



TenStep Supplemental Paper

8 July 2005

Vulnerability Assessment Services on the Rise

Like most markets these days, the vulnerability-assessment market has a new services-based component.

Using these services, organizations can remotely scan their network perimeter or demilitarized zone to identify known vulnerabilities and security weaknesses. With this approach, networks can be easily analyzed from the perspective of the outside attacker at a much lower cost than hiring a consulting firm to perform a penetration test. The information then can be used to improve the security on those Internet-facing systems. Some services even provide the means to scan internal systems, a task that was previously left to point products like the ones in our review. The leading vendors in the vulnerability assessment services market are Qualys, Vigilante, Foundstone and McAfee.

With these services, scans can be scheduled, by the enterprise user or the service provider, to run automatically, with reports e-mailed to a designated user or stored on a secure server for review. Many reports include a differential analysis to help you see how your security posture evolves over time. Foundstone offers this type of consulting.

Qualys and Vigilante focus on providing just the assessment-scanning services and then sell that service to other outfits, like consulting firms, who then brand the vulnerability-assessment services as their own. For example, NCC Networks provides vulnerability assessments to their clients using the Qualys scanning engine.

One major benefit of online services is the lack of updates. Because the service provider runs everything, it can develop signatures and updates for new vulnerabilities and automatically include them in the next scan. You do not need to perform any updates. As for the timing of updates, service providers typically have the resources to get a new update deployed within a few hours.

Because these services contain data about your network that any hacker would love to find (it prevents them from having to do all the work), reports are stored in encrypted databases and only accessible with the proper user credentials. While the data must be saved to generate comparison reports, not all services keep individual reports available. Vigilante's SecureScan creates a PDF report that is only stored on their systems for 14 days.

Like their shrink-wrapped counterparts, online vulnerability scanners take different approaches in how they determine whether a vulnerability exists on a system. Foundstone takes an analytical approach and ensures a vulnerability actually exists on a system before reporting it. This greatly reduces the number of false positives, but it also does not give you the big picture.

Foundstone sacrificed some detailed information, such as general service messages (for example, that Telnet is running on this system) to focus on vulnerability identification. In reporting, most services provide more information on system configuration, such as



TenStep Supplemental Paper

default Microsoft's Internet Information Server directories. While these are not specifically defined vulnerabilities, they can provide information and avenues of attack.

Other online scanners, such as Qualys and Vigilante SecureScan, use open source tools, such as Nmap and Nessus, combined with in-house developed tools. SecureScan takes this even one step further and combines existing commercial scanner products into an online service.

Assessment services are ideal if you are looking for a hands-free, regularly scheduled scan of your Internet-facing devices; do not want to be concerned with keeping up-to-date with newly identified vulnerabilities; or want a third-party constantly helping you evaluate and monitor your network.