Method of Network Security Situation Analysis

Jin Jin
College of Electrical Engineering
Northwest University for Nationalities
Lanzhou, China
e-mail: jinjin_2000@163.com

Song Jian*
College of Electrical Engineering
Northwest University for Nationalities
Lanzhou, China
e-mail: ljf2010@sohu.com
*Corresponding Author

Tian Changhui
School of Foreign Studies
University of Science and Technology Beijing
Beijing, China
e-mail: tian_changhui@aliyun.com

Abstract—Now with the wide use of computer network and e-commerce, network security has become an important problem that it must be considered and resolved. More and more professions in the enterprises and individuals are subjected to the security problem in different degree. It is looked for the more reliable safety solutions. In the rapid development of the networks, emphasis on network information security is growing. Through analyzing the network information security factor, several common network information security policies are proposed, and the system of network information security is formed. By using virtual machine technology, network attacks and network protection subsystem are virtually out on a server, the configuration management of the vast majority of current network operations and network attack protection can be realized. The training environment of network attack and defense with function is more comprehensive, more superior performance and more realistic simulation experiments degree. Then, network security threats and defense strategies are summarized in this paper.

Keywords-experimental platform; information security; security threats; protection system

I. INTRODUCTION

With the development of information technology, today network has become an important part of people's lives [1-4], people are dependent on the network information increasingly, but the network security has also drawn people's attention, so the reasons affecting the network security is analyzed again, proposing the countermeasures of protecting network security becomes very important. In order to solve these security issues, a variety of security policies, security tools have been developed to be applied. And experimental platform is designed [5].

The research about the network attack and defense experiments or training system is that the building of the network attack experimental platform based on virtual honey net by Hui Dong and Jian Ma. For the shortcomings of traditional passive defense network security Teaching Experiment Platform, researching the key technology of virtual machine and honey net, to build the network security Teaching Experiment Platform based on virtual honey net technology, and give the processes achieving the core function of the platform. It is that Design and Implementation of SITL based network attack and defense simulation platform by Hong shan-kong and Jun tang. For lack of network simulation tool in network security simulation, leading ring technology to the building of the network attack and defense platform, to the problems of the lack of network attack model, the application layer does not respond to the attacks, security functional modeling difficulties. In order to better carry out experiments and training related network attack and defense, designing a comprehensive network attack and defense training platform for experiments, both in the platform to carry out experiments related to network attacks, and network protection. Therefore, it can provide users with the training environment of Network attack and defense experiment, which has the following characteristics are more comprehensive function, more superior performance, more realistic degree of simulation [6-8].

II. NETWORK ATTACK EXPERIMENTAL PLATFORM

Network attack simulation platform composition structure is shown in Figure 1, the composition of the hardware structure of the network attack and defense training platform consisting mainly of terminals, which including high-performance servers, routers, switches, test equipment. Throughout the network hardware configuration, routers and switches are for the interconnection of network attack and defense simulation platform, two main servers provide virtualization operating environment for network attack and defense training, the use of high-performance server enables virtual applications of the multiple terminals on this server. With virtualization technology, network attacks subsystem and network protection subsystem are virtual out on the both servers. The user terminals of network attack and defense training platform are the terminal computers which are for the user to log in and use the network attack and defense training platform. Using each terminal computer, users can connect to the network attack and defense training platform .And on each user terminal itself installed virtual machine software, in order that four virtual terminals are virtual out on a virtual terminal, so some of the small local network

attack experiment can be implemented on the user terminal computer by virtual terminal. When the user wishes to carry out a large-scale experiment network attack and defense, it can be connectted to a train platform server. A plurality of application terminal are virtual out by the server, which are set to the application terminal of attack subsystem, or application terminal of protection subsystem. Each application terminal is applied in network management and configuration application of the attacks subsystems and network protection subsystem, so that each application terminal becomes an integral part of the attack subsystem or protection subsystems. After this, users can take advantages of a variety of application tools which come with by attack subsystem or protection subsystem to carry out network attack and defense experiment, also on the virtual terminal, and use the secondary development platform and the secondary development application interface which are provided by virtual terminal, targeted to develop a series of network attack and defense applications, enabling flexible network attack and defense practice operations [5-6].

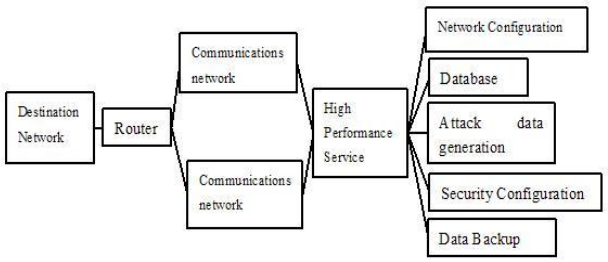

Figure 1 Experimental Platform

During the process of the design and implementation of the network attack and defense training platform, the first step is to buy the corresponding network equipment, building hardware infrastructure network attack and defense training platform. Then install all client terminals and all network servers which are on the offensive and defensive training platform virtual machine software, and complete the application configuration of network attacks subsystems and network protection subsystems respectively. Throughout process of the design and implementation, the application configuration of attacker subsystem and protection subsystem is the crucial element during the process. Two application subsystems can configure some kinds of function, some kinds of application tools provided for users, which directly determines the content of the network attack and defense training operations carried out on the experiment platform by user. Moreover, the secondary development interface provided by the network attack and defense training subsystem, also directly determines whether the user can use the platform to facilitate the flexibility to design some targeted network attack and defense applications [9-11].

III. SECURITY THREATS OF NETWORK INFORMATION

Network security threats are everywhere, the vulnerability of the network system itself, mistakes of the user operation, artificially malicious attacks, network viruses etc [8].

Firstly，it is the vulnerability of the network system itself. The biggest advantage of network technology is open, because of this wide open, it is the greatest threat to network security, the security of TCP/IP protocols that the network relies on is not too high, the network system itself running the protocol has spoofing, denial of service, data interception and other threats.

It has mistakes of the operation by user. The user's own security awareness is not strong, setting a password is relatively simple, or the user is at liberty to reveal their own account, which will pose a threat to network security.

Then, it is artificially malicious attacks. The greatest threat the network information facing is this artificially malicious attack. But malicious attacks are divided into active and passive attacks. Active attack refers to the various ways to undermine the integrity of information and validity. Passive attacks are under the situation to steal, to decipher and get important confidential information without affecting the proper work of network. Both of which attack the network information will cause great harm, and lead to leakage of important data.

Lastly, it has so many network viruses. Network virus can be stored, implemented and hided in the executable program without being discovered. When it is triggered, it is available to some executable program which the system is controlling, it has the infection, latency and trigger, destroy and other characteristics. Copy files and transfer files are the most important means of network virus transmission.

IV. NETWORK ATTACK SUBSYSTEM DESIGN

Network attack subsystem is to simulate and implement a variety of common network attack operation, to provide users with a good interface and a wealth of attack tools, it allows users to take advantage of this subsystem to carry out attacks experiments effectively .The realization of network attacks subsystem relies on the corresponding application configuration of network attacks on the virtual machine or special tools to implement various functions of network attacks subsystem. The composition structure of network attack subsystem is shown in Figure 2, the network attacks subsystems is designed in the article, including DDOS attacks, vulnerability scanner, ARP spoofing program, network renovation program, the middleman attack code and common network exploits source. Through these common attack programs or modules included in the network attack subsystem, the typical network attacks can be achieved on the target system or target network. Among them, the network exploits source code means that some exploits source is specifically developed on the basis of the security holes existed in the network operating system or some application software. Since the exploits of source in the actual application process, often requires a combination of the characteristics of the actual application environment and application objectives to carry out more targeted network attacks. Therefore, in the practical application process, the network attack subsystem often need to cut or modify the exploits source code to ensure that exploit source code can play a real attack results on the target system. To this end, this design of network attack subsystem includes a secondary development interface, which can modify, debug and dynamic configuration exploits source code which comes with network attack subsystem and also implement some user-defined attack and attack process. The network attack subsystem itself

carries a variety of common network attacks module, which can simplify the difficult of network attacks experiment, and help users take advantage of these network attack tools, to carry out a comprehensive experimental network attacks against some of the more complex a system or the target network. Using secondary development interface provided by attack subsystem can make the user adjust dynamically the attack tactics and attack methods and develop some time-sensitive, flexible network attack source according to problem reflected from the process of network attack and combing with the reality vulnerability status of the existence of the target system. Therefore, the design of the network attack subsystem is not only to provide users with the experimental verification of network attack and defense, but also to provide users with some design and innovative network attacks experiments [12-13].

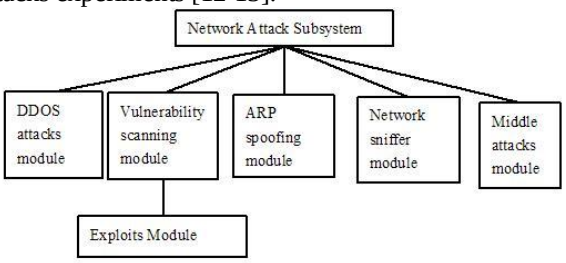

Figure 2 Attack subsystem

V. COMMON NETWORK INFORMATION SECURITY POLICIES

While the security of network information subject to appropriate threat, but to take appropriate protective measures can effectively protect the network and information security, so make the following points [14-15].

Strengthening the security of user accounts is that User account involves a wide range, including login ID and e-mail account. Firstly, set up complex system login account password, try not to set the same password or similar account and change your password regularly and set a long password.

Install a firewall and anti-virus software is that the so-called network firewall is a means to strengthen controls access between networks, to prevent external network users from entering the internal network by illegal means, to protect the special networking equipment of internal network. it checks the data packets transmitting between two or more network, according to certain security policies, to determine whether the communication between the network are allowed, and knowledge network running. Firewall and anti-virus software package to installments-virus software is the security technology which are often used, this technique is mainly for the virus, killing the virus, and now the mainstream anti-virus software can also defense Trojan program and some hacking program, but anti-virus software must be able to effectively defend the provincial level only.

Promptly install Vulnerability patch is that Vulnerability is the weaknesses which can be utilized during the process of attack, such as software, hardware, procedures shortcomings, functional design or improper, when there are loopholes in the system program, , it will cause great security risk, and in order to correct these vulnerabilities, software vendors will release a patch, what is needed to do is to install a timely manner vulnerability patch to effectively solve security problems posed by vulnerable program.

Installation of intrusion detection and network monitoring technology is that Intrusion detection is a kind of protection technology recently developed, using a combination of network communication technology, artificial intelligence, cryptography, reasoning, methods of rule, techniques and methods, its role is to monitor the network if there are signs of intrusion and abuse. According to the analytical techniques used can be divided into a signature analysis and statistical analysis. Signature analysis is used to detect the behavior attacking the known vulnerabilities of system. People summarize its signature from the attacking method, writing to Dos system code, signature analysis is actually a template matching operation. Statistical analysis method based on the theoretical basis of statistics, is used to identify whether an action deviated from the normal track, based in movement patterns observed under situation that the system work normally.

Installation file encryption and digital signature technology is that file encryption and digital technology is one of the main techniques used to improve the security and confidentiality of information systems and data, and to prevent secret data being stolen or destroyed outside. Depending on the action, file encryption and digital signature technology is classified into data storage, data transfer, data integrity. The digital signature is an effective way to solve the uniquely security problem in network communication, which enables the identification and verification of electronic documents, and play a very important role in data integrity, privacy and non-repudiation.

VI. DESIGN OF NETWORK PROTECTION SUBSYSTEM

Design composition structure of network protection subsystem is shown in Figure 3. This design of network protection subsystems mainly include is that detection module, Trojans killing module, the antivirus module, system process monitoring module, firewall network traffic monitoring module, port monitoring module and system log module. The main application purpose of the network protection subsystem is to provide users with the operation related to the management and configuration of network protection experiments, through the operation, users can understand and master the use and operating skills of a variety of network protection tools. At the same time, through the status and various phenomena which are exhibited in the actual application process network protection subsystem. According to the design target of network protection subsystems, the user can flexibly and dynamically configure and manage a variety of applied sub-modules shown in Figure 3 in order to improve network security protection level of the target system. Using the design of each application module of network protection subsystem, the user can use the system process monitoring module and port monitoring module to monitor and manage the processes which are running on the target system. And to monitor the network port connected to the current computer. Network traffic monitoring module monitors the data traffic, and if the data traffic of target system is abnormal in the actual application process, it will

prompt user to analysis the network data flow to detect whether there are abnormal data traffic, and then find out if there are some malicious network attacks. Viruses and Trojans check module can provide users with more comprehensive coverage for the currently running computer security, to prevent some malicious viruses or Trojan to invade target computer. A firewall is a valid application module for the target system to network security management. Firewall applications are often combined with network traffic module, and port monitoring module used in conjunction, when the user found abnormal in the current target system through the network traffic and communication port monitoring module, the firewall is used to prevent some unusual communication port or communication processes to block or intercept the data communication, preventing the user's target computer from illegal attacks from remote networks. Intrusion Detection System is a comprehensive network protection system, which comprehensively analysis and judge whether the current target system has suffered from the network various security threats. System log module is the module which recorded all operations of the target system, which will provide users with an important means to analysis network security situation and tracking network attacks.

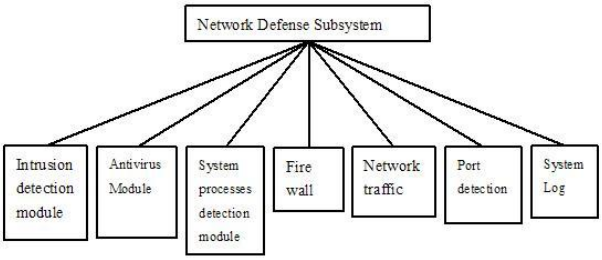

Figure 3. Defense Subsystem

According to the function and application provided by network protection subsystem, it can provide a comprehensive, flexible and configurable network protection subsystem for the user. Users can conduct experiments and training content related to network attack and defense in the environment through the various functions of the subsystem.

VII. CONCLUSIONS

In conclusion, it shows that network attack experiment is on the experimental conditions demanding, and because of the huge destructive of network attacks, making network attack experiments cannot be carried out on the general Internet. This will make the design of the network attack and defense training platform become very necessary. Network attacks and network protection subsystems is that the virtual is on the server through virtual machine technology, it enables the vast majority of configuration management of the current network attacks operation and network protection.

ACKNOWLEDGMENT

This work is supported by the Fundamental Research Funds for the Central Universities of China for Northwest University for Nationalities (Grant No. 31920140087), the Introduction of talent project for Northwest University for Nationalities (Grant No. xbmuyjrc201312).

The authors would like to express thanks to Prof. M. J. Khan with the School of PN Engineering, National University of Sciences and Technology, Islamabad, Pakistan and Prof. J. Cao with the Research Institute of Information Technology, Tsinghua University, Beijing, China for their beneficial discussions.

REFERENCES

[1] N. Cai, J. Cao, H. Ma, C. Wang, "Swarm stability analysis of nonlinear dynamical multi-agent systems via relative Lyapunov function", *Arab. J. Sci. Eng.*, vol. 39, pp. 2427-2434, 2014.

[2] N. Cai, J. Cao, M. J. Khan, "A controllability synthesis problem for dynamic multi-agent systems with linear high-order protocol", *Int. J. Control Automat. Syst.*, vol. 12, pp. 1366-1371, 2014.

[3] N. Cai, M. J. Khan, "On swarm stability of linear time-invariant descriptor compartmental networks", *IET Control Theory Appl.*,vol. 9, pp. 793-800, 2015.

[4] N. Cai, J. Cao, M. J. Khan, "Almost decouplability of any directed weighted network topology", *Physica A*, vol. 436, pp. 637-645, 2015.

[5] H. Dong and J. Ma, "The building of the network attack experimental platform based on virtual honey net",*Qiqihar University: Natural*, vol. 28, pp. 67-72, 2013.

[6] Y. Wang and H. Yang, "The design and implement of network attack and defense training simulation system based on plug-in components", *Computer Technology and Development*, vol. 20, pp. 172-174, 2011.

[7] H. S. Kong and J. Tang, "Design and Implementation of SITL based network attack and defense simulation platform", *Application of Computer*, vol. 28, pp. 172-174, 2012.

[8] F. F. Zhou and J. Pan, "DOS nuke attack and defense simulation under the OPNET environment", *Shanghai Maritime University*, vol. 29, pp. 86-90, 2014.

[9] M. Q. Zhang and J. Xie, "The modeling and simulation of the denial of service attack based on OPNET", *System Simulation*, vol. 20, pp. 2736-2739, 2010.

[10] D. J. Xiao and S. J. Yang, "Network Security Evaluation Model. Journal of Huazhong University of Science and Technology",*Natural Science*, vol. 30, pp.37-39, 2012.

[11] F. Pan and P. Sun, "A practical and efficient design and implementation of network attack and defense training simulation system", *Information Security and Communications Privacy*, vol. 07, pp.327-331, 2013.

[12] Q. N. Yan, "Discussion of Computer Network Security and defense", *Manager*, vol. 11, pp. 335-336, 2014.

[13] W. Q. Cheng and Z. R. Yang, "Network Programming Experimental Design and Teaching", *Experiment Science and Technology*, vol. 8, pp. 99-101, 2013.

[14] P. Lu, "Discussion of computer network security and protection policies", *Silicon Valley*, vol. 12, pp. 62-62, 2014.

[15] Q. Y. Chen, "Design and implementation of network attack and defense experimental models", *Experiment Science and Technology*, vol. 3, pp.39-41, 2013.