

一种高效的攻击图生成方法研究

马俊春^{1,2}, 孙继银¹, 王勇军², 李琳琳¹

(1 第二炮兵工程学院, 陕西 西安 710025; 2 国防科技大学 计算机学院, 湖南 长沙 410073)

摘 要: 提出了一种适用于大规模复杂网络系统的攻击图生成算法, 从主机间可达性、安全防护系统、主机系统和网络服务四个层面对目标网络进行建模, 提出了主机间可达性参数的自动获取技术, 从而有效支持了大规模目标网络建模的自动化, 通过实验分析证明, 本算法能够适合全面分析网络安全性和攻击者可能采取的行为方式。

关键词: 大规模复杂网络; 主机间可达性; 安全防护系统; 主机攻击图; 正向 BFS 搜索策略

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2011)04-0013-05

An Effective Method of Generating Attack Graphs

MA Jun-chun^{1,2}, SUN Ji-yin¹, WANG Yong-jun², LI Lin-lin¹

(1 The Second Artillery Engineering Institute, Xi'an 710025, China;

2 School of Computer Science, NUDT, Changsha 410073, China)

Abstract: This paper proposes a kind of attack graph generation algorithm for large-scale complex network system. Model the target network in four levels: hosts' accessibility, security systems, host systems and network services, and propose an automatic gain technology for hosts' accessibility parameters. This algorithm supports effectively the modeling automatically of large-scale target network. From the experiment results we can see, this algorithm can satisfy analyzing network security and the action of attacker roundly.

Key words: large-scale network; hosts' accessibility; security system; hosts' attack graph; forward BFS search strategy

1 引言

攻击图是一种通过综合漏洞、攻击目标、主机和网络连接关系等因素描述网络安全状态的表示方法, 它从攻击者的角度枚举了所有可能的攻击路径, 以此用来帮助用户直观地理解目标网络内各个脆弱点之间的关系和由此产生的潜在威胁。针对大规模的复杂目标网络, 传统的渗透测试过分依赖于测试人员的能力, 而且测试过程中难以控制^[1], 而攻击图能够系统地分析出可能出现的组合攻击, 从而可以为渗透测试提供指导。

攻击图的生成方法经历了从手工分析到自动分析, 从分析小型网络到分析大规模网络的发展过程。文献[2]首次提出了攻击图模型, 虽然该方法是手工完成的, 但为后来的研究者对攻击图的自动产生、自

动分析奠定了坚实的基础。文献[3]基于 EDG 模型开发出了 TVA 系统, 文献[4]提出了基于 Prolog 逻辑的多脆弱性建模方法——MulVAL。攻击图模型方法存在的主要问题是随着网络系统规模的增大, 攻击图算法的状态空间成指数级增长, 从而带来状态空间爆炸问题。当网络节点数目较多时, 使得搜索所有网络攻击路径的工作变得非常困难, 为了解决此问题, 文献[5]开发了 NetSPA 系统。在国内, 文献[6]提出基于权限提升的网络攻击图生成方法, 文献[7]提出基于精简状态空间的攻击图生成算法等。

2 基于攻击模式的攻击图生成方法

2.1 目标网络建模

从网络服务、主机系统、安全防护系统和主机间可达性四个层面对目标网络进行建模。

收稿日期: 2010-06-10; **修回日期:** 2010-09-01

基金项目: 国家“八六三”计划项目(2009AA01Z432)

• 网络服务用四元组 $\langle \text{host}, \text{service}, \text{protocol}, \text{port} \rangle$ 表示, 其中 host 表示主机的 IP 地址, service 表示主机提供的服务, protocol 和 port 为服务 service 所用的协议和端口。

• 主机系统的建模主要描述主机的漏洞信息, 用三元组 $\langle \text{host}, \text{servicename}, \text{cveid} \rangle$ 表示, 其中 host 表示主机的 IP 地址, servicename 表示主机提供的服务名称, cveid 表示主机上存在的漏洞编号。

• 由于目标网络中主机间的可达性与防火墙规则有关, 因此本文对防火墙访问控制规则进行建模, 用四元组 $\langle \text{host1}, \text{host2}, \text{protocol}, \text{port} \rangle$ 表示, 即防火墙允许主机 host1 到主机 host2 的协议为 protocol, 端口为 port 的报文。

• 主机间可达性建模主要描述攻击者的初始能力和目标网络系统中主机间的可达性。

攻击者的初始能力用二元组 $\langle \text{host}, \text{privilege} \rangle$ 表示, 即攻击者在主机 host 上, 拥有 privilege 的权限。

除防火墙过滤规则发生变化影响主机间的可达性外, 主机间的可达性一般不会发生变化, 因此可以仿照网桥的自主学习功能, 对主机间的可达性进行存储, 从而有效实现主机间可达性的自动获取, 提高攻击图的生成效率。

大规模复杂网络一般由多个子网构成, 每个子网内的主机都是网内可达的, 每个子网的管理员需要将与该子网内主机相关的防火墙过滤规则进行输入。通过将防火墙过滤规则与各子网内 Nessus 扫描器的扫描结果进行信息融合, 就可以得到每个子网内主机的可达性以及开放的端口信息。

2.2 基于 BFS 的正向攻击图生成算法及其实现

本文依据 Ammann 提出的攻击者能力“单调性假设”, 提出了基于 BFS 的正向攻击图生成算法。

算法的实现分为两个步骤: 首先根据攻击者的初始条件, 采用广度优先搜索算法, 由起始攻击点出发, 分析其可达主机的可攻击性, 将可攻击的主机及其端口记录在队列 BFSQueue-attackhost 和 BFSQueue-attack 中; 然后根据队列 BFSQueue-attackhost 和 BFSQueue-attack 中的信息, 生成攻击路径。算法流程图如图 1~图 3 所示。

攻击图生成算法说明如下: 队列 BFSQueue-start 存放待分析的攻击对集合, 即存放攻击者的起始位置和目标位置的集合, 存放格式为 (起始攻击点: 目标攻击点)。第一步, 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,

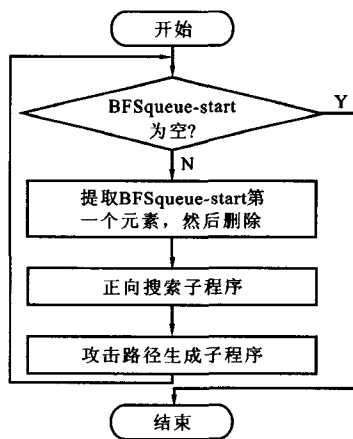


图 1 攻击图生成算法流程图

否则提取 BFSQueue-start 的第一个元素进行分析, 同时删除此元素, 依次调用正向搜索子程序和攻击路径生成子程序; 第二步, 循环执行第一步, 直至 BFSQueue-start 为空, 即分析了所有的攻击对。

正向搜索算法子程序实现攻击路径的正向搜索。在正向搜索具体的实现过程中, 本文定义了三个队列: BFSQueue-attackhost、BFSQueue-attack 和 BFSQueue。其中 BFSQueue-attackhost 以 (攻击点主机: 目标攻击点) 的格式存放攻击成功的主机对集合, 该队列反映从起始攻击点到目标攻击点的搜索路径, 由于主机可以开放多个端口, 可以同时存在多个攻击, 因此队列中有重复元素; BFSQueue-attack 以 (攻击点主机: 攻击目标主机: 目标主机端口) 的格式存放攻击成功的主机对集合, 由于该队列反映攻击点主机通过哪些端口可以攻下攻击目标主机, 因此该队列中没有重复的元素; BFSQueue 是一个动态队列, 存放起始攻击点的所有可达主机。

一方面由于攻击者不会采用很复杂的攻击手段, 就是说攻击者不会以太多的主机为跳板进行攻击, 另一方面有的攻击路径根本不会出现攻击目标, 对此攻击路径进行更深层次的搜索没有意义, 因此在正向搜索算法的实现过程中, 采用限制搜索深度的策略, 此搜索深度可以由用户设定。

攻击路径生成算法子程序实现对正向搜索结果进行读取、解码, 生成攻击路径。本文定义了间隔元素和终端元素: 所谓间隔元素, 是指由于 BFSQueue-attackhost 中有重复的元素, 即不同的搜索深度有可能具有相同的攻击路径, 因此不同搜索深度的元素之间需用 (IP: IP) 隔开, (IP: IP) 则称为间隔元素; 所谓终端元素, 是指假设 IP1 和 IP2 之间存在攻击路径, 即 (IP1: IP2) 满足, IP2 为最终攻击目标, 则称该元素为终端元素。本算法结合间隔元素和终端元

素,先不考虑端口情况,从 BFSQueue-attackhost 的队列尾开始,分析 BFSQueue-attackhost 中主机的攻击路径,然后结合 BFSQueue-attack 中主机的端口

信息,逐一写出攻击路径。

图4所示为核心算法程序。

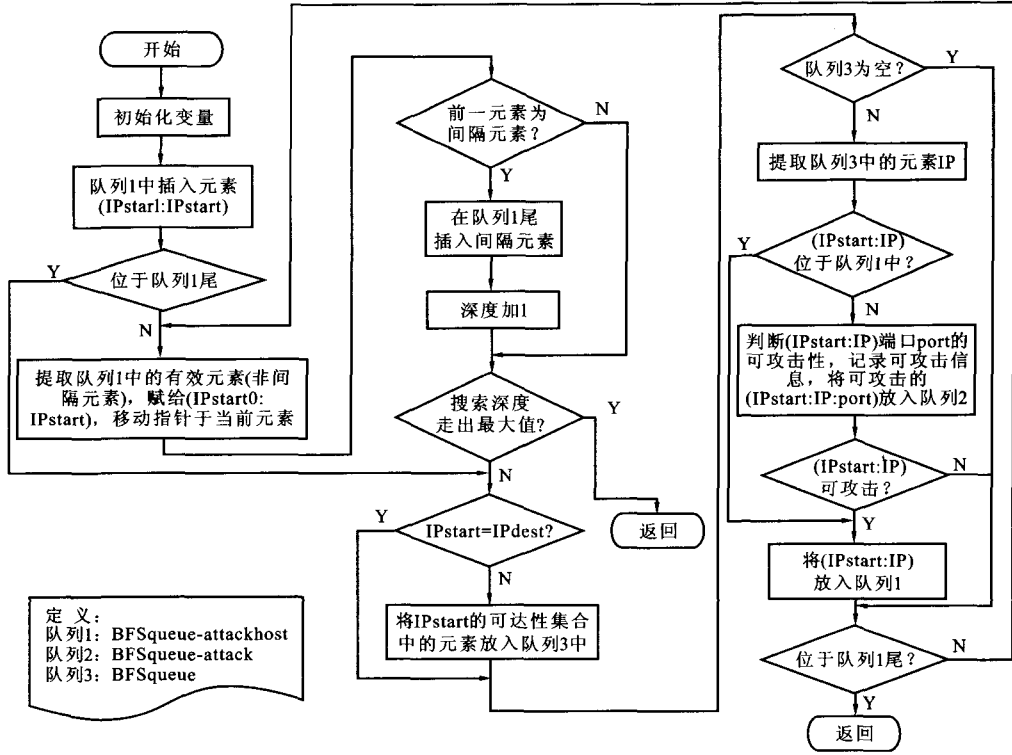


图2 正向搜索算法实现流程图

2.3 算法复杂度分析

2.3.1 时间复杂度

设攻击场景中主机的数目为 $|H|$, 每台主机开放的端口数目为 $|N_{port}|$, 攻击模式的数目为 $|N_{exploit}|$ 。

由于该算法遵循 Ammann 提出的单调性原则, 因此最坏的情况下, 每层的节点可达性数目要比其父节点数目小 1。攻击者的初始位置为广度优先搜索的第一层, 其可达性数目最大为 $H-1$, 第二层的最大可达性数目为 $(H-1)(H-2)$, 同理第三层为 $(H-1)(H-2)(H-3)$, 以此类推。根据图 4 中的核心算法, 设算法的搜索深度为 L , 由于目前常用的端口数目就十几个, 通过对网上公布的脆弱性信息进行深入分析, 总结出了 20 种攻击模式, 因此不难看出该算法的时间复杂度为

$$|N_{port}| \cdot |N_{exploit}| \cdot ((H-1) + (H-1)(H-2) + \dots + (H-1)(H-2) \dots (H-L+1))$$

即 $O(H^{L-1})$ 。

2.3.2 空间复杂度

针对主机的可达性建模, 将主机间的可达性用二维数组 $\langle$ 网内可达性, 网间可达性 $\rangle$ 表示, 在具

体的实现过程中, 当首次用到某子网内主机(设为 A) 的可达性时, 首先查询数据库得到 A 的网内可达性, 然后将该子网内的所有主机和 A 的网内可达性进行存储, 如果需要该子网内另一主机(设为 D) 的网内可达性时, 因为主机 A 与 D 处在同一子网内, 所以 D 的可达性与 A 的可达性相同, 从而不需要将 D 的网内可达性进行存储, 这样就大大减小了算法的空间复杂度, 从而使该算法能够有效适用于大规模复杂目标网络系统。

由于在目标网络建模中, 主机间的可达性用二维数组表示, 这样目标网络中主机间的连接关系数量大幅度减小, 从而减小了该算法的空间复杂度和时间复杂度, 图 5 给出了在算法复杂度实验中, 网络中主机的数目和生成攻击图所耗费的时间关系图。

3 应用实例

本文搭建了如下网络环境: 实验网络的拓扑环境如图 6 所示, 该目标网络由 10 台主机(编号为 0—9)、一台服务器(该服务器开放了两种服务: Ftp 服务和 Email 服务)和两个防火墙组成。服务器和外部主机之间设置了防火墙, 因此服务器所提供的两

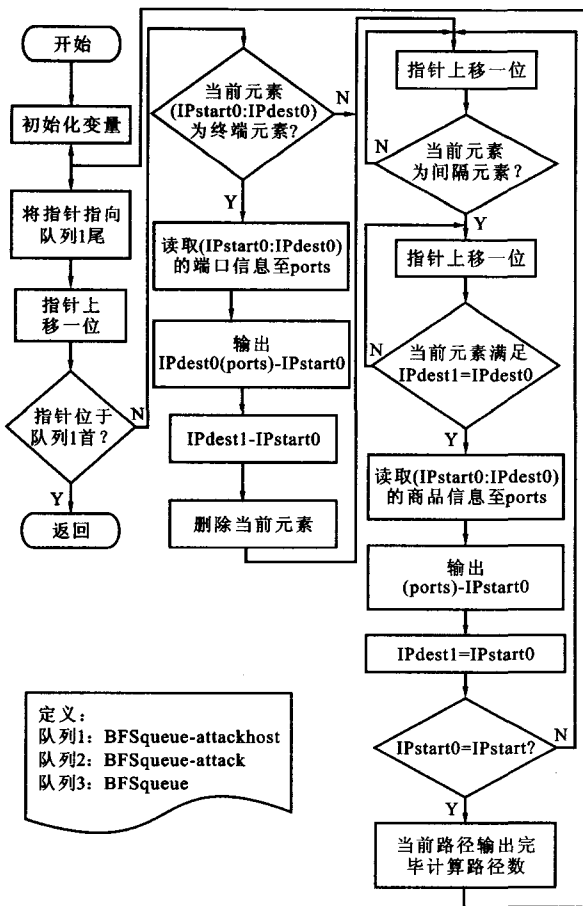


图 3 攻击路径生成实现流程图

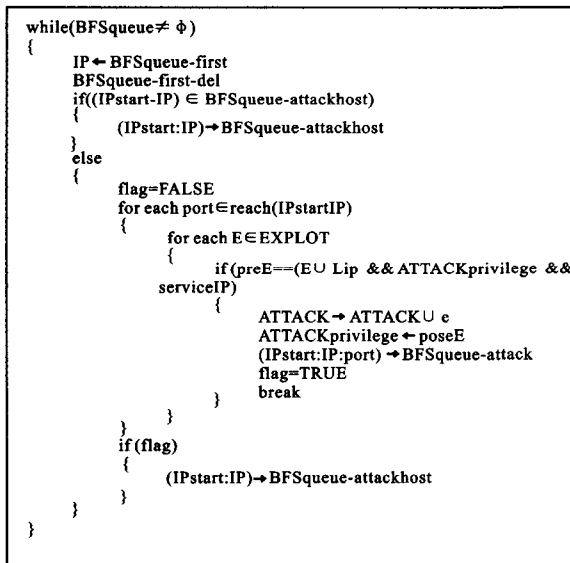


图 4 核心算法

种服务允许不同的主机访问,其中防火墙 1 只允许局域网 1 中的主机以 root 权限访问 Ftp 服务,防火墙 2 允许局域网 2 中的主机以 user 或 root 权限访问 email 服务,攻击者可以通过 Internet 与内部网的主机相连.局域网 1 和局域网 2 中的主机之间可

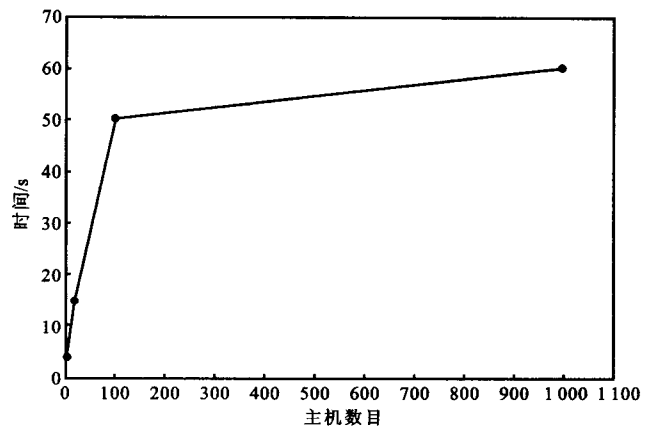


图 5 攻击图生成时间对比曲线

以互相通信,攻击者的目标是获得服务器的 root 访问权限.

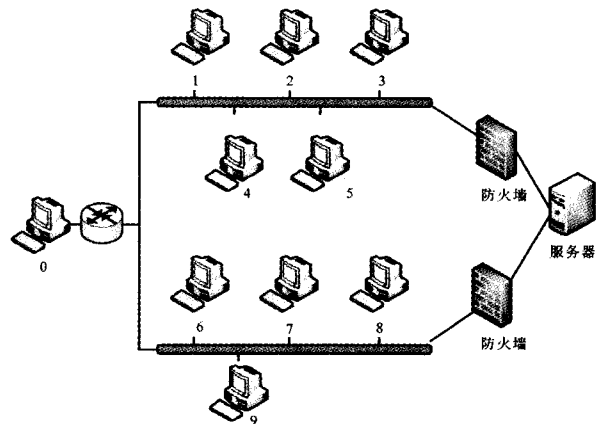


图 6 实验网络拓扑

服务器开放的 Ftp 服务存在脆弱点 CVE—2004—0148,可被攻击者利用获得该主机的 root 权限,同时服务器开放的 Email 服务存在脆弱点 CVE—2004—0159,可被攻击者利用获得 user 权限.局域网 1 中主机的操作系统存在软件错误型脆弱性 CVE—2005—2558,该脆弱性可被攻击者实施本地内存溢出型攻击获得主机的 root 访问权限,局域网 2 中的主机,一方面其操作系统存在脆弱性 CVE—2005—2558,可被利用获得主机的 root 权限,另一方面其软件存在错误性脆弱性 CVE—2002—0640,可被攻击者发起内存远程溢出型攻击获得主机的 user 访问权限.

攻击者可以通过局域网 1 中主机的漏洞获得局域网 1 中主机的权限,然后通过服务器的 Ftp 服务漏洞达到攻击目标,也可以通过局域网 2 中主机的漏洞获得主机的 user 或 root 权限,然后通过服务器的 email 服务漏洞获得服务器的 root 权限,从而达到攻击目标.

4 结束语

本文通过对模型参数的自动获取技术进行深入研究,实现了主机间可达性、安全防护系统、主机系统和网络服务四个层面的目标网络自动建模。同时,由于状态枚举攻击图存在随着主机数增加而呈指数增长的缺点,因此本文根据预定义的规则进行聚合,生成结点和边数与网络中主机的增加成线性关系的主机攻击图。以上两方面使得本文提出的算法具有较高的效率,能够适用于大规模复杂的目标网络系统。

参考文献:

- [1] 程玲. MANET入侵检测技术的研究[J]. 微电子学与计算机, 2010, 27(6): 57-59.
- [2] 孙强. 基于定量安全风险评估模型的网络安全管理平台[J]. 微电子学与计算机, 2010, 27(5): 70-73.
- [3] Swiler L P, Phillips C, Ellis D, et al. Computer-attack graph generation tool[C]//Proceedings DARPA Information Survivability Conference and Exposition (DISCEX II'01). Anaheim, California: IEEE Computer Society, 2001: 307-321.

- [4] Swiler L P, Phillips C, Gaylor T. A graph-based network-vulnerability analysis system, SAND97-3010/1[R]. New Mexico and Livermore, California: Sandia National Laboratories, Albuquerque, 1998.
- [5] Sushil Jajodia, Steven Noel. Topological vulnerability analysis, center for secure information systems[J]. Computer Science, 2010, 46(4): 139-154.
- [6] Xinming Ou, Wayne F Boyer. A scalable approach to attack graph generation[C]// Proceedings of the 13th ACM conference on Computer and communications security, USA: ACM, 2006: 336-345.
- [7] Xinming Ou. A logic-programming approach to network security analysis[D]. Princeton: Princeton University, 2005.

作者简介:

马俊春 女, (1983-), 博士生. 研究方向为网络安全。

王勇军 男, (1971-), 博导, 教授. 研究方向为高性能网络隔离技术、网络脆弱性分析技术、网络安全态势分析评估技术、网络生存性技术等。

孙继银 男, (1952-), 博导, 教授, CCF 会员. 研究方向为指挥自动化工程, 计算机应用技术。

(上接第12页)

参考文献:

- [1] 禹旺兵, 彭良玉, 禹恒州. 基于小波分析和神经网络的模拟电路故障诊断方法[J]. 微电子学与计算机, 2007, 24(7): 43-46.
- [2] 朱大奇, 于盛林. 基于D-S理论的数据融合算法及其在电路故障诊断用的应用[J]. 电子学报, 2002, 30(2): 221-223.
- [3] 彭敏放, 何怡刚, 王耀南. 基于神经网络与证据理论的模拟电路故障诊断[J]. 电路与系统学报, 2005, 10(1): 35-39.
- [4] 彭敏放, 何怡刚, 王耀南, 等. 模拟电路的融合智能故障诊断[J]. 中国电机工程学报, 2006, 26(3): 19-24.
- [5] 刘美华, 彭良玉. 基于小波分析和信息融合技术的故障诊断[J]. 微电子学与计算机, 2009, 26(1): 166-168.
- [6] 胡清华, 于达仁, 谢宗霞. 基于邻域粒化和粗糙逼近的数

值属性约简[J]. 软件学报, 2008, 19(3): 640-649.

- [7] 曾庆双. 基于邻域粒化和遗传算法的数值属性约简方法[J]. 自动化博览, 2009(8): 69-74.

- [8] 廖薇, 许春冬, 刘锦高. 基于神经网络的模拟电路故障诊断研究[J]. 微电子学与计算机, 2010, 27(5): 125-128.

- [9] 颜根廷, 李传江, 马广富. 支持向量分类器的模糊积分集成方法[J]. 哈尔滨工业大学学报, 2008, 40(7): 1017-1020.

作者简介:

马超 男, (1983-), 博士研究生. 研究方向为防空导弹模拟电路智能故障诊断方法。

陈西宏 男, (1961-), 博士, 教授, 博士生导师. 研究方向为防空导弹武器系统信息技术与智能故障诊断方法等。