2017 5th International Conference on Computer, Automation and Power Electronics (CAPE 2017)

Design and Implementation of Computer Network Vulnerability Assessment System

Hongqing Liu

Hunan vocational college of modern logistics,Changsha, Hunan,410131

Keywords: Computer network, Security, Assessment, Vulnerability.

Abstract. with the rapid development of computer network technology, in the sharing of network information at the same time, there is inevitably a security risk, network security issues have become the focus of the current network technology research. Network security risk assessment technology can detect the potential security vulnerabilities and vulnerabilities of network system, and evaluate the security status of network system, which is one of the important technologies to realize network security.

1. Introduction

With the rapid development of computer network technology, global informatization has become a major trend in the world development. In today's information society, computer network plays a more and more important role in politics, economy, military and daily life, so that people's dependence on computer network is greatly strengthened. The existing computer network in the beginning of the establishment of the most overlooked security issues, and most of the TCP/IP protocol, the TCP/IP protocol has defects in the design, because the TCP/IP protocol to the efficiency in the design, it is mainly caused by factors of network security. Because the computer network has connected form characteristics of the diversity and openness, connectivity, the network is vulnerable to various attacks, so when people fully enjoy the network brought convenience and fast and at the same time, should also be fully aware of the network security faces severe challenges.

2 .Network Security

2.1 definition of network security

Network security refers to the computer network system of hardware, data and procedures not destroyed, tampering, leakage due to unintentional or malicious, to prevent unauthorized use or access, the system can keep the continuity of service, and run reliably. The specific concept of network security varies with the angle of interest. From the user's perspective, they hope that some of their top secret information transmission on the network can be effectively protected, to prevent confidential information on the user to destroy some illegal eavesdropping, tampering, posing as a person through the means of.

From the network security administrators, they hope that the local network information access, read and write operations can be protected and controlled effectively, avoid denial of service resources, illegal occupation, illegal control and other threats, which can prevent hacker attacks. For some of the country's Secret departments, they want to filter out some illegal and harmful information, while preventing the leakage of confidential information, so as to avoid or reduce the harm to society and the country as much as possible. Network security involves both technology and management. The technical aspect mainly aims at the exterior illegal invader attack, but the management aspect mainly aims at the internal personnel's management, these two aspects supplement each other, are indispensable.

2.2 basic requirements of network security

1. confidentiality (Confidentiality), which refers to the data, programs and other information in the network will not be leaked to unauthorized users or entities. That information can only be used by authorized users, it is an important means to protect the security of network systems. Integrity (Integrity) refers to the fact that the data, programs and other information in the network remain unchanged without authorization. That is, the data, programs and other information in the network will not be tampered with, deleted, forged, replayed and so on during the transmission process. Availability (Availability) refers to the information that can be accessed by authorized users or entities in a network and can be used as required. That is, network information services can still provide effective services to authorized users or entities when they are permitted to use by authorized users or entities, or when the network part is destroyed and need to be degraded. Reliability (Reliability) refers to the characteristics of a network system capable of performing specific functions at a specific time and under specific conditions. Reliability is the most basic requirement of network system security. Controllability (Controllability) refers to the ability to control the spread and content of network information. It can ensure the network information security monitoring.

6. non repudiation (Non-Repudiation) refers to the authenticity of the identity of participants in the process of information interaction in the network system. It can ensure that the sender can not deny the information he sent, and through digital evidence, evidence preservation, so that the notary can easily intervene, through the law to manage the network.

3. Vulnerability Research in Network Security Evaluation

Vulnerability refers to the shortcomings and defects of computer or network system in hardware, software, protocol design and implementation, and the security policy adopted by the system. The direct consequence of vulnerability is to allow illegal or unauthorized users to access or improve access rights, thereby giving the attacker an opportunity to destroy the network system.

Generally speaking, the vulnerability of computer network system is mainly caused by the programmer's unsafe programming and error operation, the defects of the network protocol itself and the user's wrong use and setting. The main points are summarized as follows.

(1) setting errors

It mainly refers to the error settings of system administrators or users, and the system vulnerability caused by error setting is very popular with attackers, so it is also the most common vulnerability. Many manufacturers in the market products for users to set up many default parameters, the settings of the main purpose is to fully trust of users, easy to use for new users, but these settings may bring great security for computer network system.

(2) design errors

It refers to the design, because the programmer some back door design due to his negligence and for their own convenience, this kind of vulnerability is hard to find, but once found it is difficult to repair, it security threats to the network system is very large, this kind of vulnerability only through the re design and implementation.

(3) the defects of the network protocol itself

It refers to the security problems caused by the defects and deficiencies of the network protocol itself. Refers to the computer network protocol in order to comply with the common rules of Internet and computer network at present, most of the TCP/IP protocol, TCP /IP protocol to open and efficiency in the design stage, the lack of overall concept of safety and design, so there are a lot of vulnerability, leaving many security risks.

(4) input validation error

It refers to the validity of the user's input data validation, leading to illegal access to the system attacker. Most buffer overflow vulnerabilities and CGI class vulnerabilities are caused by this. This vulnerability exists in the dump command of RedHat6.2.

(5) access validation errors

It means that the access authentication part of a program has a logic error that can be exploited, which may allow an illegal attacker to skip access control and enter the system. This vulnerability exists in the early AIX of rlogin.

(6) handling errors in unexpected situations

It means that the program does not take into account some unexpected circumstances in the implementation logic, resulting in running errors. This is a common mistake, for example, if you don't check whether the file is present, you open the device file directly and cause denial of service.

(7) competition conditions

It refers to the problem of timing and synchronization in the process of dealing with entities, and may provide an opportunity window in the process of dealing with an illegal attacker. This type of vulnerability exists in the PS commands of the early Solaris system.

(8) environmental error

It refers to the vulnerability created by the error settings of some environmental variables.

4. Network security situation management and its prediction problem

Network situation refers to the current status and changing trend of three networks that are composed of various network equipment running status, network behavior and user behavior. Network situation awareness refers to the network environment, can cause changes in the network situation to obtain, understand, evaluate, display and predict the future development trend of [6]. In a dynamic and complex environment, decision makers need to use situational awareness tools to show the continuous changes of the current environment, so as to make decisions accurately. Therefore, the research and prediction of network security situation is of great significance to the management of network security and the healthy development of the network.

4.1 Network security situation management problem

Relevant statistics show that China's broadband network scale, the number of users, the national top-level domain name registration amount of three indicators in recent years ranked first in the world, and its growth rate over the years also showed a steady growth trend, the Internet has become a basic tool for the Chinese people's daily life and work of the. But the safety management and the development prospects of China's Internet is not optimistic, only the first half of 2011, encountered a virus or Trojan attack Internet users reached 217 million, accounting for 44.7% of Internet users, with account and password theft experienced Internet users reached 121 million people, accounting for 24.9%, the detection data of Conficker worms and also showed that [6] the severe form of network security situation in our country.

Usually, network managers usually spend a lot of data to purchase firewall, anti-virus software and other network security tools to solve the attack behavior from inside and outside the system. At the same time, these tools record a large number of network security data in the form of logs and alarms, while preventing attacks inside and outside the system. But these data are too large, scattered, messy, difficult to directly solve the problem and management, can not form a real timely guidance knowledge of security response. The application of these data mainly has the following five problems: [6]:

1) the number of security data is too large, it is difficult for network security managers to find useful information directly;

2) false alarms interfere with the normal operation of the network;

3) the security data are scattered and disorderly, and the security incidents are not easy to find;

4) the security situation is lack of real-time monitoring, and the alarm response is seriously lagging behind;

5) lack of fresh data in safety management, and risk assessment can not follow up

The problem of the management in order to solve the problem of network security situation, must abandon the complicated and redundant, wrong alarm information, grasp the trend of network security situation, effective attack behavior, found in the network monitoring network status, effectively guide the network security management, so that the network security management from passive to active, the operation of network security effective.

4.2 Research on network security situation prediction

Through literature review, we can see that there are three main methods to study network security situation, [7], that is qualitative analysis method, quantitative analysis method [4][6], qualitative and quantitative analysis method [2][5]. The qualitative analysis method is to analyze the factors that affect network security. Quantitative analysis refers to the data mining and analysis of the model from the mathematical point of view through the analysis of the relevant data of the network security situation. Because the influence factors of network security situation is complex, qualitative analysis is difficult to establish accurate model, we forecast the current network security situation is mainly through quantitative analysis and quantitative and qualitative analysis method.

According to the characteristics of network security situation, the researchers put forward lots of security situation prediction method, the quantitative analysis method such as time series analysis method, based on D-S evidence theory, combining quantitative and qualitative analysis as shown in the literature [2], [6]. Among them, the qualitative and quantitative analysis method has higher prediction accuracy and stronger persuasion, but for different problems, the influencing factors are not the same. The quantitative analysis method can solve the problem of network security situation only by studying the changing trend of the problem data and selecting the appropriate mathematical method. Through access to information, according to the characteristics of network security situation prediction problem, put forward a kind of quantitative analysis method, BP neural network prediction method based on genetic algorithm, effectively solves the combination of qualitative and quantitative model of highly nonlinear problems and difficulties of network security situation data.

5. Summary

Prediction and evaluation of network security situation of work safety management work has a significant guiding role, at present, the network security situation in our country is still in the exploratory stage, especially in many aspects such as algorithm of index system is not mature, qualitative analysis is more difficult. Neural network and genetic algorithm for quantitative analysis of the data prediction provides a powerful tool, this paper gives full consideration to the impact of network security situation is complex, high degree of nonlinear data, proposes a BP neural network model based on genetic algorithm, the effective use of existing data, to solve the extremum problem is highly nonlinear and the model of network security situation prediction factors and more complex, not easy to find and network security situation data, accurate short-term prediction model is established, the accurate tracking trends in network security situation, which makes the structure more scientific and reasonable network situation prediction.

References

[1] Jennifer W. Chan, Yingyue Zhang, and Kathryn E. Uhrich, Amphiphilic Macromolecule Self-Assembled Monolayers Suppress Smooth Muscle Cell Proliferation, Bioconjugate Chemistry, 2015, 26(7), 1359-1369.

[2] Yingyue Zhang, Evan Mintzer, and Kathryn E. Uhrich, Synthesis and Characterization of PEGylatedBolaamphiphiles with Enhanced Retention in Liposomes, Journal of Colloid and Interface Science, 2016, 482, 19-26.

[3] Yingyue Zhang, AmmarAlgburi, Ning Wang, VladyslavKholodovych, Drym O. Oh, Michael Chikindas, and Kathryn E. Uhrich, Self-assembled Cationic Amphiphiles as Antimicrobial Peptides Mimics: Role of Hydrophobicity, Linkage Type, and Assembly State, Nanomedicine: Nanotechnology, Biology and Medicine, 2017, 13(2), 343-352.

[4] Jonathan J. Faig, AlyshaMoretti, Laurie B. Joseph, Yingyue Zhang, Mary Joy Nova, Kervin

Smith, and Kathryn E. Uhrich, Biodegradable Kojic Acid-Based Polymers: Controlled Delivery of Bioactives for Melanogenesis Inhibition, Biomacromolecules, 2017, 18(2), 363-373.