

# Network Security and Firewalls: Academic Student Guide



**EVALUATION COPY**

# **Network Security and Firewalls**

## **Developers**

Timothy Crothers and James Stanger, Ph.D.

## **Contributor**

Grant Jones

## **Editor**

Jill McKenna

## **Publishers**

Joseph Flannery and Scott Evanskey

## **Project Managers**

David De Ponte, Todd Hopkins and Sheila Ramirez

## **Trademarks**

Prosoft is a trademark of ProsoftTraining. All product names and services identified throughout this book are trademarks or registered trademarks of their respective companies. They are used throughout this book in editorial fashion only. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with the book. Copyrights of any screen captures in this book are the property of the software's manufacturer.

## **Disclaimer**

ProsoftTraining makes a genuine attempt to ensure the accuracy and quality of the content described herein; however, ProsoftTraining, makes no warranty, express or implied, with respect to the quality, reliability, accuracy, or freedom from error of this document or the products it describes. ProsoftTraining makes no representation or warranty with respect to the contents hereof and specifically disclaims any implied warranties of fitness for any particular purpose. ProsoftTraining disclaims all liability for any direct, indirect, incidental or consequential, special or exemplary damages resulting from the use of the information in this document or from the use of any products described in this document. Mention of any product or organization does not constitute an endorsement by ProsoftTraining of that product or corporation. Data used in examples and exercises is intended to be fictional even if actual data is used or accessed. Any resemblance to, or use of real persons or organizations should be treated as entirely coincidental. ProsoftTraining makes every effort to ensure the accuracy of URLs referenced in all our materials, but we can not guarantee that all will be available throughout the life of the course. When this manual/disk was published, all URLs were checked for accuracy and completeness. However, due to the ever-changing nature of the Internet, some URLs may no longer be available or may have been re-directed.

## **Copyright Information**

This training manual is copyrighted and all rights are reserved by ProsoftTraining. No part of this publication may be reproduced, transmitted, stored in a retrieval system, modified, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without written permission of ProsoftTraining, 3001 Bee Caves Road, Austin, TX 78746.

Copyright © 2000 - 2002 by ProsoftTraining  
All Rights Reserved

ISBN: 1-58143-650-5



EVALUATION COPY

# Table of Contents

Course Description.....	xi
ProsoftTraining Courseware .....	xii
Course Objectives .....	xiv
Classroom Setup.....	xiv
System Requirements .....	xv
Conventions and Graphics Used in This Book.....	xviii
<b>Lesson 1: What Is Security?.....</b>	<b>1-1</b>
Pre-Assessment Questions .....	1-2
Network Security Background.....	1-3
What Is Security?.....	1-4
Hacker Statistics.....	1-8
What Is the Risk?.....	1-9
The Myth of 100-Percent Security.....	1-10
Attributes of an Effective Security Matrix.....	1-11
What You Are Trying to Protect.....	1-12
Who Is the Threat?.....	1-14
Security Standards .....	1-15
Lesson 1 Review .....	1-20
<b>Lesson 2: Elements of Security .....</b>	<b>2-1</b>
Pre-Assessment Questions .....	2-2
Security Concepts and Mechanisms .....	2-3
Elements of Security .....	2-3
The Security Policy.....	2-4
Encryption.....	2-13
Authentication.....	2-17
Specific Authentication Techniques .....	2-21
Access Control.....	2-25
Auditing .....	2-35
Security Tradeoffs and Drawbacks.....	2-36
Lesson 2 Review .....	2-39
<b>Lesson 3: Applied Encryption.....</b>	<b>3-1</b>
Pre-Assessment Questions .....	3-2
Reasons to Use Encryption .....	3-3
Creating Trust Relationships.....	3-3
Rounds, Parallelization and Strong Encryption .....	3-4
Symmetric-Key Encryption .....	3-5
Symmetric Algorithms.....	3-6
Asymmetric Encryption .....	3-14
Hash Encryption.....	3-17
Applied Encryption Processes .....	3-20
Encryption Review.....	3-38
Lesson 3 Review .....	3-42

---

<b>Lesson 4: Types of Attacks</b> .....	<b>4-1</b>
Pre-Assessment Questions .....	4-2
Attack Categories.....	4-3
Brute-Force and Dictionary Attacks .....	4-3
System Bugs and Back Doors.....	4-4
Social Engineering and Non-direct Attacks.....	4-10
Lesson 4 Review .....	4-21
<b>Lesson 5: General Security Principles</b> .....	<b>5-1</b>
Pre-Assessment Questions .....	5-2
Common Security Principles: Introduction .....	5-3
Be Paranoid.....	5-4
You Must Have a Security Policy.....	5-5
No System or Technique Stands Alone .....	5-5
Minimize the Damage.....	5-6
Deploy Companywide Enforcement.....	5-6
Provide Training .....	5-7
Use an Integrated Security Strategy.....	5-8
Place Equipment According to Needs .....	5-8
Identify Security Business Issues.....	5-9
Consider Physical Security .....	5-10
Lesson 5 Review .....	5-16
<b>Lesson 6: Protocol Layers and Security</b> .....	<b>6-1</b>
Pre-Assessment Questions .....	6-2
TCP/IP Security Introduction .....	6-3
TCP/IP and Network Security .....	6-3
The TCP/IP Suite and the OSI Reference Model .....	6-4
Physical Layer.....	6-5
Network Layer .....	6-5
Transport Layer.....	6-9
Application Layer .....	6-13
Lesson 6 Review .....	6-22
<b>Lesson 7: Securing Resources</b> .....	<b>7-1</b>
Pre-Assessment Questions .....	7-2
TCP/IP Security Vulnerabilities .....	7-3
Implementing Security.....	7-3
Resources and Services.....	7-5
Protecting TCP/IP Services.....	7-6
Simple Mail Transfer Protocol (SMTP) .....	7-14
Testing and Evaluating .....	7-18
Implementing New Systems and Settings.....	7-18
Security Testing Software.....	7-19
Security and Repetition.....	7-25
Lesson 7 Review .....	7-31
<b>Lesson 8: Firewalls and Virtual Private Networks</b> .....	<b>8-1</b>
Pre-Assessment Questions .....	8-2

Access Control Overview .....	8-3
Definition and Description of a Firewall .....	8-3
The Role of a Firewall .....	8-4
Firewall Terminology .....	8-5
Firewall Configuration Defaults .....	8-12
Creating Packet Filter Rules .....	8-13
Packet Filter Advantages and Disadvantages .....	8-16
Configuring Proxy Servers .....	8-27
Remote Access and Virtual Private Networks (VPNs).....	8-33
Public Key Infrastructure (PKI).....	8-36
Lesson 8 Review .....	8-43
<b>Lesson 9: Levels of Firewall Protection .....</b>	<b>9-1</b>
Pre-Assessment Questions .....	9-2
Designing a Firewall .....	9-3
Types of Bastion Hosts .....	9-4
Hardware Issues .....	9-6
Common Firewall Designs .....	9-9
Putting It All Together .....	9-14
Lesson 9 Review .....	9-23
<b>Lesson 10: Detecting and Distracting Hackers .....</b>	<b>10-1</b>
Pre-Assessment Questions .....	10-2
Preparing for the Inevitable .....	10-3
Proactive Detection .....	10-3
Distracting the Hacker .....	10-5
Deterring the Hacker .....	10-10
Lesson 10 Review .....	10-15
<b>Lesson 11: Incident Response .....</b>	<b>11-1</b>
Pre-Assessment Questions .....	11-2
Planning for Response .....	11-3
Create a Response Policy .....	11-3
Decide Ahead of Time .....	11-3
Do Not Panic .....	11-4
Document Everything .....	11-4
Assess the Situation .....	11-5
Stop or Contain Activity .....	11-6
Execute the Response Plan .....	11-6
Analyze and Learn .....	11-8
Lesson 11 Review .....	11-11
<b>Appendixes.....</b>	<b>Appendixes-1</b>
<b>Glossary .....</b>	<b>Glossary-1</b>
<b>Index.....</b>	<b>Index-1</b>
<b>Supplemental CD-ROM Contents.....</b>	<b>Supplemental CD-ROM Contents-1</b>

## List of Labs

Lab 1-1: Causing a NetBus Trojan infection .....	1-5
Lab 2-1: Viewing and modifying default access control settings in Windows 2000 .....	2-27
Lab 2-2: Viewing the effects of hostile JavaScript in Netscape Navigator .....	2-30
Lab 2-3: Configuring execution control lists in Windows 2000 .....	2-32
Lab 2-4: Creating an Execution Control List for the su command in Linux .....	2-34
Lab 3-1: Reviewing symmetric encryption algorithms .....	3-12
Lab 3-2: Installing PGP 6.5.8 in Windows 2000 .....	3-25
Lab 3-3: Generating a key pair using PGP for Windows 2000 .....	3-26
Lab 3-4: Exporting and signing public keys using PGP for Windows 2000 .....	3-28
Lab 3-5: Exchanging encrypted messages using PGP for Windows 2000 .....	3-31
Lab 3-7: Encrypting files with PGP in Windows 2000 .....	3-32
Lab 4-1: Sending fake e-mail messages .....	4-11
Lab 5-1: Conducting a physical attack against a Windows 2000 server .....	5-11
Lab 6-1: Enabling TCP/IP filtering on Windows 2000 .....	6-20
Lab 7-1: Securing a Windows 2000 Web server .....	7-10
Lab 7-2: Securing the FTP service .....	7-13
Lab 7-3: Deploying simple network scanners .....	7-20
Lab 7-4: Scanning systems using Red Hat Linux .....	7-24
Lab 8-1: Installing WinRoute in Windows 2000 .....	8-17
Lab 8-2: Configuring packet filtering rules .....	8-18
Lab 8-3: Configuring a proxy server in Windows 2000 .....	8-30
Lab 9-1: Creating an internal network with WinRoute (instructor-led) .....	9-15
Lab 9-2: Establishing a packet filter (instructor-led) .....	9-17
Lab 9-3: Denying HTTP access (instructor-led) .....	9-20
Lab 9-4: Configuring an FTP packet-filtering rule for a specific host (instructor-led) .....	9-21
Lab 10-1: Setting a logon Tripwire script in Windows 2000 .....	10-7

## List of Figures

Figure i-1: Classroom configuration .....	xvii
Figure 1-1: NetBus Client interface .....	1-5
Figure 1-2: Client connected to loopback address .....	1-6
Figure 1-3: Remote file manager within NetBus .....	1-6
Figure 1-4: Removing NetBus Server .....	1-7
Figure 1-5: anticode.com Web site .....	1-9
Figure 2-1: Elements of effective security .....	2-3
Figure 2-2: Policy and technology .....	2-9
Figure 2-3: American Express Blue Web site .....	2-18
Figure 2-4: Windows 2000 Properties dialog box .....	2-27
Figure 2-5: Directory Permissions dialog box .....	2-28
Figure 2-6: Lockup.htm alert screen .....	2-31
Figure 2-7: Viewing Microsoft Management console settings .....	2-33
Figure 3-1: Symmetric or single-key encryption .....	3-5
Figure 3-2: RSA security home page .....	3-8
Figure 3-3: Apocalypso interface .....	3-12

Figure 3-4: Apocalypso – Rijndael Encryption dialog box .....	3-13
Figure 3-5: Encrypting information into cipher text, using public key .....	3-15
Figure 3-6: Asymmetric key encryption .....	3-22
Figure 3-7: Asymmetric key decryption .....	3-22
Figure 3-8: PGP home page .....	3-23
Figure 3-9: PGP passphrase dialog box .....	3-27
Figure 3-10: PGPkeys management client .....	3-28
Figure 3-11: Export Key to File dialog box .....	3-29
Figure 3-12: PGPTools dialog box .....	3-32
Figure 3-13: Netscape Messenger e-mail program .....	3-33
Figure 3-14: BestCrypt Web site .....	3-35
Figure 3-15: Asymmetrically encrypted information passed through network .....	3-36
Figure 3-16: Viewing Encrypted Data Recovery Agent for Windows 2000 system .....	3-40
Figure 6-1: OSI model .....	6-4
Figure 6-2: Establishing TCP connection .....	6-10
Figure 6-3: Terminating TCP connection .....	6-11
Figure 6-4: Securing DNS in Windows 2000 .....	6-18
Figure 6-5: TCP/IP Security dialog box .....	6-20
Figure 7-1: Default Web Site Properties .....	7-10
Figure 7-2: Altering Local Path window to change Web server root .....	7-11
Figure 7-3: FTP properties dialog box for IIS .....	7-13
Figure 7-4: Creating hidden share .....	7-20
Figure 7-5: Happy Browser scanning program .....	7-22
Figure 7-6: Winfingerprint interface .....	7-23
Figure 7-7: Completed Winfingerprint scan .....	7-23
Figure 7-8: Viewing permissions in C:\webfiles directory .....	7-26
Figure 7-9: Viewing custom permissions for C:\webfiles directory .....	7-27
Figure 7-10: Viewing object permission entries for C:\webfiles directory .....	7-28
Figure 7-11: Denying access to a particular IP address .....	7-29
Figure 8-1: Implementing NAT in network .....	8-9
Figure 8-2: Packet Filter dialog box .....	8-18
Figure 8-3: Add Item dialog box .....	8-19
Figure 8-4: Add Item box for ICMP .....	8-20
Figure 8-5: Proxy server configuration .....	8-27
Figure 8-6: Understanding VPN connection .....	8-33
Figure 9-1: Triple-homed bastion host .....	9-5
Figure 9-2: Packet filter configuration .....	9-10
Figure 9-3: Single-homed bastion configuration .....	9-11
Figure 9-4: Dual-homed bastion configuration .....	9-12
Figure 9-5: Screened subnet firewall .....	9-13
Figure 9-6: Open Configuration dialog box .....	9-15
Figure 9-7: Packet Filter dialog box .....	9-17
Figure 9-8: Add Item dialog box .....	9-18
Figure 9-9: Add Item dialog box for ICMP .....	9-18
Figure 9-10: Rule denying FTP access to single host caption .....	9-21
Figure 10-1: Creating logon tripwire script with Notepad .....	10-8

---

Figure 10-2: User environment profile dialog box .....	10-9
Figure 11-1: CERT home page .....	11-7

## List of Tables

Table 1-1: Effective security system attributes .....	1-11
Table 1-2: Hot spots and potential threats .....	1-13
Table 1-3: Security services .....	1-16
Table 2-1: Typical tri-level classification scheme .....	2-6
Table 2-2: Security education levels .....	2-12
Table 2-3: Reasons for encryption .....	2-14
Table 2-4: Computers and key-breaking ability .....	2-16
Table 2-5: Kerberos terms .....	2-23
Table 3-1: Security technology summary .....	3-38
Table 4-1: Virus types and descriptions .....	4-15
Table 5-1: Security management terminology .....	5-9
Table 6-1: ICMP message types .....	6-7
Table 7-1: Security implementation model .....	7-3
Table 8-1: Telnet packet filter .....	8-14
Table 8-2: Telnet packet filter—advanced rules .....	8-14
Table 8-3: FTP packet filter .....	8-15
Table 10-2: Tools for responding to attacks .....	10-12

---

## Course Description

---

*Network Security and Firewalls* teaches you how to secure your network from unauthorized activity. This course teaches you about security principles, such as establishing an effective security policy, and about the different types of hacker activities that you are most likely to encounter.

This course identifies security principles and techniques that enable you to stop a hacker by understanding how to implement access control lists, operating system hardening, and firewall technology. It also teaches you how to personalize your network security system so you can create a solution that adheres to universal principles, but also conforms to your business needs in responding to specific hacker attacks.

You will learn about authentication procedures, encryption standards and implementations that help ensure proper user authentication. You will also learn about the specific ports and protocols that hackers manipulate, and about direct and indirect ways to protect your network operating systems. Finally, you will learn how to respond to and report hacker activity, engage in proactive detection, and always keep your company's needs in mind. Appendixes are included in the back of this coursebook to provide resources for you as you continue to learn about applying security measures to your network.

---

### Length

---

*Network Security and Firewalls* is a twelve-hour course.

---

### Series

---

*Network Security and Firewalls* is the first course in the CIW Security Professional series. CIW Security Professional consists of the following three courses:

- *Network Security and Firewalls*
- Operating Systems Security
- Security Auditing, Attacks, and Threat Analysis

---

### Prerequisites

---

Students must have completed the CIW Foundations and CIW Internetworking Professional series or be able to demonstrate equivalent Internet knowledge.

# ProsoftTraining Courseware

This coursebook was developed for instructor-led training and will assist you during class. Along with comprehensive instructional text and objectives checklists, this coursebook provides easy-to-follow hands-on labs and a glossary of course-specific terms. It also provides Internet addresses needed to complete some labs, although due to the constantly changing nature of the Internet, some addresses may no longer be valid.

The student coursebook is organized in the following manner:

course title	
table of contents	
list of labs	
list of figures	
list of tables	
lessons	
lesson objectives	
pre-assessment questions	
narrative text	
<input checked="" type="checkbox"/> graphics	
<input checked="" type="checkbox"/> tables and figures	
<input checked="" type="checkbox"/> warnings	
<input checked="" type="checkbox"/> tech notes	
labs	
<input checked="" type="checkbox"/> graphics	
<input checked="" type="checkbox"/> tables and figures	
<input checked="" type="checkbox"/> warnings	
<input checked="" type="checkbox"/> tech notes	
lesson summary	
lesson review	
appendixes	
glossary	
index	
supplemental CD	

When you return to your home or office, you will find this coursebook to be a valuable resource for applying the skills you have learned. Each lesson concludes with questions that review the material. Lesson review questions are provided as a study resource only and in no way guarantee a passing score on CIW exams.

The course is available in either an academic or a learning center version, and each version has an instructor book and a student book. Check your book to verify that you have the correct version, and whether it is an instructor or a student book. Following is a brief description of each version.

- **Academic:** Designed for students in an academic classroom environment; typically taught over a quarter (10-week) or semester (16-week) time period. Example syllabi for both timeframes are included on the instructor CD-ROM. The instructor's book and CD-ROM contain all answers, as well as activities (pen-and-paper-based labs), optional labs (computer-based labs), quizzes, a course assessment, and handouts for the instructor to assign during class or as homework. No answers exist in the student book or on the student CD-ROM. Students must obtain answers from the instructor.
- **Learning Center:** Designed for students in a learning center classroom environment; typically taught over a one-day to five-day time period (depending on the length of the course). An example implementation table is included on the instructor CD-ROM. Similar to the academic version, the instructor's book and CD-ROM contain all answers, as well as activities (pen-and-paper-based labs), optional labs (computer-based labs), quizzes, a course assessment, and handouts for the instructor to assign during class or as homework. However, the student CD-ROM also contains answers, including those to the pre-assessment questions, labs, review questions, activities, optional labs, quizzes, and the course assessment.

## Course Objectives

---

After completing this class, you will be able to:

- Explain the need for network perimeter security, and identify the various elements of an effective security policy.
- Describe encryption, and identify the three main encryption methods used in internetworking.
- Describe the universal guidelines and principles for effective network security, and use those guidelines to create effective specific solutions.
- Consistently apply security principles, and identify a security attack.
- Identify firewall types, and discuss common firewall terminology.
- Plan a firewall system that incorporates several levels of protection.
- Deploy a network firewall.

## Classroom Setup

---

Your instructor has probably set up the classroom computers based on the system requirements listed below. Most software configurations on your computer are identical to those on your instructor's computer. However, your instructor may use additional software to demonstrate network interaction or related technologies.

### Security disclaimer

---

The code, examples, and techniques found in this course are provided for the purposes of teaching about security concepts. Never, under any circumstances, use any of the software or techniques discussed in this course against any local or remote system that is not your own. ProsoftTraining and its partners are not responsible or liable for illegal or unethical use of software or techniques discussed or used in this course.

# System Requirements

## Hardware

The following table summarizes the hardware requirements for all courses in the CIW program. Each classroom should be equipped with enough personal computers to accommodate each student and the instructor with his or her own system.

*Note: The CIW hardware requirements are similar to the lowest system requirements for Microsoft implementation (Level 1 requirements) except that CIW requires increased hard disk space (8 GB) and RAM (128 MB). This comparison may be helpful for the many training centers that implement CIW and are also CTEC because personnel at these centers are familiar with the Microsoft hardware specifications.*

CIW hardware specifications	Greater than or equal to the following
Processor	Intel Pentium II (or equivalent) personal computer with processor speed greater than or equal to 300 MHz
L2 cache	256 KB
Hard disk	8-GB hard drive
RAM	At least 128 MB
CD-ROM	32X
Network interface card (NIC)	10BaseT or 100BaseTX (10 or 100 Mbps)
Sound card/speakers	Required for instructor's station, optional for student stations
Video adapter	At least 4 MB
Monitor	15-inch monitor
Network hubs	Two 10-port 10BaseT or 100BaseTX (10 or 100 Mbps) hubs
Router	Multi-homed system with three NICs (Windows NT 4.0/2000 server)*

*\* Must meet universal CIW hardware requirements.*

## Software

---

The recommended software configurations for computers used to complete the labs in this book are as follows.

Software used in this course:

- Microsoft Windows 2000 with Microsoft IIS and Internet Explorer 5.0 or later.
- Microsoft Certificate Server (optional, for the IPsec labs in the appendix).
- PGP version 6.5.x ([www.pgp.com](http://www.pgp.com), or the International version, available at [www.pgpi.org](http://www.pgpi.org).)
- NetBus 1.7. Available at <http://ssl.prosofttraining.com/security/2nsf>.

and/or

- Red Hat Linux 7.x, full installation, with Gnu C and C++ compilers (gcc and g++), Gnu gpg, MD5sum, as well as Perl, FTP, SMTP and Apache Web server. Include the bash and the Korn shells. You can obtain the Korn Shell (pdksh) at [www.rpmfind.net](http://www.rpmfind.net).
- NTChangePass (also known as a Linux boot disk). Available on student disk.
- Netscape Communicator 4.x or higher, with e-mail client.
- Ipswitch Ping ProPack (Ping Pro, available at [www.ipswitch.com](http://www.ipswitch.com)).
- MDAemon e-mail server ([www.deerfield.com](http://www.deerfield.com)), which is necessary for students to send e-mail to each other. Any e-mail server will work for this class.
- Portscan and Plisten.exe ([ssl.prosofttraining.com/security/2nsf](http://ssl.prosofttraining.com/security/2nsf)).
- Happy Browser ([packetstorm.securify.com](http://packetstorm.securify.com) or [ssl.prosofttraining.com/security/2nsf](http://ssl.prosofttraining.com/security/2nsf)).
- WinFingerprint ([ssl.prosofttraining.com/security/2nsf](http://ssl.prosofttraining.com/security/2nsf)).

To be installed by students:

- Apocalypso (on student disk, or at [www.hacknet.com](http://www.hacknet.com)).
- Tripwire for Linux ([www.rpmfind.net](http://www.rpmfind.net) or [ssl.prosofttraining.com/security/1OSS](http://ssl.prosofttraining.com/security/1OSS)).
- iishack2000.c (available on student disk, or at [packetstorm.securify.com](http://packetstorm.securify.com)). This file is optional.
- bad.cgi ([ssl.prosofttraining.com/security/2nsf](http://ssl.prosofttraining.com/security/2nsf)).
- Net-fizz.exe, Winfingerprint, and Happy browser. All are available at <http://ssl.prosofttraining.com/security/2nsf>.
- Tribe Flood Network (TFN), available at [ssl.prosofttraining.com/2nsf](http://ssl.prosofttraining.com/2nsf).
- WinRoute 4.1. Available at [www.winroute.com](http://www.winroute.com).
- One floppy disk per student.

## Connectivity

Due to the sensitive nature of some of the programs used, this class takes place in a special network classroom, closed off from the rest of the company network and from the Internet. The classroom is configured by the instructor. The instructor's computer must be able to communicate with all student computers, acting as a router. TCP/IP is the network protocol used in the course.

### LAN requirements

The course is designed for use with at least three physical networks, connected by an IP router (which can be a multi-homed computer). Network A (192.168.3.0) students will use odd-numbered IP addresses. Network B (192.168.4.0) students will use even-numbered IP addresses. The instructor will use a third network with the network address 192.168.2.0. The subnet mask is 255.255.255.0. Classroom configuration is illustrated in Figure i-1.

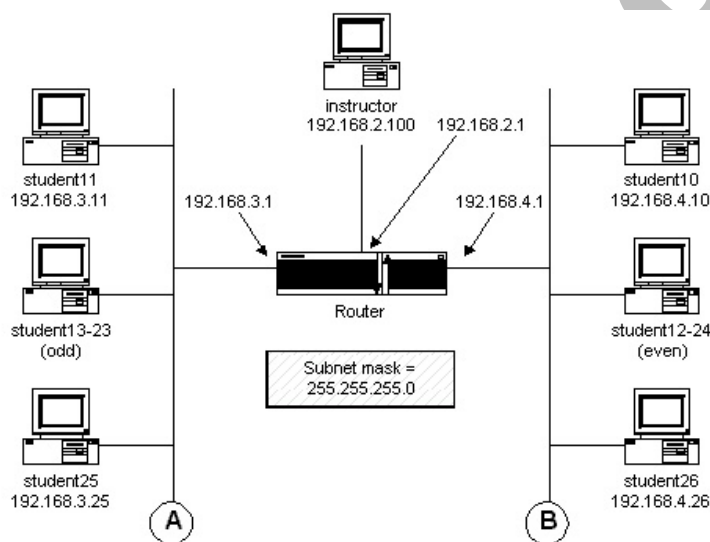


Figure i-1: Classroom configuration

Again, due to the sensitive nature of the information presented in this course, Internet connectivity is not recommended. TCP/IP is the only network protocol used in this course. The instructor will find specific instructions on how to configure the three subnets in the Instructor Guide.

The instructor's computer must be able to communicate with all the others through a router. The instructor can use a multi-homed Windows 2000 or Windows NT 4.0 Server computer as the router. If the instructor does not have a Windows system acting as a router, he or she can use whatever router is available.

## Conventions and Graphics Used in This Book

The following conventions are used in Prosoft coursebooks.

<b>Terms</b>	Technology terms defined in the margins are indicated in <b>bold</b> the first time they appear in the text. Not every word in bold is a term requiring definition.
<b>Lab Text</b>	Text that you enter in an lab appears in <b>bold</b> . Names of components that you access or change in an lab also appear in <b>bold</b> .
<b>Notations</b>	<i>Notations or comments regarding screenshots, labs or other text is indicated in italic type.</i>
<b>Program Code or Commands</b>	Text used in program code or operating system commands appears in the Lucida Sans Typewriter font.

The following graphics are used in Prosoft coursebooks.



*Tech Notes* point out exceptions or special circumstances that you may find when working with a particular procedure. Tech Notes that occur within a lab are displayed without the graphic.



*Tech Tips* offer special-interest information about the current subject.



*Warnings* alert you about cautions to observe or actions to avoid.



This graphic signals the start of a lab or other hands-on activity.



Each lesson summary includes an *Application Project*. This project is optional, and is designed to provoke interest and apply the skills taught in the lesson to your daily activities.



Each lesson concludes with a summary of the skills and objectives taught in that lesson. You can use the *Skills Review* checklist to evaluate what you have learned.



This graphic indicates a line of code that is completed on the following line.

# Lesson 1: What Is Security?

---

---

## ***Objectives***

By the end of this lesson, you will be able to:

- ↻ Define security.
- ↻ Explain the need for network security.
- ↻ Identify resources that need security.
- ↻ Identify the two general security threat types.
- ↻ List security standards and organizations.

## Pre-Assessment Questions

---

1. What is the name of a series of documents and procedures developed by an international consortium to serve as an international security standard?
    - a. British Standard 7799.
    - b. The Common Criteria.
    - c. The Orange Book.
    - d. A security matrix.
  
  2. Patrick is viewing the `/var/log/messages` file to search for attacks. In regards to security, what does this file provide?
    - a. Threat identification.
    - b. Risk analysis.
    - c. An audit trail
    - d. Event detection.
  
  3. To what kinds of attacks are network resources most vulnerable?
-

## Network Security Background

### hacker

Someone who illegally penetrates a computer network to access and manipulate data. Many networking professionals make the distinction between "white hat" (i.e., "good guy") hackers, and "black hat" hackers (sometimes called "crackers").

The media frequently relate sensational incidents concerning Internet-related security threats. From security problems with the popular Netscape Navigator and Microsoft Internet Explorer browser programs to sophisticated attacks aimed at compromising e-commerce servers, computer and network administrators and users must contend with an increasingly complex security environment. Attacks by **hackers**, which include computer and e-mail viruses, have become increasingly common. Major online businesses have also proved vulnerable. Amazon.com and eBay, for example, have been victims of serious attacks.

Well-known hackers include Kevin Mitnick and John Draper (who is also known as Captain Crunch), but many more unknown hackers can wreak havoc across the Internet. Even though the following news story reads like an excerpt from a spy novel, it actually did occur:

### Security Headlines

News Item: March 22, 1997--*San Jose Mercury News*

A master spy believed by the Pentagon to be the No. 1 threat to U.S. security and deadlier (yes, deadlier!) than the KGB turned out to be a 16-year-old British music student hacker working out of his bedroom. The U.S. Senate Arms Committee was told that the FBI feared an east European spy ring had gotten our innermost secrets including the U.S. Air Defense Systems ballistic missile design.

The schoolboy, who was known as the "Datastream cowboy" in the Internet world, was fined \$1,915. "These places were a lot easier to get into than university computers in England," explained the boy.

The age of the preceding article is important. Consider that systems and software applications have become even more powerful and available. Also, now that the business community has embraced the Internet for commerce, communication and collaboration, the integrity of sensitive information and lines of communication becomes an all-important concern. Responding to and countering threats such as viruses and hackers is an important part of any network administrator's job.

### open network

A group of servers and computers, such as the Internet, which allows free access.

The Internet is available to anyone with a network connection and an Internet Service Provider (ISP) account. In fact, it was designed to be an **open network**, and therefore has little built-in capacity for securing information. From a security standpoint, the Internet is inherently insecure. However, businesses and individuals now want to apply principles of security to the Internet, effectively using it in a way its inventors did not intend. For Internet users, the new challenge is to protect sensitive data while allowing authorized personnel to use it.

This course will introduce you to information security principles and teach you how to protect your systems from unauthorized access using the latest available technology. You will learn to deploy host-based solutions, along with network-based technologies, such as firewalls.

## What Is Security?

Put simply, security in a networking environment is the ability to identify and eliminate threats and vulnerabilities. A general definition of security must also address the need to safeguard organizational assets, including information and physical items, such as the computers themselves. The idea of security is also intertwined with the notions of appropriateness and subordination. A specific person must be designated as the security manager. This person will be in charge of security, and must determine who can take appropriate actions on specific items and when. All people who enforce security on the network must act in roles subordinate to this leader. Regarding company security, what is appropriate varies greatly from organization to organization, but any company with a network must have a security policy that addresses appropriateness, subordination and physical security.

**network perimeter**  
The outer limit of a network as defined by a firewall.

This course discusses security as it relates to the Internet. With the advent of modern, sophisticated technologies such as Local Area Networks (LAN), Wide Area Networks (WAN), the Internet, and Virtual Private Networks (VPN), the idea and practice of security have become somewhat more complex than simply patrolling the **network perimeter**. With regard to networking, one could define security as a continuing process in which an administrator ensures that information is shared only among authorized users.

By the end of this course, you will be familiar with the processes and technologies used to establish and limit behavior to what your organization considers appropriate. You will focus on the aspects of security that relate to connecting your organization to the Internet. Internet connectivity makes it extremely easy for unknown users to connect to exposed resources. You need to ensure that users can access only what you want them to access. This course will explore methods of controlling user and hacker access, and responding to events and minimizing damage when someone circumvents those controls.

**illicit server**  
A service or daemon installed on a host that thwarts authentication by allowing remote users to avoid the password database.

The following lab gives an example of how a hacker can remotely control a vulnerable system through the use of an **illicit server**. Although many hackers do not engage in such activities, you must understand that such practices can victimize an unsecured network.



### Lab 1-1: Causing a NetBus Trojan infection

In this lab, you will install NetBus and infect your machine with the NetBus server Trojan program. NetBus is an example of a Trojan that illustrates how your machine can be remotely controlled across the Internet. NetBus is often sent via an e-mail message, in hopes that an unsuspecting user will run the patch.exe program.

1. Obtain the NetBus files from your instructor, uncompress them using WinZip, if necessary, and double-click **Patch.exe**.

*Note: You have just infected your computer with the NetBus server software.*

2. Double-click **NetBus.exe**. Your screen should resemble Figure 1-1.

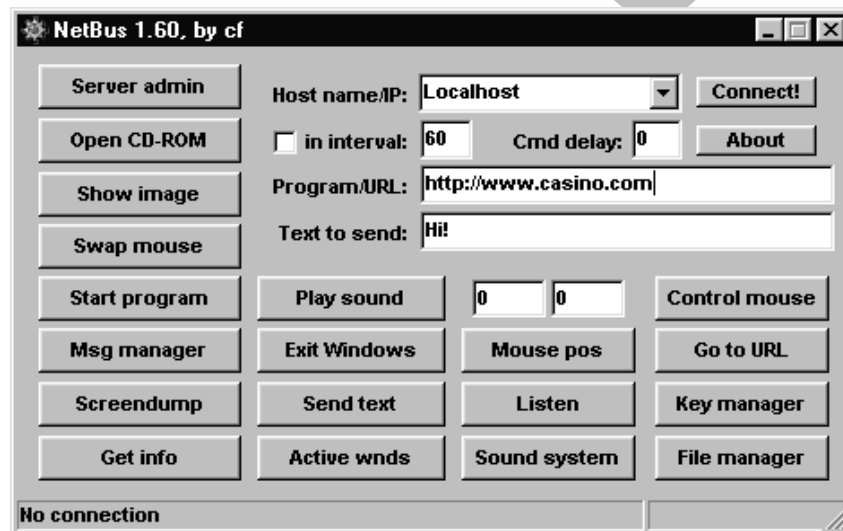


Figure 1-1: NetBus Client interface

3. In the NetBus interface, insert **127.0.0.1** into the **Host name/IP** field, then click **Connect!** Your screen should resemble Figure 1-2.

*Note: This is the loopback address to your system and allows you to use the client interface on yourself.*

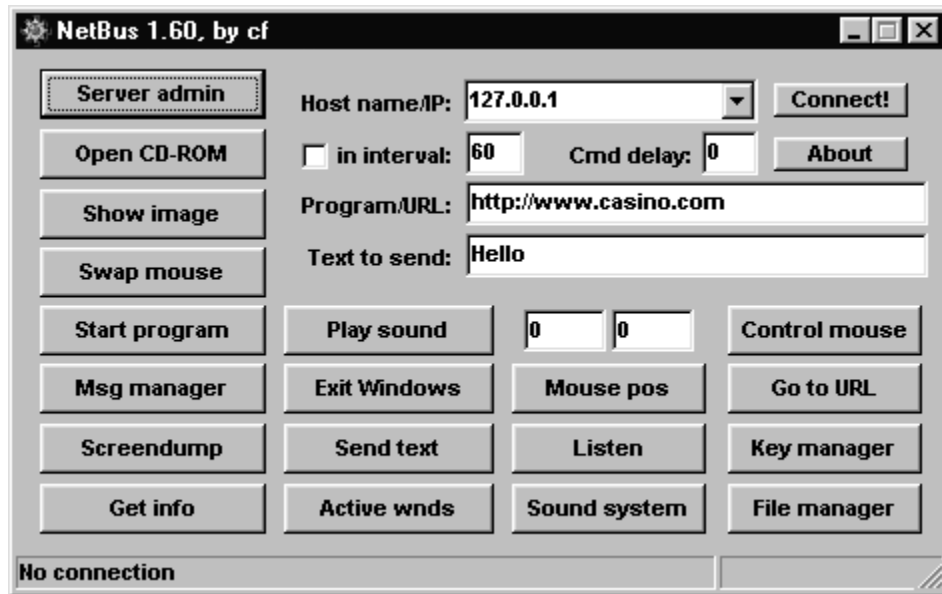


Figure 1-2: Client connected to loopback address

4. Click **File Manager: Show Files**. Here you can download, upload or delete files. Do not delete files at this screen. (See Figure 1-3). Click **Close**.



Figure 1-3: Remote file manager within NetBus

5. Click **Server admin: Remove server**. This action will remove the NetBus server from your system. (See Figure 1-4.) Close the NetBus Client.

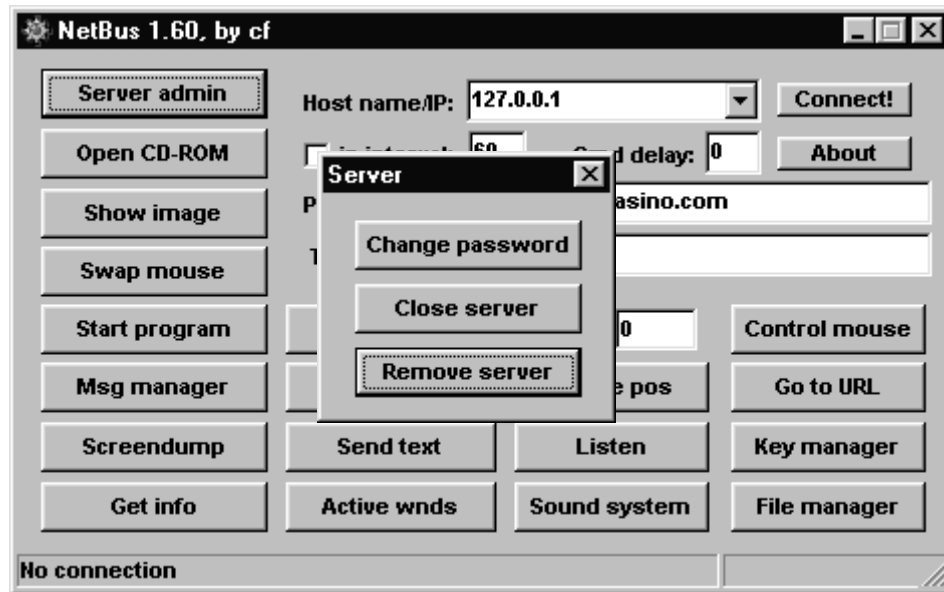


Figure 1-4: Removing NetBus Server

*Note: To remove NetBus, completely remove the file and make an adjustment to the Registry. This procedure is not included in this course.*

If time allows, the instructor will lead an lab in which you will connect to a remote host.

*Note: Connecting to a remote system without permission is illegal. This lab is presented for informational purposes only.*

Now, consider how you can protect your network hosts from this threat. Anti-virus applications generally find NetBus, but variants of NetBus that avoid detection do exist. Intrusion detection, which is the use of internal network hosts to detect and track network transmissions, is another method. For your network, however, the first line of defense against avoid remote NetBus use is to implement a firewall.

## Hacker Statistics

---

### Computer Emergency Response Team (CERT)

An organization devoted to dealing with computer-related security issues. Based out of Carnegie Mellon University, in Pittsburgh, Pennsylvania, CERT is a part of the Internet Society, which establishes the protocols that govern the Internet.

In spite of the romantic representations of hackers in movies such as *Sneakers*, *Hackers* and *War Games*, hacker activity is proving to be costly. According to the Computer Security Institute and **Computer Emergency Response Team (CERT)**, hacking is on the rise and is becoming increasingly destructive. CERT has provided the following statistics to show the effects of hacker activity. Its Web site ([www.cert.org/stats](http://www.cert.org/stats)) has released the following statistics concerning the increase of reported attacks:

- Reported incidents have risen steadily, from 252 in 1990 to 9,859 in 1999.
- In 2000 alone, losses due to security breaches were estimated at U.S. \$12 billion annually.
- In 2000, 21,756 incidents were reported, and more than 774 specific vulnerabilities were listed, affecting more than 9,350,000 hosts on the Internet.

Yet, according to a February 2001 *Information Security Magazine* article, it is estimated that about 90 percent of the attacks that occur every year are not reported (Richard Clarke, interviewed by Richard Thieme in *Information Security Magazine* Volume 4, number 2, page 62, February 2001). You can read the article at [http://www.infosecuritamag.com/articles/february01/features\\_q&a.shtml](http://www.infosecuritamag.com/articles/february01/features_q&a.shtml).

This last statistic suggests that most surveys reveal only part of the problem. For example, according to a 2001 survey of IT professionals conducted by *Information Security Magazine* ([www.infosecuritamag.com](http://www.infosecuritamag.com)), 52 percent of respondents said they had experienced some form of attack, intrusion or leakage of proprietary information in the previous 12 months. The majority of attacks were conducted not from outside, but from employees based inside the network.

- The IT community has responded to such attacks. Most companies have created security policies. Businesses, organizations and e-commerce sites now implement firewalls, intrusion detection systems and programs to help track network activity. You will learn more about some of these solutions in this course.

## The System Administration, Networking, and Security (SANS) Institute

---

The System Administration, Networking, and Security (SANS) institute is dedicated to providing advice and information concerning common systems vulnerabilities. Among other things, The SANS home page ([www.sans.org](http://www.sans.org)) provides a helpful "top 20" list to help administrators remain aware of the most important security vulnerabilities.

## What Is the Risk?

Gathering statistics is always an imperfect art, and the exact meaning of the statistics gathered by various "experts" is always open to some question. However, consider the site pictured in Figure 1-5.



Figure 1-5: anticode.com Web site

This site is quite popular among new, less talented hackers (often called "script kiddies"). It is just one of many that provide readily available resources for new Internet users to:

- Gain fairly accurate advice on how to begin hacking.
- Scan networks to determine what targets to attack.
- Attack e-mail, Web, database and file servers with false information to either compromise their security or bring them down.
- Crash and penetrate routers and additional network connectivity equipment.
- Defeat and crack authentication and encryption schemes.

Guarding against attacks is difficult unless you know how to categorize the attacks and counter them systematically. Still, to entirely secure your systems is impossible.

## The Myth of 100-Percent Security

---

Connectivity implies risk. If you allow legitimate users to access your computers or networks, the opportunity exists for abuse. One popular saying is that the only secure computer is one that has been disconnected from the network, shut off and locked in a safe with the key thrown away. Although this solution might make the computer secure, it also makes the computer useless. However, although you can never reach a point of complete security, you can achieve a level that prevents all but the most determined and skilled hackers from accessing your system. Proper security techniques can minimize the negative effects of hacker activity on your organization. They can deter even the most determined hacker. Regarding Internet security, you can usually restrict the network permissions of legitimate users so they can still accomplish their tasks, but have no more access than necessary. The result of this simple measure is that even if a hacker can steal a legitimate user's identity and enter into the system, he or she will be able to gain only the level of access authorized for that user. Such a restriction will confine any possible damage that the hacker may cause using the stolen user name and password.

### Security as balance

---

A key security principle is to use solutions that are effective, but that do not improperly burden legitimate users who want access to needed information. Finding ways to actually apply this principle is often a difficult balancing act. This need for balance applies especially to Internet security. It is quite easy to employ security techniques that become so onerous that legitimate users disregard and even circumvent your security protocols. Hackers are always ready to capitalize on such seemingly innocent activity. Thus, having an overzealous security policy could result in less effective security than if you had no security policy at all.

You always need to consider the effect that your security policy will have on legitimate users. In most cases, if the effort required by your users is greater than the resulting increase in security, your policy will actually reduce your company's effective level of security.

## Attributes of an Effective Security Matrix

### security matrix

All components used by a company to provide a security strategy. Includes hardware, software, employee training, security policy, etc.

Although the components and configurations of a security system vary from company to company, several characteristics remain constant. A reliable **security matrix** is necessary to ensure that all security measures are cost effective and reasonable. A security matrix is composed of individual operating system security features, logging services and additional equipment including firewalls, intrusion detection systems and auditing schemes.

Table 1-1 summarizes the most important aspects of an effective security system.

Table 1-1: Effective security system attributes

Attribute	Description
<b>Allows access control</b>	<ul style="list-style-type: none"> <li>You have achieved your goal of allowing access to only legitimate users.</li> <li>You have maximized the ability to communicate while minimizing the possibility of hacker access.</li> <li>You have minimized the possibility for damage in the event of hacker access.</li> </ul>
<b>Easy to use</b>	<ul style="list-style-type: none"> <li>If a security system is difficult to use, many employees will find ways to circumvent it.</li> <li>You have ensured that the interface is intuitive.</li> </ul>
<b>Appropriate cost of ownership</b>	<ul style="list-style-type: none"> <li>You have considered not only the initial purchase cost, but also the price of upgrades and service.</li> <li>You have also considered the cost of administration. How many employees, at what skill level, are necessary to successfully implement and maintain the system?</li> </ul>
<b>Flexible and scalable</b>	<ul style="list-style-type: none"> <li>Your system allows your company to do business the way it wants to.</li> <li>Your system will grow as the company grows.</li> </ul>
<b>Superior alarming and reporting</b>	<ul style="list-style-type: none"> <li>In the event of a security breach, your system notifies the administrator quickly and in sufficient detail.</li> <li>You have configured the system to alert you as efficiently as possible. Notification options include alerts by e-mail, computer screens, pagers and so forth.</li> </ul>

## What You Are Trying to Protect

---

Now that you have learned about the general principles involved in a security system, it is time to discuss exactly what needs protection. As you construct the security profile for your network, it is helpful to classify your assets into four resource groups:

- End-user resources (Windows 98/Me/2000, Linux or Macintosh hosts used by employees).
- Network resources (routers, switches, wiring closets, telephony).
- Server resources (including file, DNS, Web, FTP and e-mail servers).
- Information-storage resources (including human resources and e-commerce databases).

### End-user resources

---

Be sure you have enabled the members of your organization to protect their workstations. Not all damage to your resources is the result of malicious user activity, nor of hacker entry into your system. Often, computers are damaged by simple user error.

#### **Trojan**

A program disguised as a directory, archive or game that, when downloaded to a system, has an alternative, damaging motive. Many times, illicit servers, such as NetBus, are made into Trojans that end users unwittingly install on their systems.

For example, many employees are largely unaware of the hazards involved in downloading ActiveX files and using Java applets. Still others have not enabled password-protected screen savers to prevent snooping while they are out of the office for even short periods of time. Users can also inadvertently download viruses and **Trojans**, thereby compromising your network's ability to function. A Trojan is a file or program that purports to operate in a legitimate way, but which also has an alternative, secret operation, such as sending sensitive company information to a hacker via e-mail.

However, employees can improve security by making sure their browsers are configured for maximum security settings for ActiveX and Java. You should also make sure that each employee uses a virus checker and observes caution when downloading anything from the Internet.

Protecting local resources is largely a matter of educating individual users about easily applied security techniques. However, Internet security involves more than protecting individual resources.

**system snooping**

The action of a hacker who enters a computer network and begins mapping the contents of the system.

**Transmission Control Protocol/Internet Protocol (TCP/IP)**

A suite of protocols that turns information into blocks of information called packets. These are then sent across networks such as the Internet.

## Network resources

---

Your networks are the primary communications medium for the entire company. If a skilled hacker gains access to or control of your networks, he or she will probably gain access to all or most company data. You must be aware that many hackers can imitate any Internet Protocol (IP) device that has an Internet Protocol address. Called IP spoofing, this activity allows hackers to gain access to engage in various activities with impunity, because it helps them thwart detection via audit trails. Because no inherent protection is available in version four of the **Transmission Control Protocol/Internet Protocol (TCP/IP)**, a hacker can take advantage of any device that does not have specific mechanisms in place. As a result, users can take control of network resources and then move on to **system snooping**.

## Server resources

---

Your World Wide Web, e-mail and FTP servers are vulnerable to attacks designed to crash the server so that its services are unavailable, or attacks designed to allow the hacker to log on and obtain or alter information. Many times, server resources become a target because compromising one of these resources often allows hackers to move on to controlling other resources. Some servers provide backbone services (e.g., DNS), whereas others provide mission-critical services (e.g., Web, e-mail and so forth). Regardless of category, it is vital that you find ways to protect each as much as resources allow.

## Information-storage resources

---

The most vital function of any company is how it organizes and disseminates information. These server types represent a hacker's ultimate goal, because these databases contain sensitive information (e.g., credit card numbers, employee payroll records and so forth). Hackers want information for many reasons. Some are merely curious, and others are malicious. Still others wish to engage in industrial espionage. Table 1-2 lists potentially vulnerable parts of a network.

Table 1-2: Hot spots and potential threats

Hot spot	Potential threat
<b>End-user resources</b>	Viruses, trojans and applets can damage local systems. End users can also introduce problems through illicit activity.
<b>Network resources</b>	IP spoofing, system snooping and obtaining information.
<b>Server resources</b>	Unauthorized entry, interrupted service and Trojans. Server resources are the primary target in most cases.
<b>Database and information resources</b>	Obtaining trade secrets, customer data and so forth.

## Who Is the Threat?

---

Popular culture often represents the hacker as a brilliant, underachieving adolescent male who has a problem with authority. Although this description is sometimes accurate, categorizing hackers in terms of their attitude and motivation is probably more useful.

Malicious activity occurs for a number of reasons. However, such activity typically falls into three broad categories. Perhaps the most important thing to consider when determining your company's security is to identify the type of hacker who will target your company and to anticipate that hacker's attitude. The three categories are the casual attacker, the determined attacker and the spy.

### Casual attackers

---

The casual attacker is sometimes an information seeker, but most often he or she is a thrill seeker. The casual attacker has what might be called an "Everest mentality." In other words, the casual attacker is hacking into your system simply "because it is there." The vast majority of hackers fall into this category. They can be stopped with the proper application of security, especially if this security policy specifies that you find and respond to the hacker. Some casual attackers are teenage pranksters with access to a phone line. A large underground network of these attackers exists.

### Determined attackers

---

The determined hacker will gain access to your system, regardless of difficulty or consequence. This type of hacker is going to get in via the Internet, or by manipulating a careless or uninformed employee. These hackers have access to tested methods and tools specifically designed to allow access into your network. In spite of your effective equipment and clear security policy, this type of hacker's determination and willingness to employ any method will eventually lead him or her to success.

Determined hackers will often break into highly sophisticated systems to prove their hacking prowess. Typically, these hackers are not out to destroy information, but will often obtain information about your company and network just because they can. Determined hackers have many motivations. One hacker might be a disgruntled employee, whereas another might be motivated by resentment toward large businesses or governments. Many attacks have occurred as the result of hackers' interest in removing the presence of what they consider to be objectionable or controversial content. Still others—the majority, perhaps—are motivated by financial gain.

**Web graffiti**

The act of defacing a Web site by replacing authorized content with illicit information.

Other hackers have more idiosyncratic motivations, which can be based upon an interest in achieving fame, a need to gain a sense of accomplishment, or a need to demonstrate their networking skills. Such motives may explain the majority of **Web graffiti** that has occurred over the past few years.

**Spies and industrial espionage**

Spies have very specific targets and want to gain information or disrupt service. They are well funded and have nearly unlimited access to resources. Primary motivations for spies include monetary gain and ideological beliefs. These hackers will stop at nothing to gain access to the networks they have targeted. Businesses interested in industrial espionage and various governments often fund spy groups, but some spies are mercenaries who will work for the highest bidder.

**auditing**

Reading and interpreting log files to identify hacker activity.

Later lessons discuss how to implement firewalls and offer specific ways to defend against hackers. For stopping a determined hacker, **auditing** is the most effective tool. With proper auditing, you will discover and stop a hacker as soon as possible. A more detailed discussion of auditing is presented in a later lesson, and another lesson offers a plan by which you might respond to the hacker and report such activity. Sometimes you need to contact law enforcement agencies, such as local authorities or possibly the U.S. Federal Bureau of Investigation (FBI).

## Security Standards

---

To complete our discussion of security basics, we must mention several standards that exist to help provide security.

The International Organization for Standardization (ISO) 7498-2 *Security Architecture* document defines security as minimizing the vulnerabilities of assets and resources. An asset is defined as anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential security violation.

ISO further classifies threats as either accidental or intentional, and active or passive. Accidental threats are those that exist with no premeditated intent. Such threats as natural disasters and system malfunctions fall within this group.

Intentional threats may range from casual examination of computer or network data to sophisticated attacks using special system knowledge. Passive threats do not modify information contained in the systems; neither the operation nor the state of the system is changed. Alteration of information or changes to the system's state or operation is considered an active threat to the system.

## Security services

The ISO 7498-2 document further defines several security services, as summarized in Table 1-3. These services will be examined in more detail in upcoming lessons.

Table 1-3: Security services

Service	Purpose
<b>Authentication</b>	The process of proving identity. These services provide for the authentication of a communications peer entity and the source of data (origin).
<b>Access control</b>	Determines what system resources a user or service may use, view or change. After a user has been authenticated, the access control service on an operating system determines where that authenticated user can go.
<b>Data confidentiality</b>	Protects data from unauthorized disclosure. Data confidentiality protects from passive threats, which include users who read data from the network wire using packet sniffers.
<b>Data integrity</b>	Data integrity services protect against active threats (such as altering data) by verifying or maintaining the consistency of information.
<b>Non-repudiation</b>	Repudiation is the ability to deny participation in all or part of a transaction. For networking, one can repudiate an e-mail message or a piece of data, such as a traceroute ping packet or SYN packet, by saying "I did not send that." Non-repudiation services allow all parties to provide proof of origin and/or proof of delivery concerning any service, process or piece of information.

## Security mechanisms

According to ISO, a security mechanism is a technology, a piece of software or a procedure that implements one or more security services. ISO classifies mechanisms as either specific or pervasive. A specific security mechanism is a technology or piece of software that implements only one security service at a time. Encryption is an example of a specific security mechanism. Although you can use encryption to ensure data confidentiality, data integrity and non-repudiation (all services), the actual encryption technique you use requires different encryption techniques (i.e., mechanisms) to implement each service.



You will learn more about the different uses of encryption throughout this course.

A general security mechanism lists procedures that help implement one or more of the security services at a time. Another element that differentiates general security mechanisms from specific mechanisms is that general mechanisms do not apply to any one layer of the OSI/RM. Examples of pervasive mechanisms include the following.

- **Trusted functionality:** Any procedure that strengthens an existing mechanism. For example, when you update the TCP/IP stack or run some software to strengthen the ability of your Novell, NT or UNIX system to authenticate, you are using a pervasive mechanism.
- **Event detection:** The ability to detect and report local and remote incidents.
- **Audit trail:** Any mechanism that allows you to monitor and document your network's activities.
- **Security recovery:** The ability to react to an event, including creating short-term and long-term solutions to known vulnerabilities. Also includes the ability to repair damaged systems.

### ***Additional security standards***

Many other government and industry standards exist in addition to ISO 7498-2. A selected list includes:

- **British Standard 7799:** Outlines specific "controls," such as the system access control, the use of a security policy and physical security measures. Designed to help managers and IT professionals create procedures to keep information secure.
- **The Common Criteria:** A series of documents and procedures developed by an international consortium. Parties that created the Common Criteria include the Communications-electronics Security Group (Great Britain), the National Institute of Standards and Technology (United States) the Communications Security Establishment Organization (Canada), and the Service Central de la Securite des Systemes d'Information (France).
- **The Orange Book (United States).**

## **The Orange Book**

In an attempt to standardize levels of security, the U.S. government released a series of standards defining a common set of security levels. These standards were released in a series of books commonly called the "Rainbow Series" because each book had a different color cover. The "Orange Book" has been of particular importance to security professionals, even despite some problems. It defines a series of standards, which begin with D (the lowest level) and continue through A1 (the most secure). Unfortunately these standards have suffered from several deficiencies. The first problem is that the Orange Book has tried to be too comprehensive in its standards. This meant that official adoption of the Orange Book standards resulted in an inordinate amount of work for the resulting level of security. Additionally, many companies have found that the Orange Book standards do not address the specific business needs for having a network in the first place, which can lead to serious problems between the IT department and the rest of the company.

Another problem has been the fact that the Orange Book has fallen out of favor with many in the networking industry. As with anything in computer networking, changes in capabilities create gaps that become more significant over time. This issue, coupled with the fact that the standards were designed specifically for government entities, has caused the NSA and NIST agencies to jointly release a new series of standards called Trust Technology Assessment Program (TTAP). TTAP defines seven security levels, beginning with Evaluation Assurance Level (EAL) 1 (lowest) and continuing through EAL 7 (the most secure). To also combat problems of long delays in evaluation, the NSA and NIST are also certifying third parties to conduct evaluations. Although still in its early development, TTAP shows promise of helping in industry-wide security standardization.

As a result, several security standards are in place. Some have argued that some of these standards, such as the Orange Book codes, are no longer used, which is not necessarily true. Although some standards may be falling out of favor in certain security circles, you will find that an awareness of past and present standards is useful, because some companies still apply standards from the Orange Book.

---

## Lesson Summary



### Application project

---

In this lesson, you have learned about specific risks to your systems, as well as some of the standards used to measure network security. Each organization has different security concerns. Compile a list of potential security threats to your organization. Determine which of the four elements of security can most effectively provide a countermeasure to your potential security problems:

1. Answers will vary.
2. Answers will vary.
3. Answers will vary.
4. Answers will vary.



### Skills review

---

In this lesson, you were introduced to the concept of security, and you saw demonstrations of several security threats. You also learned about the categories of resources that need protection, the attributes of an effective security system, and the types of people who make security systems necessary.

Now that you have completed this lesson, you should be able to:

- ✓ Define security.
  - ✓ Explain the need for network security.
  - ✓ Identify resources that need security.
  - ✓ Identify the two general security threat types.
  - ✓ List security standards and organizations.
-

## Lesson 1 Review

---

1. What is an open network?

---

---

---

---

---

2. The advent of sophisticated networking technologies has required network protection to become more sophisticated than simply patrolling the network perimeter. Give an example of an attack that could allow a computer to be controlled remotely.

---

---

3. What is the Computer Emergency Response Team (CERT)?

---

---

---

---

4. What are the components of an effective security matrix?

---

---

5. To what kinds of attacks are server resources most vulnerable?

---