Installation and Getting Started

NetRecon™

Version 2.0

The information in this document is subject to change without notice and must not be construed as a commitment on the part of AXENT Technologies. AXENT Technologies assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such a license.

No part of this documentation may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means—graphic, electronic, or mechanical, including photocopying and recording—without the prior written permission of the copyright owner.

© 1998, by AXENT Technologies, Inc.

All rights reserved.

Printed in the United States of America.

CONFIDENTIAL AND PROPRIETARY INFORMATION OF AXENT TECHNOLOGIES, INC.

Additional copies of this document or of other AXENT Technologies publications may be ordered from your authorized distributor or directly from

AXENT Technologies, Inc.
796 East Utah Valley Drive, Suite 200
American Fork, Utah 84003
Phone: (801)224-5306 Fax: (801)227-3791
World Wide Web: http://www.axent.com

Trademarks

AXENT Technologies is a registered trademark of AXENT Technologies, Inc.; NetRecon and the AXENT logo are trademarks of the same company registered in the United States of America and certain other countries. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other brands and product names are trademarks, or registered trademarks, of their respective companies.

Revised September 1998

Contents

Installation 1-1
- System Requirements 1-1
- Installation 1-2

License Key and Serial Number 2-1
- Entering a License Key and Serial Number 2-1
- Creating or Changing a Password 2-4
- Demo Mode 2-4

NetRecon Features 3-1
- Overview 3-1
- Program Window 3-2
- Scanning 3-4
- Reports 3-6
- UltraScan 3-8

Documentation 4-1
- Online Help 4-1
- Objective and Vulnerability Descriptions 4-5

Installation

This chapter includes the NetRecon system requirements and instructions for installing NetRecon.

System Requirements

In order to run NetRecon, your system must meet the following minimum system requirements:

- Windows NT 4.0 (Workstation or Server)
- 32 MB RAM
- 12 MB disk space

Installation

How you install NetRecon depends on whether you are installing from a CD, or downloaded the NetRecon installation program from the Internet.

Follow the instructions below that apply to your media type.

Installation Notes

- The Start menu shortcut to the NetRecon program is installed in the Window NT personal profile that is active when the software is installed. Therefore, before installing NetRecon, be sure to log in to the system using the account you plan to use when performing NetRecon scans.
- The account you plan to use for installing and using NetRecon should have administrative access to the system where NetRecon is being installed.

Installing from a CD

To install NetRecon from a CD:

1. Insert the NetRecon CD into your CD-ROM drive.

   The NetRecon CD has an autorun program that should start when your system reads the CD.

2. Click Install.
3. Follow the on-screen instructions for the NetRecon installation program.

If the autorun feature does not work correctly on your system, you can install NetRecon from a CD using the following steps:

1. Insert the NetRecon CD into your CD-ROM drive.
2. From the Windows Start menu, choose Run.

3. Type D:\nrinstall.exe.

   If your CD-ROM has a drive letter other than D, replace D with the that drive letter.

4. Click OK.
5. Click Install.
6. Follow the on-screen instructions for the NetRecon installation program.

Installing from the Internet

To install from the Internet, you must first download the NetRecon installation program from the AXENT Web site. For more information, go to *http://www.axent.com/netrecon/*. The installation program file is a self-extracting executable named *netrecon.exe*.

To install using a NetRecon installation program file you have downloaded from the Internet:

1. From the Windows Explorer, double-click the NetRecon installation program file.
2. Follow the on-screen instructions for the NetRecon installation program.

1.4 Installation

License Key and Serial Number

Before you can perform live NetRecon scans (i.e. scans of actual network resources), you must enter a license key and serial number in NetRecon. If you do not enter these, NetRecon runs only in Demo Mode.

This chapter describes how to enter a license key and serial number, how to enter or change a password, and how NetRecon Demo Mode works.

Entering a License Key and Serial Number

If you do not already have a license key and serial number, see *Obtaining a License Key and Serial Number* in the *Release Notes.*

First Time Execution of NetRecon

When NetRecon is run, and no license key and serial number have been entered previously, the following dialog box appears:

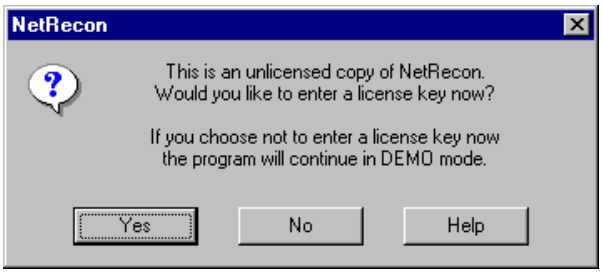


Figure 2-1: Unlicensed Copy of NetRecon

Click Yes if you have the license key and serial number. If you do not, click No, which allows you to run the program in Demo Mode (see *Demo Mode* at the end of this chapter).

If you click Yes, a dialog box appears (see Figure 2-2) to let you enter your company name and a license key, serial number, and license type.

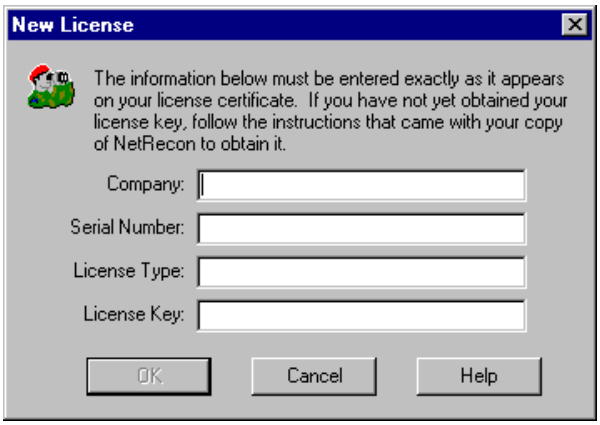


Figure 2-2: Entering a license key and serial number.

Changing a License Key

If you have previously entered a license key and serial number, but now have a new license (for example, if you previously had an Evaluation license, but have since purchased an Unlimited license), you can change the existing license information.

To change your existing license information:

1. Open NetRecon.
2. Choose Administration, Enter License Key.

   The dialog box shown in Figure 2-3 appears to let you enter the new license information.

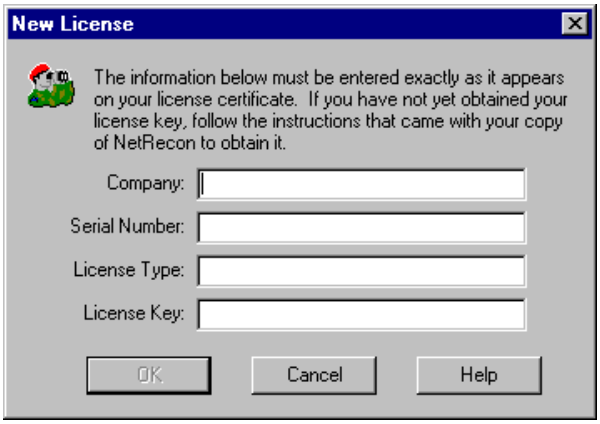


Figure 2-3: Entering a license key and serial number.

The license type is included with your license key.

Creating or Changing a Password

New License

Immediately after entering new license information, the program always asks you to specify a password. The password ensures that only authorized personnel can perform NetRecon scans. You are asked to enter the password twice to protect against making typographical errors.

Changing an Existing Password

You can change an existing password any time.

To change a password:

1. Choose Administration, Change Password.
2. Type the old password and the new password in the appropriate text boxes.
3. Click OK.

Demo Mode

Even if you do not enter a license key and serial number, you can still run NetRecon in Demo Mode. Running a scan while in Demo Mode causes NetRecon to produce simulated scan data. You can use this simulated data to see how NetRecon's features work. For example, you can still manipulate the data in the Data Table pane, or create and view reports. You cannot scan any real networks or network resources while NetRecon is running in Demo Mode.

Chapter 3

NetRecon Features

This chapter describes some of NetRecon's key features.

Overview

NetRecon is a network vulnerability detection system. It allows a security administrator to scan networks to discover their security vulnerabilities. NetRecon combines ordinary testing and information gathering tools available in most networks with specialized system-cracking tools. NetRecon helps administrators identify which parts of a network are most susceptible to unauthorized access and denial of service.

Since NetRecon probes systems in many ways, it demonstrates the many ways that networks are vulnerable, and since the process is automated, a large amount of information can be gathered in a short amount of time. NetRecon reports provide detailed information about potential problems (weak passwords, system services vulnerable to denial of service attacks, etc.), allowing administrators to fix particular problems and see vulnerability patterns.

One thing you don't need to worry about while using NetRecon is losing data or crashing your network. NetRecon does not affect any files on local or network drives, and while NetRecon tests for the possibility of denial of service attacks, it does not actually perform such attacks.

NOTE

NetRecon demonstrates vulnerabilities—it does not fix them. Using NetRecon is just one part of the network security process, and should be used to help formulate good security policies and put them into practice.

Program Window

The NetRecon program window is divided into several areas, called *panes*. Figure 3-1 highlights sections of the NetRecon window.

The Objectives pane lets you choose what type of scanning you want to perform.

The Graph pane is dynamically updated to provide an overview of the number and severity of vulnerabilities found.

The Data Table pane shows details about each vulnerability discovered.

The Status Bar shows you scan progress and how many records are in the Data Table pane.

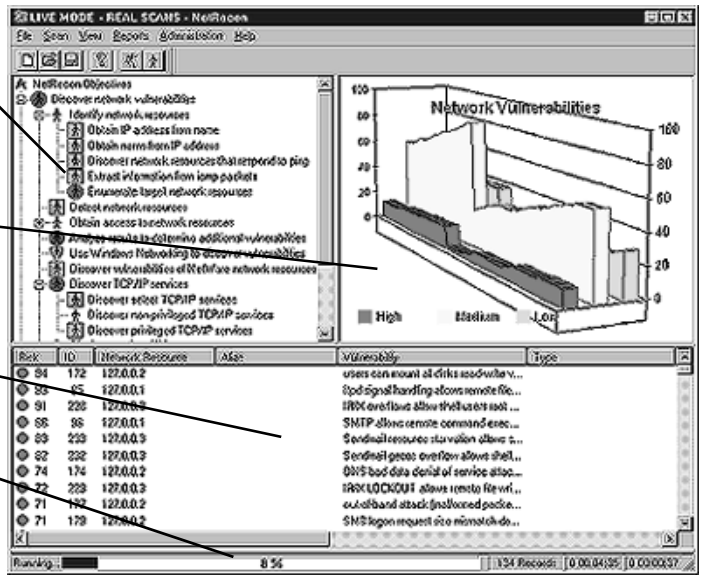


Figure 3-1: The NetRecon program window

Objectives Pane

In order to discover network vulnerabilities, NetRecon has a number of set goals, some for gathering information about your networks and some which use that information to gain access to network resources. These goals are referred to in NetRecon as **objectives**.

The Objectives pane (upper left corner of the NetRecon main window) is where all NetRecon objectives are listed. The objectives are organized into a hierarchy, as represented by the tree format of the objectives.

To expand any part of the tree (i.e. to view the children of any particular parent objective):

1. Click the plus symbol to the left of any parent objective.

Selecting an objective in the Objectives pane limits the records displayed in the Data Table pane, the Graph pane, and vulnerabilities listed in reports to those that meet the selected objective.

Graph Pane

The Graph pane (upper right corner of the NetRecon main window) shows the number of low-risk, medium-risk, and high-risk records discovered as NetRecon runs. The graph is refreshed as the program runs and discovers new records.

The record count displayed by the Graph pane depends on what is selected in the Objectives pane, since NetRecon filters records on that basis.

The Graph pane gives you a quick at-a-glance overview of the results of a scan. When you generate a report, the current state of the graph can be placed in the report.

Data Table Pane

Records *are pieces of data about networks being scanned by NetRecon. When NetRecon discovers vulnerabilities or information that could lead to the discovery of vulnerabilities, it stores the information it finds in records. Records usually have multiple fields. Each row in the Data Table pane shows one record.*

The Data Table pane (bottom half of the NetRecon main window) shows records generated by NetRecon as it runs. Each row contains one record. The columns in the table show field values in those records.

By default, NetRecon limits the records displayed to those that are specifically related to the objective selected in the Objectives pane. You can show all records generated during a scan using the All Records command in the View menu.

You can change the display order of the columns by dragging the column headers. To sort the table data by the data in any of the columns, click the column header. To change the sort order (ascending / descending), click the column header again. During a scan, by default NetRecon sorts records by risk (descending order) every 15 seconds. You can turn off Auto Sort if you wish.

To the left of each record is an icon indicating its risk level.

Scanning

Before you begin scanning network resources, you should determine which network resources you want to scan and who can grant permission to scan those resources, and then be sure to secure permission. **Scanning network resources without permission is a very serious matter that may result in legal action and/or civil litigation.**

In order to perform a scan:

1. Select an objective in the Objectives pane.

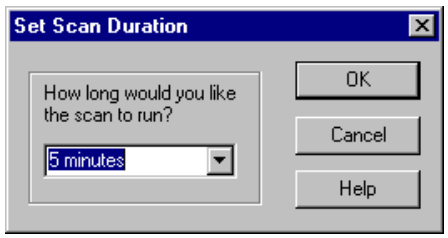
   The Discover network vulnerabilities objective contains all other scan objectives, and is selected by default. In most cases, it is the objective you'll want to run.

2. Click in the Toolbar.

   OR

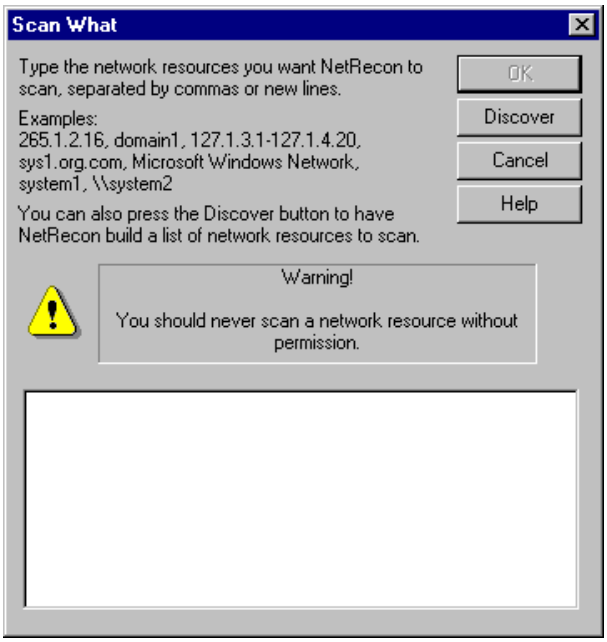
Choose Scan, Start Scan.

The Set Scan Duration dialog box appears.



3. Choose an option from the drop-down list or type a value and a unit (seconds, minutes, hours, or days), then click OK.

   The Scan What dialog box appears.



4. Type the systems you want to scan, or click Discover to have NetRecon build a list of network resources you may want to scan.

   You can specify IP addresses, including ranges (see the example in the dialog box above, which is a range that covers one full class C network and part of a second); system names; domain names; a Microsoft Windows Network, or a NetWare or Compatible Network. You can include reference to network resources exactly as they appear in the Windows Network Neighborhood window. Separate entries with a comma or a line break.

You can also drag the icon of a text file containing network addresses from the Windows Explorer into this dialog box to specify network resources.

If you click Discover to have NetRecon search for network resources, be sure to look carefully at the list of network resources NetRecon discovers and edit it if necessary before proceeding with a scan. **Scanning networks without authorization can result in criminal prosecution and/or civil litigation.**

5. Once you are satisfied that you have specified only network resources you want to scan, click OK to begin the scan.

Reports

As NetRecon runs it gathers information about the networks it scans. The graph in the Graph pane is a visual indicator of the accumulation of scan data (each piece of data called a record).

The Data Table pane shows records related to the objective selected in the Objectives pane (only those that meet the currently selected objective are shown by default; you can also choose to show all records).

At any point during the scan, you can have NetRecon generate a report, which is a summary of the information gathered to that point.

Reports list only vulnerabilities that meet the objective selected in the Objectives pane when the report is created. If you want the report to show all vulnerabilities discovered by NetRecon, select the Discover network vulnerabilities objective in the Objectives pane before creating the report.

To create and view a report:

1. Choose Reports, Create and View Report
2. Type the name of the report in the Report File Name text box (be sure to give this filename a .htm extension).
3. Type the name of the folder where you want the report to be created in the Report Folder text box.

   OR

   Click Browse and select a folder using the Windows Open dialog box.
4. Select the check boxes next to each item you want included in the report, then click OK.
5. Click OK.

   A dialog box appears confirming that a report was created.
6. Click OK.

UltraScan

Each NetRecon objective runs separately and simultaneously. Most objectives receive information from or pass information to other objectives. The interdependency of NetRecon objectives is their strength—because they share information with each other, NetRecon can probe a system much like a human being would, using all the information gathered as a lever to gain still more information.

Particularly with UltraScan (as opposed to other scanning methodologies), the vulnerabilities reported during a network scan may vary from scan to scan. That's because some network resources may be offline, and since NetRecon uses the information found by some vulnerabilities to detect others, having a network resource offline might reduce an entire "branch" of information.

Chapter 4

Documentation

This chapter describes what NetRecon user documentation is available in addition to this manual.

Online Help

The most complete source of information about the NetRecon program is the online help. The online help provides complete information about common tasks you might want to perform with NetRecon, conceptual information about the program, explanations of NetRecon's user interface, definitions of common terms, and more.

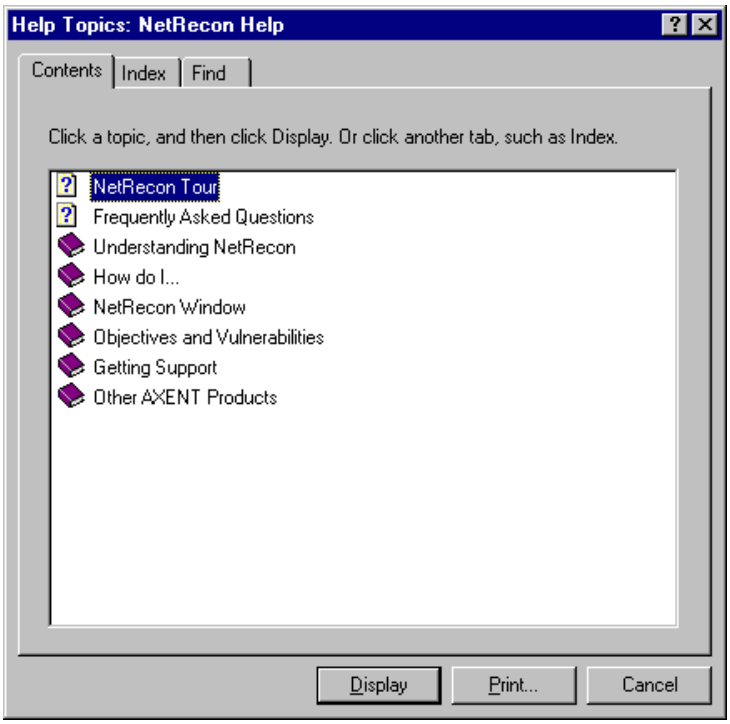
You can enter help in any of the following ways:

- Click in the Tool Bar.
- Choose Help Topics from the Help menu.
- Press F1 (this does not work in all parts of the program)
- Click the Help button in dialog boxes that have one.

Windows Help provides three ways to find the information you need: the Contents Tab, the Index tab, and the Find tab.

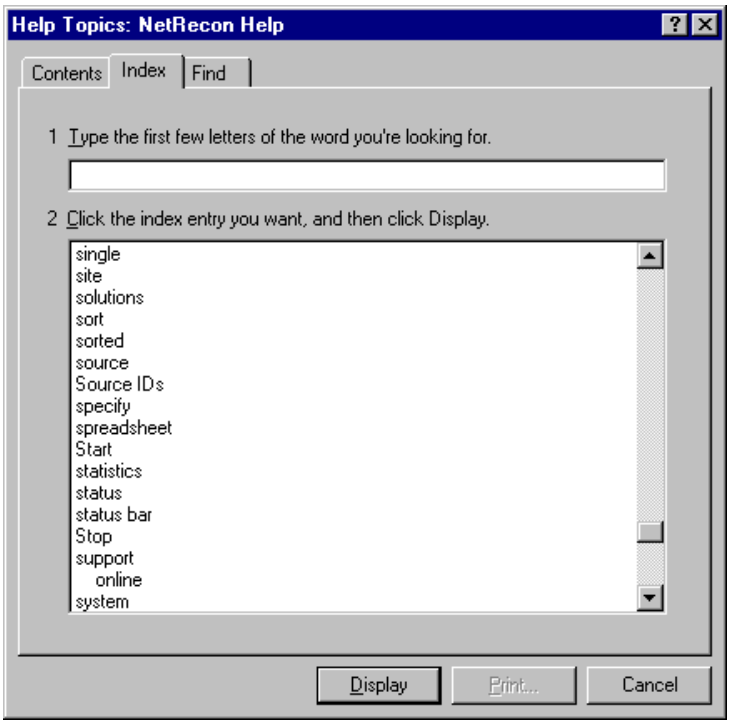
Contents Tab

The Contents tab contains a hierarchical listing of topics, organized much like the table of contents of a book.



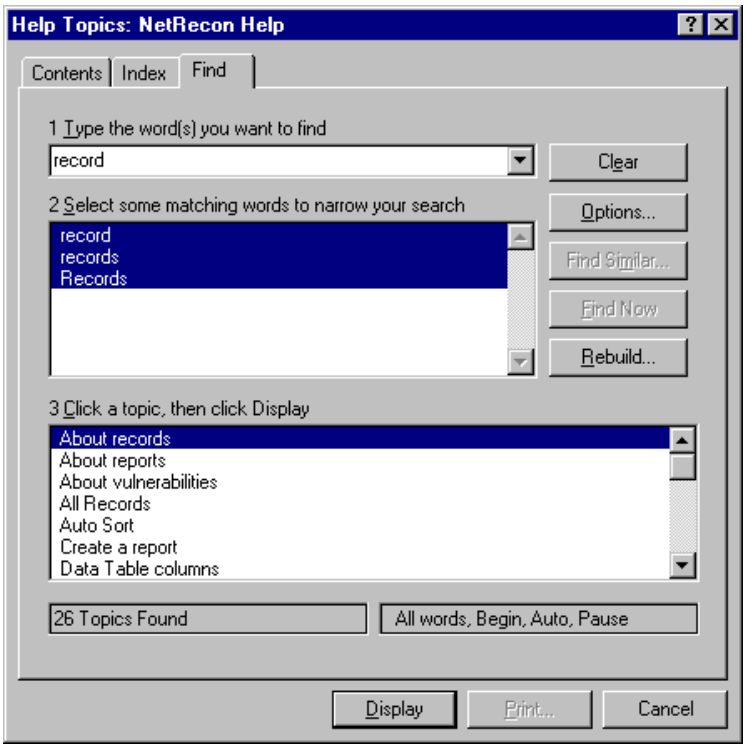
Index Tab

The index tab contains a list of words or phrases either contained in the help file or designed to help you find topics (synonyms of program terms, features, etc.).



Find Tab

The Find tab lets you search for any words found in any of the topics in the help file. The first time you open Help and select the Find tab, the Find Setup Wizard will appear. This wizard makes a list of all the words in the help file that the Find tab uses when you perform searches. Follow the wizard instructions for creating the Find word list.



Objective and Vulnerability Descriptions

NetRecon also comes with two HTML files that contain descriptions of all the objectives you can run in NetRecon (`objlist.htm`) and all the vulnerabilities NetRecon can discover (`vulnlist.htm`). These files are located in the same folder as the NetRecon program (which you specified when you installed the product). These files can be opened directly into a web browser.

You can also open either one of these files from within NetRecon:

1. Choose Reports, View Objective Descriptions to view the descriptions of NetRecon objectives.

   OR

   Choose Reports, View Vulnerability Descriptions to view the descriptions of vulnerabilities NetRecon searches for.

4.6 Documentation

Index

A

administration 2-3
administrative access 1-2
administrator, security 3-1

C

children 3-3
columns 3-4
common tasks 4-1
conceptual information 4-1
contents 4-2

D

Data Table Pane 3-4
data, table 3-4
Demo Mode 2-1, 2-4
denial of service 3-1
discover 3-6
disk space 1-1
documentation 4-1

F

features 3-1
find 4-4

G

Graph Pane 3-3

H

help 4-1
how do i 4-1

I

install
    CD 1-2
    Internet 1-3
installation 1-2
interdependency 3-8
interface 4-1

L

length 3-5
license
    changing 2-3
license key 2-1, 2-2

N

network resources 2-1, 3-5

O

objective 3-4, 4-5
Objectives Pane 3-3
objectives (definition) 3-3
online help 4-1

P

pane
    Data Table 3-4
    Graph 3-3
    objectives 3-3
panes 3-2
parent 3-3
password 2-4
    change 2-4
    new 2-4
passwords 3-1
personal profile 1-2
policies 3-2
program window 3-2

R

RAM 1-1
records 3-3, 3-4
records (definition) 3-4
reports 3-6

S

scan 3-4
    simulated 2-4
scans 2-1
security 3-2
security administrator 3-1
serial number 2-1, 2-2
services 3-1
sort 3-4
start 3-5
summary 3-7
synonyms 4-3
system requirements 1-1
system services 3-1

T

table data 3-4
table of contents 4-2
terms 4-1
tree 3-3

U

UltraScan 3-8
unauthorized access 3-1
user documentation 4-1
user interface 4-1

V

vulnerability 3-1, 4-5

W

weak passwords 3-1