Network Security Risks and Defensive Measures under IPv6 Environment

Lei JIANG

Audio-visual Information Center of Guangdong Food and Drug Vocational College, Guangzhou, Guangdong, China

jiangl@gdyzy.edu.cn

Keywords: IPv6 environment, Network security risks, Defensive measures

Abstract: Under the environment of IPv6, the network operation is complex, and there are many new applications, putting forward an important test for the security protection of network operation. In view of this, this paper expounds the network security risk problems, security defensive measures and the construction of dynamic defensive system under IPv6 environment, and analyzes the security defensive measures, including vulnerability scanning, firewall manual detection system and network security audit system, hoping to provide valuable reference for the construction of scientific and effective IPv6 network security operation environment.

1. Introduction

IPv6 network operation solves the limitation of IPv4 network operation and releases the space of network operation. However, due to the lack of access to effective management measures and security protection measures, IPv6 network operation is faced with many security loopholes. These problems make the network operation security unable to be guaranteed, causing illegal tampering, illegal intrusion and other problems. In view of this, we should aim at the network security risks under IPv6 environment to build effective defensive measures, so as to ensure the demand of network security operation.

2. Analysis of Network Security Risks under IPv6 Environment

Compared with IPv4, IPv6 has made great progress in application and achieved the effective expansion of application functions. However, IPv6 application in the network also faces many problems, especially the network security risks, which greatly restricts the efficient use of computer Internet functions. The main security problems include hacker intrusion defense, loss of response after IDS denial of service, firewall under ACL control list unable to work, poor response after DOS denial of service, etc. These problems restrict the development of Internet applications and bring application problems. In addition, in the current operating environment, IPv6 also has some new security problems, mainly including the following points.

First, IPv6 management experience is insufficient. The management of IPv6 operating environment often takes the help of IPv4 management experience, but there are essential differences between IPv6 and IPv4 in operation. For example, in the use of SNMP technology, whether through external introduction or self-development, we should fully consider its security, but in fact, there is no experience to learn from the monitoring method of technology, and there is no advanced, mature and applied equipment to assist in troubleshooting, analysis and positioning. Therefore, under the IPv6 operating environment, the security risk coefficient is high, difficult to ensure the efficient operation of computer network.

Second, the research and development of IPv6 security technology is lagging behind. The same as the safe operation of IPv4, IPv6 needs the corresponding security measures, such as anti-virus gateway, network filtering, VPN, vulnerability scanning, etc., but the research results about the virus situation of IPv6 operating environment and the feasible security defensive measures have not yet appeared.

Third, the simplification of network protocol authentication in IPv6 environment is not

Copyright © (2021) Francis Academic Press, UK DOI: 10.25236/icited.2021.104

conducive to the effective restriction of different users, which provides a hotbed and entrance for unsafe network intrusion, leading to virus intrusion, hacker attack and other destructive behaviors. In addition, the network application of IPv6 has been expanded, and the wide application of mobile devices has been realized. For this is a new field of network operation, the research of network security operation measures needs to be further strengthened and updated.

Fourth, there are many uncertain and nonstandard factors in the management and operation of security equipment, which restrict the implementation of network security defensive system. For example, DHCP matching with IPv6 is not practical and needs to be upgraded and updated, but there are no relevant research results on the upgrade and update. In addition, PKI management is a new problem in IPv6 operation without corresponding solution.

3. Network Security Defensive Measures under IPv6 Environment

In the process of the transition from IPv4 to IPv6, there is an intermediate transition of IPSee. This transition is only the transition between network environments, and does not involve the transition of network security defensive strategies. Therefore, the network security in IPv6 still needs basic security protection strategies, such as vulnerability scanning, firewall, manual monitoring system, etc.

3.1 Vulnerability Scanning

In the environment of IPv6 network operation, the security defense of vulnerability scanning is an important measure to ensure network security, but there are still essential differences between the network security scanning of IPv6 and that of IPv4. Usually, the vulnerability security scanning of IPv4 is aimed at the monitoring of the Internet and the server in the temporal LAN, which is installed on the network management machine. In the intermediate transition stage of IPSee, the environment of vulnerability security scanning has not changed, but the scanning object has changed, mainly for IPv6 host and two-way host scanning, and the layout position has also changed accordingly. Scanning in the IPv6 phase can also use the corresponding means to achieve the maintenance of the security system. By setting the corresponding IPv6 scanning function in the original scanning, we can achieve the scanning and monitoring of network vulnerabilities. Because the vulnerability scanning is realized through the scanning module, which has the attribute of highly performing tasks, and there is no rigid requirement for the scanned tasks in the specific execution process, so we can modify the module to scan the vulnerability of IPv6 network.

3.2 Firewall

Compared with IPv4, IPv6 network realizes the effective expansion of network applications, so it has the application attributes that IPv4 does not have. It not only has some common properties in IPv4 operating system, but also has some special properties, such as IP processing problems, port connection problems and IPSec inline problems in mobile Internet access. These are new problems in the current network operation. How to use the firewall to protect the safe operation of the network needs in-depth research and analysis to make the firewall have a strong matching. On the one hand, it can solve the new problems in the operation of IPv6 network and ensure the safe operation of the network. On the other hand, it can adapt to the expansion of IPv6 and provide space support and guarantee for the development of IPv6 network.

3.3 Intrusion Detection System

With the continuous upgrading of network security defense technology, the application of new technologies, such as the data mining technology, appears in the IPv6 network environment. The application of this technology simplifies the intrusion procedure, improves the intrusion efficiency, and has an important positive significance to ensure the safe operation of Internet. On the one hand, it uses data mining technology to collect, analyze and research big data information, find the regularity of orientation, and form an effective defense intrusion detection system, which plays a significant role in dealing with the intrusion of complex information. On the other hand, data

mining technology simplifies the data detection program, especially the extraction of some complex coding, greatly improving the detection efficiency. Secondly, data mining technology not only has the advantage of efficient data collection, but also has the advantage of high applicability. It can realize the data processing of different complex structures, so it can adapt to different network operation environment. Therefore, although IPv6 network operation environment is different from traditional general network operation environment, it can also realize the efficient guarantee of network operation environment through the effective access of data mining system. According to the different structures and data characteristics of network operation environments, the main application methods of data mining technology in intrusion detection system are classification, sequence, association and so on.

3.4 Network Security Audit System

Under IPv6 environment, different operations will be involved. Some of these operations are normal to meet the use of work and functions, while some operations are abnormal, destroying the system. The network protection system needs to monitor these operations comprehensively to protect the safe operation of the network. The IPv6 environment needs network security audit system to monitor and analyze all the operations in the network operation. The protection mechanism is mainly realized by making corresponding rules. The scope of protection includes internal scope and external scope. For example, the monitoring of internal network security mainly includes information acquisition audit monitoring, document content audit monitoring, resource transfer audit monitoring, etc. In addition, when some safety factors are found in the detection, the corresponding warning will be given.

Under IPv6 environment, the audit system construction for network security mainly protects two aspects. The first is the construction of internal system, and the main function is to ensure the safe operation of the internal use of the computer, such as preventing malicious tampering and destruction. This kind of safeguard not only protects the network operation security of the internal system of the computer under IPv6 environment, but also provides relevant data reference for network security questions. The second is the construction of external system, mainly preventing the intrusion of external information. The defensive system can intercept the sabotage program and behavior, timely discover some illegal intrusion behaviors and send warning signals, playing an important role in effectively avoiding the security problems of the external intrusion of computer network.

4. Construction of Network Security Dynamic Defense under IPv6 Environment

The IPv6 network operation environment is complex, and the intrusion technology continues to upgrade iteratively. How to realize the real-time monitoring of the network system and realize the all-round protection of the network security plays an important role in ensuring the network operation security. In view of this, we should build a real-time, dynamic network security dynamic defensive system, in which the general defensive model is PDRR model, mainly including four aspects: detection, protection, warning and system recovery. However, this kind of security protection system can’t cover all the detection of security problems under the dynamic changes of the network. We should build a dynamic defensive system and enrich the system. For example, security protection includes not only the protection of network security problems, but also the protection of predictive security network problems, so as to realize dynamic detection and prevention, and reduce the occurrence of network security intrusion. In short, with the increasingly complex network environment, network intrusion technology continues to upgrade and network security problems can’t be avoided. Optimizing the network defense structure and upgrading the defense system can effectively avoid the occurrence of security problems.

5. Conclusion

The network operating environment under IPv6 environment is complex, and the network

intrusion technology is constantly upgrading. The construction of security defense system can effectively reduce the network security problems. However, the imperfect network equipment and management under IPv6 operating conditions cause the security problems. The security defense measures mainly include vulnerability scanning, firewall, manual detection system and network security audit system. In addition, due to the complexity of the network operation environment, we need to build a dynamic defense system to realize the comprehensive detection and protection of the network operation environment.

References

[1] Dai Renjie. Network Security Risks and Defense Measures under IPv6 Environment. China High-tech, no.15, pp.143-144, 2020.

[2] Lin Zheng. Discussion on Network Attack under IPv6 Network Environment. Digital Communication World, no.12, pp.112, 2019.

[3] Tian Yanwei, Li Jie, Shi Zhenyu. Security Risks and Challenges of Recursive DNS System in IPv6 Environment. Network Security Bureau of the Ministry of Public Security. Proceedings of Forum on Internet Security and Governance in 2019 [C]. Network Security Bureau of the Ministry of Public Security: *Information Network Security*, Beijing Editorial Department, pp.4, 2019.