Global Information Assurance Certification Paper

Vulnerability Assessment – A Case Study

Homyar B. Naterwala
GSEC Practical Paper
Version 1.4b Option 2
May 19th, 2004

Table of Contents

Introduction

There are new attack signatures being developed, viruses and worms being written, natural disasters occurring, changes in the organization workplace taking place and new technologies evolving. These factors all affect the security posture in any organization. Any one piece of the lifecycle cannot be effective without the provision of the other components.

A solid Information Systems Security Policy is essential, but can you be assured you are secure once you have taken a snapshot and taken actions to fix them? The lifecycle needs to be a continued effort for any organization to keep abreast of changes in technology and weaknesses in security that are created as a result of these changes. Key elements of the lifecycle are:

- Perimeter Protection
- ***Risk and Vulnerability Assessment Process***
- Information Systems Security Policies & Remediation Process
- Penetration Testing
- Intrusion Detection

All elements must adhere to the four basic steps in managing risk: Detect, Analyze, Recover, and Protect.

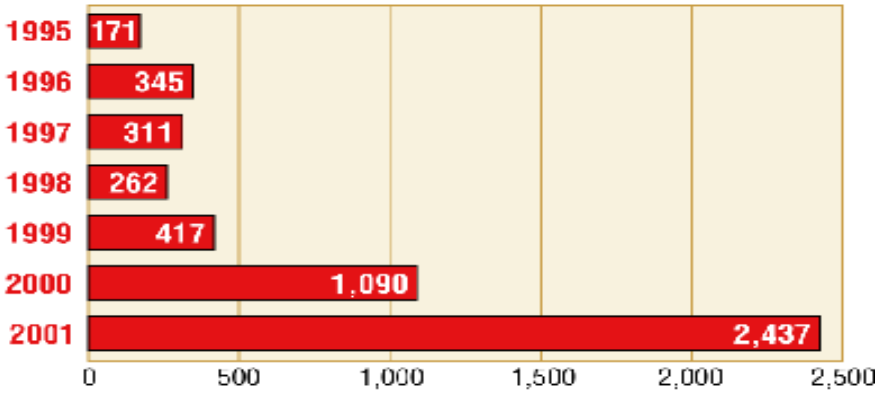
Purpose

It is the intent of this document to address *the* ***Risk and Vulnerability Assessment Process*** element in the lifecycle, the tools utilized in this process, and the supporting physical and logical models required to produce effectiveness in the environment.

Architecture Overview

Newly discovered Operating System (OS), application or hardware vulnerabilities

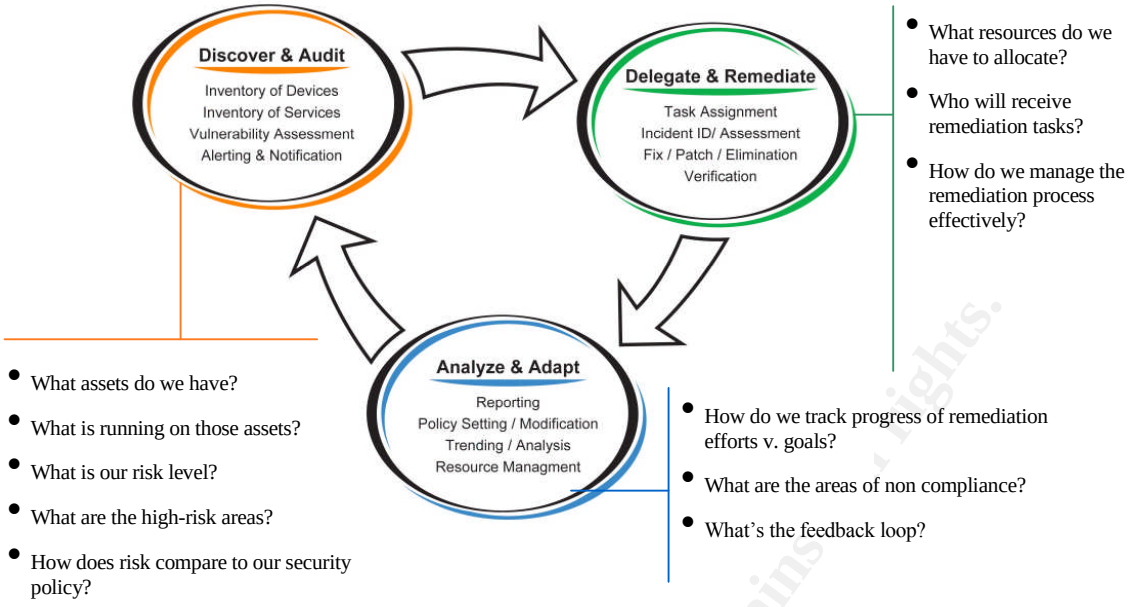
The number of computer vulnerabilities reported to Carnegie Mellon's Computer Emergency Response Team (CERT) more than doubled from 2000 to 2001. (1)



While hardware and software vendors make every effort to provide error free devices and/or software, new vulnerabilities are inevitably discovered. Typically these vulnerabilities are addressed in a vulnerability patch, service pack or firmware flash. Effective detection and remediation of these vulnerabilities relies on the proper procedures in place to review all CERTs and patches. Any tool utilized in the detection of vulnerabilities must have a knowledge base that is current, accurate, and updated in a timely and automated manner.

Known vulnerabilities found on an improperly configured system or network device

With the increasing workload on device and system administrators and the increase in vulnerabilities and threats, improperly configured devices can become common place in the environment without a proactive process in place to continually check these devices. Devices deemed secure today can be vulnerable tomorrow without the proper continuous detection process or tool in place. Architecture and design of an infrastructure to support Vulnerability Remediation and Management must address these issues and assist in answering the following questions.



(2)

Assessment Criteria

After reviewing the tests published by Network Computing Magazine [3], the following criteria were considered in our evaluation of products that provide the vulnerability assessment tool.

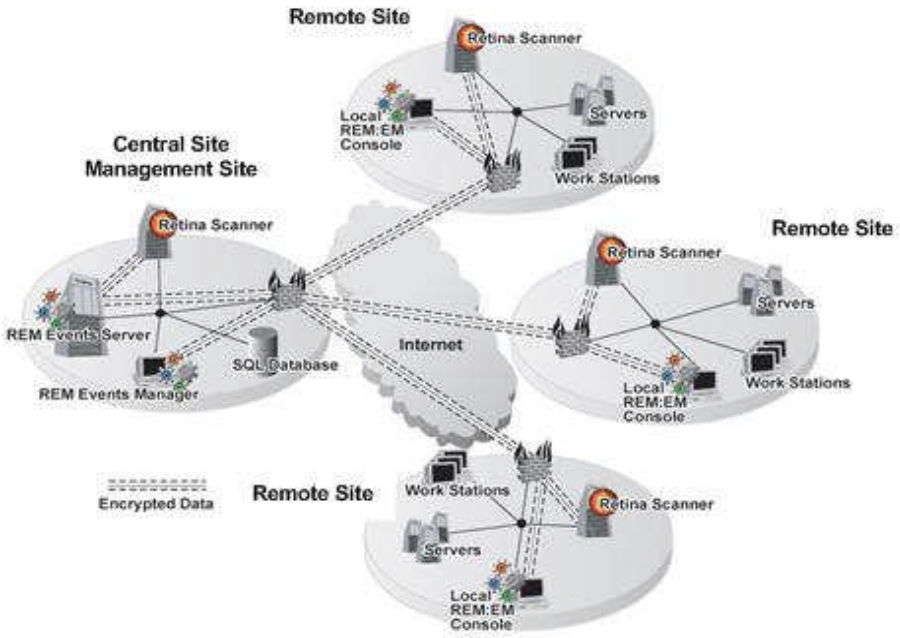
1. Ease of operation and install
2. Platform / OS vulnerability detection
3. Application vulnerability detection
4. Network identification and vulnerability detection
5. Access Control
6. Reporting
7. Performance
8. Cost

We also took into consideration the points listed in the SANS GSEC study guide in the chapter on Vulnerability scanning namely flexible product licensing, support CVE standard for cataloguing vulnerabilities, baseline reporting and executive reports [4].

While we could not find a product that excelled in all the criteria above, eEye Digital Security suite of products were selected based on quick reporting and remediation for lower cost and better operational success. Also besides scanning for vulnerabilities, eEye offers a comprehensive list of security audits to be performed on the target devices. These audits can be used to enforce internal security policies to verify such items as anti-virus deployments, approved machine configurations and application version control [5].

Architectural Components

To facilitate the Vulnerability Detection and Remediation Management process, the following eEye Digital Network Security products will be introduced into the environment. eEye products utilized in this architecture can be distributed as shown below.



Event Server - REM™

REM consists of an Events Server and Events Manager applications which centralize event management. These components typically reside on the same server.

REM™ Events Server

Events Server provides a secure virtual network for transferring predefined security events from eEye product engines — such as specific Retina vulnerability audits or particular SecureIIS events — deployed on remote machines across your enterprise to a centralized SQL database. REM Events Server can scale to handle large amounts of data transfer using a fast and secure delivery mechanism. The REM Event Server functions as a hub between the REM database and REM Event Clients. Each event created by an REM Event Client is sent via a secured connection to the REM Event Server, which in turn processes the event and inserts it into the REM database.

REM™ Events Manager

The Events Manager module of REM is the consolidated enterprise-level command center for monitoring, administering, and reporting on all eEye engines. The web-based REM Events Manager interface allows IT security staff to determine and address problems proactively and provide them with diagnostics data to quickly resolve issues across the entire enterprise. The interface also provides a number of useful reporting options as well as the ability to create custom reports that meet your organizational needs.

Scan Engine

Retina Scanner / Remote Manager

Retina operates as the vulnerability scanner, which runs on Windows NT/2000 and XP platforms. Retina has the ability to scan many types of operating systems for vulnerabilities, including Unix-based operating systems (Solaris, Linux, *BSD, etc.) as well as networked devices (such as routers and firewalls) that run "home-grown" operating systems. Retina includes vulnerability auditing modules for many systems and services that include but are not limited to: NetBIOS, HTTP, CGI and WinCGI, FTP, DNS, DoS vulnerabilities, POP3, SMTP, LDAP, TCP/IP, UDP, Registry, Services, Users and Accounts, password vulnerabilities, and publication extensions. Retina is able to audit databases and wireless networks for vulnerabilities. Scan results from Retina are relayed to the central REM Event Server via the REM Event Client interface. Retina Remote Manager allows you to configure Retina installations via a web interface. You can schedule scans, perform updates and set options remotely.

REM™ Event Client

The REM Event Client functions as a bridge between the REM Event Server and other eEye products. It accepts REM messages, and securely relays them to the REM Event Server.

Placement and Sizing

With the use of scanning technology, several sizing and placement factors must be considered. Key areas of consideration should encompass:

Network Bandwidth Availability

The Retina scanner “auto-senses” events from devices and network utilization as it scans. In geographical areas or sites where network bandwidth is limited, it is recommended that a scanner be placed at the site or within the LAN when necessary. This will increase the ability of Retina to obtain scan results in a timelier manner. Typical results from testing have shown that Retina will utilize approximately one to two percent of the given available bandwidth to accomplish a scan.

Firewall Placements

Retina will scan network devices and report any security vulnerabilities identified on those devices. In the case of firewall technology, as these devices are hardened, or for those reporting no vulnerabilities, it becomes impossible for a scanner to see past the firewall. A scanner must be placed within the intranet side of the firewall to allow for vulnerability detection of any devices located within that network space.

Scan Results Speed and Accuracy

The ability to get vulnerability results promptly proves to be a "moving target" and can be met by adjusting three key variables or decision points:

Scan Schedule

When will scanning be done and with what frequency? Timing and frequency play a large role in speed and accuracy of the detection process. The more frequently a scan is allowed to run, the more accurate the data is being reported and the less likely hood that a scan of the infrastructure within a single point in time would have to be executed. Timing plays a large role in accuracy. In the area of servers, scans must be scheduled to be run within a window when there is no scheduled downtime and when utilization is at its lowest. Likewise with desktops, scanning must be allowed to be performed at a time that they are connected to the network. Retina can be positioned to scan devices within the same window that other functions such as inventory, policy configuration, software distribution are delivered to the managed device.

Number of devices per Scanner

The speed and timing of scan results can be increased by utilizing more scanners with fewer devices to scan. If results must be received within a given period of time or time window, reduce the load of a given scanner by implementing additional scanners. Based on testing and general product guidelines, Retina can scan a class C (256 IP Addresses) within 30 minutes utilizing exhaustive connected and forced scan capabilities. The eEye optimized configuration built for non–intrusive, fast scans. Only scanning 1912 ports but including all the audits. Using the syn-scan and only scanning those hosts that respond to pings. Scans fast, but variables include:

- Slow links, network congestion or latency.
- Domain controllers where Retina must enumerate a large number of users.
- Hardware devices with poor IP stacks. (Common w/ all port scans).
- Low horsepower on the scanner machine.
- Non-sequential IP ranges.
- How many ports and services are actually open on the remote machine being scanned.

- The effective rights the Retina Scanner has on the network/local machine that is being scanned.

Variables outside the scope of the Complete scan policy are:

- Using connect scan mode.
- Using force scan mode.
- Performing a full port scan or adding more ports to the list (more than 1912).
- Scanning running CHAM.
- Decrease in standard performance or modules in Options.
- Increase in Ping Timeouts or Data Timeouts.

Scan Types

As more information is requested from the scan being performed with retina, the longer the scan will take. Scans can range from simple device discovery to scans utilizing common hacking attack methods (CHAM). The following benchmarks can be used in assessing scanner quantities and placement

Theory of Operations

Roles & Responsibilities

Vulnerability detection products should be able to detect vulnerabilities across multiple platforms, OS, applications, and networking devices. The product(s) should be capable of supporting multiple types of users and support their roles in the detection and remediation process.

Customer Interfacing / Management Status

Within the remediation process, senior management will be able to report vulnerabilities detected, new vulnerabilities identified and progress of the remediation process. Management will not only be able to report totals but be able to discern what areas of the enterprise may be experiencing difficulties in remediation and apply the proper resources or changes to the process to facilitate timely response. Data gathered will contain the adequate data points to facilitate these types of reports and should provide the tools to generate these basic reports.

Senior Security Advisory and Consulting / Security Operations

In the event of a vulnerability threat, Senior Security personnel must be able to compile a list of potentially vulnerable devices and report the impact in a timely manner. Security personnel, typically from a central location, perform analysis on a scale ranging from global, regional, site, subnet or individual host basis.

Any device must be able to be checked from an internal (intranet) or external (Internet or DMZ) perspective. When scanning from an internet perspective, a tool must provide common hacking methods, port scanning, and password detection capabilities to validate a devices configuration and the hardening of any OS or application.

Security Operations owns and operates the security architecture design outlined in this document. Responsibilities should include:

- System Hardening
- Device Monitoring
- User Access and Delegation

Administration and Remediation Personnel / Network Operations

Scan results must support the ability to group devices by owner and advise the owner accordingly to the vulnerability, the remediation process, and the ability to validate the success of the remediation. Once a vulnerabilities corrective action has been applied, a combination of tools and processes must support the validation of successful remediation. The use of port scanning, common hacking methods and other potentially hazardous scanning methods should be disabled for this user environment. These capabilities should be reserved for security personnel understanding the methodology, impact and risk.

Process Flow

Retina/REM provides flexibility, allowing the distribution of detection and auditing technology within the customer environment. This flexibility allows us to introduce this technology into existing support models with minimal impact.

- CERTS and vendor patch notifications are received on a regular basis to the security operations team. The introduction of Retina does not eliminate this required review and analysis, but rather supplies another avenue of notification of vulnerabilities as it relates to the environment being managed.
- As Retina detects vulnerabilities, events will be recorded in the Events Server. These events are reviewed by Security teams for prioritization and applicability.
- Notification or reminders are sent to identify program / engineering teams.
- Security Advisory with impact assessment and position published.
- Utilizing the supplied vendor patch to remediate the vulnerability, the patch is bundled and initial testing is performed. In the case of patch not being made available or a vulnerability relating directly to configuration, a patch will be developed, bundled, and initial testing performed.
- Upon completion of initial testing and bundling, the patch is submitted for formal testing and certification against all supported builds.
- With testing completed and certification received, the patch is promoted to production. In the event of testing failure, the bundle is rejected and sent back to the engineering / program teams for re-work.

- With change control approval, the bundle is applied to the effected devices.
- Upon application of the patch bundle, the device is validated for continued functionality and is re-scanned utilizing the localized scan engine for vulnerability elimination. In the event of a vulnerability remaining after the patch is applied, the appropriate engineering / program teams are notified for possible re-work.
- Administration teams, utilizing local reports, may detect vulnerabilities due to inadvertent configuration changes on devices or may have completed a patch installation which requires re-scanning the device manually or via a defined scanning schedule.
- Devices are scanned and results reported back to the local scanner.
- Events are sent to the regional or centralized REM server for further investigation and/or reporting.
- Report generated shows identified devices with no owners or contacts identified.
- Security Operations works with Network information to narrow down area/site and contact local or central administration teams. Report indicating unidentified devices can be sent to administration teams where large quantities are applicable.
- Database is updated with proper contact and owner information.

Reporting

Reports are aggregate event data presented in graphical format to help ascertain refinements in policy making and visualize trending in vulnerabilities throughout the enterprise.

There are three categories of reports, Event, Retina Specific and Task Reports. Event reports are snap shots that show the relative amount of work that needs to be done, has been done or will be done. Each report will detail its use when clicked on. For instance under the Agent, Task Status, and Severity report it will list the following:

This report displays events grouped by Agent, Task Status, and Severity. The information in this report provides a quick overview of unique agents and the severity of unresolved tasks for each

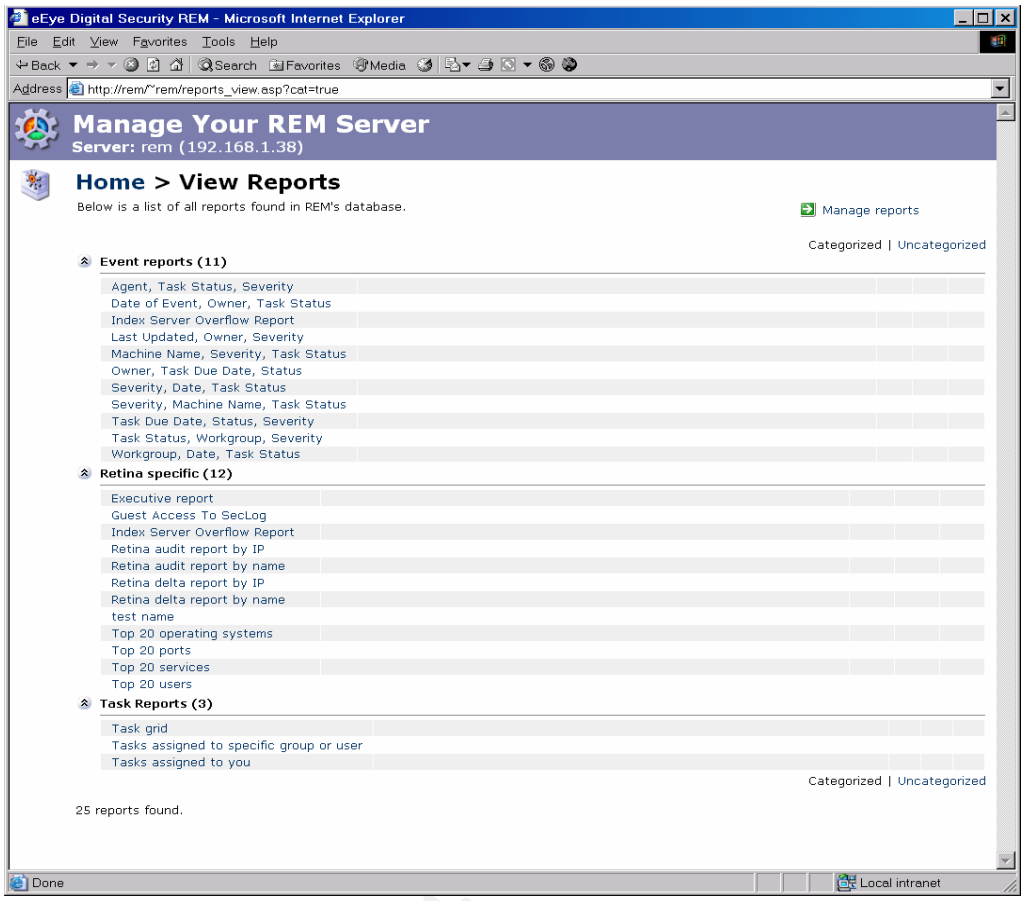


Figure 1 - Report Viewer Interface

Retina specific reports allow for useful visualizations of the vulnerability profiles for specific scopes. One of the more exciting pieces of data shown here are lists of network devices that are affected by certain vulnerabilities. As shown below the Audit Report will list all vulnerabilities found (within the scope of the user's group) and all the machines affected.

Figure 2 - Retina Audit Report

The executive report contains a quick visualization of the vulnerability threats over the last 30 days. This quick assessment is designed for executives who are looking for a fast trending benchmark which will allow them to make decisions based on increased of decreased threats from vulnerabilities.

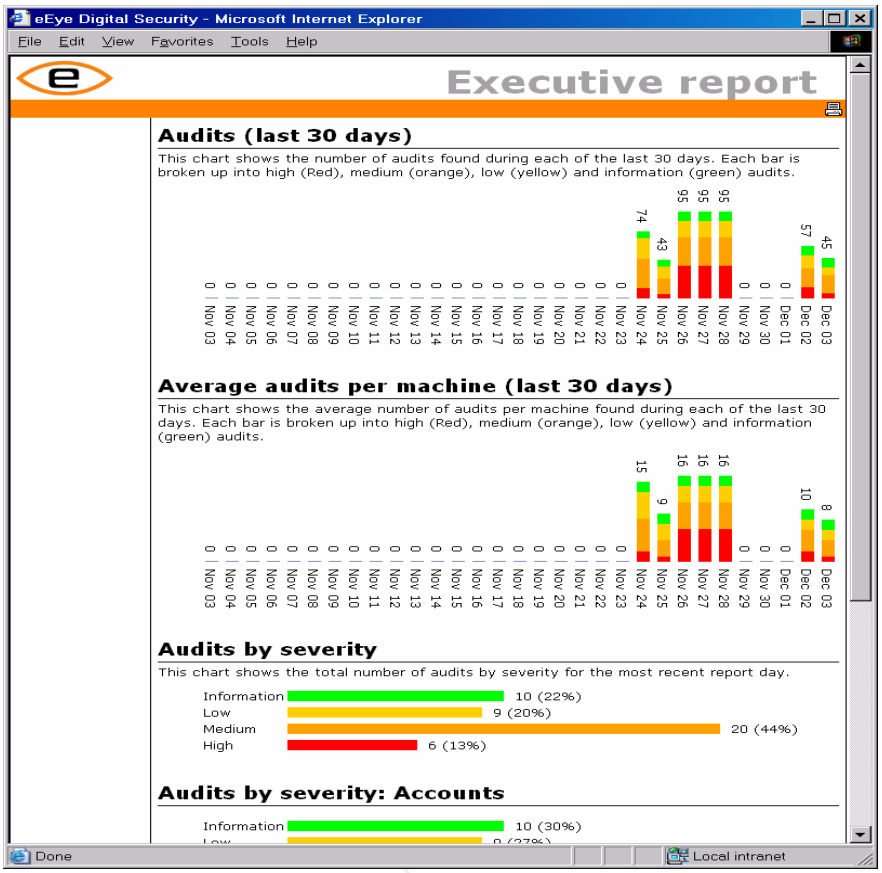


Figure 3 - Executive Report

Task reports are designed to give the user a quick sense of how far along specific remediation efforts are progressing. Individual, group, and total reports allow for flexible planning with concise information grids.

Security Definition

Access to the retina scanner is limited utilizing Domain or local user ID and administration. Access to the scanner should be limited to only those persons administering network servers and clients. Further control such as what can be scanned, what time a scan be performed, what type of scan is performed, is further defined in utilizing scopes. Scan reports are available locally and can be viewed via Retina remote manager for local administration remediation purposes.

REM access is controlled utilizing eEye (proprietary) internal user ID and password capabilities. The use of an internal access control is deliberate and is to provide limited access to the vulnerability data. This data, if not secured properly, could be used to compromise the infrastructure.

All data collected by each scanner is sent to the central REM server utilizing SSL capabilities. In addition, connection to a REM server can only be made with the appropriate PKI certificate.

Networking Considerations

Minimal 10MB connections are assumed to be available. This design takes into consideration the use of 1000MB (GigE) connections wherever available. It is minimally required to be utilized on all Event, Database and Reporting servers.
Retina has shown to utilize <1% of given bandwidth when performing a scan. Retina throttles the number of scans (IP Addresses scanned at once), and the speed of the scan of the device. Based on an algorithm which takes into consideration the speed in which a device is responding and the bandwidth available, care is taken to not degrade device performance and utilize maximum bandwidth available. These throttling options are configurable as required.

Firewall Placements

Retina will scan network devices and report any security vulnerabilities identified on those devices. In the case of firewall technology, as these devices are hardened, or for those reporting no vulnerabilities, it becomes impossible for a scanner to see past the firewall. A scanner must be placed within the intranet side of the firewall to allow for vulnerability detection of any devices located within that network space.

High Availability

Retina scanning engines perform independently and send results to the REM server when available. In the event of network, server, or database unavailability; the data will be stored local to the Retina scanner and data transferred to the REM server when available. In the event of a scanner failure, other scanners deployed in the environment can be directed to scan the failed scanners area of responsibility. High availability can be obtained by utilizing cluster servers but is not in this design and is an acceptable risk.

Summary:

As difficult as 2003 was for businesses battling waves of security problems, this year promises to be just as bad, perhaps worse, as additional threats develop from peer-to-peer file sharing software and spyware [(6)]. A quality tool should be able to detect vulnerabilities across multiple platforms, OS, applications, and networking devices. The tool should be capable of supporting multiple types of users and support their roles in the detection and remediation process. The implementation of eEye's suite of products will enable us to provide:

Senior Security Advisory and Consulting

In the event of a vulnerability threat, Senior Security personnel will be able to compile a list of potentially vulnerable devices and report the impact in a timely manner. Security personnel also will be able to utilize the tool from a central location, perform analysis on a scale ranging from global, regional, site, subnet or individual hosts.

Any device could be checked from an internal (intranet) or external (Internet or DMZ) perspective. When utilizing the tool from and internet perspective, it will provide common hacking methods, port scanning, and password detection capabilities to validate a devices configuration and the hardening of any OS or Application.

Administration and Remediation Personnel

Device groups will be setup with owners identified and the ability to advise the owner accordingly to the vulnerability, the remediation process, and the ability to validate the success of the remediation. Once a vulnerabilities corrective action has been applied, the tool and processes will validate the success of the remediation. Capabilities like the use of port scanning, common hacking methods and other potentially hazardous scanning methods will be reserved only for security personnel understanding the methodology, impact and risk.

Management Status

Within the remediation process, senior management will be able to report vulnerabilities detected, new vulnerabilities identified and progress of the remediation process. Management will not only be able to report totals but also discern what areas of the enterprise may be experiencing difficulties in remediation and apply the proper resources or changes to the process to facilitate timely response. Data gathered will contain the adequate data points to facilitate the various types of reports and provide the tools to generate these basic reports.

The securing of systems is not a single person or organization responsibility…."Security is everybody's responsibility" It is imperative that any tool selected be powerful enough to support security specialists and yet controllable to allow local sites and administration to stay current with the security of their environment. Any product must be flexible enough to allow for the unknown and possess the appropriate vendor support, expertise, and commitment to staying abreast and advising on any new vulnerabilities.

References

1. AL BERG, CISSP. February 2002. “VULNERABILITY MANAGEMENT FEELING VULNERABLE? If you're bedeviled by swarms of vulnerability alerts, you can take control by practicing good management”. http://infosecuritymag.techtarget.com/2002/feb/features_vulnerable.shtml.

2. “Welcome to Security”. http://www.eeye.com/html/Solutions/RetinaEnterprise/index.html

3. Novak, Kevin. 26th June 2003. “VA Scanners Pinpoint Your Weak Spots”. http://www.nwc.com/1412/1412f2.html

4. Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. **SANS SecurityEssentials with CISSP CBK**. Pg. 724.

5. List of Audits performed by Retina. http://www.eeye.com/html/Products/Retina/RTHs/index.html

6. Keizer, Gregg. 29th December 2003. “Security Threats: Bad In 2003, Worse In 2004?” http://www.securitypipeline.com/shared/article/showArticle.jhtml?articleId=17100252

Last Updated: February 20th, 2018

Upcoming Training

SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event
Mentor Session - AW SEC401	Melbourne, FL	Mar 01, 2018 - May 10, 2018	Mentor
SANS London March 2018	London, United Kingdom	Mar 05, 2018 - Mar 10, 2018	Live Event
Mentor Session - SEC401	Vancouver, BC	Mar 06, 2018 - May 15, 2018	Mentor
Mentor Session - SEC401	Grand Rapids, MI	Mar 09, 2018 - Apr 13, 2018	Mentor
SANS Secure Osaka 2018	Osaka, Japan	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, Singapore	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Paris March 2018	Paris, France	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CA	Mar 12, 2018 - Mar 17, 2018	Live Event
San Francisco Spring 2018 - SEC401: Security Essentials Bootcamp Style	San Francisco, CA	Mar 12, 2018 - Mar 17, 2018	vLive
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TX	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Munich March 2018	Munich, Germany	Mar 19, 2018 - Mar 24, 2018	Live Event
Mentor Session - SEC401	Studio City, CA	Mar 20, 2018 - May 01, 2018	Mentor
Mentor Session - AW SEC401	Mayfield Village, OH	Mar 21, 2018 - May 23, 2018	Mentor
SANS Boston Spring 2018	Boston, MA	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS 2018 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 03, 2018 - Apr 08, 2018	vLive
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201804,	Apr 09, 2018 - May 16, 2018	vLive
Community SANS Charleston SEC401	Charleston, SC	Apr 09, 2018 - Apr 14, 2018	Community SANS
SANS Zurich 2018	Zurich, Switzerland	Apr 16, 2018 - Apr 21, 2018	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Apr 16, 2018 - Apr 21, 2018	Community SANS
SANS London April 2018	London, United Kingdom	Apr 16, 2018 - Apr 21, 2018	Live Event
Mentor Session - AW SEC401	Memphis, TN	Apr 17, 2018 - May 17, 2018	Mentor
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WA	Apr 23, 2018 - Apr 28, 2018	Live Event
Baltimore Spring 2018 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Apr 23, 2018 - Apr 28, 2018	vLive
SANS Riyadh April 2018	Riyadh, Saudi Arabia	Apr 28, 2018 - May 03, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, IL	May 01, 2018 - May 08, 2018	Live Event
Community SANS Houston SEC401	Houston, TX	May 07, 2018 - May 12, 2018	Community SANS
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event