ISSN : 0974 - 7435 Volume 10 Issue 22

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(22), 2014 [13804-13808]

Design and implementation of performance evaluation for network information security system

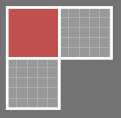
Hualin Huang
Guangdong Women's Polytechnic College, Guangzhou, 511450, (CHINA)

ABSTRACT

The performance evaluation of network security system generally requires combining vulnerability scanning technology and expert system in order to better discover security vulnerabilities existing in the system, also conducive to a comprehensive assessment of the overall network security, and be able to offer a complete and improved security reports. With the rapid development of network technology, requirements on network security have become more and more sophisticated, but related mature testing methods have been behind the overall growth rate, therefore, there is a need to establish a new set of performance evaluation for network information security. This paper proposes an evaluation of separating the control and experiment, establishes a new two-tier testing system of network information security, whose test results can provide a better theoretical basis and reference value for actual design and evaluation. First, the study reviews the current testing methods at home and abroad. Then it explains the working principle, architecture platform and application of this system, and studies on the safety requirements of the components and application of environmental analysis. At last, overall performance evaluation is made according to the actual test results, testing methods are verified to meet the requirements, and the entire test methods are summarized. From the verification, it can be seen that the testing program has a repeatable, fast and automotive features, and can help testers design more rational and effective test environment, besides, the entire testing process is very simple and test efficiency is very high.

KEYWORDS

Network information security system; Testing approach; Performance evaluation.



INTRODUCTION

Network and information security has been treated as a main factor of national security and social stability by all countries over the world in the 21st century. Its importance can never be ignored with the pace of the globalization of information. Especially with the Internet, the security is more vulnerable to virus attacks from the outside, facing dangers of the entire network information being stolen, modified, etc., or evens a network paralysis. Network information security system is a comprehensive discipline with lots of disciplines involved, its main purpose is to protect the network hardware and software, and data from destroy, disclosure, alteration, and safeguard the stability of the network system. Generally, network information security system is composed by several major components such as a firewall, intrusion detection system (IDS), encryption system, authentication system, anti-virus system and safety evaluation system[1]. With these components, the network attacks, viruses and other Internet hazards can be timely detected and dealt with, and emergencies can be treated too. But now for the testing and evaluation method of network information security system is not perfect, there is no unified and mature testing standards, methods, software, especially the majority of users are unable to effectively complete the test comparison of the product[2]. To solve this problem, countries around the world have launched the relevant testing standards to judge whether the network information security system meets the requirements.

RESEARCH STATUSES AND BASIC STRUCTURE

Definition of network information security system

The main responsibility of network information security system is to protect the information content communicated, processed and used by network system, to ensure its integrity and confidentiality, as well as safeguard the relevant technologies, structures and management equipments[3]. In general, it is to ensure the use network information by legitimate users and enable them with related operations processing within the permissible range, meanwhile to prevent unauthorized users' attack.

Theoretically there is no totally secure network information system, but it is necessary to follow certain basic principles from the start of design to ensure the safety of the final network information system. If the design is flawed, it is a considerable danger for the latter reparation. As for the design principles of network information security systems, there are generally the following aspects:

(1) Cannikin Law: The protection of information security should be a comprehensive one.
(2) The Integrity Principle: Establish flawless emergency management measures of prevention, detection and recovery, reduce the losses to its maximum.
(3) Limit the users' powers, and reduce misuse and illegal operation of the system by non-administrator users.
(4) Establish a hierarchy of network information system security, and the storage will be processed according to the security level, such as top secret, confidential, secret. By so, targeted security algorithms and constitution can be provided to meet the actual needs[4].
(5) Principle of Effectiveness and Practicality: Under the protection of the safety, reduce the calculating amount of security operations, while ensure the normal operation of the network and for the legitimate operation.

Main security problems

Openness and sharing make network systems the essential item in people's lives, and it is the same features that make the network systems vulnerable to alien attacks and destroy. Even if some of the unintentional destruction will bring the common legal users a great deal of disadvantage, even loss of property[5]. There are the following four main causes of danger to the network information.

(1) Sharing, as one of the fundamental purposes of the network information system, is also a problem most vulnerable to illegal attack;

(2) Complex computer systems result difficulties in its safety management;

(3) Scalability, as a feature of computer network information system, brings risks of uncertain network boundaries. Some unauthorized users can easily access to legitimate users' information, which poses a huge threat to their information security;

(4) Multipath is the main characteristic of information and communication networks, which also leads to ineffective protection to a particular aspect of communication, where unauthorized users will be able to attack the loopholes endangering the users' information security.

Facing numerous illegal acts of sabotage attacks, the normal legal means cannot control effectively, and therefore the reliability of network information security system has become the most important fortress. Countries across the world have devoted a lot of manpower and resources on security-related technologies to protect the network information data from theft, damage and so on. The causes of these security problems are mainly from the following three aspects[6].

(1) Loopholes existing in the internal network protocol. As the cornerstone of the Internet, internal loopholes will make the entire network system vulnerable to attack. For instance, PRISM of the USA is to disguise and deceive the IP address entering the system by the back door for illegal collection of information.

(2) Computer viruses. They are great in destruction and concealment, difficult to be effectively prevented. Computer viruses have become the most serious and severe threat.

(3)Loss or disclosure of network information by users themselves. This is mainly because most users lack adequate safety awareness, and there is no relevant technical means, resulting nothing can be done to cyber attacks.

Therefore, in building a network information security system, the above mentioned information needs to be fully analyzed, and the internal relation and laws between users and network need to be explored and sketched so as to improve the overall security.

DESIGN OF TESTING SYSTEM

The traditional practice of network information security system test is fixed network topology, but the test system is extremely inconvenient due to the lack of flexibility and the need of too much manpower. There is other approach of simulation using applications, but its authenticity and reliability is greatly reduced. By comparison, the new test method proposed in this paper is very efficient and flexible, and it can also retest and be configured according to the actual situation, not only to meet the basic safety test, but also collect and analyze data.

Structure and principle of the system

Test system uses the IP network architecture program, and users or testers can easily access to allocated resources at the far end mainly through remote access and control tools such as VNC, PuTTY. Figure 1 shows a schematic diagram of the system in detail.

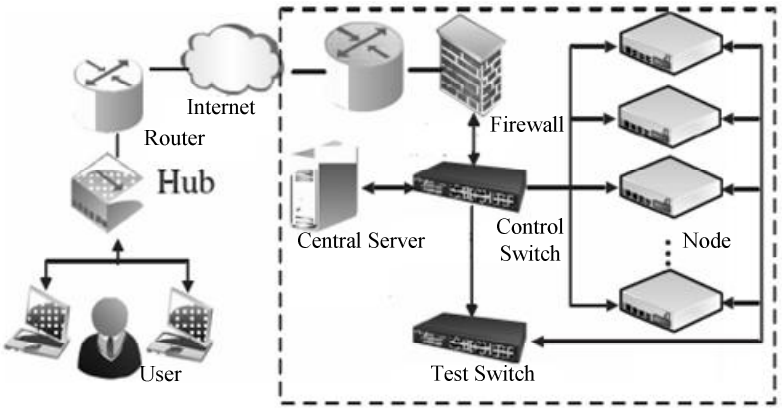


Figure 1 : Principle diagram of the test system

The test system has the appropriate initiating service software installed on all nodes, so the user can test through a local client. As can be seen from the diagram, the system is a double layers network applying a multi-radio node configuration method, and finally to control and test the network through controls and experiments with network card respectively. This design can well achieve the requirement of physical isolation, and also can ensure the greatest degree of safety and reliability.

Besides, the system provides two views according to the requirements of different users (as shown in Figure 2). View in Figure 2 (a) is aimed primarily at ordinary users[7] to facilitate their access to the required test environment; view in Figure 2 (b) is for professional system managers and testers, providing distributed portioned views and cluster, including equipments of the central server, control switch and test switch.

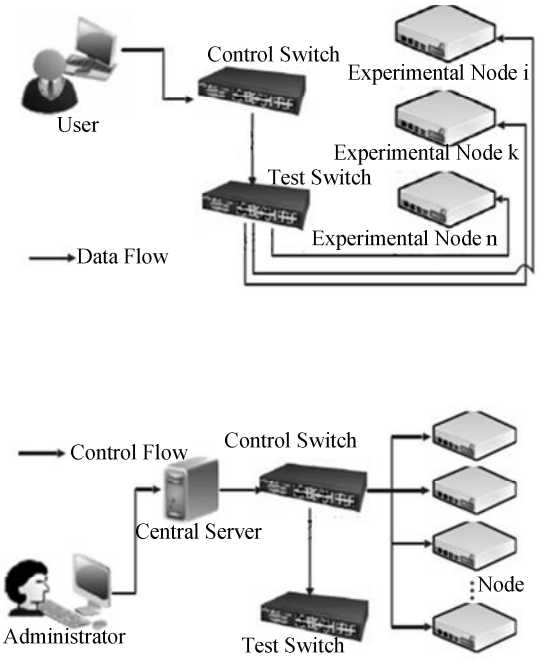


Figure 2 : Users' system view

Functional design of the test system

The test solution for network information security system in this paper is mainly composed by three layers, namely resource layer, platform layer and user layer, and the entire management functions run through the whole system layers. Here are detail introductions.

(1) Resource Layer. Resource layer is to provide a shared pool of resources for the platform layer, composed by VMWare virtual machine clusters[8] and the physical machine clusters. The main purpose is to facilitate demands of different levels of users to the maximum. This is beneficial in variety of application needs to get support from the required type of server nodes of its own. There is resource management module for related management, generally including cluster management and node management. Cluster management is to monitor, configure and maintain clusters and other tasks, such as monitoring CPU usage, system temperature, etc; and node management is to monitor and maintain running of a node, such as creating a virtual machine and resolving problems of downtime and so on.

(2) Platform Layer. It belongs to the core layer of the test system, its duty is to create a user-defined test environment based on the underlying shared pool of resources, and maintain and manage this environment. After the user selects the network information security test template, it comes to the corresponding configuration, where changes can be personalized according to the users' own actual demand. Then send the configured list to the central server. When the test environment configuration is finished, users or testers can make relevant experiments and research on information security. When an experiment is over, it can be closed, and then the used resource will be returned to the test system for repeated use. Of course, the test environment configuration can also be deleted.

The test system also set some monitoring tools, mainly to a clear real time understanding of the operation state of the entire server. And more information can be analyzed from the monitoring records. Here also contains a relatively simple network security actual assessment mechanism, which is to provide comprehensive unified management, analysis and cluster of network security incidents, then form a unified view, such as traffic statistics, attack statistics, vulnerability and so on. Thereby, the user can make associative analysis of these events, filter false alarms. Evaluation module generally consists of various types of probes, the for-end agent and data collection processing, system configuration, event and knowledge databases and other components.

(3) User Layer. The main object is administrators and researchers. This layer allows administrators to manage and maintain the entire system, and researchers to process test tasks, as well as manage and maintain the test environment.

Verification of the test system

In the test, each node is configured with at least two straight board card, mainly as control network card and experimental network card respectively. It also requires four three-layer gigabit switches. Then enter the system as administrator, check the available nodes of the system. Meanwhile configure the test model. The system provides verification-driven, design-driven and comprehensive security testing repository. Generally there are two kinds of verification-driven security testing template, namely false attacks and news-gathering attacks.

Users can create their own personalized actual test environment using templates. Here is the method. Select the required template, then comes to the Web-based GUI network topology design interface, use it to modify the content of node size and IP address. After the completion of the personalized settings, it can be submitted to the test system, as shown in Figure 3.

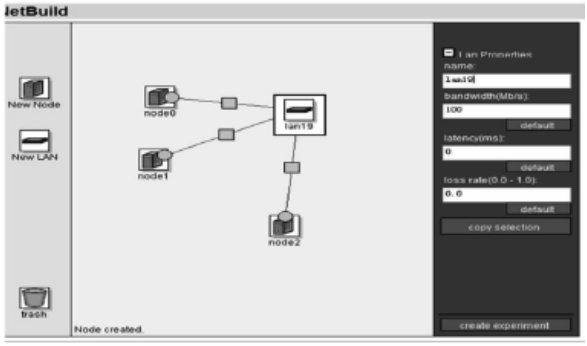


Figure 3 : Schematic construction of individualized testing environment

TABLE 1 : Average time required for construction of network topology

System Type/Node Size	1	10	30	50	70	90
Windows XP SP2	11.4	12.1	12.4	12.9	13.2	13.8
Ubuntu 12.04 32bit	4.2	4.5	4.7	5.1	5.5	6.1
CentOS 5.5 64bit	4.8	5.0	5.4	5.9	6.2	6.9
FreeBSD 7.3 64bit	3.5	3.8	4.2	4.8	5.2	5.5

Next, create a personalized user network topology using various operating system images provided by the system (such as Windows XP, Fedora, etc.), thus establishing the final physical test environment. TABLE 1 shows the currently average time required to create a test environment of multi-node star topology. It is obvious that the speed of large-scale network system construction is far beyond the physical network created manually.

CONCLUSION

With the advent of the information era, network security has become a long-standing problem which can never be underestimated. The network information security has become the focus of the protected objects, so there must be a set of comprehensive security defense system to better protect the security of information. The test system proposed in this paper can be said an effective one, and significantly simplifies the hardware structure. The effects have been shown clearly through the explanation of its working principle and system structure. Currently the test system is still in its testing phase, and there are still many problems to be solved, which requires the joint efforts of researchers.

REFERENCE

[1] Liu Ying, Tian Ye; Performance evaluation for network information security system[J], Computer Engineering, **32(20)**, 140-142 **(2006)**.

[2] Atwal, Maya; Edw in Bacon, The youth movement Nashi: Conten-tioous politics, civil society, and party politics [J], East European Politics, **28(3)**, 256-266 **(2012)**.

[3] Luo Kaitian; The design and implementation of network information security system in ethnic universities[J], Journal of Chifeng University(Natural Science Edition), **28(10)**, 42-44 **(2012)**.

[4] Meng Xueqi; About the establishment of the computer network and information security system and technology to explore[J], Network Security Technology & Application, **(8)**, 86-87 **(2014)**.

[5] Liu Yang; Design and implementation institute of network information security system[J], Coal Technology, **30(3)**, 227-229 **(2011)**.

[6] Wang Peiguo, Fan Dong; Risk analysis and countermeasures of network information system security [J], Communication & Information Technology, **(3)**, 86-88 **(2011)**.

[7] A.Dolgikh, T.Nykodym, V.Skormin et al.; Computer network testbed at Binghamton university[C], Military Communications Conference, 2011-milcom 2011, IEEE, 1146-1151 **(2011)**.

[8] B.Ward; Book of vmware:the complete guide to VM ware work station[M], Barkeley, CA: No Starch Press, **(2002)**.

[9] J.Mink; The basal ganglia : Focused selection and inhibition of competing motor programs[J], Progress in Neurobiology, **50(4)**, 381-425 **(1996)**.