.

```
- ftest.conf -
# simulating a ssh connection
connect=192.168.0.10:1025:10.1.7.1:22:AP:TCP:0
# checking unmatched RST packets
192.168.0.10:1025:10.1.7.1:23:UR:TCP:0
# checking matched RST packets
connect=192.168.0.10:1025:10.1.7.1:23:UR:TCP:0
stop_signal=192.168.0.10:1025:10.1.7.1:80:S:TCP:0

And again:

[root@hostb]# ./ftestd -i eth0 -s 0:3 -v
[root@hosta]# ./ftest -f ftest.conf -v -d 0.01 -s 1
Sent Syn Probe => 192.168.0.10:1025 > 10.1.7.1:22 S TCP
Sleeping for 1 seconds

Sent Ack Reply => 192.168.0.10:1025 > 10.1.7.1:22 A TCP
3 - 192.168.0.10:1025 > 10.1.7.1:22 AP TCP 0
5 - 192.168.0.10:1025 > 10.1.7.1:23 UR TCP 0
Sent Syn Probe => 192.168.0.10:1025 > 10.1.7.1:23 S TCP
Sleeping for 1 seconds
Sent Ack Reply => 192.168.0.10:1025 > 10.1.7.1:23 A TCP
8 - 192.168.0.10:1025 > 10.1.7.1:23 UR TCP 0
Stop packet => 192.168.0.10:1025 > 10.1.7.1:80 S TCP
```

**Figure 3-23** Connection spoofing mode can be activated with the "connect=" prefix.

**Connection Spoofing Mode** This mode can be activated with the "connect=" prefix. Use this mode with packets that usually would not traverse a stateful inspection firewall (Figure 3-23).



This time, ftest is configured to wait 1 second for fttestd replies. The log comparison can be seen in Figure 3-24.

The first RST has been dropped. This confirms that there is a stateful inspection firewall.

```

Authorized packets:
-----
3 - 192.168.0.10:1025 > 10.1.7.1:22 PA TCP D
8 - 192.168.0.10:1025 > 10.1.7.1:23 UR TCP D
10 - 192.168.0.10:1025 > 10.1.7.1:80 S TCP D
Modified packets (probably NAT):
-----
????????????>>>>>
Filtered or dropped packets:
-----
5 - 192.168.0.10:1025 > 10.1.7.1:23 UR TCP D

```

Figure 3-24 The first RST has been dropped.

```

ftest.conf
ida=192.168.0.10:1025:10.1.7.1:25:S:TCP:0:VRFY
ida=192.168.0.10::10.1.7.1::ICMP:3:5:+++ath
ids-conn=192.168.0.10:23:10.1.7.1:1025:PA:TCP:0:to      su      root
ids-conn=192.168.0.10:1025:10.1.7.1:80:PA:TCP:0:cmd.exe
ids-conn=192.168.0.10:1026:10.1.7.1:80:PA:TCP:0:ftp.exe
insert/etc/snort/exploit.rules      192.168.0.10      10.1.7.1
          0
insert-comm /etc/snort/web-misc.rules 192.168.0.10 10.1.7.1 0

```

Figure 3-25 The ftest tool can directly use a Snort rule definition file.

If more than one packet is specified with the “connect=” prefix and the same connection parameters (source address/port, destination address/port) are chosen, then -r/-F flags must be used to correctly close (with an RST or a FIN handshake) each connection. Otherwise, if the firewall is performing sequence number tracking, connections other than the first will be blocked. Sometimes leaving the connection open can be useful as it will flood the firewall and fill the connection state table. Additionally, it can be set to fragment, or segment, all IP and TCP traffic to see how the firewall reacts.

**IDS Testing** The IDS testing option permits the injection of arbitrary packets with a custom payload meant to trigger an IDS alert. In this way, visibility of the IDS on the network and its ability to sniff fragmented/segmented packets can be tested. A number of common IDS evasion techniques are also implemented for activation during packet injection. Additionally, ftest can directly use a Snort rule definition file. A syntax example can be seen in Figure 3-25.

The -conn option works just like the connect option. This is useful if the IDS is performing a stateful inspection. When using this mode, ftestd is needed; otherwise, when the IDS is being tested, the sniffer is not required. The insert option takes four arguments: the definition file, the source address, the destination address, and the type of service. Use this feature to test Snort’s ability to elude evasion techniques. Use a common alert and assume that Snort is performing stateful inspection, discarding unmatched traffic.

**Step 1:** The configuration file is as follows:

```
ida-conn=192.168.0.1:1025:10.7.0.1:80:PA:TCP:0:cmd.exe
```

**Step 2:** Start Snort on the sensor with the command `snort -A full -c /etc/snort/snort.conf -D -b -d -1 eth0 -1 /var/log -s -z`.

**Step 3:** Start ftestd as root on Host B with the command `ftestd -I eth0-c0:3-v`.

**Step 4:** Inject the packets as root on Host A with the command `ftest -f ftest.conf-v-d 0.01-s 1-F`. Immediately, Snort alerts with the syslog message seen in Figure 3-26.

Repeat the process using tricks such as fragmentation and evasion techniques.

Snort correctly identifies the triggering payload each time:

- Jun 5 16:29:32 lcars snort[4467]: [111:5:1] spp\_stream4: DATA ON SYN detection {TCP} 192.168.0.10:1025 -> 10.1.7.1:80
- Jun 5 16:29:34 lcars snort[4467]: [1:1002:2] WEB-IIS cmd.exe access [Classification: Web Application Attack] [Priority: 1]: DATA ON SYN detection {TCP} 192.168.0.10:1025 -> 10.1.7.1:80

```

Jun 5 16:25:13 lcars snort[4467]: [111:5:1] spp_stream4: DATA ON SYN
detection [Classification: Unknown Traffic] [Priority: 3]: {TCP}
192.168.0.10:1025 -> 10.1.7.1:80
Jun 5 16:25:14 lcars snort[4467]: [1:1002:2] WEB-IIS cmd.exe access
[Classification: Web Application Attack] [Priority: 1]: {TCP}
192.168.0.10:1025 -> 10.1.7.1:80

```

**Figure 3-26** Snort alerts with a syslog message.

- Jun 5 16:30:16 lcars snort[4467]: [111:5:1] spp\_stream4: DATA ON SYN detection {TCP} 192.168.0.10:1025 -> 10.1.7.1:80
- Jun 5 16:30:18 lcars snort[4467]: [1:1002:2] WEB-IIS cmd.exe access [Classification: Web Application Attack] [Priority: 1]: DATA ON SYN detection {TCP} 192.168.0.10:1025 -> 10.1.7.1:80
- Jun 5 16:30:40 lcars snort[4467]: [111:5:1] spp\_stream4: DATA ON SYN detection {TCP} 192.168.0.10:1025 -> 10.1.7.1:80
- Jun 5 16:30:42 lcars snort[4467]: [1:1002:2] WEB-IIS cmd.exe access [Classification: Web Application Attack] [Priority: 1]: DATA ON SYN detection {TCP} 192.168.0.10:1025 -> 10.1.7.1:80
- Jun 5 16:31:00 lcars snort[4467]: [111:5:1] spp\_stream4: DATA ON SYN detection {TCP} 192.168.0.10:1025 -> 10.1.7.1:80
- Jun 5 16:31:02 lcars snort[4467]: [1:1002:2] WEB-IIS cmd.exe access [Classification: Web Application Attack] [Priority: 1]: DATA ON SYN detection {TCP} 192.168.0.10:1025 -> 10.1.7.1:80

The generated log will help clarify what has been sent:

```

# ftest started
IDS mode > 3 - 192.168.0.10:1025 > 10.1.7.1:80 "cmd.exe" PA TCP
0
# ftest stopped
# ftest started
IDS mode > 3 - 192.168.0.10:1025 > 10.1.7.1:80 "cmd.exe" PA TCP
0
# ftest stopped
# ftest started
IDS mode > 3 - 192.168.0.10:1025 > 10.1.7.1:80 "cm" PA TCP 0
IDS mode > 4 - 192.168.0.10:1025 > 10.1.7.1:80 "d." PA TCP 0
IDS mode > 5 - 192.168.0.10:1025 > 10.1.7.1:80 "exe" PA TCP 0
# ftest stopped
# ftest started
IDS mode > 3 - 192.168.0.10:1025 > 10.1.7.1:80 "c" PA TCP 0
IDS mode > 4 - 192.168.0.10:1025 > 10.1.7.1:80 "m" PA TCP 0
IDS mode > 5 - 192.168.0.10:1025 > 10.1.7.1:80 "d" PA TCP 0
IDS mode > 6 - 192.168.0.10:1025 > 10.1.7.1:80 "." PA TCP 0
IDS mode > 7 - 192.168.0.10:1025 > 10.1.7.1:80 "e" PA TCP 0
IDS mode > 8 - 192.168.0.10:1025 > 10.1.7.1:80 "x" PA TCP 0
IDS mode > 9 - 192.168.0.10:1025 > 10.1.7.1:80 "e" PA TCP 0
# ftest stopped
# ftest started
IDS mode > 3 - 192.168.0.10:1025 > 10.1.7.1:80 "cmd" PA TCP 0
IDS mode > 4 - 192.168.0.10:1025 > 10.1.7.1:80 "" S TCP 0
EVASION PACKET!
IDS mode > 5 - 192.168.0.10:1025 > 10.1.7.1:80 ".exe" PA TCP 0
# ftest stopped

```

**Conclusions and Recommended Usage** By applying FTester's ability to create real traffic instead of mere probes and port scans, the user can determine whether a security device's configuration complies with predefined security policies. By creating TCP connections with different options and states, users can evaluate security device stack integrity and its behavior under high-traffic load conditions. Additionally, the user can test IDS stateful inspection capabilities and alarm triggering traffic sensitivity. This is very important, considering script kiddies often flood networks with false alarms, expecting such alarms will be ignored when proper stateful inspection is in place. Finally, because both the ftest and ftestd scripts are entirely command line based and configuration file driven, it is possible to automate any tests the user creates.

### Traffic IQ Pro

Traffic IQ Pro (Figure 3-27) enables security professionals to quickly and easily audit and validate the behavior of security devices by generating standard application traffic, or to attack traffic between two virtual machines. The unique features and packet transmission capabilities of Traffic IQ Pro make the task of reliably auditing, validating, and proving security compliance very easy and quick to complete.

Traffic IQ Pro can be used to assess, audit, and test the behavioral characteristics of the following nonproxy, packet-filtering devices:

- Application-layer firewalls
- Intrusion detection systems
- Intrusion prevention systems
- Routers and switches

### Next-Generation Intrusion Detection Expert System (NIDES)

NIDES (Next-Generation Intrusion Detection Expert System) monitors user activity on multiple target systems linked through the Ethernet. This tool resides on its own workstation and analyzes audit data acquired from various interconnected systems that track abnormal behavior of systems.

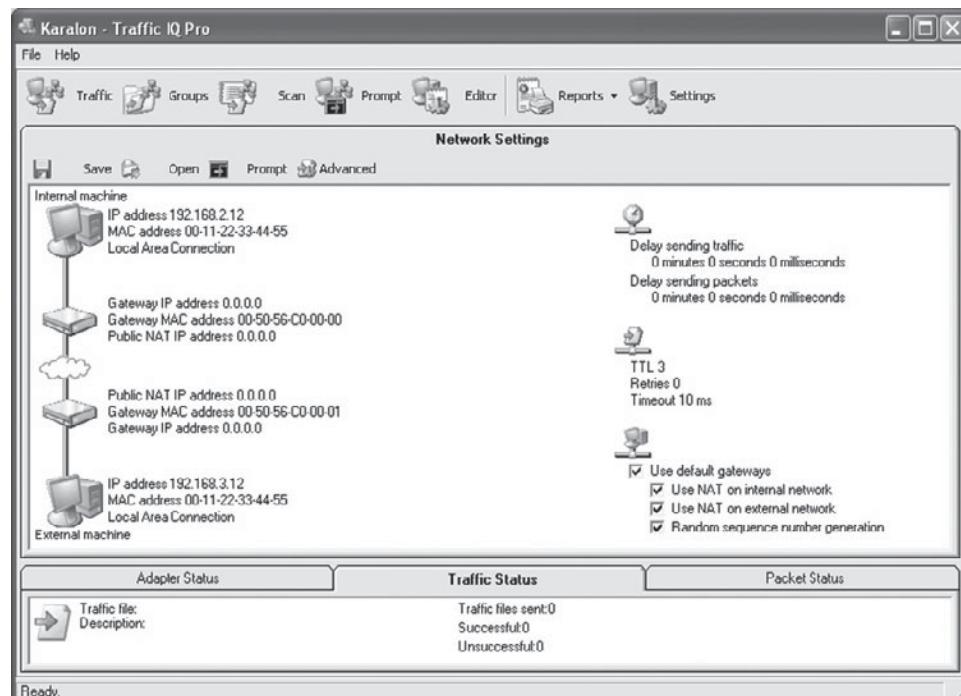


Figure 3-27 Traffic IQ Pro allows users to audit security devices.

NIDES performs the following two types of analysis:

1. *Rule-based signature analysis*: Employs expert rules to characterize known intrusive activity represented in activity logs and raises alarms when the observed activity logs and the rule encoding match
2. *Statistical-profile-based, anomaly detection*: Maintains historical profiles of user's access and triggers an alarm when observed activity varies from established patterns of usage for an individual

NIDES contains archives that store audit records, analyze results and alerts, and allow browsing of an archive. It includes a system monitoring facility that displays information about the monitored system. This tool permits the security officer to experiment with new statistical parameter settings or new rule-based configurations. Test results are archived for the purpose of comparison. NIDES operates in both real time and batch mode. In real-time mode, NIDES monitors the user activities continuously; in batch mode, it performs periodic batch analysis of audit data. NIDES can monitor numerous, possibly heterogeneous, machines. The monitored systems provide audit data to NIDES for analysis. The process that runs on each monitored system converts audit data in the monitored system's native audit record format to a generic audit. NIDES receives data from multiple monitored systems and merges the data into a single audit record stream for analysis.

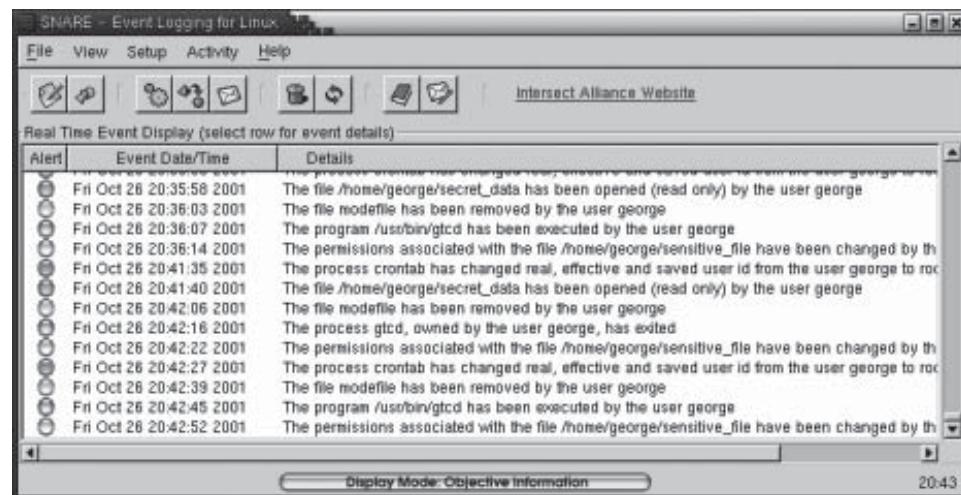
### **SecureHost**

SecureHost, along with SecureHost Console, is a Web-based management system installed on a Microsoft Windows 2000 server. It is a host-based intrusion detection system. SecureHost acts as a deterrent to attack. It gives support to Windows 2000/NT and Solaris platforms. It deploys intelligent agents to defend against any intrusion. Agents react to incidents depending on the application security policy of an organization. It integrates with other SecureNet intrusion detection products, thus maximizing security. It monitors file integrity in real time. Downtime of network components is reduced. Total cost of ownership is low as it detects intrusions by adapting a policy-based approach as opposed to conventional, signature-based detection.

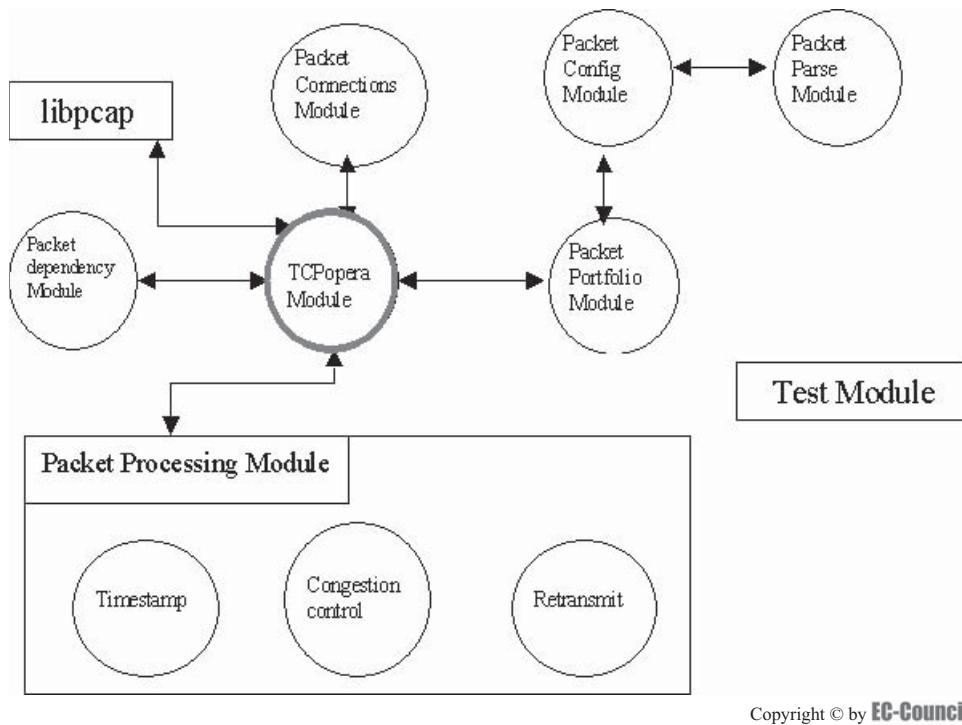
### **SNARE (System iNtrusion Analysis and Report Environment)**

SNARE (Figure 3-28) is an open-source, host-based intrusion detection tool designed for Linux. This tool contains three main components:

1. *Dynamic kernel audit module*: The dynamic kernel audit module component covers critical system calls like mkdir, open, and execve. This module collects information about users and processes that have executed the calls and stores this information in a temporary buffer.
2. *User space audit daemon*: The user space audit daemon component then reads the event data from the temporary buffer by using the command /proc/audit <device> and converts this information from binary format to text format.
3. *Front-end GUI*: The front-end GUI component is used to display these events in a colorful manner and display the text in an easy-to-read window. It provides information related to event logs on a configuration screen.



**Figure 3-28** SNARE is a host-based intrusion detection tool.



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

**Figure 3-29** TCPOpera enables IDS to handle retransmitted packets.

## TCPOpera

The TCPOpera tool (Figure 3-29) enables the replication of different variations of a base file with a given Tcpcap file. It provides the ability to define the network conditions and replay the traffic in a realistic environment where packets are delayed or lost.

TCPOpera can also provide IDS testing environments with traffic that displays TCP performance accurately. Overall, this tool holds a simple working paradigm that enables IDS to handle retransmitted packets and track TCP connection states.

## Firewall Informer

Firewall Informer (Figure 3-30) actively tests the configuration and performance of any firewall or other packet-filtering device, including routers, switches and gateways.

Firewall Informer can perform the following functions:

- Send and receive packets without the need for protocols to be bound to the network cards
- Customize testing via rate of transmission (per attack or per packet), packet timeout, and expiration values
- Retransmit stateful attacks between two unique hosts from one PC
- Spoof any source or destination IP address and port combination
- Spoof any source or destination MAC address
- Guarantee packet delivery
- Control packet expiration, timeout, and retries

## Atelier Web Firewall Tester

Atelier Web Firewall Tester (Figure 3-31) is a tool for probing personal firewall software strengths against outbound attempts from network Trojan horses and other malware or spyware. It is intended to help the user enhance existing personal firewall software for improved protection. Atelier Web Firewall Tester offers six different tests, each of which establishes an HTTP connection and attempts to download a Web page.

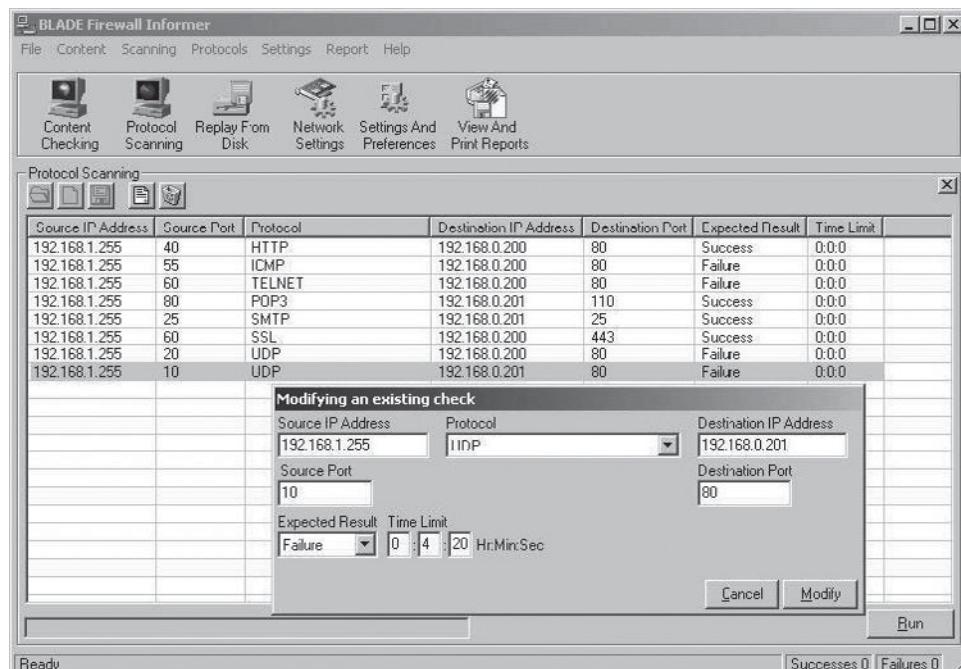


Figure 3-30 Firewall Informer actively tests firewall configurations.

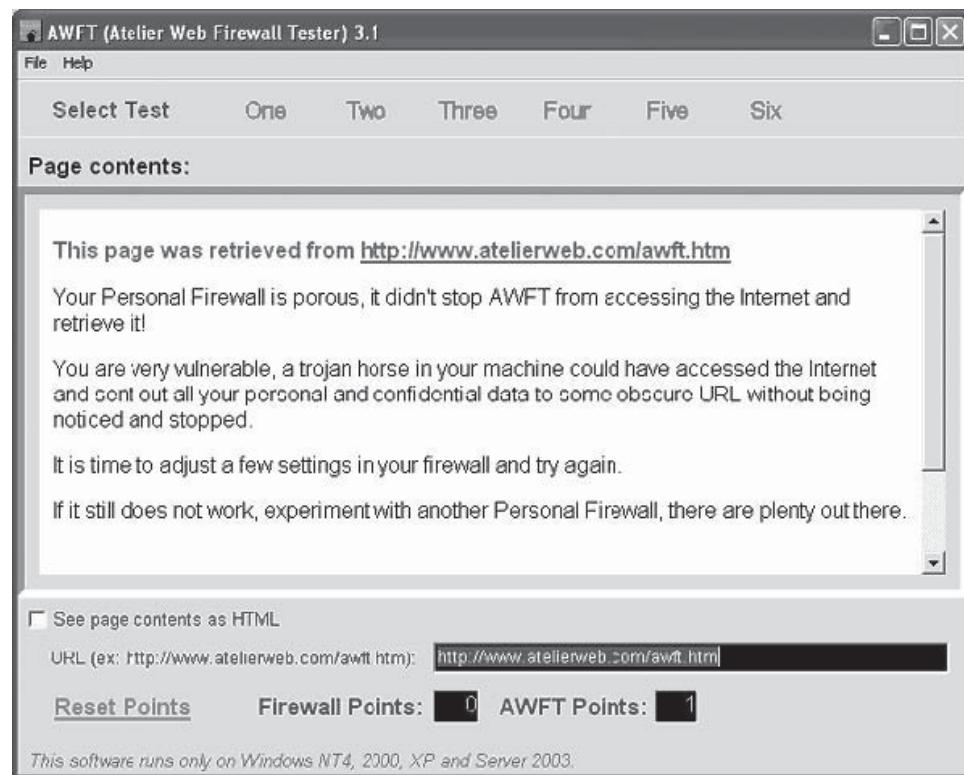


Figure 3-31 Atelier Web Firewall Tester tests personal firewall software.

## Honeypot Tools

### SPECTER

SPECTER (Figure 3-32) is a smart honeypot system. It simulates a complete system, providing an interesting target to lure hackers away from production systems. SPECTER offers common Internet services such as SMTP, FTP, POP3, HTTP, and telnet, which appear perfectly normal to attackers. They are, however, traps that cause traces to be left without the attacker knowing that he or she is connected to a decoy system that does none of the things it appears to do; instead, it logs everything and notifies the appropriate personnel.

Furthermore, SPECTER automatically investigates the attackers while they are still trying to break in. SPECTER provides massive amounts of decoy content and it generates decoy programs that will leave hidden marks on the attacker's computer. Automated weekly online updates of the honeypot's content and vulnerability databases allow the honeypot to constantly change without user interaction.

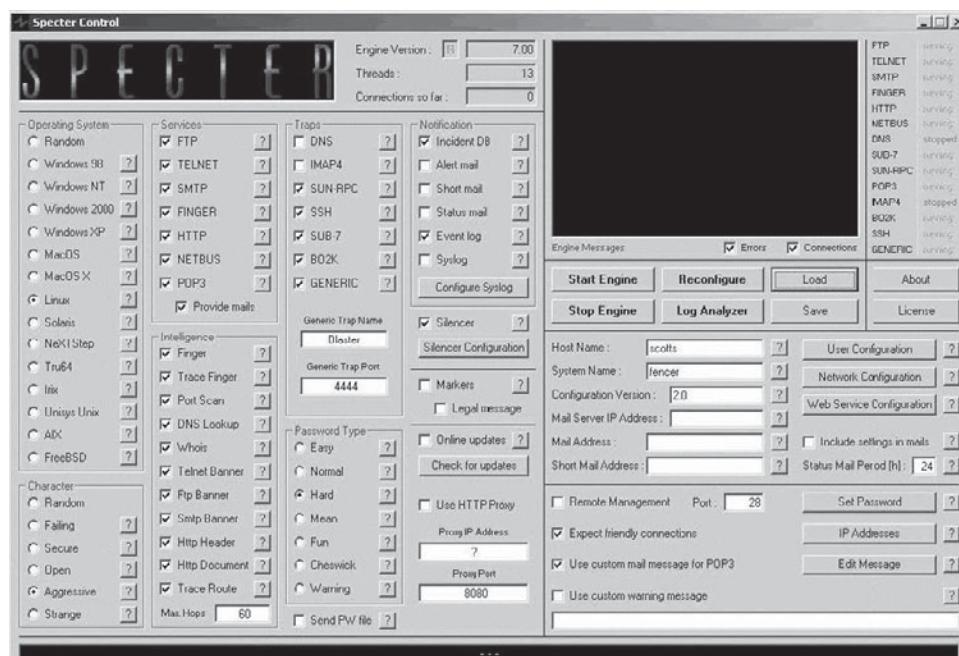
A SPECTER system consists of a dedicated PC and SPECTER software. It is connected to the network where attacks are expected. This usually means it is connected close to the Internet access point, typically in the DMZ; however, it can also be connected directly to the Internet. SPECTER can also be installed on internal networks to discover suspicious activities originating from within an organization or to detect security breaches.

SPECTER includes the following features:

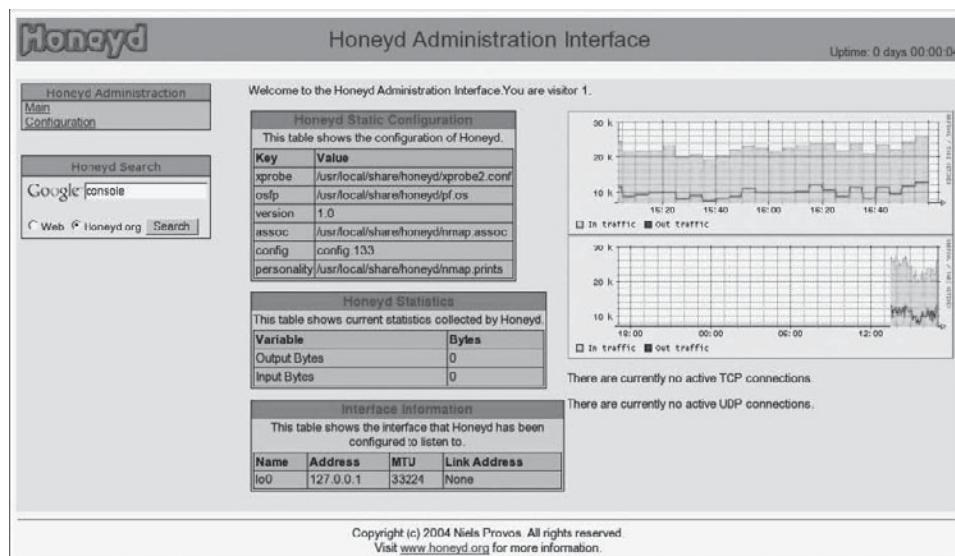
- Suspicious interest in the network and computers can be detected immediately.
- Administrators are notified of hostile activity when it happens, so they can immediately look at the problem and take action.
- By illegally downloading programs and other content from the honeypot system, attackers place hidden evidence on their own computers. This evidence may be used in court.
- Detailed logs of the activities provide information about character, skill level, and intentions of an attacker. These can be valuable evidence for proving the hostile nature of an attacker's activities.
- Important information about the identity of an attacker can be collected automatically.
- There will be no false alerts, as a legitimate user will not connect to the honeypot.

### Honeyd

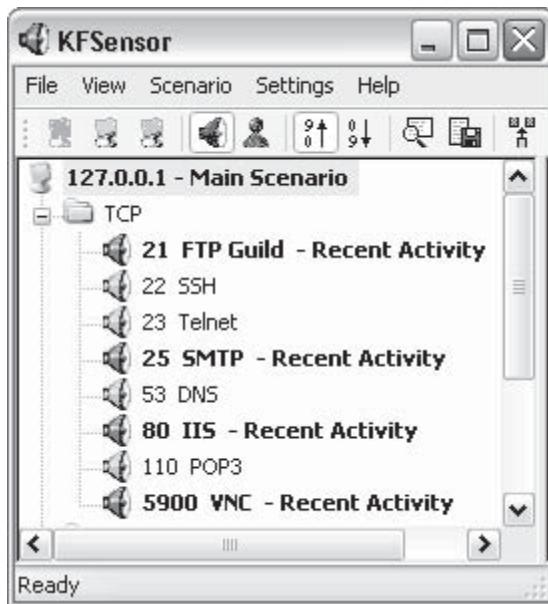
Honeyd (Figure 3-33) is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and the daemon's personality can be adapted so that it appears to be running certain



**Figure 3-32** SPECTER can simulate a complete system acting as a honeypot.



**Figure 3-33** Honeyd creates virtual hosts on a network.



**Figure 3-34** KFSensor is a host-based IDS that acts as a honeypot.

operating systems. Honeyd enables a single host to claim multiple addresses. It improves cyber security by providing mechanisms for threat detection and assessment. It also deters adversaries by hiding real systems in the middle of virtual systems. Honeyd is open-source software released under the GNU General Public License.

### KFSensor

KFSensor (Figure 3-34) is a host-based intrusion detection system (IDS) that acts as a honeypot by simulating vulnerable system services and even Trojans to attract and log potential hackers and port-scanner kiddies. The system is highly configurable and features detailed logging, attack analysis, and security alerts. The user can create different scenarios by selecting which ports the program should act upon and what actions to take when access is attempted.

KFSensor lies dormant until attacked, consuming very little processor time or network resources. Sensors can be installed on user systems without affecting normal use and without any additional hardware. KFSensor emulates real servers (FTP, POP3, HTTP, telnet, and SMTP) to improve deception and gain valuable information about an attacker's motives. Attacks are detected, analyzed, and reported immediately, allowing fast response to an attack.

while it is still in progress. KFSensor does not rely on signatures of known attacks and can therefore detect new or zero-day threats such as new worms, viruses, and elite hackers. KFSensor is effective at detecting internal threats.

## Sebek

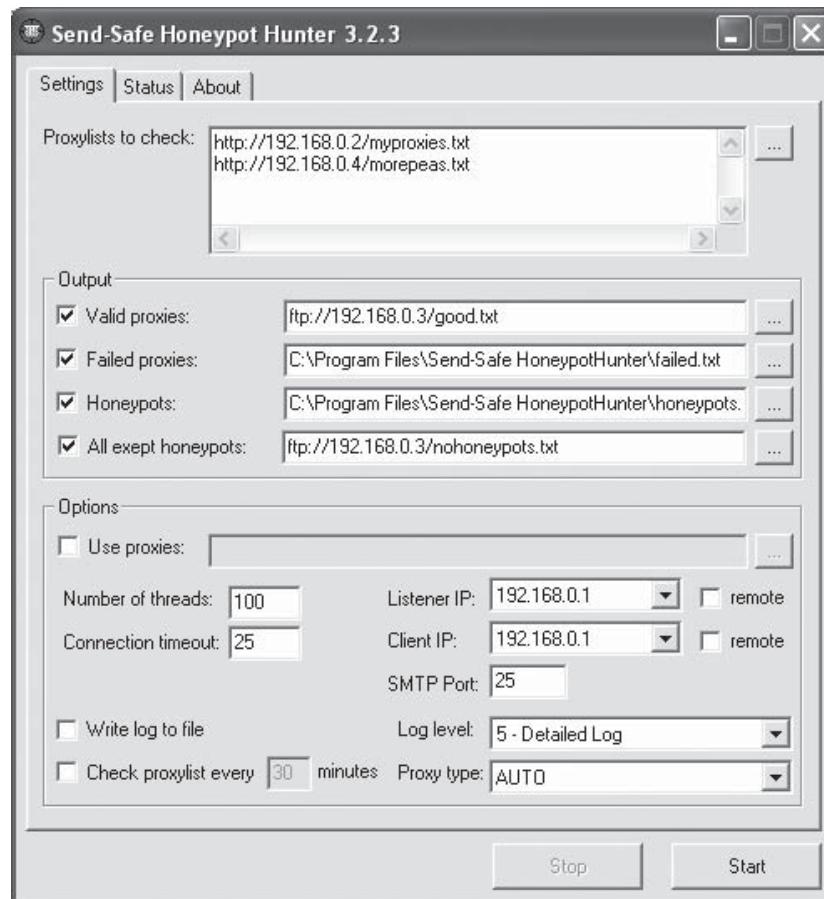
Sebek has two components: a client and a server. The client captures data on a honeypot and exports it to the network, while the server collects it. The server collects the data from one of two possible sources: either a live packet capture from the network or from a packet-captures archive stored as a Tcpdump-formatted file. Once the data is collected, it is either uploaded into a relational database or the keystroke logs are immediately extracted. The communications used by Sebek are UDP-based.

**Typical Sebek Deployment** The client module is installed on the honeypot. The attacker's activity, captured by the honeypot, is passed through the wire (hidden to the attacker) and passively collected by the honeywall gateway. The client resides entirely in kernel space on the honeypot, and the Linux version is implemented as a loadable kernel module (LKM). The client can record all of the data that a user accessed via the read() system call. This data is then exported to the server over the network in a manner that is difficult to detect from the honeypot. The server then gathers the data from all of the honeypots. As there is a standard, platform-independent log format, the server can collect from any honeypot, independent of operating system type.

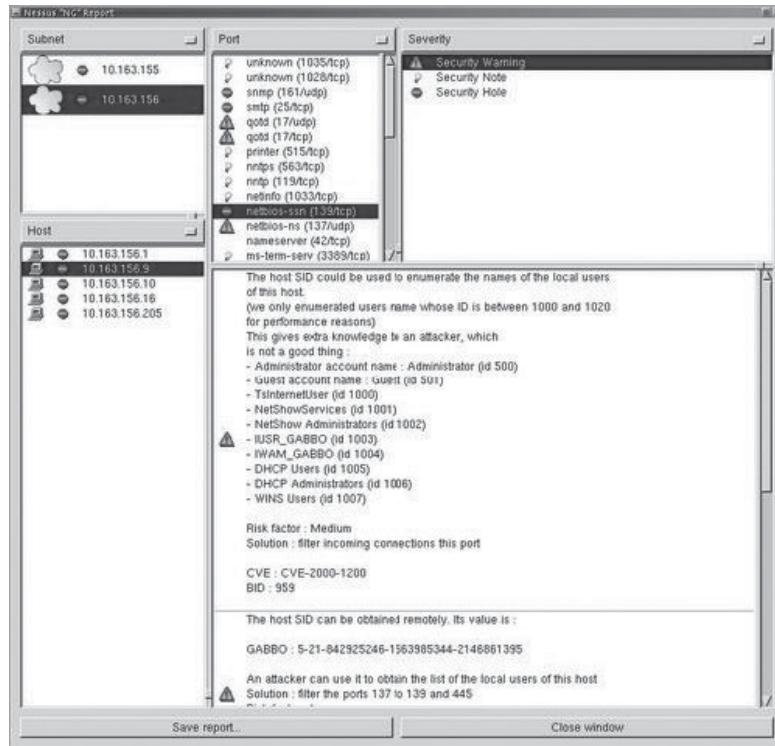
## Tools to Detect Honeypots

### Send-Safe Honeypot Hunter

Send-Safe Honeypot Hunter (Figure 3-35) is a tool designed for checking lists of HTTPS and SOCKS proxies for honeypots. It checks lists of HTTPS, SOCKS4, and SOCKS5 proxies with any ports. It can be also used for proxy-list validating.



**Figure 3-35** Send-Safe Honeypot Hunter checks lists of proxies for honeypots.



**Figure 3-36** Nessus Security Scanner can detect honeypots.

### Nessus Security Scanner

The Nessus Project (Figure 3-36) aims to provide the Internet community with a free, powerful, up-to-date and easy-to-use remote security scanner. A security scanner is a software package that will audit a given network remotely and determine whether the attacker/hacker might break into or misuse it in some way. Nessus checks for the validity of services running on particular ports. It does not test for the version of a remote service but exploits the vulnerability of the service. Nessus is fast, reliable, and has a modular architecture that is flexible to the user's needs.

---

## Chapter Summary

- Intrusion detection systems (IDS) monitor packets on the network wire and attempt to discover if an attacker/hacker is attempting to break into a system.
- System integrity verifiers (SIVs) monitor system files to determine when an intruder changes them. Tripwire is one of the most popular SIVs.
- Intrusion detection happens either by anomaly detection or signature recognition.
- A simple protocol verification system can flag invalid packets. This can include valid but suspicious behavior, such as severely fragmented IP packets.
- Installing network software on an internal system that communicates using a port address permitted by the firewall configuration.
- Honeypots are systems that simulate a live system but are intended to allow administrators to monitor and track an attacker without jeopardizing a critical system.

## Review Questions

1. What is signature analysis?

---

---

---

---

2. Explain the ways to evade intrusion detection systems.

---

---

---

---

3. Explain some techniques for firewall identification.

---

---

---

---

4. What is banner grabbing?

---

---

---

---

5. Describe several banner-grabbing countermeasures.

---

---

---

---

6. What are the differences between IDS and IPS?

---

---

---

---

7. What is ACK tunneling?

---

---

---

---

8. Explain low-interaction and high-interaction honeypots.

---

---

---

9. List the advantages and disadvantages of honeypots.

---

---

---

10. Name three measures that should be carried out if a hacking attack is detected.

---

---

---

---

## Hands-On Projects



1. Use TrapServer for system monitoring, notification, and problem resolution of the communications network.
  - Navigate to Chapter 3 of the Student Resource Center.
  - Install and run trapserver1beta.exe (Figure 3-37).

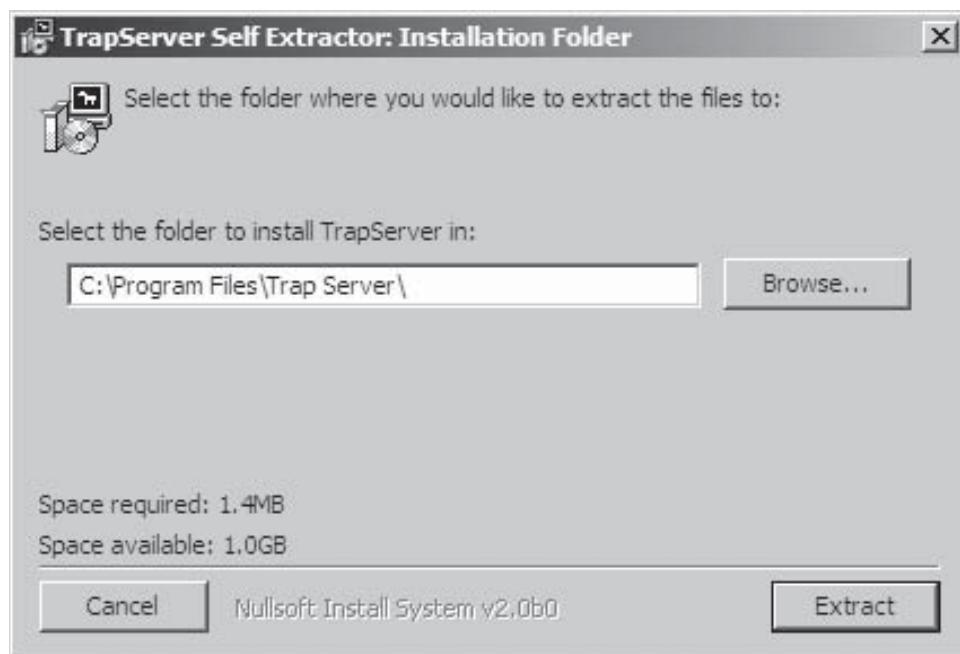


Figure 3-37 Install TrapServer.

- Stop the WWW service in Services before proceeding. TrapServer uses port 80.
- Navigate to C:\Program Files\Trap Server and run Trap Server.exe.
- Click **Start Listen** (Figure 3-38).
- Go to another machine and navigate to this machine's IP address using a browser.
- A default IIS page should be displayed.

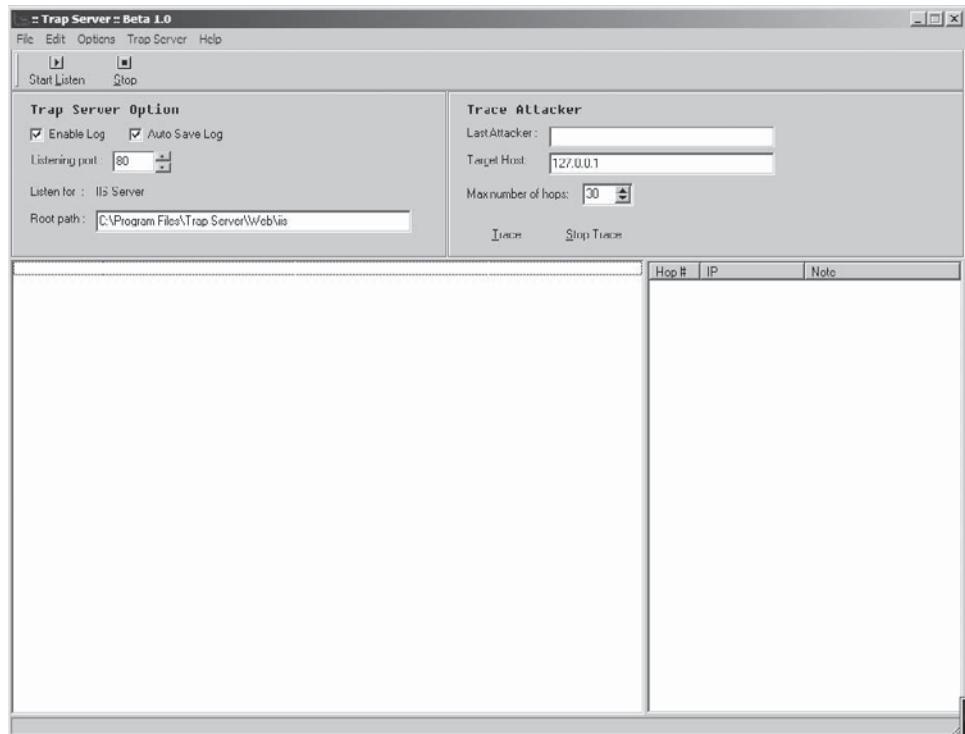


Figure 3-38 Click Start Listen.

2. Use the Send-Safe Honeypot Hunter tool to check lists of HTTPS and SOCKS proxies for honeypots.
  - Navigate to Chapter 3 of the Student Resource Center.
  - Install and launch the Send-Safe Honeypot Hunter program.
  - Click on the **Settings** menu (Figure 3-39).
  - In the Settings menu, click **Proxylist** to check a field, and enter the local path to or URL of a proxy list to be checked.

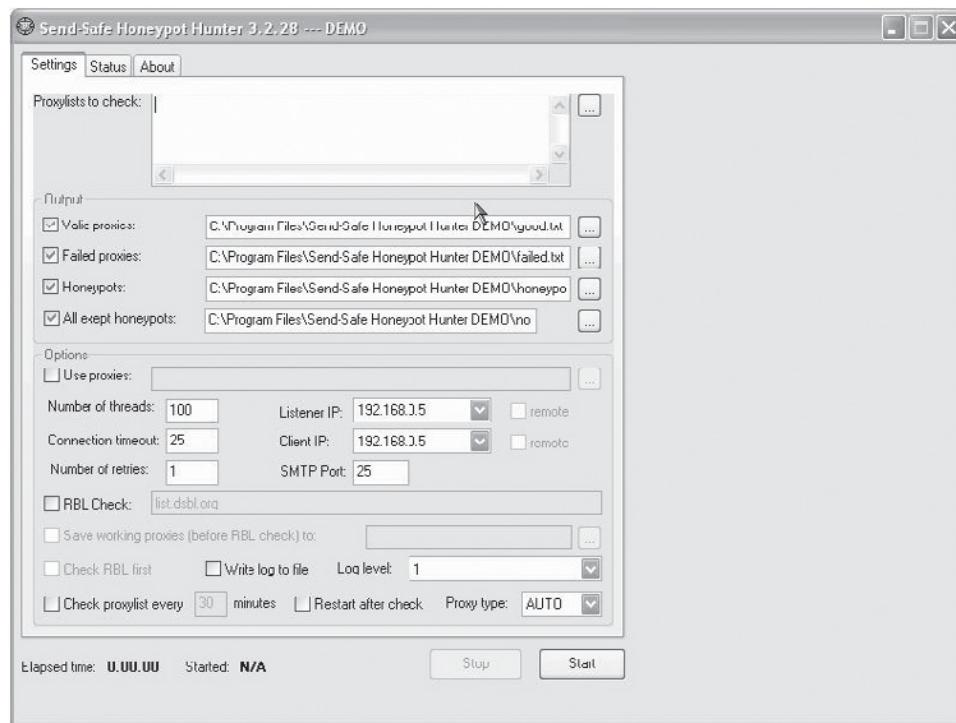


Figure 3-39 Click on the Setting menu.

- Check for the required options and then click the **Start** button (Figure 3-40).
- The Send-Safe Honeypot Hunter tool performs a check on the lists of HTTPS and SOCKS proxies.

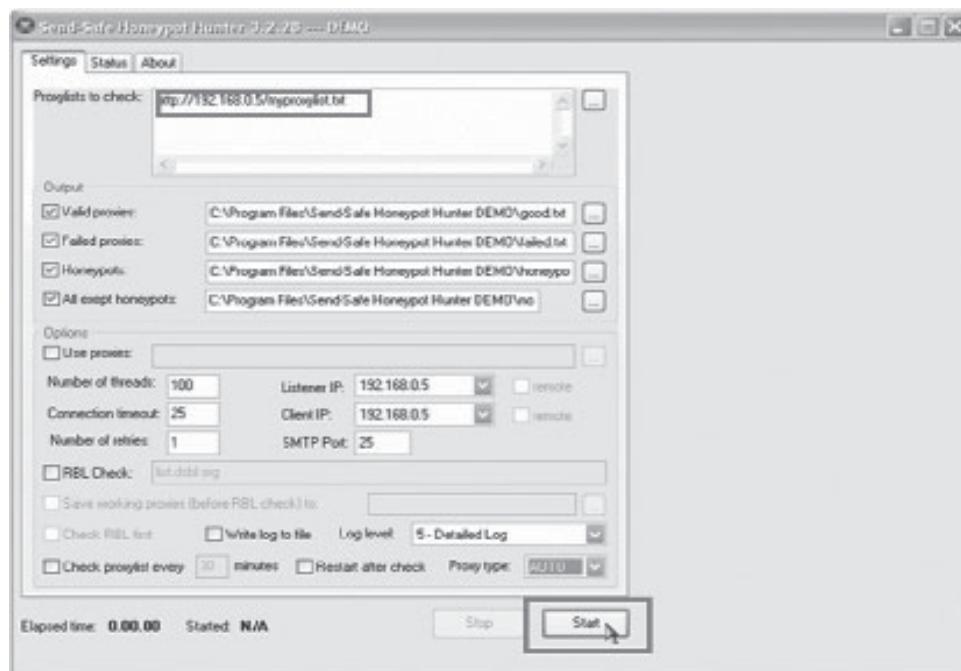
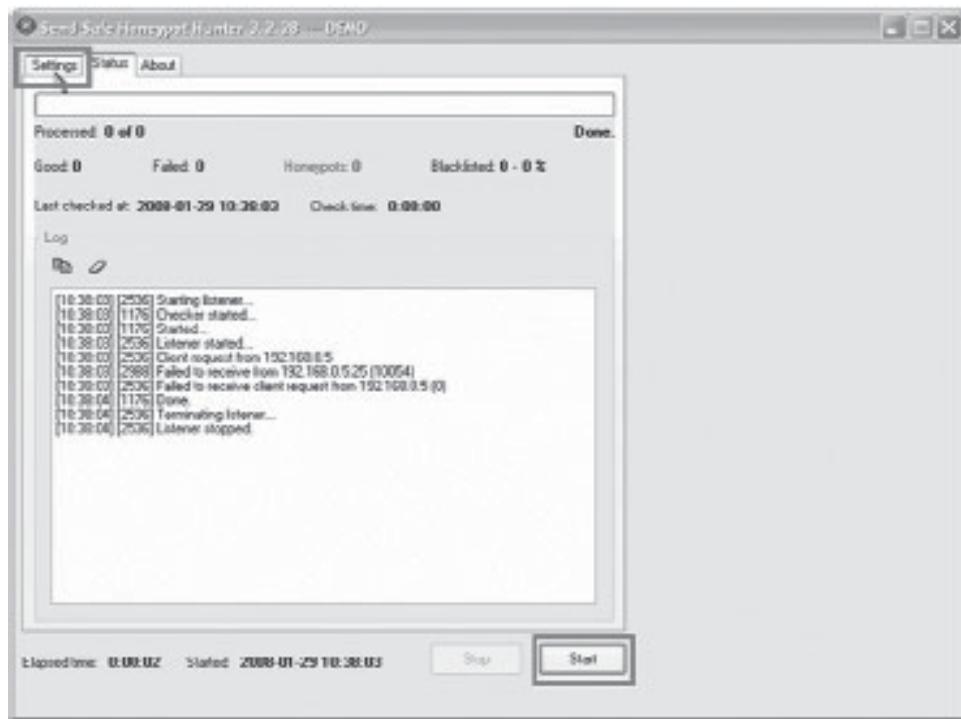


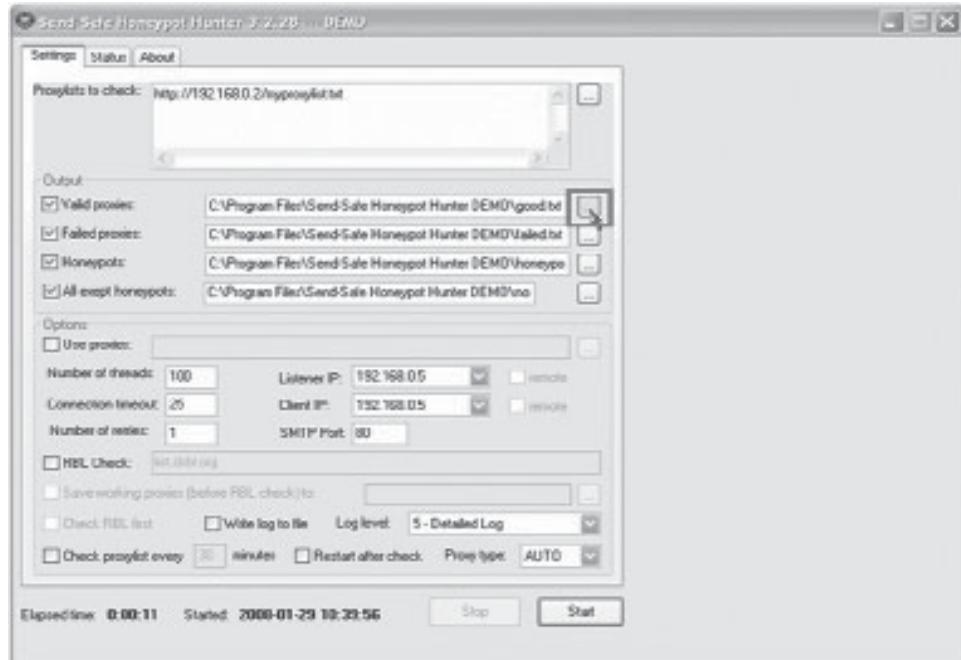
Figure 3-40 Click the **Start** button.

- Click the **Settings** menu once the Send-Safe Honeypot Hunter tool has completed checking the lists of HTTPS and SOCKS proxies (Figure 3-41).



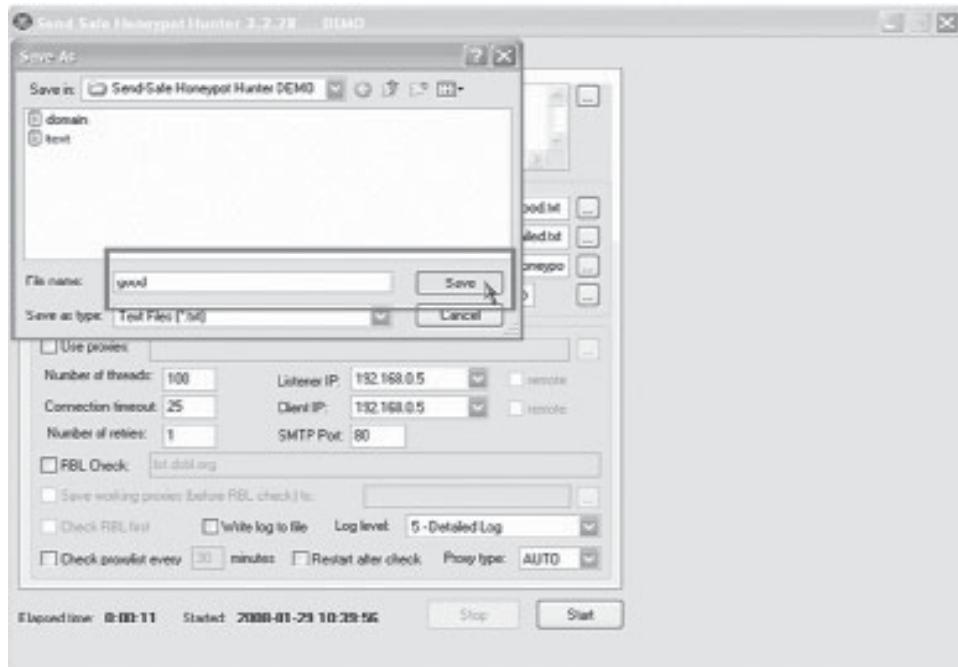
**Figure 3-41** Click the **Settings** menu.

- In the **Output** options, click on the various buttons to save the valid and failed proxies, honeypots, and all except honeypots files (Figure 3-42).



**Figure 3-42** Save the valid and failed proxies, honeypots, and all except honeypots files.

- Enter the filename and click the **Save** button in the **Save As** dialog box to save the good proxies list (Figure 3-43).
- Explore the various options of this program.



**Figure 3-43** Save the good proxies list.

3. Read Types of Firewalls.pdf.
  - Navigate to Chapter 3 of the Student Resource Center.
  - Open Types of Firewalls.pdf and read the content.

*This page intentionally left blank*

# Cryptography

## Objectives

After completing this chapter, you should be able to:

- Understand public-key cryptography
- Identify a digital signature
- Explain RSA
- Explain algorithms and security
- Explain a message digest
- Understand SHA
- Explain SSL
- Understand SSH
- Name code-breaking methodologies
- Explain the various cryptography attacks
- Name various cracking tools

## Key Terms

**Asymmetric key system** an encryption method using a key pair, one public key available to anyone, and one private key held only by the key owner, that is used to provide confidentiality, integrity, authentication, and nonrepudiation in data management

**Blowfish** a secret-key cryptographic method that uses a variable key length from 32 to 448 bits

**Cryptography** the practice of concealing information by turning it into an unreadable code

**Data Encryption Standard (DES)** a relatively insecure symmetric key system using 64-bit encryption (56 bits for key size and 8 bits for cyclic redundancy check) to encrypt data

**Digital signature** a cryptographic means of authentication

**Message-digest functions** a set of functions that distill the information contained in a file (small or large) into a single fixed-length number

**Public-key certificate** a digital certificate used to verify that an individual's key pair is actually assigned to that individual

**RSA** a public-key cryptosystem that uses modular arithmetic and elementary number theories to perform computations using two large prime numbers

**Rainbow table** a large, pregenerated data set of hashes from nearly every possible password, that reduce the difficulty in brute-force cracking of a single password

**Secure Shell (SSH)** a protocol that is used to securely log onto another computer over a network and transfer files from one computer to another

**Secure Sockets Layer (SSL)** a protocol used to provide a secure authentication mechanism between two communicating applications

**Symmetric key system** an encryption method using a single key possessed by both the sender and receiver to encrypt and decrypt messages

---

## Introduction to Cryptography

The word *crypto* is derived from the Greek word *kryptos*, meaning “concealed, hidden, veiled, secret, or mysterious.” *Graph* is derived from *graphia*, which means “writing”; hence, *cryptography* means “the art of secret writing.” *Cryptography* is the practice of concealing information by turning it into an unreadable code. This is done through the use of a key or encryption scheme. A simple example of an encryption key is: A = 1, B = 2, C = 3, etc. This key tells the key holder that each letter in a message has been replaced with a corresponding number, allowing the key holder to decode the message. This technique, called a *symmetric key system*, requires that both the sender and the receiver of the message possess the same key. Because the sender and receiver must share the key prior to sending any messages, this technique is of limited use for the Internet where individuals who have not had prior contact frequently require a secure means of communication. The solution to this problem is public-key cryptography.

---

## Public-Key Cryptography

Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in 1976, in order to solve key-management problems. According to this concept, individuals receive a public key and a private key. The public key is publicly available, but the private key is held as a secret. Public-key cryptography is a type of asymmetric encryption. An *asymmetric key system* is an encryption method using a key pair, one public key available to anyone, and one private key held only by the key owner, that is used to provide confidentiality, integrity, authentication, and nonrepudiation in data management. Public-key encryption uses the following sequence to send a message (Figure 4-1):

1. An individual finds the public key of the person he or she wants to contact in a directory.
2. This public key is used to encrypt a message that is then sent to the intended recipient.
3. The receiver uses the private key to decrypt the message and reads it.

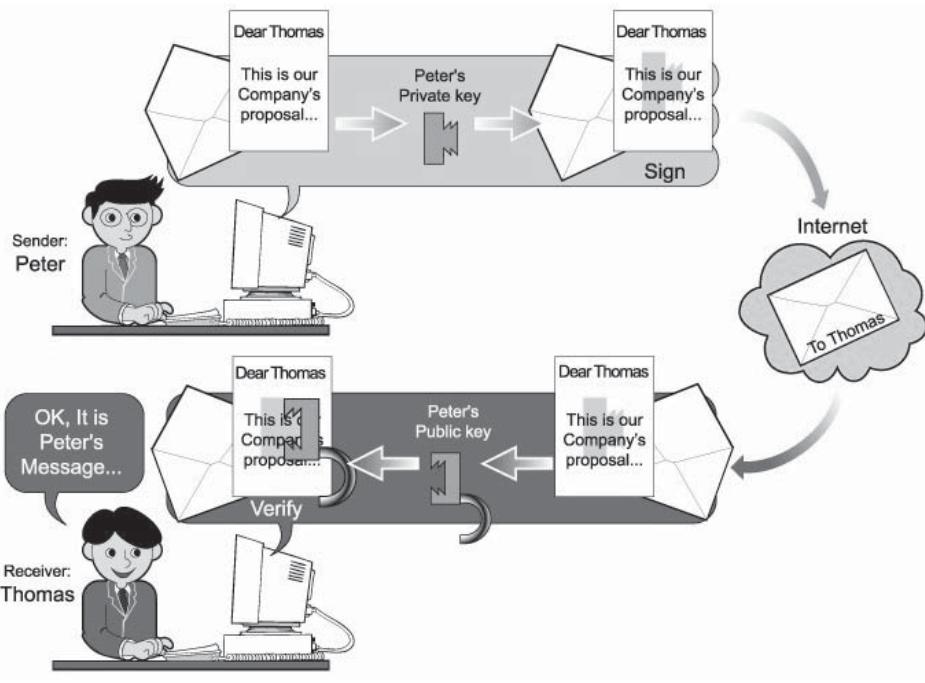
No one but the holder of the private key can decrypt a message composed with the corresponding public key. This increases the security of the information because all the communications involve only the public keys; the private keys are never transmitted or shared.

The public keys must be linked with the usernames in a secured method to ensure that information is not intercepted by individuals claiming to be the intended recipient. This authentication need is met with the use of digital signatures.

## Digital Signature

A *digital signature* is a cryptographic means of authentication. Public-key cryptography, because it uses asymmetric encryption, is used to create a digital signature. A hash function is an algorithm that is used to create and verify a digital signature. This algorithm creates a digital representation, also known as a fingerprint, of a message. This fingerprint has a hash value that is much smaller than the message, but one that is unique to it. If any change is made to the message, the hash function will automatically produce a different hash value.

The hash value of the original message and the hash function that is used to create the digital signature are required to verify the digital signature. With the help of both the public key and the new result, the verifier checks to see if the digital signature was created with the related private key and whether the new hash value is the same as the original.



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

**Figure 4-1** Public-key encryption is asymmetric.

## Public-Key Certificate

A **public-key certificate** is used to verify that an individual's key pair is actually assigned to that individual. Public-key certificates can be obtained by subscribing to a certification authority such as Microsoft Internet Information Services. A certification authority digitally signs the public-key certificate to assure the authenticity of both the public key and the subscriber's identity. The authority's digital signature on the certificate can be verified via the public key of the certification authority recorded in another certificate, which belongs to another certification authority. This certificate can be authenticated through another public key recorded in another certificate, and so on.

The retrieval and verification of digital signatures is made with the help of an online database called a repository. The repository holds the certificates and other information. The certification authority may suspend or revoke the certificate. Figure 4-2 is a flow chart of the public-key communication process.

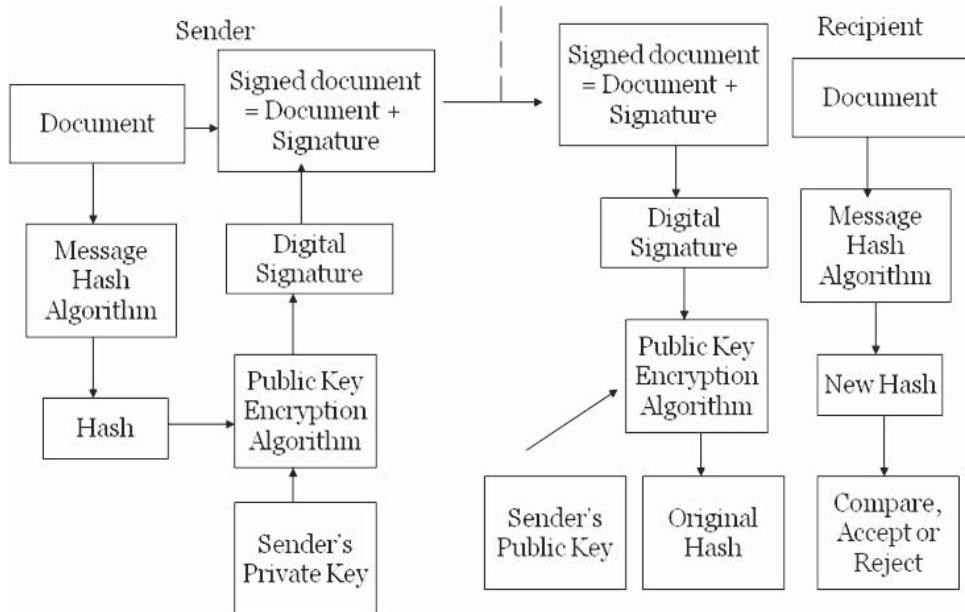
## Encryption Algorithms

### RSA (Rivest Shamir Adleman)

**RSA** is a public-key cryptosystem. It uses modular arithmetic and elementary number theories to perform computations using two large prime numbers. The RSA system is widely used in a variety of products, platforms, and industries. Companies such as Microsoft, Apple, Sun, and Novell build the RSA algorithms into their operating systems. RSA can also be found on hardware secured telephones, Ethernet network cards, and smart cards.

RSA works as follows:

1. Two large prime numbers are taken ( $a$  and  $b$ ), and their product is determined ( $c = ab$ , in which  $c$  is called the modulus).
2. A number  $e$  is chosen such that it is less than  $c$  and relatively prime to  $(a - 1)(b - 1)$ . Therefore,  $e$  and  $(a - 1)(b - 1)$  have no common factors except 1.
3. Separate from this, a number  $f$  is chosen such that  $(ef - 1)$  is divisible by  $(a - 1)(b - 1)$ .
4. The values  $e$  and  $f$  are called the public and private exponents, respectively.



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

**Figure 4-2** Public keys allow messages to be encrypted so that only the corresponding private key can open them.

```

The encryption function is:

$$\begin{aligned} \text{encrypt}(T) &= (T^E) \bmod PQ \\ &= (T^{17}) \bmod 3233 \end{aligned}$$


The decryption function is:

$$\begin{aligned} \text{decrypt}(C) &= (C^D) \bmod PQ \\ &= (C^{2753}) \bmod 3233 \end{aligned}$$


To encrypt the plaintext value 123, do this:

$$\begin{aligned} \text{encrypt}(123) &= (123^{17}) \bmod 3233 \\ &= 337587917446653715596592958817679803 \bmod 3233 \\ &= 855 \end{aligned}$$


To decrypt the ciphertext value 855, do this:

$$\begin{aligned} \text{decrypt}(855) &= (855^{2753}) \bmod 3233 \\ &= 123 \end{aligned}$$


```

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

**Figure 4-3** RSA uses modular arithmetic and elementary number theories to perform computations using two large prime numbers.

5. The public key is the pair  $(c, e)$ ; the private key is the pair  $(c, f)$ .
6. It is considered to be difficult to obtain the private key  $(c, f)$  from the public key  $(c, e)$ . However, if someone can factor  $c$  into  $a$  and  $b$ , then that person can decipher the private key  $(c, f)$ .

The security of the RSA system is based on the assumption that such factoring is difficult to carry out, making the cryptographic technique safe.

The process of RSA is illustrated in Figure 4-3.

The following sequence is an example of how RSA algorithms can be used in a practical interchange:

1. The sender of a message encrypts it using a randomly chosen DES symmetric key. **DES (Data Encryption Standard)** is a relatively insecure symmetric key system using 64-bit encryption (56 bits for key size, 8 bits for cyclic redundancy check) to encrypt data.

2. The sender will then look up the recipient's public key and use it to encrypt the DES key using the RSA system.
3. An RSA digital envelope, consisting of a DES-encrypted message and an RSA-encrypted DES key, is sent to the recipient.
4. The recipient will decrypt the DES key and then use the DES key to decrypt the message itself.

## **RC4**

RC4 is a variable key-size symmetric-key stream cipher with byte-oriented operations, and is based on the use of a random permutation. According to some analyses, the period of the cipher is likely to be greater than 10,100. For each output byte, eight to 16 system operations are used, meaning the cipher has the ability to run fast when used in software. Products like RSA SecurPC use this algorithm for file encryption. RC4 is also used for safe communications such as traffic encryption (which secures Web sites) and for Web sites that use the SSL protocol.

## **RC5**

RC5 is a fast symmetric-key block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security) in 1994. The algorithm is a parameterized algorithm with a variable block size, key size, and number of rounds. The block sizes can be 32, 64, or 128 bits. The range of the rounds can vary from 0 to 255, and the size of the key can vary from 0 to 2,040 bits. This built in variability can offer flexibility at all levels of security. The following three routines are used in RC5:

- Key expansion
- Encryption
- Decryption

In the key expansion routine, the secret key that a user provides is expanded to fill the key table (the size of which depends on the number of rounds). The key table is used for both encryption and decryption. The encryption routine has three fundamental operations: integer addition, bitwise XOR, and variable rotation. The intense use of data-dependent rotation plus the combination of different operations makes RC5 a secure encryption algorithm.

## **RC6**

RC6 is similar to the RC5 algorithm in that it is a parameterized algorithm with a variable block size, key size, and number of rounds. Two features that differentiate the RC6 algorithm from RC5 are integer multiplication (which is used to increase the diffusion achieved in fewer rounds and increased speed of the cipher), and the use of four 4-bit working registers rather than two 2-bit registers. Four 4-bit registers are used in place of the two 2-bit registers because the block size of the AES is 128 bits.

## ***Blowfish***

*Blowfish* is a secret-key cryptographic method that uses a variable key length from 32 to 448 bits. It uses a method called block cipher, which breaks data into chunks of 64 bits each before encrypting them. Blowfish is considered secure, and it is freely available for use.

## ***Algorithms and Security***

Forty-bit encryption appears hard to crack. However, with the help of modern computers, the combination can be cracked in a reasonable amount of time. Forty-bit encryption is no longer considered secure in the cryptographic community. Fifty-six-bit encryption keys are also easily susceptible to attacks and are not considered secure. The creators of Web browsers introduced 128-bit encryption to offer a more secure means of communication.

128-bit encryption offers greater cryptographic security than 40-bit and 56-bit encryption. It is 288 times stronger than 40-bit encryption.

Experts have estimated that it would take approximately 1,019 years to break a 128-bit encryption message. 256-bit and above encrypted keys are usually more difficult to break.

## Message-Digest (Hash) Functions

*Message-digest functions* distill the information contained within a file (small or large) into a single fixed-length number, typically between 128 and 256 bits in length. If any given bit of the function's input is changed, every output bit has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message-digest value (Figure 4-4).

Message-digest functions are also called one-way hash functions because they produce values that are almost impossible to invert, resistant to attack, mostly unique, and widely distributed. Message-digest algorithms themselves are not used for encryption and decryption operations. They are used in the creation of digital signatures and message authentication codes (MACs), and the derivation of encryption keys from passphrases.

The main role of a cryptographic hash function is to provide integrity in document management. Cryptographic hash functions are an integral part of digital signatures. They are relatively faster than digital-signature algorithms; hence, their characteristic feature is to calculate the signature of the document's hash value, which is smaller than the document. In addition, digests can be used publicly without revealing the contents or source of the document. Widely used message-digest functions include the following algorithms:

- MD5
- SHA-1

### MD2, MD4, and MD5

MD2, MD4, and MD5 are message-digest algorithms used in digital signature applications in which the document is compressed securely before being signed with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits (Figure 4-5).

The structures of all three algorithms appear similar, although the design of MD2 is reasonably different from MD4 and MD5. MD2 was designed for 8-bit machines, while MD4 and MD5 were designed for 32-bit machines. The message is padded with extra bits to ensure that the length of the bits is divisible by 512. A 64-bit binary message is added to the message.

Attacks on versions of MD4 have become increasingly successful. Recent research has shown how collision attacks for the full version of MD4 could be carried out in under a minute on a typical PC. MD5 is slightly more secure, but is slower than MD4. This algorithm has four different rounds, which are designed with slight differences from those of MD4. However, both the message-digest size and padding requirements remain the same.

The effectiveness of hash functions can be defined by checking the output produced when an arbitrary input message is randomized.

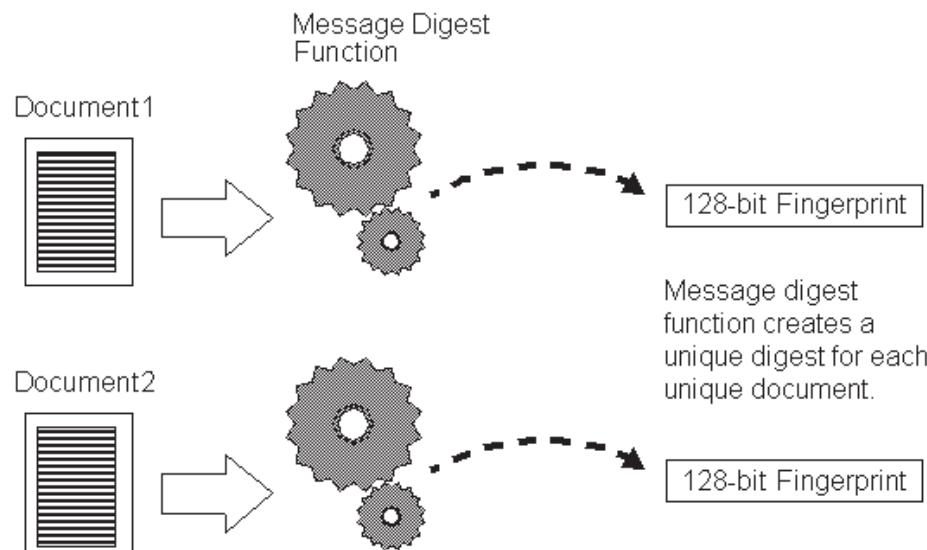


Figure 4-4 Message-digest functions reduce information to a hash.

File	Size	CRC	MD5
batch_rename.png	14 472	18528C0A	EAF2C712F6E537AE1FEFD3FA1A4F4AAB
change_attributes.html	8 574	58101E09	E18D9F81CCF9A300F79321E8C768E021
change_attributes.png	7 957	2531FC3E	5E8A8FB259C7FDF790E5597C8154AF38
change_case.html	8 756	FC41186B	DDCAD7CF08BF7897D5B8B5F9806B47FD
change_case.png	6 821	2D34D339	04FED507091F5F095D977B358EC20EED
checksum_verify.png	8 117	3D8D9801	AC8AFE99B76BD1022AC7B2E34A7E1C49
convert.html	9 269	BE535A89	902BA23D7CC95EA2999CDA2EF1B27B41
convert.png	7 080	D760CFC6	F1176C7967E1DA2CA743D26DE9F1B0C0
convert_menu.png	8 735	638F8F0F	3F1BBD5E0B0B9E86970EDBA9705F14D4
file_comparator.html	8 575	44ED5DC4	959961C3E7D7559C9EE77965302A6E0A
file_comparator.png	17 787	D16F0E2B	C1AE1516BEABC17EDEFB58212D2C5331

Figure 4-5 MD5 codes are the same length regardless of the file size.

The following are examples of minimally different message digests:

- echo “There is CHF1500 in the blue bo” | md5sum
  - e41a323bdf20eadaf3f0e4f72055d36
- echo “There is CHF1500 in the blue box” | md5sum
  - 7a0da864a41fd0200ae0ae97afd3279d
- echo “There is CHF1500 in the blue box.” | md5sum
  - 2db1ff7a70245309e9f2165c6c34999d

Even minimally different texts produce radically different MD5 codes.

## SHA-1 (Secure Hash Algorithm)

The Secure Hash Algorithm (SHA-1), specified in the Secure Hash Standard (SHS), was developed by NIST and published as a federal information-processing standard (FIPS PUB 180).

SHA-1 is similar to the MD4 message-digest algorithm family of hash functions. The algorithm accepts a message of 264 bits in length and produces a 160-bit message-output digest. The digest is designed to complicate the searching of the text, which is similar to the given hash. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks.

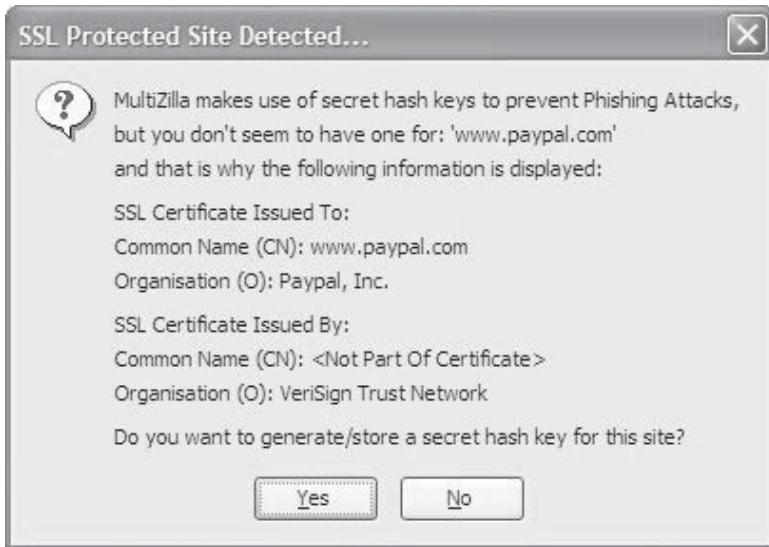
SHA-1 is part of the Capstone project. Capstone is the U.S. government’s long-term project to develop a set of standards for publicly available cryptography, as authorized by the Computer Security Act of 1987. The basic organizations responsible for Capstone are NIST and the NSA. As SHA-1 has been demonstrated to have collision weaknesses that can be exploited in a manner similar to MD5, NIST is presently seeking the creation of a more secure hashing algorithm for government use. The following are the four chief mechanisms of Capstone:

- A symmetric bulk-data encryption algorithm (Skipjack)
- An asymmetric digital-signature algorithm (DSA)
- A key-exchange protocol
- A hash function (SHA)

---

## SSL (Secure Sockets Layer)

*Secure Sockets Layer (SSL)* is a protocol used to provide a secure authentication mechanism between two communicating applications, such as a client and a server (Figure 4-6). SSL requires a reliable transport protocol, such as TCP, for data transmission and reception.



**Figure 4-6** SSL is an authentication protocol.

Any application-layer protocol that is higher than SSL—such as HTTP, FTP, and telnet—can be transparently layered on top of SSL. SSL acts as an arbitrator between the encryption algorithm and session key. It also verifies the destination server prior to the transmission and reception of data. The complete data of the application protocol is encrypted to ensure security.

## SSL Sessions

SSL uses both asymmetric and symmetric authentication mechanisms. Public-key encryption is used to verify the identities of the server, the client, or both. Once authentication has taken place, the client and server can create symmetric keys allowing them to communicate and transfer data rapidly. An SSL session is responsible for carrying out the SSL handshake protocol to organize the states of the server and clients, thus ensuring the consistency of the protocol.

## SSL Handshake Protocol Flow

The SSL handshake protocol works on top of the SSL record layer. The processes that are executed in the three-handshake protocol are summarized as follows:

1. The client sends a hello message to the server, which the server must respond to with a hello message or the connection will fail due to the occurrence of a fatal error. The attributes established due to the server and client hello are: protocol version, session ID, cipher suite, and compression method.
2. After the connection is established, the server sends a certificate to the client for authentication. In addition, a server-key exchange message might be sent. If the server is authenticated, the client may be asked for the certificate (if appropriate to the cipher suite selected).
3. The server sends a hello done message to inform the client that the handshake phase is complete and waits for the client's response.
4. If the client receives a certificate-request message, the client must respond to the message by sending a certificate message or “no certificate” alert. The client key-exchange message is sent. The content of the message depends on the public-key algorithm between the server hello and client hello. If the certificate sent by the client has signing ability, a digitally signed certificate verifies the message and is transmitted.
5. The client transmits the changed cipher-spec message and copies the pending cipher spec into the current cipher spec. The client sends a message to initiate the completion of the message under the new algorithm, keys, and secrets. In response, the server replies by sending its own changed cipher-spec message,

transfers the pending cipher spec to the current cipher spec, and initiates the completion of the message under the new cipher spec. At this point, the handshake is complete and the server starts to exchange the application-layer data.

The resumption of a previous session or the replication of an existing session proceeds as follows:

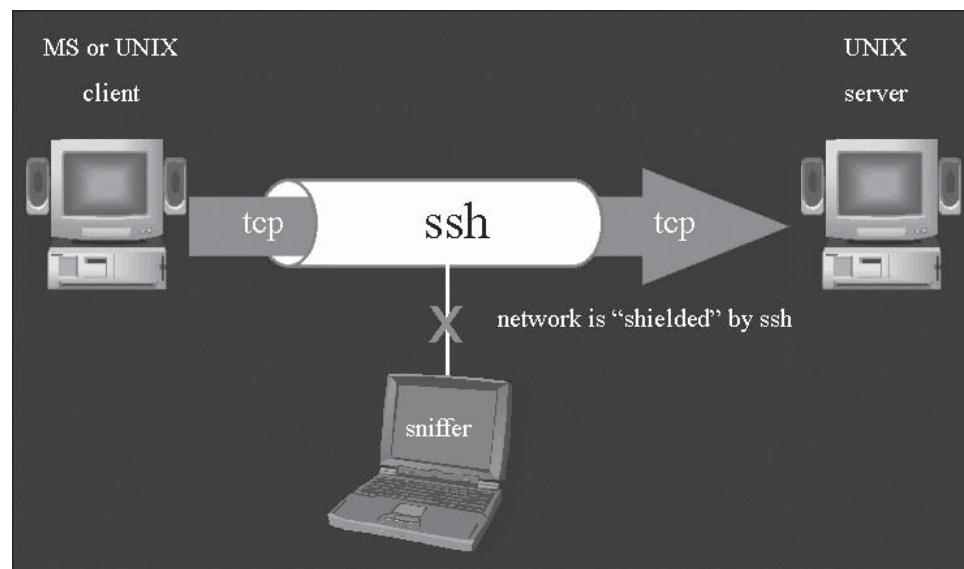
1. The client initiates the communication by sending a hello message with the session ID of the session that is to be resumed.
2. If the server finds a match, it reestablishes the session under the specified session state with the same session ID.
3. At this point, both the server and the client exchange the changed spec messages and proceed directly to the finished messages.
4. After reestablishment, the server and client exchange data at the application layer.
5. If the session ID is not found, the server creates a new session ID. The SSL client and server then carry out a complete handshake.

## Secure Shell (SSH)

*Secure Shell (SSH)*, and its replacement SSH-2, are protocols that are used to securely log onto another computer over a network and transfer files from one computer to another. It offers reliable authentication and a secure communication channel over an insecure medium (Figure 4-7). It can be used as a replacement for telnet, login, rsh, and rcp. In SSH-2, sftp is a replacement for ftp. In addition, SSH offers secure connections and secure transfer of TCP connections. SSH and SSH-2 are completely different protocols and are not compatible. SSH encrypts the user's server and host keys to authenticate, while SSH-2 only uses the host keys. SSH-2 is more secure, performs better, and is also more portable than SSH. Additionally, SSH is vulnerable to attacks due to the presence of structural weaknesses.

SSH authenticates with the help of one or more of the following mechanisms:

- Password (the /etc/passwd or /etc/shadow in UNIX)
- User public key (RSA or DSA, depending on the release)
- Kerberos (for SSH)
- Host-based authentication (.rhosts or /etc/hosts equivalent in SSH, or public key in SSH-2)



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

Figure 4-7 SSH shields TCP communications.

Secure Shell protects against the following attacks:

- A remote host sending out packets that pretend to come from another trusted host (IP spoofing)
- A host pretending that an IP packet comes from another trusted host (IP source routing)
- An attacker forging name-server records (DNS spoofing)
- Intermediate hosts capturing passwords and other data
- People who control the intermediate hosts exploiting captured data
- Attackers listening to X authentication data and spoofing connections to the X11 server

## Disk Encryption

Disk encryption works in a manner similar to text-message encryption. By using an encryption program for the user's disk, the user can safeguard any and all information burned onto the disk and save it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after the disk information is decrypted that it can be read and used.

Disk encryption is useful when the user needs to send sensitive information through the mail. In addition, disk encryption can also be used to prevent the real-time exchange of information from being compromised. When the exchange of information is made in an encrypted form, the chances of the information being compromised are minimized. The only way an attacker could access the information is by decrypting the message.

Furthermore, encryption software installed on a user's system ensures the security of the system. Encryption software should be installed on any systems that hold valuable information or are exposed to unlimited data transfer.

## Encryption-Breaking Initiatives

### RSA Factoring Challenge

The RSA Factoring Challenge was a contest promoted by RSA Laboratories to study the difficulty in factoring the large numbers used in RSA keys. A group of eight challenging numbers, ranging from 576 to 2048 bits were given. Every number was a product of two large prime numbers and similar to an RSA key pair. The challenge ended in 2007 due to advances in cryptography that made it obsolete. The highest prize amount was given to the individual who factored RSA-640. Figure 4-8 gives an estimate of the number of machines required to find the factors of numbers of various sizes over a one-year time period.

General number field sieve (GNFS) is the best known algorithm for factoring large numbers. It has a sieving phase, which searches a limited set of prime numbers for the candidates that are related algebraically. The sieving phase is effective if it is distributed (usage of many processors simultaneously). The matrix solving phase needs large volumes of storage and is usually performed on supercomputers.

Number Length (bits)	Machines	Memory
430	1	Trivial
760	215,000	4 Gb
1020	342,000,000	170 Gb
1620	$1.6 \times 10^{15}$	120 Tb

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

**Figure 4-8** To find the factors of the 760-bit number in one year, 215,000 Pentium machines with 4 gigabytes of physical RAM are required.

## Distributed.net

Distributed.net is a nonprofit organization that serves as a gathering point for topics related to distributed computing (the process by which a large number of computers work together toward solving a particular problem).

This process is carried out through the use of software that allows idle computers to communicate through the Internet, enabling an unlimited number of computers to work toward one common goal.

Distributed.net has solved public encryption challenges such as a contest sponsored by RSA Laboratories to decode a message encrypted with a 56-bit RC5 algorithm. The combined effort found the winning key by using the computing power of an estimated 26,000 PCs to evaluate over 34 quadrillion keys. The group's efforts have proven that, given enough computing power, almost any encryption key can be broken.

---

## Encryption Countermeasures

### Code-Breaking Methodologies

The strength of an encryption algorithm can be measured by using various code-breaking techniques. The following code-breaking techniques are commonly used:

- Brute force
- Frequency analysis

#### Brute Force

Code-breakers, or cryptanalysts, work to recover the plaintext of a message without knowing the required key in advance. They may first try to recover the key or they may go after the message itself. A common cryptanalytic technique is a brute-force attack, or exhaustive search, in which the keys are determined by trying every possible combination of characters.

The efficiency of a brute-force attack depends on the hardware configuration (Figure 4-9). Use of faster processors means testing more keys per second. Cryptanalysts carried out a successful brute-force attack on a DES encryption method that effectively made DES obsolete.

#### Frequency Analysis

Frequency analysis of letters and words is another method used to attack ciphers. This technique examines the number of times that a particular symbol comes up in a ciphertext. For example, the letter *e* is a common letter in the English language. If the letter *k* appears commonly in a ciphertext, it can be reasonably concluded that *k* = *e*.

Encrypted source code is more vulnerable to these types of attacks because words like *#define*, *struct*, *else*, and *return* are repeated frequently in code. Sophisticated cryptosystems are required to maintain the security of messages against frequency analysis.

Estimate Time for Successful Brute-Force Attack				
Power / cost	40 bits (5 char)	56 bits (7 char)	64 bits (8 char)	128 bits (16 chars)
\$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	$10^{20}$ years
\$ 100 K (This can be achieved by a company)	2 sec	35 hours	1 year	$10^{19}$ years
\$ 1 M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	$10^{18}$ years

**Figure 4-9** Brute-force attacks require a great deal of processing power to be effective.

## Cryptography Attacks

Cryptography attacks are based on the assumption that the cryptanalyst has knowledge of the encrypted information. The following eight types of attacks are categorized according to the cryptanalyst's given information:

- *Ciphertext-only attack*: The cryptanalyst has the ciphertext of several messages, all of which were encrypted using the same encryption algorithm.
- *Known-plaintext attack*: The cryptanalyst can retrieve the ciphertext and the plaintext.
- *Chosen-plaintext attack*: The cryptanalyst not only has access to the ciphertext and associated plaintext for several messages, but can choose the plaintext that is encrypted and obtain the resulting ciphertext.
- *Adaptive chosen-plaintext attack*: The cryptanalyst chooses the plaintext that is encrypted and can modify this choice based on the results of the previous encryption.
- *Chosen-ciphertext attack*: The cryptanalyst can choose different ciphertexts to be decrypted and has access to the decrypted plaintext.
- *Chosen-key attack*: The cryptanalyst has some knowledge about the relationship between the different keys, but cannot choose the key.
- *Rubber-hose attack*: The cryptanalyst threatens, blackmails, or tortures someone until the key is handed over.
- *Bribery attack*: This attack is sometimes referred to as a purchase-key attack.

## RSA Attacks

**Brute-Force RSA Factoring** This kind of attack is possible when the attacker has access to the public key ( $n$ ). The goal is to obtain the private key ( $d$ ). To get the value of  $d$ , the factors of  $n$  need to be found. The following are a few of the algorithms that are used in factoring:

- *Trail division*: This is not only the oldest, but it is also the most inefficient algorithm because it tries all the prime numbers less than the square root of  $n$ .
- *Quadratic sieve (QS)*: This is an efficient algorithm for numbers less than 110 digits.
- *Multiple polynomial quadratic sieve (MPQS)*: This is a faster version of QS.
- *Double large prime variation of the MPQS*: This is a faster version of MPQS.
- *General number field sieve (GNFS)*: This is the fastest algorithm for numbers greater than 110 digits.

The above-listed algorithms are high-tech attacks against large composite numbers. Table 4-1 lists the approximate requirements to factor PGP-based RSA public-key module lengths with the help of GNFS.

Table 4-2 displays a few of the approximate equivalents of the brute-force key searches of symmetric keys and brute-force factoring of asymmetric keys, with the help of GNFS.

**Esoteric RSA Attacks** These attacks depend on the weaknesses in certain implementations of the RSA protocol.

Key size	MIPS Years Required to Factor
512	30,000
768	200,000,000
1024	300,000,000,000
2048	300,000,000,000,000,000,000

**Table 4-1** Large key sizes are nearly impossible to break without enormous computing capabilities

Symmetric	Asymmetric
56 bits	384 bits
64 bits	512 bits
80 bits	768 bits
128 bits	2304 bits

**Table 4-2** Brute-forcing asymmetric keys is exponentially more difficult than cracking symmetric keys

**Chosen-Ciphertext Attack** In this kind of attack, an attacker listens to the insecure channel in which RSA messages are passed. The attacker assembles an encrypted message ( $c$ ) from the target. To retrieve the original message ( $m$ ), the attacker chooses a random number, where  $r < n$ . The attacker then launches the attack by computing the following:

- $x = r^e \bmod n$  (The attacker encrypts  $r$  using the target's public key.)
- $y = x \times c \bmod n$  (The ciphertext is multiplied by the public key.)
- $t = r^{-1} \bmod n$  (multiplicative inverse of  $r \bmod n$ )

The attacker takes into consideration that if  $x = r^e \bmod n$ , then  $r = x^d \bmod n$ .

The attacker then forces the target to sign  $y$  with the private key, which is used in the decryption of  $y$ , and forward  $u = y^v \bmod n$  to the attacker. The following is the simple mathematical computation used by the attacker:

$$tu \bmod n = (r^{-1})(y^d) \bmod n = (r^{-1})(x^d)(c^d) \bmod n = (c^d) \bmod n = m$$

To spoil this type of attack, arbitrary documents **must not be signed**[but] the one-way message **must be signed**.

**Low Encryption-Exponent Attack** The speed of public-key operations depends on the encryption exponent: if the encryption exponent is small, the public encryption is faster. However, using small values for  $e$  as a public exponent for encrypting small messages makes this encryption vulnerable. For instance: if  $e$  is 3 and  $m$  is a smaller number than the cubic root of  $n$ , the message can be recovered by simply determining the cubic root of  $m$  because  $m$  [for  $m < \text{cubic root}(n)$ ]<sup>3</sup> mod  $n$  will be equivalent to  $m^3$ . Therefore, the cubic root of  $m^3 = m$ . To protect from attack, a user can add the message with the nonce before encryption, so that  $m^3$  is reduced to mod  $n$ .

**Error Analysis Attacks** Error analysis attacks are performed when the attacker compels the target to make encryption or decryption errors. By analyzing the resultant output and input, the encryption/decryption engine is forced to make a one-bit error in the operation. This attack is primarily of interest to people who use an encryption scheme in which the input, output, and encryption are accessible to the attacker.

**Modulus Attacks** Modulus attacks are used in situations where a number of users share the  $n$  but they have a different  $e$  and  $d$ . Division of the common modulus for a number of users can help the attacker recover the message without factoring  $n$ . If  $d$  is up to one-quarter the size of  $n$ , and  $e$  is less than  $n$ ,  $d$  can be recovered without factoring. PGP will not choose small values for the decryption exponent.

## Tools

### Encryption-Cracking Tools

#### OrphCrack Live CD

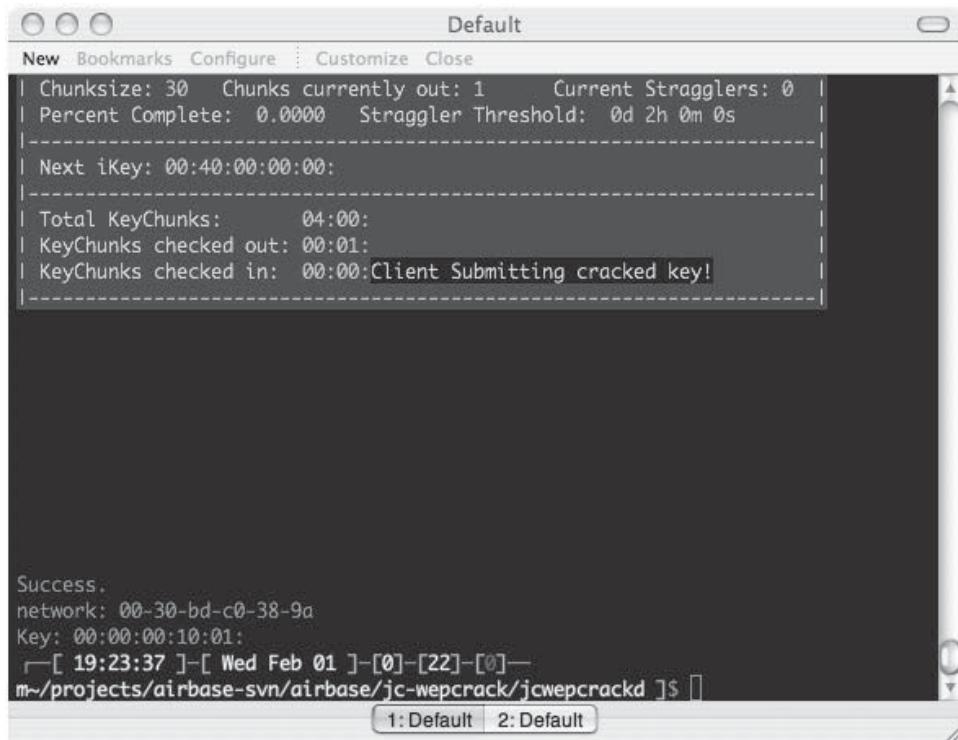
OrphCrack is a free image of a bootable Live CD that includes a Windows password-cracking program. This program makes use of included **rainbow tables**, which are large, pregenerated data sets of hashes from nearly every possible password that reduce the difficulty in brute-force cracking of a single password.

#### John the Ripper

John the Ripper is a free password-cracking tool that runs on various platforms. It is one of the more popular password-cracking programs as it combines a number of password crackers into one customizable program platform.

#### Cain & Abel

Cain & Abel is a password-recovery tool that can recover passwords using methods such as network packet sniffing. It can crack various password hashes by using methods such as dictionary, brute force, and cryptanalysis attacks.



**Figure 4-10** WEPCrack is a set of tools that can break encryption.

## WEPCrack

WEPCrack (Figure 4-10) is an open-source toolset, written in Perl, that was developed to crack the 802.11 WEP secret key. It includes the following tools:

- *WeakIVGen.pl*: This script imitates the IV/encrypted output seen at the 802.11 access point. It produces a series of initialization vector (IV) combinations that are used to weaken the encryption strength of the WEP traffic.
- *Prism-getIV.pl*: This script works with the help of either Prismdump or Ethereal and scans for the IVs that match the weakened secret keys. It also traps the first byte of an encrypted message and puts it in the log file of weak IVs (IVfile.log). This script accepts input from stdin or from a file specified on the command line. For Prismdump output, a user can either run `prismdump | prism-getIV.pl` or run `prismdump > capturefile` and then `prism-getIV.pl capturefile`.
- *WEPCrack.pl*: This script, with the help of the data collected from the WeakIVGen.pl script, tries to identify the secret WEP key. It can be used for 40-bit or 128-bit WEP. It scans the IVFile.log and, with weak IVs and the encrypted output, identifies the secret key.

## Idle CPU Time

Idle CPU Time is a tool developed by Counterpane Systems to scan the vulnerabilities of S/MIME 40-bit encryption. This tool applies the brute-force method on S/MIME-encrypted e-mail messages by decrypting them to RC5 format and checking for the possible key to decrypt the message. This tool is feasible to use on any kind of computer system, and some weaknesses of the RC2 encryption algorithm enhance its speed. This tool has been designed to operate using idle machine time.

This brute-force utility comes in two forms:

1. *Command line*: If the program is run from the command line in low priority, it ensures that the program uses only idle processor time.
2. *Screensaver*: Displays a polite screensaver during the cracking process of the cipher. It can also perform distributed computing, through which many computers can utilize the search space.

Both programs can save work automatically. The source code available with this package can be used to decrypt other algorithms.

## Data-Protection Tools

### Cleversafe Grid Builder

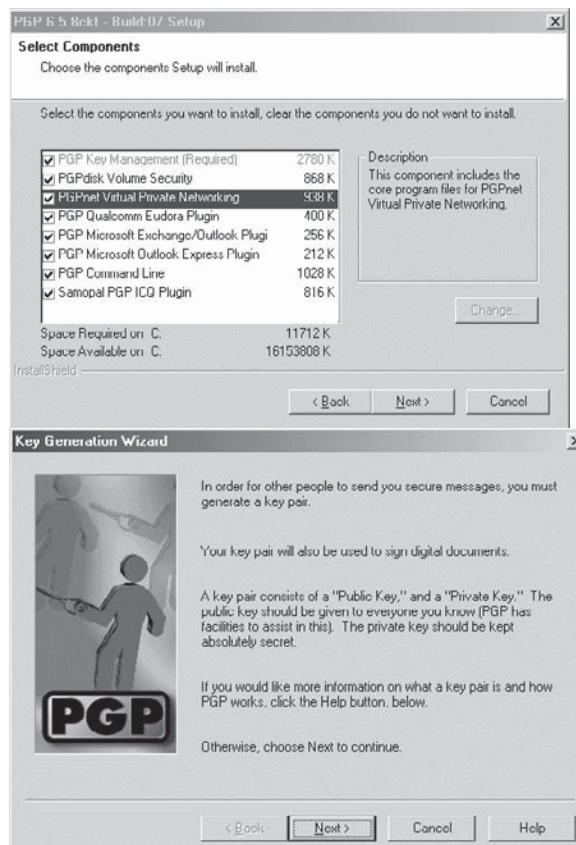
Cleversafe Grid Builder software subscriptions provide all the software needed to build a dispersed storage grid. The 11 dispersed storage nodes can be spread across up to 11 servers for maximum security.

Building a grid provides the following benefits:

- Controls data within the user's building
- Avoids expensive hardware costs
- Is customizable
- Creates derivative works by changing source code to meet the user's storage needs and processes

### PGP (Pretty Good Privacy)

Pretty Good Privacy (PGP) (Figure 4-11) is a software package developed to provide cryptographic procedures for e-mail and file storage applications. It also provides other features such as: message encryption, digital signatures, data compression, and e-mail compatibility. The algorithm used for message encryption is RSA for key transport and IDEA for bulk-message encryption. PGP uses RSA for computing digital signatures and MD5 for computing message digests.



**Figure 4-11** PGP provides encryption for e-mail and file storage.

The freeware program is used for message compression, transportation, and storage. E-mail compatibility is accomplished with the help of Radix-64 conversion.

PGP is used for five things:

1. Encrypting a message or file prior to transmission so that only the recipient can decrypt and read it
2. Clear signing of the plaintext message to ensure the authenticity of the sender
3. Encrypting stored computer files so that no one other than the person who encrypted them can decrypt them
4. Deleting files, rather than just removing them from the directory or folder
5. Data compression for storage or transmission

A PGP signature is different for every message because PGP performs a calculation on the message utilizing the user's secret key. The signature is also different, so that no one can cut and paste signatures. Each key is a long number, such as a 1,024-bit number (around 300 decimal digits).

The following is an example of a PGP signature:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQCNAzGvwGAAAAEAMQXI06gfdoZzy2Ngdqua6Zf6q4Bfdotc8qGHk9RncuEHSBf
2DrqYrkVmn6cANJp/HdBkJH39LcKybOGbxiahmjVnngPp+PzvX8+Wi7kQ5NP267S
0JIituePxuk1EQ5pqywHw8yxtOGIqLjkJtb/pRvZyiC0CywlbjnbPFHw2SetAAUR
tCZSb2JpbIBXaG10dGx1IDxmaXJzdHByQG96ZW1haWwuY29tLmF1PokA1QMFEDEgv
WGE52zxR8NknrQEBbV0D/1gJSldscj2bFJ0uD9LOY+LSTj71yxONZ3cycPZ+3zp
ShCNcsqNAGvHXDtqcGQrNrxHmYqnKBaJ/+46n/FSkDnt/bvEAb105m+6T5oTK8h+
MaaVuvdcphwKfIPQbIoI6LcmtwSd0cyBBndp+O+02x0xhcd2Qx7Gni7J+fz8mm0y
=Ysjn
-----END PGP PUBLIC KEY BLOCK-----
```

### **Command Line Scriptor**

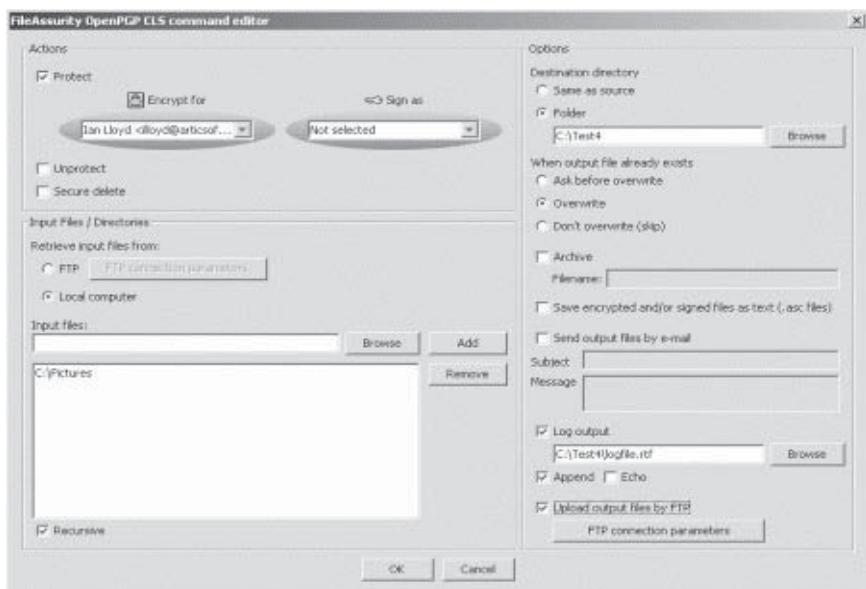
Command Line Scriptor is a server-side product that can be used to secure vulnerable files from attackers (Figure 4-12). It is based on OpenPGP and PKI standards, and provides complete integration with existing systems. Command Line Scriptor performs the following functions:

- Automates file encryption/decryption, digital signing, and verification
- Sends files and e-mail securely without any user intervention
- Ensures that all important data is secured without relying on user input
- Deletes bulk files at a predefined date and time
- Integrates cryptographic techniques into existing applications
- Processes incoming secure files from any OpenPGP-compliant application

### **CryptoHeaven**

CryptoHeaven (Figure 4-13) is used by groups to e-mail encrypted messages and securely back up and share files, pictures, charts, business documents, and any other type of electronic media. This tool does not allow third-party access to the plaintext version of transmitted information. The information is encrypted and stored on the server. Only the sender and the recipient possess the keys to gain access to the information.

All the services CryptoHeaven provides are encrypted with the AES symmetric cipher Rijndael, 256-bit encryption keys, SHA-256 message-digest function, and asymmetric encryption with keys of 2,048–4,096 bits in length. In normal cases, when a user forgets a username and password, all of the user's data that is stored on the server is lost or inaccessible forever. When a new user account is created, the user generates a personal private/public key pair. The public key of the encrypted message is sent to the server, where other users can collect keys by connecting to the server. The private part of the key is encrypted and is stored with the user's password on the local computer or transferred to the server at the user's request.



**Figure 4-12** Command Line Scriptor can be used to protect server files.



**Figure 4-13** CryptoHeaven can encrypt e-mail.

## ***Microsoft Cryptography Tools***

Microsoft provides command-line tools for code signing, signature verification, and other cryptography tasks. The publishing tool and the signing DLL for each cryptography tool are installed in the \Bin directory of every Microsoft SDK installation. Microsoft's cryptography tools include those shown in Figure 4-14.

File name	Remarks
Cert2SPC.exe	Creates an Software Publisher Certificate (SPC) for testing purposes only
CertMgr.exe	Manages certificates, CTLS, and certificate revocation lists (CRLs)
MakeCat.exe	Creates an unsigned catalog file that contains the hashes of a set of files along with associated attributes of each file
MakeCert.exe	Creates an X.509 certificate for testing purposes only
MakeCTL.exe	Creates a CTL
SetReg.exe	Sets registry keys that control certificate verification
Signer.dll	Required only by the tools in Internet Explorer 4.01
SignTool.exe	Signs and time stamps a file Additionally, checks the signature of a file

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

**Figure 4-14** Microsoft provides a variety of cryptography tools.

## Chapter Summary

- Using public-key cryptography, anyone can send a confidential message that can only be decrypted with a private key in the sole possession of the intended recipient.
- RSA encryption is a widely used de facto encryption standard.
- The MD5 algorithm is intended for digital signature applications, in which the document is compressed securely before being signed with a private key.
- An SHA algorithm accepts a message of 264 bits in length and produces a 160-bit message-output digest.
- Secure Sockets Layer (SSL) is a protocol used to provide a secure authentication mechanism between two communicating applications.
- RC5 is a fast block cipher designed by RSA Security.

## Review Questions

1. Name and describe two cryptographic techniques.

---



---



---



---

2. Briefly explain encryption.

---



---



---



---

3. What are the various types of RSA attacks?

---

---

---

---

4. Describe SHA (Secure Hash Algorithm).

---

---

---

---

5. Describe the WEPCrack tool.

---

---

---

---

6. What is SSH?

---

---

---

---

7. Name three encryption ciphers.

---

---

---

---

8. What does Distributed.net do?

---

---

---

---

9. Name two encryption-breaking techniques.

---

---

---

---

10. Describe the uses of disk encryption.

---

---

---

---

## Hands-On Projects



1. Use Advanced HTML Encrypt and Password Protect to encrypt HTML pages with strong encryption algorithms and protect them with a password.
  - Navigate to Chapter 4 of the Student Resource Center.
  - Install and launch the Advanced HTML Encrypt and Password Protect program (Figure 4-15).

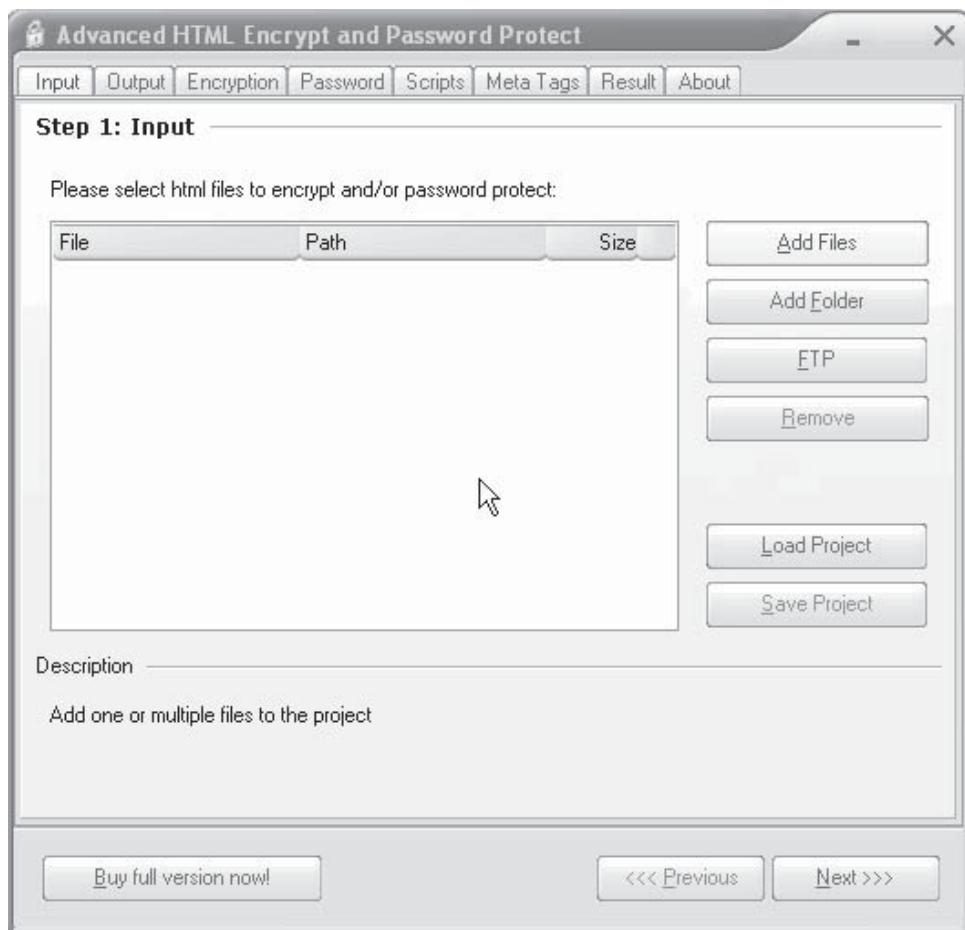


Figure 4-15 Launch Advanced HTML Encrypt and Password Protect.

- Click the Add Files button (Figure 4-16).

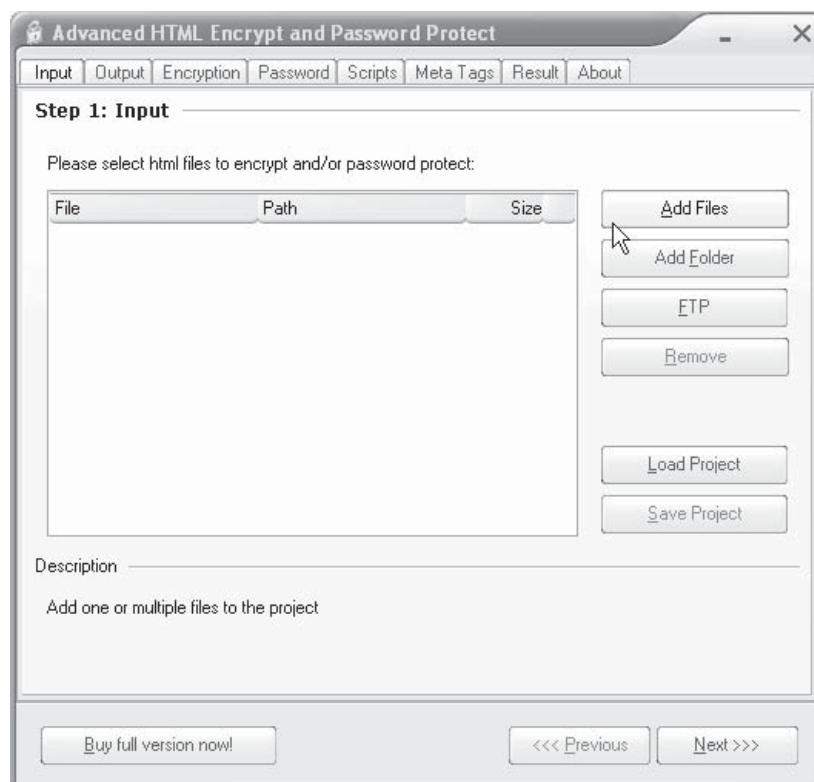


Figure 4-16 Click the Add Files button.

- Click the Open button to open a file (Figure 4-17).

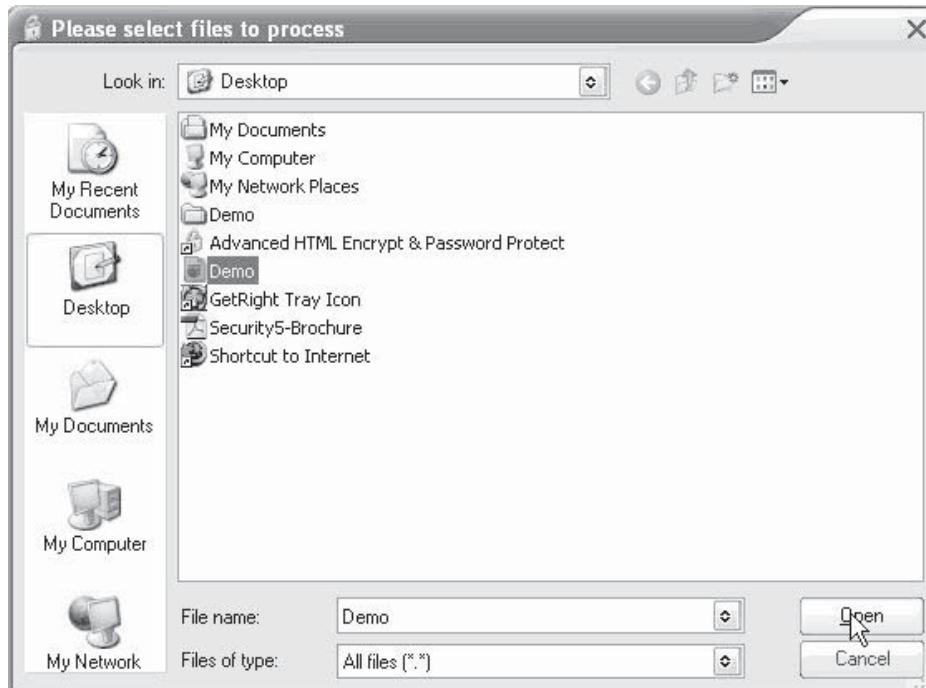


Figure 4-17 Click Open to open a file.

- Click **Next** to navigate to the **Output** tab (Figure 4-18).

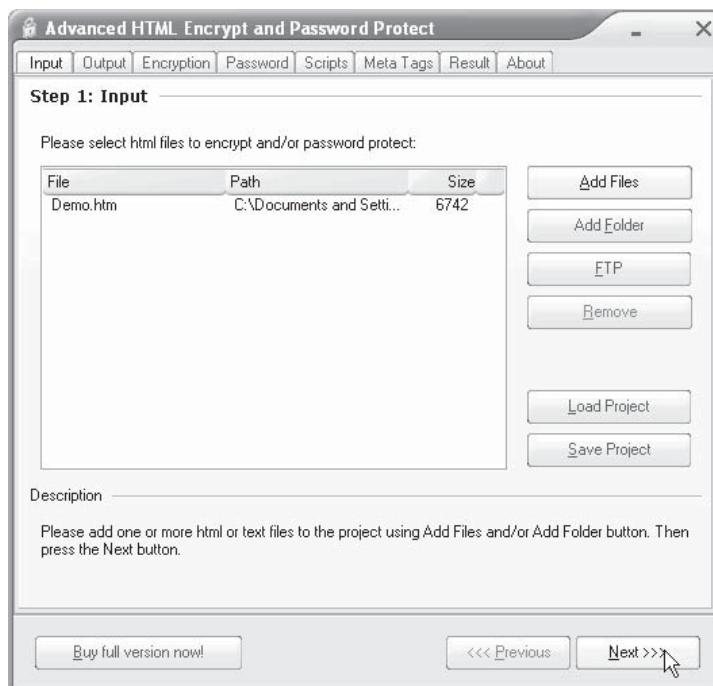


Figure 4-18 Click **Next** to navigate to the **Output** tab.

- Select the destination folder by enabling the button **Copy files to the following folder** (Figure 4-19).

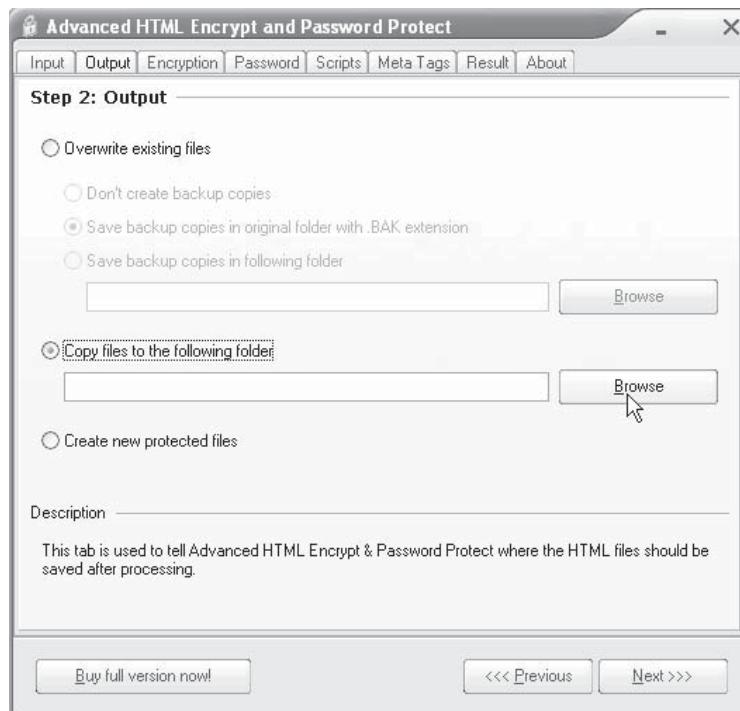
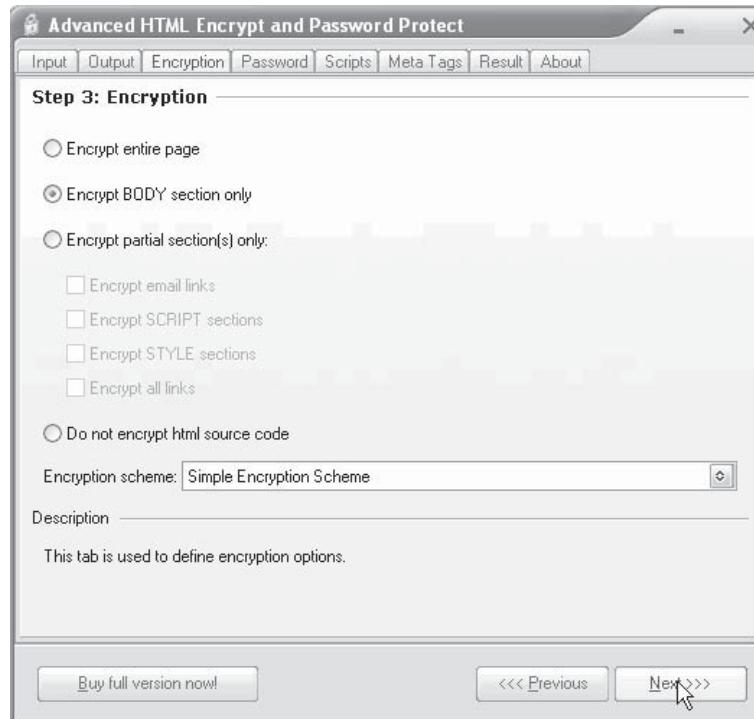


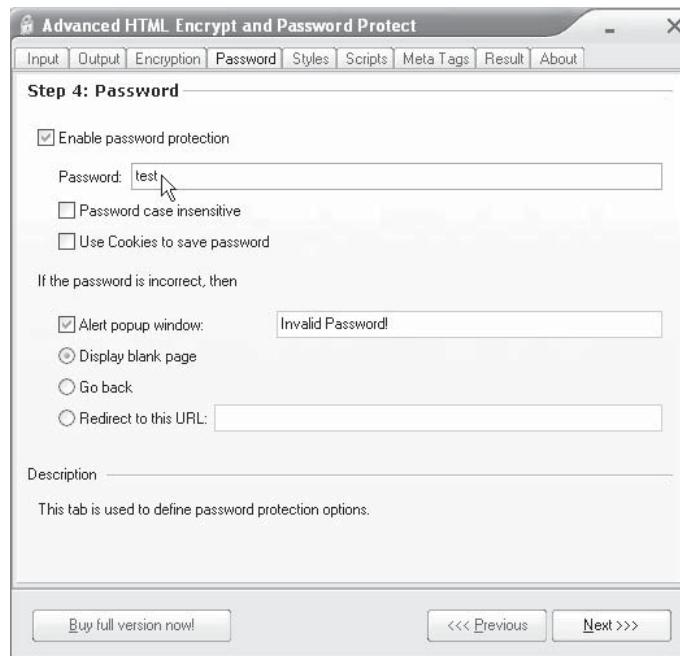
Figure 4-19 Select the destination folder.

- Click the **Next** button to navigate to the **Encryption** tab and then the **Password** tab (Figure 4-20).



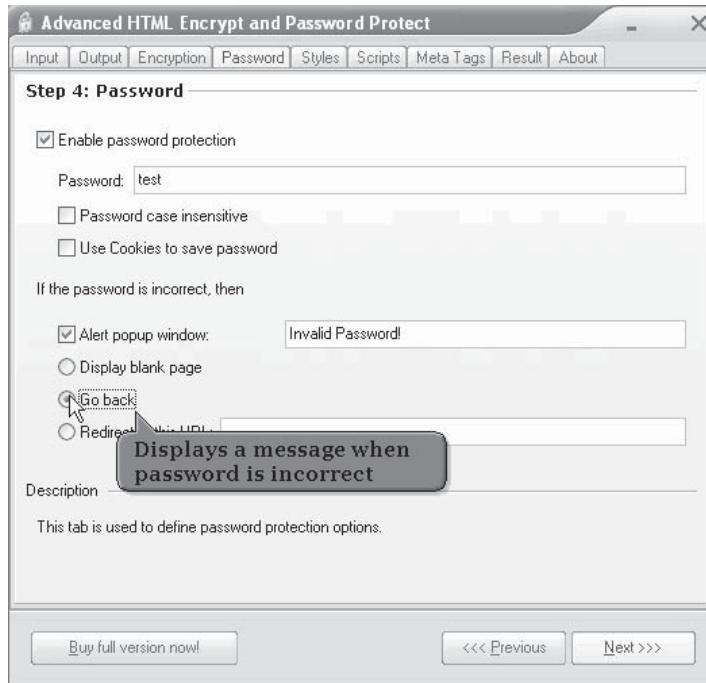
**Figure 4-20** Click the **Next** button to navigate to the **Encryption** tab.

- Enter the password in the **Password** field by enabling the **Enable password protection** check box (Figure 4-21).



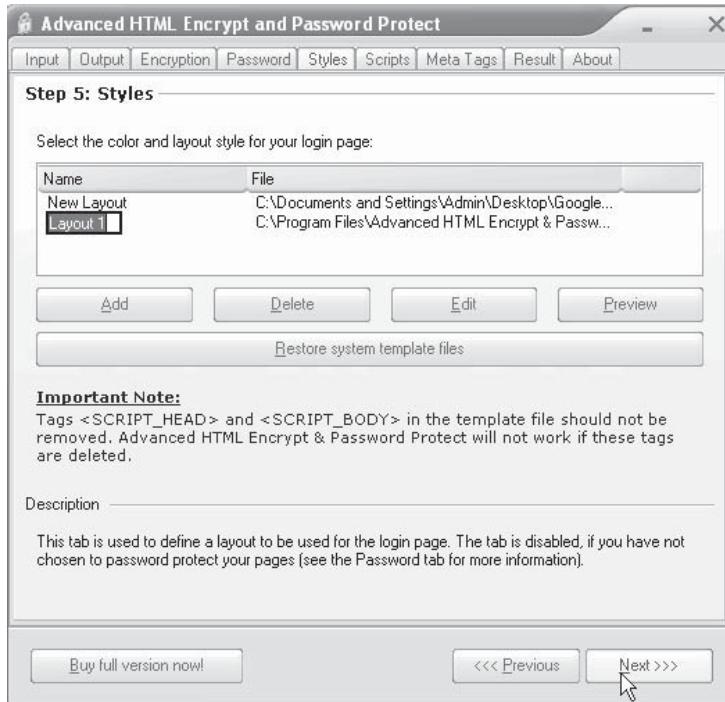
**Figure 4-21** Enter the password in the password field.

- To alert with a message when the password is incorrect, enable the check box **Alert popup window**, and select **Go back** (Figure 4-22).



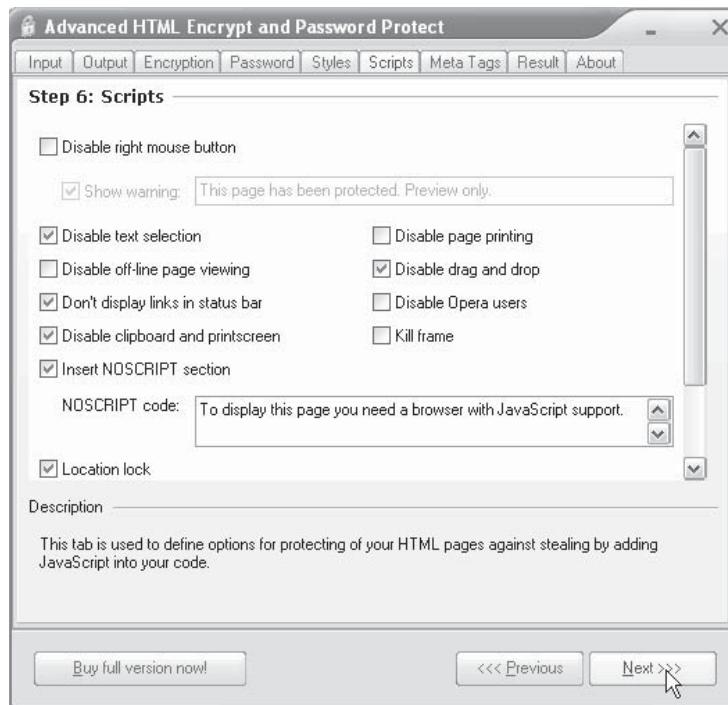
**Figure 4-22** Select **Go back** if the password is incorrect.

- Click the **Next** button to navigate to the **Styles** tab.
- Select the color and layout for the login page and click the **Next** button to navigate to the **Scripts** tab (Figure 4-23).



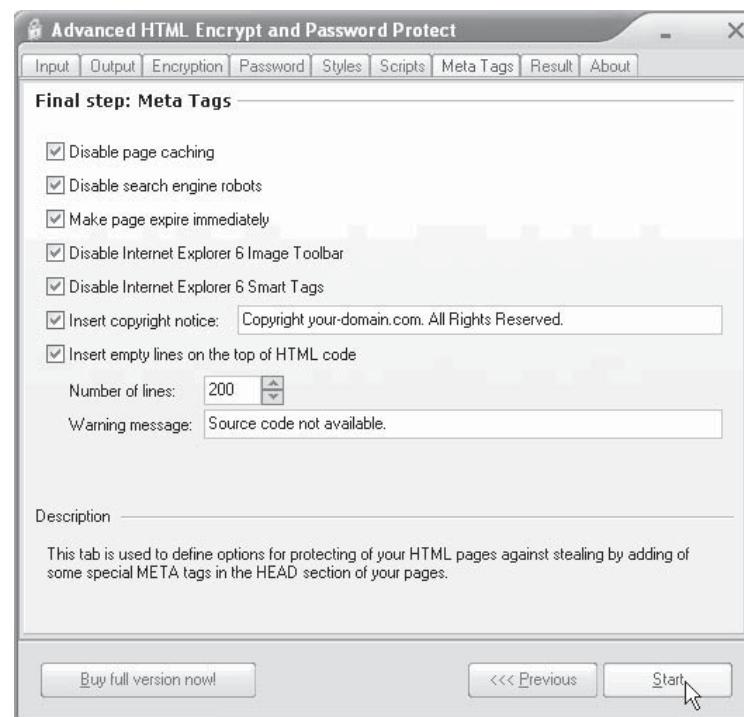
**Figure 4-23** Select the layout for the login page.

- Click the Next button to navigate to the Meta Tags tab (Figure 4-24).



**Figure 4-24** Click the **Next** button.

- Click the Start button (Figure 4-25).



**Figure 4-25** Click the **Start** button.

- Open the output file (Figure 4-26).

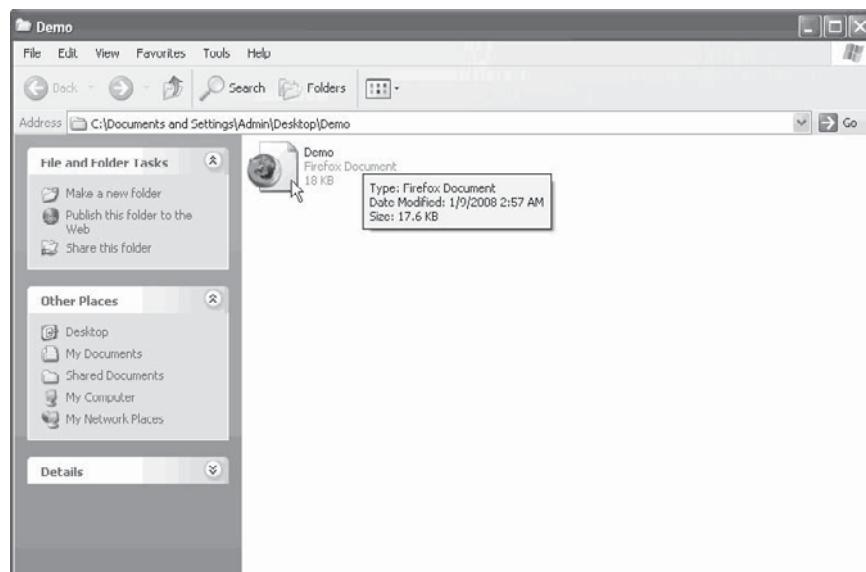


Figure 4-26 Open the output file.

- Enter the password in the **Password** field of the page and click the **Show** button.
- If the password entered is correct, the file is opened (Figure 4-27).

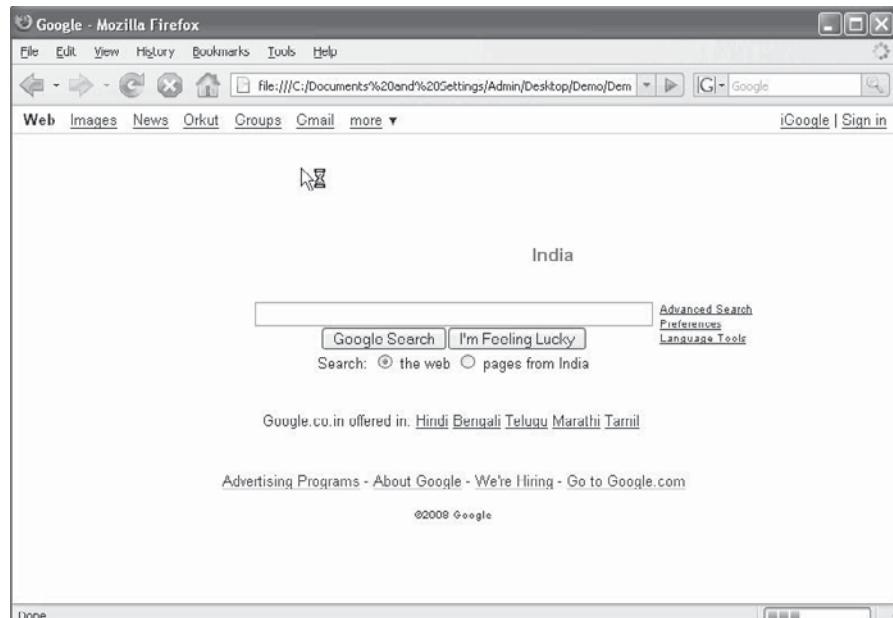
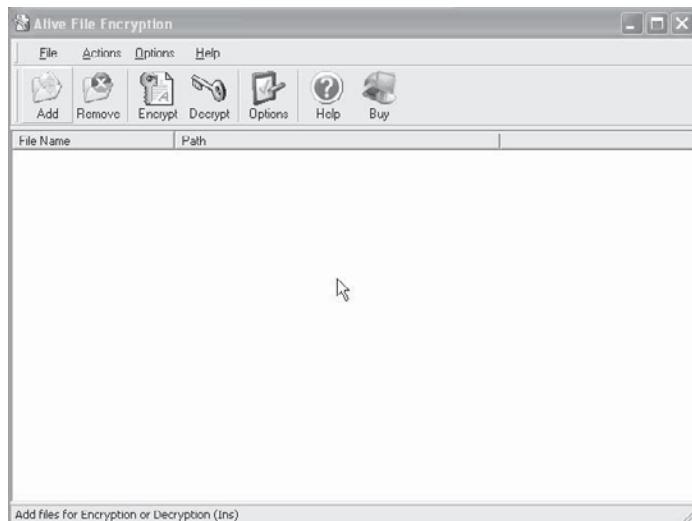


Figure 4-27 If the password is correct, the file is opened.



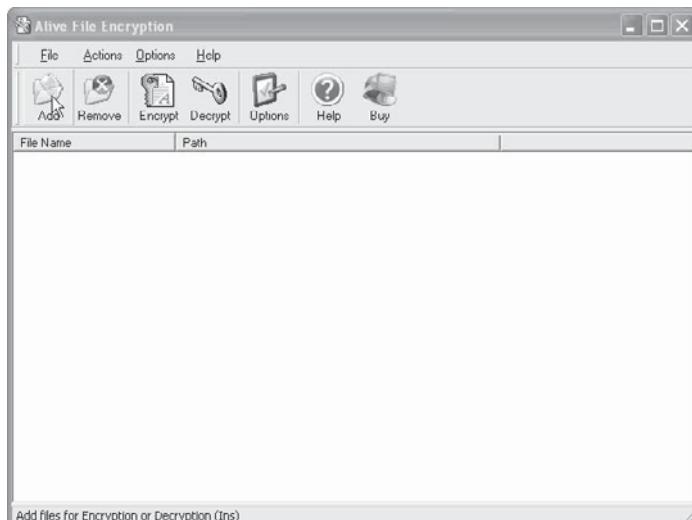
**Figure 4-28** If the password is incorrect, an “Invalid Password!” message is displayed.

- If the password is incorrect, an “Invalid Password!” message is displayed (Figure 4-28).
2. Use Alive File Encryption to encrypt or decrypt files and folders.
- Navigate to Chapter 4 of the Student Resource Center.
  - Install and launch the Alive File Encryption program (Figure 4-29).



**Figure 4-29** Install and launch Alive File Encryption.

- Click the Add button in the application bar to open a file (Figure 4-30).



**Figure 4-30** Click the Add button.

- Select the file and click the Encrypt button (Figure 4-31).

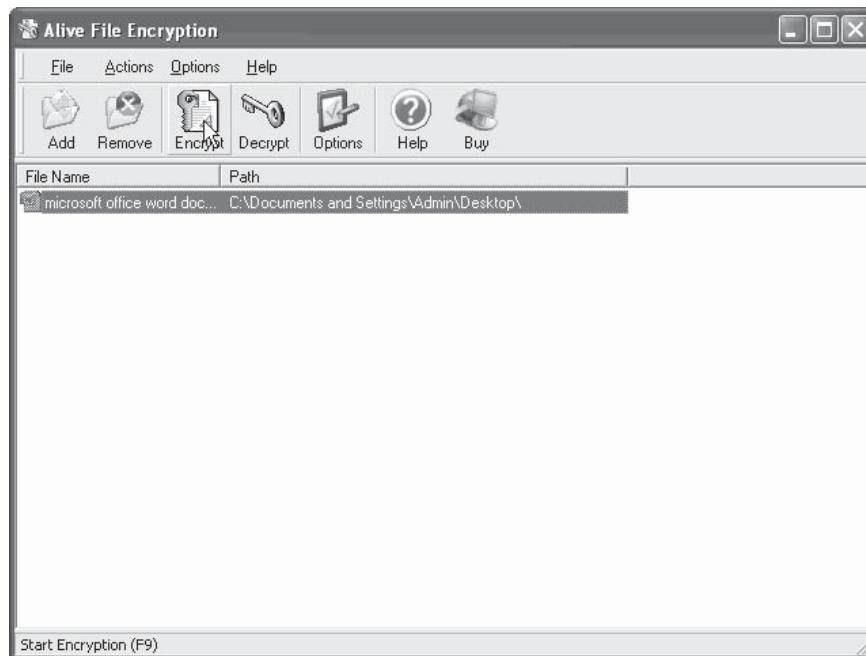


Figure 4-31 Select a file.

- Enter the password and click the OK button (Figure 4-32).

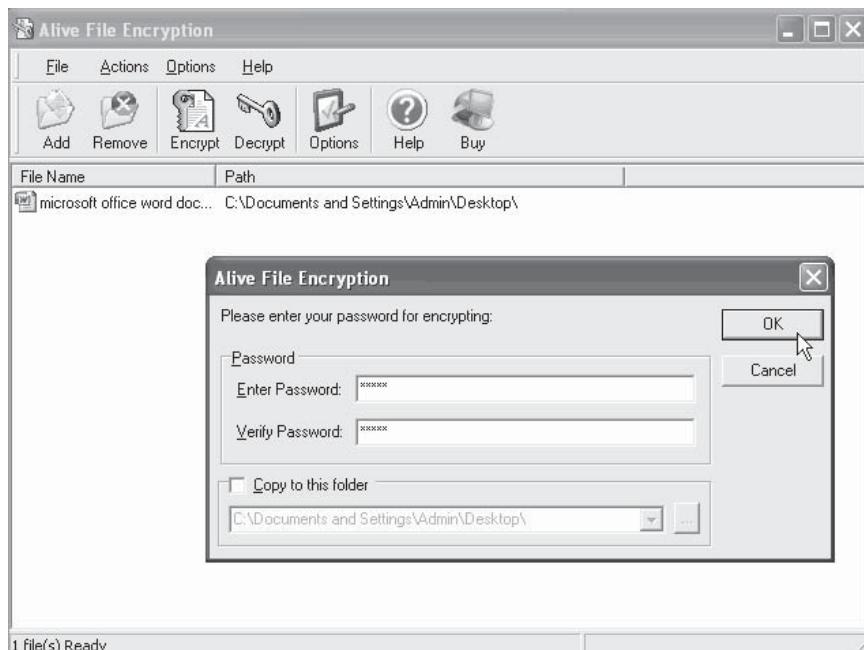


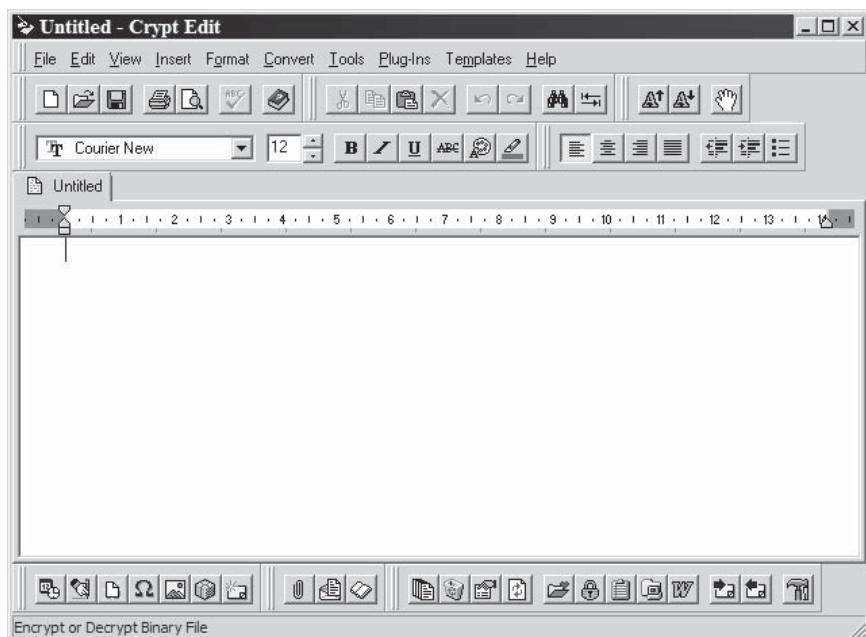
Figure 4-32 Enter the encrypting password.

- Select the encrypted file for decrypting.
- Enter the password in the **Enter Password** field and click the **OK** button to decrypt the file (Figure 4-33).



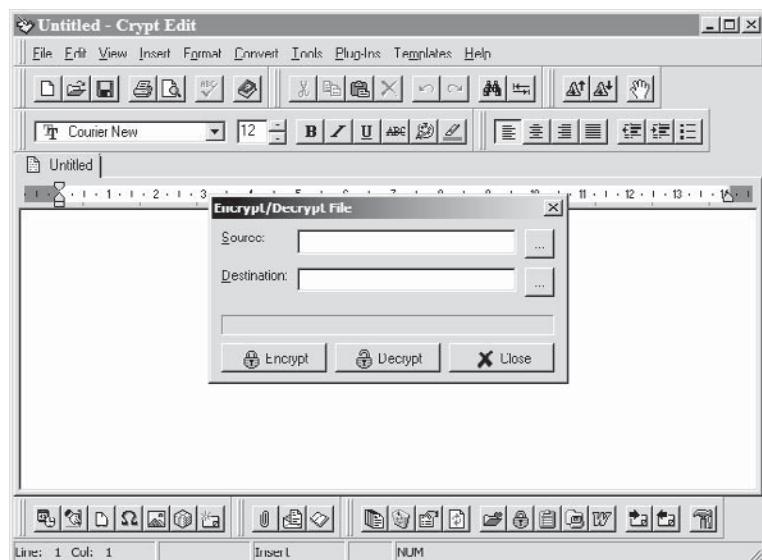
**Figure 4-33** Enter the password for decrypting.

3. Use Crypt Edit to encrypt and decrypt binary files and save the files in different formats.
  - Navigate to Chapter 4 of the Student Resource Center.
  - Install and launch the Crypt Edit program (Figure 4-34).



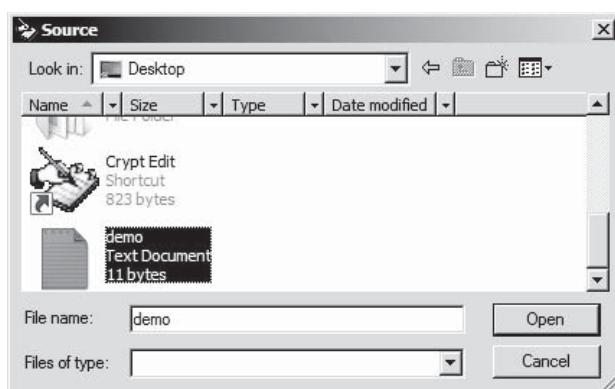
**Figure 4-34** Install and launch Crypt Edit.

- For encryption, click on the Encrypt/Decrypt File button (Figure 4-35).



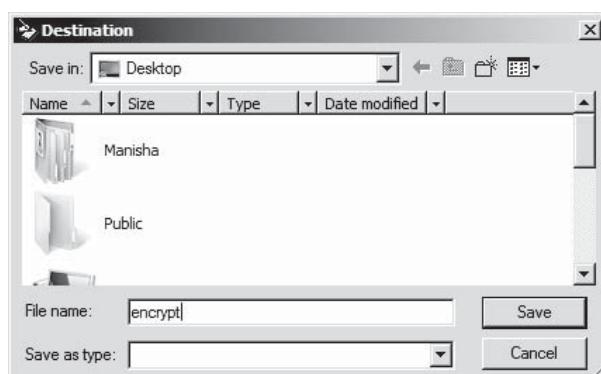
**Figure 4-35** Select the Encrypt/Decrypt File button.

- Select the file to be encrypted in the Source window (Figure 4-36).



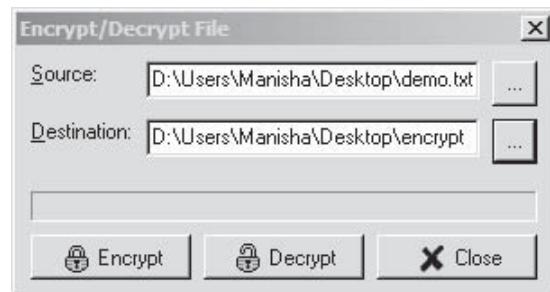
**Figure 4-36** Select the file to be encrypted.

- Select the destination of the encrypted file in the Destination window (Figure 4-37).



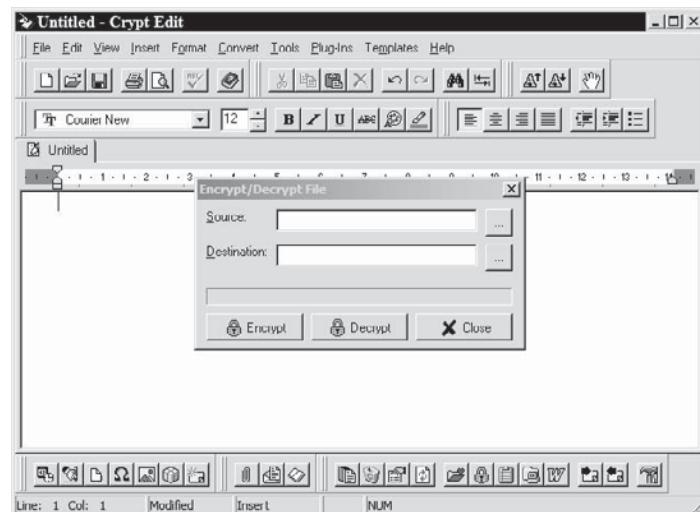
**Figure 4-37** Select the file's destination.

- Click the **Encrypt** button (Figure 4-38).



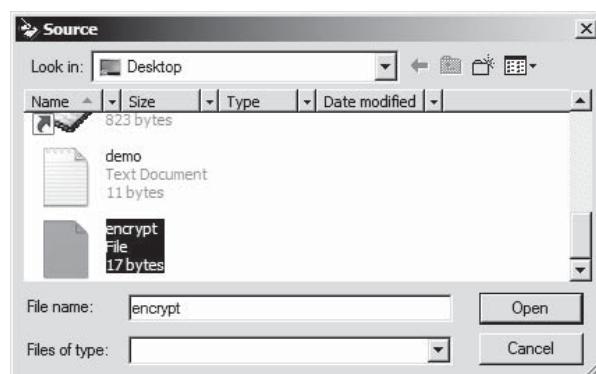
**Figure 4-38** Click the **Encrypt** button.

- Enter the password in the **Setting Password** window and click the **OK** button. A message is displayed in the **Information** window for the successful conversion of the file; click the **OK** button.
- For decryption, click on **Encrypt/Decrypt Binary File** (Figure 4-39).



**Figure 4-39** Click on **Encrypt/Decrypt Binary File**.

- Select the file to be decrypted in the **Source** window (Figure 4-40).



**Figure 4-40** Select the file to be decrypted.

- Select the destination of the decrypted file in the Destination window (Figure 4-41).

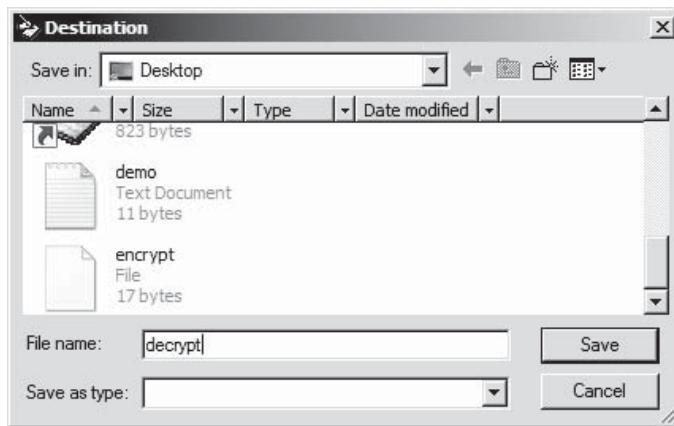


Figure 4-41 Select the destination of the decrypted file.

- Click the Decrypt button (Figure 4-42).

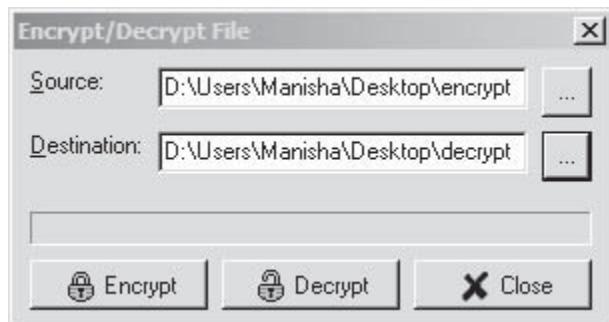


Figure 4-42 Click the Decrypt button.

- Enter the password in the Password field and click the OK button. A message is displayed in the Information window for the successful conversion of the file; click the OK button.

# Index

007 Shell, 3-35

## A

Access control checklist, 2-19

Access controls, as security measure, 2-3

Access points (APes), 1-2

AckCmd, 3-36

ACK tunneling, 3-20–3-21

Address filtering, 3-14

ADMutate, 3-31–3-32

Aicmpsend, 3-32

Aircrack, 1-20

AirDefense Guard, 1-38

AirMagnet, 1-33, 1-34

AirMagnet Handheld Analyzer, 1-36–1-37

AiroPeek NX, 1-31

AirPcap, 1-20, 1-21

AirTraf, 1-29

Anomaly detection, 3-4

Antennas, 1-8–1-9

Anzen NIDSbench, 3-31

APes (access points), 1-2

Application-level firewall, 3-17

Apsend, 3-32

AP spoofing, 1-8

Asymmetric key system, 4-2

Atelier Web Firewall Tester, 3-44, 3-45

Authentication, 1-7–1-8, 2-5–2-7

## B

Backdoors, through firewalls, 3-20

Banner grabbing, 3-19

Baseline, 3-4

Beacon frames, 1-9

Beacons, 1-23

Biometric authentication, 2-5–2-6, 2-12

Biometric technology, 2-4

BlackICE, 3-26

Blast, 3-32

Blowfish, 4-5

Brute Force, 4-11

## C

Cain & Abel, 1-21–1-22, 4-13

CASL, 3-32

CE (compromising emanations), 2-15

Circuit-level gateway, 3-16–3-17

Cisco Secure IDS, 3-27

Cisco-Security Agent (CSA), 3-25–3-26

Cleversafe Grid Builder, 4-15

Cloaked access point, 1-25

Command Line Scriptor, 4-16, 4-17

CommView for WiFi PPC, 1-36, 1-37

Company surroundings checklist, 2-15–2-16

Complex attacks, 3-9

Compromising emanations (CE), 2-15

Computer equipment maintenance checklist, 2-19

ComputracePlus, 2-23

Covert\_TCP, 3-36

Covert channel, 3-20

Cryptography

defined, 4-2

disk encryption, 4-10

encryption-breaking initiatives, 4-10–4-11

encryption countermeasures, 4-11–4-13

introduction, 4-2

message-digest (hash) functions, 4-6–4-7

public-key, 4-2–4-5

secure shell (SSH), 4-9–4-10

secure sockets layer (SSL), 4-7–4-9

tools for, 4-13–4-17, 4-18

CryptoHeaven, 4-16, 4-17

CSA (Cisco Security Agent), 3-25–3-26

The CyberAngel, 2-23

CyberCop Monitor, 3-26–3-27

## D

Data Encryption Standard (DES), 4-4–4-5

Data-protection tools, 4-15

Denial-of-service (DoS) attacks, 1-17–1-18, 3-8–3-9

DES (Data Encryption Standard), 4-4–4-5

Desynchronization, 3-9

Device Lock, 2-20–2-21

Digital certificates, 2-7

Digital signatures, 4-2

Disk encryption, 4-10

Distributed.net, 4-11

Dragon, 3-27

driftnet, 1-33, 1-34

Dust, as physical security threat, 2-10

## E

Easy Tcplp Library, 3-32

eEye Retina Network Security Scanner, 1-29, 1-30

Encryption, 2-7

Equipment checklist, 2-19

EtherPEG, 1-33

Ettercap, 3-32

Evasion attacks, 3-8

Evil-twin attack, 1-13

Explosions, as physical security threat, 2-11

## F

Fakeap, 1-24

Filtering, 3-12

Firewalking, 3-18

Firewall Informer, 3-44, 3-45

Firewalls

ACK tunneling, 3-20–3-21

breaching, 3-19

bypassing, using HTTP Tunnel, 3-19–3-20

countermeasures to, 3-17–3-19

defined, 3-3

explained, 3-13–3-14

introduction, 3-2

limitations of, 3-15

Loki, 3-20

methodology, 3-14–3-15

packet filtering, 3-14

placing backdoors through, 3-20

purpose of, 3-13

types of, 3-15–3-17

Fragmentation, 3-9

Fragment reassembly, 3-12

Fragrouter, 3-31

Frequency analysis, 4-11

FTester, 3-36–3-42

## G

Google Secure Access, 1-38, 1-39

## H

Hardware firewalls, 3-15

Hash functions, 4-6–4-7

HIDS (host-based intrusion detection system), 3-5–3-6

Honeyd, 3-46–3-473

Honeynet Project, 3-21–3-22

Honeypots

advantages and disadvantages, 3-22–3-23

available, 3-23

defined, 3-3

detection introduction, 3-2

explained, 3-21

Honeynet Project, 3-21–3-22

physical and virtual, 3-24

placing, 3-23

types of, 3-22

Host-based intrusion detection system (HIDS), 3-5–3-6

Host-based IPS (HIPS), 3-11

Hping2, 3-32

HP OpenView Node Sentry, 3-27

HTTP Tunnel, 3-19–3-20

## I

ICMP Shell, 3-35–3-36

ICMP Push, 3-32–3-33

Icrzo, 3-33

Idle CPU Time, 4-14–4-15

IEEE (Institute of Electrical and Electronics Engineers) standards, 1-3–1-5

Information flow, in IDS and IPS, 3-12–3-13

Insertion attacks, 3-8

Intrusion detection systems (IDS)

common tools for testing firewalls and, 3-36–3-45

defined, 3-2

evading, 3-8–3-10, 3-31–3-32

host-based tools, 3-25–3-26

indications of intrusion, 3-7

information flow in, 3-12–3-13

introduction, 3-2–3-3

vs. IPS, 3-13

placement, 3-3

post-attack steps, 3-8

techniques for, 3-3–3-5

tools for, 3-26–3-31

types of, 3-5–3-6

Intrusion prevention system (IPS)

defined, 3-3

deployment risks, 3-11

explained, 3-10

vs. IDS, 3-13

information flow in, 3-12–3-13

strategies for, 3-11

types of, 3-11–3-12

Ippacket, 3-33

ipsend, 3-33

ISIC, 3-33

## J

John the Ripper, 4-13

## K

KFSensor, 3-47–3-48

Kismet, 1-22, 1-23

Knowledge-based authentication, 2-6

## L

Laptops

securing, 2-7–2-8, 2-9

security tools for, 2-21–2-22

tracking and recovery tools, 2-22–2-24

Laptop Tracker —XTool Computer Tracker, 2-23

LEAP (Lightweight Extensible Authentication Protocol), 1-14–1-15

LFM (log file monitors), 3-6

Libnet, 3-33

LibnetNT, 3-33

Lightweight Extensible Authentication Protocol (LEAP), 1-14–1-15

Lock picking, 2-12–2-13, 2-14, 2-20–2-21, 2-22

Locks, as security measure, 2-3–2-4

Log file monitors (LFM), 3-6

Logging tools, 3-25

Loki, 3-20

Lucent RealSecure, 3-27

## M

MAC sniffing, 1-8

MacStumbler, 1-26, 1-27

Man-in-the-middle attack (MITM), 1-17

Mantrap, 2-25

MD2/4/5, 4-6–4-7

Mendax, 3-31

Message-digest functions, 4-6–4-7

MGEN Toolset, 3-33

Microsoft Cryptography tools, 4-17, 4-18

Microsoft Network Monitor, 1-36

MiniStumbler, 1-24, 1-25

Mognet, 1-26–1-27

Mpac, 3-33

Multiple access points, 1-3

## N

Natural calamities, as physical security threat, 2-10

Nemesis, 3-33

Nessus Security Scanner, 3-49

Net::RawIP, 3-34

Netcat, 3-34

NetChaser, 1-28

NetProwler, 3-27

Netsh, 3-34

Network-based intrusion detection system (NIDS), 3-5

Network-based IPS (NIPS), 3-11–3-12

Network Flight Recorder (NFR), 3-27

Network Stumbler, 1-24, 1-25

Next-Generation Intrusion Detection Expert System (NIDES), 3-42–3-43

NIDS (network intrusion detection system), 3-5

## O

Obfuscation, 3-9

Object-based authentication, 2-7

OrphCrack Live CD, 4-13

## P

Packet decoding, 3-12

Packet-filtering firewalls, 3-15–3-16

The Packet Shell, 3-35  
 PacketX, 3-34  
 Pad collection attacks, 1-19  
 Peer-to-peer networks, 1-2  
 PGP (Pretty Good Privacy), 4-15–4-17, 4-18  
 Phone jammers, 1-9–1-10  
 Physical security  
     challenges, 2-10–2-25  
     checklists, 2-15–2-20  
     countermeasures to, 2-11–2-15  
     introduction, 2-2–2-3  
     operational measures, 2-9  
     personnel, 2-9–2-10  
     physical measures, 2-3–2-4  
     technical measures, 2-4–2-8, 2-9  
     threats, 2-10–2-11  
     tools for, 2-20–2-25  
 Port scanning, 3-17  
 Premises checklist, 2-16  
 Pretty Good Privacy (PGP), 4-15–4-17, 4-18  
 Prismstumbler, 1-26  
 Protocol anomaly detection, 3-4–3-5  
 Protocol filtering, 3-14  
 Public-key certificate, 4-3  
 Public-key cryptography, 4-2–4-5

**R**

Rainbow tables, 4-13  
 Raw packet capture, 3-12  
 RC4/5/6, 4-5  
 RealSecure, 3-27  
 Reception area checklist, 2-17  
 Remote access checklist, 2-20  
 Removable media devices, disabling, 2-5  
 Rivest Shamir Adleman (RSA), 4-3–4-5  
 Roaming, 1-3  
 Rogue access points, 1-23–1-25, 1-26  
 RogueScanner, 1-38, 1-39  
 RSA attacks, 4-12–4-13  
 RSA Factoring Challenge, 4-10  
 RSA (Rivest Shamir Adleman), 4-3–4-5

**S**

Sebek, 3-48  
 SecureHost, 3-43

Secure Shell (SSH), 4-9–4-10  
 Secure Sockets Layer (SSL), 4-7–4-9  
 Security personnel, as security measure, 2-3  
 Security responses, to hacking attacks, 3-24–3-25  
 Security tokens, 2-7  
 Security Tracking of Office Property (STOP) plates, 2-23–2-24  
 SendIP, 3-34  
 Send Packet, 3-34  
 Send-Safe Honeypot Hunter, 3-48  
 Server checklist, 2-17  
 Service set identifier (SSID), 1-6  
 Session interception, 3-11  
 Session splicing, 3-9–3-10  
 SHA-1 (Secure Hash Algorithm), 4-7  
 SideStep, 3-31  
 Signature recognition, 3-3–3-4  
 SilentRunner, 3-27  
 SING, 3-34  
 Smart cards, 2-7  
 SNARE (System iNtrusion Analysis and Report Environment), 3-43  
 Sniffing the air, 1-23–1-24  
 Sniffing tools, 1-31–1-36  
 Snort, 3-27–3-31  
 Socket Script, 3-34  
 Software firewalls, 3-15  
 Spak, 3-34  
 SPECTER, 3-46  
 Spyware technologies, 2-11–2-12  
 SSH (Secure Shell), 4-9–4-10  
 SSL (Secure Sockets Layer), 4-7–4-9  
 Stateful inspection of TCP session, 3-12  
 Stateful multilayer inspection firewall, 3-17, 3-18  
 Stick, 3-31  
 STOP (Security Tracking of Office Property) Plate, 2-23–2-24  
 Storage, 3-12  
 Stream assembly, 3-12  
 Stream cipher, 1-20  
 Super Bluetooth Hack, 1-16–1-17  
 Symmetric key system, 4-2  
 System integrity verifier (SIV), 3-6  
 System iNtrusion Analysis and Report Environment (SNARE), 3-43

**T**

TCP/IP Library, 3-35  
 TCPOpera, 3-44  
 Tcpreplay, 3-35  
 Technical security, 2-4–2-8, 2-9  
 TEMPEST monitoring, 2-13, 2-15  
 Temporal Key Integrity Protocol (TKIP), 1-13–1-14  
 Terrorist attacks, as physical security threat, 2-11  
 THC-RUT, 1-35  
 Theft, 2-10  
 Time delays, 3-11  
 TKIP (Temporal Key Integrity Protocol), 1-13–1-14  
 Track Stick GPS Tracking Device, 2-22–2-23  
 Traffic IQ Pro, 3-42  
 Tripwire, 3-25  
 TrueCrypt, 2-24

**U**

USI++, 3-35

**V**

Vandalism, as physical security threat, 2-10  
 Vanguard Enforcer, 3-27  
 Virtual private network (VPN), 2-18  
 vxSniffer, 1-32

**W**

WAP (wireless access point), 2-18  
 Water, as physical security threat, 2-11  
 Wavemon, 1-28  
 WaveStumbler, 1-27  
 WEPCrack, 4-14  
 WEP (wired equivalent privacy), 1-10–1-12, 1-18–1-22, 1-23, 2-18  
 Whackers, 1-2  
 Wi-Fi Protected Access (WPA), 1-12–1-13, 2-18  
 WifiScanner, 1-29  
 WinDump, 1-33, 1-35  
 Wired equivalent privacy (WEP), 1-10–1-12, 1-18–1-22, 1-23, 2-18  
 Wireless access points (WAP), 1-9, 2-18  
 Wireless Lan Scanner, 1-29, 1-30  
 Wireless LAN (WLAN), 1-2

- Wireless networks  
advantages and disadvantages, 1-3  
concepts of, 1-5–1-8  
devices for, 1-8–1-10  
hacking introduction, 1-1  
hacking methods, 1-15–1-18  
open, detecting, 1-15  
rogue access points, 1-23–1-25, 1-26  
scanning tools, 1-26–1-30, 1-31  
sniffing tools, 1-31–1-36  
standards for, 1-3–1-5
- TKIP and LEAP, 1-13–1-15  
types of, 1-2–1-3  
wired equivalent privacy (WEP), 1-10–1-12, 1-18–1-22, 1-23  
vs. wired networks, 1-2  
wireless security tools, 1-36–1-39  
WPA, 1-12–1-13  
Wireless Security Auditor (WSA), 1-28–1-29  
Wireless security tools, 1-36–1-39  
Wireshark, 1-31, 1-32  
Wiretapping checklist, 2-20
- Workstation area checklist, 2-17–2-18  
WPA (Wi-Fi Protected Access), 1-12–1-13, 2-18  
WSA (Wireless Security Advisor), 1-28–1-29

**X**

- Xipdump, 3-35  
XOR encryption, 1-19

**Z**

- Ztrace Gold, 2-23

*This page intentionally left blank*

# General Notice

The Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. You will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and you shall indemnify EC-Council and its partners from all liability with respect to the use or misuse of these tools, regardless of intent.

EC-Council provides the hacking skills and tools used in the CEH classroom for educational use. The hacking tools are not authored by EC-Council, and in many cases are submitted by the security community. EC-Council will not be held accountable for any damages caused by the proper or improper usage of these materials, and makes no guarantee in regards to their operation or suitability for any specific purpose.

The hacking tools used in the CEH program are meant for research and educational purposes only. The primary intent of these tools is to provide the user with hard to find content for research or self education relevant to network security and various protection methods and their intrinsic flaws by demonstrating exploitation methods and techniques used to circumvent them. We hope that you become more aware of the dangers that lurk in society today and learn how to protect yourself from them with the knowledge you are about to learn. In order to continue you must accept that you are going to use this information only for educational and research purposes only.

While possession of information or programs included in this training violates no laws, actually using or implementing some of the programs or content may violate U.S. Federal and other laws. For this reason, the user is instructed not to use any programs or content contained in this training which may violate any laws or infringe on the rights, including intellectual property rights, of others. We provide them for research and educational purposes only.