计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
44(12):2012~2019, 2007

基于攻击能力增长的网络安全分析模型

张海霞　苏璞睿　冯登国
(中国科学院软件研究所信息安全国家重点实验室　北京　100080)
(zhanghx@is.iscas.ac.cn)

A Network Security Analysis Model Based on the Increase in Attack Ability

Zhang Haixia, Su Purui, and Feng Dengguo
(*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080)

Abstract In recent years, network vulnerability analysis, which is attracting more and more domestic researchers and foreign researchers, has become a hotspot in the field of information security. A new model of network security analysis based on the increase in attack ability is proposed. It takes into account the network environment and simulates the attacker's behavior, and considers improving the attack ability as attacker's ultimate target to generate attack graph. The method used to represent attack graph make the attack target more clear, because it uses the attack ability's increment to describe a goal, which is more accurate than the attack ability itself. The minimum attack cost analysis considers the influence of similar attacks to compute the cost of each path for the first time, which conforms to the actual process of attack execution. The minimum environment change analysis can help people find out which attack path is most likely to be adopted by the attacker, which deals with IDS in a more reasonable way. These two analysis methods are helpful for improving the network configuration. The algorithm of attack graph generation and the method to analyze the attack graph proposed by the network security analysis model is more feasible than the existing ones.

Key words network security; network security analysis; attack model; attack graph; attack ability

摘　要　网络脆弱性分析是近年来国内外研究的热点问题之一.基于攻击能力增长的网络安全性分析模型以攻击者的能力增长为主导,参考网络环境配置,模拟黑客攻击自动生成攻击图.使用攻击能力增长表示攻击者的最终目标使得攻击图的表示更为准确.最小攻击代价分析第1次考虑了相似攻击对攻击代价的影响,以便对各条路径的攻击代价进行计算;最小环境改变分析考虑入侵检测的因素对最可能的攻击路径进行分析,对于入侵检测系统的处理更加科学合理;两种分析都为改善网络配置提供了依据.与已有成果相比,模型提出的算法和方法更为实际可行.

关键词　网络安全;网络安全分析;攻击模型;攻击图;攻击能力

中图法分类号　TP393.08

近年来,网络技术飞速发展的同时,黑客攻击技术也取得了相应的进步.利用系统多个脆弱性的多步攻击较之于几行代码扫描、一两个脆弱性利用之类的攻击更为常见.随着脆弱性扫描技术的不断成熟[1-3],网络安全分析技术成为国内外研究人员关注的焦点.它综合考虑网络环境配置、主机脆弱性

收稿日期:2006-09-20;修回日期:2007-08-20
基金项目:国家自然科学基金项目(60403006);国家"八六三"高技术研究发展计划基金项目(2006AA01Z437,2006AA01Z412,2006AA01Z433)

以及攻击者的能力对网络安全性进行合理的推断,并据此对安全配置进行改进,对抗攻击改善安全.

Swiler 和 Phillips 在文献[4-5]中提出了基于图的网络安全分析模型. 该模型以攻击为中心,通过从攻击目标出发的单向回溯来生成攻击图. 他们的工作在网络安全分析领域具有开创性的意义. Ammann 在文献[6]中提出的基于脆弱性的攻击图在简化了攻击图的表示空间的同时,攻击单调性的假设使得攻击图的构建在多项式时间内就能完成.

Ritchey 和 Ammann 在文献[7]中提出了基于模型校验的网络脆弱性分析方法,他们使用 SMV 作为分析的后台引擎,由模型校验的反例生成思想构建与安全属性相违反的攻击路径. 该方法第 1 次将形式化验证的思想应用于网络安全分析,然而一次仅生成一条攻击路径显然不能够满足网络安全分析的需要. 随着模型校验技术的不断发展,Sheyner 及其同事在 Ritchey 等人工作的基础之上,基于 NuSMV 提出了一种自动产生攻击图的算法[8-10];该算法能够对网络的所有可能的攻击路径进行分析,但随着主机和脆弱性数目的增加,攻击图生成的时间复杂度呈指数级增长.

后来,Ou 和 Govindavajhala 等人提出的基于逻辑推理的网络脆弱性分析方法[11-12]. Ammann 和 Pamula 提出的基于主机的网络脆弱性分析[13],都在降低时间和空间复杂度上付出了努力. 国内相关研究包括蒋屹新等人基于 Petri 网的主机或网络系统脆弱性分析[14]以及冯萍惠等人基于可靠性理论的分析模型[15],他们都在脆弱性分析的理论方面提出了独到的见解.

本文在前人工作的基础之上提出了一种基于攻击能力增长的网络安全分析模型. 该模型以攻击能力增长为主导,参考网络环境配置,从模拟攻击的角度对网络安全性进行分析,产生攻击图. 基于攻击图的最小攻击代价分析和最小环境改变分析能够预测攻击者最有可能采取的攻击路径. 与 Swiler 和 Phillips 在文献[4-5]的工作相比,由于初始环境描述的准确性,该模型生成的攻击图更为准确;与 Sheyner 等人在文献[8-10]的工作相比,该模型生成的攻击图在攻击图生成时间上有所减少. 此外,文中提出的最小环境改变分析对入侵检测系统的处理更加科学合理.

1 网络安全分析模型

1.1 模型基本定义

定义 1. 脆弱性是指由于系统硬件、软件或者安全策略上的错误而引起的缺陷,是违背安全策略的软件或硬件特征[16];信任脆弱性是指由于主机之间的信任带来的安全缺陷.

这里脆弱性和信任脆弱性均表示为 V. 攻击者对脆弱性的利用表示为 $V_x(Host\_sour, Host\_dest)$,其中下标 x 表示不同的脆弱性;$Host\_sour$ 表示脆弱性的源主机,即攻击的源主机;$Host\_dest$ 表示脆弱性的目标主机,亦即攻击的目标主机.

攻击者每发动一次原子攻击,都会带来环境和攻击能力的双重变化. 因此,我们有如下定义:

定义 2. 环境变化量 ΔE 是攻击者利用脆弱性或其他手段对网络发起攻击时的环境改变量.

攻击者利用脆弱性 V_x 对网络发起攻击时,攻击对网络环境带来的变化表示为环境变化量 ΔE_x,则可表示为 $V'(Host\_sour, Host\_dest) = \Delta E_x$.

定义 3. 攻击能力增量 ΔA 指攻击者利用脆弱性或其他手段对网络发起攻击时,攻击者的能力增加量.

攻击者利用脆弱性 V_x 对网络发起攻击时,攻击者能力的增长表示为攻击能力增量为 ΔA_x. 表示为 $V''_x(Host\_sour, Host\_dest) = \Delta A_x$. 攻击者一次攻击或者脆弱性利用带来的影响表示为 $V_x(Host\_sour, Host\_dest) = \Delta A_x + \Delta E_x$.

定义 4. 攻击模型 M 是一个有限状态自动机. 表示为 $M(S, \tau, \Delta A_0, \Delta A_t)$. 其中 $S = \{\Delta A\}$ 表示攻击者能力变化增量集;初始增量为 $\Delta A_0 = \varnothing$,且 $\Delta A_0 \in \{\Delta A\}$;终止增量 $\Delta A_t \in \{\Delta A\}$,为攻击者的目标增量;$\tau = \{V_x\}$ 表示利用的脆弱性和攻击集合.

1.2 网络连通性

网络连通性描述了攻击者与主机之间、主机与主机之间的通信关系. 如图 1 所示:

	h_1	h_2	…
h_1		p	…
h_2	p		…
□	□	□	□

Fig. 1 The graph of network connectivity.

图 1 网络连通性关系图

第 m 行 n 列的矩阵元素表示主机 h_m 和 h_n 之间的连通关系. p 表示两主机连接的端口或协议;两主机不连通表示为 n,物理连通表示为 y.

1.3 主 机

我们将主机描述为一个服务集、一个敏感数据集以及一个脆弱性集合. 即 $Host$:{$Services$, $Data$,

$Vuls$}.

服务集 $Services$:{$Service1$,$Service2$,…}. 主机开放了一个服务,表示为[$Hostid$]. $services$. $serviceid$.

脆弱性集合 $Vuls$:{$Vul1$,$Vul2$,…}. 主机存在特定的脆弱性,表示为[$Hostid$]. $vuls$. V_x.

敏感数据集 $Data$:{$Data1$,$Data2$,…}. 主机上存在敏感数据,也看做主机对数据的拥有关系,表示为[$Hostid$]. $Data$. $data\_id$.

1.4 攻击者模型

我们以攻击者的能力来表示攻击者,并假设攻击者具有最高水准的攻击技能. 攻击者能力包括 3 个方面:

1) 攻击者对各个主机的权限集合. 这里我们考虑 3 类权限 $none < user < root$. 权限集合表示为 Att_pri,攻击者具有某个主机的特定权限,表示为 Att_pri. $Hostid$. att_pri, $att\_pri \in$ {$none$, $user$, $root$}. 对于每一个主机仅保存最大权限.

2) 攻击者对数据的访问权限. 表示为 Att_data. $Hostid$. $data\_id$.

3) 攻击者与目的主机的连通性. 攻击者的每一步攻击都有一个目的主机,根据攻击的源主机、网络的联通矩阵和目的主机可以确定攻击者与目的主机的联通关系[Att_host_sour]. [$Host\_dest$]. [$Comm$]. $comm$,其中,$comm \in$ {$servicename$, $physical$, $none$, $port$}.

1.5 信任关系模型

信任关系有两个主机之间的信任关系,也有域之间的信任关系. 这里我们将信任关系全部模型化为主机和主机之间的信任关系. 当信任关系为域和域之间时,将信任关系模型化为多主机与多主机之间. 信任关系可以是双向的也可以是单向的,源主机对目的主机单向的信任关系表示为

[$Host\_sour$]. [$Host\_dest$]. $trust$. [$username$].

两个主机之间双向的信任关系,例如主机 A 和 B 之间的双向信任关系表示为

[$HostA$]. [$HostB$]. $trust$. [$username$];

[$HostB$]. [$HostA$]. $trust$. [$username$].

出于整体考虑,我们将基于信任关系的信任脆弱性($Trust\_vul$)表示为

前提条件:

[$Host\_dest$]. [$Host\_sour$]. $trust$. [$username$];

[Att_pri]. [$Host\_sour$]. $user$. $username$.

后果:

[Att_pri]. [$Host\_dest$]. $user$. $username$.

1.6 脆弱性利用模型

脆弱性的形式化表示如下.

前提条件:

1) 目的主机存在脆弱性 V_x

[$Host\_dest$]. $vuls$. V_x;

2) 目的主机与源主机相连

[$Host\_sour$]. [$Host\_dest$]. $comm$;

3) 攻击者拥有源主机的用户权限

[Att_pri]. [$Host\_sour$]. $user$;

4) 攻击者拥有目标主机的用户权限

[Att_pri]. [$Host\_dest$]. $user$;

5) 目标主机存在数据 $data$

[$Hostdest$]. [$Datas$]. $data$.

攻击能力增长:ΔA_x.

环境改变:ΔE_x.

2 攻击图生成

2.1 攻击树生成算法子函数

该算法是当前节点的子节点生成算法. 即对于所考虑的每一个脆弱性,依次检查前提条件是否为真,如果为真,就在当前攻击树中增加以 $N_{current}$ 为头节点,以脆弱性利用所带来的供给能力增长 ΔA_x 为尾节点的边. 具体算法如图 2 所示:

Variables:

$N_{current}$—the current node;

N_{goal}—the attacker's goal node;

$Path$—the path from $N_{current}$ to the root node of tree;

VS—vulnerability set exists on the hosts that the attacker can reach.

Algorithm:

① Function Generate AllSubNode($N_{current}$)

② If($N_{current}$!= N_{goal})

③ Foreach v_x, $v_x \notin Path$ and $v_x \in VS$

④ If(v_x. $Precondition$ == true)

⑤ $Attack\_tree$. $AddEdge$(V_x($attack\_host$, $host$, v_x. $host$), $N_{current}$, ΔA_x).

Fig. 2 The first algorithm.

图 2 算法 1

2.2 攻击树生成算法

算法 2 描述了攻击树的生成算法. 如图 3 所示,首先,对当前节点执行广度搜索,如果当前节点的深度没有达到预定深度减 1,将对当前节点的第 1 个孩子节点执行搜索;如果当前节点的深度等于预定深度减 1,就对当前节点的第 1 个兄弟节点执行遍历搜索;如果当前节点不存在兄弟结点就对当前节点的父节点的兄弟节点执行搜索;如果当前节点

的父节点不存在兄弟节点,就向上搜索,直到找到节点 找不到没有被搜索过的节点算法结束. 通过算法 2 可以得到一个有初始节点出发的攻击树,也即一系列的攻击链. 为了安全分析的方便,设定算法 3 来生成一个攻击图.

```
Variables:
    N_current — the current node;
    N_goal — the attacker's goal node;
Constant: n — the search depth which set in advance;
Algorithm:
① Function GenerateTree(N_current)
②   If(N_current.depth < n)
③     GenerateAllSubNode(N_current);
④   If(N_current.depth != n-1 && N_current.hasUnsearchedChildN())
⑤     N_current = N_current's first child node;
⑥     GenerateTree(N_current);
⑦   else
⑧     If(N_current.hasUnsearchedBN())
⑨       N_current = N_current's first brother node;
⑩     Else
⑪       While(!N_current.parenthasUnsearchedBN())
⑫         N_current = N_current.parent;
⑬         If(N_current == root)
⑭           Flagend = true;
⑮           Break;
⑯     If(Flagend == false)
⑰       GenerateTree(N_current)
```

Fig. 3 The second algorithm.

图 3 算法 2

2.3 攻击图生成算法

通过执行攻击图生成算法,将攻击树中的相同路径合并,减少表示上的冗余. 相同路径指具备相同攻击能力的路径,环境因素可能不尽相同. 具体的攻击图生成算法如图 4 所示:

```
Variables:
    AG — the attack graph;
    AT — the attack tree;
    AC — the array of Attack ability;
    TN — tree node;
    ac — certain attack ability;
    AC[i].NodeSet — the nodes set according to the ith element of AC.
Algorithm:
① Function GenerateAttackGraph()
②   Foreach TN ∈ AT
③     If(TN.ac ∈ AC)
④       TN.code = ac.suffixInAC();
⑤     Else
⑥       InsertIntoAC(ac);
⑦       TN.code = AC.length;
⑧   Arrange AC from small to big;
⑨   Foreach ac in AC
⑩     Foreach two treenode out-of-order(TN1, TN2)
⑪       If(TN1.hasSameEdge(TN2))
⑫         Combine the next node of them.
```

Fig. 4 The third algorithm.

图 4 算法 3

攻击图生成算法主要由攻击树来生成攻击图. 关于攻击图生成算法有以下几点需要特别说明:

首先,攻击图生成算法的①~⑥行是对攻击树攻击能力相等的节点(简称等能力节点)的标示. 等能力节点标示不会出现如图 5、图 6 所示的情况:

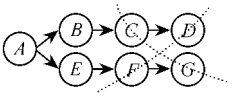

Fig. 5 Unreasonable result (a).

图 5 不合理标示结果(a)

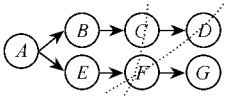

Fig. 6 Unreasonable result (b).

图 6 不合理的标示结果(b)

即节点 C 的攻击能力(A_C)等于节点 G 的攻击能力(A_G),节点 D 的攻击能力(A_D)等于节点 F 的攻击能力(A_F). 因为根据攻击的不可回溯性 $A_C < A_D, A_F < A_G$;由于 $A_C = A_G, A_F = A_D$,将导致 $A_C > A_D$,显然矛盾. 因此,攻击能力节点集也不会有交集,即不会出现图 6 所示的情况.

其次,攻击图生成算法的第⑦行是对等能力节点集合的排序. 该排序算法使用快速序算法对攻击能力节点集进行排序. 攻击树由多个攻击链组合而成. 这里我们说某一节点集与某个攻击链相关是指某一节点集包含某攻击链上的节点. 关于两个节点集攻击能力大小的比较依据这两个节点集合共同关联的攻击链上节点的深度来比较. 例如,节点集 N_a 与节点集 N_b 公共关联的链集为 $\{L_1, L_2, L_3, \cdots, L_m\}$,$N_a$ 对应的节点集为 $\{na_1, na_2, na_3, \cdots, na_m\}$,$N_b$ 对应的节点集为 $\{nb_1, nb_2, nb_3, \cdots, nb_m\}$,根据上面的推理可知或者 $na_1.depth > nb_1.depth$,$na_2.depth > nb_2.depth$,$na_3.depth > nb_3.depth$,$\cdots$,$na_m.depth > nb_m.depth$ 或者 $na_1.depth < nb_1.depth$,$na_2.depth < nb_2.depth$,$na_3.depth < nb_3.depth$,$\cdots$,$na_m.depth < nb_m.depth$,如果存在第 3 种情况与攻击的不可回溯性的假设相违背.

此外,排序过程还可能存在另外一种情况,就是两个节点集不存在公共关联链. 该种情况又可分为两种:一种是两个节点集通过别的结合间接相关,如图 7 所示;另外一种即完全不相关联,如图 8 所示. 图 7 所示的情况,通过间接的比较可以进行排序;图 8 所示的情况我们认为节点集不可比较. 但对后续算法并无影响,只须对节点集单独进行合并即可.

再次,攻击图生成算法的第⑨~⑪行是在能力节点集合排序的基础上,从深度最大的节点集开始进行合并,这样每一次针对两个节点的合并仅需考虑第 1 个子节点情况.

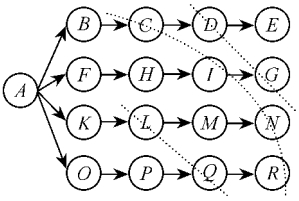

Fig. 7 Related nodes sets.

图 7 等势节点集关联

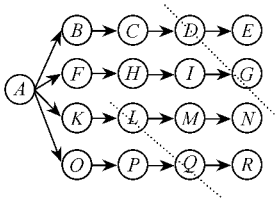

Fig. 8 Unrelated nodes sets.

图 8 等势节点集不关联

3 安全性分析

3.1 最小攻击代价分析

攻击者往往希望仅仅最小的付出就能达到攻击目标. 从攻击角度出发的最小攻击代价分析应依据能力增长的代价,对各个能够达到攻击目标的攻击路径代价进行分析. 攻击者达到攻击目标所付出的总代价就是攻击者各步攻击所付出代价的综合,然而并不是简单的加和. 考虑如下情形:攻击者利用主机 A 上的脆弱性 V_x,获得对目标攻击主机 B 上的用户权限;与攻击者利用主机 B 上的脆弱性 V_x,获得对目标攻击主机 D 上的用户权限;对攻击者而言,一旦进行了第 1 次攻击,第 2 次攻击尽管环境因素有所影响,但攻击变得容易很多,代价就小很多. 因此,最小攻击代价分析需要考虑相似攻击因素.

如果一次攻击过程没有发生过相似攻击,攻击过程代价就表示为

$$Cost = \sum_{i=1}^{n} cost_i, \tag{1}$$

其中 i 表示攻击过程的步骤序号. n 表示攻击过程的子攻击数目. $cost_i$ 表示第 i 个子攻击成功需要付出的代价. 如果一次攻击过程发生过相似攻击,攻击过程代价就表示为

$$Cost = \sum (d_i)^{time-1} \times cost_i. \tag{2}$$

这里的 d_i($d_i<1$)表示攻击过程对攻击者经验的依赖系数,$time$ 指攻击过程相似子攻击的重复次数. 最小攻击代价分析即在对各个攻击链的攻击代价进行分析之后,对攻击代价进行排序,值最小的即为最小代价攻击链.

3.2 最小环境改变分析

为了不引起网络管理员和网络用户的注意,攻击者期望攻击过程在达到攻击目标之前能够最小地改变环境. 最小环境改变分析针对以下 3 方面的因素对环境改变进行分析:1)环境改变是否会引起入侵检测系统的警报;2)环境改变是否会引起网络用户的注意;3)环境改变可能引起警报或用户注意相对于整个攻击过程的位置. 这里我们借鉴 Sheyner[10] 将入侵检测模型化为

$$IDS: \{H, H, \Delta E\} \rightarrow \{s, d, b\} \text{ 和}$$
$$IDS: \{H, H, \Delta A\} \rightarrow \{s, d, b\}.$$

所不同的是这里在产生攻击图的过程中并不考虑入侵检测系统的影响,而是将入侵检测系统作为对环境改变分析的参考. 如果环境改变会引起入侵警报,计算过程需要引进放大系数;如果环境改变不会引起入侵警报,无须放大;介于两者之间则根据具体情况进行放大.

另外,每一次子攻击对环境的改变不尽相同,过大的环境改变可能会引起用户的注意从而使得用户采取措施干扰入侵. 因此对环境改变是否会引起用户的注意我们定义如下函数:

$$\begin{cases} h(\Delta E) = a, 0 \leqslant a < 1, \\ h(\Delta E) = b, 1 \leqslant b. \end{cases} \tag{3}$$

环境改变可能引起警报或用户注意相对于整个攻击过程的位置对于攻击者是否会采用该攻击过程来达到攻击目标十分重要. 如果在系统做出反应前能够达到攻击目标,那么该改变相对来说是比较小的;如果系统响应在攻击刚刚开始的阶段,显然这样的改变是比较大的. 因此我们定义

$$p\_pos = 1 - \frac{depth - 1}{length}. \tag{4}$$

p_pos 表示位置对环境改变的贡献系数;$depth$ 表示可能引起警报或用户注意的攻击深度;$length$ 表示攻击链的长度. 综合各种因素的环境改变表示为

$$E\_Change = \sum_{i=1}^{length} ids_i \times h(\Delta E_i) \times p\_pos_i, \tag{5}$$

其中 ids_i 表示第 i 个子攻击的入侵检测放大系数;$h(\Delta E_i)$表示环境改变引起用户注意的系数;p_pos_i 表示第 i 个子攻击的位置对环境改变的贡献系数.

环境改变结果我们用两部分来表示:一部分是量化的环境改变表示;另外一部分就是是否会引起入侵警报的表示. 从攻击者角度出发,如果攻击发生在白天,入侵警报可能会严重影响入侵;相反,如果在晚上,入侵警报可能较少地影响入侵. 因此环境分析的结果表示为 $ids + E\_Change$,其中 $ids \in \{s, d, b\}$. 最小环境改变分析可以根据上述两项结合具体实际情况进行分析. 通过最小环境改变分析,我们可以分析得出攻击者在特定条件下可能采取的攻击路径,从而有效地阻止攻击.

4 网络安全分析实例

我们对图 9 所示的网络进行分析以便更好地分析和理解本文所提到的网络脆弱性分析模型. 如图 9 所示,外部防火墙和内部防火墙将网络分为 3 部分:一部分是外部网络,即我们所说的因特网;另一部分是内部网络,也是攻击者的目标网络,有两台分别运行 Linux,Windows 的主机;第 3 部分是内网和外网的临界区域,这里安放了一台运行了 IIS 的 Web 服务器. 入侵检测系统存在于内网和内部防火墙之间.

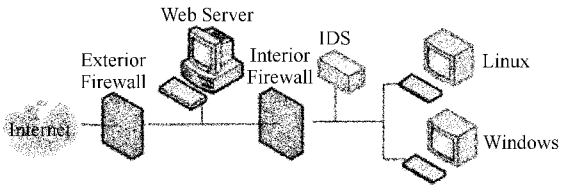

Fig. 9 Topology of network example.

图 9 网络拓扑图

内部网络安装了 Windows 的主机主要用来工作和上网,Linux 机安装了 mysql 数据库,为了开发和使用的方便,通过 Windows 主机可以直接访问 Linux 上的 mysql 数据库. 外部网络所有用户都可以访问 IIS Web 服务器,通过内网的 Windows 主机也可访问.

IIS Web 服务器存在一个缓冲区溢出漏洞,攻击者利用该漏洞可以获得根权限,同时使得 IIS 服务关闭;Windows 主机存在一个 JDBC 的远程漏洞,该漏洞允许攻击者远程以用户身份执行任意的 dll;Windows 系统存在一个 SMB 权限提升漏洞,成功利用此漏洞的攻击者可以完成本地用户的权限提升;Linux 系统存在信任脆弱性,即信任 Windows 主机,允许该主机以特定用户身份访问 mysql 数据库;Linux 系统存在一个缓冲区单字节溢出漏洞,远程攻击者利用这个漏洞可以以 Root 用户权限在系统上执行任意命令. 根据上面的描述,实例网络的主机之间的连通性如表 1 所示:

Table 1 Connectivity Relationship of Hosts

表 1 实例网络的主机连通关系

Hosts	Attacker	Web Server	Windows	Linux
Attacker	y	80	n	n
Web Server	y	y	y	y
Windows	n	80	y	trust
Linux	n	n	y	y

连通矩阵中 n 表示两个主体物理不相连;y 表示物理相连;80 表示 A 可以通过 80 端口访问 B;trust 表示 A 由于为 B 信任可以以某一用户登录 B. 在整个攻击过程中,主机连通矩阵有所变化,主要用来获得当前主机的连通信息. 本文考虑的脆弱性如表 2 所示:

Table 2 List of Vulnerabilities

表 2 脆弱性列表

Vulnerability Name	Exploit Type	CVE Code
Trust Vulnerability	Remote user logon	
IIS buffer overflow	Remote get root privilege	CAN-2002-0364
JDBC remote code execute	Remote get user privilege	CVE-2002-0866
Linux single byte overflow	Remote get root privilege	CAN-2003-0252
SMB privilege elevation	Local get root	CVE-2006-2373

根据前面的算法 1 对实例网络执行算法生成的攻击树如图 10 所示:

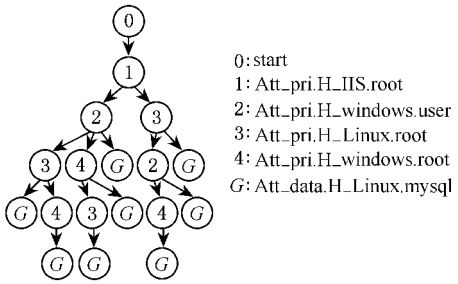

Fig. 10 The generated attack tree.

图 10 攻击树

根据算法 2 对图 10 的攻击树进行合并后得到的攻击图如图 11 所示:

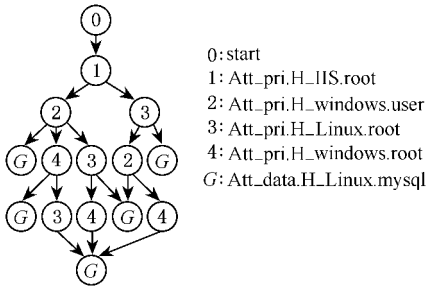

Fig. 11 The attack graph after incorparation.

图 11 经过等攻击能力合并的攻击图

根据算法 3 得到的基于攻击能力的攻击如图 12 所示.

对脆弱性 V_1, V_2, V_3, V_4, V_5 利用带来的攻击能力增长分别为 1,2,2,2,3,该实例网络不存在相似攻击. 根据攻击能力增长分析算法计算可得图 10

所示的 $B\rightarrow1\rightarrow2\rightarrow G$ 路径所需攻击能力增长是最小的.

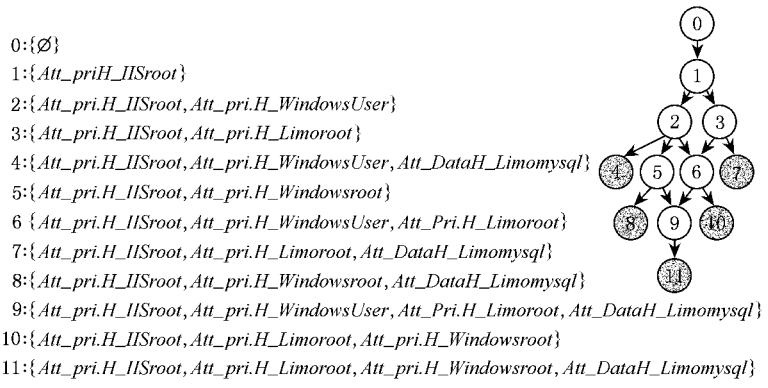

Fig. 12 The attack graph representing attack ability.

图 12 使用攻击能力表示的攻击图

如下所示,表 3 给出了每一个脆弱性的入侵检测放大系数和环境改变引起用户注意的系数.

Table 3 The Coefficient List of Vulnerabilities

表 3 各个脆弱性的隐秘系数

Related Function	V_1	V_2	V_3	V_4	V_5
$Ids(\Delta E)$	1	1	1.5	1	2
$h(\Delta E)$	0.5	1.5	0.5	1	1

各个路径的环境改变分析如表 4 所示:

Table 4 The Result of Minimum Environment Analysis

表 4 最小环境改变分析结果

No	Vul Sequene being used	Nodes Sequene in Fig.7	d/n	Result
1	2,3,5,1	$B\rightarrow1\rightarrow2\rightarrow3\rightarrow G$	d	3.1875
2	2,3,5,4,1	$B\rightarrow1\rightarrow2\rightarrow3\rightarrow4\rightarrow G$	d	3.8000
3	2,3,4,5,1	$B\rightarrow1\rightarrow2\rightarrow4\rightarrow3\rightarrow G$	d	3.6000
4	2,3,4,1	$B\rightarrow1\rightarrow2\rightarrow4\rightarrow G$		2.6875
5	2,5,1	$B\rightarrow1\rightarrow3\rightarrow G$	d	3.0000
6	2,5,3,1	$B\rightarrow1\rightarrow3\rightarrow2\rightarrow G$	d	3.5000
7	2,5,3,4,1	$B\rightarrow1\rightarrow3\rightarrow2\rightarrow4\rightarrow G$	d	4.0500
8	2,3,1	$B\rightarrow1\rightarrow2\rightarrow G$		2.1667

通过如上分析可知,路经 8 具有最小的环境改变系数,入侵检测系统能否检测未知;路经 4 次之.其余攻击路径的某一步或几步可能会引起入侵检测警报.

5 结 论

本文在前人工作的基础之上提出了基于攻击能力增长的网络安全分析模型.与已有的模型相比,其优势有以下几点:一是使用攻击能力增长能够确切地描述出攻击者的攻击目标,较为准确地构建攻击图;二是从攻击者角度出发的与 IDS 相结合的环境改变分析较之将 IDS 作为攻击图形成的一个因素考虑更为科学合理;再者,从相似攻击的角度对攻击代价的分析尚无先例.

基于模型校验的脆弱性分析模型具有指数级的复杂度[8].基于图的模型[4-5]生成时间主要取决于攻击模板的数量,此种条件下生成的攻击图存在较大局限性.而基于 Prolog 的模型[11-12]通过脆弱性归类降低了复杂度却不能有效地生成攻击图.以脆弱性为节点的攻击图生成模型[17]的时间复杂度为 $O(n^4)$.本文中提出的模型由于攻击树的生成过程限制了攻击路径的长度,因此随着网络系统的增大,攻击图生成时间在可接受范围内,且能生成满足分析需要的攻击图.相比之下更为实际可行.下一步工作将着眼于模型的优化改造和推广.

参 考 文 献

[1] Dan Farmer, Wietse Venema. Improving the security of your site by breaking into it [R]. USENET Newsgroup Comp. Security Unix, Tech Rep: ITSTD-721-FR-90-21, 1993

[2] Internet Scanner. Internet Security Systems [OL]. http://www.iss.net/, 2002

[3] Nesssus Homepage [OL]. http://www.nessus.org/, 2002

[4] C A Phillips, L P Swiler. A graph-based system for network vulnerability analysis [C]. New Security Paradigms Workshop, Charlotte sville, VA, 1998

[5] L P Swiler, C Phillips, D Ellis, *et al*. Computer-attack graph generation tool [C]. The DARPA Information Survivability Conference and Exposition, Los Alamitos, CA, 2000

[6] P Ammann, D Wijesekera, S Kaushik. Scalable graph-based vulnerability analysis [C]. The 9th ACM Conf on Computer and Commuincations Security, Washington, DC, 2002

[7] R Ritchey, P Ammann. Using model checking to analyze network vulnerabilities [C]. IEEE Symp on Security and Privacy, Oakland, CA, 2001

[8] O Sheyner, J Haines, S Jha, *et al*. Automated generation and analysis of attack graphs [C]. IEEE Symp on Security and Privacy, Oakland, CA, 2002

[9] O Sheyner, J M Wing. Tools for generating and analyzing attack graphs [C]. Workshop on Formal Methods for Components and Objects, Tehran, Iran, 2004

[10] S Jha, O Sheyener, J M Wing. Two formal analyses of attack graphs [C]. Workshop on Computer Security Foundations, Nova Scotia, Canada, 2002

[11] Xinming Ou. A logic-programming approach to network security analysis: [Ph D dissertation] [D]. Princeton: Princeton University, 2005

[12] Xinming Ou, Sudhakar Govindavajhala, Andrew W Appel. MulVAL: A logic-based network security analyzer [C]. The 14th USENIX Security Symp, Baltimore, Maryland, 2005

[13] P Ammann, J Pamula. A host-based approach to network attack chaining analysis [C]. The 21st Annual Computer Security Applications Conf, Tucson, Arizona, 2005

[14] Jiang Yixin, Lin Chuang, Qu Yang, *et al*. Research on model-checking based on Petri nets [J]. Journal of Software, 2004, 15(9): 1265-1276 (in Chinese)
(蒋屹新, 林闯, 曲扬, 等. 基于 Petri 网的模型检测研究[J]. 软件学报, 2004, 15(9): 1265-1276)

[15] Feng Pinghui, Lian Yifeng, Dai Yingxia, *et al*. A vulnerability model of distributed systems based on reliability theory [J]. Journal of Software, 2006, 17(7): 1633-1640 (in Chinese)
(冯萍慧, 连一峰, 戴英侠, 等. 基于可靠性理论的分布式系统脆弱性模型[J]. 软件学报, 2006, 17(7): 1633-1640)

[16] Matt Bishop. Computer Security: Art and Science [M]. Boston: Addison-Wesley Professional, 2002

[17] Steven Noel, Brian O'Berry, Charles Hutchinson, *et al*. Combinatorial analysis of network security [C]. The 16th Annual Int'l Symp on Aerospace/Defense Sensing, Simulation, and Controls, Orlando, Florida, 2002

Zhang Haixia, born in 1981. Ph. D. candidate. Her main research interests include network information security.
张海霞,1981 年生,博士研究生,主要研究方向为网络信息安全.

Su Purui, born in 1976. Ph. D. and associate professor. His main research interests include network information security.
苏璞睿,1976 年生,博士,副研究员,主要研究方向为信息安全、网络安全.

Feng Dengguo, born in 1965. Professor and Ph. D. supervisor in the Institute of Software, the Chinese Academy of Sciences. He is mainly engaged in the research and development of information and network security.
冯登国,1965 年生,研究员,博士生导师,主要研究方向为信息安全.

Research Background

Over recent years, network security evaluation and analysis became a research focus of network security. There are many works on network modeling and vulnerability analysis, but they are not perfect, and still need to be improved. In this paper, a new network security analysis model and two analysis methods have been proposed to analyze the security character of network more reasonably, which can be more feasible and reasonable.

This research work is supported by the National Natural Science Foundation of China under the grant No. 60403006; and by the National High-Tech Research and Development Plan of China (863) under the grant No. 2006AA01Z437, 2006AA01Z412 and 2006AA01Z433.