第32卷 第14期 计 算 机 工 程 2006年7月
Vol.32 № 14 Computer Engineering July 2006
·安全技术· 文章编号：1000—3428(2006)14—0130—03 文献标识码：A 中图分类号：TP393.08

基于入侵意图的报警信息关联分析技术

史 亮，王备战，姚俊峰
(厦门大学软件学院，厦门 361005)

摘 要：针对目前报警信息关联技术中存在的问题，提出了基于入侵意图的报警信息关联分析技术。该技术不仅继承了基于入侵策略的报警信息关联分析方法所具有的时效性、预见性强等优点，而且提高了入侵策略模型的泛化能力，并通过建立“跳步”分析机制，提高了系统对入侵的理解能力。

关键词：入侵检测；报警信息关联分析；入侵策略模型

Alerts Information Association Analysis Technology Based on Intrusion Intention

SHI Liang, WANG Beizhan, YAO Junfeng
(Software School, Xiamen University, Xiamen 361005)

【Abstract】 This paper presents an alerts association analysis technology based on intrusion intention in order to overcome the problems exited in today's alerts association analysis technologies. This method not only inherits the merits of the alerts association analysis technology based on intrusion strategy such as foreseeable, but also improves the adaptability of the intrusion strategy model. Furthermore, it gives the "skipping step" analysis mechanism and its improvement on the comprehension ability of the intrusion detection system.

【Key words】 Intrusion detection; Alerts information association analysis; Intrusion strategy model

1 概述

传统的入侵检测系统往往注重于低层面的入侵和异常活动并独立地产生报警，而忽视了这些报警信息之间可能存在的内在联系以及报警背后所反映的问题，导致系统对报警信息的处理能力和对入侵的理解能力较差[1]。如何提高入侵检测系统对报警信息的关联分析能力，已经成为入侵检测领域中的一个重要的研究方向。

报警信息关联分析是根据来自系统内部不同入侵检测模块所产生的报警在特征上的相似性、在逻辑上的相关性，从系统的整体角度对分布式、阶段性入侵进行分析的过程。其目的是通过对各种报警信息的关联，构造入侵方案，从而使我们可以更准确地把握入侵的发展动向，提高对入侵的分析能力。目前报警信息关联分析技术可以划分成3大类。

(1)以文献[2,3]所提出的技术思路为代表。其特点是根据报警信息在相关属性上的相似性来进行关联。该技术对于某些类型的报警信息的关联分析比较有效，但不能很好地揭示报警信息之间的内在联系。

(2)以 Requires/Provides 模型[4]提出的 Prerequisites and Consequences 模型[1]为代表，该技术根据不同入侵步骤之间的服务与被服务关系，将隶属于同一入侵方案中的多个报警信息按合理顺序关联在一起。这种关联分析方法具有较大的灵活性，可以揭示报警信息之间的内在联系，指明入侵者所采取的入侵路线，并且具有发现未知入侵模式的能力。但是该方法对来自底层的报警信息的依赖性较强，如果某些关键入侵步骤没有被发现，那么新获得的报警信息和原先获得报警信息之间的关联分析将变得困难，虽然根据服务与被服务原则可以将某些在顺序上存在间隔的报警信息关联在一起，但是没有对隐藏在这些现象背后的有关入侵者、入侵进度和系统安全状况的信息进行分析。

(3)关联分析技术以入侵策略分析模型[5]为代表，该技术根据对入侵者入侵策略的研究，建立入侵策略模型，并根据所获得入侵报警信息，确定入侵者所采取的入侵方案，推测入侵者真正的目的和下一步将要进行的入侵行动，从而有可能在入侵者达到其目的之前对其采取相应的措施。同前两种方法相比，这种方法能更好地揭示报警信息之间的内在联系，具有更好的时效性和预见性，提高了系统对入侵的理解能力和控制能力。但是，这种利用攻击类型表述的入侵策略的泛化能力较弱，在进行关联分析时，某个步骤是否完成是以策略中对应位置所给出的入侵是否被证实已经完成为依据的，如果入侵者采用可以实现相同目的的不同攻击方法，即使实现了预期目标，在关联分析时系统也会因为没有发现预定攻击而误认为该步骤尚未完成。而且，该方法对于报警信息中存在“跳步”现象的问题没有给出具体的解决方案。这里“跳步”是指：从所获得的报警信息来看，入侵者不按入侵方案中攻击步骤的次序进行下一步攻击，而是跳过部分步骤直接进行后续攻击。

针对目前报警信息关联分析技术所存在的不足，本文提出了一种基于意图分析的报警信息关联分析方法，该方法在

基金项目：厦门大学“985”二期信息创新平台基金资助项目；厦门大学引进人才科研启动基金资助项目

作者简介：史 亮(1973—)，男，博士、讲师，主研方向：智能信息处理与网络信息安全；王备战，博士、副教授；姚俊峰，博士后、副教授

收稿日期：2005-12-12 **E-mail**：sliang@xmu.edu.cn

分析思想上与第 3 类关联分析方法相似，不同的是，我们用反映入侵者在不同步骤处意图的入侵目标取代具体的入侵类型，采用一种基于攻击流的表述方式来对入侵策略模型进行描述。这种基于意图的报警信息关联分析技术不仅继承了第 3 类关联分析方法所具有的时效性、预见性强等优点，而且提高了入侵策略模型的泛化能力。并通过建立“跳步”分析机制，提高了系统对入侵的理解能力。

2 入侵策略模型

众所周知，为了达到入侵目的，入侵者需要采取一系列的攻击步骤。在一个入侵方案中，不同攻击步骤的发生次序是具有规律性的，我们可以利用这种入侵步骤的规律性来构造入侵检测方案，从而可以更准确地把握入侵的发展动向，提高对入侵的分析能力。

入侵策略模型是根据入侵者为了达到某种目的所采取的一系列有规律性的攻击步骤所建立起来的、反映入侵者意图的一种表述模式。这里用一种基于攻击流的表述方式来对入侵方案进行描述，其基本表述单元如图 1 所示。其中，每个单元节点表示入侵者在该阶段所期望实现的攻击目标，单元与单元之间的箭头方向表示目标实现上的先后顺序，Shortcut_ij(其中 i,j=1,2,…,n)表示单元 i 到单元 j 间可能出现的“跳步”现象。

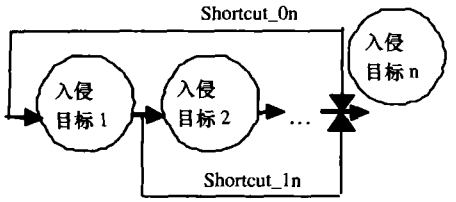

图 1 基于攻击流入侵方案描述方法中的基本描述单元

在利用攻击流描述的入侵策略模型中，我们用入侵目标表示模型中的单元节点，这就是意味在关联分析时，判断入侵策略模型中某个步骤是否实现的依据不再局限在某个或某种入侵方式是否被实施，而是在于入侵者是否已经通过某种途径达到其在该步骤处期望达到的目的。这种方法可以使整个入侵方案的设计更具有普遍性，降低了由于入侵者通过调整攻击手段，导致其产生的报警信息无法同已知信息进行正确关联的风险。并且这种入侵策略模型也为分析诸如“跳步”现象等问题提供了技术基础。

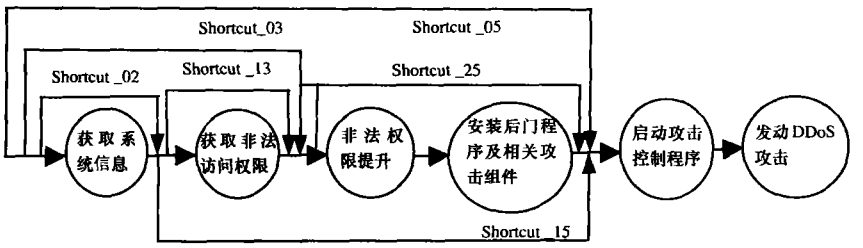

图 2 完成一次分布式拒绝服务攻击的入侵方案

比如入侵者希望对某个主机发动分布式拒绝服务攻击，那么他就可以通过以下步骤来逐步达到他的目的：

(1)信息采集，查找系统可能存在的安全漏洞；

(2)对于存在问题的主机，利用发现的安全漏洞，获取系统的访问权限；

(3)进行非法权限提升；

(4)安装后门程序、DDoS 控制程序和 DDoS 攻击程序；

(5)获取足够网络资源；

(6)通过 DDoS 控制端启动驻留在其它被渗透主机上的 DDoS 攻击程序；

(7)对目标主机进行 DDoS 攻击。

针对这种入侵方案，我们可以利用基于攻击流的表述方式对该方案进行描述，图 2 给出了具体的描述方案。

3 关联分析技术

3.1 对新的报警信息的关联原则

现在我们来分析一下根据基于攻击流的入侵策略对报警信息进行关联分析的基本原则。当接收到一条新的报警时，分析引擎将根据新报警信息中各属性的具体值，在已获得的多个入侵方案实例中查找具有相似特征的入侵实例，如具有相同的目标 IP 地址等，并根据匹配结果分两种情况来确定其关联方式：

(1)如果匹配，那么首先根据报警所描述的入侵类型来确定该入侵的目的，然后根据入侵目的，结合与该报警相匹配的一个或多个入侵实例，来推测入侵者的所采取的入侵方案，从而进一步确定哪些入侵实例更符合入侵者的入侵策略，并找到在这些入侵实例中新报警信息所反映的攻击步骤的具体位置。

(2)如果不匹配，那么将为其产生新的入侵实例。同样，首先要确定该报警信息所描述的入侵的目的是什么，然后根据入侵目的，在入侵方案中查找具有该入侵环节的一个或多个方案。对于那些满足条件的方案，将各产生一个新的入侵实例，这些实例分别反映了分析系统对入侵者所采取的入侵策略的推测。最后，在这些入侵实例中确定新报警信息所反映的攻击步骤的具体位置。

3.2 对存在“跳步”攻击现象的处理

下面我们来分析一下对如何处理在入侵实例中存在的“跳步”现象。现有关联分析技术在遇到这一类问题时，要么导致关联分析无法正常进行，要么系统依据新的攻击与已检测到的入侵之间是否满足服务与被服务条件来确定是否关联，而对于为什么会出现“跳步”攻击的原因和该现象背后所反映的问题没有加以分析。

对于“跳步”攻击的处理方法来说，最简单的方案是假定被“跳过”的攻击已经被实施。应该说这种假设思想是有一定现实意义的，这是因为攻击步骤是否实施，其证据完全依赖于该攻击活动是否被底层 IDS 所发现，如果入侵者采用一种比较隐蔽的手段，比如利用新的系统漏洞或依靠非技术手段，使得入侵者可以利用不触发报警的方法来到达攻击目的，这时对被跳过步骤的已实现假设是合乎情理的。但是，在处理“多跳步”(多个步骤的实现情况未被证实)和一些关键步骤被跳过的情况时，这种假设就显得比较牵强，并且这种假设方法在某种程度上忽视了“跳步”现象所反映出来的有关入侵和入侵者的信息。

从入侵者的角度分析，为了实现入侵的最终目标，入侵者会充分利用一切可用信息和手段，以尽可能小的代价(时间开销、被发现的概率以及攻击的成功率等因素)来完成任务。基于这种低风险原则的认识，我们认为，由于入侵者入侵所产生的报警信息，无论入侵的结果是成功还是失败，无论在入侵步骤上是否存在“跳步”现象，报警信息本身都从一个侧面揭示了入侵者的入侵能力和对系统的了解程度等相关信息，这为分析入侵、控制入侵提供了分析依据。在我们所提

出的基于意图分析的报警信息关联分析方法中，对于那些被认为是“跳步”攻击所产生的报警信息，其处理方法为：

(1)根据“跳步”攻击的入侵目的，确定其在入侵实例中的位置，并将该单元(假定为 J)设置为已实施；

(2)将入侵实例中连接上一个已实施单元(假定为 I)与单元 J 的条件通道设置为攻击流的流动通道，将 Shortcut_ij 设置为“短路”；

(3)根据 Shortcut _ij，给出对当前入侵的分析。为每个入侵策略模型建立“跳步”攻击分析表，通过查表方式获得该入侵策略中对各个 Shortcut _ij 的分析结果及应当采取的对策。

对“短路”原因的推断是建立在入侵者所遵循的低风险原则的基础上的。这里以图 2 所示的入侵策略中 Shortcut_13 的“短路”现象为例来看一下如何根据“跳步”攻击来对入侵进行分析。Shortcut_13 表示从报警信息来看，入侵者在完成对系统的信息探测之后，在没有进行对某个主机的非法渗透攻击的情况下直接对该主机进行了非法权限提升攻击，除了“入侵者从其它位置上发动攻击”和“入侵者采取较为隐蔽的入侵手段”等一般可以想到的原因之外，我们认为还存在以下几种可能的推断：

(1)入侵者对系统的先验知识不足。正因为如此，入侵者才被迫冒着被发现的风险对系统进行信息的探测；

(2)系统本身可能存在安全漏洞。如果在信息探测中发现了系统内部所存在的安全漏洞，本着低风险原则，入侵者极有可能会利用了该漏洞，以合法身份登录到主机 A 上，并直接进行下一步的非法权限提升攻击。

4 实验结果与分析

实验中，采用的是 DARPA 2000 提供的测试样本——Lincoln Laboratory Scenario(DDoS) 1.0[6]。该入侵样本中包含了入侵者为发动 DDoS 攻击所采取的步骤，这些攻击信息被划分成 5 个阶段：探测，获取非法访问权限，安装用于拒绝服务攻击的 Server 端程序并发动拒绝服务攻击，这同我们所设计的 DDoS 的入侵策略模型基本吻合。

为了模拟实际的攻击现场，用 NetPoke[7]来完成数据包的重发过程。用文献[8]中所提出的方案来进行底层检测，并将其产生的报警结果作为输入供高层分析模块进行关联分析。

在高层分析端，其分析机制主要依据前面所提出的技术方案来实现。除了入侵策略第 1 阶段以外(第 1 阶段对应信息探测，在实际检测中，其可能的后续步骤有许多种选择)，每当发现新的入侵进展情况，系统都会给出入侵的发展动向，并对存在跳步攻击的情况给出分析结果和对策。

由于在实验所采用的样本数据所反映的入侵过程中，入侵者在对主机进行渗透攻击时，针对该主机上的安全漏洞(运行 sadmind 服务)采用了基于该漏洞的远程缓冲区溢出攻击，成功获取了该主机的 Root 权限，所以高层分析模块在实际分析时并没有发现非法渗透攻击。因此当发现权限提升攻击时，关联分析模块在给出报警和下一步攻击预测的同时，也对存在跳步的情况给出了相应的分析结果。图 3 给出了由记录的实验结果所绘制的入侵者整个攻击的实施方案，该方案同 LLS-DDOS-1.0-inside 样本数据的介绍资料所给出的入侵方案基本吻合。

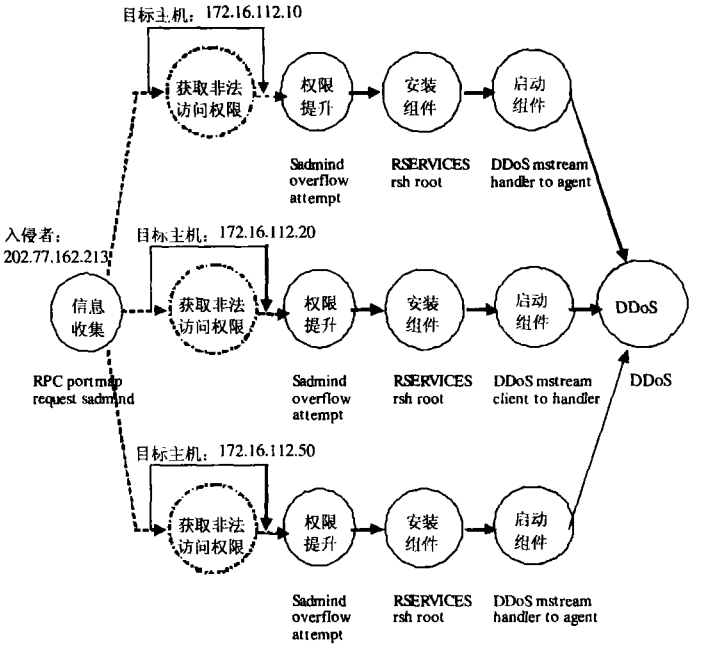

图 3 LLS-DDoS-1.0 inside 样本数据中入侵者的攻击方案

5 结束语

本文中，针对目前报警信息关联技术中存在的问题，提出了基于入侵意图的报警信息关联分析技术。该技术不仅继承了基于入侵策略的关联分析方法所具有的时效性、预见性强等优点，而且提高了入侵策略模型的泛化能力。并通过建立“跳步”分析机制，提高了系统对入侵的理解和监控能力。

由于报警信息关联分析技术是建立在底层报警信息和入侵策略模型的基础上，因此其分析的准确性和效率很大程度上依赖于底层检测系统和相关入侵策略模型是否可靠、准确。如何提高底层 IDS 检测的可靠性，如何从实际攻击样本中发掘出入侵者的策略，从而使所建立的模型更合理，这些工作将是我们下一步的研究方向。

参考文献

1 Ning P, Cui Y, Reeves D S. Constructing Attack Scenarios through Correlation of Intrusion Alerts[C]. Proceedings of the 9th ACM Conference on Computer & Communications Security, Washington D.C., 2002-11: 245-254.

2 Valdes A, Skinner K. Probabilistic Alert Correlation[C]. Proc. of the 4th International Symposium on Recent Advances in Intrusion Detection, 2001: 54-68.

3 Dain O, Cunningham R. Fusing A Heterogeneous Alert Stream into Scenarios[C]. Proc. of the ACM Workshop on Data Mining for Security Applications, 2001-11: 1-13.

4 Templeton S, Levit K. A Requires/Provides Model for Computer Attacks[C]. Proc. of New Security Paradigms Workshop, 2000-09: 31-38.

5 Huang M Y. A Large Scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis[J]. Computer Networks, 1999, 31(23/24): 2465-2475.

6 LLS_DDOS_1.0[Z]. http://www.ll.mit.edu/IST/ideval/data/2000/LLS_DDOS_1.0.html.

7 DARPA2000[Z]. http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_index.html.

8 史 亮, 庄镇泉. 一种基于入侵事件的检测分析技术[J]. 计算机工程与科学, 2005, 27(8): 13-15.