CyberCop Scanner 5.5

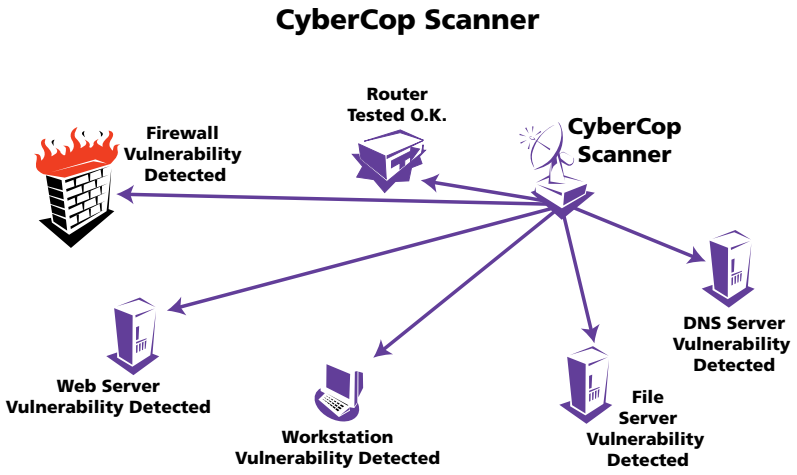
TOTAL NETWORK SECURITY

Measure, Manage and Secure Against Network Risk

An important first step in any committed enterprise security strategy, risk assessment of network assets enables a company to quantify and qualify security threats. CyberCop Scanner quickly reveals previously undiscovered threats and vulnerabilities that could be used by hackers as a doorway to your most sensitive data. CyberCop Scanner's new auditing tools allow you to quickly scan and evaluate multiple security scenarios using comprehensive "real-world" resolution data to fix these holes. CyberCop Scanner offers a unique architecture with comprehensive security data in a streamlined security tool that helps protect e-business operations.

On-the-Spot Vulnerability Resolution with Auto Fix

CyberCop Scanner is the only security tool that offers a state-of-the-art Auto Fix feature, enabling security professionals to immediately apply solutions to vulnerabilities and instantly thwart attacks. CyberCop's AutoUpdate feature allows companies to keep pace with real-world threats by continually updating the scanning engine, scan tests and vulnerability database on a regular, automated basis.



Risk assessments of your network using CyberCop Scanner reveal previously undiscovered security threats.

Extensive Vulnerability Detection

CyberCop Scanner is unparalleled in locating critical vulnerabilities. In addition to extensive firewall configuration checks, CyberCop Scanner tests e-business and mission critical web servers, file servers, workstations and networking services to uncover vulnerabilities. Only CyberCop Scanner includes IDS, DNS and custom audit tools to detect weaknesses in a multitude of enterprise environments. CyberCop Scanner then goes beyond traditional security solutions to check for policy violations and gather additional information about the expanding network infrastructure. Security professionals can use CyberCop Scanner not only to validate policy, but enforce adherence to corporate security strategies.

NET TOOLS			
Net Tools Secure		Net Tools Manager	
McAfee Total Virus Defense	PGP Total Network Security	Sniffer Total Network Visibility	Magic Total Service Desk

GAUNTLET FIREWALL
CYBERCOP INTRUSION PROTECTION
PGP VPN AND DATA SECURITY

Features and Benefits

- Auto Fix capabilities instantly repair known vulnerabilities to save time, resources, and your critical data
- New scan modules and updated resolution information on over 720 vulnerability checks extend security
- AutoUpdate feature keeps the scanning engine, scan tests and vulnerability database current
- New scan configuration and module selection templates allow for multiple environment configurations of scan and vulnerability settings
- Operating System (OS) detection identifies the operating system type of hosts on a network. Once operating system types are identified, CyberCop Scanner optionally disables modules not pertaining to specified operating systems, increasing scanning speed
- Active Security architecture integrates event orchestration for advanced security policy management

"CyberCop seems to have taken the vulnerability testing market by the scruff of the neck and given it a damn good shake."
—Secure Computing

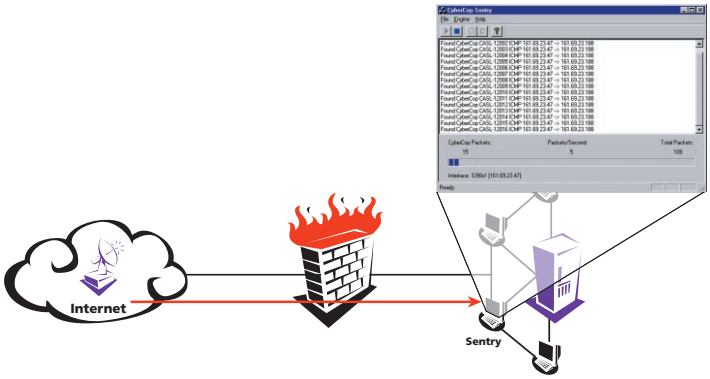
network ASSOCIATES
Who's watching your network

CyberCop Scanner 5.5 Features

- New graphical user interface (GUI) provides faster navigation through comprehensive features and controls of CyberCop Scanner
- New OS scanning selection allows for the specific targeting of groups of systems to easily manage scanning of multiple hosts within large heterogeneous environments
- New scan engine utilizes Microsoft's 32Bit architecture for vastly improved scanning speed and bandwidth usage configuration to allow scanning of over 100 hosts simultaneously
- Probe feature detects hosts without scanning to identify responsive hosts, the operating system type, and a "snap-shot" network map
- ODBC compliant vulnerability database includes detailed module descriptions and links to sites that contain additional information about vulnerabilities
- New and enhanced reporting engine via MMC allows for customized report generation using Crystal Reports 6.0
- Visual Basic scripting allows security professionals to write scripts for customizable modules and then integrate them into the vulnerability database
- Intrusion detection sensor tests verify baseline functionality and survivability of Network IDS sensors
- 3D Network Map for qualifying network devices and connections streamlines manageability
- Custom Audit Scripting Language (CASL) Scripting Tool helps create custom scan tests for any IP device or protocol

Hassle-Free Management Tools

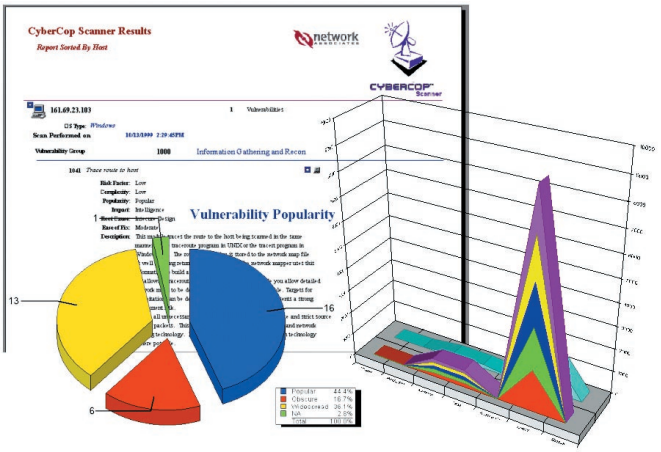
CyberCop's new reporting format arms a company with the ability to view "at-a-glance" a company's weaknesses and security policy violations to prioritize threats within the enterprise environment. By means of an ODBC compliant database structure, CyberCop Scanner's reporting tools allow for graphical executive and line management level reporting that is fully customizable. Analytical reporting also provides risk prioritization by breaking out your least and most vulnerable systems to quickly alert you to issues and granular vulnerability information provides detail resolution advice.



The new Firewall Sentry allows for ease-of-use and report generation during firewall audits and extensive access control checks to secure firewalls and other packet filtering devices.

Active Security Integration

CyberCop Scanner is a member of the premier release of Network Associates' integrated family of Active Security products. These products represent the next evolutionary step in enterprise security—proactive, automated enforcement of network security policies. Active Security performs customized, automated responses to network security vulnerabilities as they are discovered on your network. Responses can include creating helpdesk tickets and routing them to the appropriate person in your organization, sending SMTP messages or pager alerts to administrators, and shutting down specific ports on Gauntlet Firewalls thus preventing malicious users from exploiting these vulnerabilities.



In addition to executive summaries and granular technical reporting, graphical charts are used to visually convey the level of risk specific to each device enabling a security professional to quickly determine the most vulnerable systems.

Secure Computing 5 Star Rating

SC INFOSECURITY MAGAZINE

INFOWORLD

network ASSOCIATES

Who's watching your network

For more information on products, services, and support, contact your authorized Network Associates sales representative.

CORPORATE HEADQUARTERS

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (408) 988-3832*
Fax (408) 970-9727

Call for additional Worldwide Sales Offices

Visit our Website

www.nai.com

1-TNS-CCS-001 11/99