文章编号:1672 - 058X(2012)12 - 0044 - 05

# 基于攻击模式的广度搜索攻击图生成算法*

吴淑语, 李 波
(重庆理工大学 计算机科学与工程学院,重庆 400054)

**摘 要**:网络攻击者一旦发生攻击行为,通常希望攻击行为能危害到最大范围,基于这一前提,依据广度优先搜索策略及属性攻击图模型,提出了基于攻击模式的广度搜索攻击图的生成算法,算法可以很快的生成攻击图并且规模明显减小,最后对该算法的性能进行了分析和实验分析。

**关键词**:广度搜索;攻击图;网络安全
**中图分类号**:TP273 **文献标志码**:A

随着网络信息技术的不断发展,越来越重视网络的安全性,但网络攻击事件不断的增加,最根本的原因是网络系统中存在可以被渗透的脆弱性。目前,有很多脆弱性扫描工具可以发现网络系统存在的脆弱点,但是这些工具只是单独的研究节点的脆弱性,不能研究脆弱性之间的联系和存在的潜在风险。基于攻击图的网络安全分析方法,可以对网络系统进行综合脆弱性分析,发现系统未知的脆弱性及脆弱性之间的关系。基于攻击的方法是目前网络安全分析方法中非常重要的研究方法,而攻击图的生成方法又是其中关键的环节。由于攻击图中存在很多无效的攻击路径,由此导致攻击图规模比较大,难以理解的问题。网络攻击者一旦发生攻击行为,通常希望攻击行为能危害到最大范围。在这种情况下为了能解决上述的问题,依据广度优先搜索策略及属性攻击图模型,提出了基于攻击模式的广度搜索攻击图的生成算法,算法可以构建出在一定攻击步数之内所达到的所有攻击路径,应用广度优先搜索策略来约束攻击图的生成过程,从而减小攻击图的规模。

## 1 相关研究

生成攻击图 1 所使用的方法是一种正向搜与逆向搜索相结合的一种方法。寻找攻击路径时采用正向宽度优先算法,生成完所有攻击路径后,采用逆向搜索算法消除那些未达到攻击目标的节点。此方法用到二次处理攻击图来降低攻击图的规模[1]。文献[2]在生成的攻击图中所使用的方法是一种由初始状态到目标状态的正向、宽度优先的搜索算法。为了限制攻击图的规模,采用了限制攻击步骤数和状态节点可达概率的优化策略,生成的攻击图是多目标攻击图。方法中的概率是一个需要应用专家知识才能确定的量,而其最大攻击步骤则不易确定,不同类型的网络可能值也不同,过大则导致约束败果不好,过小将会损失很多重要的攻击路径[2]。文献[3]提出利用攻击图模型分析网络的脆弱性。其所实现的攻击图生成方法是根据已有的攻击模板,从目标状态开始,采用深度优先的逆向搜索策略生成网络攻击图。攻击图完全靠手工生成,没有实现自动化[3]。文献[4]构建了一种新的称为 MP 图的攻击图,采用由初始状态向目标状态进行宽度

**收稿日期**:2012 - 04 - 10;**修回日期**:2012 - 05 - 24.
* **基金项目**:重庆市教委科技项目资助(KJ110831).
**作者简介**:吴淑语(1987-),男,山东临沂人,硕士研究生,从事网络安全研究.

优先搜索的算法,最后生成的攻击图为多目标的 MP 攻击图。这种攻击图的规模得到了控制,同时也易于理解,但是不能直接应用于网络安全分析[4]。

## 2　基于攻击模式的攻击图生成算法

### 2.1　相关定义

攻击图的生成,首先要将抽象的事物用形式化语言具体化,用模型来表示,也是建模的一个过程,以下给出了目标网络 4 个层面的定义[5]。

(1) 网络服务。是指一些在网络上运行的、面向服务的、基于分布式程序的软件模块,可表示一个四元组(HD,SC,PL,PT)分别表示主机的 IP 地址、主机提供的服务、服务 SC 所用的协议、服务 SC 所用的端口。

(2) 漏洞。漏洞指在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷,从而可以使攻击者能够在未授权的情况下访问或破坏系统。采用 1 个三元组表示,即(HD,SN,CVE),分别表示主机的 IP 地址、主机提供的服务名称、漏洞编号。

(3) 防火墙访问控制规则。目标网络中的各主机间的可到达性与防火墙规则有关系,所以应该对防火墙访问控制规则进行定义。采用四元组表示(HT1,HT2,PL,PT),表示在防火墙允许的情况下,通过端口 PT,协议 PL 的主机 1 到主机 2 的一段报文。

(4) 攻击图。攻击图是目标网络从初始状态到目标状态的状态转换图,$T=(S,E,S_0,S_G)$,其中,$S$ 是网络系统的安全状态节点的所有集合;$E\subseteq S\times S$ 为改变网络安全状态的相应攻击行动;$S_0\in S$ 表示目标网络初始状态的节点集合;$S_G\in S$ 为目标状态节点的所有集合[6]。

### 2.2　算法设计思路

基于攻击者能力的"单调性"假设,依据广度优先搜索策略及属性攻击图模型,提出了基于攻击模式的广度搜索攻击图的生成算法,算法的是列举所有可能的攻击路径,然后利用其中攻击路径的联系将所有攻击路径绘制成属性攻击图,该攻击图能够表示所有的攻击方法,而且还能够分析目标网络脆弱节点的关联性和由此产生的潜在威胁。算法流程图如 1 所示。

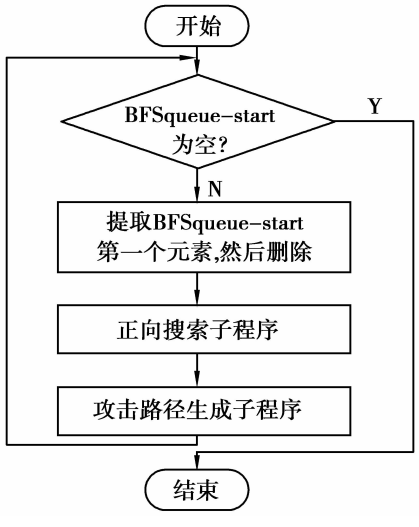


图 1　攻击图生成算法流程图

队列 BFSqueue-start 所有要分析的攻击节点集合,即存放攻击者的起始位置和目标位置的集合。

首先判断 BFSqueue-start 是否为空,如果为空,说明没有攻击目标,则程序结束,否则提取 BFSqueue-start 的第一个元素进行分析,然后删除此元素,接着依次调用广度搜索子程序和攻击路径生成子程序;循环执行第一步,直至存放攻击节点的集合为空。

### 2.3　广度搜索攻击图生成算法

广度搜索攻击图生成算法采用广度优先的算法,枚举所有可能的攻击路径。从初始目标攻击节点开始访问,如果该节点的脆弱性可以被攻击利用那就做相应的标记,并输出访问的节点属性值,从被访问的节点出发,依次搜索与该节点有关联的所有未被访问的邻接点,将所得到的节点属性值合并到攻击节点集合当中去,重复进行,直到所有节点都被访问为止。

广度搜索攻击图生成核心算法如下:

```
while(BFSqueue≠φ)
{IP←BFSqueue - first
BFSqueue - first - del
if((IPstart - Ip) ∈ BFSqueue - attackhost)
```

```
{(IPstart:IP)→BFSqueue - attackhost
}
else
{flag = false
foreachport ∈ reach(IPstartIP)
{foreachE ∈ explot
if(preE = =(E∪Lip&&ATTACKprivilege&&serviceIP)
{ATTACK→ATTACK∪e
ATTACKprivilege←poseE
(Ipstart:IP:port)→BFSqueue - attack
flag = true
break
}
}
}
if(flag)
{(IPstart:IP)→BFSqueue - attackhost
}
}
```

利用 C++ 和 SQL 数据库来实现整个攻击图生成算法。C++ 的模块简单有效,能提高算法的效率从而保证攻击图生成的有效性和完备性。SQL 数据库简单易用,可以存储海量数据且查询速度快,改善了整个算法的性能。广度搜索算法结束后输出目标网络攻击图,包含被攻击的脆弱性节点、这些节点之间的联系以及所有攻击路径。

### 2.4 算法分析

在算法分析过程中,使用 Connection 词语表示网络中两个主机之间的连接关系。Connection(s:Host,d:Host,PL:Protocol,PT:Port),表示在防火墙允许的情况下,通过端口 PT,协议 PL 的一台主机到另一主机的一段报文。

**定理 1** 目标网络模型中,最多有 $\sum_{i=1}^{N-1} i$ 条连接关系,其中 $N$ 为网络中主机的数目。

证明:在表示连接关系的变量中,只有变量 $s$ 和变量 $d$ 与主机数目 $N$ 相关,可以被实例化成目标网络中所有可能的主机 IP 地址,其他的变量则与网络规模 $N$ 没有相关性,因此最多具有 $\sum_{i=1}^{N-1} i$ 个实例化结果。

在上面的基于攻击模式的广度搜索攻击图生成算法中,将实例化后的攻击模式与攻击者能力进行匹配,单一的攻击模式与攻击者能力匹配的时间是不变的,所以匹配的时间消耗与进行匹配的次数成正比的关系。

**定理 2** 攻击模式与攻击者能力的匹配次数最多需 $O(A^2)$,其中 $A$ 为实例化后的攻击模式数量。

**证明** 根据定理 1,从初始状态 $s_0$ 出发,依据上述算法进行迭代运算最终可以获得最小不动点;依据攻击者的单调性假设,攻击者在攻击的过程中不会失去已经获得的攻击能力,因此最多进行 $O(A^2)$ 次匹配,就可能将所有的攻击模式全部实例化成功,即攻击模式与攻击者能力的匹配次数最多需 $O(A^2)$。

基于广度搜索算法中,实质是枚举目标网络中所有可能存在的攻击路径。假设目标网络中有 $N$ 台主机,存在的 $V$ 个脆弱性,有 $M$ 个攻击模式与之相对应,因为一个脆弱性可以对应多个攻击模式,所以 $M \geqslant V$。假设 $M = V$,首先将攻击模式实例化,在最坏的状态下,目标网络主机位全连接关系,根据定理 1 实例化后将产生 $M \times \sum_{i=1}^{N-1} i$ 个攻击模式,攻击模式与攻击者能力的最多进行 $(M \times \sum_{i=1}^{N-1} i)^2$ 匹配,所以本算法的复杂度为 $o(\delta v^2 N^4)$,其中 $\delta$ 为进行一次匹配所需的时间。

在星型网络环境下,网络主机之间有 $N-1$ 连接,$N$ 为网络中的主机数量,该算法的复杂度为 $o(\delta v^2 N^2)$,其中 $\delta$ 为进行一次匹配所需的时间。

在环形网络环境下,网络主机之间有 $N$ 个连接,$N$ 为网络中的主机数量,该算法的复杂度为 $o(\delta v^2 N^2)$,其中 $\delta$ 为进行一次匹配所需的时间。

通过以上分析,可以发现在大多数情况下,该算法可以满足在大型网络规模环境下构建攻击图,但少数

出现的大量全连接的网络会使算法的复杂度飘升。图 2 给出了在算法复杂度实验中,目标网络中主机的数目和生成攻击图所耗费的时间关系图。

## 3　实验分析

图 3 为实验网络拓扑图,该网络共有 3 个网段。主机 0 为所在网段为 0 的攻击者;主机 1 为在网段为 1 隔离区的 Web 服务器。主机 2 为内部网络使用的 FTP 服务器;主机 3 为数据库服务器,向 Web 服务器提供数据访问;主机 4 为普通用户终端。主机 2、主机 3、主机 4 都位于网段号为 2 内部网络。

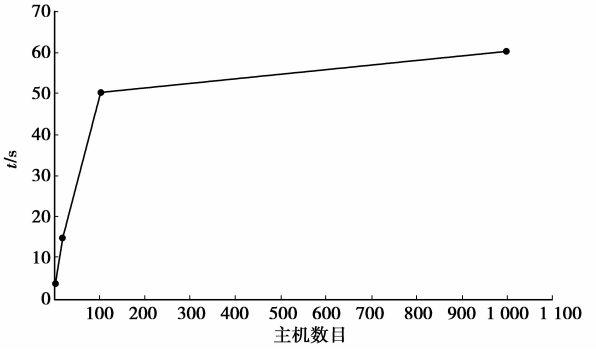


图 2　攻击图生成时间对比曲线

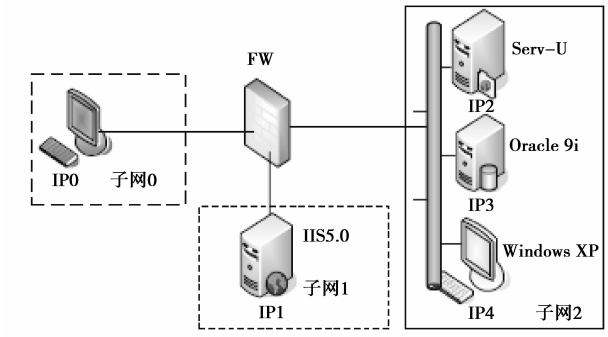


图 3　实验网络拓扑

主机 1 提供 Web 访问服务,服务端口是 80,此服务存在的漏洞为远程缓冲区溢出漏洞。主机 2 为 FTP 服务器,提供文件下载服务,存在的漏洞为一个远程缓冲区溢出漏洞。主机 3 为数据库服务器,服务端口为 1521,存在的漏洞为一个远程缓冲区溢出漏洞。主机 4 为客户机,存在的两个漏洞,一个是远程的信息泄露漏洞,另一个为本地缓冲区溢出漏洞(表 1)。

为了网络的安全,防止外来黑客的入侵,防火墙都是按照严格的规则进行配置的,内部网络中只有主机 4 可以访问 web 服务器主机 1,主机 1 只能访问数据库服务器,而外部网络的主机只能访问主机 1,内部网络不能访问。具体的访问规则如表 2 所示。

表 1　为实验室主机配置信息

| HD(主机 IP 地址) | 网段标识 | SC(主机提供的服务) | CVE(漏洞编号) |
|---|---|---|---|
| 192.128.0.1 | 0 | — | — |
| 192.128.1.1 | 1 | HTTP | 8 116 |
| 192.128.2.1 | 2 | FTP | 4 983 |
| 192.128.2.2 | 2 | TNS | 4 845 |
| 192.128.2.3 | 2 | MSRPC | (8 523,3 770) |

表 2　防火墙规则配置信息

| 源主机 | 目标主机 | PL(协议) | PT(端口) |
|---|---|---|---|
| 主机 0 | 主机 1 | HTTP | 80 |
| 主机 1 | 主机 3 | TCP | 1 521 |
| 主机 4 | 主机 1 | Any | Any |

应用广度搜索的攻击图生成算法最后生成的攻击图如图 4(a)所示,而未采广度搜索的生成算法得到的攻击图如图 4(b)所示。图 4(b)未采用广度搜索的生成算法得到的攻击图,形成了许多虚线表示的攻击路径没有价值,而且这样的攻击路径多数会形成环,比较复杂,规模明显比左边的图大。两种方法比较得出,广度搜索的攻击图生成算法可以构建出在一定攻击步数之内所达到到的所有攻击路径,从而减小攻击图的规模。

## 4 结 论

攻击图生成算法是自动构建攻击图的关键,算法的好坏直接决定了攻击图的生成效率和准确性,本文采用基于攻击模式的广度搜索攻击图生成方法,算法适用大型网络规模环境下构建攻击图,同时大大降低了所生成的攻击图的复杂程度,此文的研究具有非常重要的意义。

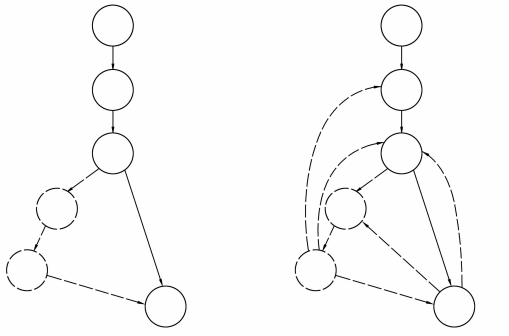


图4 两种方法生成的攻击图

**参考文献:**

[1] 赵芳芳,陈秀真,李建华. 基于权限提升的网络攻击图生成方法[J]. 计算机工程,2008,34(23):158-160

[2] 荷大鹏,周渊,杨武,等用于评估网络整体安全性的攻击图生成方法[J]. 通信学报,2009,30(3):1-5

[3] 张静,陈新岗,向险峰. 自动化技术在评审系统中的应用[J]. 四川兵工学报,2012(5):100-102

[4] SWILER L P,PHILLIPS C. A Graph-based System for Netwodc Vulnerability Analysis Report[C]//Proc. of ACM Workshop on New Security Paradigms. [S.1.]:ACM Pmss,2008

[5] AMMANN P,WIJESEKERA D,KAUSHIK S. Scalahle Cmaph-based NetworkVulnerability Analysis[C]//Proc,of ACM Confen:nce on Computer and Communications Security. [S. L]:ACM Press,2002:217-224

[6] KYLE I,RICHARD L. KEITH P. Practical Attack Graph Generation for Network Defense[C]//Proc. ofAnnual Computer Security Applications Conference. Miami Beach,USA:[s. n.],2006:121- 130

[7] INGOLS K,LIPPMANN R,PIWOWARSKI K. Practical Attack Graph Generation for Network Defense[J]. Computer Security Applications Conference,2006:121-130

# Attack Graph Generation Algorithm Based on Attack Mode Breadth Search

**WU Shu-yu, LI Bo**

(School of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400050, China)

**Abstract**: When network attacker once attacks, he or she usually hopes that the aggressive behavior can be harmful to the maximum extent, based on the premises, in accordance with the breadth-first search strategies and attribute attack graph model, the breadth search attack graph generation algorithm based on attack mode is forwarded, the algorithm can quickly generate the attack graph and the scale is significantly reduced, finally, the performance of the algorithm is analyzed and experimental analysis for it is conducted.

**Key words**: breadth of the search; attack graph; network security

责任编辑:代小红