SearchSecurity.com
Security School

Checklist of known IIS vulnerabilities

By Michael Cobb

When attacking Web sites, script kiddies go for an easy kill. They look for common exploits. Here is a list of some of the top vulnerabilities found in Web sites running on Microsoft's Internet Information Server (IIS). Some of the vulnerabilities, such as open ports, are not particular to IIS. Both CERT (www.cert.org) and CIAC (www.ciac.org) are excellent sources on the latest vulnerabilities affecting Web sites.

Make sure your systems and networks are not vulnerable to these exploits by keeping your patches up to date. Microsoft Baseline Security Analyzer is a security hotfix checker available from Microsoft that scans local or remote systems for current patches. You may also want to consider upgrading your IIS installation to IIS 6.0, which offers dramatically increased security over earlier versions. I cover how to protect a Web site from these and other vulnerabilities in more detail in Web Security School (SearchSecurity.com/WebSecuritySchool).

Default installs of operating system and applications
Many users fail to appreciate what an installation program actually installs on their machine. Windows and IIS both install superfluous services and dangerous samples. The unpatched services, sample programs and code provide means for attacking a Web site.

Accounts with weak or nonexistent passwords
IIS uses several built-in or default accounts. Attackers commonly look for these accounts. They should be identified and changed if not removed from the system.

Large number of open ports
Every visitor, good or bad, connects to a site and system via an open port. By default, Windows and IIS ship with more ports open than are required to function correctly. It is important to keep the least number of ports open on a system. Close all other ports.

Windows License Logging Service overflow
By sending a specially formatted message to a Web server running the License Logging Service, an attacker can exploit an unchecked buffer. This can cause the service to fail, creating an opening for the hacker to execute code on the server with "SYSTEM" privileges.

Microsoft Server Message Block (SMB) vulnerability
The Server Message Block Protocol is used by Windows to share files and printers and to communicate between computers. A hacker's SMB server can leverage that ability to execute arbitrary code on a client with "SYSTEM" privileges.

ISAPI Extension Buffer Overflows
Several Internet Server Application Program Interface (ISAPI) extensions are automatically installed with IIS. ISAPI extensions, which are actually dynamic link

libraries, extend the capabilities of an IIS server. Several, like idq.dll, contain programming errors that allow attackers to send data to the ISAPI extension in what is known as a buffer-overflow attack. Thus, an attacker can take full control of the Web server.

Unicode vulnerability (Web Server Folder Traversal)

By sending an IIS server a carefully constructed URL containing an invalid Unicode sequence, an attacker can bypass the normal IIS security checks and force the server to literally “walk up and out” of a directory and execute arbitrary scripts.