

## ***SCANNING TOOLS VERSUS VULNERABILITY ASSESSMENTS***

Chris Goggans

We are often asked what a true vulnerability assessment offers that would not be available to customers using a commercial tool such as ISS or Nessus. While these tools are extremely useful as aids in initial discovery and compliance checking, they are not intended to be an “audit in a box.” We often use such tools as part of our assessment process. However, using them *instead* of a comprehensive professional assessment can produce dangerously misleading results. The comments below summarize just a few of the reasons why scanning tools alone are not sufficient to determine an enterprise’s vulnerability baseline.

### ***Blind repetitive testing***

Tools are created to provide a base level security inventory of corporate resources. They are very effective at conducting repetitive tests across a large number of network hosts. Unfortunately, they are unable to dynamically determine which tests are applicable at which hosts. Instead, most commercial tools produce voluminous output, testing every target host for every possible apparent vulnerability. This leaves the customer in the position of wading through extensive reports and attempting to prioritize and correlate the findings.

There is also an issue regarding how these tests are actually implemented. There are no standards regarding how these tools check for vulnerabilities or how they determine what constitutes a vulnerability. Despite this, most companies institute a policy of utilizing these tools without a full understanding of what they truly do. In a recent test of scanning technology, two implementations (NT and Solaris) of the same version of a commercially available scanning tool were run against the same target host. Both of these implementations performed their scans quickly and efficiently and each provided what appeared to be consistent results. Unfortunately they were consistently different from each another. The fact that two versions of the same product produced different results illustrates the dilemma facing those who rely solely on commercial tools. A user who runs a single tool and believes he has a reliable baseline may be dangerously misinformed.

With a full vulnerability assessment report, not only are assessments done using a consistent base set of proprietary and commercial assessment tools, but the results are analyzed and reported by experienced computer security professionals. Findings are presented with emphasis on explanation of the threat and steps needed for remediation.

## ***Testing repertoire lags the threat***

Scanning tools must be continually updated to be effective. They resemble virus scanners, in that both must constantly strive to incorporate the newest threat into their recognition software. Unfortunately, unlike viruses, the newest hacker attack is often the most widely used, and therefore one of the biggest threats to consider.

Recently, a regional Internet service provider suffered an attack. This provider, a well-known repository of computer underground information, was a constant target of thousands of attacks. This provider had access to numerous tools to check the security of their installations, made use of OpenBSD (one of the more secure UNIX variants), and provided diligent security reviews of their systems. Over a weekend, an exploit tool specifically coded for the OpenBSD Qpopper was released, and was immediately used to gain access to this provider and replace the login program with a Trojan horse.

Our consultants work hard to address the latest threats in every assessment. The difference is that while commercial products require time to design, implement, and distribute a software upgrade, our consultants can immediately add a separate tool or program into their test repertoire, sometimes even while an assessment is in progress. By not relying solely on commercial tools, we have the flexibility to check for the latest and most severe threats to corporate computing environments.

## ***Limited exploitation capability***

Most tools do nothing more than conduct a basic “surface” scan. They check service banners for version information and consult a database of known vulnerabilities to determine the “possibility” of weakness. Further, most commercial scanning tools do not understand vulnerabilities outside the TCP/IP realm. Our team has expertise in a wide range of alternative and legacy network infrastructures. Services using network protocols such as SNA, IPX, DECNET, and others must be examined during an assessment. Most commercial tools lack the ability to examine anything other than TCP/IP and are not sufficient for assessing large enterprises.

On most vulnerability assessments, new potential weaknesses are uncovered. On one assessment a service offering a bridge between IPX and IP networks was discovered and successfully exploited to attack NetWare Servers over the Internet. Commercial scanning tools would have passed over this highly significant vulnerability. On other assessments, modems, terminal servers or additional services have been found running on several Cisco router TCP ports (2001, 4001, 6001, and 9001). Scanning tools generally pay no attention to these ports. As a final example, back-door programs allowing unauthorized access have been found on unregistered ports. While some scanning tools check for the common ports used by some hacker tools (e.g., 31337), most lack the ability to check for backdoors on all unusual ports.

On a full vulnerability assessment, actual attacks are executed against target hosts and services to determine if a vulnerability truly exists, regardless of version or banner

information. Furthermore, a true assessment will examine vulnerability state on all networked devices irrespective of protocol or operating system. All network devices are probed, including printers, hubs, routers, x-terms, terminal servers, network modems as well as standard servers and workstations. This is critical since low-priority devices such as network printers may still disclose important information such as SNMP community strings that will be useful to an attacker. All services are examined for potential vulnerability, even those services operating without the customer's knowledge. By not relying solely on a database for analysis, our consultants can ensure a much more thorough assessment.

### ***No ability to integrate external information to “create” vulnerabilities***

One of the most useful tools the attacker has is the human brain. A human can find inroads to a system that no tool can hope to uncover. Information about a company or a system may be found in places that are not accessible by automated scanning tools, yet that very information may hold the key to successful penetration.

While performing a recent vulnerability assessment, scanning tools and generic attack tools were wholly unsuccessful in uncovering security vulnerabilities. Most services were disabled, and those that were active (Microsoft's POP server, a firewall TELNET proxy and a firewall FTP proxy) were secure versions. Since the POP server was active, searches of Internet WWW servers and news groups were conducted and employee information and email addresses were uncovered. It was then discovered that the firewall's TELNET proxy responded differently to valid usernames than to invalid usernames during the authentication process. These valid usernames were then subjected to a brute force password attack on the POP server, since most POP servers do not track invalid authentication attempts. Using the assumption that many users would have the same password across services, discovery of a valid POP server password could be the key to accessing other services. The lack of user password discipline proved to be a vulnerability, but one which no scanning tool could have detected. For a human attacker, however, the integration of data acquired via an external “discovery” process would have been routine, and represented a significant vulnerability to the enterprise.

### ***Summary***

There is certainly a place for commercial assessment tools in a sound network security plan. They are invaluable for compliance checking, and can provide an inexpensive way to conduct limited recurring audits. They are not, however, an “assessment in a box”, and relying solely on a commercial tool for vulnerability assessment is not recommended. These tools, like many others such as firewalls and intrusion detection systems, are best deployed as part of a multifaceted security strategy that includes periodic professional vulnerability assessments.