ABSTRACT

This dissertation analyzes weaknesses on web servers, focusing on Microsoft's Internet Information Server (IIS). As part of the research, an IIS scanner (IIS-SCAN) has been implemented to probe only on URL vulnerabilities. The need for a vulnerability scanner stems from the alarming number of successful attacks on computer systems that are connected to the Internet. The security flaws threatening e-businesses and the Internet community has prompted bona fide defense measures. Internet firewalls – gateways controlling access between one network and all the others – became a must-have for any organization connecting to the Net. If the firewall is considered the perimeter defence, vulnerability scanners can be used as a second line of defence to determine initial security holes. Prior to the development phase, a thorough research has been done on aspects such as an overview of Internet security, IIS mechanisms and the security integration between Windows NT and IIS. In order for IIS-SCAN to fulfill the needs and features of an industrial standard scanner, a few commercial and open-source scanners have also been reviewed, including CISCO Secure Scanner, Internet Security Systems (ISS) Internet Scanner and Nessus Security Scanner. For the development stage, IIS-SCAN is written using Visual Basic 6.0 running on Windows NT platform. IIS-SCAN provides an efficient and stable scanning engine to scan for IIS vulnerabilities on an Intranet or Internet platform. Testing procedures were also stringently conducted to ensure that each vulnerability could be scanned successfully by IIS-SCAN. These proved that IIS-SCAN has achieved its objectives of scanning for IIS vulnerabilities in a network.