

## Vulnerability Assessment: It's not just about scanning

**By Mitchell Ashley, CTO and VP Customer Experience**

*Originally published in CyberDefense Magazine, April 2004*

Vulnerability assessment, frequently referred to as VA, is rapidly becoming a standard practice for security-conscious organizations. Best-practice techniques test for and discover security holes in an organization's network infrastructure. Many IT departments have incorporated vulnerability assessment products into their security toolset to satisfy regulatory and auditing reporting requirements.



The state of the art has evolved from a tedious, manual process to one that is highly automated. While a wide variety of commercial and open-source scanning tools are available, their level of automation and process management varies considerably. Herein lies the problem: How to transform the traditionally labor-intensive vulnerability assessment process into a scalable vulnerability management system that incorporates and ensures vulnerability repair.

### **The drawbacks of a manual VA process**

Traditionally, VA was performed by a third party, such as a security consultant or auditing firm, on an annual basis. The VA audit was performed by an engineer using a variety of port mapping, vulnerability scanning, and general TCP/IP utilities (that were usually free, open-source tools). These efforts produced large reports detailing each device, the services and ports available, and any vulnerabilities or configuration issues existing at the time the scan was performed.

Performing VA audits through this type of process had (and still has) a number of inherent flaws. In today's environments, computers and network devices, their configurations, and the ever-growing list of vulnerabilities are rapidly changing. A point-in-time snapshot of network security is obsolete the moment the assessment is complete.

To combat this issue, many network and security engineers have taken VA assessment in-house. They run commercial and open source VA tools on their own. While this approach provides a more frequent security snapshot, it is still a manual process. There is little value unless the IT staff runs the assessments frequently and actually takes the time to correct the identified vulnerabilities.

A more significant problem is the delivery of the assessment report only marks the beginning of the real work. The network vulnerabilities discovered in the audit now need to be fixed. Additionally, processes must be implemented to ensure that these problems don't reoccur or become "undone" as a result of future software upgrades and device configuration changes. Often the effects of such changes are difficult to track due to overlapping and split organizational responsibilities and the fast-paced dynamics of the network and computing environment.

To make VA a truly valuable, sustainable process, systems are required that provide ongoing, systematic scanning, immediate notification, tracking of security vulnerabilities and their respective repairs, and the creation of a detailed audit trail.

### **Internal, external, or both?**

Historically, VA assessments have been performed from outside the firewall, testing the security of the network's perimeter defenses. The proliferation of rapidly spreading worms and trojans such as MyDoom (Novarg.a), SoBig, and others have shown just how susceptible networks are to attacks from inside the network. Many email attachments, instant messaging clients, and peer-to-peer applications pass traffic through the firewall unabated, allowing the sharing of files and distribution of attacks directly into the network. Remote and mobile devices also present significant risks as they are frequently exposed to other networks and can act as the delivery vehicle for attacks when connected to the internal LAN.

Network security is no longer something that lives primarily at the network perimeter. Network security must be viewed from all points of entry into the network: desktops and laptops, remote access (VPN and dial-up), connections to third-party networks, and wireless access points.

This comprehensive approach to security requires that tests for vulnerabilities be performed from points within the network as well as outside the firewall. The goal is to eliminate or minimize all security holes; by doing so you protect the network from both external and internal attack.

### **Essentials for vulnerability management**

In today's hostile environment, single-point solutions and a casual approach to vulnerability management are not enough. In 2003, CERT reported that 90 percent of large firms and government agencies detected computer security breaches within the last 12 months. Additionally, 99 percent of security breaches resulted from known vulnerabilities and misconfigured devices. Clearly, more than just vulnerability scanning tools are needed to effectively prevent networks from being compromised. If new vulnerabilities are to be identified and addressed in a timely manner, then automated processes are required.

The solution for streamlining this important component of network security is called "vulnerability management" -- a system consisting of processes, software automation, and a secure information repository. The key characteristics of an effective vulnerability management system include:

1. Frequent, regular scans for vulnerabilities that adjust to the business importance, risk level and location (geography, internal/external) of devices on the network.
2. Systematic, schedule-based scanning that accommodates network, computer and business operations schedules.
3. Updates to scan rules and algorithms (much like the automatic update of virus signatures in antivirus software) that check for the latest vulnerabilities and exploits.
4. Assignment, notification, and tracking of repair tasks to the appropriate system or security personnel.

5. Automated scheduling of critical personnel resources to perform the repair tasks.
6. Readily available information resources and industry references, such as CERT and SANS Institute, to assist in the investigation and repair processes.
7. Application of software patches and fixes for known vulnerabilities.
8. Verification that repairs have eliminated or mitigated the vulnerability risk.
9. Information preparation and report generation to meet the needs at all levels of the organization: senior management, security and IT management, security engineers, auditors and external regulatory reporting.
10. Audit trail of processes (including scanning, tracking, repair, verification and reporting) to demonstrate proactive and prudent attention to security vulnerabilities.

Today, accomplishing many of these key functions is a labor-intensive effort. A closer examination reveals the need to scale these processes. Using manual methods to manage the information needed to track, repair and report vulnerability repair progress in a network of thousands or tens of thousands of devices rapidly becomes impractical. It is common for vulnerability scans to uncover tens, even hundreds of vulnerabilities for each computer or network device. Automated tools and processes are vital to staying on top of the most critical vulnerabilities and ensure the network is protected.

### **Special considerations for a large enterprise**

Vulnerability management within a large commercial or government enterprise brings additional challenges. It is easy to think that large enterprises merely have to deal with a much larger number of devices. The SANS Institute recently reported on the vulnerability management efforts at NASA. Between 5 and 30 vulnerabilities per system were found, resulting in over 50,000 vulnerabilities to repair. The ability to prioritize the most critical vulnerabilities and then assign the resources needed to implement repairs was crucial to NASA's success.

While the number of vulnerabilities requiring attention can be quite large, the greater challenge is supporting the diverse set of organizational structures, responsibilities, and accountability relationships. It is common in larger organizations for a centralized security team to perform the vulnerability scanning tasks, but not be responsible for repair of the vulnerabilities identified. A variety of system administration and operations groups throughout the organization are then allocated to the repair tasks. These repairs may be performed by different divisions of the IT organization, system administrators within the business units, or by subsidiaries and companies owned under the corporate business structure. Verification that repairs resolve the vulnerability may then again be the responsibility of a central security team. These overlapping and poorly defined areas of responsibility can cause tremendous inefficiencies and lead to security holes.

Automated processes are essential to manage the chain of accountability in large, diverse organizational structures, information flow between departments, assignment and performance of repairs, verification that vulnerabilities are no longer a risk, and auditing requirements to document due diligence within organizations. Vulnerability

management systems are critical to assisting each part of the organization with their role in removing or mitigating this risk.

### **It takes a system**

Vulnerability management isn't just about using scanning tools. Effective vulnerability management requires a system of security processes, automation, resource management, and the right set of vulnerability management products and processes to ensure accountability for repairs. Large enterprises face additional challenges in meeting these objectives.

Consider the list of vulnerability management essentials as you put your processes and software tools in place. A little bit of planning and well-thought-out execution can save volumes of work and the associated costs when the next MyDoom or Blaster worm shows up in the news reports or worse, takes advantage of vulnerable devices on your network.

### **About the Author:**

Mitchell Ashley is CTO and VP of Customer Experience at StillSecure. He is responsible for the product strategy and development of the StillSecure suite of network security software. Mr. Ashley has more than 20 years of experience in data networking, network security and software development. He can be reached at (303) 381-3830.