基于本体的网络攻击模型及其应用

王 前 冯亚军 杨兆民 姚 磊
(空军雷达学院 武汉 430019)

摘 要 在对攻击理论进行深入研究的基础上,构造了一个多维分类模型,并利用本体构造攻击本体中概念之间的逻辑关系和层次结构,建立攻击本体模型,从而利用攻击原子本体构造攻击场景,对目标系统实施攻击。

关键词 网络攻击,攻击分类,本体,攻击模型,攻击场景
中图法分类号 TP393.08 **文献标识码** A

Network Attack Model Based on Ontology and its Application

WANG Qian FENG Ya-jun YANG Zhao-min YAO Lei
(Air Force Radar Academy, Wuhan 430019, China)

Abstract The paper, which is based on attack theory, presented an architecture of multi-dimensional attack classification. According to attack classification, attack ontology model was built, and the logical relationship and hierarchy structure between the ontology of attack concepts were described. Finally according to attack scenario based on atomic ontology of attack, the attack on the target was realized.

Keywords Network attack, Attack classification, Ontology, Attack model, Attack scenario

1 引言

攻击模型是攻击技术发展的知识需求的重要来源,它有助于深入理解攻击的本质及其特点,分析整个攻击过程中攻击行为之间的相互关系。如攻击树模型[1,2]采用"与"节点和"或"节点表示攻击步骤之间的关系,基于Petri网的攻击网模型[3,4]采用有色Petri网对攻击进行建模,攻击图模型[5,6]基于图论采用攻击模板描述攻击行为,供求模型[7]通过需求/提供来刻画攻击行为之间的关联关系。攻击树模型侧重于描述攻击过程所包含的各种攻击行为之间的联系,攻击行为和结果都用节点表示,不进行区分,容易造成混乱。基于Petri网的攻击模型只能描述单一攻击行为,不能提供正在发生的攻击场景的清晰描述。攻击图能够描述发起攻击的初始状态与攻击成功的终态之间所有的攻击路径,但难以构造,尤其是网络节点和漏洞数量较多时,常依靠手工构图。总的来说,现有的攻击建模并非建立在攻击分类的基础之上,攻击分类和攻击模型缺乏有机结合,从而使得攻击建模存在全面性和层次性不强等问题。

在进行网络攻击时,攻击知识库的构建和对攻击进行建模是进行网络攻击的关键。若要系统化构建一个为网络攻击提供技术支持的攻击知识库,首先就要选取合适的分类方法对数量庞大的攻击技术进行分类。鉴于此,必须对攻击理论和技术进行深入研究,在对其合理分类的基础上,建立攻击模型,并根据攻击模型构造攻击场景,对目标系统实施攻击。

2 攻击分类方法

网络攻击是攻击者通过系统的某个安全漏洞,利用某种攻击技术进入系统,对攻击目标执行非法操作,从而产生某种结果,影响或破坏系统的安全性。以上描述指出了攻击的多个要素,这些要素可以作为攻击分类的着眼点。由此我们从攻击者角度出发,提出了攻击技术的层次化分类结构,以利用漏洞、攻击过程、攻击目标、攻击结果4个要素作为分类的依据,构造一个多维分类模型。

2.1 利用漏洞

攻击者能够进行未授权访问和使用系统资源的前提是目标网络和系统存在安全漏洞。系统漏洞是计算机系统在硬件、软件、协议的设计与实现过程中或系统安全策略上存在的缺陷和不足;非法用户可利用系统安全漏洞获得计算机系统的额外权限,在未经授权的情况下访问或提高其访问权限,破坏系统,危害计算机安全。根据造成漏洞的原因可分为以下几类:应用软件系统漏洞、网络协议漏洞和配置漏洞。

2.2 攻击过程

通过对已发生的黑客攻击事件的分析和归纳,从网络攻击的操作流程来看,一次网络攻击行为主要包括目标系统探测分析、攻击实施和踪迹隐藏。据此,对攻击方法从攻击过程的角度进行层次化分类,大体可分为:目标探测、漏洞扫描、权限获取、权限提升、预留后门和踪迹隐藏。攻击过程的关键阶段是目标信息探测和目标使用权限获取阶段。根据收集到的

到稿日期:2009-07-25 返修日期:2009-09-25 本文受军队2110工程项目(07010205)资助。
王 前(1978—),女,博士,讲师,主要研究方向为网络安全与网络生存技术等,E-mail:wangqianzz@126.com;冯亚军(1977—),男,硕士,讲师,主要研究方向为计算机网络应用等。

目标系统信息，攻击者对这些信息进行分析，获取系统的一般访问权，进而寻找系统漏洞来提升自己的权限。上述的攻击过程并不是每一步都会执行，例如，攻击者若在权限获取阶段就获得系统的特权权限，便可以跳过权限提升阶段。

2.3 攻击目标

和常规作战中选择打击对象一样，网络攻击也是把对敌方的战略目标作为首要进攻对象。一般情况下，我们认为目标系统是一个拥有硬件资源、数据并能够对外提供服务的一个综合体。由此，可将攻击目标归为以下 4 类，即硬件资源、网络、数据、服务。

2.4 攻击结果

攻击是指任何试图危害资源的完整性、保密性和可用性的行为集合。攻击结果可能是滥用系统或系统中的数据，使系统不可靠或不稳定，甚至无法正常使用服务，或者试图访问系统中的数据，或者试图篡改或操作数据。由此，将攻击结果分为以下几种：破坏系统机密性、破坏系统完整性和破坏系统可用性。

综合以上分析，整个网络攻击分类体系可以用图 1 表示。

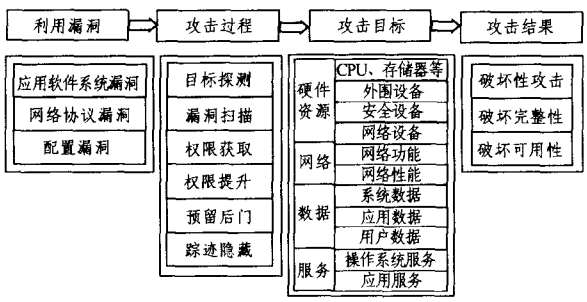

图 1 攻击分类体系

该分类体系具有以下几个特点：

(1)以多个属性为依据，从多个维度对攻击进行分类，通过对上述分类标准各个子项的逻辑组合，就可以描述各种攻击方式，具有较好的完备性。

(2)根据新出现攻击的特点，对各个分类标准不断扩展，添加实例节点，从而可以描述新的攻击方式，而且不会影响整个分类体系，使得分类具备良好的可扩展性。

(3)分类研究从攻击者角度出发，以网络攻击为目的，满足分类的可用性要求。

3 攻击本体模型

3.1 本体的概念

本体是对某一领域内的概念及其关系的一种概念化描述[8,9]。也就是说，本体是某领域内概念的显示说明，即把现实世界的某个领域抽象成一组概念及概念间的关系。由此可以看出，本体的基本元素包括概念、实例和关系等。从语义上分析，概念表示的是对象的集合；实例则是组成概念的成员。这里的关系是指概念之间、实例之间，以及概念与实例之间的关系，如整体与部分关系(part of)、实例关系(instance of)、子类关系(subclass of)等。本体的基本元素以及它们的合成能够形成对领域内对象的正确表达。

3.2 本体的构筑

本体的构筑是一种人为的对领域概念按某种层次结构进行分层刻画的过程。本体建模首先要抽象信息模型内部的关键概念，定义关系来表达概念之间的联系，定义属性来表示概念中类对象之间的关系。本体在其最深层次上包含一种分类法。本体应用的概念分类方法可从多种角度对事物进行更全面的描述，同时其概念在组织结构上具有可重组、可继承等特点。

上文的攻击分类结果为攻击领域概念之间的关联关系提供了一个框架，因此借助本体来构建攻击模型，有助于攻击分类和攻击模型的有机结合。攻击本体的构造过程是按照攻击分类中的分类层次来安排本体中概念之间的层次关系。攻击本体构建流程如图 2 所示。

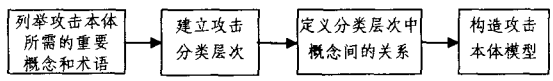

图 2 攻击本体构建流程图

在攻击本体的概念类层次结构中，攻击本体模型依据攻击分类，采用层次模型进行逐级概念类的抽象，最高层为攻击领域本体，用于提供攻击领域的概念、关系的声明。每种概念还要进一步划分子类，直至形成具体可用的概念和具体的属性变量值。攻击领域本体的下层为攻击应用本体，对应于应用子领域共性的概念和关系，最下层为攻击原子本体，对应于应用实体可直接运用的实体概念声明。

3.3 攻击本体模型

(1)攻击领域本体

攻击领域本体是用于描述攻击领域知识的一种专门本体，它给出了攻击领域实体概念及相互关系领域活动以及该领域所具有的特性和规律的一种形式化描述。图 3 采用词汇概念图 LCG(Language Concept Graph)描述攻击领域本体结构。LCG 是一种带标签的有向图，其中椭圆形顶点表示概念，有向边表示类间的语义关系，顶点中的词汇代表概念的名称，有向边上的词汇表示连接的 2 个顶点(概念)之间的关系。

攻击领域本体用于描述当前攻击所需的概念和关系集，包含 4 个子类：攻击目标、利用漏洞、攻击过程、攻击结果。攻击类概念之间包含 4 种关系：利用(攻击利用的漏洞)、使用(攻击采用的方法)、针对(攻击指向的目标)、导致(攻击产生的结果)。也就是说，攻击者发现目标的漏洞，采用攻击方法，对目标发动攻击，从而实现一定的攻击效果。

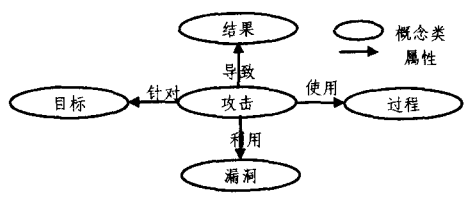

图 3 攻击领域本体

(2)攻击应用本体

攻击应用本体是对攻击领域本体的进一步描述。根据上文的攻击分类结果，各类攻击应用本体描述如下：

① 利用漏洞应用本体包括应用软件系统漏洞、网络协议漏洞和配置漏洞。

② 攻击过程应用本体包括目标探测、漏洞扫描、权限获取、权限提升、预留后门和踪迹隐藏。

③ 攻击目标应用本体用于描述攻击目标所需的概念和关系集，包含的子类有硬件、网络、数据和服务。

④ 攻击结果应用本体包括 3 种：破坏系统机密性、破坏系统完整性、破坏系统可用性。

图 4 是攻击应用本体图示，攻击领域本体和攻击应用本体之间是整体与部分的关系。

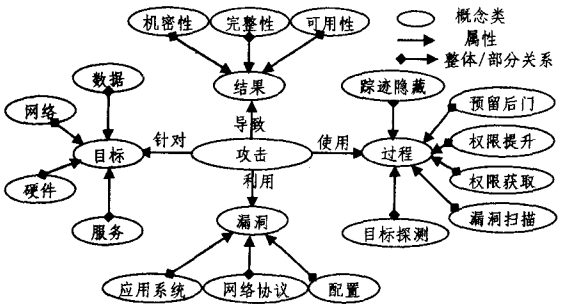

图 4　攻击应用本体

(3)攻击原子本体

攻击原子本体是攻击应用本体可直接运用的实体概念声明，原子本体中的类型实例与应用本体中的概念是类与实例的关系。各类攻击应用本体的原子本体描述如下，其中攻击结果因其不可再分性，没有原子本体。

①攻击利用漏洞原子本体

攻击利用漏洞原子本体如图 5 所示，图中的矩形是类型实例，类型实例与应用本体中的概念是类与实例的关系。

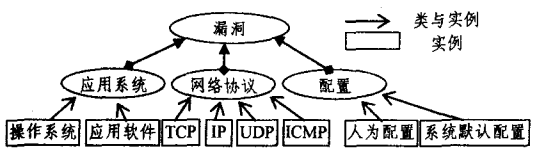

图 5　攻击利用漏洞原子本体

②攻击过程原子本体

攻击过程原子本体是指该攻击在功能和操作上为单一的主体，可不与其它攻击操作交互而单独完成，是攻击的最小行为序列。复合攻击本体在功能和操作上应是由若干个原子攻击本体按照一定逻辑关系所组成的攻击序列。大部分的网络攻击都可由这些底层类复合而成。攻击过程原子本体如图 6 所示。

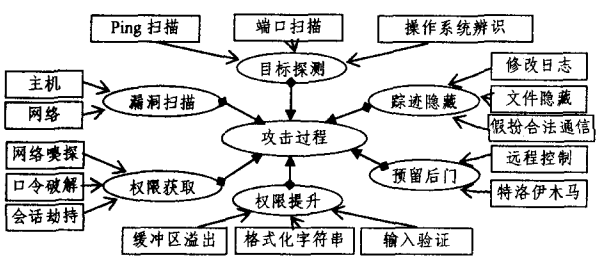

图 6　攻击过程原子本体

③攻击目标原子本体

依据攻击目标分类，攻击目标原子本体如图 7 所示。

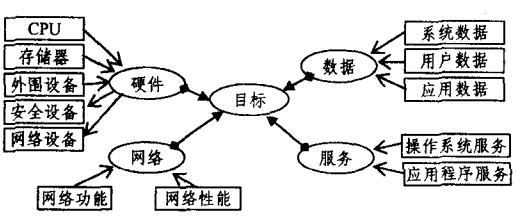

图 7　攻击目标原子本体

攻击宏观描述的上层——领域本体：以攻击者为中心的攻击概念与其下层概念是整体与部分关系。宏观层次的终端节点——应用本体：由攻击描述的微观层次即原子本体来进一步描述，它们之间是类与实例的关系。攻击领域的概念分层定义了一组由底层概念集到高层概念集的映射，表示攻击知识由细化到抽象的提升过程。它使得攻击可以在较高的、泛化的抽象层上进行处理，从而可以在更有意义、更明显的抽象层次观察攻击。同时从高层概念集到底层概念集的替换，使攻击模式更易于理解，从而可提高攻击知识的准确性和可理解性。

3.4　攻击本体模型分析

网络攻击本体模型包括攻击者行为描述的层次化概念以及各种攻击在不同细节层次上的实现。攻击本体模型实现了攻击分类和攻击模型的有机结合，能对整个攻击过程进行结构化和形式化描述以及有效分析，有助于安全知识的共享。从知识表示的角度来讲，攻击本体不应是仅被某个应用主体所接受，而应得到领域内各应用主体的认可；从共享的角度来说，攻击本体作为一种概念化的说明，采用框架系统对客观存在的攻击概念及其关系进行描述，应用的是在各种应用主体之间交换意见时所用到的共同语言。这样本体最根本的优势——共享和重用得以实现，这也是本文将本体引入构建攻击模型的原因。对应于工程实际，本体方法就是将具体应用领域按层次抽象成为概念类，领域内不同的应用主体通过使用攻击本体类可以达到对资源和对象的一致描述，从而对攻击进行形式化建模。

4　攻击场景

网络攻击是非常复杂的过程，攻击者在进行攻击时，往往是分步骤、多阶段实施，通过一系列的攻击行为才能达到最终目的，每个阶段的攻击都是为达到一个目的，按照攻击目的可以将攻击过程分成若干个攻击序列。这一系列隶属于同一攻击过程的攻击序列称之为攻击场景。攻击场景中的每一个攻击序列都对应着一定的目的，即攻击意图，这样可以把攻击场景看成由一系列攻击意图组成。由于一个攻击意图可以对应于多个攻击行为，每个攻击行为可以看作一个原子攻击，因此使用攻击意图构建攻击场景能够更加抽象地表示攻击过程[10]。

攻击意图中的攻击行为具有一定的执行顺序，可以用一系列攻击过程原子本体节点来表示，或者说攻击意图是攻击过程原子本体的有序组合。一个粗略的攻击意图可以被细分为多个较细粒度的攻击过程原子本体，意图能在不同层次上组成攻击场景。不同的攻击场景可能需要不同层次的攻击意图。在最底层，意图由原子攻击行为来实现。原子攻击行为具有独立的、不可分解的攻击目的，而复合攻击则是将原子攻击按照一定的逻辑关系进行排列，在特定的时间和空间中形成一个攻击序列，从而达到仅用原子攻击无法实现的目的。攻击者对系统的攻击行为可以用一系列攻击过程原子本体节点来表示，从而建立较高层次的攻击意图，实现复合攻击。

5　实例分析

假定对目标实施两类攻击：DDoS 攻击和口令破解攻击。

分布式拒绝服务攻击 DDoS(Distributed Denial of Ser-

vice)采用分布、协作的大规模攻击模式，给网络的正常运行带来了极大威胁。DDoS 攻击可以导致网络瘫痪，从而使得网络信息系统无法为用户提供服务，造成不可估量的损失。口令破解攻击是攻击者只要能猜测或者确定用户的口令，就能获得机器或者网络的访问权，并能访问到用户能访问到的任何资源。这个用户若有域管理员或 root 用户权限，则是极其危险的。下面对这两类攻击建立攻击场景，实现其网络攻击目的。

(1)场景一：DDoS 攻击

攻击者首先探测网络上有哪些存活主机，然后探测主机系统的 Sadmind 漏洞，对存在此漏洞的主机采用缓冲区溢出攻击方式进入系统；然后再从该主机通过 Rsh 连接到攻击者主机，将拒绝服务攻击代理软件拷贝到该主机上，使其成为分布式拒绝服务的代理系统；最后从多个这样的代理系统向拒绝服务的目标发起 DDoS 攻击。上述攻击场景可用多个攻击意图来描述，如图 8 所示，图中的每一个方框代表一种攻击意图。

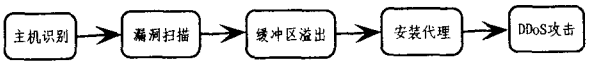

图 8 DDoS 攻击场景

对应于图 8 攻击场景中的每一种意图，又有多种攻击方式来实现。图 9 中的每一个椭圆框代表一种攻击方式，在具体实现中，可根据需要选择。

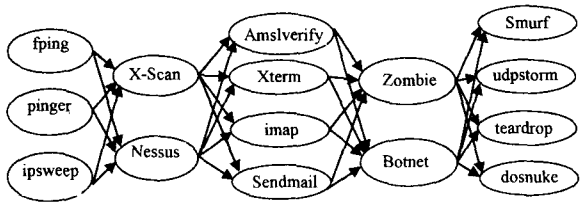

图 9 DDoS 攻击实现

(2)场景二：口令破解攻击

口令破解攻击包括以下 5 个步骤：主机探测、漏洞扫描、获取口令文件、口令破解和安装后门。其攻击场景如图 10 所示，攻击场景实现如图 11 所示。

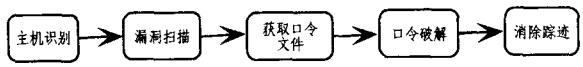

图 10 口令破解攻击场景

从以上两个例子可以看出，任意一种网络攻击方式代表攻击者的一种攻击意图，根据攻击实施过程可建立相应的攻击场景，而每一个攻击场景可由多种攻击原子本体来实现。攻击过程原子本体模型能对整个攻击过程进行结构化和形式化描述，有助于建立攻击场景和实施网络攻击。在实战中，我们可以根据相应的攻击目的，构造攻击场景，选择适当的攻击方法，从而达到攻击效果。

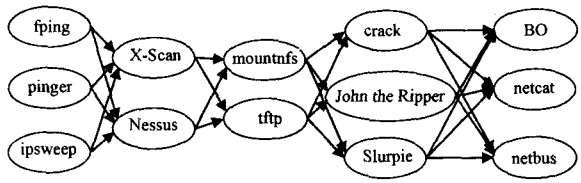

图 11 口令破解攻击实现

结束语 网络攻击研究的一个关键问题是攻击分类方法和攻击建模技术。本文首先从攻击者角度出发，提取出攻击的 4 个基本要素，提出了符合分类标准的攻击技术层次分类结构，建立了一个多维网络攻击分类体系；然后在攻击分类的基础上用攻击本体模型对攻击技术进行描述，实现攻击知识的表达、共享及重用；最后基于攻击过程原子本体构造攻击场景，实现对目标系统的攻击。

参 考 文 献

[1] Schneier B. Attack trees: Modeling Security Threats [J]. Dr Dobb's Journal, 1999, 12(24): 21-29

[2] Moberg F. Security Analysis of an Information Systems: Using an Attack Tree-Based Methodology[D]. Department of Computer Engineering, Chalmers University of Technology, Sweden, 2000

[3] Mcdermott J. Attack Net Penetration Testing[A]// The 2000 New Security Paradigms Workshop[C]. 2000: 15-22

[4] Steffan I, Schumacher M. Collaborative attack modeling[A]// Proceedings of SAC[C]. 2002

[5] Swiler L, Phillips C, Gaylor T. A Graph-Based Network Vulnerability Analysis System[R]. Sandia National Laboratories, 1997

[6] Sheyner O, Haines J, Jha S. Automated Generation and Analysis of Attack Graphs[C]// Proceedings of the IEEE Symposium on Security and Privacy. 2002

[7] Templeton S J, Levitt K. A Requires/Provides Model for Computer Attacks[A]// Proceedings of the New Security Paradigms Workshop [C]. Cork Ireland, 2000: 31-38

[8] Guarion N. Formal Ontology, Concept Analysis and Knowledge Representation[J]. International Journal of Human-computer Studies, 1995, 43(3): 625-640

[9] 邓志鸿，唐世渭，张铭，等. Ontology 研究综述[J]. 北京大学学报：自然科学版，2002，38(5)：730-738

[10] 柳亚明，许峰，吕志军，等. 基于攻击意图的报警信息关联研究[J]. 计算机科学，2005，32(9)：61-65

(上接第 39 页)

[6] Chia-Yu Yu, Chih-Heng Ke, Reuy-Shin Chen, et al. MyEvalvid_RTP: A New Simulation Tool-set Toward More Realistic Simulation[J]. Future Generation Communication and Networking, 2007(1): 90-93

[7] Surucu D, Surucu M, Ozturk E. Performance comparison of 802.11 and 802.16 technologies for video transmission in NS2-EvalVid [C]// IEEE 16th Signal Processing, Communication and Applications Conference. April 2008: 1-4

[8] Abdel-Hady M, Ward R. A Framework for Evaluating Video Transmission over Wireless Ad Hoc Networks Communications [C]// IEEE Pacific Rim Conference on Computers and Signal Processing. Aug. 2007: 78-81

[9] 数字图像基础[EB/OL]. http://is.cs.nthu.edu.tw/~chunk/slide/图像基本观念.doc

[10] Mangold S, Choi S, May P, et al. IEEE 802.11e Wireless LAN for Quality of Service (invited paper)[C]// Proc. of the European Wireless. Florence, Italy, Feb. 2002(1): 32-39

[11] 柯志亨，程荣祥，邓德隽. NS2 仿真实验—多媒体和无线网络通信[M]. 北京：电子工业出版社，2009：284-297

[12] ffmpeg[EB/OL]. http://ffmpeg.sourceforge.net/index.php

[13] ffmpeg doc[EB/OL]. http://www.ffmpeg.org/ffmpeg-doc.html

[14] http://www.isi.edu.nsnam/ns [EB/OL]

[15] YUVvierwe[EB/OL]. http://eeweb.poly.edu/~yao/VideobookSampleData/video/application/YUVviewer.exe