CHAPTER 6

EVALUATION AND CONCLUSION
CHAPTER 6

EVALUATION AND CONCLUSION

In general, IIS-SCAN has demonstrated a powerful capability of identifying vulnerabilities on an Internet Information Server. The ability of using efficient Internet data transfer in this program serves as a stepping-stone to obtain better algorithm of enhancing the vulnerability scanning process in future.

Even though IIS-SCAN does have its weaknesses and limitations as discussed in section 6.3, it has successfully achieves its objectives. All functionalities and design specifications have been implemented precisely and competently.

6.1 Achievements

In the process of developing IIS-SCAN, several achievements in terms of theory and practice have been obtained. The achievements can be categorized as follows:

i. Theoretical knowledge in Internet Information Server
ii. Theoretical knowledge in IIS vulnerabilities
iii. Theoretical knowledge in Internet Transfer Control
iv. Practical knowledge in IIS-SCAN

6.1.1 Theoretical Knowledge in Internet Information Server

This dissertation presents a great deal of information related to the introduction of IIS and its mechanisms. An in-depth overview is also given on the security integration between IIS and Windows NT. Aspects of theoretical knowledge that has been covered range from access control, NTFS permissions, confidentiality, and integrity to SSL technology and digital signatures.
6.1.2 Theoretical Knowledge in IIS Vulnerabilities

Statistics on IIS vulnerabilities have been well analyzed in the Literature Review section and should provide a clear view to users about the disturbing numbers of vulnerabilities found on IIS throughout the last few years. However, Microsoft should not solely shoulder the blame as in the midst of packing powerful and complete features into IIS, some vulnerabilities are bound to be left unchecked or most probably these vulnerabilities results from extensive usage from users worldwide.

This dissertation only focuses on IIS vulnerabilities resulting from direct URL vulnerabilities. A complete guide on each IIS vulnerability has been compiled in Appendix A and should serve as a “bible” to all network administrators and web server administrators.

6.1.3 Theoretical Knowledge in Internet Transfer Control

In order to develop IIS-SCAN, research has to be done upon the technical mechanism of sending and getting responses to a web server. Internet Transfer Control has been chosen and thoroughly studied to make full use of its features and to determine exactly how can it be used in developing IIS-SCAN as well as the protocols that are supported. A detailed explanation has already been documented in Chapter 5.

6.1.4 Practical Knowledge in IIS-SCAN

Real time programming experience can be obtained through the coding stage of IIS-SCAN. The eminent part of practical programming knowledge can be seen from ADO data access method to Microsoft Access database, usage of multiple Visual Basic ActiveX controls to build up the main interface and code manipulation of Internet Transfer Control to send and obtain requests from the IIS server. Stringent testing measures have also been implemented to stabilize the program. Valuable optimization and stabilization steps have also been practically obtained from the testing stage.
6.2 Advantages of IIS-SCAN

Although IIS-SCAN is developed as a small-scale vulnerability scanner, there are a few advantages as listed below:

- **Up-to-date IIS vulnerability database** – an extensive research has been done and most of IIS vulnerabilities have been compiled into IIS-SCAN database.

- **Usage of ADO data access method** – IIS-SCAN deploys one of Microsoft’s latest and fastest data access methods to retrieve data from its vulnerability database. Coupling with Visual Basic’s compatibility with ADO, it provides the most optimum performance for IIS-SCAN.

- **Reduced learning curve** – IIS-SCAN is designed to have a compact and user-friendly interface to reduce the learning curve for users. The reduction on the total number of screens available in IIS-SCAN ensures that complexity of the program is prevented.

- **Accurate reporting** – Reports containing vulnerabilities found on an IIS server are tested thoroughly to be accurate. Scanning results are consistent to avoid false alarms on vulnerabilities.

- **Effective error recovery** – If any errors are encountered by the IIS-SCAN scanning engine, it will perform auto-recovery and will continue with the scanning process as in the case of scanning a DoS vulnerability.

6.3 System Limitation

Due to time constraints and environment facilities limitation, IIS-SCAN weaknesses have been identified and listed as follows:

- **Future version upgrades** – New IIS vulnerabilities can appear anytime. In cases of upgrading the current IIS-SCAN program to cater for new vulnerabilities, it is quite a troublesome process. This is because the database and IIS-SCAN executable file will have to be re-submitted and may result in a large file to be downloaded.
- **Limited IIS vulnerabilities** – The current version of IIS-SCAN only scans for vulnerabilities based on weak URL parsing. Other classes of attacks have not been considered and they may pose a danger of hackers still being able to take advantage of even a single vulnerability.

- **Enhanced scan sessions** – IIS-SCAN scan session configuration only handles very basic settings only. It is unable to store multiple scan sessions and provide means to perform trend analysis.

- **Lack of analysis report** – The reports currently available in IIS-SCAN is limited to only vulnerability listing only. More powerful analysis reporting is not built into the program, thus reduces the assistance to the network administrator to gather analysis information.

### 6.4 Future Enhancements

The IIS-SCAN system provides excellent opportunities for enhancement purposes. Therefore, for interested readers who are keen on developing a vulnerability scanner, he or she can consider to build in more functionalities as part of an academic project in future. Among the constructive suggestions and propositions to further improve the IIS-SCAN program include:

- **Increase capability of vulnerability scanning** – IIS-SCAN scanning engine can be further improved to scan IIS vulnerabilities that include Denial of Service attacks, third party hacking tools and IIS vulnerabilities that are exposed when integrated with other Microsoft servers and software. Due to time constraint, these classes of vulnerability attacks have been omitted.

- **Multiple scan sessions** – Another revision of IIS-SCAN can have the ability to store multiple scan session results and perform trend analysis by pulling up past vulnerability scans for comparison. Different types of graphs or charts can be used to illustrate a better analysis view to the users.

- **Probing on client side vulnerabilities** – A vulnerability scanner can also be enhanced to perform vulnerability scanning on software used on client or
workstations. For instance, a scanner can actually probe workstations to obtain vulnerability on web browsers used on that machine.

- **Auto switching of vulnerability scanning** – A platform free vulnerability scanner can be developed to automatically switch the scanning vulnerabilities according to server. If the targeted web server is an Apache web server or even a Lotus Domino server, the vulnerability scanner can automatically make the appropriate changes. A wider market can then be catered with the vulnerability scanner.

6.5 Conclusion

In the course of completing this dissertation, all of the targeted objectives have been successfully achieved. Besides gaining theoretical knowledge on Internet security and IIS vulnerabilities, practical development experience is also acquired through the implementation phase of IIS-SCAN.

Although IIS-SCAN has its own limitations, the scanning algorithm of IIS-SCAN can be a foundation for future enhancements. It is hoped that this dissertation will be beneficial as a reference guide for Internet server vulnerabilities and development of any vulnerability scanner in future.