基于网络攻击平台的攻击分类方法研究

Research of Attack Taxonomy Based on Network Attack Platform

毛承品 范冰冰 （华南师范大学计算机学院 广东广州 510631）

摘 要： 首先分析了已有的网络攻击分类法的不足；概要介绍新开发的基于教学培训和公安侦讯目的网络攻击平台及功能框架，介绍网络攻击平台的特点以及关键技术；网络攻击分类是攻击平台的关键，本文提出“维”度的攻击分类法，此分类法非常符合网络攻击平台的特点要求，以据此分类法对当前新出现的网络攻击进行分类，符合网络攻击分类原则，以建立网络攻击知识库为目标。

关键字： 网络攻击平台 分类 网络攻击 知识库

1 引言

设计和开发的基于教学、培训和公安侦讯的网络攻击实验平台主要目的和功能是在网络攻击的真实环境下，将典型攻击进行生成重演和展现，使受训者直观感受到此种攻击造成的危害和效果。深入的理解攻击的原理机制是为了更好的防御网络攻击，因此网络攻击平台的研究和成功开发具有重要的现实意义。网络攻击平台中，有效、准确的对网络攻击进行归类对网络攻击的生成和展现非常关键。

由于人们对于各种网络攻击的理解、把握程度相差很大，以及对网络攻击的判定和特征提取的方法不同，对攻击造成的危害或潜在威胁的认识难以保持一致，因此不适合此网络攻击平台的攻击分类。

1.1 已有的网络攻击分类方法

在计算机和网络安全领域已有较多针对网络攻击的分类法，国内外对此也做出了很多有益的研究。早期的最重要的两种分类法包括①防护分析分类（Protection Analysis Taxonomy）和②安全操作系统的研究分类；Bishop[1]的弱点漏洞分类法展现 Unix 系统的弱点漏洞分类，其用六个“轴”实质、时间、攫取领域、危害的范围、来源、最小代价来对弱点划分。另外 Bishop 也对其它的弱点漏洞进行了分析并且将前期的 PA，RISO 和 Aslam 分类法进行了比较和评估。

1.1.1 基于经验术语的分类

基于经验术语分类方法是利用网络攻击中常见的技术术语、社会术语等来对攻击进行描述的方法。如 Icove[2] 曾经按经验将攻击分成病毒和蠕虫、资料欺骗、拒绝服务等 20 余类。此攻击分类方法存在较大的问题，(1) 某些术语不仅不属于相同或相近的技术层面而且相互之间相差往往很大 (2) 很难满足完备性的原则 (3) 明显缺乏互斥性，一些术语之间存在着较大的交叉术语内涵重复。例如现在的病毒和蠕虫中往往同时包含着特洛伊木马逻辑炸弹。

综合以上可以看出这种基于术语分类的方法往往内涵界定不清，没有得到多数人的认可，对于新出现的攻击只能通过增加术语的方式加以补充，扩展性很差，另外一个缺陷就是对于同一种攻击不同人的分类可能出现完全不同的结果。

1.1.2 Howard 和 Christy[3] 基于攻击过程的分类方法

Howard[4,5] 在总结分析了计算机应急处理协调中心 CERT/CC 所收到的事件报告基础上提出了一种新的基于过程的攻击分类方法。对攻击过程中的 5 个方面进行了描述，具体包括攻击者的类型、攻击工具、入侵过程信息、攻击结果和攻击目的。

Howard 尝试将重点集中在过程驱动的攻击分类上面，这无疑是有价值的。但是 Howard 的分类法也有相互交叉的缺陷，例如在攻击者类型的分类中，Vandal 也可能是个 Terrorist，Spy 也不能与 professional criminal 区分。不过与基于经验术语的分类方法比，Howard 的分类方法在有用性和实用性方面都有了很

大的提高。另外较好地解决了可扩展的难题，它可以增加初始权限、转换方法、动作等属性值，并通过增加或细分属性将不断出现的新的攻击纳入到此分类体系中去，其在普适性、全面性、准确性、可扩展性等方面都有了很好表现。

1.1.3 Lough 多属性攻击分类方法

Lough 在 2001 年提出 VERDICT[6]（Validation Exposure Randomness Deallocation Improper Conditions Taxonomy）的攻击分类法，其是基于多属性的攻击分类描述方法，Lough 采用 4 种攻击属性来描述攻击①不合适的确认②不合适的暴露③不合适的随意性④不合适的分配。Lough 的分类方法类似于 Bishop 的 6 "轴"分类方法，其能很好处理划分复杂、混合的攻击种类，但是其缺点就是需增加较多的属性来归类新的攻击。

1.2 当前网络攻击分类普遍存在的问题[7]

（1）一种攻击可能包含另外一种攻击，结果可能存在多种分类方法。

（2）攻击不像动植物界分类，有共同的特征，要划分出清晰的攻击分类是比较困难的。蠕虫跟病毒可能相关，这二者与缓冲区溢出攻击又几乎没关系。

（3）不同机构对攻击分类原则的把握差度较大，有的按经验技术术语分，有的从攻击者的角度的分类，有的按照基于防御者的角度分类。造成不同安全产品的兼容问题，不利于安全产品的推广和正常使用。

（4）当前的主流安全防护产品，对某类攻击事件危害结果只能向用户反馈"高""中""低"几个模糊的危险等级，没有一个明确的界定。把具体的危害认识留给用户去判定，用户即使知道攻击事件的严重性，也无法深入具体的了解造成的危害和可能带来的后果，使安全产品功能降低。

（5）不同机构或人员对于网络攻击的认识存在着差异，对于同一类甚至同一种网络攻击事件，对其属性的判断和描述差异很大，从而得出不同的归类结果。

基于以上原因，已有的网络攻击分类法不适用于此网络攻击平台，不便于此网络攻击平台的推广和使用。

2 新的攻击分类法

2.1 基于教学和培训的网络攻击平台体系结构

新开发的网络攻击实验平台是网络安全研究、实验、设备研发、教学和培训的重要基础设施。此网络攻击实验平台的研究，主要目的在相对通用网络（互联网、LAN）信息系统环境中开发自动调用、生成、重演目前典型的网络攻击，从攻击准备阶段到网络攻击结束阶段整个过程和效果的展现以及对网络攻击的底层机制的仿真，展现攻击形成的危害和影响，并可扩展性形成网络攻击库，它的实现将是对国内外网络攻击实验平台的创新和突破，有助于促进网络安全其他领域理论研究的进一步发展，尤其是安全评估、攻击机理研究、网络攻击测试的发展，具有重要的理论价值。有利于带动网络安全教学和培训事业，更高效地完成网络安全专门人才培养；作为网络犯罪案件库、网络犯罪模拟重现和痕迹分析研究，有利于进一步提高网络犯罪侦破和防范水平，具有重要的社会价值和经济效益。

2.2 网络攻击实验平台的框架体系

网络攻击实验平台框架模型结构如图 1 所示，主体有实验客户端、攻击源端、攻击目标端、攻击实验网络平台、攻击知识库、攻击实验管理系统和攻击效果检测/展现系统，此系统基于 Web service 体系结构，各个通信模块采用封装 XML 的 SOAP 协议实现交互式通信，此平台已经开发成功、运行良好。

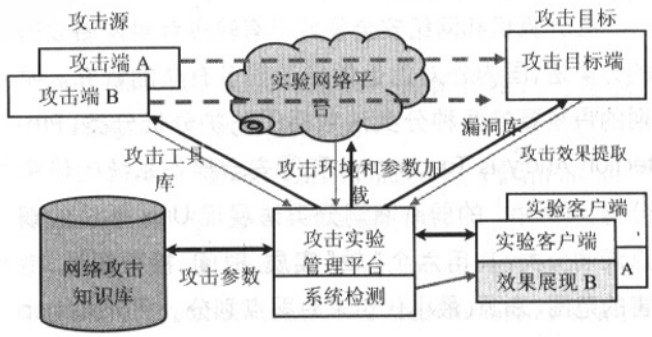

图 1 网络攻击实验平台框架模型结构

其中网络攻击知识库即网络攻击特征的提取，通过将网络攻击适当的分类、结构化描述，建立特色网络攻击

知识库,攻击端通过查询此攻击特征库来实现,网络攻击的生成、模拟,网络攻击知识库是网络攻击实验平台的基础和核心。攻击实验管理系统和攻击效果检测/展现系统主要功能是将相关攻击环境和参数加载(漏洞、网络环境、攻击工具)到攻击源、实验网络平台和攻击目标主机,完成某网络攻击实验准备,并获取整个攻击过程的数据,向用户展现攻击。

2.3 网络攻击分类的基本原则[1,2]

20 世纪 80 年代后期,欧美国家如 MIT 的林肯实验室、Carnegie Mellon University 和 Virginia 州立大学的相关网络安全专家和学者提出了攻击分类的基本原则,相关学者也进行了讨论,主要包括下几点。

- 易接受:提出的分类法应该结构清晰,能被业界接受和支持。
- 易理解:分类体系不仅让网络安全领域的专家学者易于理解,非安全领域的人也能够理解。
- 完整性/无遗漏:尽可能考虑所有的攻击并对这些进行攻击分类。
- 一致性:分类的步骤须清楚的定义。
- 互斥性:每一种攻击只能划分为一种类别。
- 重复性:不同人对同一种攻击采用同一原则划分能够得到相同结果。
- 术语一致性:使用现有的术语来分类,避免混淆。

此攻击分类(以下简称分类)引入"维"的概念,"维"可以从整体的角度来观察攻击。采用四个"维"来划分攻击,介绍如下:

(1) 第一维。基本的"维"度,将攻击以攻击矢量为基础划分,如果没有攻击矢量,则划分为相近的一类攻击类别。

(2) 第二维。将攻击目标划分为第二维。攻击目标可以划分得很细,如:Send mail 8.12.10;也可以是一个比较大的类别,如:基于 Unix 系统的攻击。

(3) 第三维。其包括已存在并被攻击利用的弱点漏洞,弱点漏洞可能存在无限的分类问题,其没有结构化的分类;为了保持术语一致的原则,采用 CVE 的弱点漏洞定义。

(4) 第四维。其主要考虑攻击的额外代价(除开攻击本身)和负载。在大多数情况下,一种攻击能够明显区分和分类,但是在某些情况下,其带有其他的负载代价或影响,譬如,病毒可以在被攻击的机器上安装木马,其仍然是病毒,木马只是它的负载代价。

在分类的时候,针对每一个"维"度,必须将攻击尽可能的细分和具体,即每一"维"度能够具有最大的区分度。有必要的情况下,允许划分更多的"维"度,也可以减少"维"度,但是至少有第一个"维"度。

2.4 攻击分类法介绍

2.4.1 第一维

木马,则无法正确对蠕虫进行分类。若攻击的攻击矢量没有表现出来或者不好辨认,则将攻击的分类转向攻击是如何工作的。例如,某攻击在本地运行通过缓冲区溢出获取另一进程的控制权,那么将其划分为缓冲区溢出。

对没有明显攻击矢量的攻击进行分类,选择与下面匹配得最好的定义,将攻击划分为大类的同时也可能将其进一步划分为子类,第一维划分的情况如表 1 所示。

2.4.2 第二维

第二维涵盖了攻击目标,对于一个攻击其可能有多个攻击目标,即有多个入口。攻击目标的细分是一个关键点,若服务器 A 遭受到 DDOS(分布式拒绝服务)攻击,我们所要关心的不是服务器 A,而是服务器的操作系统和运行在操作系统上运行的服务。攻击目标包括硬件攻击目标、软件攻击目标、网络攻击目标。

硬件攻击目标分类三个类别:计算机、网络设备和外设。计算机目标包括计算机部件,如 CPU、内存、硬盘等;网络设备包括集线器、路由器、交换机等;外设如显示器等。

表1 第一维基于攻击矢量的分类结构

第一维攻击分类					
类 别			类 别		
病毒	文件感染		拒绝服务	基于主机	占用资源
	系统引导区感染				硬件破坏
	宏病毒			基于网络	TCP 泛洪
蠕虫	MassMailing				UDP 泛洪
	网络蠕虫				ICMP 泛洪
木马	逻辑炸弹			分布式	
缓冲区溢出	栈溢出		网络攻击	欺骗	
	堆溢出			会话劫持	
物理攻击	备破坏			无线攻击	WEP 攻击
	能量攻击	LERF		Web 应用攻击	跨站脚本攻击
		HER			
		FEMP			参数阻塞
	Van Eck				利用 Cookie
密码攻击	密码猜测	暴力破解			数据库攻击
		字典攻击			隐蔽性攻击
	直接攫取		社会工程学	获取重要信息	
信息收集攻击	嗅探	包嗅探			
	Mapping				
		安全扫描			

软件攻击目标分为两类:操作系统和应用程序。

网络攻击目标是对网络自身或者协议的攻击,如 Ping – Flood 攻击是对网络带宽的阻塞。

2.4.3 第三维

第三维主要涵盖了弱点和攻击所利用的漏洞。某攻击可能利用和挖掘多种弱点、漏洞,因此在第三维可能中有多个入口。第三维描述主要利用 CVE[8] (Common Vulerability and Exposure)库,由 Mann and Christy 提出的 CVE 现在已成为实际上的弱点、漏洞标准。已知的漏洞在 CVE 里面都有入口,如果是新的漏洞在 CVE 里不存在,则按照 Howard 提出的漏洞类型来分类:(1)实现上的漏洞(2)设计上的漏洞(3)配置方面的漏洞。

2.4.4 第四维

第四维主要处理攻击中存在的负载代价和附带的其他影响(除自身)。例如,蠕虫可能以木马作为负载代价,或可能损坏某些文件。若这些负载代价本身是另外一种攻击,则按照第一维为准。第四维主要包括以下 5 种类别(1) 第一维中攻击类别存在的负载代价(2) 信息损坏(3) 信息泄露(4) 窃取服务(5) 获取控制权。

2.4.5 其他的维

除了前面提到的四个维度,同时提出其他"维"来

更有效的进行攻击分类，主要包括以下几个方面：

（1）损害：度量损害的程度

（2）成本：度量攻击恢复的成本

（3）传播：度量复制、传播的速度，对于蠕虫和病毒的分类需要使用这个方面

（4）防御：从防御者的角度看

以上提到的四个方面，属于后攻击维度，即攻击发起后才会表现出这些潜在特征，使用这些特征能够将攻击分类做的更加具体、准确。

3　攻击归类的总结

按照以上提出攻击分类原则，对近几年新出现的网络攻击进行分类，并将部分归类结果给出（表 2），其

表 2　网络攻击归类图表

网络攻击分类结果				
攻　击	第一维	第二维	第三维	第四维
熊猫烧香（Nimaya）	蠕虫	EXE，ASP，JSP，PHP，	COM 文件	生成病毒文件
				病毒 spoclsv. exe
威金（Viking）	蠕虫	可执行文件，系统文件，注册表		生成病毒文件，病毒进程 logo1. exe
LAND	拒绝服务	Windows 95 and NT 4.0	CVE－1999－0016	占用资源
Banker（工行钓鱼木马）	社会工程学	应用程序	配置弱点漏洞	获取密码或相关重要信息
分布式拒绝服务（DDOS）	拒绝服务	Ms Windows NT 4.0，2000，XP，Server 2003	系统漏洞（多个 CVE 入口）	TCP、UDP、ICMP 包泛洪拒绝服务，占用资源
征途木马（Zhengtu）	木马	应用程序		盗取密码
Blaster	网络蠕虫	Ms Windows NT 4.0，2000，XP，Server 2003	CAN－2003－0352	TCP 包泛洪型拒绝服务
Code Red	网络蠕虫	IIS 4，5&6.0 beta	CVE－2001－0500	堆栈溢出
				TCP 包泛洪型拒绝服务
Chernoby	文件感染型病毒	MS Windows 95&98		信息损坏
Melissa	Mass－mailing 蠕虫	MS Word 97	配置弱点漏洞	宏病毒
		Word 2000		TCP 包泛洪型拒绝服务
Wuarchive FTPD	木马	Unix 系列		获取控制权
Slammer	网络蠕虫	MS SQL Server 2000	CAN－2002－0649	堆栈溢出
				UDP 包泛洪拒绝服务
Nimda	Mass Mailing 蠕虫	MS IE 5.5 SP1	CVE－2001－0333	文件型感染病毒，木马，拒绝服务
			CVE－2001－0154	
Sobig	Mass Mailing 蠕虫	E－mail 客户端	配置漏洞	

表示了从第一到第四维的归类状况，第二维只保留了最终的入口，另外有些入口也不完全，例如 Land Attack 的攻击目标 40 多种，这里只保留几种（但在创建攻击知识库的过程中已补充完整）。本归类法能够解决已有网络攻击分类的缺陷，如：前面提到的病毒和蠕虫中往往同时包含着特洛伊木马逻辑炸弹，可以根据用此归类法的第一"维"度和第四"维度"联合区分。

4 结束语

建立网络攻击知识库达到预期目标效果。但是，也有提高和改进的空间，有些原则也不能完全满足，需要提炼。

(1) 有些复杂、混合的攻击包含很多子攻击类别，不是分类多，而是这些复杂、混合的攻击如何描述和分析。未来的工作重点之一是需要提取详细的信息来处理此类攻击。

(2) 分类的目的是创建攻击知识库，当前和未来的攻击的量很大，必须考虑知识库的人工智能及自动学习功能，其能识别攻击之间的相互关系和对当前的攻击进行有效分析。可以采用一步一步的询问方式来实现。自动学习的方式进行有效的划分，分类的过程变得比较容易同时也减少了出错的几率。

(3)攻击分类法须更深入的分析。虽然前面提到此分类法的很多优点，但是后面的工作必须对此分类法进行严格、深入的划分，并且对大多数具有代表性的攻击进行分类，然后利用 AI 对其进行检测，这样就可以运用 AI 来添加和维护攻击知识库。

参考文献

1 BISHOP M. Vulnerabilities analysis [A]. Second International Symposium on Recent Advances in Intrusion Detection[C]. USA, 1999. 125 - 136.

2 KRSUL I. Computer Vulnerability Analysis[R]. The COAST Laboratory, Department of Computer Sciences, Purdue University, 1997.

3 CHRISTY J. Cyber threat & legal issues [A]. Shadowcon Conference[C]. USA, 1999.

4 HOWARD J. An analysis of Security Incidents on the Internet [D]. USA: Carnegie Mellon University, 1989 - 1995.

5 HOWARD J. An analysis of Security Incidents on the Internet[D]. USA: Carnegie Mellon University, 1997.

6 Daniel Lowry Lough. A Taxonomy of Computer Attacks with Applications to Wireless Networks. PhD thesis, Virginia Polytechnic Institute and State University, 2001.

7 刘欣然. 网络攻击分类技术综述. 通信学报,2004,25(7).

8 CVE. CommonVulnerabilitiesandExposures. 2003. http://www.cve.mitre.org/.