云南大学学报（自然科学版），2012，34（3）：271～275　　CN 53－1045/N　ISSN 0258－7971
Journal of Yunnan University　　http://www.yndxxb.ynu.edu.cn

攻击图算法在入侵防御系统中的应用*[1]

罗智勇，孙广路，刘嘉辉，王卫兵
（哈尔滨理工大学 计算机科学与技术学院，黑龙江 哈尔滨　150080）

摘要：针对目前及时发现网络漏洞，增强网络安全十分困难等问题，提出了基于攻击图的入侵防御方法. 该方法通过生成全局网络攻击图算法来建立网络初始攻击图，并调用攻击图优化算法来去除全局攻击图中不合理路径，达到简化攻击图目的. 最后，通过计算攻击图各状态节点损失度算法来为管理人员提供优化网络安全策略的依据. 实验证明，这种入侵防御方法合理有效，并具有简单易行等优点.

关键词：网络安全；入侵防御；攻击图；漏洞；状态节点
中图分类号：TP 393.08　　**文献标识码**：A　　**文章编号**：0258－7971(2012)03－0271－05

伴随网络攻防技术的进一步发展，网络入侵手段日趋复杂，其表现形式也呈现出多样化等特点，给网管人员带来巨大困难[1-5]. 然而，一个漏洞少的网络操作系统可以大大提高网络的安全性[6]. 为此，能否尽早找到引起网络状态改变的攻击序列成为入侵防御系统关键. 基于图论的攻击模型可以更快地为网管人员发现攻击序列，以便尽早解决网络的漏洞问题[7].

本文提出了一种基于攻击图的入侵防御系统模型. 首先对网络整体生成攻击图并对其进行优化，其次调用计算状态节点损失度算法计算攻击图中各节点的损失度，形成节点关键度，最后根据关键度大小来优化网络策略解决网络漏洞问题. 通过实验，验证了这种入侵防御系统模型的有效性及正确性.

1　攻击图检测模型

1.1　相关定义　网管人员利用全局攻击图并结合各种攻击动作之间发生的因果关系，从而挖掘出网络渗透攻击序列，进而把握攻击策略，达到发现网络漏洞，实现增强网络安全的目的[8]. 本文将入侵者入侵动作的变迁设定为网络不同状态的变迁，因此得出相关定义如下.

定义 1　入侵复杂度. 是指入侵者利用某漏洞成功达到入侵主机难易程度的数值度量，本文用 Cd 表示.

定义 2　漏洞. 是网络潜在的弱点，表示为 B(Bid，Cd，deg). 其中，Bid 是漏洞 B 在漏洞库中的 ID 号；deg 为利用该漏洞成功入侵后给主机在保密性、完整性和可用性方面带来的危害程度. 有关 Bid，Cd 和 deg 之间的量化关系请参阅文献[9].

定义 3　节点损失度. 指入侵者成功入侵网络某节点 $N_i(i\neq 0)$ 后，对该节点设备安全方面所造成的损失程度，本文记为 LD(N_i).

定义 4　节点关键度. 指入侵者成功入侵网络某节点 $N_i(i\neq 0)$ 后，对网络整体安全方面所造成的损失程度，本文记为 KD(N_i).

定义 5　主机. 一种网络设备用 H 表示，其构成为(Name，SR，IDeg). 其中，Name 为主机名；SR 为安全需求程度；IDeg 为重要程度.

定义 6　状态节点. 状态节点表示为 N(Nid，H，BS，SS，SN，LD，KD，P，NetD)，在攻击图中用椭圆表示. 其中，Nid 为状态节点 ID 号；H 为该节点所对应的主机或网络设备；BS 为该主机或网络设备所存在的漏洞集合；SS 为该状态下主机或网络设备所受到安全威胁的网络服务集合；SN 为该状

* 收稿日期：2011－09－26
基金项目：国家自然科学基金资助项目(60903083)；黑龙江省教育厅海外学人科研资助项目(1251HO18).
作者简介：罗智勇(1978－)，男，山东人，讲师，博士生，主要从事网络安全、网络数据库方面的研究. E－mail：luozhiyongemail@163.com.

态节点的儿子节点集合;LD 和 KD 分别为该节点的损失度和关键度;P 为网络状态变迁到该状态节点的概率;NetD 为该网络状态下给主机在保密性、完整性和可用性方面带来的危害程度.

定义 7 攻击图. 是一有向图,也是状态转换系统,表示为 $G=(NS,CS,T,N_0,NS_g)$. 其中,NS 为网络状态节点集合;CS 为网络入侵条件集合,每个条件在攻击图中用纯文字表示;T 为状态转换关系集合;$N_0 \in NS$ 为初始状态节点;$NS_g \subseteq NS$ 为网络入侵最终目标状态节点集合. G 满足约束:$t_i(N_0, Ns \cup Cs) \rightarrow N_g$. 其中,$t_i \in T(i=1,2,\cdots)$ 是某一具体转换关系;$Ns \subseteq NS$ 是网络状态节点集合的某一子集;$Cs \subseteq CS$ 是网络入侵条件集合的某一子集;$N_g \in NS_g$ 是网络入侵某一最终目标状态.

定义 8 攻击路径. 对于网络入侵最终目标状态节点 $N_g \in NS_g$,若在攻击图中存在一组条件和状态节点构成序列 $L(C_1,C_2,N_0,N_1,\cdots,C_i,N_j,\cdots,C_{n-1},N_{m-1})(0<i<n-1,0<j<m-1)$,使得 $t_z(N_0,L) \rightarrow N_g$. 其中,$t_z \in T(z=1,2,\cdots)$ 是某一具体转换关系,则 N_0L 是一条攻击路径,本文记为 R.

由定义 7 和定义 8 可以得出 $KD(H_i)=\sum_{N_j \in NS_i} LD(N_j)$,其中 H_i 为网络中某一主机且 $i \neq 0$,NS_i 为 H_i 在状态图中影响的状态节点集合,$N_j \in NS_i$ 为任意一状态节点.

1.2 攻击图生成算法 由于攻击图是模拟入侵者入侵整个网络多种方法的抽象,因此全局攻击图生成的好坏对网管人员管理好网络安全起着非常重要的作用[10]. 结合本文提出的相关定义,给出生成全局攻击图步骤如下:

(1) 搜集网络信息,将网络拓扑结构、主机漏洞、入侵条件等信息形式化;

(2) 将形式化后的网络安全信息分类,分别加入相应的队列,构建网络状态节点初始队列;

(3) 根据网络漏洞信息并利用漏洞的渗透规则,构造攻击队列;

(4) 根据网络节点状态队列并搜索攻击队列元素,形成新的网络状态节点和新的条件节点,重新加入网络状态节点队列;

(5)重复步骤(4)直到成功入侵网络,将网络状态节点形成最终状态;

(6)形成全局攻击图.

根据上述步骤,本文给出攻击图生成算法如下:

输入:参数 NS, CS, N_0, MaxStep, P;//MaxStep 为最大入侵步数,P 成功入侵概率

输出:攻击图 G;

算法:

State_queue = NULL, N0. step = 0, NS = NULL, G = NULL, $k=1$;

ADD($NS, N_{1\sim n}$);//将网络全部状态节点加入集合 NS 中

Insert(State_queue, N_0);//将网络初始状态 N_0 加入状态队列中

while(state_queue < > NULL){ S_i = Delete(State_queue);//出队

CS_i = Detect(S_i);//检测状态节点 S_i 生成的入侵条件

if((S_i. step - MaxStep) = =0) break; else{ for each N_j in NS}

$g_j = N_j$;//将状态节点在攻击图 G 中编号

//g_j 节点入侵条件在 CS 中,入侵后形成的新条件不在 CS 中

if((Person(g_j) in CS_i)&&(Result(g_j) not in CS_i)){ S_k = NEW();//生成新的状态节点 S_k

if((i = =0) OR(CS_i in N_j. precondition))//是否为初始状态节点或新生入侵条件已存在

{if(Probability (N_0, S_k) > P) //从初始状态至状态 S_k 入侵成功概率大于 P

{if((Exists(S_q, State_queue)) and(S_q like S_k) and((S_i, S_q) in G)) //判断新状态节点是否在攻击图中已存在

{S_q. P = max(S_q. P, S_k. P);//更新入侵成功概率

e_j = Mark (S_i, CS_i, S_q); Insert(e_j, G); Delete S_k;}//更新攻击图并删除 S_k 节点

else{e_j = Mark ((S_i, CS_i, S_k); Insert(e_j, G);//标注有向边并加入攻击图中

$k++$; S_k. step = S_k. step + 1;//更新状态节点 S_k 入侵步数

Insert(State_queue, S_k);//将新状态节点 S_k 加入到状态队列

}}}else Delete S_k;}}}}

1.3 攻击图优化算法 通过大量实验发现,按照 1.2 节中攻击图生成算法在特殊情况下所生成的攻击图会出现某些攻击路径在实际入侵过程中不

可能发生. 例如在图 1(a)中,攻击图中的攻击路径 $R(N_0,C_1,N_1,C_3,N_3,C_6,N_1,C_3,N_3,C_7,N_5)$,在实际的入侵过程中不可能发生. 因为,状态节点 N_1 若想发生,必须入侵条件 C_1、C_2、C_6 必须满足,而条件 C_6 的发生是在成功入侵状态节点 N_1 后,所以产生悖论. 从该例得出全局攻击图必须优化,本文给出优化攻击图算法,图 1(b)是算法优化(a)后的攻击图.

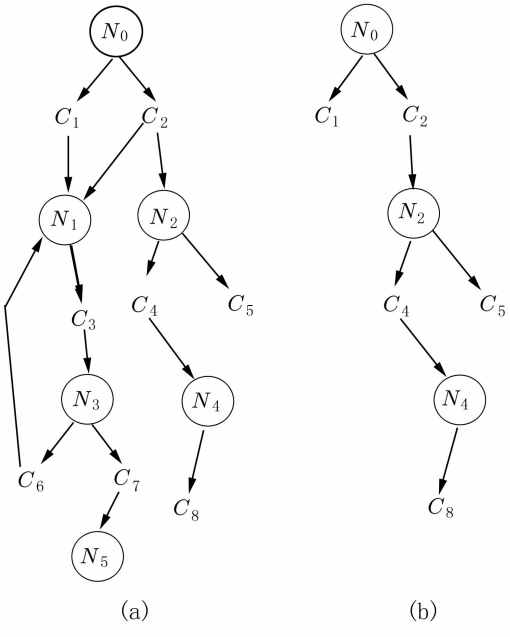

图 1　攻击图优化前后实例

Fig. 1 Attack graphs before and after optimization example

输入:优化前攻击图 G

输出:优化后攻击图 G'

算法:

for each N_i in NS {

Sumi = Count(Pre(N_i));// N_i 父节点数

flag(N_i) = false;}

for each C_i in CS Insert (Condition _ queue, C_i);//将 C_i 插入队列 q

for each q in Condition_queue

for each N_j in Post(q) { //条件 q 的渗透状态节点

num[N_j] = num[N_j] + 1;

if num[N_j] = Sumj flag(N_j) = true;}

for each C_k in Post(N_j) {

Insert (Condition_queue, C_k);} //加入条件队列

for each N_i in NS if (flag(N_i) = = false) Delete (G,N_i);//优化攻击图

return G;

1.4　计算状态节点损失度算法　当攻击图优化完毕后,还要对攻击图中各状态节点计算其损失度,进而得出各状态节点的关键度. 网管人员根据各状态节点的损失度和关键度来优化安全配置,从而达到增强网络安全的目的.

计算状态节点损失度算法如下所示:

输入:状态节点结合 NS 相关信息

输出:状态集合各节点损失度 LD(NS)

算法:

N_0. P = 1, i = 1;//初始化状态节点 N_0

while(NS < > NULL) {

N_i = Delete(NS, i);//取出 NS 集合中一个状态节点

N_j = Pre(N_i);//状态节点 N_j 为 N_i 的直接父亲节点

N_i. NetD = 0, N_i. P = 0;// N_j 初始化 N_i

N_i. P = N_i. B. Cd × N_j. P;//计算 N_i 入侵成功概率

N_i. NetD = N_i. P × N_i. B. deg;//计算 N_i 危害程度

N_i. LD = N_i. H. IDeg × N_i. NetD × N_i. H. SR;//计算 N_i 的损失度

i = i + 1;}

return NS;

2　网络安全策略优化方法

由于攻击图是用来模拟入侵者入侵网络的各种方法,因此网管人员可用其判断网络的漏洞,对其进行修补从而达到增强网络安全的目的. 本文给出这个过程的一般方法如下:

(1) 调用算法生成网络的全局攻击图;

(2) 调用算法对攻击图进行优化;

(3) 调用算法计算各状态节点安全损失度;

(4) 将攻击图中可以删除或修补的安全状态节点放入队列 Q;

(5) 计算队列 Q 中元素关键度;

(6) 队列 Q 中关键度最大状态节点出队并对其漏洞进行修补;

(7)重复执行(1)至(6)直到队列 Q 为空.

3 实 验

本文以某企业网络为实验对象,验证运用上述方法管理其网络安全的有效性和正确性. 网络环境为:使用5 台主机组建企业网,其中主机 IP_1 为 FTP 服务器,IP_2 为 MySQL 数据库服务器,IP_3 为 Telnet 服务器,IP_4 为 HTTP 服务器,IP_5 为 Oracle 数据库服务器;企业防火墙只允许外网访问 Telnet 服务器,而内网的访问不做任何限制. 企业网环境中主机信息和漏洞信息分别如表 1 和表 2 所示,其网络拓扑结构如图 2 所示.

表 1 主机信息

Tab. 1 Host information

Name	SR	IDeg	Server	Bid	Inv_cond_ID
IP_1	6	2	FTP	9904,13454	C_2,C_3
IP_2	3	3	MySQL(FTP)	7974	C_4
IP_3	4	2	Telnet	12815	C_1
IP_4	5	1	HTTP	9691	C_6
IP_5	2	3	Oracle	14312	C_5

表 2 漏洞信息

Tab. 2 Loophole information

Bid	Cd	deg	Type
9 904	0.5	2	特权提升类
13 454	0.7	1.5	特权提升类
7 974	0.7	2	特权提升类
12 815	0.7	3	特权提升类
9 691	0.3	3	特权提升类
14 312	0.9	1	拒绝服务类

由于在表 1 和表 2 所示的网络信息中,Telnet 漏洞目前还没有有效的修复办法,再加之主机 IP_3 是 Telnet 服务器防火墙不能关闭供外网访问,所以主机 IP_3 是攻击图中初始漏洞,入侵者可通过该服务器进入内网,再进行权限提升最终达到入侵 Oracle 数据库服务器的目的.

根据以上分析,利用攻击图生成算法和优化算法得出该企业网全局攻击图如图 3(a)所示.

调用计算状态节点损失度算法来计算图 3(a)中状态 N_1 至 N_8 的损失度:LD(N_1) = 16.8;LD(N_2) = 8.82;LD(N_3) = 8.82;LD(N_4) = 3.087;LD(N_5) = 6.174;LD(N_6) = 2.205;LD(N_7) = 0.771 8;LD(N_8) = 1.852.

根据图 3(a)中各状态节点损失度可以得出网络中各主机关键度如表 3 所示.

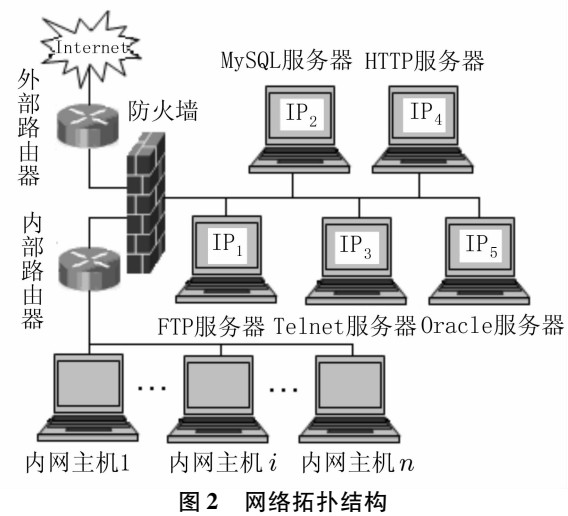

图 2 网络拓扑结构

Fig. 2 Network topology

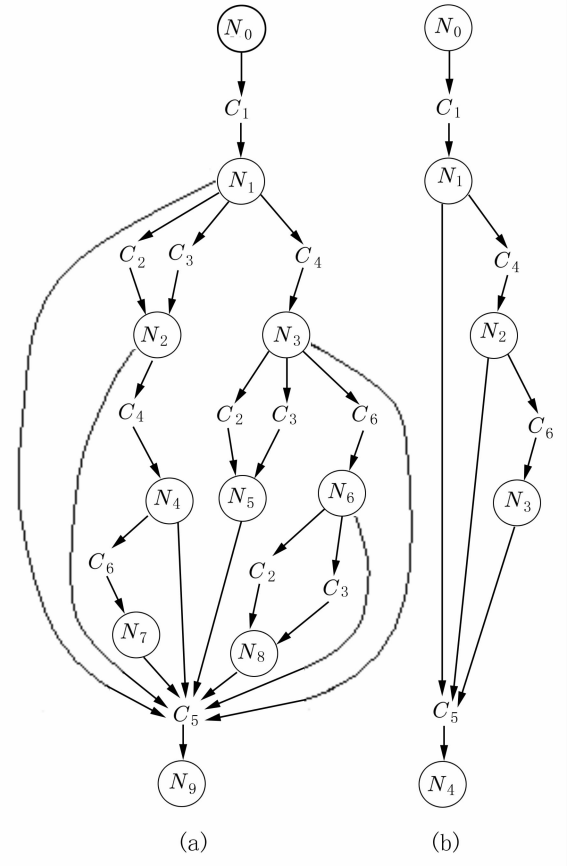

图 3 企业网攻击图构

Fig. 3 Enterprise network attack graphs

在表 3 中,发现主机 IP_1 的关键度最大,因此应该优先修复主机 IP_1 的漏洞,即:给漏洞编号为 9904 和 13454 打补丁. 当主机 IP_1 漏洞修补完毕后,应重新调用攻击图生成算法和优化算法,重新生成企业网攻击图如图 3(b)所示.

重新调用计算状态节点损失度算法来计算图 3(b)状态节点的损失度并重复上述步骤,得出各主机关键度为:$KD(IP_2)=8.82$;$KD(IP_3)=16.8$;$KD(IP_4)=2.205$. 可以发现主机 IP_3 的关键度最大,但由于其所存在的 Telnet 漏洞无法修复故不能修复主机 IP_3 漏洞,所以取 $KD(IP_2)$和 $KD(IP_4)$最大值进行漏洞修复,修复主机 IP_2 漏洞,即:给漏洞编号为 12815 打补丁. 修复主机 IP_2 后重新执行上述步骤发现攻击图中只存在一个可以修复的漏洞即主机 IP_4. 修复主机 IP_4 漏洞,即给漏洞编号为 9691 打补丁. 主机 IP_4 修复完毕后,发现只要禁止主机 IP_3 直接访问主机 IP_5 即可达到确保整个网络安全的目的.

经过以上分析,得出整个网络安全策略制定步骤为:先修复主机 IP_1 漏洞,再修复主机 IP2 漏洞,再修复主机 IP_4 漏洞,最后禁止主机 IP_3 直接访问主机 IP_5.

4　结束语

提高网络的安全性是网管人员的一大难题. 为有效、正确地解决此问题,本文提出基于攻击图的入侵防御方法. 该方法首先建立网络的全局攻击图,再对其进行优化,最后利用计算状态节点损失度算法来计算各网络设备的关键度. 网管人员根据网络设备的关键度来调整网络安全策略,修补相应的漏洞,从而使管理的网络变得更加安全.

表 3　主机关键度

Tab. 3 Host key degrees

Name	Bid	State_Nodes	LD(State_Nodes)	KD
IP_1	9904,13454	$\{N_2,N_5,N_8\}$	{8.82,6.174,1.852}	16.846
IP_2	7974	$\{N_3,N_4\}$	{8.82,3.087}	11.907
IP_3	12815	$\{N_1\}$	{16.8}	16.8
IP_4	9691	$\{N_6,N_7\}$	{2.205,0.7718}	2.977

参考文献:

[1] SINGHAL A,OU X M. Security risk analysis of computer networks:Techniques and challenge[C]// Proceedings of the 16th ACM Computer and Communications Security(CCS). Chicago,USA,2009.

[2] SAWILLA R,OU X M. Identifying critical attack as set s in dependency attack graphs[C]//Proceedings of the 13th European Symposium on Research in Computer Security(ESORICS). Malaga,Spain,2008:18-34.

[3] WANG L Y,TANIA I. An attack graph – based probabilistic security metric[C]// Proceedings of the 22nd Annual IFIP WG11,3 Working Conference on Data and Applications Security(DBS ec). London,UK,2008:283-296.

[4] SHEYNER O, HAINES J, JHA S. Automated generation and analysis of attack graphs[C]//Proc 2002 IEEE Symposium on Security and Privacy, Oakland, California,USA,2002:254-265.

[5] 李晓哲,谭智勇,戴一奇. 安全局域网主机入侵防御系统[J]. 清华大学学报:自然科学版,2010,50(1):54-57.

[6] XING Xu-jia,LIN Chuang,et al. A survey of computer vulnerability assessment[J]. Chinese Journal of Computers,2004,27(1):1-11.

[7] 叶云,徐锡山,贾焰,等. 基于攻击图的网络安全概率计算方法[J]. 计算机学报,2010,33(10):1 987-1 996.

[8] 柴争义,刘芳,朱思峰. 新型智能入侵防御模型[J]. 华中科技大学学报:自然科学版,2010,38(1):22-24.

[9] 苘大鹏,杨武,杨永田,等. 基于弱点关联和安全需求的网络安全评估方法[J]. 高技术通讯,2009,19(2):141-146.

[10] 苘大鹏,杨武,杨永田. 基于攻击图的网络脆弱性分析方法[J]. 南京理工大学学报:自然科学版,2008,32(4):416-419.

(下转第 284 页)