Advanced Science and Technology Letters
Vol.53 (AITS 2014), pp.484- 487
http://dx.doi.org/10.14257/astl.2014.53.98

Study on The network attack model

Yongfu Zhou

Heyuan Polytechnic,
HeYuan 517000, china,
afuyours@126.com

Abstract. In the paper, a global network attack model based on Hierarchical Expanded Stochastic Petri Net (HESPN) is presented. The model is suitable for the cooperative attack simulation and can describe both macroscopic network attack and microcosmic host attack synthetically. The dissertation represents model generation algorithm and digs for potential attack relationships among hosts according to the definition of rough path. Then utilize ant colony algorithm to find k-critical vulnerable paths after expanding sub Petri net. By analyzing rough paths and accurate paths synthetically, a network risk evaluation method is proposed.

Keywords: Network Security, Attack Model, Threat Evaluation, Attack and Defense Strategy, Object Petri net

1 Introduction

Aiming at the existing problems in the network attack model, this paper puts forward the whole network attack model of a Hierarchical Expanded Stochastic Petri Net (HESPN). It is more suitable for modeling large complex network [1-2]. Compared with the attack graph model, the model has the following advantages:

(1) To have more strong attack process and network state description ability. Coordinated attacks on distributed system can be modeled, articulate weaknesses use complex logic and timing relationships of host attack

(2)Extended the definition of random Transitions in SPN, so that the model can reflect the attack cost and attack benefit comprehensive influence on the attacker decision.

(3) From the fundamental solution is to the problem of exponential growth in the attack graph state. In the guarantee to host leak state comprehensive description of the situation, the design of the network object and hierarchical structure can effectively control the state of the network scale

4) Generation model is more convenient. Generation of network attack path need not search the network state, only need to the attack rule base in the known state domain to add attack Transitions.

(5) The model generation algorithm in simulation of multi target attack time and space complexity is superior to the degree, it can generate an integrated Petri net

ISSN: 2287-1233 ASTL

model for multiple target attack, save the target to attack rules library search time matching.

In this paper proposed the whole network attack modeling method to aim to help the defenders grasp each kind of aggressive behavior, according to some key attack path and weak nodes forward defense measures [3-4]

2 The definition of network attack model

Hierarchical expansion will describe the complex network attack system Petri net, which can effectively reduce the number of nodes in each layer of the network, at the same time the object creation the sub-graph reuse possible [5]. The network attack model is abstracted into two aspects, macro attack and micro attack: from the macro perspective to study on the relationship of the various nodes attack domain network, mining path by using network vulnerabilities; from the microscopic point of view of a node on the leak and risk evolution. The network attack and host attacks are by combining research, which can effectively grasp of what nodes in the whole network is the network leak and the leak in which the key setting and service is worthy of attention, so as to lay the foundation for network defense. The hierarchical structure of Petri net can be a good solution to the problem of macro attack and micro attack. In this paper, the modeling approach is taken from top to bottom, the top Petri net description is on attack relationship of nodes in the network domain, while ignoring the nodes on the details of the attack, the leak of use and risk communication focus on the remote network attacks. In the lower Petri net, the hosts on the local attacks were modeled respectively, with detailed description of host attack state evolution. The macro and micro subnet network are integrated to achieve full network attack description of complex network system.

3 Construction method of the whole network attack model and path mining

The initial state set (ISS) corresponds to the node of Initial, it is an internal only contains special object interface library, it is composed of all network host services and leak information. Host, Webserver, FTPserver, DBserver and SMTPserver are node types in the network. Various classes contain multiple instances, each instance is as the object in the network, 6 kinds of state is the interface library in the VS. Various nodes of known connections and trust relationship transform into Transitions in the network, by Initial objects and NARS reasoning are to get attacked relationship of network nodes.

Each object can be extended subnets, describe the relationship of host interface States, such as the HostA node is as shown, the remaining nodes can also be extended.

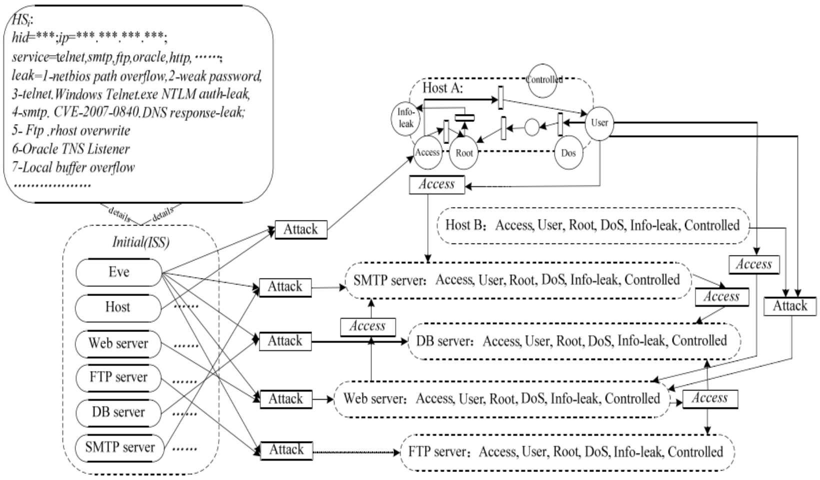
HS_i:
hid=***;ip=***.***.***.***;
service=telnet,smtp,ftp,oracle,http, ……;
leak=1-netbios path overflow,2-weak password,
3-telnet.Windows Telnet.exe NTLM auth-leak,
4-smtp. CVE-2007-0840.DNS response-leak;
5- Ftp .rhost overwrite
6-Oracle TNS Listener
7-Local buffer overflow
……………
details
details
Initial(ISS)
Eve
Host
Web server
FTP server
DB server
SMTP server
Attack
Attack
Attack
Attack
Attack
Host A:
Controlled
Info-leak
User
Access
Root
Dos
Access
Host B: Access, User, Root, DoS, Info-leak, Controlled
SMTP server: Access, User, Root, DoS, Info-leak, Controlled
Access
Access
Attack
Access
DB server: Access, User, Root, DoS, Info-leak, Controlled
Web server: Access, User, Root, DoS, Info-leak, Controlled
Access
FTP server: Access, User, Root, DoS, Info-leak, Controlled

Fig. 1. diagram of the whole network attack Petri net

4 Experiment Design and Discussion

In order to illustrate the method of establishment and analysis of the whole network attack model, the network environment structure is as shown in figure2

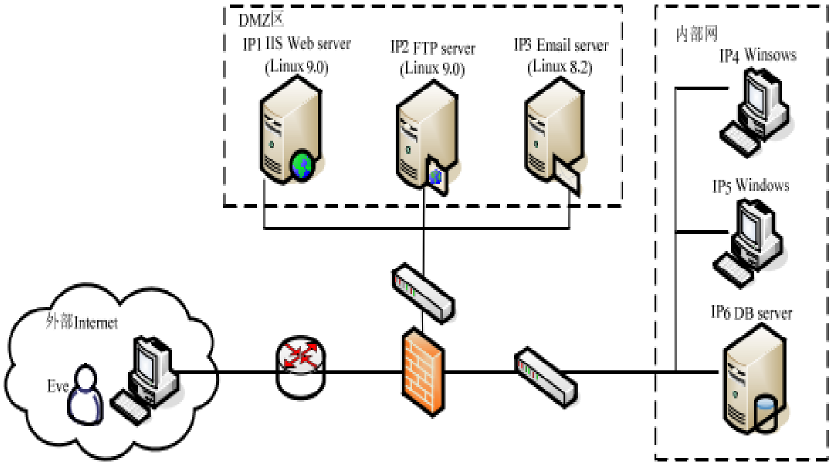
DMZ区
IP1 IIS Web server (Linux 9.0)
IP2 FTP server (Linux 9.0)
IP3 Email server (Linux 8.2)
内部网
IP4 Winsows
IP5 Windows
IP6 DB server
外部Internet
Eve

Fig. 2. topology network

The environment consists of three components: an Internet DMZ network, the isolation zone and the internal Lan. DMZ zone has three servers, network IP6 stored enterprises important data, IP5 is as the control machine, network administrator is responsible for the DMZ and intranet server resource allocation through it. The firewall is running the Linux operating system workstation, it controls access network between extranet and intranet, the host can access the DMZ zone of the server, you cannot access the internal LAN, between DMZ zone in the host can access each other, internal Lan only IP4 can be DMZ region of Web server and FTP server access, IP5 and IP6 are not visible. Hackers in the network is to launch an attack on the server and the host node DMZ and intranet.

4 Conclusion

This paper uses HESPN to achieve modeling for the whole network attack behavior, and puts forward the method of generating the model. Rough attack path mining in the top Petri is to search and attack the target host node and attack relationship, we extend object node to establish to the whole HESPN attack model. On the basis of the ant colony algorithm to further tap the k key vulnerable path, these path of attack effectiveness are the highest, it was most likely taken by an attacker. By comprehensive consideration the rough path and precise path, presented assessment methods of each node of the risks and vulnerabilities, provide an important basis for decision of network defense.

References

1. Huang Guangqiu, Zhang Bin, Wang Chunzi. The network attack model based on extended
2. SPN. Computer Engineering, 2011,22:12-18.
3. Wang Chunzi, Zhang Bin, Huang Guangqiu. The attack strategy mining and risk assessment model based on attack the whole network. Computer engineering and applications, 2012,04:14-18.
4. Huang Guangqiu, Wang Jincheng. The fuzzy Petri net attack model of double branch fuzzy sets based consistency. Computer applications, 2009,02: 529-534.
5. Wang Yuanzhuo, Lin Chuang, Cheng Xueqi, Fang Binxing. Network attack defense game model based on stochastic analysis method. Chinese Journal of computers, 2010,09:1748-1762.
6. Huangdan. Encryption based on attribute based trust management combination scheme in wireless sensor networks. Journal of computer applications, 2014,04:1047-1050.