A Scalable Network Attack Platform Design[1]

Li Gen, Wang Bailing*, Liu Yang

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

Abstract. For the current network security events occur frequently and new cyber attack methods continue to emerge, this paper proposes a scalable network attack platform framework. The system can integrate existing methods of attack and help the operator to complete a full step experimental network attack. In addition, the system is designed with plug-in technology and has good scalability, integration. The operator can use the platform to test new type of network attack methods by making them into plugins, so that to learn and study them in more detail. Therefore design a scalable network attack platform has a very high level of teaching and practical significance.

Key words: Network security, Attack platform, Scalable, Plug-in technology

1 Introduction

We all know that the 21st century is the age of information technology. 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 [1].

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 [2], the Information security engineering practice comprehensive experimental platform designed by Shanghai Jiaotong University [3], Several key network security technology and Prevention experimental platform designed by Chinese Academy of Science [4], Network attack and defense training platform designed by Zhongyuan University of Technology, 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.

2 System Design

2.1 System Function Design

[1] Supported by the National Science Nature Foundation of China under Grant No 61170262

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 [6], the system includes the following main modules:

- Control and display: Module that interacts directly with the users of the platform.
- Information collection: The module's main function is to complete the scanning on the target system and information profiler.
- 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.
- 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.
- 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 Fig. 1:

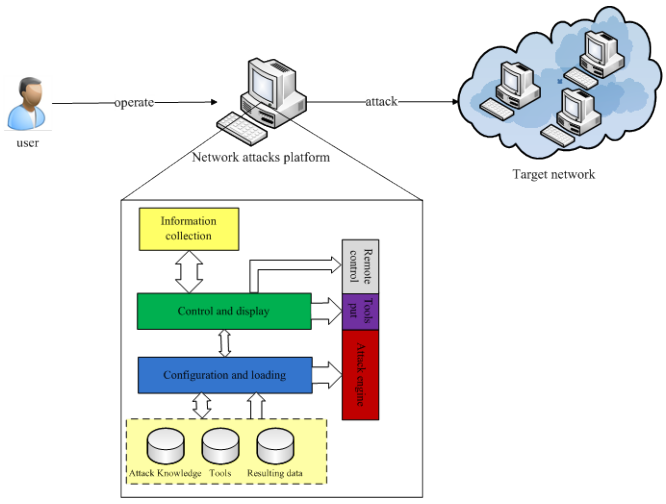

Fig. 1. System block diagram

3 System Testing Experiment

3.1 System Environment

In order to verify the functionality and performance of the system in a laboratory environment, the hardware configuration shown in Table 3.1.

Table 3.1 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 Fig. 4. Attack platform is in the campus network, and test target is hosts of other campus LAN.

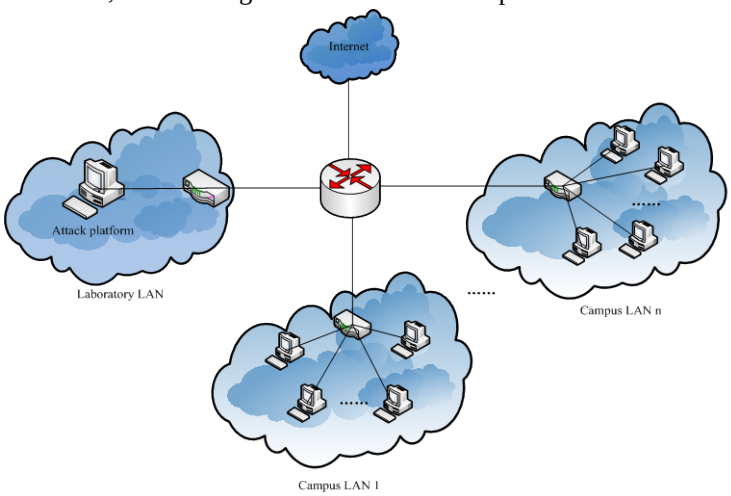

Fig. 4. The attack platform network topology

3.2 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 3.2 and Table 3.3 shows.

Table 3.2. 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 3.3 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

4 Conclusion

For different network attacks are difficult to study and test, this paper proposes a scalable network attack platform. The platform can be integrated with the existing network attacks and make them plugins that stored in the Attack Knowledge Base. It can guide the platform operator complete experimental network attacks. The platform can reproduce a variety of well-known network attacks and help the operator get a clear understanding of the network attacks works. Moreove, the platform can also be used to study and test a new type of network attack. 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.

References

1. Fan Bingbing.: Common network attack platform for research and application, Confidentiality of Science and Technology, 56--59 (2010)
2. The West Point Information Assurance Battle Lab designed, http://www.china.com.cn/chinese/junshi/871235.htm
3. The Information security engineering practice comprehensive experimental platform, Shanghai Jiaotong University, http://topics.sjtu.edu.cn/newsdisplay.php?id=1518
4. 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
5. Pei Fei, Zheng Qiusheng, Guo Jifeng, etc.: Design of Network Attack and Defense Training Platform, Zhongyuan Institute of Technology, 5--8 (2004)