

基于攻击效用的复合攻击预测算法

陈 灿^{1,2}, 阎保平¹, 李 俊¹

(1 中科院 计算机网络信息中心, 北京 100190; 2 中国科学院 研究生院, 北京 100039)

摘 要: 网络攻击以复合攻击形式为主, 但当前的安全设备只能检测无法预测, 针对这个问题, 提出了一种基于攻击效用的复合攻击预测方法, 通过该方法识别攻击者的最终意图, 预测攻击者下一步可能进行的攻击行为. 该方法利用攻击意图描述复合攻击过程, 建立了基于攻击意图的复合攻击逻辑关系图, 并引入攻击效用的概念, 表示入侵者在攻击过程中完成每步攻击所获得的收益的大小, 是复合攻击预测的重要参考. 最后, 通过实验验证了该方法的有效性.

关键词: 攻击预测; 复合攻击; 攻击意图; 攻击效用

中图分类号: TP31

文献标识码: A

文章编号: 1000-7180(2011)03-0081-04

Forecast Algorithm for Multi-step Attack Based on Attack Utility

CHEN Can^{1,2}, YAN Bao-ping¹, LI Jun¹

(1 Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China;

2 Graduate School of the Chinese Academy of Sciences, Beijing 100039, China)

Abstract: This paper presents an approach based on attack utility to recognize the attacker's finally intention and forecast the next possible attack. This paper describes a multi-attack by the attack intent, and establishes the multi-attack the logic diagram based on the attack intention. During the procedure of the attack forecast, attack utility is used to represent the attackers benefit for each attack step. The attack utility is an important reference for the multi-step attack forecast. At the end, the validity of the algorithm is proved by the experimental results.

Key words: forecast attack; multi-step attack; attack intention; attack utility

1 引言

近几年的统计分析显示, 对网络攻击事件的防范已经成为一个亟待解决的问题, 入侵检测与预警系统作为保障网络安全的重要设施已成为研究的焦点.

复合攻击的攻击行为之间表现出规则的行为流动, 各攻击行为之间存在串联、并联、并发的关系. 一个攻击行为发生的前提往往是需要当前的目标网络和主机处于一定的状态, 满足一定的条件. 同时, 一个攻击行为发生以后, 必然会产生一定的结果和系统局部状态的改变等等, 所以需要一个很好的模型来描述这些攻击行为之间以及攻击行为与系统状态之间的关系. 主要的模型^[1-6]有扩展的有向图、CPN、

CTPN、知识规划图和隐马尔可夫模型等, 这些模型各有优缺点. 目前并没有一个比较完善实用的模型来进行复合攻击的预测.

2 复合攻击的定义

攻击是尝试破坏资源完整性、保密性和可用性的行为集合. 当攻击行为具有独立的、不可分解的攻击目的时, 称其为单步攻击. 而复合攻击则是将单步攻击按照一定逻辑关系进行排列, 在特定的时间和空间中形成一个攻击序列, 从而达到仅用单步攻击无法实现的目的.

在复合攻击中, 两个相关联的单步攻击可能会有以下逻辑关系:

- 依赖关系: 一个单步攻击的成功是另一个单

步攻击实施的前提条件;

- 并列关系:多个单步攻击以任意次序全部成功,才是另一个单步攻击实施的前提;
- 选择关系:多个单步攻击中任意一个成功实施,即为另一个单步攻击创造了前提.

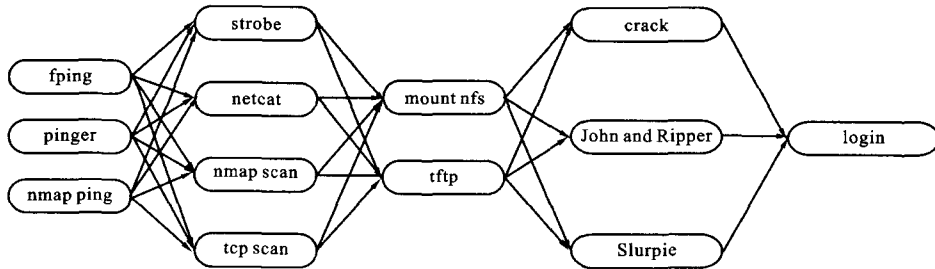


图1 复合攻击示意图

3 攻击效用的定义和计算方法

攻击者每次发动攻击都是为了某种利益的最大化,而又希望承担最小的风险.为此,提出攻击效用的概念,表示攻击者在完成某步攻击后所获得的收益的大小,这里收益可以指经济利益和某种心里满足等.为攻击效用设定两个方面的制约:攻击行为本身和被攻击系统的安全状态.

攻击效用 $w(v_i)$ 受到攻击本身和目标系统两方面的制约.

(1) 来自攻击本身的制约,在 Stuart McClure 的研究中,给出的一种对攻击危害的评估方法,从这三个角度进行评估攻击:攻击的流行度(popularity)、攻击的易用度(simplicity)和攻击的影响度(impact),综合这三者,给出一个综合风险指数,取值在 0 到 10 之间,并且给出了相应攻击的具体数值.

(2) 来自目标系统的制约

① 目标系统的脆弱性,表示目标系统受到攻击的频率,如果频率越高,它的脆弱性越高,攻击者得到的攻击效用就越大.取值在 0 到 10 之间,把它分为四个等级 1~4,对应的取值为 10,8,5,2.

② 攻击与目标系统的相关度,安装在目标系统上的操作系统版本,开放的服务以及网络结构等都会响应到攻击效用.取值在 0 到 10 之间,根据攻击所需条件的满足程度分为三个级别:完全满足,部分满足和不满足.取值分别为 10,5,0.相关度越高,攻击者的攻击效用就越大.

$w(v_i)$ 的值等于其中各项权值之和,是一个局限于 0 到 30 之间的整数,它的数值越大,则说明攻击者得到的收益就越大.

图1是一个实际的复合攻击示意图,图中的每个节点代表一种具体的攻击方式.整个攻击过程分 5 个步骤:地址探测、端口扫描、获取口令文件、口令破解和登录系统.每个步骤都有多种方式可供选择,攻击者只要成功地使用其中一种即可实现目的.

4 预测模型和算法

4.1 模型

攻击意图逻辑关系图 G 是一个五元组, $G = \{V(G), E(G), R(G), W(G), H(G)\}$, 其中各元素定义如下:

(1) $V(G) = \{v_1, v_2, \dots, v_n\}$ 是顶点集合,每个顶点代表一种攻击意图.

(2) $E(G) = \{e_1, e_2, \dots, e_n\}$ 是有向边集合,由顶点的有序对唯一确定, $e_i = (v_{i1}, v_{i2})$ 表示攻击间的依赖关系,即单步攻击 v_{i1} 的完成是 v_{i2} 实施的前提条件.对于 $\forall v_i \in V(G)$, 定义集合 $S_{\text{before}}(v_i) = \{u \mid u \in V(G), (u, v_i) = e \in E(G)\}$ 表示的前驱节点集合, $S_{\text{after}}(v_i) = \{u \mid u \in V(G), (u, v_i) = e \in E(G)\}$ 表示的后继节点集合.

(3) $R(G) = \{R(v_1), R(v_2), \dots, R(v_n)\}$, $R(G)$ 和 $V(G)$ 中的元素一一对应: $v_i \leftrightarrow R(v_i)$, $R(v_i)$ 表示攻击意图是 v_i 的报警记录的集合. $R(v_i) = \{\text{alert}_1, \text{alert}_2, \dots, \text{alert}_k\}$.

(4) $W(G) = \{w_1, w_2, \dots, w_n\}$ 表示每个顶点对应的加权值,与 $V(G)$ 中的元素一一对应: $v_i \leftrightarrow w(v_i)$, $w(v_i)$ 是取值在 0 到 30 之间的整数,表示攻击意图 v_i 在入侵过程中的攻击效用.

(5) $H(G) = \{h_1, h_2, \dots, h_n\}$ 与 $E(G)$ 中的元素一一对应,表示顶点间的关联条件: $e_i \leftrightarrow h_i$, h_i 是一个真值表示式, $\forall e_i \in E(G), e_i = (v_j, v_k), \exists \text{alert}_1 \in R(v_j), \text{alert}_2 \in R(v_k)$, 使 $h_i(\text{alert}_1, \text{alert}_2) = \text{true}$, 称 alert_1 是 alert_2 的关联记录,记为 $\text{alert}_1 \leftrightarrow \text{alert}_2$.

4.2 算法思想和流程

为了实现攻击状态的动态维护,为每个报警事件 alert_i 引入四个参数:累计加权变量 $T(\text{alert}_i)$,表

示当前复合攻击的完成度,即复合攻击到当前位置所经历的所有步骤的攻击效用和;累计加权变量 $C(alert_i)$,表示复合攻击的检测度,即复合攻击到当前位置所被检测到的步骤的攻击效用和; $ALL(alert_i)_k$ 表示到当前位置所形成的攻击意图序列相匹配的复合攻击序列 k 的所有步骤的攻击效用和; $P(alert_i)_k = C(alert_i)/ALL(alert_i)_k$ 表示复合攻击 k 的完成度。

算法的主要思想:收到经过聚合的报警信息后,按照其所属的攻击意图记录到相应的攻击意图节点 v_{jk} 中,根据当前阶段所形成的攻击意图序列与已知的复合攻击序列进行不完全匹配,然后通过比较每个相匹配的复合攻击的完成度和该复合攻击中下一步的攻击意图节点的攻击效用,来进行攻击预测,识别攻击者的最终意图。

步骤1:收到报警信息 $alert_i$ 后,根据其所属攻击意图记录到相应的节点 v_i 中。

步骤2:计算 $C(alert_i)$ 、 $T(alert_i)$,计算方法按以下情况有所不同:

(1) $S_{before}(v_i)$ 为空,即该节点为初始节点, $C(alert_i) = W(v_i)$ 、 $T(alert_i) = W(v_i)$ 。

(2) $S_{before}(v_i)$ 不为空,且 $S_{before}(v_i)$ 存在 $alert_i$, 使 $h_i(alert_j, alert_i) = true$,即该节点为中间节点,且存在记录 $alert_j$ 与 $alert_i$ 满足关联条件,用 $Q(alert_i)$ 表示 $alert_i$ 与满足关联条件的报警信息集合,计算 $C(alert_i)$ 、 $T(alert_i)$:

$$C(alert_i) = W(v_i) + \sum_{alert_j \in Q(alert_i)} C(alert_j) \quad (1)$$

$$T(alert_i) = W(v_i) + \sum_{alert_j \in Q(alert_i)} T(alert_j)$$

(3) $S_{before}(v_i)$ 不为空,且 $S_{before}(v_i)$ 不存在 $alert_i$,使 $h_i(alert_j, alert_i) = true$,即该节点为中间节点,且不满足关联条件,假设存在一条虚拟记录 $alert_j$, $alert_j \in S_{before}(v_i)$,使 $h_i(alert_j, alert_i) = true$,然后在 $S_{before}(v_i)$ 的前驱节点集合中查找是否存在记录 $alert_k$,使 $h_i(alert_k, alert_j) = true$,若不存在,则认为该记录为孤立事件, $C(alert_i) = W(v_i)$ 、 $T(alert_i) = W(v_i)$ 。若存在,则认为节点 v_j 可能存在漏报事件, v_j 为 $alert_j$ 对应的攻击意图,计算 $C(alert_j)$ 、 $T(alert_j)$:

$$C(alert_j) = \sum_{alert_k \in Q(alert_j)} C(alert_k) \quad (2)$$

$$T(alert_j) = W(v_j) + \sum_{alert_k \in Q(alert_j)} T(alert_k)$$

由于该记录是虚拟记录,计算 $C(alert_i)$ 时,不

计入该节点的加权值,按照(2)计算 $C(alert_i)$ 、 $T(alert_i)$,并删除虚拟记录。

步骤3:如果 $S_{after}(v_i)$ 不为空,根据 $Q(alert_i)$,由 $alert_i$ 向前搜索找到每个报警记录对应的攻击意图,将这些攻击意图形成的序列,与已知的复合攻击序列进行不完全匹配,找到相匹配所有的复合攻击,计算 $ALL(alert_i)_k$ 、 $P(alert_i)_k$,如果 $P(alert_i)_k$ 满足事先设定的阈值 λ ,则该复合攻击序列 k 中 v_i 的下一步攻击,就是要预测的结果,继续接收下一个报警事件。如果匹配的复合攻击有 m 种,其中 n 种复合攻击的 $P(alert_i)_k$ 均满足 λ ,则需要计算 $W(v_{jk}) \times P(alert_i)_k$, v_{jk} 表示复合攻击 k 中 v_i 的下一个节点 v_{jk} , $W(v_{jk}) \times P(alert_i)_k$ 最大的复合攻击 k ,就是预测的正在发生的复合攻击,其中 v_i 的下一个攻击意图 v_{jk} 节点就是下一步将要发生的攻击。图2为基于攻击效用的复合攻击预测算法的流程图。

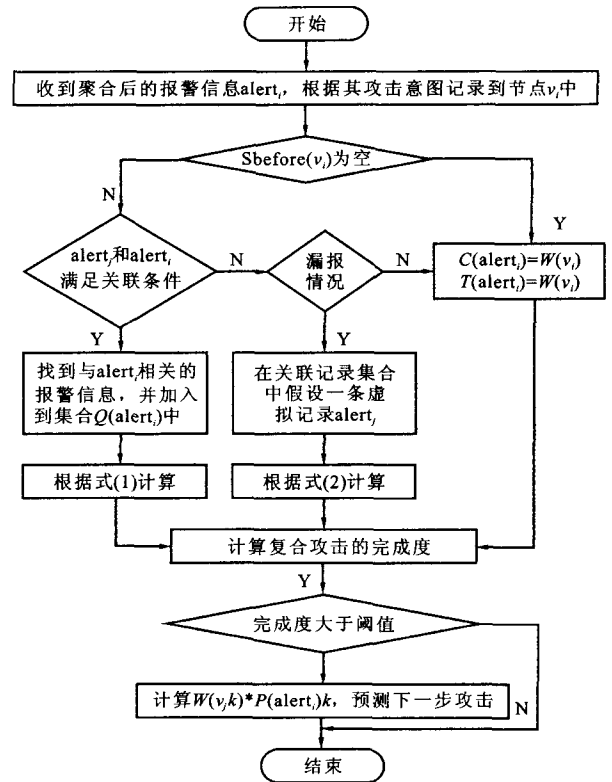


图2 算法流程图

5 实验

本文建立了一个基于攻击效用的复合攻击预测模型,它的系统结构如图3所示,其中预测决策处理模块是整个入侵预测系统的核心部分。

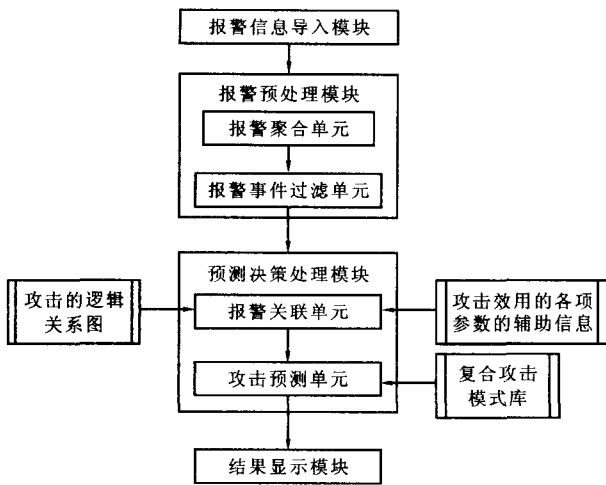


图 3 实验系统模型

为了验证算法的有效性,使用局域网环境下采

表 1 MS SQL server SA 弱口令入侵报警信息

报警名称	源 IP	目的 IP	攻击意图
步骤 1	ICMP ping windows	192. 168. 1. 1	192. 168. 1. 1—255 Ip_sweep
步骤 2	TCP Portscan	192. 168. 1. 1	192. 168. 1. 1—255 Tcp_port_scan
步骤 3	Open port:1433	192. 168. 1. 1	192. 168. 1. 10 Mssql_port_scan
步骤 4	MS-SQL SA brute force login attempt TDS v7/8	192. 168. 1. 1	192. 168. 1. 10 Remote_login
步骤 5	MS-SQL xp_cmd shell—program execution	192. 168. 1. 1	192. 168. 1. 10 Remote_program_execution

实验中,阈值 λ 的设定关系到预测算法的准确性, λ 值过大,会提高漏报率, λ 值过小,会提高误报率,产生过多预测结果,根据实验得出的经验数据和目标系统的安全配置信息,认为阈值 λ 取值为 35% 是一个比较合理的选择. 阈值 λ 可以根据具体环境而动态调整.

在进行 MS SQL server SA 弱口令入侵时,在收到报警信息 ICMP PING WINDOWS,Tcp_Port_scan 后, $P(\text{alert}_2)_{\text{MSSQL server SA}} = 0.364$, $P(\text{alert}_2)_{\text{RPC_overflow_exploit}} = 0.354$,均大于 λ ,再计算 $W(v3_{\text{MSSQL server SA}}) * P(\text{alert}_2)_{\text{MSSQL server SA}}$;

$$W(v3_{\text{MSSQL server SA}}) * P(\text{alert}_2)_{\text{MSSQL server SA}} = 8.008$$

$$W(v3_{\text{RPC_overflow_exploit}}) * P(\text{alert}_2)_{\text{RPC_overflow_exploit}} = 7.434$$

由此预测正在发生的应该是 MS SQL server SA 弱口令入侵,下一步的攻击意图为 Mssql_port_scan.

6 结束语

实验证明算法是有效的. 下一步要解决的问题: (1)实验中攻击效用有些参数的设定缺乏标准性,参数的取值大小会影响到阈值的取值;(2)复合攻击

集的利用 MS SQL server SA 弱口令入侵系统的数据集进行实验. 该实验环境为实验室局域网环境,局域网内有一台数据库服务器,利用服务器的数据库弱口令漏洞入侵系统,入侵者 IP 为 192. 168. 1. 1,服务器 IP 为 192. 168. 1. 10,入侵工具为 SQL TOOLS. MS SQL server SA 弱口令入侵的攻击意图序列为:Ip_sweep—>Tcp_port_scan—>Mssql_port_scan—>Remote_login—>Remote_program_execution.

由于实验中会产生大量的重复报警和误报警,所以报警信息进入预测阶段前要进行预处理,选择 MS SQL server SA 弱口令入侵报警信息 49 条,测得重复报警 29 条,重复报警率 59. 2%,免疫报警 4 条,免疫报警率 8. 16%,经过报警聚合后的 MS SQL server SA 弱口令入侵的综合报警信息见表 1.

模型库建立的不全面,进而影响复合攻击预测的准确性;(3)本算法不能处理连续出现漏报的情况,但实际上这种情况出现的概率是很低的.

参考文献:

- [1] 王祖俤,程小平. 入侵响应中基于事件相关性的攻击预测算法[J]. 计算机科学, 2005,32(4):144—146.
- [2] 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—64.
- [3] 鲍旭华,戴英侠,冯萍慧,等. 基于入侵意图的复合攻击检测和预测算法[J]. 软件学报,2005,16(12).
- [4] Cheung S, Lindqvist U, Fong MW. Modeling multistep cyber attacks for scenario recognition[C]// Proc of the 3rd DARPA Information Survivability Conf and Exposition(DISCEX III). Washington: IEEE computer Society Press,2003:284—292.
- [5] 孙永强,徐昕,黄遵国. 基于 HMM 的分布式拒绝服务攻击检测方法[J]. 微电子学与计算机,2006(10):176—186.
- [6] 罗洪方,钟诚. 基于小波和分形原理的 DDoS 攻击检测方法[J]. 微电子学与计算机,2007(10):85—87.

作者简介:

陈 灿 男,(1982—),博士研究生. 研究方向为网络安全.