Advanced Science and Technology Letters
Vol.111 (NGCIT 2015), pp.175-178
http://dx.doi.org/10.14257/astl.2015.111.34

Network Attack Defense Awareness

[1]Man Li and [2]Jinjing Cao

[1,2]Shandong Huayu University of Technology,
Dezhou, ShanDong 253034, china
[1]xdclm@126.com, [2]Lancaoer19831230@163.com

Abstract. By defining attack-defense action sequence and utility function of both sides, combine with dynamic Bayes game theory to analyze the confrontation and interdependence between the two agents' strategies. Dynamic Bayes attack-defense game model can describe each possible strategy in every stage.

Keywords: model Network Security, Attack Model

1 Introduction

Static game can't reflect the temporal sequence of acts by the attack side and the defense side [1-2]. When the attack behavior happens, the defendant can't change its defensive strategy in the real time by only counting on what's observed. So the model is not workable if used to study the dynamic confrontational situations in the generating process of attack and defense behaviors [3-4]. The scope of its application is limited. To overcome the aforesaid shortcomings, we propose the use of multistage gaming strategy based on incomplete information to describe situations between both sides. The new model is more universal than the former one [5-6].

On that basis, we develop a dynamic gaming method of incomplete information based on attack defense model to probe into the whole countervailing course of attack and defense in network systems and the choice of strategy [7-8]. After the acting sequence of both sides and the method for quantifying strategy effectiveness are defined, the constructing algorithm of attack-defense game's extensive form is developed; and also the generation method of perfect Bayesian equilibrium is discussed. In the end, by citing examples, it introduces the new method and proves its correctness. The defendant can get the best active defending strategy set and the best passive defending strategy set in each phase while considering fully its own strategy and the attacker's [9-10] . The proposed method shows completely the situation and tendency of strategy confrontation at each of both the attack and defense stages [11].

2 Dynamic attack and defense game model based on incomplete information

ISSN: 2287-1233 ASTL

In real life, network attack and defense is usually a multistage process of strategy confrontation. At each stage, i.e. in every possible security situation, either the attack side or the defensive side would forecast any possible acts taken by the other side in the next phase, by according to network information they collect and observed historical conducts of the counterparty, as for them to decide the best strategy in the next period.

The following example illustrates multi-stage dependence phenomenon of attack defense strategy.

Some attackers decided to attack the internal LAN hosts to obtain the Root permissions, the attacker can use the buffer overflow attack and weak password attack in two ways. Assumptions regarding the host vulnerability of buffer overflow attack has an existing mode of attack, the attack cost is much lower than the latter, in the previous analysis of the attacker will use the former, but if the installation of intrusion detection system to detect the entrance of the LAN attacker, then the attacker will choose weak passwords to obtain permission to attack the host, because the IDS is able to detect this kind of attack, and shielding the attacker's IP, at this time the attacker spent a certain attack cost, but income is 0, and the IP is shielded "punishment" back to the attacker to bring negative effect.

If used weak password attack, although attack cost is higher, but the other attacker can achieve its purpose and positive returns, the attacker will take a weak password attack in the strategy of balance, the attacker can access to the host on the Root permissions and implant malicious code, if the attack defense confrontation process has not ended, the defender also has two kinds of strategies to resist an attack:

(1)Scanning system, clear the virus program and delete the doubtful account;

(2)Re-install the system, and change the system all the account password. When the defensive side to take the first way, defense cost is low but the internal system still remained partial backdoor programs cannot be deleted, the attacker can continue to use this backdoor attack, or use other account again obtain permission, defending party finally still will suffer heavy losses. If adopt second ways although defense cost is high, but can completely remove the attacker's threat, this time the attacker will pay no income attack cost. Based on the above consideration, the confrontation process description of the case is shown in figure 1.

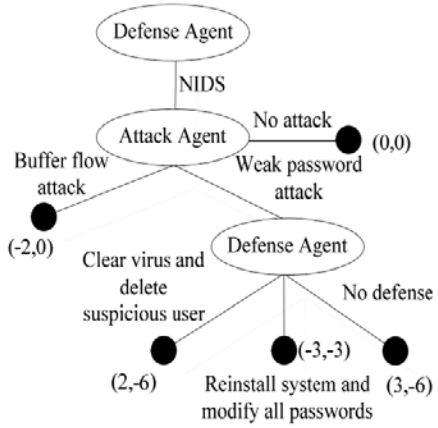

Fig. 1. Instruction of attack and defense strategies

4 Experiment Design and Discussion

To describe and validate the analysis method used in the attack-defense model, we create the attack-defense scenario as seen in the following:

The network topology in the experiment is shown in Fig. 2. The attacker Eve is located in the external network. Protective devices like firewall and IDS exist between the exterior and local network. The firewall allows the external hosts to access only the host in DMZ area, rather than direct visit to the internal local network. In the isolation area DMZ, there are two hosts responsible for providing services to outer net users. IP2 is an IIS Web server, with IIS ASP remote buffer overflow vulnerabilities (BID: 18858). IP3 is an SSH server running RedHat Linux, providing FTP services. Its OpenSSH buffer zone manages and manipulates remote overflow vulnerabilities including AS3 (BID: 8628). IP2 has trust relation to IP3. The inner net includes one PC and one DB server. DB server is Oracle database type, with Windows operating system. There is Oracle TNS Listener remote buffer overflow leak (BID: 4845). PC installs Windows operating system, with RPC overflow and deformed SMB packet remote data destroy loopholes (BID: 8152). WWW service in Web server allows data reading and writing to DB server, which has trust relationship with SSH server.

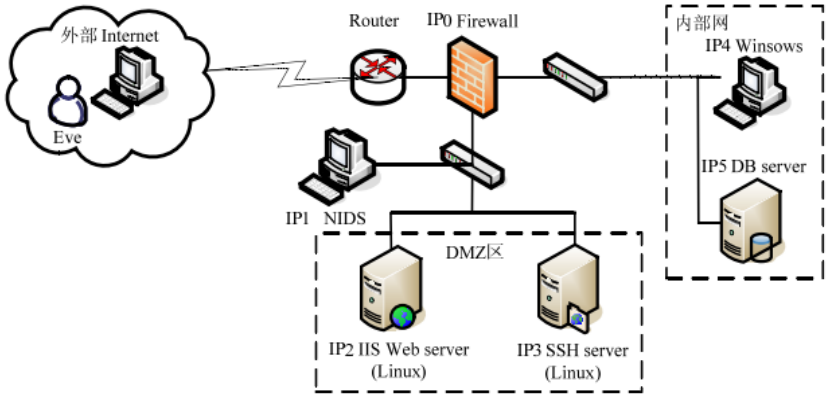

Fig. 2. Diagram of the experimental network topology

Assume the attacker Eve attempts to acquire from DB server in the internal net the classified information or Root authority. Based on the above information, we can build a network attack-defense model, which depicts attacking relationship of the attacker to various vulnerabilities in the network device and every accessible path to the attack targets.

5 Conclusion

In view of the lack of modeling and analysis in active defense technology. This paper presents Network Attack Defense Awareness based on dynamic game of incomplete information. This method can describe the attack may occur in network system.

References

1. Chen Hongfei. Research on cloud security attack and defense strategies and security technology evaluation based on game theory. Yunnan University of Finance and Economics, 2014
2. Wang Zhiwei, Jo Han, Li Ziran, Zhao Yingxue. Secret strategy research of incomplete information dynamic game model based on science and technology. System engineering theory and practice, 2013,12:3182-3189.
3. Zhu Jianming, Song Biao, Huang Qifa. Evolution game model of network security attack and defense based on system dynamics. Journal of China Institute of communications, 2014,01:54-61.
4. Chen Xia, Zhao Mingming, Xu Guangyan. Fuzzy dynamic game of UAV air combat based on Multi Strategy. EO and control, 2014,06:19-23.
5. Wu Wen, Meng Xiangru, Ma Zhiqiang, Liang Xiao. Three side dynamic game network can choose the survivability strategy. Journal of Applied Science, 2014,04:365-371.
6. Wang Xiaodan, Huang Yanyan, Wang Jianyu. Analysis of computer network defense strategy. The command information systems and technology, 2014,05:13-19.
7. Wang Wentao, Xie Yangqun, Li Yang. Research on organizational error information dynamic game model of incomplete information transfer mechanism. Based on information theory and practice, 2014,11:76-80.
8. Shen Shigen. Research on some key problems security in wireless sensor networks based on game theory. Donghua University, 2013
9. Han Wenying, Yan Chai Yanmei, star, Wang Xiuli. Study on the strategies of enterprise information security based on game theory. Computer Engineering, 2013,09:162-166.
10. Dong Xingzhi, Wang Lian. Incomplete information dynamic game analysis on competition in the banking industry. Hunan social science, 2012,04:137-140.
11. Yu Liying, Jiang Zongcai. Research on Crisis Management Based on dynamic game of incomplete information. Shanghai management science, 2012,05:87-90.

