Research of Intrusion Protection System using correlation policy

Li Shuo, Zhang Quan

School of Electronic Science and Engineering, National University of Defense Technology, Changsha, 410073, China

email: duanyidetianshi019@sina.com

Keywords: Intrusion Protection System; correlation policy; honeypot

Abstract. Aimed at the limitations of single technology in network security defense, an Intrusion Protection System using correlation policy was proposed. This system consists of firewall, Intrusion Detection System and honeypot. The system extends the firewall redirection rules, sets up honeypot host monitors, and comes up with the linkage plug-in module of firewall, Intrusion Detection System and honeypot to achieve the close interaction of the three modules. On the basis of traditional Intrusion Protection System, the system based on proactive defense to defense the attack from internal and “0day attack” by honeypot.

Introduction

The information security technology such as firewall, Intrusion Detection System is an indispensable part in the maintenance of information network security. But because these techniques are highly targeted, they have limited effect when face to the network attack that beyond their strength[1]. At the same time, with the change of the network vulnerability, network attack technology is also developing constantly, malicious attackers evade the existing security system through exploiting new attack methods and tools. Therefore, static network security system is unable to satisfy the needs of network security[2]. In order to improve the defense ability of network security, we should comprehensive different security technologies, make the modules to cooperate with each other using correlation policy, assess the threat from a global perspective, take measures at the right position, prevent the occurrence of the network security threats effectively. Based on this thought, We come up with a Intrusion Protection System that makes up with firewall, Intrusion Detection System and Honeypot[3][4], carry out linkage protection aimed at traditional external attack, internal attack and “0day” attack.

Analysis of existing network security technologies

Among the existing network security technologies, firewall is widely used. As the isolation device between different segments, firewall isolates the internal network and the Internet effectively, centralized manages the network security policy formulation and information flow, is one of the most effective means to resist the invasion of the network[5].

However, with the continuous development of network technology, attack tools and techniques are becoming more sophisticated, firewall is unable to satisfy the security needs as a static defense technology: Firstly, when firewall is working, intruder may invade the internal network through the backdoor of the firewall. Secondly, firewall can only prevent the outside intruders rather than the inside intruders. On the third point, due to the limitations of the characteristics, firewall can not detect the intrusion in time and can do nothing with malicious code. Consequently, it is impractical to use a single firewall device to ensure the security of the network. Dynamic defense technology gradually comes into people’s vision.

IDS[6](Intrusion Detection System) as the representative of the dynamic defense technology can aware the intrusion behavior actively and alarm. The traditional response mode is to notify the security administrator by displaying messages and forming logs, and the the administrator take response measures manually. However, due to the traditional Intrusion Detection System is rarely able to response the intrusion behavior promptly, its security is also greatly reduced. In the experiment of the relationship between the response time and the success rate of attack, Cohen find that timely response to intrusion behavior is the key factor to resist invasion[7]. Time between the alarm from the Intrusion Detection System and the response measurement called opportunity window. The smaller the opportunity window, the shorter the attack time for the intruder, the lower the success rate of attack.

Honeypot is the resource under the monitoring of protection system, its purpose is to allow an attacker to deploy itself. By monitoring the data stream that the intrusion attack the honeypot, the administrator can aware the attack data stream that bypass peripheral protective device. For example, although the attack data stream is encrypted, honeypot can still records the attack data in the interaction process[8]. By the aid of honeypot, research on the honeypot data can comprehend the intruder effectively. While honeypot can not defense actively, can not prevent the intrusion behavior.

Aimed at three familiar intrusion behavior, analyses the insufficient of single security in the realization of defense and detection function:

External attack

Attack mode: The external malicious host scans the specific port of the internal host, detect whether there is X loophole. If X loophole is existed, the external malicious host sends virus file to internal host in order to infect the internal host. Then the external malicious host sends some of the penetration attack tools to scan and intrude other hosts in the internal network. After removing the imprint on the internal host, the intruder exits the system.

When facing external attack, the three security technology will encounter the following problems: when firewall is opening the specific port, that means the firewall think it is reasonable for the external and internal hosts communicating with each other by this port, and the firewall will admit this communication, defense and detection capabilities are not achieved. The Intrusion Detection System installed in the internal host aware the intrusion behavior and record logs, the detection capability is achieved. If the administrator check the logs after the intruder removing the logs, he can only find the scanning log instead of the whole logs. If the attack spreads to the honeypot, the honeypot record the log and upload to the log server, the detection capability is achieved.

Internal attack

Attack mode: Installed the sever of the Trojan in the internal host and make the Intrusion Detection System out of operation. The internal host carries out two threads to complete the attack. The function of Thread 1 is to communicate with the client of the Trojan in the external host, remote controlled by the attack host. The function of Thread 2 is scanning and intrusion other internal host under the control of the intruder.

When facing the internal attack, the three security technology will encounter the following problems: Due to its own characteristic, firewall can do nothing with the internal attack, defense and detection capabilities are not achieved. The Intrusion Detection System installed on other hosts in the internal network can aware the intrusion behavior and record logs, the detection capability is achieved. If the attack spreads to the honeypot, the honeypot record the log and upload to the log server, the detection capability is achieved.

“0day”attack

Attack mode: The external malicious host scans the specific port of the internal host, detect whether there is X loophole. If X loophole is existed, the external malicious host sends new-pattern virus file to internal host in order to infect the internal host. The intrusion behavior can not be found in the rules of Intrusion Detection System. Then the external malicious host sends some of the penetration attack tools to scan and intrude other hosts in the internal network. After removing the imprint on the internal host, the intruder exits the system.

When facing “0day” attack, the three security technology will encounter the following problems: when firewall is opening the specific port, that means the firewall think it is reasonable for the external and internal hosts communicating with each other by this port, and the firewall will admit this communication, defense and detection capabilities are not achieved. The Intrusion Detection System installed in the internal host aware the scanning behavior and record logs, while due to the intrusion behavior can not be found in the rules of Intrusion Detection System, the Intrusion Detection System can not aware the intrusion behavior, defense and detection capabilities are not achieved. If the attack spreads to the honeypot, the honeypot record the log and upload to the log server, collect characteristic information of the intrusion, the detection capability is achieved.

In summary, when facing external attack, internal attack and “0day” attack, separate firewall, Intrusion Detection System and honeypot can not achieve the defense and detection capabilities at the same time. Network security should be dynamic, three-dimensional and comprehensive system, single security technology can not solve all problems. By using correlation policy to integral the three security technologies, it can form a real security defense system, will be the highest security[9].

The system architecture and work flow of the Intrusion Protection System using correlation policy

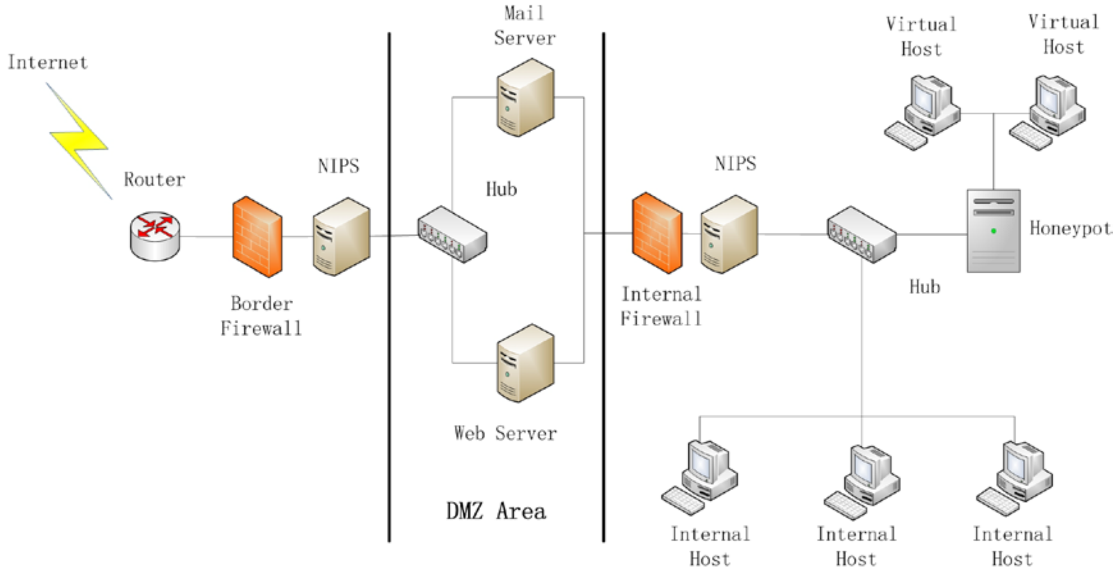

Fig.1 Architecture of the Intrusion Protection System using correlation policy

The Intrusion Protection System using correlation policy is developed under the Linux platform, system architecture is shown in Figure 1. For separating the Ethernet and the Internet, and the staff may connect to the Internet using their mobile devices, this plan set up Cisco ASA 5500 firewall to separate the Ethernet and the Internet. At the entrance of DMZ area, this plan set up a NIDS to monitor malicious flow from internal network. At the entrance of the internal network, this plan set up Netfilter/iptables firewall. In the internal network, this plan sets up several honeypots which is installed different operating systems and install Snort in every honeypots and internal hosts. For this plan aims at the protection of internal network, the correlation policy opens up around Netfilter/iptables firewall, NIDS, Snort and honeypot. The linkage plug-in communicate using C/S mode, the firewall is server and the other three module are the clients.

The response process of external data packet is shown in Figure 2. When new external data packer wants to enter the internal network passing by the DMZ area, the Netfilter/iptables firewall checks the head information of the data packet with the redirection rules firstly. The firewall affirm the packet is malicious when matching successfully, then redirects the packet to the honeypot to gather more intrusion information. The firewall checks the preinstall rules when matching failed. The firewall drops the packet if the packet does not match the preinstall rules. After that, Snort analyses the data packet in the internal host. If Snort aware intrusion behavior, it activates linkage plug-in to collect redirection message of the attack host and the target host such as IP address and port information. When finishing collection, Snort package the information into a struct and sends to firewall. When the Netfilter/iptables firewall receives the struct, it checks the redirection address table. If there has the same item, the redirection time will be lengthened. If there has not that item, the firewall adds a new redirection item to the table.

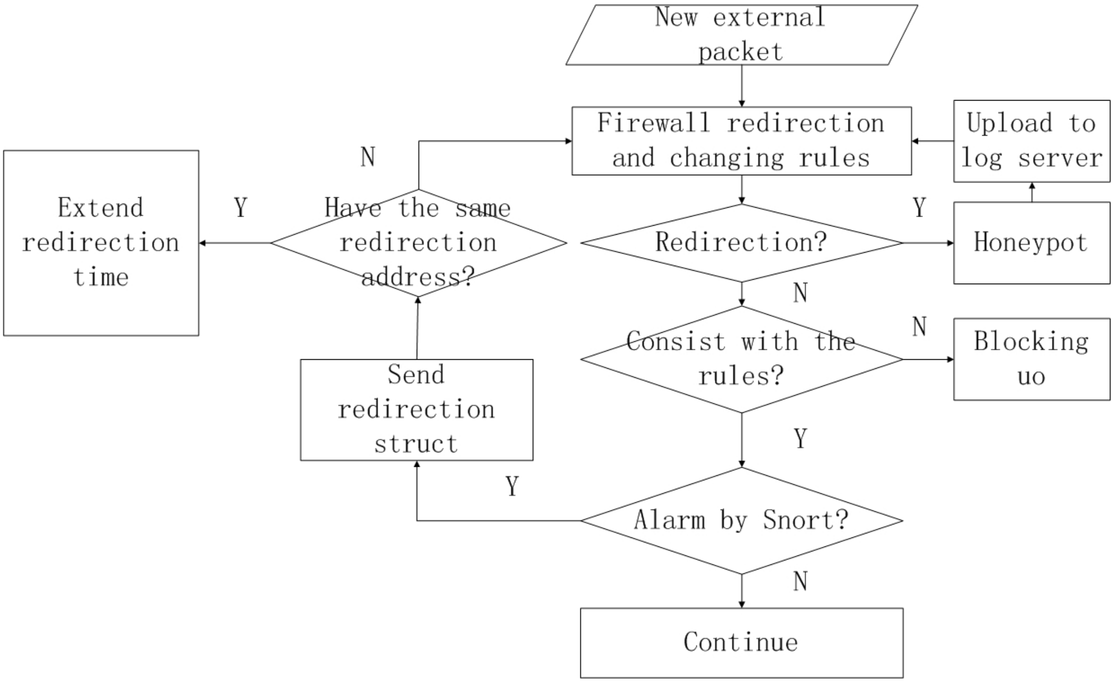

Fig.2 Response process of external data packet

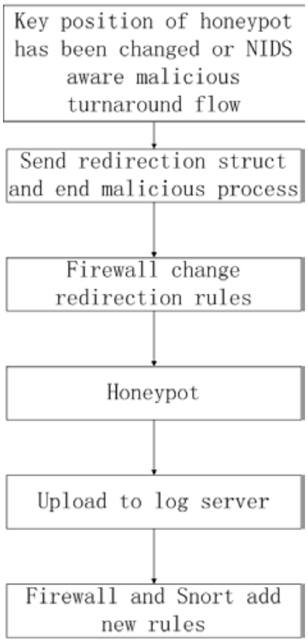
Key position of honeypot has been changed or NIDS aware malicious turnaround flow
Send redirection struct and end malicious process
Firewall change redirection rules
Honeypot
Upload to log server
Firewall and Snort add new rules

Fig.3 Response process of internal attack and “0day” attack

The response process of internal attack and “0day” attack is shown in Figure 3. When the internal network suffers from internal rebound attack such as Trojan rebound connection, The NIDS sniff the rebound flow and activate the linkage plug-in to collect redirection information, package those into a struct and send it to the firewall. After Netfilter/iptables firewall receives that struct, it add a new redirection item to the redirection table and lead the external attack host to the honeypot. When the internal network suffers from “0day” attack, the administrator aware important information of honeypot has been tampered maliciously by maintaining the log server such as registry. Then the administrator ensure the malicious process and stop that process in other internal host. The other processing mode is the same as internal attack. After the intrusion flow has been lead to the honeypot, the honeypot tries to collect more intrusion information in order to extract the characteristic of the intrusion. According to the characteristic, the firewall and Snort adds corresponding rules.

Experimental simulation

Experimental network configuration: The external network gateway is 1.1.8.1, the IP address of the attack host in the external network is 1.1.8.4. The internal network gateway (Netfilter/iptables firewall) is 192.168.1.1, the IP address of the NIDS is 192.168.1.100. The IP address of internal host B and C are 192.168.1.2 and 192.168.1.3. The gateway of honey net is 1.1.1.1, the IP address of honeypot A installed Windows operation system is 1.1.1.2, and the IP address of honeypot A installed Linux operation system is 1.1.1.3.

External attack

Attack procedure and network configuration: The external network gateway is 1.1.8.1, the IP address of the attack host A in the external network is 1.1.8.4. The internal network gateway (Netfilter/iptables firewall) is 192.168.1.1, the IP address of the NIDS is 192.168.1.100. The IP address of internal host B and C are 192.168.1.2 and 192.168.1.3. The gateway of honey net is 1.1.1.1, the IP address of honeypot A installed Windows operation system is 1.1.1.2. The attack host A in the external network start Tftp server to monitor UDP port and scan 80 port of internal host B in order to ensure the existence of IIS loophole. If there has IIS loophole, the attack host A send the virus file to internal host B through Tftp service to infect the target host. After that, the attack host A upload some of the penetration tools to internal host B in order to try to scan and attack internal host C. Finally, the intruder clear related logs in host B and exit the system.

Simulation results are as follows:

Without correlation policy, implement the above attack process, the NIDS system record scanning attack logs but there has no attack logs in the internal host B.

With correlation policy,implement the above attack process, Snort installed in the internal host B sniff the scanning attack and activate linkage plug-in, generate the redirection struct according to the intrusion characteristic and send it to the Netfilter/iptables firewall. Snort alarm and record to the log.

The attack host A send the virus file to internal host B through Tftp service and start the virus file remotely. However, due to the redirection rules, the virus file has been sent to the honeypot A. The virus file is in the honeypot A instead of internal host B. Snort installed in the honeypot A alarm and record to the log. It proves that the attack has been transfer from internal host B to the honeypot A.

The experimental result proves that the Intrusion Protection System using correlation policy can timely defense against traditional external attack and ensure the security of internal network.

Internal attack

Attack procedure and network configuration: The external network gateway is 1.1.8.1, the IP address of the attack host A in the external network is 1.1.8.4. The internal network gateway (Netfilter/iptables firewall) is 192.168.1.1, the IP address of the NIDS is 192.168.1.100. The IP address of internal host B and C are 192.168.1.2 and 192.168.1.3. The gateway of honey net is 1.1.1.1, the IP address of honeypot B installed Linux operation system is 1.1.1.2. Install Trojan server terminal in internal host C in advance and close the IDS in internal host C. The internal host C carry out two threads at the same time: The function of Thread 1 is to connect to external host A which IP address is 1.1.8.4, hand over itself to external host A. The function of Thread 2 is when the internal host C has been controlled, the internal host C scan and attack internal host B which IP address is 192.168.1.2 using penetration tools from external host A.

Simulation results are as follows:

Without correlation policy, implement the above attack process, the NIDS system record scanning attack logs but there has no attack logs in the internal host C, some of the important information has been tampered maliciously.

With correlation policy, implement the above attack process, NIDS sniff the rebound flow and activate linkage plug-in, generate the redirection struct according to the intrusion characteristic and send it to the Netfilter/iptables firewall.

When the external host A find the target host A is online, it send attack command to the internal host C. However, due to the redirection rules, this command has been sent to the honeypot B. Because there has no Trojan server terminal in the honeypot B, there has no response in the honeypot B and the rebound packet from the internal host C has been dropped by firewall.

The experimental result proves that the Intrusion Protection System using correlation policy can timely defense against internal attack and ensure the security of internal network.

“0day” attack

Attack procedure and network configuration: The attack procedure and network configuration is the same as external attack, but the virus file has been suffered from shell processing and the intrusion characteristic can not be found in the rules of Snort.

Simulation results are as follows:

Without correlation policy, implement the above attack process, the NIDS system record scanning attack logs but there has no attack logs in the internal host B.

With correlation policy,implement the above attack process, Snort installed in the internal host B sniff the scanning attack and activate linkage plug-in, generate the redirection struct according to the intrusion characteristic and send it to the Netfilter/iptables firewall.

The attack host A send the virus file to internal host B through Tftp service and start the virus file remotely. However, due to the redirection rules, the virus file has been sent to the honeypot A. The virus file is in the honeypot A instead of internal host B. Snort installed in the honeypot A does not alarm.

the administrator aware important information of honeypot has been tampered maliciously by maintaining the log server, ensure this is intrusion behavior. Then the honeypot activate linkage plug-in and send the redirection struct to the firewall. The firewall lengthen the redirection time in order to collect more intrusion information. When collecting enough characteristic, the firewall change its rules.

The experimental result proves that the Intrusion Protection System using correlation policy can timely defense against “0day” attack and ensure the security of internal network.

Conclusion

This paper analysis of common security solutions on the basis and propose the Intrusion Protection System using correlation policy. The design and implementation of the system are also given.

This scheme combine the technical of firewall, Intrusion Detection System and honeypot. Not only improving the response ability of the Intrusion Protection System to security incidents, but also enhance the confusion of hackers, improve the security of the network as a whole.

But there are still some problems in this project: Defense “0day” attack need many human factor, and this scheme can not prevent the attack by the honeypot as a springboard. These aspects need to be further studied.

References

[1] John Hoopes, Aaron Bawcom, Fred Shore. Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis and Honeypotting[M]. Beijing: Science Press,2010.12-13.

[2] Ma Chuanlong, Zhang Tao, Xiong Wei. Research on Intrusion Prevention System Based on Snort[J/OL]. 1994-2010 China Academic Journal Electronic Publishing House. http://www.cnki.net.

[3] PERKINS CE, BELDING-ROYER EM, DAS S. Ad hoc On-Demand Distance Vector(AODV) Routing[EB/OL]. http://moment.cs.ucsb.edu/pub/draft-perkins-manet-aodvbis-00.txt. Mobile Ad Hoc Networking Working Group INTERNET DRAFT, 19 October 2003.

[4] JOHNSON D. The Dynamic Source Routing Protocol for Mobile Ad Hoc

Networks(DSR)[EB/OL]. http://www.ietf.org/internetdrafts/draft-irtf-manet-dsr-09.txt, April 2003.

[5] Liu Baoxu, Jiang Wenbao, Wang Xiaozhen. Active Defense against hackers[M]. Electronics Industry Press, 2007.

[6] Tang Zhengjun, Li Jianhua. Intrusion Detection Technology[M]. Beijing:Tsinghua University Press, 2004.

[7] F.B.Cohen. Simulating Cyber Attacks, Defenses, and Consequences[EB/OL]. http://all.net/journal/ntb/simulate/simulate.html, 2004.

[8] Seungwon Shin, Jaeyeon Jung, and Hari Balakrishnan. Malware prevalence in the kazaa filesharing network[C]. Internet Measurement Conference, 2006:333-338.

[9] Liu Yong, Chang Guocen, Wang Xiaohui. Integrated Network Security Management System Based on Linkage Mechanism[J]. Computer Engineering, 2004:136-137.