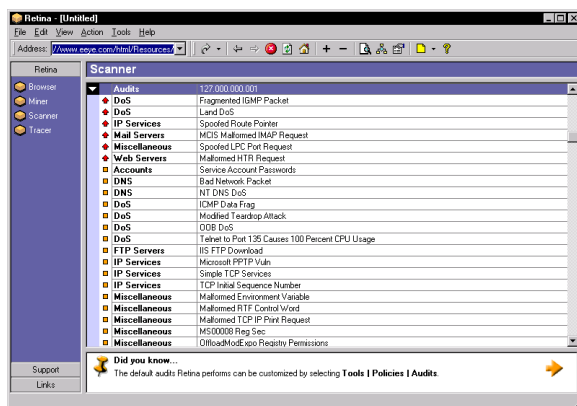# Retina

The Network Security Scanner

Retina is a network vulnerability scanner unlike any other. Unrivaled in its capabilities, Retina provides a continuous security presence in places no other application has dared go before. While most security scanners confine themselves to searching for only known vulnerabilities, Retina shatters the mold of the typical security scanner through its use of state-of-the-art AI (Artificial Intelligence). The AI component allows Retina to think like a hacker or security analyst would if they were attempting to break into your network. Thus, Retina eclipses most current security scanners on the market that only look for known vulnerabilities. Retina searches for both known *and* unknown vulnerabilities, giving an organization the most complete network security analysis possible.

Validating this claim of pioneering security research and application was our recent discovery of a hole in Microsoft Internet Information Sever. Using Retina, a hole that affected over a million Windows NT web servers on the Internet was identified. A serious flaw, which left unchecked, could have been devastating. Retina has been the force behind several other high-profile vulnerability advisories including a flaw in Ultraseek, the Infoseek search engine. For a complete list of Retina vulnerability advisories, please visit eeye.com/html/Advisories/index.html.

Retina has the ability to scan, monitor and fix vulnerabilities within a network's Internet, Intranet, and Extranet. Thus, giving the network administrator complete control across all possible points of attack within an organization and the confidence required in operating a network to its fullest potential. Retina includes easy-to-navigate reporting tools to help identify and isolate high priority fixes, allowing total command over auditing network security and open network gateways into an internal network.

Vulnerability Scanning

Vulnerability scanning is the process of checking for all the potential methods that an attacker might use to tamper with an organization's network. By analyzing what types of software and software configurations are on a given network, scanners are able to determine what types of attack are possible against a network so it can defend itself accordingly. Vulnerability scanning has become a primary focus of network administrators as the potential threat of a security breach has become preeminent.

Network and software vulnerabilities exist in two basic forms: known vulnerabilities and unknown vulnerabilities. Known vulnerabilities are those that have been identified and isolated by a security scan. An advisory is then published to alert users of the existing hole or flaw. Unknown vulnerabilities have not been discovered or publicly acknowledged, making them a potential security threat.

Retina Features and Functions

Retina is designed to identify and alert security vulnerabilities, suggest fixes and report possible security holes within a network's Internet, Intranet and Extranet systems. Its' superior scanning capabilities provide a network with the most comprehensive security analysis available.

Retina includes vulnerability auditing modules for the following systems and services:

- NetBIOS
- HTTP, CGI and WinCGI
- FTP
- DNS
- DoS vulnerabilities
- POP, SMTP and LDAP
- TCP/IP and UDP
- Registry
- Services
- Users and Accounts
- Password vulnerabilities
- Publishing extensions
- Database servers
- Firewalls and Routers
- Proxy Servers

Graphical User Interface
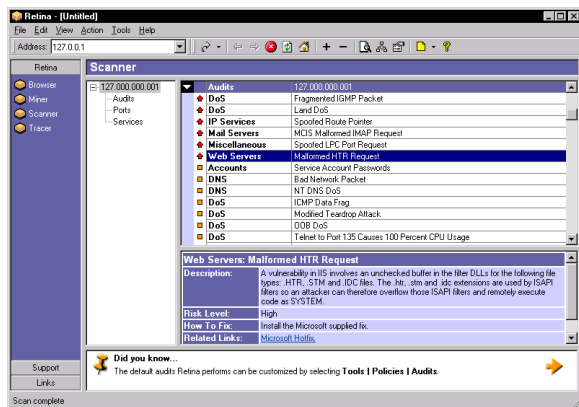
Retina contains a simple to navigate graphical user interface. This interface can easily be used to control all aspects of scanning and reporting features within Retina. A lack of security expertise among IT personnel is no longer a compromise to an organization's network security. Visionary in its function, this technology gives overworked and under-resourced IT personnel a viable network security presence without the constant attention required to

monitor it. As a result, an organization's IT talent can focus more effectively on its daily operations.

CHAM (common hacking attack methods)

This groundbreaking feature is the first of its kind. CHAM employs AI technology in order to simulate the thought process of a hacker or security analyst in finding holes in networks and software packages. A software program or network might have no known vulnerabilities, but that does not mean it is completely secure. Even if no hacker or security analyst has attempted to find and exploit holes in the software or network, damaging flaws may still exist. Retina will adopt the mindset of a hacker or security analyst to find those potential holes in network software to thwart off any potential security breach.

Fix-It

Retina includes advanced Fix-It technology. This distinct feature allows the network administrator to automatically correct common system security issues including registry settings, file permissions and more. Rather than wasting valuable time manually fixing vulnerabilities, a simple click of a button will command Retina to do it for you. This rare component can also work remotely across a vast network, affording the network administrator the freedom and flexibility to operate under any conditions.

Audits
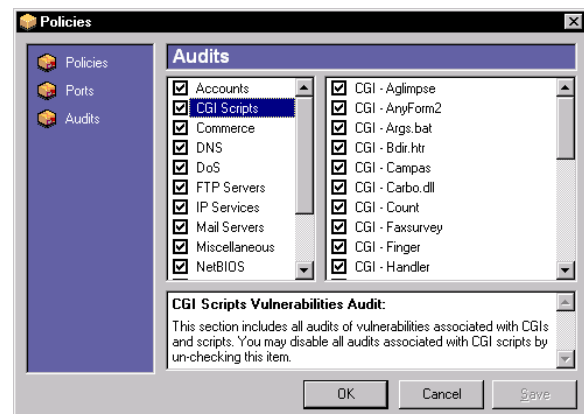
A Retina Audit is a network assessment that identifies and details any problems found that

might compromise network security. Retina offers a variety of examples of potential security flaws that can be scanned for. Retina also has a wizard interface to create new audits. These audits can be used to find vulnerabilities specific to an organization's needs and concerns. Most scanners currently on the market claim of easy to use scripting languages to create new audits. However, in most scenarios these are essentially just interfaces to scripting languages such as Perl, forcing you to adapt to their predetermined programming guidelines. By contrast, Retina has a truly easy way of creating custom audits in any scripting language you prefer, saving valuable time and resources.

Smart Scanning

Retina includes an AI (Artificial Intelligence) module that makes it vastly smarter and intensely thorough about pinpointing real world vulnerabilities. Current security scanners on the market will initiate a port scan of a remote system and assume that a certain port is a certain protocol. In contrast, Retina never assumes anything. Retina does not stop at merely grabbing banners on ports,. It analyses specific input/output data on a port to determine what protocol and service is actually running. For example, if Retina determines a port to be open, the AI component within the Smart Scan will not assume it is an FTP Server and do only FTP Server checks. Retina will actually determine what protocol is on the open port and proceed to initiate checks accordingly.

Smart Reporting

Retina can produce fully documented network audit reports based on its security scans. Smart Reporting allows the network administrator to access, read and print these real-time security test results with ease. The reports detail all security holes and flaws that are detected in a scan and are ready to print with just a simple click of the mouse. Two options are available for reporting: the Technical Report with intricate detail to satisfy IT personnel, and the Executive Report for high-level management summaries.

Auto Update

Retina encompasses an auto-update feature that provides continuous updates for its modules using an Internet connection. This feature will allow the network administrator to update Retina's modules on a regular basis, thus keeping pace with the latest vulnerabilities.
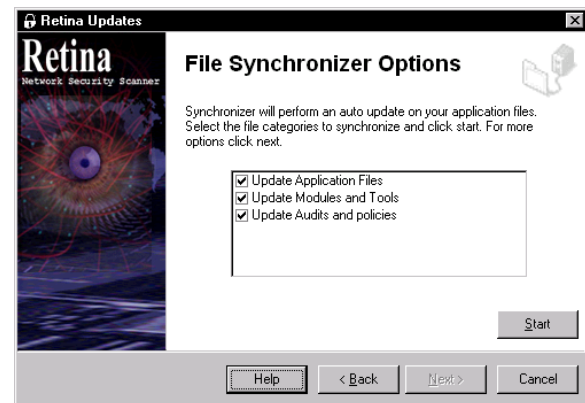
Open Architecture

Retina has an open architecture that provides the administrator the opportunity to develop vulnerabilities tests and auditing modules tailored to an organization's precise requirements. What differentiates Retina from other security scanners on the market is that it does not force the administrator to use a certain programming language to create these modules. Retina offers the flexibility to create customized modules with any programming language that best suits the administrator, including Perl, C, C++, Visual Basic, Delphi etc…

Competitive Assessment

The release of Retina signifies a revolution in network security. With iconoclastic precision, Retina integrates technical sophistication with a simple graphical interface creating the ultimate network vulnerability scanner. There are several existing systems scanners available on the market. Retina distinguishes itself from the rest by employing advanced proprietary features that function ingeniously as a whole.

CHAM offers a unique opportunity to test services on your network for unknown holes. It implements a scan using IETF (Internet Engineering Task Force) standards to test expected responses against actual responses. It sends commands and arguments in an attempt to cause problems. With the rise in remote buffer overflows appearing on technical lists such as Bugtraq and NTBugtraq, it is important for you to find these types of problems before they are exploited. CHAM is the only technology that offers tests for these types of holes.

Retina eclipses current security scanners by utilizing technologies not offered by our competitors.

FEATURES	NETWORK VULNERABILITY SCANNERS				
	eEye RETINA	ISS SCANNER	NAI CYBERCOP	BINDVIEW HACKERSHIELD	AXENT NETRECON
REPORTING	✓	✓	✓	✓	✓
SMART SCANNING	✓				
AUTOFIX	✓		✓	✓	
AUTOUPDATE	✓	✓	✓	✓	
CHAM	✓				
OPEN ARCHITECTURE	✓		✓		

eEye Approved

eEye approved is the essential support element behind Retina. Mirroring our ingenious software, the eEye Digital Security Team is constantly striving to keep your organization's network safe. The eEye Digital Security Team will keep network administrators informed on the latest up-to-the-minute security vulnerabilities, hacking techniques and analysis methods.

eEye Digital Security

eEye Digital Security is a security product development company with one paramount goal in mind, complete security for your organization. Our singular existence stems from the lack of state-of-the-art security products currently available for network administrators in need of the finest protection their networks deserve.

Many digital security companies mistakenly operate under the guise of "security experts."

They advertise their knowledge, yet fail to release any advisories (a document containing information about a vulnerability in a piece of software) with appropriate regularity. This advisory information is critical, and must be provided instantly in order to preserve the integrity of your network. The eEye security team works tirelessly around the clock to discover the latest and most damaging security vulnerabilities.

In the increasingly competitive security marketplace, what separates eEye from other security providers is not only our expertise, but our unique ability to adapt that knowledge to the individual needs of your organization. The list of Fortune 500 and government organization clients who employ our products is impressive, as is the peace of mind that comes with using our products, but that is merely a reflection of the people standing behind it.

But who are we? eEye is a team of seasoned security experts possessed of the most cutting-edge security scanning techniques and applications. We are young, but years do not necessarily equal wisdom in the Digital Era. Besides, what other security company employs a Chief Hacking Officer? Our security experts believe that a product must sell itself on its own merits. There are no affected marketing campaigns here, no cryptic visuals of broken chains and busted locks. The endless dedication we have for what we do is instilled in every product we offer. Our commitment to network security is evident in everything we do. If it is not, then we are not doing our job. We invite you to visit our Website at www.eeye.com and download our products for demonstration. We believe they will speak for themselves. In short, we mean business. And our business is your digital security.

Contact Information

For additional information please contact eEye Digital Security at one of the following:-

Phone: 949.675.8160
Fax: 949.675.8191
Web: http://www.eEye.com
Email: info@eEye.com