一种基于攻击树的网络攻击系统

周　伟[1]　王丽娜[2]　张焕国[2]
[1](华中师范大学计算机科学系,武汉　430079)
[2](武汉大学计算机学院,武汉　430072)

摘　要　随着计算机安全技术的高速发展,黑客的攻击已经受到了越来越多的限制。如何突破安全技术的封锁,建立一种全新的黑客攻击技术与体制已经成为当前黑客的主要研究方向。文章介绍了攻击树模型,提出了一种基于攻击树的网络攻击系统,它可以根据目标的实际情况制定出攻击策略,实施攻击。该系统使得攻击有自动性和智能性,大大提高了攻击成功的可能性。

关键词　攻击树　攻击策略　攻击模型　自动

文章编号　1002-8331-(2006)24-0125-04　　文献标识码　A　　中图分类号　TP393.08

A Network Attack System Based on Attack Tree

Zhou Wei[1]　Wang Li'na[2]　Zhang Huanguo[2]
[1](Department of Computer Science of CCNU, Wuhan 430079)
[2](College of Computer of Wuhan University, Wuhan 430072)

Abstract: As the high-speed development of computer security technology, the attack behaviors of hackers have been limited more and more.How to break through the blockage of security technology and establish a new hacker attack technique or system has been the key direction of today's research.This paper introduces the attack tree model, presents a network attack system based on attack tree, which can make attack scenario base on the target's practice and do it. This model system makes the attack has automaticity and intelligence, which enhances the possibility of success attack.

Keywords: attack tree, attack scenario, attack model, automation

1　引言

随着计算机网络发展,尤其是 Internet 的发展,网络攻击活动出现的越来越频繁。其中大部分的网络攻击活动都是由一些被称为脚本小孩(script kids)利用某些攻击工具发起的。一般来说,虽然这些网络攻击工具只具备某一项特殊攻击的技能,针对性很强,他们没有攻击战术分析能力,不能像人一样制定出合适的攻击策略。基于这些攻击工具的不足,本文提出了一种基于攻击树的网络攻击系统,它可以根据目标的实际情况制定出攻击策略,实施自动攻击。

2　攻击树模型

2.1　基本概念

Bruce Schneier 在近年首次提出了这个概念。他的原本目的是希望攻击树提供一种描述安全系统的方法,允许对系统的安全性进行精确的计算,比较不同的安全系统,并做出一套比较完善的安全解决方案。

在一棵攻击树的树形结构中,根节点代表了总目标,各个分支代表达到总目标的方法。通过对各个节点的赋值,就可以依据此树形结构做一些基本的计算用来描述针对总目标的各种攻击方式,因此将其应用到攻击的领域仍是可行的。根据一棵给定的攻击树,我们可以从树的某一个叶节点开始找到一条能够实现我们攻击目的同时开销又比较小的路径。

可以使用攻击树来表示攻击,树的根结点表示最终的入侵目标,节点则表示取得上级节点入侵目标的方法,节点之间的关系可能是"或","与","顺序与"三种关系之一,叶结点可以在不同的环境中被具体事件实例化,如图 1 所示。

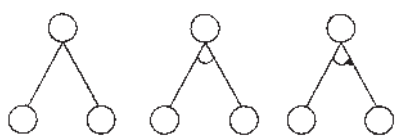

图 1　攻击树的三种节点

"或"关系表示任一子结点目标的取得都可以导致父结点目标的取得;"与"关系表示所有子结点目标的取得才可以导致父结点目标的取得;"顺序与"关系表示所有子结点目标的按顺序取得才可以导致父结点目标的取得。攻击树之间可以做加法运算,如图 2 所示。

2.2　用攻击树具体分析 IP-Spoofing 攻击

网络当中的攻击一般都是针对 TCP/IP 的不完善之处或者系统漏洞发起的,下面我们使用攻击树模型来分析一个典型的 IP-Spoofing 攻击。

当一个主机 A 要使用 TCP 访问主机 B 提供的资源时,它们之间要通过三次握手建立连接。入侵者要冒充主机 A 与主

基金项目:国家自然科学基金资助项目(编号:90104005,66973034)
作者简介:周伟(1980-),男,助教,主要研究领域为计算机网络安全。王丽娜(1964-),女,博士,副教授,主要研究领域为计算机网络安全。张焕国(1946-),男,教授,博士导师,主要研究领域为密码学、容错计算。

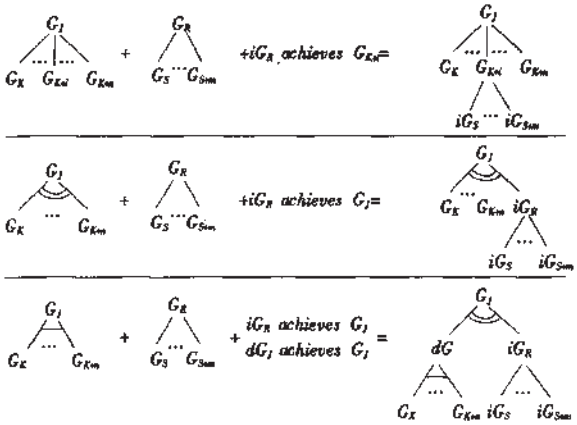

图 2　攻击树加法

机 B 进行连接和入侵，可以通过以下步骤。

(1) 首先要使主机 A 瘫痪，不能回应主机 B 的 SYN-ACK 包，这可以通过一些 DoS 攻击(如 Land, SYN-FLOODING, DDoS 等)使得主机 A 不能工作。

(2) 猜测主机 B 的连接初始值 y，发送 ACK(Y+1)来冒充主机 A 与主机 B 的 513 端口(RLOGIN)建立连接，当前的一些 IP-Spoofing 工具使这个任务更简单了。

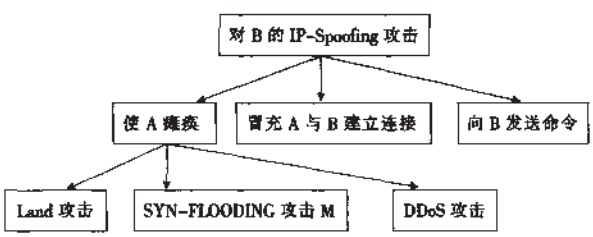

图 3　IP-Spoofing 的攻击树

```
IP-Spoofing 攻击
{
TAND 使 A 瘫痪
  {
   OR Land,
      SYN-FLOODING,
      DDoS
  },
   来自 A 的连接请求,
      来自 A 的命令
}
```

如果攻击的最终目标是获取 root 权限，那么这棵树只是整个攻击模型的一小部分。根据一个完整的攻击树模型，并给树的每个节点赋一个权值，就可以从每个叶子开始寻找一条由底至顶的并且所经过各节点权值之和最小的路径，这将为攻击方案提供有一定价值的参考数据。

2.3　基于攻击树的形式化描述

使用攻击树可以很好地表示大规模的网络入侵，Tidwell 在此基础上定义一个攻击模型语言(Attack Specification Language BNF)，每个攻击模型包含属性(properties)、前提(preconditions)、子目标(subgoal)、后果(postcondition)四大部分。属性包含 description(攻击描述)、CVElink(CVE 相应编号)、version(版本号)等描述信息。前提指要完成攻击所需的系统环境与配置，前提之间的关系可以是“与”或者“或”。子目标表示完成该攻击必须先完成的子目标，对应攻击树上它的子结点，子目标之间的关系只有“与”关系。后果指示系统环境的改变。基于这个语言就可以对攻击进行描述，如果某攻击的子目标与前提都得到满足(被实例化)，则判断该攻击为真。

下面是缓冲区溢出的攻击模型语言：

Buffer Overflow Attack Pattern:

Goal: Exploit buffer overflow vulnerability to perform malicious function on target system

CVELink: CVE-1999-083

Precondition: Attack can execute certain programs on target system

Attack(subgoals):

AND 1.Identify executable programe on target system susceptible to buffer overflow vulnerability

2.Identify code that will perform malicious function when it executes with programe privilege

3.Construct input value that will force code to be in program address space

4.Execute program in a way that makes it jump to address at which code resides。

Postcondition: Target system performs malicious function

一个攻击目标的完成依赖于若干个子目标的完成，子目标之间的关系可以是“或”、“与”、“顺序与”三种关系。一个攻击目标的标识符是一个以字母开头的字母和数字的字符串。由攻击语言定义的攻击称为攻击模式，多个攻击模式的集合称为攻击模式库。

3　基于攻击树的网络攻击系统

3.1　系统功能描述

利用动态的攻击树模型，我们设计实现了一个网络攻击系统 NAS(Network Attack System)。

在 NAS 中我们建立通用的攻击模板库和攻击模式库。当需要进行攻击时，NAS 进行以下工作：

(1) 从攻击模板库中找出一种攻击模板。

(2) 根据扫描得到的目标系统的相关信息从攻击模式库中选取相应的攻击树与攻击模板组合成为一棵完整的攻击树，并抽取一棵权值最小的子树作为最终的攻击树实施攻击。

(3) 根据攻击树和攻击工具集组成攻击策略，实施攻击。

NAS 基本满足了以下的功能基本要求：

(1) 智能性

NAS 可以根据目标主机的基本信息如开放的端口、操作系统类型、已知的漏洞等智能地选择攻击树。

(2) 可扩展性

因为存在成千上万种不同的攻击方法，而且还不断有新攻击方法出现。所以必须将攻击策略和攻击方法分开，保证出现新的攻击方法出现时可以无需对系统进行改动就可以使用。通过向 NAS 的攻击模式库中添加新的攻击树就可以方便地实现扩充。

(3) 自动性

NAS 可以自动完成攻击的全部过程，包括扫描、选择攻击策略、攻击实施、隐藏痕迹、留下后门等。

(4)层次分明

NAS将攻击中的攻击策略、攻击方法和具体的攻击工具相分离,使攻击的层次更加分明,更加容易管理。它们之间是松散耦合的关系,可以很方便地对其中的某一部分进行扩充修改,而不会影响其它部分。

3.2 系统结构

NAS各模块的关系如图4所示。

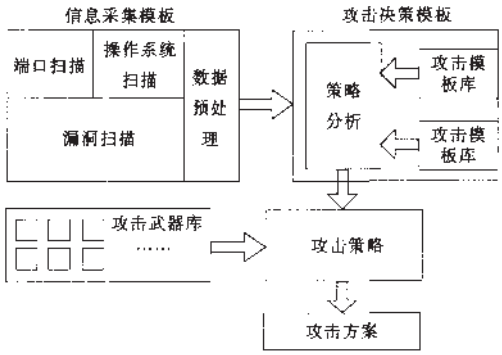

图4 NAS基本框图

NAS由三个模块组成,信息采集模块、攻击决策模块和攻击武器库。信息采集模块部分包含端口扫描、远程操作系统扫描、漏洞扫描和数据预处理。信息采集模块将采集的关于目标系统的基本信息如开放的端口、存在的漏洞等通过数据预处理形成一种结构化的数据送给攻击决策模块。攻击决策模块采用动态攻击树的方法构造一棵攻击树,形成攻击策略,攻击武器库中是各种各样的攻击程序。根据攻击策略在攻击武器库中选取相应的攻击程序,形成最后的攻击方案。

3.2.1 信息采集模块

该模块的主要功能是通过远程操作系统探测器、端口扫描器和漏洞扫描器收集目标系统的基本信息,如操作系统的类型、开放的端口和存在的知名漏洞等。该模块对于保证攻击准确性至关重要。信息采集模块将采集到的信息和这次攻击的目的,通过预处理后形成一组属性(Propertiy),发送给攻击决策模块。

Attack Goal:攻击的目的,如获得管理员权限、添加一个用户、清除日志等;

OS:目标系统的操作系统类型及版本信息;

Port:目标系统开放的端口;

CVELink:CVE1;CVE2…CVEn,目标系统存在的漏洞的CVE编号。

3.2.2 攻击决策模块

攻击决策模块是NAS的核心模块,它的主要功能是根据信息采集模块收集到的信息计算出最合适的攻击方法,包括使用哪些攻击,各种攻击方法之间的同步等。该模块包含一个攻击模板库和一个攻击模式库,攻击模板库是由各种攻击模板组成的,攻击模式库由各种攻击模式组成。攻击模板和攻击模式都由攻击树来描述。

攻击模板采用的是比较粗的线条来刻画攻击的,它只描述攻击的途径,而不描述攻击的具体细节,如进行密码攻击的获得目标系统的访问权的攻击模板,它只包含三个子目标,一个是获得用户名的文件;一个是获得用户密码文件;另一个是相应的破解工具。至于如何获得用户名文件如何获得用户密码文件并不说明。用来描述攻击模板的攻击树是一种比较特殊的树,它只有两层。根结点是攻击的目的,叶子节点是攻击的子目标,它们的关系可以是或、与和顺序与。举例如下:

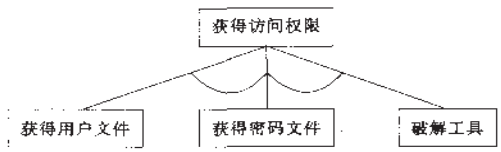

图5 举例1

攻击模式用来描述比较具体的攻击,它通常是和具体的操作系统,特定的漏洞相关的。例如下面就是专门针对Windows2000 IIS UNICODE漏洞的攻击模式,它的根结点是在目标系统上获得一个具有系统或者管理员权限的SHELL。举例如下:

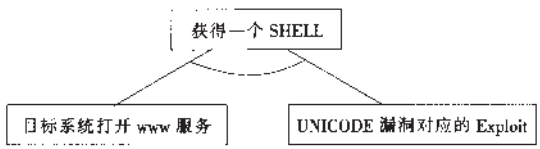

图6 举例2

动态生成攻击树的算法如下:

(1)根据信息采集模块收集的信息(主要是目标操作系统的类型、版本和开放的端口)从攻击模板库中找出一个合适的模板。

(2)如果没找到,提示没有合适的攻击模板并退出。

(3)如果找到一个合适的模板,进入(4)。

(4)扩展该模板成为一棵完整的攻击树,如果未完成进入(5),如果完成进入(6)。

(5)根据信息采集模块收集的目标系统开放的端口、存在的漏洞等信息,结合步骤(3)中选择的攻击模板,在攻击模式库中选择攻击树和步骤(4)中的攻击树进行加法运算,形成新的攻击树。返回(4)。

(6)从这棵完整的攻击树中找出一棵权值(代表攻击的代价)最小的子树,作为最终的攻击树。

(7)根据最终生成的攻击树从攻击武器库中选择相应的攻击程序进行攻击,如果攻击成功,报告攻击成功并退出。如果没有成功,进入(8)。

(8)从完整的攻击树中找一棵权值次小的子树,作为最终的攻击树。如果找到,返回(7)。如果没有找到,报告攻击失败并退出。

其流程如图7如示。

3.2.3 攻击模式库

攻击模式库由各种攻击模式组成,举例如下:

(1)DNS服务器缓冲区溢出漏洞攻击模式

```
attack  bind.ExploitBIND_nxt_Vulnerability
(Service s)
{
property string CVE_ID="CVE-1999-0833";
Multiple Vulnerabilities in BIND";
property string BugTraqID="788";
preconditions
{ s instanceof named_Service &
```

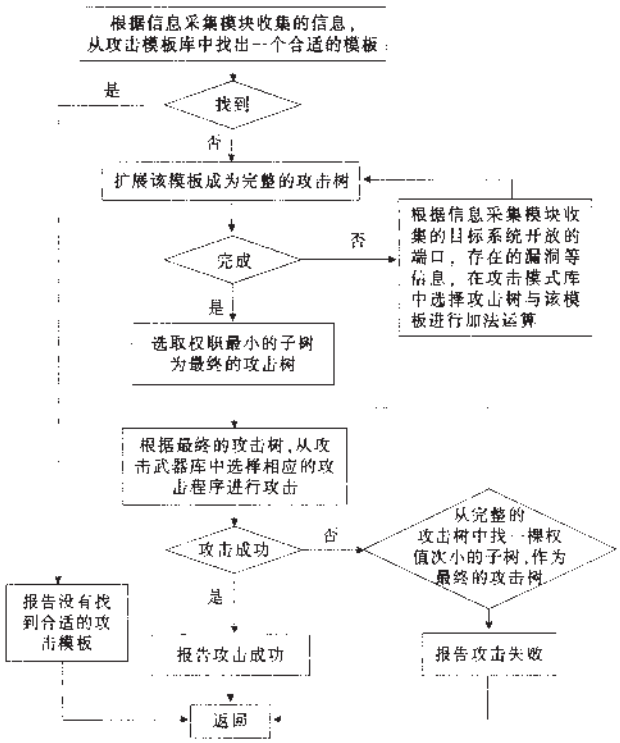

图 7　攻击决策算法

```
s.version >= v8.2 & s.version < v8.2.2
}
postconditions{}
subgoals
{( ConnectToHost( s.host, 53 ))}
}
```

(2) Mysql SQL 攻击模式

```
attack mysql.ExploitMySQL_SELECT_Vulnerabilit
y
(Application a)
{
property string CVE_ID="CVE-MAP-NOMATCH";
property string BugTraqID="2262";
preconditions
{ a instanceof MySQL_Application &
a.version >= v3.22.26 & a.version <= v3.23.9
}
postconditions {}
subgoals
{( ExecuteProgram(a))}
}
```

3.2.4　攻击武器库

攻击武器库由各种类型的攻击程序组成，包含前面讲的拒绝服务攻击、缓冲区溢出类的攻击、欺骗类的攻击、密码攻击和嗅探类的攻击等，它们是攻击的真正实施者。对每种工具按照 CVE 的漏洞进行编号，可以很方便地进行查找，这些工具可以自己编写，也可以用已有的工具。

3.2.5　攻击方案

攻击方案是根据攻击决策模块产生的最终的攻击树，在攻击武器库中选择相应的攻击程序形成的攻击的具体实施过程。例如，某次攻击的目的是获得局域网中某个服务器的共享目录的访问权，该服务器的操作系统为 Windows2000 server，开放的端口为 TCP139。经过策略分析，我们得出的攻击树如图 8 所示。

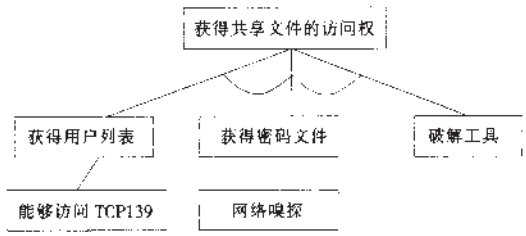

图 8　获取共享文件的访问权的完整攻击树

根据攻击树我们在攻击武器库中选择以下攻击程序：CVE 编号为 CVE-2002-027 的 T-SMB，编号为 CVE-1999-002 的 SnifferPro，编号为 CVE-2000-040 的 LC4。T-SMB 可以获取局域网中某台计算机上的用户名列表，前提是该计算机开放端口 TCP139。SnifferPro 是一种功能强大的网络嗅探工具，它可以监视局域网里的数据流，这里我们用它来获取密码散列(LanHash)值，它的前提是能够访问该局域网。LC4 是破解 Windows2000/NT 密码速度最快的工具，它工作的前提是获取用户名和对应的密码散列值。

攻击方案如下：

(1) 用 T-SMB 获取该服务器的用户列表。

(2) 用 SnifferPro 监听该用户列表中用户的密码散列。

(3) 将该密码散列送入 LC4 进行破解，得出明文口令。

(4) 用用户名/明文口令访问共享文件，攻击完成。

4　结束语

本文介绍了攻击树的基本概念，并在此基础上提出了一种基于攻击树的网络攻击系统。该系统可以根据攻击目的自动完成攻击准备，并根据目标网络的信息智能的选择攻击策略，形成攻击方案实施攻击。自动性和智能性是网络攻击系统的发展方向之一，本文在这方面作了有益的探讨。

(收稿日期：2006 年 3 月)

参考文献

1.Bruce Schneier.Secrets and Lies: Digital Security in a Networked World[M].John Wiley & Sons, 2000

2.Anonymous.Maximum Security[M].Second Edition, Sams, 1998

3.庄朝晖.基于攻击树的多层次入侵检测及其在 Linux 上的原型[D].硕士研究生答辩论文.厦门大学, 2002-05

4.Eric Cole.Hackers Beware[M].New Riders, 2001

5.Saenchai K, Benedicenti L, Paranjape R.The Design of a Secure Agent Platform[C].In: Electrical and Computer Engineering, IEEE CCECE 2002 Canadian Conference on, 2002

6.Komiya T, Ohsida H, Takizawa M.Mobile Agent Model for Distributed Objects Systems[C].In: Object-Oriented Real-Time Distributed Computing, 2002 (ISORC 2002), Proceedings Fifth IEEE International Symposium on, 2002: 62~69

7.Gunter M, Braun T.Internet Service Monitoring with Mobile Agents[J].IEEE Network, 2002; 16(3): 22~29

8.Weiming Shen.Distributed Manufacturing Scheduling using Intelligent Agents[J].IEEE Intelligent Systems, 2002; 17(1): 88~94