eEye Digital Security®

RETINA® Network Security Scanner

Integrated Security & Threat Management Solution.

Network vulnerabilities are an increasingly common issue in today's highly complex computing environments. With exploit attacks appearing faster than ever before, it has become significantly more challenging for organizations to protect against attack. A notable case in point is the Sasser worm. Sasser was based on exploit code released two days earlier and only 18 days after the initial vulnerability was announced.

With such a dynamic threat environment to contend with, IT professionals need a proactive security management strategy that goes beyond routine patch deployment. To meet the challenge, and reduce overall network security TCO in the process, organizations are adopting integrated security and threat management solutions from eEye Digital Security.

Unsurpassed Vulnerability Management

Retina® Network Security Scanner is a professional-grade security solution with a lengthy track record of success and industry leadership. Retina contains all the integrated security and threat management tools needed to effectively identify and remediate the network vulnerabilities that lead to exposure and malicious attacks. Retina secures networks by:

- **Accurately discovering all the assets in the network infrastructure** including operating system platforms, networked devices, databases and third party or custom applications. Retina also discovers wireless devices and their configurations, ensuring these connections can be audited for the appropriate security settings. Additionally, Retina scans active ports and confirms the services associated with those ports.

- **Implementing corporate policy driven scans** to audit internal security guidelines and ensure that configuration requirements are enforced and comply with defined standards. These custom scans can also assist with meeting any regulatory compliance requirements (SOX, HIPAA, GLB, PCI etc) customers may face.

- **Remotely identifying system level vulnerabilities** to mimic an attacker's point of view, providing information that an outsider would see about your network. These remote checks do not require administrator rights, providing an accurate assessment, with fewer resources required to scan across departments, locations or geographies.

- **Incorporating the most comprehensive vulnerabilities database** and scanning technology available, allowing users to proactively secure their networks against attacks. Retina was developed and is constantly updated by the eEye Research Team, leveraging its expertise and superior vulnerability discovery methodology. Updates are automatically uploaded at the beginning of each Retina session.

- **Providing a workflow approach to vulnerability management.** Retina's user interface allows for multiple views and reporting options with which to analyze assessment data. This gives users the opportunity to view assets criticality correlated with complete vulnerability data. This approach allows users to effectively prioritize remediation efforts.

"The Retina vulnerability management solution identified vulnerable computers, servers, printers, video-encoders, access control systems and provided informative reports which made remediation possible. Retina significantly improved network security, facilitates security compliance, and continues to be an important tool in the Enterprise."

- Martin Maxwell, Network Management Team
California Department of Transportation
November 2009

Fast Facts

- Accurately discovers all network-connected assets
- Non-intrusive scanning optimizes network performance
- Utilizes a highly comprehensive vulnerability database
- Allows users to create custom, corporate-policy driven scans
- Designed with an open architecture for customized audits and easy integration with third party platforms
- Maintained and constantly updated by the eEye Research Team

Secure Your Business.

www.eEye.com
866-282-8276

The endpoint to vulnerability starts here.

RETINA® Network Security Scanner
Additional Features and Benefits

- Accurate Asset Discovery and Inventory
Retina discovers all the assets on a given network, including operating systems, applications, services, databases and wireless devices. Retina's advanced OS discovery utilizes ICMP, registry, NetBIOS, and the Nmap signature database, as well as eEye's proprietary OS fingerprinting for more accurate & definitive OS identification. Additionally, Retina has profiles for nearly 2,000 of the most commonly utilized ports, and allows for scanning of all 65,536 ports on a network device.

- Custom Security Audits
Users can create custom audits for the enforcement of corporate security policies, including anti-virus deployments, application version control, file sharing, permissible ports and P2P, as well as enabling regulatory compliance requirements.

- Remediation Assessment
Retina allows prioritized remediation through its intuitive user interface, categorizing vulnerabilities according to risk level. Integration with third party help desk and ticketing systems is a simple process. Additionally, Retina's Fix-it function can be used to remotely correct security issues such as registry settings, file permissions, etc.

- Localized System Audits
Auditing of non-Windows devices includes SSH tunneling to perform local vulnerability assessment of UNIX, Linux, Cisco, and other devices. This allows security professionals to identify vulnerabilities on non-Windows devices that need local file or setting checks.

- Smart Protocol Scanning
Retina reconciles the input/output data on each port to determine which protocols and services are actually running, including SSL. In this way, Retina makes adjustments for custom or unconventional machine setup.

- Advanced Scheduling Capabilities
Retina's scheduler function allows you to set the scanner to run on a regular basis to periodically check for vulnerabilities. Because Retina is non-intrusive, you can pre-schedule your scans without the risk of unplanned network downtime.

About eEye Digital Security

eEye Digital Security is the global leader in the next generation of security solutions: comprehensive vulnerability management and zero-day endpoint security protection. eEye enables secure computing through world-renowned research and innovative technology, supplying the world's largest businesses with integrated and research-driven vulnerability assessment, intrusion prevention, asset security and compliance solutions. eEye's research team is consistently the first to identify new threats in the wild and our products leverage that research to deliver the tools necessary to protect our customers' environments. The endpoint to vulnerability starts here.

eEye's customers represent the largest deployments of vulnerability assessment and prevention technology in the private and public sectors. eEye protects the networks and digital assets of a growing network of more than 9,000 corporate and government deployments worldwide. Founded in 1998, eEye Digital Security is an award-winning CA internet security company headquartered in Orange County, California.

U.S. Tel: 1.866.282.8276
N. America: 1.949.333.1900
Germany: +49 (0) 8031 2227 432
U.K.: +44 (0) 20 8432 3490

N. America Sales: sales@eEye.com
International Sales: sales.eu@eEye.com

System Requirements

- Windows 2000 Professional
- Windows 2000 Server
- Windows XP (32-bit)
- Windows Server 2003 (32-bit)
- Windows Vista SP2 (32-bit or 64-bit)
- Windows Server 2008 SP2 (32-bit or 64-bit)
- Intel Pentium IV 1.4Ghz (or compatible)
- 512 MB of RAM
- At least 80MB of free disc space
- Microsoft .Net Framework 2.0 (included with installer)
- Network Interface Card (NIC) with TCP/IP enabled

The endpoint to vulnerability starts here.

© 2009 eEye Digital Security. All Rights Reserved.