科技导报 2007 年 第 25 卷 第 7 期 (总第 229 期)

基于攻击分类的异构检测引擎构建技术

赵 蓓[1,2], 胡昌振[1]

1. 北京理工大学网络安全与信息对抗技术研究中心,北京 100081
2. 装备指挥技术学院信息装备系计算机应用技术教研室,北京 101416

[摘要] 由于攻击的复杂性,单一的检测技术难以具有全面的攻击检测能力。具有多检测引擎的入侵检测系统能够克服单一检测技术的检测局限性。但是目前的多检测引擎构建技术缺乏有关检测功能划分的理论指导。本文基于攻击的检测者观点,提出了基于检测特征的攻击分类方法,将攻击按照检测特征分为 5 个基础类。在此基础上,构建以攻击分类为基础的具有异构检测引擎的入侵检测系统框架。实验表明,该框架可以有效地检测各类攻击,并具有较好的变形攻击检测能力。

[关键词] 攻击分类;检测特征;异构检测引擎

[中图分类号] TP393.08 [文献标识码] A [文章编号] 1000-7857(2007)07-0005-05

A Detection-centered Classification of Network Attacks

ZHAO Bei[1,2], HU Changzhen[1]

1. *Network Security and Information Countermeasure Technology Research Center, Beijing Institute of Technology, Beijing 100081, China*
2. *Teaching Group on Computer Applications, The College of Equipment, Command & Technology, Beijing 101416, China*

Abstract: An intrusion detection system with multi detection engines could overcome the limitations of one with a single detection engine. But up to now, the methodology dealing with network attacks lacks theoretical guidelines for the partition of the inference function. From the detector's point of view, this paper proposes a detection-centered methodology dealing with network attacks. Network attacks can, therefore, be divided into five categories: character string attack, overflow attack, repeating attack, multi-step attack and multi-stage attack. An intrusion detection system with isomerous detection engines is built on that basis. Experiments show that it can avoid the deficiencies of existing detection methods.

Key Words: network attack classification; detection-centric; isomerous detection engine

CLC Number: TP393.08 **Document Code:** A **Article ID:** 1000-7857(2007)07-0005-05

0 引言

一直以来入侵检测系统的研究者都力图找到更加有效的攻击检测技术,而很少研究入侵检测技术自身的局限性。

网络攻击是极为复杂的活动,没有一种检测技术能够完成对所有类型攻击的检测。各种检测技术在检测某些攻击时表现出较高的检测能力,而对于某些攻击又会显得力不从心。如传统的两大类检测技术的基本原理,它们的检测范围就有很大的不同。误用检测技术只能检测出已知的攻击模式,对与已知攻击没有明显关联的新的攻击手段就无法做到正确报警。通过适当训练的异常检测技术,能够识别一些新攻击,但是它的学习功能容易被攻击者利用,使得入侵检测系统维护的轮廓偏离正常值,从而产生误警。

即使同属于某种检测技术类,不同检测技术对不同攻击类型的检测能力也有很大的差别。例如模式匹配技术和状态转移技术,状态转移技术是针对不断引起系统状态变化的多步骤攻击进行检测,而简单模式匹配就难以对这种攻击做出准确识别;但是简单模式匹配技术可以快速识别较为简单的攻击方式,而状态

收稿日期:2007-03-05

作者简介:赵 蓓,女,北京市海淀区中关村南大街 5 号北京理工大学网络安全与信息对抗技术研究中心,博士研究生,研究方向为入侵检测、人工智能;E-mail: Linda_zhaop@163.com

胡昌振(通讯作者),男,北京市海淀区中关村南大街 5 号北京理工大学网络安全与信息对抗技术研究中心,教授,研究方向为信息安全、智能识别

转移技术对于这类攻击检测的时间效率相对较低。

随着攻击日趋多样化和复杂化，单一的检测引擎很难做到对目标系统所有可能遭受的攻击进行全面的检测和防护。多检测引擎的入侵检测系统能够针对各类攻击分别进行检测，能够有效地提高入侵检测系统的检测率[1]。因此，合理有效地配置多种检测引擎，对于构造高效入侵检测系统具有特别重要的意义。

目前对检测引擎的功能划分主要基于应用服务和信息层次两种方式。Sekar 等[2]根据网络攻击利用的应用服务，对 TCP 攻击、UDP 攻击、FTP 攻击和 Web 服务器攻击使用不同的检测引擎分别进行检测。Giacinto 等[3]根据获取的攻击信息所包含的不同层次，将攻击信息进行特征抽取，分为固有特征、流量特征和内容特征。然后对不同的特征使用多个分类器检测攻击。Helmer 等[4]同时采用了应用服务和信息分层两种方式，将获取信息分为系统调用、登陆、TCP 连接等应用服务，同时把获取信息分为数据精简、低层和高层 3 个层次进行检测。

上述几种检测引擎的功能划分方法对提高入侵检测系统的检测攻击覆盖率和降低误警率都产生一定的作用。但是这些检测引擎都采用了相同的检测技术，因此存在以下两个方面的不足。

1）使用应用服务对检测引擎进行功能划分不能适应日益增加的服务种类。如果对各种应用服务分别建立检测引擎，势必使得入侵检测系统的服务线程直线上升，不利于入侵检测系统的实时性。

2）使用同构引擎不适合越来越复杂多样的攻击活动。攻击的多样性使得不可能使用一种“全能”的检测技术成功地完成对所有类型攻击的检测。

要解决上述两个问题，必须从科学的角度出发，对攻击进行适当的分类，并在此基础上进行检测引擎的功能划分。本文提出一种基于检测特征的攻击分类方法，并在此基础上建立了一种具有通用性的异构多检测引擎的入侵检测框架。实验表明，该框架能够较好地完成各种类别攻击的检测。

1 基于检测特征的攻击分类

1.1 攻击分类原则

Amorso[5]和 Lindqvist[6]等人认为一个科学合理的分类方法必须满足以下几点：互斥性、穷举性、无二义性、可重现性和可用性。其中，可用性是至关重要的。即使一个攻击分类方法能够完全满足前 4 项特性要求，但是如果不能够满足可用性的要求，那么这种攻击分类方法对入侵检测而言，不能够认为是一种科学合理的分类方法。

此外，一个完备的分类学应该满足的准则还应包括可接受性、一致性、客观性、决定性、可重复性和特异性。

1.2 检测者角度和入侵判别时机

目前对攻击的分类方法很多，但是大多数的攻击分类方法没有将检测者从其他安全角色中分离出来。即使同样处于目标位置，检测者和普通用户看待攻击的层次和重点也有很大差别，如表 1 所示。表 1 中没有将单独的一次攻击作为用户和检测者关注的对象，而是将系统所处的安全状态和趋势作为考察的重点。从表中可以看出，用户关注的重心是结果层面，而检测者关注攻击进行中的细节信息。

表 1 用户视角和检测者视角

Table 1 The views of a client and an attacker with respect to an attack

用户角度	检测者角度
是否有已经成功的攻击	是否有已经发生的攻击，该做出何种响应
攻击会造成什么样的后果	是否有可能发生的攻击，该如何收集证据，进一步对攻击进行监控
能否将影响降低到最低程度	攻击进行到何种程度，是否需要报警
攻击者是谁	攻击从那里发起，和以往的攻击是否有某种联系，攻击者未来可能采取哪些动作

如果入侵检测系统能够在攻击目标位达到之前就锁定攻击行为，将会为系统响应提供足够的时间。因此，识别时机是入侵检测性能的一个重要指标。但是对于某些攻击，如攻击信息是并行传到目标系统和入侵检测系统的检测机制的，此时入侵检测系统无法获得攻击成功前的准备信息，进而不能够做到攻击成功前识别。

1.3 攻击分类

根据对攻击做出识别的时间，攻击可以分为原子类攻击和复合类攻击。

1.3.1 原子类攻击

原子类攻击指在入侵检测系统不能获得任何先验信息的情况下，攻击者可以通过触发一个单独的安全事件完成的攻击。原子类攻击可以分为两类：字符串攻击和溢出类攻击。

1）字符串攻击，指那些无须在目标机器上作任何信息准备，直接键入特别的字符串或者发送一个特别的数据包，就可以成功的攻击。ASP 代码泄漏漏洞攻击就是通过在远程输入的 Web 地址后加入特定的字符串获取系统权限。对这类攻击的检测只能通过加强字符串的智能识别能力提高检测效率，做到攻击成功后报警。

2）溢出类攻击，指利用缓冲区溢出漏洞和边界溢出漏洞进行的权限提升攻击。事实上，许多溢出类攻击都有字符串攻击的特征，通过输入特别的字符串一次完成攻击。但是由于溢出攻击是在程序的地址空间完成，通过暴力改写程序指针，达到攻击的目的，对这类攻击的检测可以通过对程序地址空间的实时监测完成，因此将这类攻击特别地归为一类。

1.3.2 复合类攻击

复合类攻击指攻击者必须通过多次触发安全事件才能达到攻击目的。根据多次触发的安全事件相互之间的关系，复合类攻击可以分为重复性攻击和非重复性攻击。

1）重复性攻击，指攻击者对目标系统进行反复的同一或类似动作，以达到攻击目的。这类攻击从开始攻击到攻击目标实现是一个渐变过程，而且在渐变过程中系统的变化无法以明确的状态描述并加以界定。此类攻击中，除了少量的口令猜测攻击，绝大多数都是通过反复发送网络畸形包消耗系统资源的拒绝服务攻击。

2）非重复性攻击，指在攻击最终目标完成之前，攻击必须具备若干前提，并且这些前提可以通过目标系统所处的不同状态加以区别。非重复性攻击根据所取得前提的类型，可以分为多步攻击和多阶段攻击。多步攻击是指攻击成功前取得的前提条件都属于系统的合法操作或输入；多阶段攻击是指攻击成功前取得的前提条件中有已成功的攻击。

1.4 分类方法试验验证

为了验证基于检测特征的分类方法，本文使用了卡内基梅隆大学（Carnegie Mellon University）计算机工程研究所的计算机应急反应/协作中心（Computer Emergency Response Team/Coordination Center，CERT/CC）和美国国家标准研究所维护的英特网攻击技术目录（Internet Catalog of Assailable Technologies，ICAT）的相关数据作为研究对象。

ICAT 库中包含的 7 426 条相关漏洞记录，分别根据漏洞的严重性、损失类型、漏洞类型和受威胁系统收录。由于 ICAT 中的分类方法并不满足互斥性，因此实际研究中使用的攻击方法只有针对 6 919 个漏洞的 7 168 条攻击。

CERT/CC 自 1985 年创建以来收录了 327 条漏洞，共有 391 条攻击。所有的这些都被本文用于研究。使用基于检测特征的攻击分类方法的分类结果见图 1。

攻击类别	数目
字符串	2 271
溢出类	1 673
重复类	1 223
多步	1 927
多阶段	74
合计	7 168

攻击类别	数目
字符串	76
溢出类	134
重复类	109
多步	65
多阶段	7
合计	391

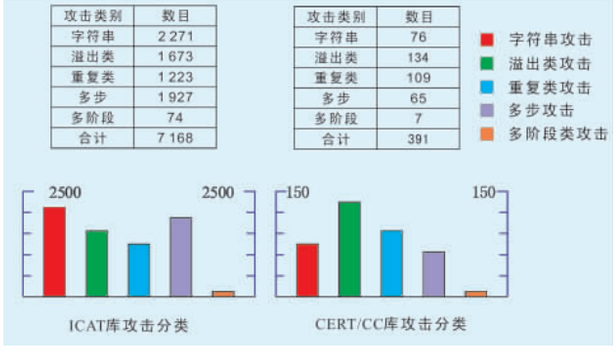

图 1 ICAT 和 CERT/CC 库攻击分类

Fig. 1 The classification of attacks on ICAI and CERI/CC based on detection characteristics

2 具有异构检测引擎的入侵检测系统框架

根据基于检测特征的攻击分类方法，所有的攻击可以根据其检测特性分为 5 个基本类别。如果能够针对每个类别的攻击方法的本质特征分别进行检测，必将最大程度地利用各种现有技术对各种类别攻击的检测优势，从而提高入侵检测系统的检测效率。

本文提出了一种具有通用性的分布式多检测引擎入侵检测系统框架。图 2 为异构检测引擎的框架示意图。该框架中，5 类攻击分别由不同的检测引擎完成，每类攻击的检测引擎可以根据该类攻击的特点对检测方法进行定制。

如图 2 所示，字符串攻击检测引擎、多步攻击检测引擎和重复性攻击检测引擎的输入来自预处理模块，预处理模块根据分发策略将获取的主机和网络信息分别发送给这三个检测引擎。分发策略分为两部分，一部分是预先设定的；另外一部分是各个检测引擎根据检测过程中的实际情况，向预处理模块实时发送的。

溢出类攻击是在目标系统地址空间发生的攻击，对地址空间的监控是最为有效的检测方法。因此溢出类攻击检测引擎不需要入侵检测系统获取的信息。

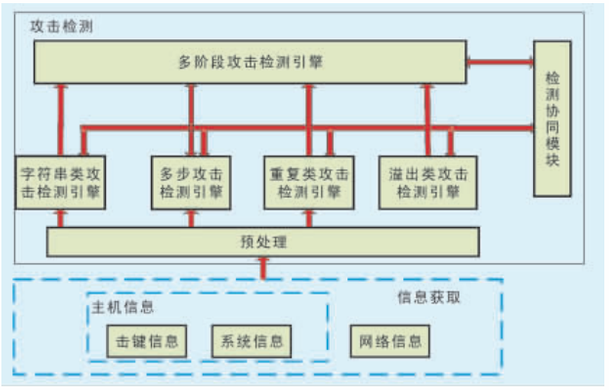

图 2 基于攻击为中心的攻击分类方法的检测框架

Fig. 2 The detection framework based on attack–centered classification

多阶段攻击检测引擎需要获取的报警信息中不仅包括监测主机的攻击报警信息，还包括监测主机的信任网络中其他主机的报警信息。多阶段攻击检测引擎对这些报警信息进行关联，检测可能发生的多阶段攻击。如果多阶段攻击的某些步骤是针对其他主机进行的，多阶段攻击检测引擎通过检测系统模块向信任网络发出广播信息。如果多阶段攻击中有的攻击步骤不是已完成的攻击，而是对目标系统的某种状态的改变，多阶段攻击将这些步骤以检测任务的形式发送给多步攻击检测引擎。多步攻击检测引擎将检测任务的执行结果报告给多阶段检测引擎。

检测协同模块负责多阶段攻击检测协同检测任务和报警信息的广播和分发。对于需要其他信任主机协同检测的多阶段攻击步骤，多阶段检测引擎通过检测协同模块在信任网络中广播。检测协同模块同时监听

信任网络中其他协同模块的广播，并且将任务分发给相应的检测引擎。

攻击报警格式和协同检测任务使用统一的消息格式，由以下的 6 元组表示

Attack={Attackstat, AttackID, Hyperattack, Intruderproperties, Networkproperties}

Attackstat 表示攻击的状态，即攻击报警或协同检测任务；AttackID 表示攻击编号，同时可以说明攻击的类型；Hyperattack 表示发布信息的多阶段攻击检测引擎认为该攻击涉及的多阶段攻击名称；Intruderproperties 表示入侵者的相关属性信息；Networkproperties 表示相关网络属性信息。

3 原型系统与实验验证

本文在 Micorsoft Windows XP 的环境下使用 Sun´s Java Development Kit 软件仿真实现了一个异构检测引擎的原型系统。系统中各检测引擎使用的检测方法如下。

字符串类攻击检测引擎，用于检测通过直接键入特别的字符串或者发送特别的数据包就可以完成的攻击。这类攻击检测的难点在于攻击者针对入侵检测系统采取的躲避技术。本文采用了能够有效识别各种字符串躲避攻击的检测技术[8]进行检测。

重复类攻击检测引擎，主要用于检测通过发送网络畸形包耗费系统资源，从而达到使服务器不能响应某些或全部服务请求的攻击。通过对这些网络畸形包的研究，分别针对不同的特征属性，采用分形的方法来识别攻击[9]。

溢出类攻击检测引擎，主要检测通过利用缓冲区溢出漏洞达到权限提升目的的攻击。基于溢出类攻击暴力改写程序指针的特点，通过对堆栈指针的监视达到检测攻击的目的[10]。

多步攻击检测引擎和多阶段攻击检测引擎，所检测的两类攻击同前几类攻击有很大不同。本文采用基于先决条件的关联方法[11]，通过比较先发生报警信息行为的结果和后发生报警信息行为的先决条件对两个报警信息进行关联，完成攻击的识别。入侵的先决条件指一次入侵取得成功的必须条件，结果指一次攻击成功后所产生的结果。这种方法能够准确而灵活地对非重复性复合攻击的攻击步骤信息进行关联，并且不需要给出固定的报警序列，可以适应攻击者变化的攻击模式。

由于攻击分类方法的不同，实验中没有采用通用的攻击数据库。在 CERT/CC 漏洞库中，本文使用其中的 82 条攻击方法，通过攻击变形将其扩展为 342 个。在实验中，首先对两台配置有信息获取代理的 RedHat Linux 8.2 主机发动攻击，信息获取代理将收集到的信息记录下来，然后将异构检测引擎分别配置在两台操作系统为 Micorsoft Windows XP 的主机上。经过同步调试后，启动两个检测系统读取攻击信息进行处理。首先使用原始的 82 条攻击，然后每次测试增加 50 条攻击，直至使用了全部的 342 条攻击。图 3 为分别选取攻击数为 82，191 和 342 的实验结果绘制 ROC 曲线图。实验结果表明，异构检测引擎对变形攻击具有较好的检测能力。

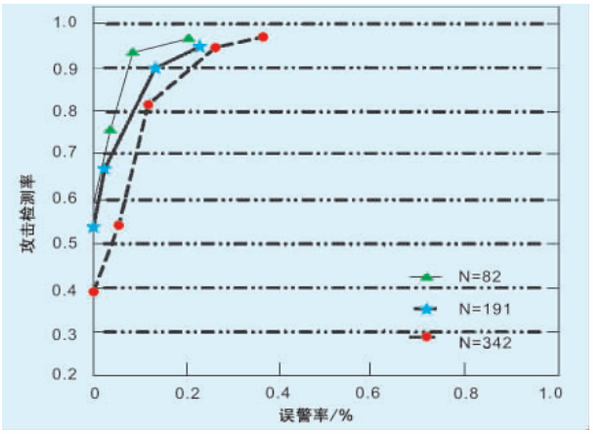

图 3 变形攻击实验

Fig. 3 Diversified attack experiments

4 结束语

网络攻击的分类方法直接影响入侵检测系统对攻击的描述和识别，本文依据攻击在检测方面的本质特征，提出了基于检测特征的攻击分类方法，并以该分类方法为基础，构建了具有异构引擎的入侵检测系统框架。该框架中对每一基础类攻击使用专门的检测技术，这种框架结构主要有两方面的优点：① 可以利用各种现有攻击检测技术的优点，对各个类别的攻击采用“各个击破”的策略；② 对于具有高度复杂性的多阶段攻击，采用分布分析报警的方式，更有利于提高攻击的检测率和系统的抗攻击性。通过实验验证表明该方法切实可行，并且起到使各种攻击检测方法扬长避短的作用。下一步的工作是进一步研究各个基础类攻击的检测特征，研究出更加高效的检测算法，同时，各检测引擎如何更加协调地配合多阶段攻击检测，也是进一步研究的方向。

参考文献 (References)

[1] BALASUBRAMANIYAN J S, GARCIA-FRENANDEZ J O, ISACOFF D, *et al*. An architecture for intrusion detection using autonomous agents [R]. Purdue University, West Lafayette: Technical Report TR 98-05, 1998.

[2] SEKAR R, GUANG Y, VERMA S, *et al*. A high-performance network intrusion detection system[C]//ACM Conference on computer and communications security, Nov. 2-4, 1999, Singapore. ACM Press, 1999: 8-17.

[3] GIACINTO G, ROLI F. Intrusion detection in computer networks by multiple classifier systems [C]//Proceedings of the 16th International Conference on Pattern Recognition (ICPR), Quebec, Canada. IEEE Press, 2002, 2:11-15, 390-393.

科技导报 2007 年 第 25 卷 第 7 期 (总第 229 期)

攻防对抗环境下的网络安全态势评估技术研究

姚淑萍

北京理工大学计算机网络攻防对抗技术实验室,北京 100081

[摘要] 为了弥补当前网络安全态势评估系统的不足,提出了一种基于攻防对抗环境的网络安全态势量化评估算法。该方法在深入分析影响安全态势各项因素的基础上,将传统的风险评估与网络防护状况、资产安全特性等环境因素相结合,提取出多个量化指标,按照攻击类别进行安全态势的量化评估。实验结果表明,该方法能够为安全管理人员提供更为客观、详实的态势信息,使之更为清晰地把握整个网络的安全状况。

[关键词] 攻防对抗;网络安全;态势评估

[中图分类号] TP393 [文献标识码] A [文章编号] 1000-7857(2007)07-0009-04

Research on Network Security Evaluation Technology Based on Attack-defense Confrontation

YAO Shuping

Laboratory of Computer Network Defense Technology, Beijing Institute of Technology, Beijing 100081, China

Abstract: In order to improve the current network security evaluation systems, a novel evaluation algorithm, called the quantitative network security evaluation based on attack-defense confrontation, is proposed in this paper. In this algorithm, the traditional risk assessment is combined with network environment factors such as the network running status, asset security characteristics and so on, and several quantitative indexes are extracted based on the analysis of factors which can affect the LAN's security situation. Then, evaluations are made based on a classification of attacks. Experiment results show that the novel algorithm can be used to

收稿日期: 2007-03-06

作者简介: 姚淑萍,女,北京市海淀区中关村南大街 5 号北京理工大学计算机网络攻防对抗技术实验室,讲师,研究方向为信息安全;
E-mail: yaosping@163.com

[4] HELMER G, WONG J, HONAVAR V, *et al*. Automated discovery of concise predictive rules for intrusion detection[J]. J Systems and Software, 2002, 60(3): 165-175.

[5] GLASS R L, VESSEY I. Contemporary application-domain taxonomies[J]. IEEE Software, 1995, 12(8): 906-916.

[6] AMOROSO E G. Fundamentals of computer security technology[M]. USA: Prentice-Hall PTR, 1994.

[7] FAN Jang-Jong, SU Keh-Yih. An efficient algorithm for match multiple patterns[J]. IEEE Trans on Knowledge and Data Engineering, 1993, 5(2): 339-351.

[8] 赵 蓓, 胡昌振. 基于有限自动机的躲避攻击快速检测技术[J]. 计算机应用研究, 2006, 23: 973-974.
ZHAO Bei, HU Changzhen. Effcient algorithm for detection evade IDS attack based on finite state automata [J]. Application Research of Computers, 2006, 23: 973-974.

[9] 邢江宁, 张炜, 张铁军, 等. FPW 对缓冲区溢出的实施检测[J]. 小型微型计算机系统, 2004, 25(4): 151-152.
XING Jiangning, ZHANG Wei, ZHANG Tiejun, *et al*. FPW detects buffer overflow in realtime[J]. Mini-Microsystems, 2004, 25(4): 151-152.

[10] LINDQVIST U, JONSSON E. How to systematically classify computer security intrusions [C]//Proceedings of the 1997 IEEE symposium on security and privacy, oakland, USA, May, 1997. IEEE Press, 1997: 154-163.

[11] TEMPLETION S J, LEVITT K. A requires/provides model for computer attacks [C]// Proceedings of the 2000 new security paradigms workshop. Cork, Ireland: ACM Press, 2000: 31-38.

(责任编辑 赵 佳)