攻击行为系统化分析方法*)

严 芬[1,2,3] 黄 皓[1,2]

(南京大学软件新技术国家重点实验室 南京 210093)[1] (南京大学计算机科学与技术系 南京 210093)[2]

(扬州大学工学院计算机科学与工程系 扬州 225009)[3]

摘 要 针对日益严重的攻击行为,通过对大量攻击以及现有攻击分析方法的研究,本文提出了一个系统地分析和描述攻击行为的方法。此方法不仅能够有效地分析和描述攻击的本质特征,还能分析攻击的过程,具有广泛的适用性。文中还讨论和分析了在此基础上对该方案进行裁剪的原则和方法,以增加其适用性。通过诸多攻击实例验证了所给方案的有效性和适用性。

关键词 安全,攻击,攻击过程,裁剪,裁剪规则

Research on Systematically Describing Attacks

YAN Fen[1,2,3] HUANG Hao[1,2]

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)[1]

(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)[2]

(Department of Computer Science and Engineering, Technology Institute, Yangzhou University, Yangzhou 225009)[3]

Abstract To deal with the increasingly serious problem of attack, after researched on many attack and existing attack analyzing methods, a systematical method to analyzing and describing attack is put forward in this paper. This method can not only effectively analyze and describe the essence characteristics of attack, but also can analyze attack process, thus it has extensive applicability. Then, how to tailor the method and the corresponding tailoring rule are talked in order to enhancing the method's applicability. The validity and applicability of this schema are validated via many attack examples.

Keywords Security, Attack, Attack process, Tailoring, Tailoring rule

1 引言

计算机和网络的广泛应用和普及,造成攻击日益增多,安全问题越来越突出。为了尽早地防御攻击的发生,更好地检测攻击的存在,有效地采取措施响应攻击,减少攻击造成或可能造成的危害,首先需要对攻击行为本身进行分析和描述。攻击行为的分析和描述具有深远意义,在密码学与信息安全、计算机网络、操作系统、软件工程、计算机应用技术等研究领域都发挥着重要的作用。攻击的复杂多样性导致很难找到一个有效、通用的方法来分析和描述所有的攻击行为。目前,已有的研究工作或者是侧重于对攻击的概念性介绍[1],或者是针对某一个或者某一类攻击行为的详细分析[2],还有一些则侧重于攻击行为模型分析[3]。总的来讲,现有工作缺乏对攻击行为分析和描述的系统性和通用性。

通过对大量攻击行为的分析和研究,在研究攻击分类和攻击方法[4~11]的基础上,本文提出了一个利用多特征属性来分析攻击行为、具有一定的通用性的攻击行为分析方法,并且提出了对其进行不同程度的裁剪后,可以使该方法具有更强的适用性,能更好地用于分析和描述攻击,且可以描述攻击行为之间存在的关联性。文中的攻击分析和描述方法不仅可以有效地分析和描述攻击的本质特性,还可以分析攻击的过程。

本文第2部分介绍系统化的攻击行为分析方法;第3部

*)国家863高技术研究发展计划"分布式网络监控与预警系统"(2003AA142010)和江苏省高技术研究计划"计算机网络分布式主动防御、监控与预警技术研究"(BG2004030)资助项目。严 芬 博士研究生,主要研究方向为网络与信息安全;黄 皓 博士生导师,主要研究方向为计算机信息系统安全、网络与信息安全。

2 Blakley G. Safeguarding cryptographic key. In:Proc. AFIPS 1979 Natl. Conf., New York,1979. 313~317

3 Asmuth C, Bloom J. A Modular approach to key safegrarding [J]. IEEE Transactions On Information Theory, 1983, 29(2):208~210

4 Karnin E D, Green J W, Hellman M E. On sharing secret system [J]. IEEE Transactions On Information Theory, 1983, 29(1):35~41

5 Wu T C, He W H. A geometric approach for sharing secrets [J]. Computers & Security, 1995, 14(2):135~145

6 Pang Liao-jun, Wang Yu-min. A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing [J]. Applied Mathematics and Computation, 2005, 167(2):840~848

7 Yang Chou-Chen, Chang Ting-Yi, Hwang Min-Shiang. A (t, n) multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2004, 151(2):483~490

8 Benaloh J, Leichter J. Generalized secret sharing and monotone functions [A]. Advance in Cryptology-Crypto'88 [C], Springer-Verlag, Berlin, 1990. 27~35

9 Hwang Ren-Junn, Chang Chin-Chen. An on-line secret sharing scheme for multi-secrets [J]. Computer Communications, 1998, 21(13):1170~1176

10 Wang Shiuh-Jeng. Direct construction of a secret in generalized group-oriented cryptography [J]. Computer Standards and Interfaces, 2004, 26(5):455~460

11 Yuanbo Guo, Jianfeng Ma. An efficient and secure fault-tolerant conference-key distribution scheme [J]. IEEE Transactions on Consumer Electronics, 2004, 50(2):571~575

12 Tan K J, Zhu H W, Gu S J. Cheater identification in (t, n) threshold scheme [J]. Computer Communications, 1999, 22: 762~765

13 Wiedemann D H. Solving sparse linear equations over finite fields [J]. IEEE Transaction on Information Theory, IT-32(1), 1981. 54~62

分说明如何对这种分析方法进行有效的裁剪，增强方法的适用性；最后总结我们的研究工作。

2 系统化的攻击行为分析方法

2.1 相关术语

首先给出文中引入的几个术语及其用途。

攻击过程：用来说明攻击行为的一般过程；复合攻击、子攻击：用来表示不同抽象程度的攻击；攻击粒度：用来表示描述攻击的强度。

攻击过程是复杂的，一次成功的攻击过程往往包含若干分散的攻击步骤，每个攻击步骤可以看成独立的子攻击。因而，分析攻击行为的粒度有粗有细。从细粒度看，攻击可以获得系统的软件信息、端口开放情况、帐号、访问特权，查看未授权的信息，造成系统出错，执行代码等；从粗粒度看，攻击可以由一系列的子攻击过程组合而成。例如，先收集到系统信息，然后发掘系统的弱点，再利用弱点取得目标系的访问权限，从而在目标系统中执行代码，最终达到可以开展一切非法操作的目的等。我们将诸如这些细粒度的攻击行为称为子攻击，而将由它们组合而成的整个攻击过程称为复合攻击。

2.2 攻击行为分析方法

本文给出了一个利用多特征属性，系统化地分析攻击行为的方法。虽然攻击是复杂多样的，但是不同种类的攻击之间也存在一定的相似性。研究发现，攻击往往表现出过程性特点：由攻击者发起，使用某种攻击工具，利用某些技术从攻击的入口点进入被攻击的目标系统，并在其中寻找系统、服务或应用等有弱点的对象作为攻击的落脚点。确定了攻击的对象以后，再利用这些弱点进行攻击，以达到攻击者的攻击意图，最终造成特定的攻击后果。为简化描述，我们将攻击过程分解成图1所示的几个阶段。

攻击者 —采取→ 攻击手段 —攻击→ 攻击对象 —造成→ 攻击结果

图1 攻击阶段的简化形式

表1 攻击属性项与攻击阶段对照表

阶 段	属 性
攻击者	2,3
攻击手段	1,4,5,7,8
攻击对象	6,9
攻击结果	10,11,12

对大量攻击进行分析和研究后，本文中采用若干特征属性分析攻击行为，对各属性项的功能和作用的简要说明如表2。其中，属性1说明了攻击所属的种类，属性{2、3、4、5、6、7、8、9、10、11}可以清楚地描述攻击的过程，属性12可以进一步说明攻击造成后果的严重性，属性13可以说明攻击的复杂性，而属性14、15描述了攻击的防治难度和攻击影响的范围，也从侧面对攻击的复杂性作了补充说明。这些属性同样可以刻画图1所示的攻击各阶段的特性，其对照关系见表1。

表2 攻击描述表

属性项	作 用	描 述
(1)攻击所属的类别	从经验的角度说明攻击技术所属的种类	我们分成拒绝服务攻击、数据驱动攻击、信息收集攻击、信息利用攻击、伪造信息攻击5大类，每大类再分成若干子类，具体参见文[13]。
(2)攻击的来源	确定攻击者相对于被攻击目标的位置	主要有远程网络、本地网络、本地主机、本地系统4类
(3)攻击者	说明攻击是由何人发起的	包含操作者、程序员、数据录入者、系统管理者、入侵者等
(4)攻击的入口	攻击者进入到被攻击目标系统的通道，指系统与外界进行信息交换的接口，是攻击者解决“进得去”问题的途径	包含用户接口、网络协议接口、网络管理接口、设备接口几类[12]
(5)攻击者使用的工具	主要指攻击者在发动攻击时借助了什么工具和技术	包含物理攻击、电磁泄露、命令行、脚本或程序、自治代理、攻击工具软件、分布式攻击工具软件等
(6)所攻击的平台	指攻击针对哪种(或哪些)操作系统平台展开，所攻击平台的多样化程度，反映出了攻击对平台的依赖程度	包括Sun公司的Solaris、SCO等，UNIX和Microsoft系列的平台等
(7)攻击对漏洞的利用情况	主要说明攻击是否利用了漏洞，以及利用了什么漏洞	大多数攻击利用现存的漏洞，有些攻击不利用任何漏洞。可以从漏洞可能造成的直接威胁、漏洞形成的原因、漏洞的严重性、漏洞被利用的方式等描述安全漏洞
(8)攻击所使用的方法	主要指攻击时采取的技术手段	包含刺探、扫描、洪水、窃听、身份认证、旁路、欺骗、窃取、拷贝、修改、删除等
(9)攻击的对象	对目标系统造成间接或直接影响的“点”，即攻击点	包含硬件资源、网络、系统、系统成分、数据、服务等
(10)攻击的意图	攻击者在攻击成功实施后所达到的目的	攻击者一般对所攻击的对象采用破坏、收集、占用、利用等手段展开攻击，达到获取信息、修改信息、删除信息、利用服务、拒绝服务、增加服务、执行任意代码等攻击意图
(11)攻击造成的后果	攻击所造成的直接后果	包含破坏性信息的机密性、破坏性信息的完整、破坏性信息的可用性、破坏性信息的真实性几类
(12)攻击对目标系统的破坏程度	说明攻击造成后果的严重程度	不但要从攻击造成的外在结果来分析攻击的破坏程度，还要考虑该攻击产生的结果被后继攻击利用会造成的潜在破坏性
(13)攻击的复杂程度	说明攻击实施的复杂性	反映出攻击实施的难度，也从侧面反映出攻击的防治难度
(14)攻击的防治难度	说明攻击是否容易及时被阻止和防御	从侧面反映出攻击的危害性与复杂程度
(15)攻击的传播性与繁殖能力	说明攻击是否具有传播性和自我复制能力	反映出攻击所影响的范围的大小，同时能反映出攻击所造成危害的大小

2.3 攻击行为分析方法的应用

下面用本文所给的攻击行为分析方法分析若干攻击，从实例中可以发现该方案不仅可以分析和描述某个具体的攻击，还可以描述某类攻击。具体的分析和评价见2.4。为清晰起见，我们以属性项列表的形式给出分析结果。

攻击1：CodeRed攻击

- 攻击类别：数据驱动类攻击-蠕虫-网络蠕虫
- 攻击的来源：一般来自远程网络
- 攻击的入口：以Web应用提供的与用户的接口为攻击的入口点
- 攻击者使用的工具：使用特殊构造的输入脚本
- 所攻击的平台：支持IIS Web服务器的并含有.ida/.idq漏洞的Windows操作系统平台
- 漏洞利用：利用IIS Web服务器的.ida/.idq缓冲区溢出漏洞(CVE-2001-0500和CVE-2001-0506)，从受感染的机器扫描同一网段内的其它机器，并通过80端口传播到其它的Web服务器上
- 攻击方法：采用缓冲区溢出的攻击方法，可在Web服务器上留下后门，以取得受影响Web服务器的超级用户的安全权限
- 攻击的对象：攻击IIS Web服务器
- 攻击意图：达到获取系统权限的攻击意图
- 攻击后果：造成破坏信息机密性的攻击后果
- 危害性：攻击的危害性较大，当获得了系统权限以后，就可以进行任何攻击操作
- 攻击的复杂程度：不复杂，有自动化的攻击工具
- 防治难度：攻击的传播速度快，不易防范
- 传播性与繁殖能力：攻击具有很强的传播性与繁殖能力

攻击2：IIS Web服务器的.ida/.idq缓冲区溢出漏洞攻击

- 攻击类别：信息利用类攻击-错误和漏洞-应用软件漏洞-Web服务器漏洞
- 攻击的来源：一般来自远程网络
- 攻击的入口：以用户与系统的接口(IIS提供通过Web应用的客户端浏览器，对管理员脚本和internet数据进行查询)为攻击的入口点
- 攻击者使用的工具：使用特殊构造的输入脚本
- 所攻击的平台：支持IIS Web服务器的并含有该漏洞的Windows操作系统平台
- 漏洞利用：利用IIS的index server .ida/.idq ISAPI扩展没有对用户提交的输入参数进行边界检查的输入验证错误
- 攻击方法：采用缓冲区溢出的攻击方法
- 攻击的对象：攻击IIS 4.0/5.0 index service
- 攻击意图：获得SYSTEM权限来访问远程系统，达到获取系统权限的攻击意图
- 攻击后果：造成破坏信息机密性的攻击后果
- 危害性：由于攻击可以获取系统权限，因而后继攻击可能会造成较大的破坏
- 攻击的复杂程度：不高，有现成的攻击脚本
- 防治难度：防治的方法比较简单，直接打补丁即可
- 传播性与繁殖能力：不具备传播性与繁殖能力

攻击3：空会话攻击

- 攻击类别：信息利用类攻击-错误和漏洞-操作系统漏洞
- 攻击的来源：一般来自本地网络
- 攻击的入口：利用操作系统与外界进行通信的网络协议接口作为攻击的入口点
- 攻击者使用的工具：采用自己编写的命令行代码
- 所攻击的平台：Windows NT 4.0和Windows 2000操作系统平台
- 漏洞利用：利用NTFS系统允许匿名用户获取网络中信息的特性(即不需要认证就可进行连接的特性)
- 攻击方法：采用基于身份认证的攻击方法
- 攻击的对象：系统中的数据
- 攻击意图：达到获取系统中用户名和共享数据等攻击意图
- 攻击后果：造成破坏信息机密性的攻击后果
- 危害性：对空会话攻击本身来看，其破坏性不是很大，但从一次完整的ipc$入侵来看，空会话是一个不可缺少的跳板，后继攻击可能会造成较大的破坏
- 攻击的复杂程度：不高
- 防治难度：防治的方法比较简单，可以使用修改注册表打补丁的方法
- 传播性与繁殖能力：不具备传播性与繁殖能力

攻击4：DDOS类攻击

- 攻击类别：分布式拒绝服务类攻击-分布式拒绝服务攻击
- 攻击的来源：发起攻击的攻击者一般来自远程网络，而攻击傀儡机一般来自本地网络
- 攻击的入口：以网络协议与系统的接口为攻击的入口点
- 攻击者使用的工具：大多利用攻击程序软件
- 所攻击的平台：所有支持TCP/IP协议的操作系统平台
- 漏洞利用：利用TCP/IP协议在设计和实现上的缺陷
- 攻击方法：采用洪水攻击的方法
- 攻击的对象：系统中的数据
- 攻击意图：达到使目标网络或者主机不能正常工作的攻击意图
- 攻击后果：造成拒绝服务的攻击后果
- 危害性：危害性较大，会给目标带来很大的损失
- 攻击的复杂程度：攻击的分布性导致攻击技术本身的复杂性，难以被检测
- 防治难度：防治的方法比较困难，目前很少有完善的防御方法
- 传播性与繁殖能力：不具备传播性与繁殖能力

以上例子中，攻击1、攻击2、攻击3都是对具体攻击的描述。攻击1实施过程中要用到IIS Web服务器的.ida/.idq缓冲区溢出漏洞，攻击2正是对此漏洞攻击的描述。因而，攻击2可以看作是攻击1的一个子攻击。攻击4描述的是一类攻击的整体特征，而非某个具体的攻击。

2.4 攻击行为分析方法的评价

前面我们给出了一种系统化的攻击行为分析方法，下面对此方法做分析和评价：

(1)该分析方法可以揭示攻击的基本特征，具有普遍适用性，并且分析结果直观清晰；

(2)该方法既可以描述攻击的特征，还可以描述攻击的过程；

(3)该方法同时适用于分析复合攻击及其子攻击行为，有

利于对攻击行为的层次化分析和描述；

(4)该分析方法可用于描述一类攻击的整体特性。

虽然在描述某类攻击以及该类攻击中的具体攻击行为时，本方法也是适用的，但是对于一些比较复杂的攻击，具体的攻击方法在技术原理的细节方面仍有所区别。我们仍以DDOS类攻击为例进行说明。攻击4分析了DDOS类攻击的主要特性。直接对某些描述项细化，可以分析某个具体的DDOS攻击。如，Trinoo DDOS攻击在“漏洞的利用”上主要是利用TCP/IP协议中对UDP协议处理的缺陷，在洪水“攻击方法”上采用的是UDP Flooding。但是，如此来描述此种攻击仍不是很透彻和全面，这主要和DDOS攻击的分布性和多层次性有关系。DDOS类攻击是基于多层次的分布式的攻击模型，不同的DDOS攻击，其主控程序、代理程序的植入方式不同，攻击者与主控程序、主控程序与代理程序、代理程序与被攻击的目标等之间通信的方法和产生的数据特征也不同。因而，当要更深入、细致地分析DDOS攻击时，还需要定制更适用的攻击分析方法。同理，在分析木马、蠕虫等混合式复杂攻击时，也存在着同样的问题。

3 对攻击行为分析方法的裁剪

3.1 裁剪的必要性

上一节讨论了对攻击进行系统化分析描述的方法，它具有普遍适用性，我们可以将其看成分析描述攻击行为的一个“模板”或参照标准。然而，正如同描述软件开发的标准过程一样，没有一种软件开发的标准过程能够适用于所有的项目，这里的“模板”也能很完美地分析攻击。兼顾标准性和灵活性的一种可行的解决方法是：以攻击描述模板为基准，允许对其进行不同程度和不同角度的裁剪，得到描述特定攻击的更适用的方法。这里的裁剪是指允许对前面的模板通过增加、删除、修改攻击描述特征属性，使之能够较好地满足对某些特定攻击行为的分析和描述的需求。但是，倘若不有效地控制裁剪的力度和角度，则意味着攻击描述模板的存在失去意义。这里给出一些建议，文中称其为裁剪规则。

3.2 裁剪规则

我们制定了对这种攻击行为分析描述方法进行裁剪的规则。

· 规则1：当攻击来源不固定时，可以忽略此属性。

· 规则2：若没有直接利用漏洞来完成攻击，可以忽略此属性。

· 规则3：在描述一类攻击时，若无法描述明确的攻击平台，可暂时忽略此属性，待具体分析该类中的特定个体时，再描述此属性。

· 规则4：当攻击不具备自我繁殖能力或传播能力时，可以忽略此属性。

· 规则5：如果攻击不在特定的环境和场合下由特定的攻击者发起，则可以不明确指出攻击的发起者，在描述攻击时可以用“攻击者”统一代替任何具体的攻击发起者。

· 规则6：对于分布、多层、混合等比较复杂的攻击来讲，只用复杂程度并不足以描述它的复杂性，建议将此属性进行扩展：如攻击分布性的有无、多层结构性的有无、多阶段性的有无、攻击者需要编程经验的程度。

· 规则7：一个完整的复合攻击由多个子攻击组合而成，而这些子攻击看似孤立，实则不然。它们对应不同的阶段，前一阶段为后一阶段作准备，它们之间具有明显的时序性和因果条件关系制约性。添加“攻击发生的条件”属性，再结合“攻击得到的结果”，则可以对子攻击进行关联，得出攻击场景。

· 规则8：若攻击主要利用了漏洞来完成，为更详细地分析描述该攻击，可以扩展描述漏洞的属性，如漏洞的性质、漏洞的来源、漏洞在系统中的位置、漏洞的使用方法等。

其中，规则1、2、3、4是对模板中的属性特征进行删除的裁剪，规则5、6是对模板中的属性特征进行修改的裁剪，规则7、8是对模板中的属性特征进行增加的裁剪。

3.3 裁剪规则的应用

通过应用裁剪规则的示例来说明裁剪规则的应用。从示例中可以看到对规则1、2、3、4、7的应用，由于篇幅原因，对其它规则的应用不做详细说明。

Attack1：漏洞扫描攻击

漏洞扫描攻击属于信息收集攻击(扫描子类)类别。攻击者以系统与网络进行通信的网络协议接口作为攻击的入口点，通过使用网络漏洞扫描软件，采用扫描的方法，收集指定网络中一台或多台主机上的安全漏洞，达到收集系统漏洞信息的攻击意图，造成系统信息泄露的攻击后果。攻击得到的结果是：得到目标系统中存在的漏洞信息，为后继的攻击做准备。

Attack 2：rpc. sadmind 缓冲溢出漏洞攻击

该攻击属于信息利用(错误和漏洞子类下的操作系统漏洞子类)攻击类别。攻击发生的前提条件是：目标系统存在rpc. sadmind远程溢出漏洞。攻击来源于远程网络，攻击者以系统与远程用户通信的rpc服务的接口作为攻击的入口点，使用特殊构造的超长缓存数据，利用sadmind存在远程溢出漏洞的缺陷和sadmind以root身份运行的事实，采用缓冲区溢出的攻击方法改写堆栈指针，攻击目标系统的服务，达到可执行任意代码、获得root特权的攻击意图，造成破坏信息的完整性和保密性的攻击后果。

分析：Attack1的目的是为了收集系统漏洞信息，没有详细描述攻击来源和所攻击的平台，主要因为攻击的来源不固定，而所攻击的操作系统平台则由漏洞扫描软件本身决定，所以在用具体的漏洞扫描软件攻击时，可以细化该属性。攻击得到的结果属性说明：Attack 1可以得到系统和应用服务中存在的漏洞。假定我们只关注含有sadmind漏洞，则扫描后可以发现有sadmind漏洞的主机。Attack 2利用sadmind漏洞获取系统root权限。显然，Attack 1得到的结果是Attack 2实施的前提，因而可以将Attack 1和Attack 2进行因果条件关联，呈现出攻击者获得系统权限的更完整的过程。

Attack 3：IP欺骗攻击

IP欺骗攻击是由一系列子攻击过程组合而成的，也可以用来说明攻击关联。如果一台主机A信任某个目标主机B，并且先后存在以下几个攻击：攻击一，攻击者对B主机进行了拒绝服务攻击；攻击二，攻击者对A主机进行了TCP序列号预测攻击；攻击三，攻击者伪装成B主机的IP地址与A主机成功地进行了连接。

分析：其中，攻击一产生的结果是B主机不能工作，从而为攻击者冒充B来预测A的序列号，以及攻击者与A成功连接提供条件；攻击二的结果是攻击者成功地预测与A连接的TCP序列号，为攻击者冒充B主机成功地连上A主机提供条件。可见，通过因果条件关联可以将这几个攻击步骤组合成IP欺骗攻击的完整过程，构造IP欺骗攻击的场景。

Attack 4：邮件炸弹攻击

邮件炸弹攻击属于拒绝服务攻击(基于网络子类)类别。攻击者一般来自远程网络，攻击者使用自动产生邮件炸弹的攻击软件，以系统与网络进行通信的网络协议接口作为攻击

(下转第105页)

SEC),2001,4(3):224～274
3 Al-Kahtani M, Sandhu R. A Model for Attribute-Based User-Role Assignment. In: Proceedings of the 18th Annual Computer Security Applications Conference, Las Vegas, Nevada, December 2002
4 Al-Kahtani M, Sandhu R. Induced Role Hierarchies with Attribute-Based RBAC. In: Proceedings of the 8th ACM Symposium on Access Control Models and Technologies (SACMAT), Villa Gallia, Como, Italy, June 2003
5 Al-Kahtani M A, Sandhu R. Rule-Based RBAC with Negative Authorization. In: Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), December 2004. 405～415
6 Benferhat S, Baida R E, Cuppens F. A Stratification-based Approach for Handling Conflicts in Access Control. In: SACMAT '03: Proceedings of the eighth ACM symposium on Access control models and technologies, Como, Italy, ACM Press, June 2003. 189～195
7 Moffett J D, Sloman M S. Policy Conflict Analysis in Distributed System Management. Journal of Organisational Computing, 1994,4(1):1～22
8 Lupu E, Sloman M. Conflict Analysis for Management Policies. Fifth IFIP/IEEE International Symposium on Integrated Network Management IM'97, San-Diego, May 1997
9 Baader F, Calvanese D, et al. The Description Logic Handbook: Theory, Implementation and Applications. Cambridge University Press ,2003

(上接第 96 页)

的入口点，通过发送未经授权的、容量庞大的邮件，以洪水攻击的方式，攻击接收者的电子邮件信箱或者网站的邮件服务器系统和目标网络的带宽资源，达到摧毁接收者的电子邮件信箱的邮件信息、使邮件服务器性能下降或大量消耗网络带宽资源的攻击意图，造成破坏信息的完整性和可用性的攻击后果。

Attack 5：网络监听攻击

网络监听攻击属于信息收集攻击类别。攻击者一般来自本地网络，攻击者以网络协议与操作系统的接口为攻击的入口点，通过监听程序，使用网络监听的攻击方法，获取网络上传输的数据并分析解码，达到收集敏感信息的攻击意图，造成系统信息的保密性被破坏的攻击后果。

攻击 6：后门攻击

后门攻击属于信息利用攻击类别。直接利用事先已植入的并已运行的后门程序进行攻击时，也不存在漏洞的利用问题，且所攻击的平台是由后门程序决定的。

分析：Attack 4 由于不需要利用现存的漏洞进行攻击，因而对漏洞的利用不加描述。Attack 5、Attack 6 所攻击的平台不固定，并且没有利用漏洞，因而在描述时，忽略了漏洞利用属性，而且未对攻击的平台做说明。当使用具体的攻击软件时，再描述攻击的平台。

结论 本文提出了一个系统化的攻击行为描述方案，并在此基础上讨论了对它进行裁剪的思想和方法，为分析和描述攻击提供了参考方案。通过对大量攻击实例的分析，说明了本文分析方法和裁剪规则的有效性和普遍适用性。当然，本文提出的攻击行为分析方法也存在着不足之处，特别是对于某些攻击来说，此方法适用于在较高层次抽象分析和描述，这时只具有最基本的描述能力。应用这种攻击分析描述方法能达到比较好的分析效果，可以系统地分析攻击的多方面特征，揭示攻击的本质特性，简化对攻击的理解，还可以用来分析攻击行为之间存在的关联性，构造完整的攻击过程。

参 考 文 献

1 Stallings W. Network and Internet Work Security Principles and Practice. NJ: Prentice Hall, 1995
2 Li M, Jia W, Zhao W. Decision Analysis of Network-Based Intrusion Detection Systems for Denial of Service Attacks. 0-7803-7010-4/01, IEEE, 2001
3 Kumar S. Classification and detection of computer intrusions: [Ph D Thesis]. Purdue University, 1995
4 刘欣然. 网络攻击分类技术综述. 通信学报，2004(7):30～36
5 Conen F. Information system attacks: a preliminary classification scheme [J]. Computers and Security, 1997, 16(1):29～46
6 Landwehr C E, Bull A R, McDermott J P, et al. A taxonomy of computer program security flaws. ACM Computing Surveys, 1994, 26(3):211～254
7 Bishop M. A Taxonomy of (Unix) System and Network Vulnerabilities: [Technical Report]. CSE-9510. Department of Computer Science, University of California at Davis, May 1995
8 Bishop M. Vulnerabilities analysis [A]. Second International Symposium on Recent Advances in Intrusion Detection [C]. USA, 1999
9 Lindqvist U, Jonsson E. How to Systematically Classify Computer Security Intrusions. In: IEEE Symposium on Security and Privacy. Oakland, California, USA, 1997. 154～163
10 Howard J D. An Analysis of Security Incidents on the Internet: [Ph D dissertation]. West Lafayette, USA: Carnegie Mellon University, 1997
11 A Taxonomy of Network and Computer Attack Methodologies: [Honours thesis]. University of Canterburry, November 7, 2003. http://www.cosc.canterbury.ac.nz/research/reports/HonsReps/2003/hons_0306.pdf
12 张涛，董占球. 网络攻击行为分类技术的研究. 计算机应用，2004，24(4):115～118
13 郭林，严芬，黄皓. 基于多维角度的攻击分类方法. 计算机工程，2005