Research on Computer Network Intrusion Detection System

Yong Xia[1, a] Min Lai[2, b]

[1 2] Gannan Medical University, Ganzhou, Jiangxi, China, 341000

[a]email, [b]email

Keywords: Computer Network, Intrusion, Detection System

Abstract. With the development of economy and technology, computer network plays in people's lives more and more important position, while security problems caused by the network more and more attention has been paid each year because of network security issues, such as hacking, virus infection economic losses caused by the annual increase has reached millions of dollars. This requires us to make greater efforts to develop Internet security technology research, design more effective network security system.

Introduction

With the development of computer networks, global information has become a major trend in human development. However, due to the diversity of computer networks have links, terminal and non-uniform distribution of open networks, connectivity and other features, resulting in computer networks vulnerable to attacks by hackers, malware, and other misconduct, online security and confidentiality of information, becomes a critical issue. For the transmission of sensitive data in a computer network system, its online security and confidentiality of information is particularly important. Therefore, the computer network must have a strong enough safety measures, otherwise the network will be a useless and even endanger the national security of the network. Whether in a local area network or wide area network, there is vulnerability and potential threats of natural and man-made, and many other factors. Network security measures should be able in all directions for a variety of threats and vulnerabilities, so as to ensure the confidentiality, integrity and availability of network information. Network security is increasingly becoming a key factor restricting the development of the network.

Network security is information related to computer science, network technology, communication technology, cryptography, information security technology, applied mathematics, number theory, information theory and other disciplines comprehensive discipline. Network information security is the network hardware, software, data and systems are protected from accidental or malicious reasons those were to destroy, change, disclosure, continuous and reliable system to run properly, the network service is not interrupted. Broadly speaking, all related to the network confidentiality, integrity, availability, authenticity and controllability of the relevant technology and theory of information are the network information security research.

Intrusion detection as a proactive security technology provides internal attacks and external attacks and misuse in real-time protection, endangered before the network system to intercept and respond to the invasion. From the perspective of network security in depth, multi-layered defense point of view, intrusion detection by the people's attention, but the status quo is not mature enough intrusion detection, stage of development, the current domestic intrusion detection products substantially increase control on the basis of SNORT interface for analysis and detection technology is no substantive progress. Most current intrusion detection products using a single packet pattern matching detection method. Single packet pattern matching detection methods have showed a lot of problems, many international companies have invested efforts on the next generation of intrusion detection technology.

Existing intrusion detection methods can only achieve good results for certain or known intrusion, sometimes false alarm rate, affecting the performance of the system. And increase the effective detection or prevention of the occurrence of known and unknown intrusions, reduce the false alarm rate and improve the security and stability of the system, it has been an important

subject of active defense technology research. To improve the performance of intrusion detection systems, will be integrated, cooperation, so as to optimize selectivity to introduce the idea of intrusion detection system in an attempt to solve a single flaw detection method in the protection effect. The purpose of this research is that in the current domestic popular intrusion detection techniques and methods to analyze the intrusion detection technology, and to improve it, to design an efficient, secure, cross-platform, intrusion detection systems, network security system thus established and developed the new intrusion detection products has an important role and inspired a certain practical significance.

The Concept of Intrusion Detection System

Intrusion detection system is a system for identifying and responding to network resources and computing resources for malicious behavior. A perfect IDS system should have the following characteristics: Economy: Economic cost is not too high; timeliness: must detect intrusion; security: IDS system itself must be secure. Intrusion detection technology and its role as a safety in that: (1) identify the intruder; (2) identify intrusions; (3) testing and monitoring have been successful security flaws; (4) to provide important information in a timely manner against the invasion, to prevent the occurrence of an event and larger scale.

Intrusion detection systems can autonomously computer network, real-time attack detection and response. Reincarnation network security monitoring, allowing users to customize interrupted before the system is broken and respond to security breaches and misuse. It automatically responds to security threats for businesses provide maximum security. Upon detecting network intrusion, in addition to promptly cut off the attack, but also can dynamically adjust the firewall protection policies, so that the firewall has become a dynamic and intelligent protection system. Intrusion detection system that monitors and analyzes user behavior, system configuration and vulnerability audit, assessing the integrity of sensitive systems and data, to identify aggressive behavior, abnormal behavior statistics, automatically collects and system-related patches, an audit trail to identify violation behavioral safety regulations, the use of decoy server ---- record hacking and other functions, the system administrator can more effectively monitor, audit and evaluate their own systems.

The Development of Intrusion Detection Technology

Distributed Intrusion Detection. As the complexity of network intrusion methods and network computing environment, research and application of intrusion detection are increasingly turning Distributed Intrusion Detection System. Distributed Intrusion Detection System, among the components requires a lot of information exchange, in order to ensure the security and integrity of interaction information, which requires research and design common information exchange formats, and encrypted communication mechanism to prevent an attacker to decipher interaction information thus attack the entire intrusion detection system. In addition, the design of safe and effective detection algorithms, distributed intrusion detection is another important area of research. Focus is on secure communication mechanism based on PKI, this mechanism can effectively implement authentication and encryption detection information described between components; two new methods in intrusion detection system testing and analysis: (1) immune fuzzy logic and genetic algorithms the sequential pattern analysis method (2) clustering algorithm through simulation, test results show that using these two methods can effectively detect abnormal attacks, improve the accuracy of detection.

Intrusion Detection Based on Feature Engine Analysis. With the increasing network traffic and speed, rapid detection engine has become an important indicator of performance. How to improve the intrusion detection engine speed has always been a hot research question. Feature-based intrusion detection engine, from two aspects, one is how to effectively organize the growing invasion of rules; the second is when the packet with the invasion pattern matching rules, what kind of pattern matching algorithms to accurately detect the rapid intrusion. Using Snort

system as an experimental platform, the system is a feature-based network intrusion detection system in the world's most widely put the source code in the industry has an important position. Snort detection engine in two comparative analysis of the traditional two-dimensional linear list detection engine intrusion method organization rules, the method of decision tree classification rules tissue invasion. According to the rules at the time of the invasion of constructing decision tree classification based on attribute selection criteria has a great influence on the shape and depth of the decision tree.

Intrusion Detection System Based on Data Mining. Data mining goal is to extract implicit, unknown and non-trivial and has potential application of information or patterns from large databases or data warehouse, and intrusion detection is also analyzed data from a large number of extract useful information, make judgments, which coincides with the idea of data mining technology. Data mining in intrusion detection system, using data mining techniques in the analysis of association rules and frequent sequential pattern analysis technology to improve the corresponding algorithm, dig out potential security information collected from the host system and network behavior record mining host system and the internal network behavior recording mode, the mining system and network behavior analysis mode data between recording with frequent patterns with correlation analysis. These modes automatically builds intrusion detection system and normal behavior pattern library intrusion pattern base, and automatically update the library with the normal behavior pattern changes in the environment, achieve intrusion defense.

Intrusion Induced Control Technology Based on Network. Is a network intrusion induced control and intrusion detection and analysis can make security technology active control. This method phishing technology, host phishing technology and dynamic configuration technology, presents a new network intrusion induced control platform model, the purpose is to use the lure of virtual control technology advanced features of flexibility and dynamic configuration techniques to improve network invasion induced control performance, for the overall architecture and packet interception model, network deception, deceit host, dynamic configuration module design and implementation, and through experiments to implement each key is tested. System-level program implementation, the deception network module using a tree data structure to build virtual routing, deceiving host module, the introduction of OS fingerprinting simulation method increases the ability of the model to deceive, while introducing the concept of dynamic configuration for the entire model using an active probe dynamic configuration and combination of passive detection, when the internal network protected state changes its configuration can be adjusted to increase adaptability.

The Issues and Challenges Facing the Intrusion Detection

Improve the detection rate of intrusion detection system to meet the requirements of network traffic. The processing speed of network security devices has been a major impact on network performance bottleneck, although generally less inline IDS access network, but if it detects the speed to keep up with data transmission speed of the network, then the system will detect where missing part of the data packets, resulting in false negative affect the accuracy and effectiveness of the system. In IDS work, each network packet interception, analysis, whether the match in which the characteristics of an attack takes a lot of time and system resources, so most of the existing IDS detection rate of only a few dozen megabytes, with large number of applications, the speed of the Fast IDS technology development, and even Gigabit network has lagged far behind the development of network speed.

Reduce false negatives and false positives intrusion detection system to improve safety and accuracy. Analysis method based on pattern matching IDS intrusion and all its variants means of expression as a mode or feature, feature detection data network in major discriminating whether gathered in the library intrusion patterns, so while facing every day new attack methods to generate and publish new vulnerabilities, an attacker cannot update signature database IDS is caused by failure to report a major reason. The anomaly-based IDS discovered by traffic analysis system to establish normal behavior of the track, when the value of the system is running beyond the normal threshold is considered likely to be attacked, the technology has led to the wood itself of its high

false negative rate of false positives. In addition, most of the IDS is based on a single packet inspection, protocol analysis was small enough, and therefore does not recognize the disguised or deformed network attacks, but also caused a large number of false negatives and false positives.

Improve the interactive performance of intrusion detection system to improve the safety performance of the entire system. In large networks, with a small part of the network may use a variety of intrusion detection systems, and even security firewalls, vulnerability scanning, and other categories of each set, and how between these workers and intrusion detection systems and other security components DS to exchange information and work together to detect attacks, respond; to prevent attacks is an important factor in the security of the entire system of relations.

Intrusion protection systems and then only a smart security management tools cannot solve all problems. For network security, the real work is the people. Good technical infrastructure in favor of IDS efficient role to play, but the technical architecture as an intermediary only provide a basic platform, even though again advanced data collection or data analysis techniques, it was a medium extension. IDS as a security policy and means can be deployed in a wide range of types and sizes of companies which, at the same time, companies also require the existing security system should be gradually optimized to meet the new security policy.

Conclusion

With the development of Internet and the popularity of network technology, the new network security problems will continue to emerge. Any kind of network security technology is not facing a balky network, but a growing, evolving complex entity. Therefore there is no existence of a once and for all, forever effective network defense methods. The danger is absolute, security is relative. In attack and defense into the contest, waiting for network security professionals is a lot of work.

References

[1] Jia Xinzhang, Li Jingyuan. Computer Engineering, Vol. 6 (2014) No 53, p.25-26

[2] Peng Sue, Wang Yunhui, Wang Qunyong. Journal of Software, Vol. 12 (2015) No 27, p.74-76

[3] Qian Xiyuan. Computer Engineering and Applications, Vol. 30 (2014) No 19, p.144-145

[4] Wang Kuailiang. Computer Simulation, Vol. 29 (2011) No 27, p.21-23

[5] Zhang Gongxu, Sun Jing. Computer Engineering, Vol. 8 (2013) No 27, p.57-60

江西省赣州市渡口路 7 号南阳东升 2 栋 2 单元 504 室
手机号码：13907078663　收件人：赖敏