基于入侵意图的复合攻击检测和预测算法*

鲍旭华+, 戴英侠, 冯萍慧, 朱鹏飞, 魏 军

(信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

A Detection and Forecast Algorithm for Multi-Step Attack Based on Intrusion Intention

BAO Xu-Hua+, DAI Ying-Xia, FENG Ping-Hui, ZHU Peng-Fei, WEI Jun

(State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)

+ Corresponding author: Phn: +86-10-88258551, E-mail: xuhua_bao@hotmail.com, http://www.gscas.ac.cn

Received 2004-06-11; Accepted 2005-06-02

Bao XH, Dai YX, Feng PH, Zhu PF, Wei J. A detection and forecast algorithm for multi-step attack based on intrusion intention. *Journal of Software*, 2005,16(12):2132–2138. DOI: 10.1360/jos162132

Abstract: The multi-step attack is one of the primary forms of the current intrusions. How to detect these attacks is an important aspect of IDS research. The correlation research to intrusion detection performs mainly on the following aspects: (1) reducing the false positives and false negatives; (2) detecting unknown attacks; (3) attack forecasting. Especially the development of the third point perhaps improves the passive detection to the active protection. Through the study on patterns of the multi-step attack, a detection and forecast algorithm is designed for multi-step attack based on intrusion intention. In this algorithm, an extended directed graph is used to show attack types and their relations, while the correlation is performed according to the method of backwards matching and absent matching. Based on the weighted summation of correlation attack's chain and the branch's weights on the logic graph of attack, the probability of the next attack can be computed. The effect of this algorithm includes the detection of multi-step attack, attack forecasting, detecting unknown attacks, and reducing the false alarms. This paper also presents the process of experimental and analysis result for validity of the algorithm.

Key words: multi-step attack; intrusion intention; forecast attack; logic graph of attack

摘 要: 复合攻击是网络入侵的主要形式之一.如何检测复合攻击是当前入侵检测研究的一个重要方向.这项研究对入侵检测的作用主要表现在以下几个方面:(1) 减少误报和漏报;(2) 实现对未知攻击的检测;(3) 攻击预测.尤其是第 3 点,可能使被动的检测发展为主动的有针对性的防御.经过对复合攻击模式的大量研究,提出了一种基于入侵意图的复合攻击检测和预测算法.该算法采用扩展的有向图来表示攻击类别及其逻辑关系,按照后向匹配和缺项匹配的方式对报警进行关联,根据已关联攻击链的累计权值和攻击逻辑图中各分支的权值计算其可能性.该算法可

* Supported by the National Natural Science Foundation of China under Grant Nos.60403006, 90104030 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035801 (国家重点基础研究发展规划(973))

作者简介: 鲍旭华(1977－),男,天津人,博士生,主要研究领域为入侵检测,网格计算,分布式安全系统;戴英侠(1942－),女,教授,博士生导师,主要研究领域为信息安全;冯萍惠(1979－),女,博士生,主要研究领域为安全模型,脆弱性评估;朱鹏飞(1977－),男,博士生,主要研究领域为公开密钥基础设施;魏军(1971－),男,高级工程师,主要研究领域为网络安全与通信技术.

以实现复合攻击的检测,在一定程度上预测即将发生的攻击,并且对未知攻击有一定的检测能力,还可以大幅度地减少误报和一定的漏报.最后介绍了相应的实验过程和结果分析,证明了算法的有效性.

关键词: 复合攻击;入侵意图;攻击预测;攻击逻辑关系图
中图法分类号: TP393 文献标识码: A

入侵检测系统是保护信息系统安全的重要手段之一,然而目前这项研究还有很多不足之处.首先,多数入侵检测系统都无法检测出未知的攻击类型;其次,大部分入侵检测的实现会产生大量的报警信息,使系统管理者无法及时地作出正确反应;第 3,现有的大部分入侵检测系统都是针对基础攻击的,无法识别复合攻击;第 4,入侵检测的最终目的是阻止攻击,这就要求系统根据攻击者之前的行为作出一定的预测,而这至今依然是一大难点.

本文提出了一种基于入侵意图的复合攻击检测和预测算法,在分析单步攻击目的的基础上,将复合攻击的各个步骤关联起来,完成复合攻击的入侵检测.并以此为基础,通过分析复合攻击的整体意图,预测攻击者即将进行的攻击行为,使有针对性的动态防御成为可能.本文第 1 节讨论当前国际上的相关研究和进展情况.第 2 节描述具体的检测和预测算法.第 3 节是实验过程和结果分析.第 4 节对全文总结并讨论了未来的工作方向.

1 研究现状

对入侵检测的研究始于 1980 年 Anderson 发表的一篇技术报告[1],之后迅速发展出多个分支[2,3],大体上可以分为异常检测和误用检测两类.异常检测基于对检测对象正常行为的统计结果,任何偏离正常行为模式的动作都被视为入侵.误用检测则捕捉已知攻击和系统漏洞的特征,任何符合这种特征的行为都被视为入侵.大部分科研机构和商业组织的 IDS 都使用了异常检测和误用检测技术,包括主机入侵检测(如 USTAT[4])、网络入侵检测(如 NETSTAT[5])以及分布式入侵检测(如 EMERAID[6]).

早期的 IDS 系统都只针对基础攻击进行检测,而无法发现攻击间的逻辑步骤.为了解决这个问题,人们提出了多种关联方法,其中较有影响的有两类:原因关联法和聚类关联法.前者根据攻击之间的依赖关系关联报警信息,实现时的具体方法是将每一种攻击的前提条件和攻击结果形式化,若一种攻击的结果为另一种攻击创造了前提,则认为它们之间有依赖关系.这种方法的代表有斯坦福国际的系统设计实验室[7]、法国防御总署的 MIRADOR 实验室[8]和北卡罗莱纳大学的计算机防御实验室[9].这种方法产生的结果具有较高的可信度,但是所需的计算量非常大,而且很难检测到未知攻击.而聚类关联法是将具有某些相同或相近特征的报警关联起来[10],如时间戳、目的地址等.这种方法多采用统计学方法,观察面较宽,但关联结果的可信度较低.无论使用哪种方法,如何准确地描述攻击特征和攻击序列都是非常重要的一环,不同的研究机构开发了多种攻击描述语言,如 STATL[11],Chronicles[12].他们的研究在不同程度上含有意图分析的倾向,但还不是很明确.

此外,Ming-Yuh Huang 关于入侵意图和入侵策略的研究[13]为这个领域的进一步发展做出了宝贵的贡献,将入侵意图作为一个独立的因素提了出来.我们的研究参考了其思想.

2 复合攻击的检测和预测算法

现实中的网络攻击绝大多数不是孤立的行为,而是以复合攻击的形式出现,如何检测和预测复合攻击是入侵检测研究面临的一个重要问题,也是设计本算法的最终目的.

2.1 复合攻击

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 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.

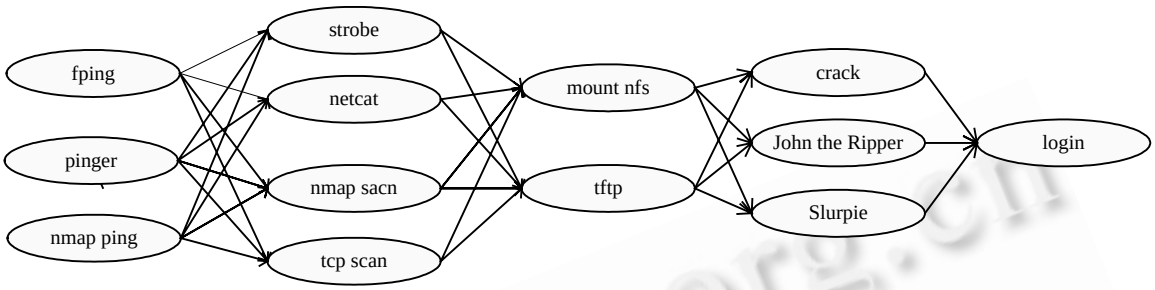

Fig.1 Example of the multi-step attack

图 1 复合攻击实例

2.2 基于意图的攻击分类

当前国际上复合攻击关联的主流方法(如 SRI)是,首先建立一个攻击特征数据库,按照攻击描述语言(如 CAML)表征所有的攻击.特征库中记录了每一种攻击的前提条件和攻击结果,以及攻击发生的环境条件.以此为基础,设计一种自动规则生成机.其原理是:对于任意两种攻击,若一种攻击的攻击后果与另一种攻击的前提条件的交集不为空,则认为后者与前者有依赖关系.按照这种自动机生成的规则集,对入侵检测的报警信息进行匹配和检测.

这种方法在理论上是完全正确的,但在实际应用中却存在严重的隐患.问题的来源在于攻击手段的多样性造成了自动机的状态数过于庞大,处理速度严重滞后于攻击的进度.例如,SRI 在最优化的条件下完成一次关联也需要 1 秒以上[7],而当前每秒需要处理的报警可能会达到数千条.当采用这种机制进行预测时,也会因为备选可能太多,概率过于分散而无法实现.

解决之道在于把匹配元素的范围缩小,匹配的依据从机械的逻辑角度转换到攻击意图的角度.为此,我们建立了基于攻击意图的匹配算法.这种算法将匹配过程分为两个层次,第 1 层是基于攻击意图的攻击分类,将基于攻击事件的报警信息转化为基于攻击意图的报警信息;第 2 层是基于意图的攻击模式匹配,按照复合攻击的逻辑关系图分析和处理基于攻击意图的报警信息.图 2 所示是与图 1 相同的复合攻击,用攻击意图的方式描述,就可以简单的用一个线性链表表示.

Fig.2 Intention format of the multi-step attack

图 2 复合攻击的攻击意图表示法

2.3 算法描述1:攻击逻辑关系图

本算法分两个部分:一是攻击逻辑关系图的建立,相当于建立匹配的框架;二是报警处理流程,也就是在攻击逻辑关系图的基础上对记录进行关联,最终实现攻击检测和预测的目的.

以下是攻击逻辑关系图的定义:

定义(攻击逻辑关系图). 攻击逻辑关系图 G 是一个六 s 元组,$G=\{V(G),E(G),R(G),W(G),H(G),L(G)\}$.定义如下:

1) $V(G)=\{v_1,v_2,v_3,\ldots,v_n\}$,是顶点集合,每一个顶点对应一种攻击类型.

2) $E(G)=\{e_1,e_2,e_3,\ldots,e_m\}$,是有向边集合,由顶点的有序对唯一确定,如 $e_i=(v_{i1},v_{i2})$,对应攻击间的依赖关系.对

于$\forall v_i \in V(G)$,定义集合 $IN(v_i)=\{e|e=(u,v_i),e\in E(G),u\in V(G)\}$表示指向 v_i 的依赖关系集合,$OUT(v_i)=\{e|e=(v_i,u),e\in E(G),u\in V(G)\}$表示由 v_i 出发的依赖关系集合.

3) $R(G)=\{R(v_1),R(v_2),R(v_3),\ldots,R(v_n)\}$,$R(G)$与 $V(G)$中的元素一一对应:$v_i\leftrightarrow R(v_i)$.$R(v_i)$表示攻击类型是 v_i 的报警记录的集合.$R(v_i)=\{r_1,r_2,r_3,\ldots,r_{ki}\}$,每一个元素对应一条报警信息.

4) $W(G)=\{w_1,w_2,w_3,\ldots,w_n\}$,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0~20之间的整数,表示攻击类型 v_i 在入侵过程中的重要性和危害程度.

5) $H(G)=\{h_1,h_2,h_3,\ldots,h_m\}$,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 是一个真值表达式,$\forall e_i\in E(G),e_i=(v_j,v_k),\exists r_1\in R(v_j),r_2\in R(v_k)$使 $h_i(r_1,r_2)$=TRUE,则称 r_1 是 r_2 的关联记录,记为 $r_1\leftrightarrow r_2$.为了表示方便,也记为 $h_i(e_j,r_2)$=TRUE,或 $e_j\rightarrow r_2$.

6) $L(G)=\{L_1,L_2,L_3,\ldots,L_n\}$是真值表达式的集合,与 $V(G)$中的元素一一对应,表示指向同一顶点的各边之间的关系.例如,IN$(v_i)=\{e_1,e_2,\ldots,e_k\}$,$r\in R(v_i)$则

$$L_i(r)=\begin{cases}\text{true}, & |IN(v_i)|=0\\ h_i(v_j,r), & |IN(v_i)|=1, IN(v_i)=\{e=(v_j,v_i)\}\\ Logic(e_1,e_2,...,e_k), & |IN(v_i)|>1\end{cases}.$$

Logic$(e_1,e_2,\ldots,e_k)$是一个具体的真值表达式,只包含 $H(G)$中的元素以及括号和与、或运算符.$r\in R(v_i)$,当且仅当 $L_i(r)$=true,表示记录 r 属于复合攻击的一部分,称为 r 可关联.

注:在 Stuart McClure 的研究[14]中,给出了一种对攻击危害的评估方法,从 3 个角度评价攻击:流行度(popularity)、易用性(simplicity)和影响力(impact).综合这三者,给出一个综合指数风险率(risk rating).这是一个在 0~10 之间取值的整数,并给出了相应攻击的具体数值.为了使不同类型的攻击区别更明显,我们为每个攻击大类加入了一个基本危险度,在 0~10 之间取值,将其与风险率相加,即得到每个结点的加权值.其取值范围是0~20之间的整数.

2.4 算法描述2:报警处理流程

现有的大部分关联算法都是先建立一系列匹配规则,收到报警信息后建立相应的匹配链,随着报警的增加,需要维护的数据会线性增加.而在我们的算法中,采用了完全不同的设计.无须维护静态的攻击匹配链,而只是对每条记录赋予特定参数.既可以实现复合攻击的检测和预测,又大为提升了系统的效率和安全性,并且在必要的时候,可以动态、完整地恢复出攻击流程.

任何复合攻击都可以用攻击逻辑关系图 G 的子图来表示,记为 CA,$CA\subseteq G$,其中每一个单步攻击记为 A,$A\in V(CA)$.

为了实现攻击状态的动态维护,我们针对每一条记录 r,添加了 3 项参数值:累计加权值 $T(r)$,用于度量当前复合攻击的完成度,是复合攻击到当前位置所经历的所有步骤加权值之和;累计攻击值 $C(r)$,用于度量当前复合攻击的检测度,是复合攻击到当前位置所有被检测到的步骤加权值之和;攻击检测率 $C(r)/T(r)$,表示当前进行的复合攻击中被检测到的比率.此外,定义回溯路径 $P(r)$为一个节点集合,记录与当前攻击步骤直接关联的所有节点,用于回溯完整的攻击过程.

若当前记录 $r\in R(v_i)$可关联,则 $L_i(r)$=true.将 $L_i(r)$中值为 False 的 h 项代入,可得化简的真值表达式,该表达式中各项所对应的依赖关系即为 $P(r)$的元素.通过 $P(r)$递推,即可恢复出完整复合攻击过程.

以下是报警信息的处理流程:

步骤 1. 记录报警:收到报警信息 r 后,将其分类并记录到对应攻击类型的节点 v_i 中.

步骤 2. 关联匹配:计算 $P(r)$,$T(r)$,$C(r)$,计算方法按照以下情况而不同:

a) $|IN(v_i)|=0$,即该节点是起始节点,则记录 $P(r)$集合为空,$T(r)=w_i$,$C(r)=w_i$.

b) $|IN(v_i)|>0$,且 $L_i(r)$=True,即该节点是中间节点,且记录 r 满足关联条件.按定义计算集合 $P(r)$.从 $P(r)$每个节点中选出一条记录 r_e,在该节点满足 $r_e\rightarrow r$ 的记录中,$C(r)/T(r)$的比值最大.这些记录构成一个集合,记为 $P'(r)$.计算 $T(r)$,$C(r)$:

$$T(r_p)=w_i+\sum_{r_e\in P'(r)}T(r_e),$$

$$C(r_p)=w_i+\sum_{r_e\in P'(r)}C(r_e).$$

c) $|IN(v_i)|>0$,且 $L_i(r)$=False,即该节点是中间节点,且不满足关联条件.遍历 $L_i(r)$中值为 False 的 h 项,寻找若将其用 True 替换,即可以使得 $L_i(r)$=True 的 h 项.若不存在,则认为该记录为孤立事件,记录 $P(r)$集合为空,$T(r)=w_i$,$C(r)=w_i$.若存在,则认为该节点可能存在未知攻击.假设在该节点中存在虚拟记录 r_p,使 $r_p\rightarrow r$.按照 b)的条件检查依赖关系,计算 r_p 的 $T(r_p)$,$C(r_p)$:

$$T(r_p)=w_i+\sum_{r_e\in P'(r)}T(r_e),$$

$$C(r_p)=\sum_{r_e\in P'(r)}C(r_e).$$

由于该记录是虚拟记录,所以计算 $C(r)$时,不计入当前节点的加权值.由于该记录的存在,使当前记录的 $L_i(r)$=True,按照 b)的步骤的 $P(r)$,$T(r)$,$C(r)$,再将虚拟记录删除.

步骤 3. 记录加成:有时在同一节点存在多条可关联记录,且彼此的 $C(r_e)/T(r_e)$和 $T(r_e)$值相同,这表示攻击者可能变换不同的环境参数进行多次攻击尝试,例如 DDOS 攻击.这时我们应当对现有的 $C(r_e)$予以加成.若同类记录有 n 条,则加成规则应当满足以下条件,a) 加成后 $C(r_e)\leq T(r_e)$;b) n 越大,加成越多.实际公式如下:

$$C(r_e)=C(r_e)\times\left(1-\frac{C(r_e)}{T(r_e)}\right)\times\left(1-\left(1-\frac{C(r_e)}{T(r_e)}\right)^{n-1}\right).$$

步骤 4. 攻击预测:若集合 $OUT(v_i)$中存在节点 v_j 属于 BREAK_IN,GET_ROOT,DOS,DDOS 类型,且当前节点的攻击记录与关联关系相符,则假设在该节点中存在虚拟记录 r_p,使 $r\rightarrow r_p$.若 $L_j(r_p)$=True,则按照步骤 2 计算 $P(r_p)$,$T(r_p)$,$C(r_p)$,并计算 $C(r_p)/T(r_p)$,若该值大于门限 G,则复合攻击预测完成,发出复合攻击预测报警.

步骤 5. 复合报警:若当前节点属于 BREAK_IN,GET_ROOT,DOS,DDOS 类型,则表示复合入侵已经进行,发出入侵警报.

注:门限 G 的设定关系到预测算法的准确性.G 值过高,会提高漏报率;G 值过小,会提高误报率.这也是所有 IDS 系统面临的问题之一.根据实验得出的经验数据,我们认为 65%是一个较理想的选择.一般的复合攻击在 5 步左右,而最后一步攻击一般危害性较大,加权值也较大.G 取 65%时可以实现大部分复合攻击的预测,同时又避免了大多数误报,是比较理想的实验数据.此外,G 值是可以根据具体环境而动态调节的.

本算法可以对复合攻击中出现的单个未知攻击进行匹配;若出现多个未知攻击,只要它们彼此不连续,也可以成功匹配;但是,如果出现两个连续的未知攻击,则无法继续匹配.然而,在一次复合攻击中出现且连续出现两个未知攻击的概率是极低的.这是由于人的心理因素造成的,一般来说,人在使用一种新工具的时候,总是要将其置于自己可以充分把握的环境中,这样才能准确了解其性能.攻击者在使用新型攻击工具时也往往是以自己最熟悉的、常规的工具作辅助工作,这种心理定式为我们的检测提供了有利条件,提高了检测的准确性.

3 实验过程及结果分析

实验采用的基础架构是国家自然科学基金重点项目“面向大规模网络的分布式入侵检测和预警模型”(90104030)的原型系统,并添加了攻击分类模块、意图关联模块和动态响应模块以实现复合攻击的检测和预测功能.我们将其统称为 MDFM(multi-step intrusion detection and forecast module).

3.1 不含未知攻击的复合攻击预测

为了验证算法的有效性,我们选取 2000 年 DARPA[15,16]的入侵检测评估数据 LLDOS1.0 进行了实验.LLDOS1.0 中包含了一个完整的攻击序列.内容如下:1) 主机探测;2) 端口扫描;3) 系统入侵;4) 安装木马;5) 利用被控主机发起 DDOS 攻击.

LLDOS1.0 的数据包括两个部分,内网检测数据和 DMZ 区域检测数据.与之对应,我们使用了两个检测器同

步监听该数据流,通过分布式入侵检测系统汇总和处理报警信息.

表 1 记录了攻击报警列表,除记录 18 外,所有的源地址都是 202.77.162.213;而记录 18 是 DDOS 攻击,数据包源地址是攻击者随机伪造的.因此,我们未在表中再列出源地址.

Table 1 Table of the attack records

表 **1** 攻击记录表

	Target address	Event alert	Intention Alert	*T*	*C*	*L*
1	172.16.112.0/24	ICMP_PING_SWEEP	IP_SWEEP	6	6	Null
2	172.16.113.0/24	ICMP_PING_SWEEP	IP_SWEEP	6	5	Null
3	172.16.114.0/24	ICMP_PING_SWEEP	IP_SWEEP	6	6	Null
4	172.16.115.0/24	ICMP_PING_SWEEP	IP_SWEEP	6	6	Null
5	172.16.112.0/24	SADMIND_PORT_REQUEST	RPC_PORT_SCAN	15	15	*e*0001_0006
6	172.16.113.0/24	SADMIND_PORT_REQUEST	RPC_PORT_SCAN	15	15	*e*0001_0006
7	172.16.114.0/24	SADMIND_PORT_REQUEST	RPC_PORT_SCAN	15	15	*e*0001_0006
8	172.16.115.0/24	SADMIND_PORT_REQUEST	RPC_PORT_SCAN	15	15	*e*0001_0006
9	172.16.115.20	SADMIND_PORT_SCAN	HIGHRISK_PORT_SCAN	27	27	*e*0006_0008
10	172.16.112.10	SADMIND_PORT_SCAN	HIGHRISK_PORT_SCAN	27	27	*e*0006_0008
11	172.16.112.20	SADMIND_PORT_SCAN	HIGHRISK_PORT_SCAN	27	27	*e*0006_0008
12	172.16.115.20	SADMIND_OVERFLOW_ATTEMPT	REMOTE_OVERFLOW_ATTEMP	41	41	*e*0008_0034
13	172.16.112.10	SADMIND_OVERFLOW_ATTEMPT	REMOTE_OVERFLOW_ATTEMP	41	41	*e*0008_0034
14	172.16.112.20	SADMIND_OVERFLOW_ATTEMPT	REMOTE_OVERFLOW_ATTEMP	41	41	*e*0008_0034
15	172.16.115.20	RSH_LOGIN	REMOTE_LOGIN	45	45	*e*0034_0012
16	172.16.112.10	RSH_LOGIN	REMOTE_LOGIN	45	45	*e*0034_0012
17	172.16.112.20	RSH_LOGIN	REMOTE_LOGIN	45	45	*e*0034_0012
18	131.84.1.31	DDOS	DDOS	61	61	*e*0012_0098

以上报警是 DIDS 经过数据融合后产生的综合报警信息,实际的报警信息远多于此.例如,对一个网段的 ICMP_PING_SWEEP 扫描就有 256 条报警.

每收到一条报警,MDFM 就将其分类,并记入攻击逻辑图中,按照第 2.4 节所述步骤可以成功进行报警关联.下面我们着重介绍攻击预测的过程:

按照第 2.4 节步骤 4,若集合 $OUT(v_i)$中存在节点 v_j 属于 BREAK_IN,GET_ROOT,DOS,DDOS 等危险类型,且当前节点的攻击记录与关联关系相符,则进行预测计算.本实验中存在两次这样的情况:

1) MDFM 收到 3 条 HIGHRISK_PORT_SCAN 报警,遍历后发现存在依赖关系 e0008_0034:HIGHRISK_PORT_SCAN→REMOTE_OVERFLOW_ATTEMPT 满足预测条件.按照步骤 4,加入假设记录 r_p,计算检测率 $C(r_p)/T(r_p)$:

$$\frac{C(r_p)}{T(r_p)}=\frac{\sum_{r_e\in PRE(r_p)}C(r_e)}{w(u)+\sum_{r_e\in PRE(r_p)}T(r_e)}=65.9\%\ .$$

$C(r_p)/T(r_p)>G$,MDFM 发出预警信息,通知主动响应模块采取预防措施.

2) MDFM 收到 3 条类型是 TROJAN 的 REMOTE_LOGIN 报警,遍历后发现存在依赖关系 e0012_0096:REMOTE_LOGIN→DDOS 满足预测条件.按照步骤 4,加入假设记录 r_p,计算检测率 $C(r_p)/T(r_p)$:

$$\frac{C(r_p)}{T(r_p)}=\frac{\sum_{r_e\in PRE(r_p)}C(r_e)}{w(u)+\sum_{r_e\in PRE(r_p)}T(r_e)}=73.9\%\ .$$

$C(r_p)/T(r_p)>G$,MDFM 发出预警信息,通知主动响应模块采取预防措施.

3.2 包含未知攻击的复合攻击预测

以上的实验证实了本算法对复合攻击的预测能力,但由于实验数据中不存在未知攻击,所以实验没有体现出本算法对未知攻击的检测能力.

为了验证本算法对未知攻击的检测与预测能力,我们屏蔽了探测器 SADMIND 端口探测的检测能力,假设这是一种未知攻击,然后再重复上述实验.这时会缺少表 1 中的 3 条 SADMIND_PORT_SCAN 报警.由于 HIGHRISK_PORT_SCAN 的缺失,无法预测 REMOTE_OVERFLOW_ATTEMP,但是依然可以对 DDOS 进行

预测.

MDFM 收到 3 条类型是 TROJAN 的 REMOTE_LOGIN 报警,遍历后发现存在依赖关系 e0012_0096:REMOTE_LOGIN→DDOS 满足预测条件.按照步骤 4,加入假设记录 r_p,计算 $C(r_p)$,$T(r_p)$:

$$T(r)=w(u)+\sum_{r_e\in PRE(r)}T(r_e)=61.$$

由于当前节点 $C(r_p)/T(r_p)\neq 1$,需要首先计算$\Delta C(r_e)$:

$$\Delta C(r_e)=C(r_e)\times\left(1-\frac{C(r_e)}{T(r_e)}\right)\times\left(1-\left(\frac{C(r_e)}{T(r_e)}\right)^{n-1}\right)=8.$$

$$C(r_p)/T(r_p)=41/61=67.2\%>G.$$

MDFM 发出预警信息,通知主动响应模块采取预防措施.

4 小 结

本文的研究目的在于建立有效的复合入侵检测和预测机制,为主动防御的实现建立基础.为了实现此目的,本文提出了基于入侵意图的复合攻击检测和预测算法,并在实验中验证了该算法的有效性.实验表明,本算法具有以下优点:1) 清晰地体现出复合攻击的流程;2) 对复合攻击的量化表示;3) 实现复合攻击的检测;4) 实现了存在未知攻击的情况下对复合攻击的检测;5) 复合攻击的预测功能.

本课题下一步的研究方向包括:1) 现有的攻击逻辑关系图主要是针对类 Unix 系统的,我们准备继续研究 Windows 的复合攻击模式;2) 现在使用的阈值是一个经验数据,如何选取阈值使之具有最好的效果;3) 成功预测到复合攻击后如何有效地与主动响应模块联动,既能有效地阻止攻击继续,又不影响系统的正常功能.

References:

[1] Anderson JP. Computer security threat monitoring and surveillance. Technical Report, Contract 79F26400. Fort Washington, Pennsylvania, James P. Anderson Company, 1980.

[2] Mukherjee B, Heberlein LT, Levitt KN. Network intrusion detection. IEEE Network, 1994,8(3):26−41.

[3] Bace RG. Intrusion Detection. Macmillan Technology Publishing, 2000.

[4] Ilgun K, Kemmerer RA, Porras PA. State transition analysis: A rule-based intrusion detection approach. IEEE Trans. on Software Engineering, 1995,21(3):181−199.

[5] Vigna G, Kemmerer RA. NetSTAT: A network-based intrusion detection system. Journal of Computer Security, 1999,7(1):37−71.

[6] Porras PA, Neumann PG. EMERALD: Event monitoring enabling response to anomalous live disturbances. In: Proc. of the 20th National Information Systems Security Conf. National Institute of Standards and Technology, 1997. 353−365.

[7] Cheung S. Lindqvist U, Fong MW. Modeling multistep cyber attacks for scenario recognition. In: Proc. of the 3rd DARPA Information Survivability Conf. and Exposition (DISCEX III), Washington: IEEE computer Society Press. Vol I, 2003. 284−292.

[8] Cuppens F, Miège A. Alert correlation in a cooperative intrusion detection framework. In: Proc. of the 2002 IEEE Symp. on Security and Privacy (S&P 2002). 2002. 202−215.

[9] Ning P, Xu DB, Healey CG, St. Amant RA. Building attack scenarios through integration of complementary alert correlation methods. In: Proc. of the 11th Annual Network and Distributed System Security Symp (NDSS 2004). 2004. 97−111.

[10] Valdes A, Skinner K. Probabilistic alert correlation. In: Lee W, Mé L, Wespi A, eds. Proc. of the 4th Int'l Symp. on Recent Advances in Intrusion Detection (RAID 2001). Davis: Springer-Verlag, 2001.

[11] Eckmann S, Vigna G, Kemmerer R. STATL: An attack language for state-based intrusion detection. Journal of Computer Security, 2002,10(1/2):71−104.

[12] Templeton S, Levitt K. A requires/provides model for computer attacks. In: Proc. of the New Security Paradigms Workshop. ACM Press, 2000. 31−38.

[13] Huang MY, Wicks TM. A large-scale distributed intrusion detection framework based on attack strategy analysis. Computer Networks, 1999. 2465−2475.

[14] McClure S, Scambray J, Kurtz G. Hacking Exposed: Network Security Secrets and Solutions. 2nd edition. McGraw-Hill/Osborne Media, 2001.

[15] Haines JW, Lippmann RP, Fried DJ, Tran E, Boswell S, Zissman MA. DARPA intrusion detection system evaluation: Design and procedures. Technical Report 1062, Lexington: MIT Lincoln Laboratory, 1999.

[16] http://www.ll.mit.edu/IST/ideval/index.html