Design and Implementation of a Network Attack Platform Based on Plug-in Technology

Li Gen, Wang Bailing*, Liu Yang, Bai Xuefeng and Yuan Xinling

Department of Computer Science & Technology
Harbin Institute of Technology at Weihai, Shandong, China
**wbl@hit.edu.cn*

Abstract

In recent years, a large number of network security tools appear constantly. However, they all in the cohabitation of the state. This article designed a the network attack platform based on plug-in technology, the prototype system has good interactivity and scalability. The system can guide the platform operator to complete a variety of different types and complete steps network attack experiments, help the platform operator research and learn network attack methods. Moreover, the Attack Knowledge Base can integrate new network attack methods. Attack Knowledge Base can be constantly updated, so that the platform can be applied to future network attack experiments. So the design of such a system has a high practical significance for teaching and researching network attack methods.

Key words*: Network attack, Prototype system, Scalable, Attack Knowledge Base*

1. Introduction

With the rapid spread of a large number of network applications, network security events occur more frequently in our lives. Network attacks initiated by a few hackers who master the superb technical in the past, and now can be exploited for the growing number of non-professional and non-technical persons. The most important reason for it is the emergence of a large number of design good automated attack tools. As long as he or she has a clear target, these tools can help attacker launch a threatening network attack [1]. However, on the other hand, tools that are able to complete a full invasion process attack are rare. Most of the existing network attack tools are designed for testing specific security vulnerabilities and the functions of them are specific and single. In order to complete a full network intrusion attack you need to look for different kinds of attack tools and combine them to use [2]. However, it is very difficult for people who don't have network security basics.

We all know that the 21st century is the age of information technology and the network will become yet another battlefield of the future national dispute. Automation, the enlargement of the target object, the organization collaboration, the intelligence and complex of the attack become the main features of the network attack [3]. It becomes critical to understand network attack information comprehensively and ensure the security of our own network. Currently, countries have begun to develop their own national network attack test system .They cultivate and format professional knowledge and skills "Cyber Army".

Now there are network attack platforms have been designed and implemented successfully. Among them the famous is the Information Assurance Battle Lab designed by West Point [4], the Information security engineering practice comprehensive experimental platform designed by Shanghai Jiaotong University [5], Several key network security technology and Prevention experimental platform designed by Chinese Academy of Science [6], Network attack and defense training platform designed by Zhongyuan University of Technology [7], *etc*. A scalable

network attack platform can integrate existing network attack tools and provide the freedom of choice of the operator to carry out the specific network attacks [8]. It can not only reproduce the classic network attack process, but also can allow an attacker to get a comprehensive understanding of the attack process and improve the operator's security knowledge and skills. Therefore design a scalable network attack platform has a very high level of teaching and practical significance.

2. System Design

2.1. System Function Design

In this paper, the design of the network attack platform can integrate a variety of well-known existing network attack methods, and provide operator of the platform a easy-to-use method. The main features include target host or network information scanning collection, attack methods selection and configuration, effective attack load release, attack tools remote launch and control, *etc*. In addition, the platform operator can also add new type of attack methods in accordance with the Attack Knowledge Base of the platform to the database according to their needs, and the operator can test and study the new method of attack on the platform.

2.2. System Architecture and Modules

According to a traditional complete network attack process: Capitol, Scanning, Inventory, Access, Privilege Escalation, Information theft, Trace mask off or Denial of Service, *etc*. [9], the system includes the following main modules: Control and display, Information collection, Configuration and loading, Attack engine, Tools put and Remote control. The detailed structure shown in Figure 1:

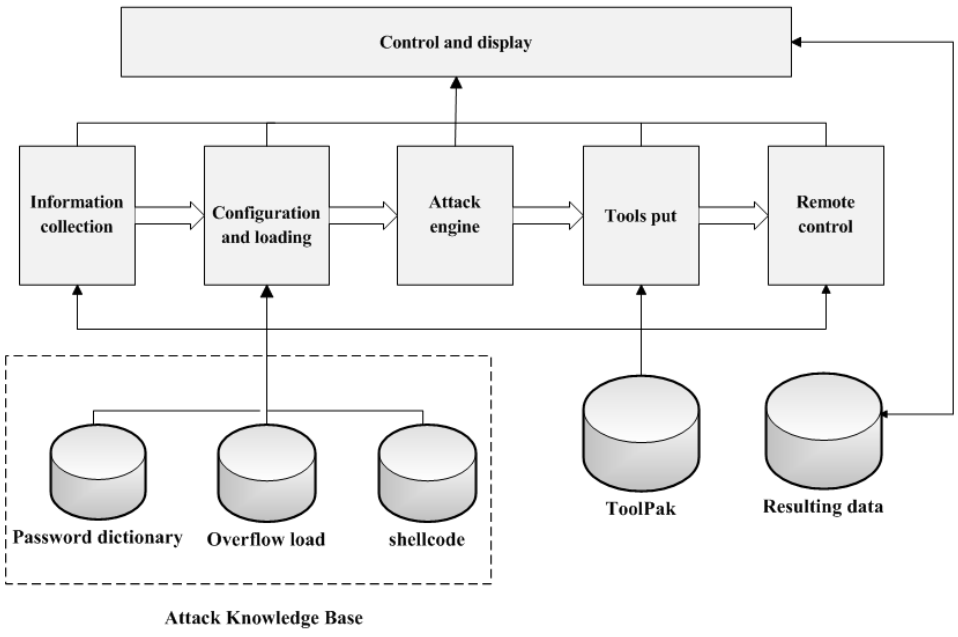


Figure 1. Diagram of the System Modules

- Control and display: Module that interacts directly with the users of the platform. The module can display the current system status information in real-time, and help guide the operator to complete the addition and perform of network attack missions. The main functions include calls to the corresponding modules in the course of a

attack process, display of the collected target system information, configuration information as well as the result of the attack.

- Information collection: The module's main function is to complete the scanning on the target system and information profiler. As much detail as possible to collect system information, the open type of service and whether there is a specific vulnerability information. It provides operator a reference to select suitable attack plugin in the subsequent steps.
- Configuration and loading: The module's main function is to achieve the assembly of attack plugins. It can configure out a complete attack method by calling the attack module in accordance with the operator's actual fill. This module can be used in combination with different attack methods and thereby be able to complete a variety of different types of attacks experiments. In addition, this module can add a new attack plugin in the practical application and achieve good scalability.
- Attack engine: The module for attack to launch and load release. This module processes attack parameters that operator configured on the previous step and compose of specific network packets sending to the target system.
- Tools put: This module is called after attack was successfully completed. The main function is to call the remote network tools in the tool library and devote to the target system that has been invaded. It can collect further information and open the backdoor on the target system. It helps operator get the full control of the target system.
- Remote control: The module uses a backdoor tool that placed on the target system and control the target system remotely.

This six functional modules in the system structural relationship as shown in Figure 2:

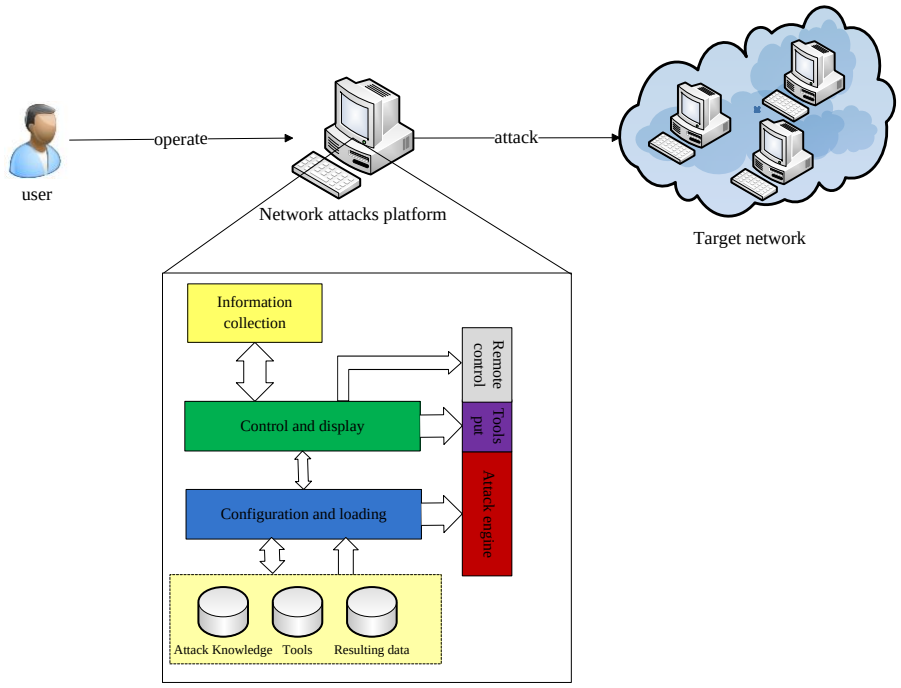


Figure 2. System Functional Modules Diagram

3. Extensible Plug-in Technology

3.1. Principles of Plug-in Technology

The plug-in technology puts the entire application into two parts of the host program and plug-ins in the design and development process of program. It can be under the same circumstances in the host program by increasing or decreasing the plug or modify the plug to adjust and enhance the functionality of the application [10].

Dynamic Link Library is a main way to achieve the implement of plugin. The dynamic link library is a certain function of software modules that can perform [11]. The module can not operate independently, but can output a function or class, its internal function is called by other running independent programs (the host program). The host program has two way to use dynamic link library: implicit link and explicit link. Using implicit link host program can directly call a function of the output of the dynamic link library or class, but will need to provide the output library file when compiled and linked, the number of dynamic link library that has been compiled and linked is fixed. Explicit link does not require an output library file, but to use the system functions provided by the operating system to load the specified dynamic link library, use the function after loaded. Explicit link is more difficult to use than implicit link, but relatively more flexible. To be able to host program can successfully invoke the plug-in and the use of function must be designed to a standard interface for communication. Interface defines the functions and provides a concrete realization of function call, does not contain a function. Interface is essentially a specification for software module call, it allows different plug-ins on the concrete implementation of the same interface, but call the same way for these plug-in host program. The adbantage of interface that call specification and function realization is separated from each other increases the flexibility of the application greatly. If you want other developers can develop their own plug-in, developers of the host program only need to announce related interfaces. Plug-in must be registered before use. After register successfully host program can find the plug-in path correctly, initialize the plugin according to the configuration parameters and can cancle the plugins that are no longer needed.

3.2. Attack Platform Plug-in Design

The attack platform design has good versatility and scalability. Each of the main module of the system design is relatively independent and has standard interface. The system makes the core of the different network attack methods a unified format plugins and stores them centrally in the Attack Knoeledge Base. Platform operator can continue to add new features according to the actual needs of applications. The attack engine is designed to a standard interface for attack plug-loaded. The system operator can extract the attack plugins that are required from the Attack Knowledge Base by using the module of Configuration and load, then configure them the relevant parameters. The operator can view real-time Attack engine configuration state. When the engine is configurated successfully, the operator can start the engine

and launch a network attack on the target system or network. The process as shown in Figure 3:

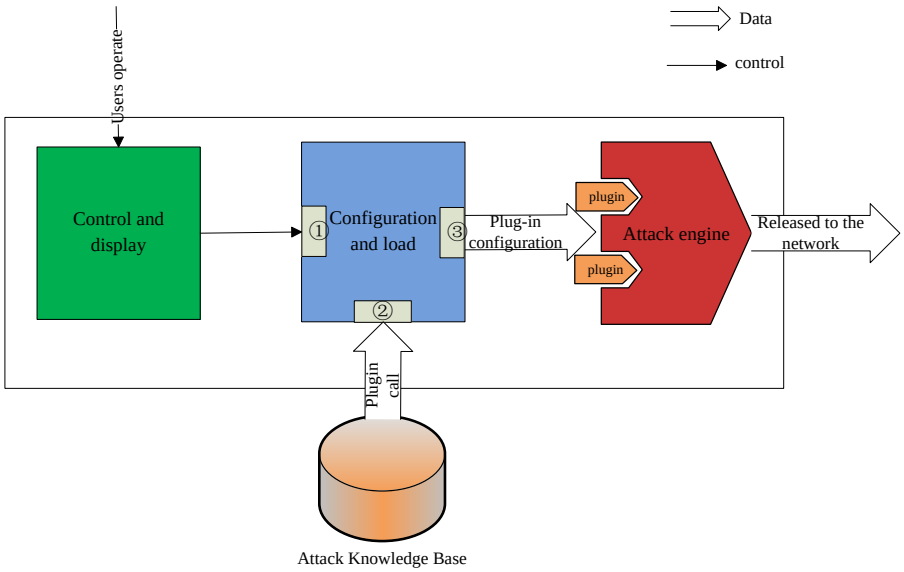


Figure 3. Attack Plug-in Call and Loading Schematic Diagram

Configuration and load module has three main interfaces. Among them interface 1 is used to receive the control information transmitted from the Control and display module; Interface 2 is used to call the appropriate plug-ins from the Attack Knowledge Base; Interface 3 is used to output the plugins that have been configured to Attack engine module.

In addition, once new attack method studied successfully, the operator can make it a new plugin-deposited into the Attack Knowledge Base and the plugin can be used in the next startup configuration loading module. This "Plug and Play" method make the maintenance and updating of the Attack Knowledge Base convenient, and enhance the flexibility and scalability of the system.

4. System Testing Experiment

4.1. System Environment

In order to verify the functionality and performance of the system in a laboratory environment, the hardware configuration shown in Table 1.

Table 1. The Attack Platform Hardware Configuration

CPU Model	Frequency	Memory	Network Interface	Operating system
Pentium(R) Dual-Core E6600	3.06GHZ	2G	Marvell Yukon 88E8057 PCI-E Gigabit Ethernet Controller	Windows XP SP3

The attack platform location in the network shown in Figure 4. Attack platform is in the campus network, and test target is hosts of other campus LAN.

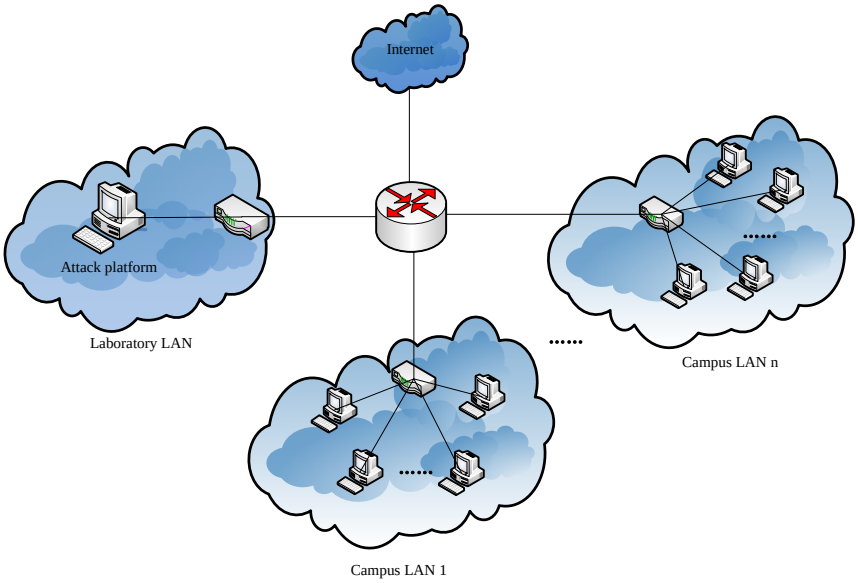


Figure 4. The Attack Platform Network Topology

4.2. Functional Test

The Attack platform scaned other hosts within the campus network by invoking the Nmap scanning software in ToolPak and specified port 20, 21, 22, 23, 139/445, 1433, 3306. We can directly enter the Nmap command on system platform. "nmap –sV –p 20,21,22,23,139/445,1433,3306 -O –oX file.xml TARGET". Scan results as shown in Table 2 and Table 3 shows.

```
---------------Nmap scan-------------------
Please input Nmap command: nmap -sV -p 20,21,22,23,139/445,1433,3306 -
O -oX file.xml 172.31.159.196
Nmap scanner has been started....
Total scan host number: 50094
Total time: 860.02s
For more information, please see the document file.xml
```

Figure 5. Nmap Scan Plug-In

Table 2. Host Scan Range

Address range	Number of hosts	The number of active hosts	Time used
172.30.8.2--172.30.205.254	50094	345	860.02s

Table 3. Port scan results

Port	Open	Filtered	Closed	Total
20/21	50	61	234	345
22	0	61	284	345
23	48	59	238	345
139/445	0	345	0	345
1433	5	62	278	345
3306	6	62	277	345

We choosed a host(172.31.159.196) that offered MSSQL service and guessed the open service password by loading the plug of MSSQL service crack. Fill in the contents of the corresponding file in accordance with the requirements of plug-in. Host IP scan results and successful solution guess and password is stored in a separate file available for viewing. The plugin operating results shown in Figure 6 and Figure 7.

```
--------------MSSQL Password Cracking-------------------
The plugin uses ip.txt as to crack IP files
uses pwd.txt as to password file
'sa' as the default database user name!
Press any key to start to crack!_
```

Figure 6. MSSQL Password Cracking Plugin

```
using 'sa', password: 'qwasyx' connect to database: 172.31.159.196
using 'sa', password: 'qwaszx' connect to database: 172.31.159.196
using 'sa', password: 'qwasyx12' connect to database: 172.31.159.196
using 'sa', password: 'qwasyx123' connect to database: 172.31.159.196
using 'sa', password: 'qwasyx1234' connect to database: 172.31.159.196
using 'sa', password: 'qwaszxc' connect to database: 172.31.159.196
using 'sa', password: 'qwdf' connect to database: 172.31.159.196
using 'sa', password: 'qwas123' connect to database: 172.31.159.196
using 'sa', password: 'qwe' connect to database: 172.31.159.196
using 'sa', password: 'QWE' connect to database: 172.31.159.196
using 'sa', password: 'qwe!@#' connect to database: 172.31.159.196
using 'sa', password: 'qwe!@#123' connect to database: 172.31.159.196
Successfully connected! IP: 172.31.159.196, user: sa, password: qwe!@#123
End of the scan 172.31.159.196
```

Figure 7. MSSQL Password Cracking plugin scanning results

The scan results are stored in a separate file available for viewing. When we get the database password can continue to choose remote management tools from the tool library database to further exploration and system control of the target host. Then we use the tool to add an administrator account on the target host to open the remote login service. Verification of the results shown in Figure 8 and Figure 9.

```
----------Add User By MSSQL-------------
Please input the target IP: 172.31.159.196
Please input the target MSSQL user: sa
Please input the target MSSQL password: *********
Success!
Please input new user(administrator): test
Please input password for new user: ********
Operation is successful!
```

Figure 8. Add user in target host by MSSQL user and password

```
---------------- Telnet --------------------
Please input the target IP: 172.31.159.196
Please input user: test
Please input password: ********
Telnet start...
Operation is successful!
A new session is established. Please open it in sessions
```

Figure 9. Telnet the target host

As Figure 9 shown above, we have choosen telnet plug-in and successfully logged to the target host. When remote login as an administrator to the target host, we have complete control over this host.

After the above steps, we carried out a network attack experiment from the start of the scan to complete control of the target host, which is able to fully verify the platform integration and practicality. Moreover, a variety of different plug can be used in combination in each step of the experiment to complete a valid attack. This no longer verify the details in this article.

5. Conclusion

For different network attacks are difficult to study and test, this paper designed a scalable the network attack platform prototype system. The system can integrate a large number of existing methods of network attacks and reproduce a variety of well-known network attacks, and can guide the platform operator to do the complete steps of the network attack experiment, to help the operator learn and research the principles and implementation of a variety of network attack methods. The system uses the extensible plug-in technology, each network attack method stored as a form of plug-in in the Attack Knowledge Base. The system module via a standard interface calls plug-ins stored in Attack Knowledge Base when needed. The use of plug-in technology not only makes the platform flexible call network attack methods, but also is conducive to the centralized management of the platform to attack. Attack Knowledge Base can be extended continuously updated, so a new type of network attack method can be added in a timely manner, which is conducive to the platform operator testing and research emerging network attack methods. In order to verify the design of the platform of scalability and effectiveness, the subsequent actual research work will gradually implement the platform and simulate it.

Acknowledgements

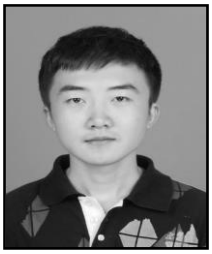
This research was supported by the National Science Nature Foundation of China under Grant No 61170262

References

[1] D. Rodrigues, J. C. Estrella and K. R. L. J. C. Branco, “Analysis of Security and Performance Aspects in Service-Oriented Architectures”, International Journal of Security and Its Applications, vol. 5, **(2011)**, pp. 13-30.
[2] M. Marchetti, M. Colajanni and F. Manganiello, “Framework and Models for Multistep Attack Detection”, International Journal of Security and its Applications, vol. 5, **(2011)**, pp. 73-90.
[3] F. Bingbing, “Common network attack platform for research and application”, Confidentiality of Science and Technology, **(2010)**, pp. 56-59.
[4] The West Point Information Assurance Battle Lab designed, http://www.china.com.cn/ chinese/junshi/ 871235.htm.
[5] The Information security engineering practice comprehensive experimental platform, Shanghai Jiaotong University, http://topics.sjtu.edu.cn/newsdisplay.php?id=1518.
[6] Several key network security technology and Prevention experimental platform, Chinese Academy of Science, http://www.kepu.net.cn/gb/innovative_project/strategic/intro/200503160011.html.
[7] P. Fei, Z. Qiusheng, G. Jifeng and S. Qifeng, “Design of Network Attack and Defense Training Platform”, Zhongyuan Institute of Technology, **(2004)**, pp. 5-8.

[8] A. Hamou-Lhadj and A. Hamou-Lhadj, "A Governance Framework for Building Secure IT Systems", International Journal of Security and Its Applications, vol. 3, **(2009)**, pp. 15-20.
[9] S. McClure, J. Scambray and G. Kurtz, "Hacking Exposed Network Security Secrets & Solutions", Computer Mcgraw-Hill, **(1999)**.
[10] G. Lei, F. Yu and P. Shulin, "Software Framework Construction Based on Plug-in Technology", IEEE Computer Society, **(2011)**.
[11] X. Hua, L. Feng-xin and P. Xiao-li, "Theoretic analysis and application of windows dynamic link library", Journal of Beijing University of Chemical Technology, vol. 31, **(2004)**, pp. 99-102.

Authors



Li Gen is studying in Harbin Institute of Technology (abstract as HIT) as a Master graduate student. He got Bachelor's degree from HIT in 2012. His research is mainly on network security, information security.

Wang Bailing is working for Harbin Institute of Technology (abstract as HIT) as an associate professor. He got the Ph.D. degree from HIT in 2006. His research is mainly on information security, network security, parallel computing.

Liu Yang, Associate Professor, Liu Yang, his research fields include Network information Security Technology, Internet of Things Security Technology, etc. He has participated in many projects of Ministry of Information Industry and National Science, and he has published over 20 academic papers in journals and conferences both home and abroad.