Progress in Human Computer Interaction (2017)

ORIGINAL RESEARCH ARTICLE

Online security detection system design

Hongyan Han,Zhongyuan Lu,Wenbing Wang

School of Computer Science and Technology, Shiyan University of Science and Technology, Hubei, China

ABSTRACT

The 21st century is the information age, information has become an important strategic resource for social development, social information has become the development trend of the world today and the core, and information security in the information society will play a very important role. With the continuous development of computer networks, global information has become the trend of human development. However, because the computer network has the form of connection diversity, terminal distribution inhomogeneity and network openness, interconnection and other characteristics, resulting in the network vulnerable to hackers, malware and other malicious attacks, the former will cause unpredictable impact on the user , While the latter often causes the system to crash. Whether in the local area network or in the wide area network, there are natural and man-made and many other factors of vulnerability and potential threats. Therefore, the network security measures should be able to all aspects of a variety of threats and vulnerabilities, so as to ensure the confidentiality of network information, integrity and availability. At the beginning of this article, the beginning of this article, through the analysis of hacker behavior and typical attacks, summarizes the inevitable reasons for the existence of network security vulnerabilities, and summarizes the status of computer network security, as well as the specific concepts, classification and limitations of vulnerability scanning technology. The focus of this paper is to improve the original system of the theme module, and the original system to add some features to make it more perfect function. Finally, the shortcomings of the system and some suggestions for further improvement and expansion are put forward.

KEYWORDS: network security scanning vulnerability

1. The purpose and status of online security research

1.1. The purpose of the study

The modern computer system is becoming more and more complicated, and the network system is becoming more and more powerful. It has great influence on the society, but at the same time, because the computer network has the characteristics of connection diversity, terminal distribution inhomogeneity and openness and interconnection of the network The network is vulnerable to hackers, malware and other bad attacks, making security more and more prominent.

1.2. Overview of the research contents

The research contents of this subject include: analyzing the hacker's attack behavior, collecting and arranging the network security loophole, the design and realization of the vulnerability scanning system, the testing and improvement of the vulnerability scanning system. I focus on the design and implementation of the vulnerability scanning system, vulnerability scanning system testing and improvement. In the system structure, we intend to use two kinds of programs to achieve two structures:

One is based on the host network security assessment system, one is based on the network security assessment system. Host-based, user-controlled interface and scan engine are in an application, flexible installation, but not easy to transplant, and by the system itself, the application platform constraints.

The other is based on the network is Browser / Server mode, scanning engine and other major parts are placed on a secure scan server. Managers monitor on separate workstations, scan control and view results through a browser. The data communication between the access workstation and the scan engine uses an encrypted channel.

1.3. System requirements analysis

1. The system function requirements

(1) The system should be able to scan the corresponding IP first, and give the corresponding report

(2) To be able to achieve the loopholes in the scan, and give a brief report and a detailed report

(3) The system should be clearly identified when scanning and updating

2. System performance requirements

(1) The system should use multithreaded scans during scanning to save time

(2) The system should take into account the user in the application of this procedure, to constantly update the vulnerability library, so the system needs to have online upgrade function.

3. The user interface requirements

(1) User interface should be simple, easy to understand,

(2) The user interface should be able to accurately show the process of the program

(3) The user interface should be given a help file, the user can independently use the program.

4. The system scalability

(1) Should be set aside enough space to facilitate the subsequent addition of control keys.

(2) The future system is mature, it should be based on any operating platform for scanning

5. The use of methods

On the online security assessment system scanning process can be divided into two categories:

One is host-based;

One is based on the network.

In this study, we intend to use two methods at the same time

6. The choice of system design tools

Microsoft developed Visua1C + + has always been a highly integrated software development tools, using it to develop the program has a fast running, portability and other advantages. Therefore, we use VC ++ to complete our system design tasks

2. The vulnerability scanning technology overview

(1) What is a vulnerability scan

Vulnerability Scanner is a program that automatically detects remote or local host security vulnerabilities. By using the vulnerability scanner, the system administrator can discover the distribution of various TCP ports of the maintained Web server, the services provided, the version of the Web service software, and the security vulnerabilities that these services and software present on the Internet. And thus in the computer network system security battle to do 'targeted', timely repair loopholes, build a solid security Great Wall.

(2) The classification of vulnerability scanners

According to conventional standards, vulnerability scanners can be divided into three categories:

1. Host vulnerability scanner (Host Scanner)

Run the system to detect system vulnerabilities locally. Such as the famous COPS, tripewire, tiger and other free software.

2. Network vulnerability scanner (Network Scanner)

Based on the Internet, remote detection of the target network and host system vulnerabilities in the program. Such as Satan, ISS software.

3. Intrusion Scanners (Intrusion Scanners)

Is the ability to remotely detect target host vulnerabilities in real time, in some cases allows real-time attempts and detection of these vulnerabilities

(3) The working principle of the leak scanning gas

The network vulnerability scanner records the response given by the target by remotely detecting the services of the different hosts of the target host TCP / IP. In this way, you can collect a lot of information on the target host (for example: whether it can use anonymous login, whether there is a writable FTP directory, whether to use Telnet, httpd is running with root). After obtaining the relevant information of the target host TCP / IP port and its corresponding network access service, it matches the vulnerability database provided by the network vulnerability scanning system. If the matching condition is satisfied, the vulnerability exists. In addition, by simulating the hacker's offensive approach, the target host system for aggressive security vulnerability scanning, such as testing the weak password, is also one of the scanning module implementation. If the simulation attack is successful, it is considered a vulnerability exists.

In the principle of matching, the network vulnerability scanner is based on the rules of matching technology, that is, according to security experts on the network system security vulnerabilities, hacker attack case analysis and system administrator on the network system security configuration of the actual experience, Standard system vulnerabilities, and then on the basis of the above constitute the corresponding matching rules, the program automatically by the system vulnerability scanning analysis.

The rule based on rules is based on a set of rules that are defined in advance by expert experience. For example, in the scan of TCP 80 port, if you find / cgi-bin / phf or /cgi-bin/Count.cgi, according to expert experience and CGI program sharing and standardization, you can infer that the WWW service there are two CGI Loopholes. It should also be noted that the rules-based matching system also has its limitations, since the reasoning rules that are the basis of such systems are generally arranged and planned according to known security vulnerabilities, and many dangerous threats to the network system Is from the unknown security vulnerabilities, which is very similar to PC antivirus.

The realization of a rule-based matching system is essentially a knowledge engineering problem, and its function should be able to use with the accumulation of experience, its self-learning ability to carry out regular expansion and correction, that is, the expansion and revision of the system vulnerability. Of course, this ability is still in the expert guidance and participation can be achieved. However, it should also be noted that some of the system vulnerabilities may not trigger any rules that are not detected by the vulnerability coverage.

The working principle of the whole network scanner is that when the user sends out the scanning command through the control platform, the control platform sends the corresponding scanning request to the scanning module. The scanning module starts the corresponding sub-function module immediately after receiving the request. Host to scan. By analyzing the information returned from the scanned host, the scanning module returns the scan result to the control platform and finally presents it to the user by the control platform.

(4) The overall structure of the vulnerability scan

The external scanning module is scanned directly from the running platform (referred to as the scanning host) on which the external scanning module is installed as the object (referred to as the scanning host). The internal scanning module uses the scanned host as the running platform, from the remote control; and control platform provides a human-computer interaction interface.

Internal scanning principle: When the user through the control platform issued an internal scan command, the control platform to the internal scan module to send the corresponding internal scan request, because the internal scanning module is installed on the scan host, so the internal scanning module received After the request, each sub-function module is started to carry on the corresponding internal scanning to the machine, and the result is returned to the control platform in real time, and then the scanning result is finally presented to the user by the control platform.

(5) The application of CGI

The entire vulnerability scanning system utilizes a browser / server (B / S) architecture in order to eliminate the differences in the operation of the program due to the different operating system platforms, and to provide a range of features such as super Text function, flexible layout editing function to build a beautiful and flexible man-machine interface. In the implementation of the network vulnerability scanner, we through CGI technology to connect the front of the browser and background scanning program.

CGI is a generic gateway interface, as a specification, which allows the Web server to execute other programs and store their output in the appropriate way in the text, graphics and audio sent to the browser. CGI programs can provide a variety of functions from simple form processing to complex database queries, which greatly enhances the dynamic processing power and interactivity of the Web. The combination of servers and CGI programs can scale and customize the capabilities of the World Wide Web.

The main steps in the CGI process are as follows:

1 Browser to decode the first part of the URL and contact the server;

2 Browser provides the rest of the URL to the server;

3 The server converts the URL into a path and a file name;

4 The server realizes that the URL points to a program, not a static file;

5 Server to prepare environment variables, the implementation of CGI procedures;

6 Program execution, reading environment variables and STDIN;

7 Program sends the correct MIME header information to STDOUT for future content;

8 Program sends the rest of its output to STDOUT and then terminates;

9 Server discovery program terminated, close the connection with the browser;

10 The browser displays the output from the program.

3. The detailed design

(1) Online upgrade working principle

The purpose of an Internet client program is through Internet protocols such as: HTTP and FTP to access the network data source (server) information. The client program can access the server to obtain information like weather forecasts, stock prices, important news data, and even exchange information with the server. The Internet client program can access the server through an external network or an internal network (typically an intranet).

In order to develop Internet client program. MFC class library provides a dedicated Win32 Internet extension interface, which is WinInet. MFC encapsulates WinInet in a standard, easy-to-use collection of classes. In the preparation of WinInet client program, you can either directly call Win32 function, you can also use WinInet class library.

The Win32 Internet Extensions provides access to common Internet protocols, including HTTP, FTP, and Gopher. Gopher has faded out. With the WinInet programming interface, developers do not have to understand the details of Winsock, TCP / IP, and specific Internet protocols to write high-level Internet client programs. WinInet provides a unified set of functions for all protocols (HTTP, FTP, and Gopher), which is the Win32 API interface. Using these unified set of functions, greatly simplifies the programming for HTTP, FTP and other protocols, so as to easily integrate the Internet into their own applications. The conversion of the underlying protocol (such as from FTP to HTTP) as long as the source code can be modified slightly.

There are two ways to use WinInet in Visual C ++ projects. One is to directly call Win32 Internet function, the other is to use WinInet class library.

MFC encapsulates WinInet by providing three implementations by the CStdioFile derived class. The three derived classes are: CInternetFile, CHttpFile, and CGopherFile. As the Gopher protocol has been rarely used, so this article will no longer discuss CGopherFile. For developers, whether or not you have used CStdioFile, WinInet is well understood and easy to use. It makes access to Internet data easy, making Internet data and local data processing consistent transparent, data storage location is no longer important.

MFC WinInet class has the following advantages:

Buffer input and output

The type of data is handled safely

Many of the parameters of the function are the default values

Ordinary Internet errors are handled exceptionally

Automatically clear open handles and connections

Using the API functions provided by WinInet, you can:

Download the HTML page via the HTTP protocol, which is specifically designed to transfer HTML pages between the server and the client browser.

Send an FTP request to upload or download a file and get the directory information for the server. Downloading files via anonymous login is a typical FTP application.

Other applications based on HTTP and FTP.

(2) Multi-threaded principle and implementation

Each process has a private virtual address space, the process of all threads share an address space. Each thread is assigned a time slice by the CPU. Once activated, he runs normally until the time slice is exhausted and is suspended. At this point, the operating system chooses another thread to run, through the time slice rotation, and because the time slice is Small (20 ms level), looks like multiple threads at the same time at work. Actually only multiprocessor systems are really running multiple threads on the available processors at the same time. Win32-based applications to enable users to improve efficiency, enhance responsiveness and background assistance.

In Visual C ++ using MFC programming, the thread is divided into the worker thread and user interface line into two categories. The former is often used to deal with background tasks, the implementation of these background tasks and will not delay the use of the user application, that users do not have to wait for the completion of background tasks. The latter is often used to independently handle user input and respond to user events.

(3) The use of MFC class

WinInet refers to the Internet function provided by Microsoft Win32, these functions are included in the WININET. DLL dynamic library so that programmers can easily use HTTP, FTP and gopher to access the Internet, and then a little bit after the Finger query and Whois Inquire. VC 4.2 or above MFC provides WinInet class, these classes shield the WinSock and TCP / IP protocol, the programmer only need to call these methods, and do not understand the specific content of the agreement can be prepared client program access HTTP, FTP , Gopher and other sites.

1. WinInet class and its function

MFC provides a total of 13 WinInet class, they achieve a series of Internet access.

(1) CInternetSession: Create one or more Internet channels.

(2) CInternetConnection: with subclass (ChttpConnection, CftpConnection, CGopherConnection) management application with the Internet server (Http server, FTP server, gopher server) to establish the connection.

(3) CInternetFile: With subclasses (CHttpFile, CGopherFile) provides a way to access the remote server (Http server, gopher server) file system.

(4) CFileFind: with subclasses (CftpFileFind, CgopherFileFind) to complete the local and remote Internet sites (FTP server, gopher server) to find the file function.

(5) CGopherLocator: Gopher site from the gopher bit (locator), and provided to CgopherFileFind used to locate.

(6) CInternetException: Describes the exceptions to Internet operations.

2. Compile Internet client program with WinInet

An Internet client application is a program that obtains information from a network data resource (server) based on Internet protocols such as gopher, FTP, HTTP, and so on. Programmers can directly call Win32 function or use MFC's WinInet class to write WinInet client applications.

In the process of compiling Internet client program, the author completes the realization of HTTP function, FTP query, gopher query, Finger query and Whois query function module with WinInet class. The main function of the query is to try to establish a connection with the server, and then directly from the server to accept the response information or access to the server-related file system control handle. The following describes the implementation of different protocol query methods.

WinInet class declaration In the header file 'afxinet.h', in the use of WinInet class to the application of the statement:

#include <afxinet.h>

3. Access the WWW server

The easiest way to do an HTTP connection is to create a CInternetSession object that calls the function OpenURL () with a valid HTTP site URL as a parameter, which returns the CInternetFile file handle, which is the web page information for this URL, The local file to read, write, search and other operations, access to the necessary information.

Visit the WWW site, you can also use the ChttpConnection class. The specific method is to http server domain name and its implementation of the http protocol port port number (default 80) as a parameter, call the CinternetSession::Ge tHttpConnection () function to establish a connection with a site, and then CHttpConnection::SendRequest function to the HTTP server Send a service request, the return value is the file handle of the CHttpFile type containing the response message.

4. The key technology to achieve

(1) The realization of online upgrade system

1. Online upgrade principle

The module is based on the principle of the Norton firewall online upgrade module, the principle is that when the user clicks the online upgrade button, the system will automatically pop up a dialog box, the user can choose whether to perform online upgrade in the dialog box.

If the user chooses to execute 'Next', the program will connect to the website we set up. After the FTP link on the website, the program automatically retrieves the site if there is a higher version of the vulnerability, if any, the system will automatically download a new version of the vulnerability, update the existing vulnerability, such as enough existing version is already a high version and the system will prompt no need to update. The user can click the 'Finish' button to end the online upgrade.

2. Online upgrade key technology implementation

M_cis.SetOption (INTERNET_OPTION_CONNECT_TIMEOUT, 5); // set an Internet option

M_phttp = m_cis.GetHttpConnection (m_strServer, m_dwPort); // connect to http server m_strServer

M_lbProduct.AddString (m_strSoft + " + m_strVersion);

And then find the available updates, first through the ChttpFile Update.INI file downloaded to the system temporary directory, and then call GetPrivateProfileString read the latest version of the Internet and to update the file to determine whether the need to update the downloaded file pFile-> QueryInfo (HTTP_QUERY_CONTENT_LENGTH, str);

To prevent the download of half of the network failure, first download the file plus suffix. Overg, download all the success of the original replacement in the use of procedures to complete the update.

(2) Multi-threaded implementation of the method

First, we define the number of threads that scan ip, the maximum number of threads defined as 500, to create a thread (management thread), the thread used to manage those threads for each IP scan. This is because the management thread may sometimes hang, if you do not create a new, then the main thread will hang, the window will stop responding. When a thread enters the critical area, the other threads that want to enter the critical section are suspended until the thread entering the critical section exits the critical section, thus ensuring that only one thread can modify the variables at the same time. This is done in order to better control the multi-threaded (to prevent multiple threads competing resources, causing the system to crash). Whenever a new scan thread is created, the program locks the semaphore once. When the maximum number of concurrent threads is reached, the scan management thread hangs when it wants to lock the semaphore again, and there is no new scan thread Is created until a scan thread ends. At the end of the scan thread, the semaphore is released so that the pending management thread is unlocked and continues to create a new scan thread. The scan thread keeps looping until all the IP addresses are scanned and all active scan threads are over. Read the ip, we are reading the entire data, by controlling the length of its right shift, and then on the FF to take 'and' approach to achieve, and:

```
StrIP.Format ('% d.% D.% D.% D',
                (DwIP >> 24) \u0026 0xff,
                (DwIP >> 16) \u0026 0xff,
                (DwIP >> 8) \u0026 0xff,
                (DwIP \u0026 0xff);
```

Then is the scan code (and the original data connected, not introduced here) Finally, the semaphore and critical resources release, return to the function value, the function module to achieve.

5. The system debugging

I am in the realization of the online upgrade function module, because it involves the server to obtain data, to write data to the database, that is, the need for database operations. Due to lack of experience, coupled with the understanding of the operation of the database is not too deep. So the operation of the database there have been some problems in the code added to the database to add data, but check the database, found that did not achieve the function, the data is not inserted into the database. So I wrote the code I wrote, I first put the code on the database operation with the try, catch the exception operation statement, the results found abnormal, suggesting that the database connection is not correct, I will re-configure the database, again to operate, everything is normal.

References

1. Zang Guipeng, Xiao Jiahua. VC ++ network and database programming hundred cases [M]. Beijing: China Electric Power Press
2. http://www-900.ibm.com/developerWorks/cn/security/se-cgiscaner/part1/index.shtml#2
3. Hou Junjie. Easy to understand MFC [M]. Wuhan: Huazhong University of Science and Technology Press
4. Rebecca Gurley Bace, Chen Mingqi Translation. Intrusion Detection [M]. Beijing: People's Posts and Telecommunications Press
5. ICAT Metabase [EB / OL] .http: //icat.nist.gov/
6. Han Donghai, Wang Chao. Intrusion Detection System and Case Analysis [M]. Beijing: Tsinghua University Press
7. Tang Zhengjun. Network intrusion detection system design and implementation [M]. Beijing: Electronic Industry Press
8. Lvlin Tao, Zhou Mingquan. Information Security Technology [M]. Xi'an: Xi'an University of Electronic Technology
9. Design and Implementation of Network Intrusion Detection [J]; Journal of Beijing University of Aeronautics and Astronautics; 2009-01