In the past few years, the number of security tools available to administrators has grown substantially. With the expansion of available solutions to solve immediate issues, the general “quick-fix” trend has created some decentralization in many corporate IT security departments. Today, enterprises are realizing the critical need to centralize and oversee security practices to ensure corporatewide network reliability. As a key component to every security practice, routine vulnerability assessments are an enterprise-wide priority and need centralized control.

After years of deploying firewalls and intrusion detection systems (IDSs), administrators have come to realize that these components alone are not enough to guard against attacks that take advantage of exposed vulnerabilities. Enterprise-based vulnerability assessment and remediation is now considered the next logical step in proactively securing network assets.

This article addresses the methodology required for successfully conducting, reviewing, and maintaining enterprise-wide vulnerability assessment and remediation.

**THE SECURITY ADMINISTRATOR DILEMMA: CONDUCTING DISTRIBUTED VULNERABILITY ASSESSMENTS**

Enterprise security administrators are faced with the daunting challenge of coordinating, implementing, and reviewing regular vulnerability assessments for...
all the digital assets across the entire enterprise. Often distributed around the
world, network intricacies specific to various divisions and regions have made
centralized network management of security practices increasingly difficult.
Many enterprises fail when it comes to running regular vulnerability assess-
ments and performing systematic remediation of identified vulnerabilities.
Often, scan results on hundreds of systems yield thousands of identified vulner-
abilities. The challenge for the central IT manager is consolidating this informa-
tion, eliminating false-positives, and assigning remediation tasks to other
administrators.

The addition of new security layers can also convince administrators that they
are somehow shielded from intrusion because of misconceptions that a certain
device guards them. This scenario is quite frequent when discussing Web server
security. Many uninitiated security professionals assume that because they have a
firewall and an IDS, their Web servers are well protected. In fact, they remain as
vulnerable as ever to Web-based attacks that have easily averted the network’s
IDSs. Likewise, in the world of vulnerability assessment technology, usage of var-
ious tools, scripts, and ad hoc testing routines often overlook critical network
weaknesses that could have been detected and corrected using a proven scanning
engine in a procedure-centric manner.

The CSI reports that the “average” company lost $4.5 million dollars in 2001
as a result of computer crime. While these numbers may sound high for small
companies, large enterprises know all too well that multimillion dollar losses as a
result of a network intrusion are not unusual. Furthermore, quantifying “exact”
figures for losses directly related to intrusion are quite difficult to calculate for
enterprises attempting to summarize tangible and nontangible costs.

In terms of being targeted for cyber-attack, it is no longer logical to assume
that a given business is safer than another (i.e., the “who would want to attack us”
syndrome). The random targeting of hosts by harmful worms has put a painful
end to that theory. Case in point, the CodeRed worm. In 2001, CodeRed alone
infected over 250,000 Web servers in its first nine hours and caused over $2.6 bil-
lion in reported damage. What was astounding about CodeRed was that the patch
to protect servers from this worm was released six weeks prior to the worm. How-
ever, more than one million servers were found by CodeRed to be unpatched
and vulnerable.

Although alarming, this data reinforces an ironic “bright side” to cyber-attacks.
CERT has reported that nearly 99 percent of all intrusions result from exploita-
tion of known vulnerabilities or configuration errors. In addition, 90 percent of all
Internet attacks are imitations. Essentially, cyber-attacks can be avoided if enter-
prises take the initiative to follow a strict policy of performing regular vulnerabil-
ity assessment tests and rectifying issues proactively.

Vendors have created enterprise vulnerability assessment and remediation
management solutions that integrate vulnerability assessment technology with
sophisticated event management systems. The combined solutions are called
Enterprise Vulnerability Assessments (EVAs). The EVA was designed to enable
large corporations to implement an effective, phased approach to vulnerability
assessment and remediation in an efficient, centrally managed fashion. The process consists of: Discovery, Audit, Delegation, Remediation, Analysis, and Adaptation. The process is ongoing and creates a closed loop for constant network threat management.

DEPLOYMENT ARCHITECTURE
Before reviewing each phase of the vulnerability assessment and remediation process in detail, it is important to review the deployment architecture associated with the process.

First- and second-generation scanning products were focused on just scanning. Built for stand-alone implementations, these tools lacked the scalability, management, reporting, remediation, and advanced performance capabilities required for enterprise-wide deployment. Conversely, today’s enterprise solutions were designed specifically for large-scale deployments and use proven scanning engines. This vulnerability assessment power, combined with an effective events management system, yields an effective solution for enterprise administrators. The events management portion of the solution enables comprehensive scheduling, reporting, assignment of remediation tasks, policy review, etc. — all perfect for large corporations in need of a complete vulnerability assessment and remediation management system.

Deployed in an enterprise setting, scanning engines can be remotely managed via a central console. All activities are reported to a centralized database that consolidates the information for analysis and remediation.

DISTRIBUTED NETWORK VULNERABILITY SCANNING IN AN ENTERPRISE ENVIRONMENT
As stated, there are several required elements in performing regular vulnerability assessments (VAs) in any environment, particularly in an enterprise where other variables (e.g., centralized management, efficient bandwidth utilization, and non-intrusiveness) must be considered. The remainder of this article describes each phase in terms of eEye’s approach to solving the distributed VA and remediation dilemma.

Discovery
For an organization to assess its network, it is important to understand the digital assets that make up the network. Therefore, the first step in the vulnerability assessment and remediation process is asset identification.

With EVA, asset identification is a completely automated, simple, unobtrusive process. The EVA can quickly determine all the elements, both active and inactive, on the network. The VA tool quickly identifies hosts and maps the assets. The EVA is able to discover all elements on the network, including:

- Firewalls
- Routers
• Switches
• Hubs
• Operating systems
• Servers
• Wireless access ports
• Desktops/laptops

To accomplish this discovery, the VA tool performs protocol analysis on DNS, FTP, HTTP, IMAP, LDAP, POP, RPC, SMB, SMTP, SSH, and Telnet.

Although elementary, the Discovery phase is an important first step in understanding the devices on a network. The VA tool quickly identifies and maps all of these elements in a centralized database.

Audit
Unquestionably, the most critical phase in the entire VA and remediation process involves properly auditing the entire network for vulnerabilities. In any business, especially complex organizations, the audit phase must be:

• Fast
• Nonintrusive
• Accurate
• Bandwidth efficient
• Customizable
• Easy to initiate
• Decipherable
• Centrally organized
• Remotely maintained

Without a powerful auditing engine, the entire vulnerability assessment and remediation management process may be severely flawed. It is imperative that the engine be the best available and supported by consistent and reliable vulnerability research. EVA tools require comprehensive auditing capabilities and unparalleled speed, accuracy, and ease-of-use.

Deployed in an enterprise setting, VA engines should be able to be remotely managed via a central console. All activities are reported to a centralized database that consolidates the information for analysis and remediation.

During the Audit phase, each VA engine must perform normal and specialized scans to proactively detect vulnerabilities and report all issues to the centralized database. Each VA engine must fulfill the Discovery and Audit phase for its respective subnet. VA engines should be flexible and provide multiple configuration options (e.g., by location, by division, by IP range, etc.), according to network topology permissions or needs.
As mentioned, a centrally managed control panel should enable individual VA instances to scan their subnets. All findings should be securely transmitted to a database within the EVA so the Review phase can begin.

Delegate and Remediate

In conventional VA applications, the ability to conduct centralized review scanning results was a laborious, inaccurate process. With EVA, the process is completely automated and enables the primary security administrator to easily examine vulnerability reports and instantly pinpoint critical issues or trends.

For example, a company may want to view its security status versus the SANS Top 20 Vulnerabilities across the network. Custom reports can be configured for that purpose by analyzing the scan data in the events database.

VA tools must offer a full suite of automated reports that can be sorted, depending on the users needs, and analyzed against previous results. In addition, EVAs should produce customized reports built upon event data collected from all engines reporting to the central database. In addition to reports produced from the management console, event data can be exported for use in any open third-party reporting or events management application.

The management console enables the central IT administrator to check on the status of assigned remediation activities. Reports outlining corrected versus non-corrected vulnerabilities can be quickly generated.

An extension of the Review phase involves the assignment of tasks (e.g., corrective actions) to IT personnel or remediators. Management capabilities should enable administrators to assign tasks to IT personnel (remediators) throughout the enterprise for corrective action. The EVA automates the process by accounting for each vulnerability and establishing a trouble ticket with corrective actions needed. Furthermore, the trouble tickets can be automatically sorted and assigned to individual administrators for remediation by establishing rule-based filters in EVA. Therefore, numerous vulnerabilities can be instantly broken down and delegated to remediators based on their geography, skillset, etc.

The EVA employs a sophisticated remediation workflow process that guides administrators through remediation efforts and tracks the entire procedure from a centralized database. Utilizing a trouble ticket approach, administrators are assigned tasks and given complete instructions regarding the nature of the vulnerability and how it can be resolved. Comprehensive reporting enables prompt resolution of vulnerabilities. As these vulnerabilities are corrected, the central database is updated and verification of these fixes occurs.

Third-party remediation packages can be utilized to fully automate remediation and integrate into the process. With the configuration approval of the network administrator, these packages will automatically perform fixes or remediation to network vulnerabilities and create reports summarizing all actions taken.
Analyze and Adapt
Once a difficult task, determining if vulnerabilities have been corrected company-wide is a simple task with EVA. Reporting, trend analysis, policy settings, and resource management are all administered through the central command console. EVA incorporates a range of useful features, including a unique “Delta Reporting” feature that will quickly enable administrators to gauge the effectiveness of their remediation efforts. Through this report, new scans are compared to historical ones to assess the rate of progress by area or administrator.

Because all testing results are reported back to the central database, instant differential reports can be generated to clearly depict successful remediation efforts across the enterprise.

Verification of corrective actions occurs via launching — or relaunching — a scan to determine if the vulnerability still exists. New scans can be comprehensive or initiated within certain divisions or subnets to test specific issues without impacting the entire network.

THE COMPLETE PACKAGE
Vulnerability assessment and remediation management systems that handle the complete process — from the asset identification and auditing phase, through the review and remediation stage, to final verification of fixes — have a high value proposition. EVA manages the entire process and minimizes the resources needed to undertake this critical security initiative.

When looking at a solution, there is a minimum set of features that must be provided. This set includes:

- **Best-of-breed scanning technology**
  - Intuitive and easy to use
  - Nonintrusive scanning
  - Frequent updates for new vulnerabilities
  - Ability to uncover unknown vulnerabilities
  - High-speed scanning ability
  - Advanced scanning technology (CHAM)
  - Remote repair capabilities
  - Advanced scheduling capabilities
  - Comprehensive and up-to-date vulnerability database
  - OS detection
  - Smart protocol scanning
  - Open architecture
  - Audit wizard
  - Advanced and Customized Reporting Capabilities

- **Distributed Enterprise Manageability**, an agent-based technology that enables enterprises to have immediate and reliable access to the status of autonomous network security events. The central console should manage event logs and complete vulnerability assessment and remediation tasks, including:
- Rapid deployment
- Full vulnerability assessment capabilities
- Total remote management capabilities
- Event ticket tracking and remediation management
- User administration
- Encrypted communication channel
- Open architecture

Rich Brazeau is Director of Marketing at eEye Digital Security.