Active Defense Security Model in the Application of Network Deception System Design

Jiawei Du*, Xing Zhang, Ying Zhou, Yongqiang Bai
Luoyang Electronic Equipment Test Center of China(LEETC)
Luoyang China
*e-mail:15236132569@163.com

***Abstract*—As the traditional network defense is built on intrusion detection and passive protection, which is weak at dynamic response. The network deception technology in active protection is analyzed, and a network deception system based on active security model is proposed in this paper. This system implements a visual service of Honeypot as bait, analyses intrusion data and extracts new features and rules to enlarge the intrusion detection system feature library. The defense policies could be delivered real-time by management center. The problems of false alarm and leaking alarm for firewall or IDS are improved. And the limitations of single technology on the cooperation are overcome by linkage of Honeypot, firewall, IDS and router. The efficiency of unknown intrusion detected is increased.**

Keywords- Active defense; security model; network deception; honeypot; linkage

I. INTRODUCTION

Nowadays, there is a big challenge on the security, usability and integrality of information with the rapid development of network. The vulnerability of network and the universality of attack have brought more and more network security problems. Traditional security techniques cannot meet the requirements of the dynamic and complex network environment. It has been an important problem to research how to take effective measures to ensure network security. Transforming the traditional passive protection to active defense is a hot topic[1]. The active defense techniques not only provide security service to reinforce local network, but also detect intrusion and attacks actively and then take measures to interrupt the intrusion and attacks. That makes the loss caused by attacks cut down directly. As one typical active defense technique, network deception could improve the security and survivability efficiently. At present, most of the researchers focus on the linkage between Honeypot and IDS (intrusion detection system), IDS based on Honeypot, etc. A Honeypot centered network deception system, which integrates firewall and IDS, is proposed according to active defense model in this paper. This system could deal with the intrusion actively, and deploy new security policies dynamically. That would improve the active defense ability of target system.

II. ACTIVE DEFENSE MODEL

Traditional security theory and technologies usually provide static passive defense. That makes the defense response lag behind the attack consequentially. So the active defense security technology was developed to meet the requirements of the fast developing information system and multidimensional network. Besides the traditional protection and detection technologies, the active defense technologies include intrusion detect tech, intrusion response tech, network deception tech, network emergency response tech, and etc. PDRR is one of the most representative active defense models[2], which includes protection, detection, response, recovery. Based on PDRR, some researchers proposed an active dynamic defense model: P2DR2M, which stresses policy and management, and reflects the association between different security components. The P2DR2M model could realize active cooperation among security components and implement dynamic defense.

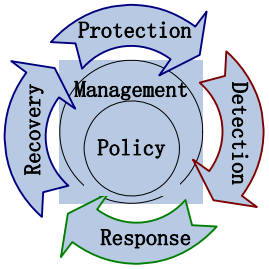

Fig.1 P2DR2M model

Illustrated as Fig.1, there are four processes and two factors in the P2DR2M model. These four processes: protection, detection, response, and recovery, build up a dynamic closed loop, which realizes dynamic feedback by interaction. The two factors are policy and management, where policy is the kernel of this model, and management is assistant approach.

Following the security policy, the P2DR2M model uses the vulnerability scanner, and IDS to inspect and assess system security status. Then several security tools (firewall, authentication, encryption, etc.) are applied to ensure the system to be secured. Protection, detection, response and recovery could be managed into an entire dynamic security cycle.

III. NETWORK DECEPTION SYSTEM BASED ON ACTIVE DEFENSE SECURITY SYSTEM

Network deception is a new active defense technology, which overcomes the disadvantages of traditional passive technologies. There are two directions of network deception

Published by Atlantis Press, Paris, France.

research: based on Honeypot and based on Honey net. Although Honeypot cannot improve the system security directly, it provides a particular service that cannot be replaced.

A. *Network deception system*

Network deception system is an important part of active defense model. It is a reaction system to attack after intrusion detected. Actually, network deception system is a controllable Honeypot, which pretends the real system to trap the attackers. The Honeypot could simulate the characters and vulnerabilities of common operation system, record all the operations and behaviors. The information of attackers could be obtained through the analysis of surveillance record [3].

Some principles should be paid attention to when designing a network deception system. Firstly, the system should work with different network environments. Secondly, the Honeypot should be segregated efficiently to avoid that the attackers may intrude the normal system through the Honeypot as a gangplank. Thirdly, it should be insured that the attack events and tracks could be captured and recorded [4].

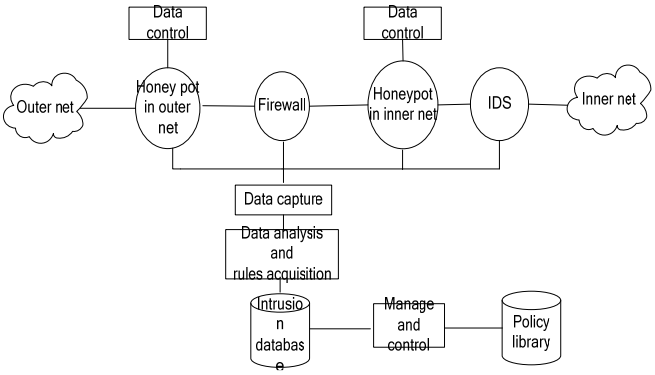

Fig.2 Network deception system logic model

As depicted in Fig.2, a network deception system is built based on P2DR2M model, which aims to increasing the cost of attack and decreasing the risk of target system. Two Honeypots are deployed separately to inner net and outer net. An IDS could detect the intrusion actions, and the firewall blocks certain connections according to the interactive security policies.

Data capture component could record the intrusion actions secretly. It is authorized to capture firewall logs, IDS logs and Honeypot logs.

Data control is one of the Honeypot's necessary functions. While the Honeypot freely opens to the data in, it strictly controls the data packets out to avoid being an attack gangplank. If the Honeypot is broken into, data control could guarantee that the attacker could not inspect a third net or execute DoS attack. The data control policy could be implemented in the firewall.

Data analysis and feature acquisition component analyze the suspicious action or intrusion deeply according to the data come from data capture component. It builds new security feature model and new policies, and then updates the intrusion library and firewall configuration library. The management component updates the security policy library real-time with the change of intrusion library, and delivers new security policies to Honeypot, firewall and IDS. This process represents the idea of active defense.

B. *System topology and interaction*

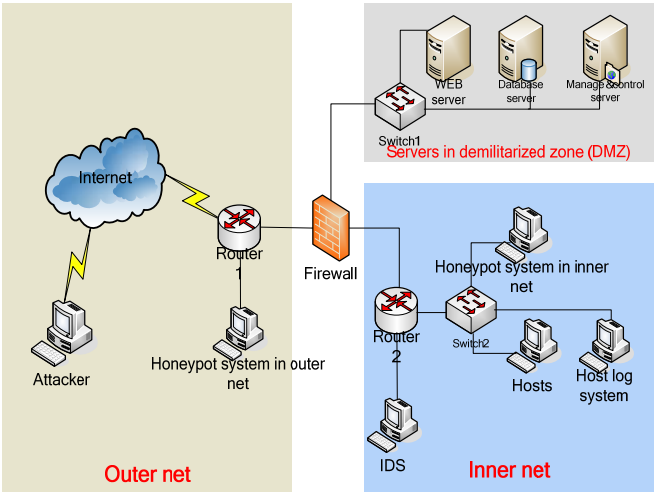

Fig.3 Topology of the network deception system

The topology of the network deception system is illustrated in Fig.3. It works as follows:

1) Apply a Honeypot at the outer net to attract the attackers' attention. Although it is too obvious to deceive the senior hackers, it could trap those juniors. That could release the burden of firewall.

2) Locate all the servers in demilitarized zone (DMZ). As the servers usually need to provide services for the outer net users, they have been an attack focus. This deployment could prevent the server to become an attack gangplank.

3) The inner net is segregated from the servers by a firewall, where is usually called local area network (LAN). The firewall could offer services through public IP, but protect local hosts by NAT rules.

4) Apply another Honeypot at the inner net hidden behind the firewall. As it is under the fog of the outer Honeypot, it would just be the actual trap of this network deception system.

5) IDS builds another defense behind firewall. It could detect some attacks and information leak that have passed firewall, such as some unknown attacks.

6) Host log system, which keeps the logs of IDS, firewall and Honeypot, works independently. As the Honeypot needs to offer information to IDS and firewall, placing the three log systems on one host could bring convenience for communication [6].

7) The inner net hosts are the kernel to be protected. It could greatly decrease the possibility of being breached that there are also IDS and host reinforcement systems located behind the firewall. [7]

Published by Atlantis Press, Paris, France.

8) Management server is deployed together with the server group in DMZ. It is in charge of monitoring and managing the whole deception process. According to the intrusion data and new acquisition rules, the management server updates the intrusion library and delivers the real-time security policies[8].

The interaction of system is analyzed as follows. All of the data packets are permitted into the outer net Honeypot. Some bunglers may be trapped here and a part of data could be captured. The firewall, which separates the inner net and outer net, could also catch some attack information. It is noted down in the host log system. The inner net Honeypot attracts the attackers covertly and logs the attack tracks for analysis. Then the firewall controls the connections dynamically according to the data control policies. IDS could detect exception, anomaly and intrusion, and give alarm in time. It would block some attackers and decrease the possibility of putting the hosts under attack. A router deployed among firewall, IDS and Honeypot could increase the fidelity of Honeypot, improve the system security through access control.

As a typical active defense technique, Honeypot is introduced into design of this system, which could capture attack data, analyze logs, extract rules, update the intrusion library, and deliver the interactive policies real time. It has more active defense ability, learning ability, and dynamic interaction than the traditional defense system 错误!未找到引用源。.

C. *Honeypot design*

As Honeypot is the kernel of the network deception system, Honeypot design is definitely a crucial step. The virtual application services, which are baits in the deception system, play an important role in Honeypot design. Take a website for example: the background could be simulated by custom web server simulation scripts. The attackers couldn't find out whether there is a real server or not, because all the operations could be done. However，those operations can neither affect the real server, nor destroy the Honeypot, while the Honeypot has recorded down the information of attacker and the operations.

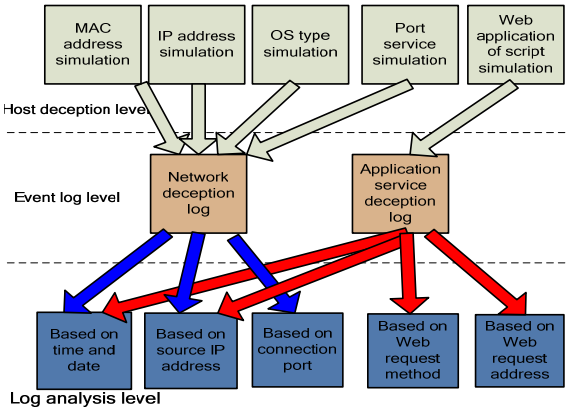

Fig.4 Honeypot system function scheme

As illustrated in Fig.4, the function scheme of Honeypot system has three levels: host deception level, event log level and log analysis level. They are realized by several virtual servers or hosts, which are implemented on net level, OS level and application level separately.

This system is driven by deception engine, which could be remote managed through graphic user interface. It could customize the virtual server type, network address and service script, etc. The host deception level can realize the simulation of MAC address, IP address, OS type, port service and web server manage pages. The logs of intrusion action and application deception are all captured and stored in event log level. The log analysis level analyzes the deception data according to attack source, event type, attack type, etc. Then it provides statistics and analysis results based on date, IP, port, web request type and web request address.

IV. CONCLUSIONS

The frame of network deception system based on active defense security model is analyzed in this paper. Through a Honeypot centered deception system, this system implements a visual service as bait, analyses intrusion data and extracts new features and rules to enlarge the intrusion detection system feature library. It could efficiently overcome the disadvantages of firewall and IDS in leaking alarm and false alarm. Through updating the policy library real time, the limitation of traditional technologies for lack of dynamic ability is breached. The ability of intrusion detection and active defense is effectively improved by linkage of Honeypot, firewall, IDS and router.

REFERENCES

[1] Zhao Hongjing, Zhou Chuangming, Zhai Pingli, Yu huan, Zhao Mingli, Inrusion Deception System based on network active defense security model, Airforce Engineering University Journal, 2010.6.

[2] Zhao Linlin, Yan Ruoyu, Li Qisheng, Network security active cooperative defense system framework based on P2DER model, Practice and experience, 2007,6.

[3] Zhai Guangqun, Chen Xiangdong, Hu Guijiang, Research and design on honeypot and IDS linked system, Computer engineering and design, 2009,30(21).

[4] Han Ruisheng, Chu Kaiyong, Zhao bing, Research and design in P2DR of policy deployment model[J], Computer Engineering, 2008(10).

[5] Wang Tiefang, Li Yunwen, Ye Baosheng, A network security defense technology based on honeynet[J], Comuputer Application Research, 2009, 26(8).

[6] Babak Khosravifar, Jamal Bentahar. An experience improving intrusion detection systems false alarm ratio by using Honeypot[C]. 22nd International Conference on Advanced Information Networking and Applications, 2008.

[7] Provos N. A Virtual Honeypot Framework [EB/OL]·[2004-12-29] (2009-10-30)· http: //www. usenix. org/event/sec04/tech/full - papers/provos/provos-htm.l.

[8] Peng Zhao, Research and Realization based on linked network intrusion defense system[Thesis], Beijing University of Posts and Telecommunications, 2010.12.

[9] http://www.cert.org.cn/.

[10] Zou Ruiyuan, Research and application survey on honeypot techonology[J], Computer security, 2010.56.