

# Foundstone Specialized Assessment Modules

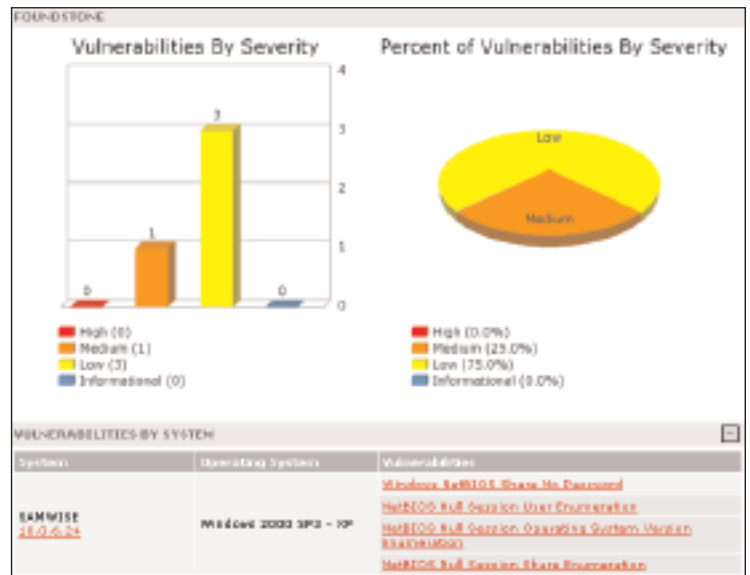
## Summary

Foundstone's specialized assessment modules compliment Foundstone's standard vulnerability checks to identify the toughest security weaknesses. Specialized individual modules uncover critical Microsoft Windows® and Web application vulnerabilities missed by other products, and provide comprehensive discovery and assessment of wireless access points. With the lowest false positive percentage in the industry, Foundstone produces results you can trust.

## Windows Assessment Module

Foundstone Enterprise's Windows Assessment Module offers a detailed, scalable analysis of Windows hosts across networks without the installation of agents on host machines. Using this module, users can enter and maintain multiple administrator credentials (i.e., usernames and passwords for domains, workgroups and individual hosts) to allow for analysis of issues that are typically provided by host-based scanning products, such as detailed patch levels and policy settings. When scanning, the credentials the user has loaded into the system are presented to target hosts prior to vulnerability analysis, providing the FoundScan Engine™ increased access to identify weaknesses and violations. Foundstone technology identifies vulnerabilities that solely network-based scanners commonly miss:

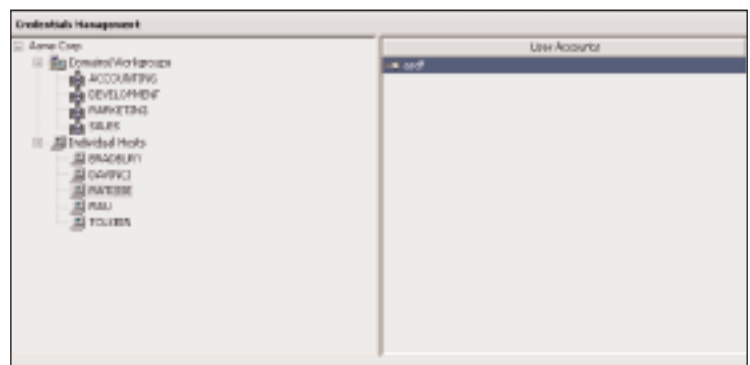
- Presence of peer-to-peer and instant messaging applications (e.g. Kazaa, ICQ, iMesh)
- Presence of desktop modems and multi-homed machines
- Outdated or missing A/V S/W
- Web browser policy compliance problems
- Missing hot fixes and service packs



Most vulnerability assessment products force the administrator to create “god” accounts that span all domains or the entire Active Directory forest. Needless to say, this approach to scanning poses a major security risk. An unauthorized user with access to a “god” account literally has the keys to the kingdom.

This method also creates significant operational headaches. Fortunately, the credentials management capability in Foundstone's Windows Assessment Module eliminates the need for “god” accounts, saving time and reducing your security risk.

The Windows Assessment Module also addresses another common pitfall of most traditional scanners, which cannot determine the access level achieved on each machine during a scan. This creates uncertainty—or worse, misplaced confidence—regarding scan results. If a scan comes back “clean,” was a vulnerability truly not present, or did the scan lack the privilege level required to detect it?



Foundstone's Windows Assessment Module reports discovered vulnerabilities and the level of access gained on each host during a review. By knowing exactly what the Windows Assessment Module accessed during a scan, you have complete confidence in its results.

Through use of the Windows Assessment Module, users gain the information they need to improve their Windows security health without the burden of deploying hundreds or even thousands of host-based agents.

**Web Application Module**

Even though your network may be protected by firewalls and an intrusion detection system, you have to let customers, partners, and vendors through the front door—your Web site. Unfortunately, security testing and secure programming are common casualties during application development due to time, budget, or other constraints. Foundstone's Web Application Module provides a detailed inventory and examination of Web servers and applications for commonly overlooked yet increasingly important vulnerabilities.

Foundstone's Web Application Assessment Module provides focused testing of vulnerabilities that otherwise requires the purchase and knowledge of a separate product. By integrating into the core system the capability to crawl and assess Web applications, users can view these "unknown" and often overlooked vulnerabilities with their network or host-level weaknesses.

The Web Application Assessment Module provides an overall summary as well as detailed report in each of the following areas of testing.



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Web server and Web application inventory:</b> Crawls Web servers and their contents for identification and analysis, resulting in a categorized listing of Web servers and the objects residing on them.                                                                                                                                                                                                                                                     |
| <b>Source-Sifting:</b> A detailed analysis of the source of scripts and static pages discovered on analyzed Web servers that reflects discovered database connection strings, e-mail addresses, hidden form fields, and other potentially sensitive items.                                                                                                                                                                                                      |
| <b>Authentication Testing:</b> Discovery of weak usernames and passwords (easily guessed or default accounts) found in web applications such as e-commerce store fronts, extranets, and web-based administration interfaces for network devices.                                                                                                                                                                                                                |
| <b>Source-Code Disclosure:</b> Through a combination of missing Web server patches or misconfigurations coupled with the Web application inventory, Web scripting source code can be presented to an attacker, revealing potentially sensitive information such as database connectivity details or even usernames and passwords.                                                                                                                               |
| <b>SQL Query Misuse:</b> The SQL usage testing component of the Web application module tests primarily for improper handling of erroneous queries that result from failure to conduct input validation within the application, resulting in the attacker gaining information that can be used to mount a more aggressive attack (i.e. privileged application and database server data).                                                                         |
| <b>Smart Guesswork:</b> Encompassing many types of security probes, Smart Guesswork searches for files and directories that are obscured to the normal user but are available on the Web server when exhaustive testing is undertaken. Examples of probes used include searches for; default directories, hidden archives, and often sensitive files such as robots.txt that either possess privileged data or point to where it can be located by an attacker. |

**Wireless Module**

The security problems surrounding wireless technology have been widely publicized, yet wireless networks continue to grow in number and popularity. As wireless access points proliferate, they silently create unseen holes into otherwise secure networks. Attackers with even basic skills can exploit these invisible, but easily, detectable entry points.

Foundstone Enterprise Risk Solutions™ locate, map and analyze wireless access points for vulnerabilities across global networks. Organizations can then understand both where WAPs are present in the environment as well as any vulnerabilities they possess. In addition, machines connected to wireless networks are also discovered, showing not only where wireless access is possible but also where wireless networks are in active use.

Foundstone maintains the largest inventory of 802.11 access point and client identification signatures in the industry today. The flexible capabilities of its Foundstone Scripting Language™ also allows new wireless device fingerprints to be added rapidly, often resulting in checks for newly discovered access point types on a customer network made available to the master list within 48 hours.

Copyright 2003 Foundstone, Inc. All Rights Reserved.

Foundstone Enterprise Manager, Enterprise Risk Solutions (ERS), Foundstone Scripting Language (FSL), FS1000, Foundstone Enterprise, FoundScan Engine, FS1000 Appliance, Foundstone Managed Service, Foundstone Professional, Foundstone Professional TL, and the Foundstone name are trademarks of Foundstone, Inc. All other company, brand and product trademarks, registered trademarks and service marks are the property of their respective owners.

CALL 1.877.91.FOUND | WWW.FOUNDSTONE.COM