IOSR Journal of Research & Method in Education (IOSR-JRME)
e-ISSN: 2320–7388, p- ISSN: 2320-737x Volume 11, Issue 6 Ser. I (Nov. – Dec. 2021), 33-36
www.iosrjournals.org

Research on Network Virus Intrusion Prevention System Technology

Pengwei Li
（Department of Computer Teaching, Anyang Normal University, Anyang China）

Abstract: *With the continuous improvement of hacker attack level and the continuous increase of network intrusion events, network security has attracted more and more attention. As a new network security technology, intrusion prevention system has superior performance that ordinary firewall and intrusion detection do not have. This paper focuses on the basic working principle, technical characteristics and types of intrusion prevention system, introduces three main problems faced by intrusion prevention system IPS, and finally gives a summary and prospect.*

Keywords: *Network virus； Intrusion Prevention System; Network Security; Invasion examination*

Date of Submission: 10-11-2021 Date of Acceptance: 26-11-2021

I. Introduction

With the continuous improvement of hacker attack level and the continuous increase of network intrusion events, network security has attracted more and more attention. As a new network security technology, intrusion prevention system has superior performance that ordinary firewall and intrusion detection do not have. This paper focuses on the basic working principle, technical characteristics and types of intrusion prevention system, introduces three main problems faced by intrusion prevention system IPS, and finally gives a summary and prospect. With the increase of network users, the inconsistency of users' knowledge level and the difference of users' Ideological and moral cultivation, hackers attack the network more and more, and the level is higher and higher. Because more and more hosts are infected by virus and Trojan horse attack, the contradiction is that the time required to kill virus and Trojan horse and clear Trojan horse increases instead of decreasing, The network has been damaged for a longer time. This situation can't be controlled by traditional firewall and intrusion detection technology. The passive situation needs to be changed. Intrusion prevention system is a security technology to solve this situation.

II. Concept and requirements of intrusion prevention system

Intrusion prevention system is a more active security technology than traditional intrusion detection system. It can not only monitor the network and warn the network threat, but also deal with the threat in time, play the role of preventing attack, but also manage it. Usually, the intrusion prevention system is deployed at the boundary of the network and connected in series with the firewall. The firewall keeps most obvious attacks out of the door. The intrusion prevention system further analyzes the possible attacks released by the firewall and actively responds to the determined attacks to better ensure the security of the system.

However, because the intrusion prevention system and firewall are connected in series on the network, because the data packets filtered by the firewall and intrusion prevention system will be superimposed on the delay, which will have an impact on the normal and legal data flow. The delay in the event of an attack event may be greater, and even become the bottleneck of network traffic, seriously affecting the performance of the whole network. Therefore, in order to keep the intrusion prevention system busy, we may also need other security technologies to work together, such as network access control technology. By forcing the security of the terminal host connected to the network, we can eliminate the spread of worm virus or Trojan horse attack caused by the vulnerabilities of the terminal system in the network, so as to reduce the burden of the intrusion prevention system. In fact, hackers in the network also like to pick soft persimmons. Generally, hackers scan some network segments through scanners and find loopholes in the network before attacking. Forcing the security of the terminal host through the network access control system can basically prevent most network attacks, but it is not easy to deal with some "fixed-point" attacks. At this time, we can introduce a deception system, such as honeypot system. First, a simple hacker can be induced to attack the deception system. Through the analysis of the attack, we can know the hacker's attack tactics and study the corresponding defense measures; Second, it distracts the attention of

hackers and ensures the security of internal network; Third, it can also deter hackers, because no hacker wants to be known about his attack.

III. Intrusion prevention principle

The intrusion prevention system analyzes whether there is a threat to the data entering from the external network and judges whether to filter or send it to the internal network. This behavior feels very similar to the firewall, but it is different from the firewall. The firewall generally only checks the data packets and works at the network layer. Some firewalls can also filter at the fourth layer, but can't prevent the attack behavior of the application layer, The intrusion prevention system can check all attacks from the data link layer to the application layer, which is a bit like the strengthening or supplement of the firewall. Therefore, the firewall and the intrusion prevention system are often connected in series on the network. The firewall is deployed on the outermost side, and the layer 3 or layer 4 attacks are filtered out first, The remaining traffic is further analyzed and processed by the intrusion prevention system.

Firstly, the intrusion detection system classifies the incoming packets, and different types of packets are transmitted to different filtering modules for analysis. Then, each analysis module analyzes the data packet according to the pre-designed feature code. If the filtering conditions are met, the data packet will be directly discarded, and the data packet that cannot meet the filtering conditions will be released. In intrusion prevention system, different filtering modules need to be designed for different attacks. Each module matches the data packets by defining corresponding feature codes. Each module is not independent of each other. Each module can be designed into a series and parallel hybrid combination to match complex and parallel attacks. The filtering process is controlled by an intelligent chip to ensure fast processing speed and no increase in network delay. And for new vulnerabilities, as long as a new filter module is added or the feature code in the existing filter module is modified, the operation is convenient.

IV. Intrusion prevention system architecture

Intrusion prevention system is developed from intrusion detection technology. In addition to the ability to detect network attacks, it can also deal with attacks in real time and actively protect the network.

Intrusion prevention system can sometimes be understood as an intrusion detection system with firewall function, which is an organic combination of the two. Firewall has advantages in dealing with TCP / IP data flow. It judges whether it is legal by detecting some fields in the protocol data unit. The filtering statement is rough and rarely deals with the data content. Intrusion detection is just complementary to it. It is specially designed to detect possible threats in the data, but it does not deal with attacks, This needs the help of firewall to filter data, so the combination of the two is inevitable and understood by many people. But in fact, intrusion prevention is much more complex than this, and it is difficult to implement. Otherwise, it will not take more than 10 years for the product to be basically accepted by the administrator. Of course, this is also inseparable from too many missing and false reports of the intrusion prevention system. After all, it takes a lot of attempts to design a reasonable filter, Fortunately, the continuous development of security technology research has been able to control the identification error rate of threat code within the acceptable range of users.

V. Classification of intrusion prevention system

Intrusion prevention system can be divided into host type and network type.

(1) Host intrusion prevention system

Host intrusion prevention system is to realize intrusion prevention on the host. It is generally realized by installing virus killing software, firewall software and vulnerability scanning software on the host. These software constitute the security defense system of the host. When the host is attacked, the defense system ensures the system security. Usually, the host intrusion prevention system is installed on the server to ensure the security of the server.

From a technical point of view, the host intrusion prevention system filters data, checks the state of data flow, and analyzes the call of various applications to system data in real time to find attacks and suspicious behaviors. On the premise of ensuring the system throughput, the system blocks attacks and suspicious behaviors, and protects the system security to the greatest extent. At present, it has been proved that the host intrusion prevention system can prevent known buffer overflow attacks, web Trojan horse attacks, unauthorized use of system resources and other attacks through feature matching and behavior monitoring, and can also monitor suspicious attacks.

(2) Network intrusion prevention system（NIPS）

The host intrusion prevention system is very effective to ensure the security of the terminal host. However, if an attack is not against the host, not to obtain some resources of the system, but against the network, such as DOS attack and ARP spoofing attack, the host intrusion prevention system is difficult to deal with, this

requires another intrusion prevention system - network intrusion prevention system. Network intrusion prevention is different from host defense system, which realizes intrusion attack analysis through software or agent program. Generally, it can only be realized through special hardware equipment. Network intrusion prevention system generally has more than two network cards, one for connecting to a secure network (intranet) and one for connecting to an insecure network (extranet).When the network intrusion detection system receives traffic on a network card, it sends the traffic to the detection engine for processing. This step is the same as that of the intrusion detection system. It determines whether it is an attack or a suspicious attack through feature matching. If it is an attack, the defense system immediately blocks the data and does not send it to the exit, which can't be realized by the intrusion detection system. For suspicious behavior, the suspicious behavior shall be released or discarded according to the security policy, and the administrator shall be informed to make further analysis to reduce missing and false reports.

Technically, the network intrusion prevention system makes full use of the mature technologies of the current network intrusion detection system, such as feature matching, protocol analysis and anomaly detection. Among them, feature matching is the most important part. The feature code extracted from the analysis of known attacks is encoded to select the data stream quickly and accurately. In fact, this function was the main function of the early system, and other functions were slowly integrated later. Because signature attacks can only be analyzed through feature analysis, it is difficult to judge insertion attacks and avoidance attacks, which requires the introduction of more complex protocol analysis. At present, this technology is relatively mature. Through protocol analysis, the network status is monitored based on the analysis of data flow to find suspicious and abnormal access behavior, so as to ensure network security more comprehensively. Although anomaly detection technology is also used in intrusion prevention system, it is not too mature in technology, with more false positives and less use.

NIPS benefits include:

①The network intrusion prevention system is deployed at the network checkpoint to protect the whole network. It is a global monitoring point. It can take the overall situation into account and implement security policies more conveniently than the host intrusion prevention system.

②The network intrusion prevention system works at the network layer and can take into account the underlying devices (devices in the network). It does not need to consider the compatibility between software and operating system like the host intrusion system.

③It is effective to deal with denial of service attacks in the network.

VI. Challenges faced by intrusion prevention system

At present, IPS technology needs many positive challenges. Generally speaking, there are three main aspects.

(1) single point of failure. In terms of design requirements, IPS must work in embedded mode in the network, which may cause single point of failure or bottleneck problems. If IPS fails, some attacks will not be detected in the most serious case. However, when the embedded IPS device fails, the normal operation of the network will be affected. If it is shut down due to IPS failure, users will face a denial of service problem caused by IPS, and each user will not be able to access the applications provided by the enterprise network.

(2) performance bottlenecks. Since IPS must keep pace with the network traffic of thousands of megabytes or more, especially when a large number of detection feature libraries are loaded, the IPS embedded device with unreasonable design will not be able to support this response speed. Even if the IPS equipment does not fail, it is still a potential network bottleneck, which will not only reduce the efficiency of the network, but also increase the lag time. Therefore, at present, most high-end IPS product suppliers use customized hardware to improve the operation efficiency of IPS.

(3) Missing and false positives. The false negative rate and false positive rate are also the problems that IPS should seriously face. In the increasingly busy network, if you count by 20 alerts per second, IPS has to process at least 72000 alerts per hour, 1728000 a day. Once the alarm is generated, the minimum requirement is that IPS can effectively handle the alarm. If the intrusion characteristics are not perfect enough, it will give an opportunity to "false positives", which may cause the legal traffic to be accidentally intercepted. Once an aggressive packet is intercepted, it will intercept all data streams from suspicious attackers. If the traffic that triggered the false alarm is just part of a customer's order, the whole session of the customer will be closed, and the consequences can be imagined. After that, all legitimate accesses of the user reconnecting to the enterprise network will be blocked by IPS.

VII. Summary and Prospect

With more and more attention to network security today, intrusion prevention system has the advantages that ordinary firewall and intrusion detection do not have, which has attracted more and more attention. It will also become a bright spot in network security. In short, future defense system research will focus on the Internet itself, network security and communication protocols, evolve disordered data into orderly data, from human controlled

network security software to computer self-learning, and from technology-based user interface to human-based intelligent user interface.

Reference:

[1]. Zou Feng. Research on intrusion detection and defense based on computer network [J]. Coal technology, 2011, (01)
[2]. Cha Donghui. Intrusion prevention system technology [J]. Information security and communication confidentiality, 2009, (02)
[3]. Armed, Chen Jiaxin, Wang Keping. Research on an improved IPv4 / v6 network intrusion detection technology [J]. Computer science,2011,(06) .
[4]. Li Xiaozhe, Tan Zhiyong, Dai Yiqi. Secure LAN host intrusion prevention system [J]. Journal of Tsinghua University (Natural Science Department) Academic Edition), 2010, (01)
[5]. Zhao Kai. Research and design of Distributed Intrusion Detection System Based on Snort [J]. Coal technology, 2011, (09)

Pengwei Li. "Research on Network Virus Intrusion Prevention System Technology." *IOSR Journal of Research & Method in Education (IOSR-JRME)*, 11(06), (2021): pp. 33-36.