
Network Computing

Security

BUYERS GUIDE

Vulnerability Assessment Scanner Enhanced Vulnerability Detection

A comprehensive security program should include a vulnerability assessment scanner, which can help decrease IDS false positives as well as with asset tracking. Here's what to look for.

Aug 4, 2005 | By Jordan Wiens

Vulnerability-assessment tools can do more than search for potential security problems. A VA scanner can make IDS data more useful, help with asset tracking, and even delegate and disseminate security data.

VA tools are not new--they've been around more than a decade--but improvements continue to expand their functionality within the security infrastructure. In the past few years, passive vulnerability detection and security data integration, for example, have changed the way VA data is used. Those developments are not unrelated--one supports the other. Without passive detection, client-side vulnerabilities can remain hidden from active scanners, and vulnerability detection is less effective if it doesn't integrate all the data retrieved from various sources.

Passive, Aggressive

The term passive vulnerability scanner is a misnomer. Nothing is scanned, so it would be more accurate to call it a vulnerability detection system. Also, passive vulnerability assessment sounds like market speak for an intrusion-detection system. But there are some similarities between the two types of products: Both are passive devices that monitor the network to identify security-related data, but the type of data each searches for is different. An IDS mainly detects intrusions (no surprise there), while a passive VA product identifies vulnerabilities in any client or server visible in the network traffic, where many vulnerabilities are discovered, or at least guessed. A vulnerable Web browser might be detected from both its user-agent string and certain behavioral characteristics on the network, for example, but it can't be detected with a conventional vulnerability scanner without local privileges on the host.

The downside to a passive approach is that quiet servers or clients aren't detectable. In this case, a passive vulnerability system can become the equivalent of an IDS, indicating a vulnerability only as it's exploited instead of helping to prevent it. Therefore, it's unlikely that active VA tools will be totally replaced by passive systems. Both passive and active VA products can--and should--co-exist in any thorough security program.

Use It Well

The effectiveness of vulnerability data lies in how it is used. One application could be making an IDS more intelligent. Having an automated system to tie together information about each scanned system's vulnerabilities, along with the specific attacks it receives, results in a dramatic decrease in IDS false positives.

Additionally, several products, such as StillSecure's VAM, can track local administrators within a large institution, allowing association of IP ranges or hosts with those responsible for them. Other products are designed to work with management software to achieve the same purpose. In this way, an enterprise vulnerability scanner can be used more effectively by the administrators who should be receiving the data. Some environments may have an external database for storing such information and credentials; if so, make sure the VA product you choose can authorize and authenticate with that data.

Another tangential benefit of VA data is the ability to track assets. If you're planning to buy a separate product to do this, you might be able to save money using a VA product with this functionality.



Go Deep and Wide

Some VA products offer a deep level of detail and proof of specific vulnerabilities. Extra information--such as a list of local user names, for example--can provide concrete proof that a host has not locked down remote queries. This makes it easier to demonstrate the vulnerability to administrators and be assured the result is not a false positive. All VA products include some level of proof; the required level depends on your environment.

Consider the total size of the vulnerability database. Numbers can be deceiving, because some types of vulnerability checks may be more relevant than others. In a Windows environment, for example, Windows-specific vulnerability checks may be more useful data than the total number of checks.

Another important factor is the level of access required. Many VA products can take advantage of administrative credentials to log in and remotely verify patches or versions. Although this is in the realm of patch-management tools, it's also a very effective way for a VA product to determine if a host is vulnerable. In many environments, however, local credentials won't be available to the scanner, so be sure you make the method of remote checks a high priority.

Providing administrators with usable data depends on the quality of the reports generated. If you're interested in tweaking the information you get, look for a product that offers flexible and customizable reports. A good vulnerability scanner can graphically demonstrate the total vulnerability surface of your environment, which you'll see decrease if the VA data is put to good use.

Vulnerability scans can cause problems with older operating systems and some embedded devices, so if your environment has several critical devices that must remain available, you may need a VA product that's more cautious in its scanning. Some environments, however, may require a more aggressive scanner, so you can find out if a host is susceptible to a DoS (denial of service) when you--not an external attacker-- are driving the scan.

Find and Fix

Ultimately, a VA product doesn't just find vulnerabilities, but helps fix them. Therefore, evaluate the quality of a product's remediation information and its ability to track patching status. In environments where servers are maintained in a distributed fashion and the level of system administrator abilities is uneven, the quality of remediation information is crucial to help less experienced staff easily patch and secure discovered vulnerabilities.

If your organization has strong change-control methods, you probably have the tools to track vulnerability patching, but if not, look for a VA product with this capability. Products most likely to have this ability are those that integrate with SIM (security information management) platforms. Others may integrate this kind of patching into an all-in-one product, such as **StillSecure's VAM**.

Many VA products are licensed based on the size of the network to be scanned. If you have a very large network, or often add or remove IP spaces from your network, you'll likely benefit from an open key that lets you scan any address. Much like antivirus or signature-based IDS, a VA product can quickly grow stale without regular updates. Make sure you account for the cost of a support license that includes an updated vulnerability database.

Passive and active VA products are both important pieces in a security program. They can be used in conjunction with other security products to help minimize the overall vulnerability surface. Look for ways that vulnerability data can be integrated into the management of your network and a VA product that supports those methods, and you can be sure your investment will continue to grow and adapt to future uses.

Jordan Wiens is a network security engineer at the University of Florida, where he works on IDS/IPS, forensics, VA and system security. Write to him at jordan@psifertex.com.

©2005 CMP Media LLC. All Rights Reserved. A [United Business Media](#) company.