基于攻防对抗的网络安全动态评估方法

连礼泉 彭 武 王冬海
(中国电子科技集团公司电子科学研究院 北京 100041)

摘 要 根据网络攻防对抗实时变化的特点,提出了一种网络安全状态的动态评估方法。首先,根据敌我双方攻防特点,建立基于脆弱性状态迁移的网络安全模型;然后,在此基础上量化攻击成功的可能性和产生的后果,并分析攻防对抗行为对关键资产保密性、完整性、可用性等安全属性的影响,并通过实验验证了该方法的可行性及有效性。

关键词 攻击图,安全评估,可视化,攻防对抗
中图法分类号 TP393.08 **文献标识码** A

Method of Network Security Dynamic Assessment Based on Attack-defense Confrontation

LIAN Li-quan PENG Wu WANG Dong-hai
(China Academy of Electronics and Information Technology, Beijing 100041, China)

Abstract According to the characteristic of the network attack-defense real-time variation, a dynamic assessment method of network security state was presented. Firstly, a network security model based on vulnerability state transition was built, according to the characteristics of attack and defense both sides. Then the success probability and the consequences of attack success were quantitated, and the effects of attack-defense confrontation behaviors on the key asset security attributes such as confidentiality, integrity and availability were analyzed. Finally, the feasibility and validity of this method were proved through an experiment.

Keywords Attack graph:, Security assessment, Visualization, Attack-defense confrontation

1 引言

对网络安全状态进行准确的评估,可以帮助网络安全管理人员从整体上了解网络的安全态势,并分析攻击者入侵意图和预测网络安全趋势,对保障网络安全具有重要的意义。因此,网络安全评估已经成为网络安全研究领域的重要课题,具有重要的实用价值。

目前,国内外有不少研究人员对网络安全评估方法进行了研究,从不同角度出发提出了多种评估方案,取得了一定的成果,但大多数的研究尚未建立成熟的评估系统。韦勇等人提出基于日志审计与性能修正算法的网络安全态势评估模型[1],可以对网络的安全态势进行预测,但该方法只是对网络安全进行了静态评估,没有考虑网络攻防对抗的动态变化和发展趋势。Philips 等提出通过研究漏洞的关联关系来发现攻击路径,根据建立的攻击模板生成攻击路径图,该方法能够较好地评价网络安全属性变化不大的网络,但当网络安全属性变化较大时,则无法对网络安全状态进行实时评估。Lau 提出使用 Spinning Cube 来表示网络连接,用不同的颜色来表示不同的网络安全状态[2],该方法使用了新颖的方式对网络安全状态进行可视化处理,但该方法以网络连接作为评估的指标,没有全面考虑网络的安全因素。

本文针对以上评估方法的不足,结合实际网络中网络安全属性实时变化、攻防对抗复杂多变的特点,提出了一种基于攻防对抗的网络安全动态评估方法。该方法从网络拓扑结构、主机脆弱性信息和入侵者攻击行为信息出发,生成攻击路径图,并根据入侵行为和防御行为的变化实时更新,用直观的可视化手段动态地展示了攻防对抗的发展情况,为了解网络安全状态的发展趋势提供了简单、有效、直观的方法。

2 基于攻防对抗的网络安全建模

2.1 攻防对抗过程建模

基于攻击图的安全评估方法和其他安全评估方法相比,具有简单、直观的特点。网络安全评估人员可以利用攻击图了解网络节点的安全属性,快速找寻整个网络系统中最容易受攻击或者对整个网络的安全影响最为重要的安全节点[3]。实际网络中,网络安全属性受攻防对抗行为的影响很大,为了全面了解脆弱性分布和攻防对抗行为的联系,展示网络攻防对抗行为所引起的脆弱性转移情况显得尤为重要。攻击图可以对网络攻防对抗行为的实时变化进行动态展示,较好地满足了攻防对抗过程建模及网络安全状态可视化的要求。

本文采用了层次化的攻击路径图进行建模,在传统攻击图的基础上,对攻击图的节点和边做了改进,以更好地满足本文的网络安全评估方法对攻防对抗过程建模的要求。

传统的网络拓扑图以主机为节点,网络通信链路为边,无

本文受国防基础科研项目(A0420110006)资助。
连礼泉(1986—),男,硕士,主要研究领域为信息系统安全,E-mail:lianliquan@139.com;王冬海(1968—),男,硕士,高级工程师,主要研究领域为网络与信息安全;彭 武(1979—),男,博士,工程师,主要研究领域为网络安全与风险评估。

法展示主机的脆弱性、资产价值等安全属性信息。传统的攻击图以脆弱性为节点，攻击路径为边，可以较全面地反映网络中的漏洞分布及相互关系，呈现了权限转移和攻击步骤等细节，以此为基础进行的安全评估较为准确，但攻击图没有反映漏洞和主机的从属关系，只见树木，不见森林，影响了安全管理人员对网络主机信息的把握。

本文针对传统攻击图的不足，结合网络拓扑图和攻击图的特点，将网络节点模型分为主机、脆弱性两个层次[4]。如图1所示，每台主机由矩形边框表示，每台主机包含若干漏洞，漏洞用圆来可视化表示，使用带箭头的连接线来表示攻击路径，连接线的粗细表示单步攻击的可能性，箭头方向指示攻击方向，同时也代表了漏洞的依赖性关系。当安全管理员通过手动或安全防护软件采取防御行为后，攻击者的攻击路径被阻断，在攻击路径图上相应的连接将消失。攻击者总是沿着实际的物理链路进行入侵，因此，通过主机及攻击路径可以直观地反映网络的拓扑结构，攻击路径结合主机的漏洞则能够直观地了解网络脆弱性的转移趋势。

网络的拓扑结构由网络管理员或者网络交换设备自带的链路探测功能提供，也可以通过第三方软件获得，实际的网络物理连接变化较小，因此，这一步的工作量可以由人工完成。主机存在的漏洞由漏洞扫描工具提供，网络管理员定期对主机进行维护，如打补丁、升级系统等活动，可能导致主机漏洞的变化，因此，在网络管理员对网络主机安全策略进行升级之后，需要对网络的漏洞重新进行扫描。

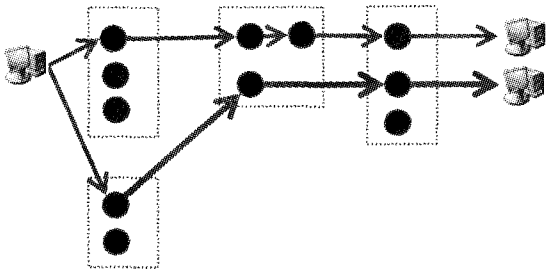


图1　攻击路径图

2.2　攻防对抗状态的可视化

实际的网络中存在着大量的攻防对抗行为，攻击者和防御者将根据网络的脆弱性状态及对方采取的行为即时改变自己的策略。攻防对抗行为对网络安全评估结果的影响很大，如何在攻击路径图上直观、准确地可视化其复杂多变的攻防过程，将是一个不小的挑战。

攻击者为了得到目标主机的资产状态信息，一般需要利用多个主机的漏洞，以已经得到的权限为跳板进行下一步攻击。主机的脆弱性状态直接关系到网络的整体安全状况，为了描述攻击行为和防御行为对脆弱性的影响，需要在图1建立的攻击图模型的基础上，对脆弱性进行量化处理。

根据主机漏洞可能被利用的情况可以将主机的脆弱性状态分为3种：a)是完整攻击路径的节点，且已被利用；b)是完整攻击路径的节点，但尚未被利用；c)存在一定的安全隐患，但由于未构成完整的攻击路径，导致其无法或很难被利用。

为了方便计算机自动处理，将以上漏洞的状态进行量化，在进行脆弱性可视化时，用不同的颜色对漏洞的状态值进行映射，从而直观地显示出攻击路径和脆弱性的关系。脆弱性状态量化值如表1所列。

表1　脆弱性状态量化

编号	漏洞状态描述	可视化颜色	脆弱性状态值
1	该漏洞已被利用	黑色	1
2	该漏洞可能被利用，但暂未被利用	灰色	(0,1)
3	该漏洞无法被利用	白色	0

本文在攻击路径图的基础上，使用不同的颜色对攻击行为进行分类，黑色表示该攻击已经成功，灰色表示可能的攻击方向。沿着黑色的攻击路径可以直观地分析一系列攻击行为的相关关联性，了解攻击过程[5]。同时，为了在攻击路径图上表示网络管理员的防御行为，本文在漏洞内部使用交叉线来标识防御行为。

图2为脆弱性可视化改进之后的攻防对抗图。从图中可以看出，主机H1－H4存在的漏洞相互关联，使得攻击者H0可以从两条攻击路径分别对主机H5和主机H6造成威胁。攻击者H0和目标主机H5存在一条被攻击概率很大的攻击路径：H0－>Vul1－>Vul2－>Vul3－>H5，从图中可以看出，只要采用防火墙等安全防护软件限制攻击者H0对主机H2的访问，就可以阻挡攻击者对资产价值较高的主机H5的入侵，主机H0到主机H2的访问权限被限制后，攻击者将无法利用主机H2的Vul1漏洞，从而维护了网络信息的安全。

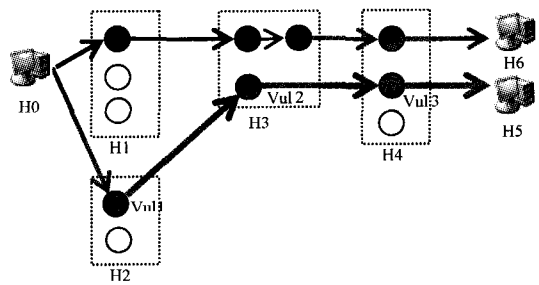


图2　攻防对抗图

3　网络安全状态的动态评估[6]

通过漏洞扫描工具获取被评估网络的脆弱性数据，可以在一定程度上了解网络的漏洞统计分布，但这些脆弱性数据很难反映漏洞之间的相互关系。攻击路径图不仅展示了漏洞在网络拓扑结构上的分布，而且也反映了漏洞之间的依赖关系。在攻击源数量较小及攻击行为变化不大的情况下，攻击路径图能够直观地展示网络的脆弱性转移情况，评估网络的安全状态。

在实际的网络中，网络的攻击源是不确定的，网络管理员很难预知网络攻击的来源及攻击行为发生的时间，这使得评估网络当前的安全状态变得困难。评估网络安全状态是一件费时费力的事，网络管理员很难根据入侵检测系统(IDS)提供的数据判断网络当前最脆弱的安全环节，也很难采取最有效的措施来防范当前的网络入侵行为。因此，需要根据网络入侵信息的变化对网络进行动态安全分析评估，提供有效的安全状态信息，及时阻止入侵行为，将损失降到最低。

3.1　攻击成功的可能性

定义1　攻击向量V是以漏洞v_i为元素的有序横向量，即$V=[v_1,v_2,,\cdots,v_i]$，其中，利用漏洞v_i需要以漏洞v_{i-1}的成功利用为前提。

攻击向量代表一条实际的攻击路径。攻击者在成功利用某台主机的漏洞获得一定权限后，就可以以此为跳板发动下

一步攻击。

假设 1 攻击者为智能主体，即攻击者总是选择较容易成功的路径发动攻击。

实际网络中，攻击者为智能主体，因此攻击者沿攻击向量 V 发动攻击的可能性与该路径成功的可能性成正比。攻击者实现单步攻击的成功概率可以由 CVSS 漏洞评分系统获得，由攻击向量 V 描述的攻击路径被利用的可能性可以由下式计算得到：

$$P(V)=\prod_{i=1}^{n}P(v_i) \tag{1}$$

式中，$P(V)$ 为攻击向量 V 描述的攻击发生的可能性，$P(v_i)$ 为单步攻击成功概率，n 为攻击路径上的漏洞数。

在网络攻击图的基础上，以攻击者为起点，目标主机为终点，可以得到多条可达的攻击路径，每条攻击路径都将增加目标主机被入侵的风险。根据攻击向量遍历所有可能的攻击路径，攻击者某次攻击意图的成功概率可以由式(2)计算得到：

$$P(A)=1-\prod_{k=1}^{m}(1-P(v_k)) \tag{2}$$

式中，$P(A)$ 为攻击意图成功的概率，$P(V_k)$ 为攻击向量 V_k 代表的攻击路径攻击成功的概率，m 为所有的攻击路径数。

攻击意图成功的概率反映了攻击者发动攻击的可能性。

3.2 攻击后果评估

资产价值反映了网络设备可以被攻击者利用的价值。理智的攻击者不可能对自己没有利用价值的网络设备发动攻击，因此，攻击行为的意图总是以网络设备的资产价值为导向。网络设备在网络中的角色决定了其自身的资产价值和保密性、完整性、可用性(CIA)属性比例。本文中，网络设备的资产价值用 S 表示。本文根据网络设备的 CIA 属性，将网络设备的资产价值分为可用性价值、保密性价值和完整性价值 3 个分量。

定义 2 主机的资产价值由可用性价值、保密性价值、完整性价值 3 个分量组成，是 3 个分量的和，主机的资产价值向量用向量 $\vec{S}=[Con,Int,Ava]$ 表示，其中，Con 为保密性价值，Int 为完整性价值，Ava 为可用性价值。

主机的可用性价值、保密性价值、完整性价值由专家根据网络设备提供的服务等信息评估得到。

定义 3 主机的资产价值比是主机的资产价值在所有主机的资产价值总和中的比例，用向量 $\vec{\eta}=[\alpha,\beta,\gamma]$ 表示，其中，α 为保密性价值比，β 为完整性价值比，γ 为可用性价值比。保密性价值比、完整性价值比、可用性价值比可以用式(3)计算：

$$\begin{cases}\alpha_i=\dfrac{Con_i}{\sum_{k=1}^{n}Con_k}\\ \beta_i=\dfrac{Int_i}{\sum_{k=1}^{n}Int_k}\\ \gamma_i=\dfrac{Ava_i}{\sum_{k=1}^{n}Ava_k}\end{cases} \tag{3}$$

式中，Con_i 为网络中第 i 台主机的保密性价值，Int_i 为网络中第 i 台主机的完整性价值，Ava_i 为网络中第 i 台主机的可用性价值，n 为网络的主机数。

网络主机的可用性价值比、保密性价值比、完整性价值比越大，其对网络安全状态的影响也越大，当攻击者对其发动攻击并成功后，造成的后果也越严重。

3.3 安全状态动态评估

网络的安全状态不但受网络拓扑结构、网络设备存在的漏洞等静态网络因素的影响，还受攻击行为、防御行为等动态网络因素的影响。因此，网络安全评估中包含了复杂多变的攻防对抗过程，要准确地评估网络安全状态，需要分别对攻击行为和防御行为造成的影响做动态评估[7]。

对网络安全状态的评估就是对网络设备资产价值被威胁程度和发展趋势的评估。当一台主机被成功攻击后，该主机的可用性价值、保密性价值、完整性价值即受到不同程度的威胁，管理员采取防御行为后，也将分别对主机的可用性价值、保密性价值、完整性价值产生不同的影响，对网络 CIA 属性的状态分别进行动态评估可以得到更为精确的安全评估结果[8]。

保密性价值是比较敏感的 CIA 属性，当可用网络信息泄露给非授权的用户后，将造成比较严重的后果。因此，本文中对保密性价值的状态量化为多个级别，以精细地表示网络攻防对抗对保密性价值的影响。保密性状态的量化方法如表 2 所列。

表 2 保密性状态量化

Ci	状态描述
1	已被非授权用户访问
0.9	存在攻击路径，非授权用户正试图访问
0.7	存在攻击路径，但没有非授权用户访问
0.5	存在攻击路径，但该路径对攻击者而言不可达
0	不存在隐患，只有授权用户可以访问

网络的保密性状态受威胁的程度可以用下式计算：

$$R_{con}=\sum_{k=1}^{n}C_i\alpha_i \tag{4}$$

式中，R_{con} 为网络保密性价值威胁指数，C_i 为第 i 台主机保密性价值状态值，α_i 为第 i 台主机的保密性价值比，n 为主机数。

网络保密性价值威胁指数表征了网络当前保密性价值所受的威胁程度，网络管理员采取防御措施后可以在一定程度上解除威胁，保障网络的信息安全。防御措施包括通过防火墙访问控制表(ACLs)、网络地址转换(NAT)控制网络可达性等方法，这些措施阻断了攻击者的攻击路径，提高了攻击者的攻击难度，增加了网络的安全性。采取防御行为后，网络的防御效果可以用下式计算：

$$S_{con}=1-\sum_{k=1}^{n}D_iC_i\alpha_i \tag{5}$$

式中，S_{con} 为网络保密性价值防御指数，D_i 为第 i 台主机采取的防御行为的量化值，C_i 为第 i 台主机保密性价值状态值，α_i 为第 i 台主机的保密性价值比，n 为主机数。

网络保密性价值防御指数表征了针对攻击行为采取的防御措施的效果。防御行为量化方法如表 3 所列。

表 3 防御行为量化

D_i	行为描述
1	没有采取防御措施，攻击可达
0.7	采取地址转换控制措施，攻击不可达
0.3	采取防火墙访问控制措施，攻击不可达
0	采用物理隔离等手段，攻击不可达

网络的完整性价值是与保密性紧密相关的网络安全 CIA 属性，当它被攻击时也会对网络安全产生重大影响。由于攻击者对网络安全完整性价值属性的威胁较少，所以其量化的级数较少。网络的完整性状态的量化方法如表 4 所列。

表 4　完整性状态量化

I_i	状态描述
1	已被非授权用户访问
0.6	存在安全隐患，且受到攻击
0	不存在隐患，只有授权用户可以访问

网络的完整性状态受威胁的程度可以用下式计算：

$$R_{int}=\sum_{i=1}^{n} I_i\beta_i \tag{6}$$

式中，R_{int} 为网络完整性价值威胁指数，I_i 为第 i 台主机完整性价值状态值，β_i 为第 i 台主机的完整性价值比，n 为主机数。

采取防御行为后，网络的防御效果可以用下式计算：

$$S_{int}=1-\sum_{i=1}^{n} D_i I_i\beta_i \tag{7}$$

式中，S_{int} 为网络完整性价值防御指数，D_i 为第 i 台主机采取的防御行为的量化值，I_i 为第 i 台主机完整性价值状态值，β_i 为第 i 台主机的完整性价值比，n 为主机数。D_i 的量化方法如表 3 所列。

网络的可用性价值和保密性价值、完整性价值相比，具有其特殊性，攻击者对网络可用性价值发动攻击时，主要影响网络的正常功能，而保密性价值和完整性价值则可能不受影响。同时，由于网络自身故障及管理员自身原因也可能导致网络的可用性价值受影响，理想的安全评估方法不应将该情况作为受攻击的情形来处理。

网络的可用性状态的量化方法如表 5 所列。

表 5　可用性状态量化

A_i	状态描述
1	已被非授权用户控制
0.6	受到攻击，授权用户无法正常使用
0.3	受到攻击，但授权用户仍可正常使用
0	安全

网络自身故障和安全策略设置不当也可能导致网络的可用性价值降低，当攻击行为 A 满足 $A\in V$（V 为攻击向量）条件时，只有在攻击向量可能影响网络设备可用性价值的情况下，才能将攻击行为 A 当作针对可用性价值的攻击来处理。

网络的可用性状态受威胁的程度可以用下式计算：

$$R_{ava}=\sum_{i=1}^{n} A_i\gamma_i \tag{8}$$

式中，R_{ava} 为网络可用性价值威胁指数，A_i 为第 i 台主机可用性价值状态值，γ_i 为第 i 台主机的可用性价值比，n 为主机数。

采取防御行为后，网络的防御效果可以用下式计算：

$$S_{ava}=1-\sum_{i=1}^{n} D_i A_i\gamma_i \tag{9}$$

式中，S_{ava} 为网络完整性价值防御指数，D_i 为第 i 台主机采取的防御行为的量化值，A_i 为第 i 台主机可用性价值状态值，γ_i 为第 i 台主机的可用性价值比，n 为主机数。D_i 的量化方法如表 3 所列。

4　实验与分析

本文搭建如图 3 所示的实验环境。该实验环境包括 3 个子网，每个子网内都有入侵检测系统（IDS），用于检测网络的攻击事件。子网 2 和子网 3 都分别通过防火墙 2 和防火墙 3 与防火墙 1 相连，然后通过防火墙 1 与因特网相连，子网 1 通过防火墙 1 与因特网相连。各主机运行的服务信息如表 6 所列。

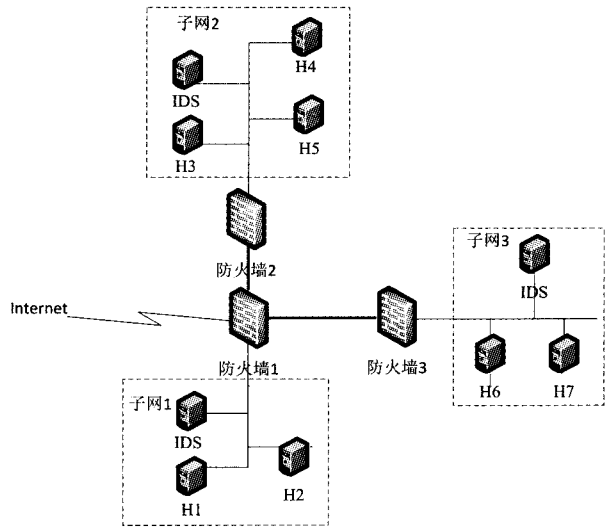


图 3　实验网络拓扑结构图

表 6　主机服务

主机名	操作系统	主机描述
H1	Linux	VPN 服务器
H2	Windows 2003 server	Web 服务器
H3	Linux	工作站
H4	Windows XP	工作站
H5	Windows XP	工作站
H6	Windows2003 server	FTP 服务器
H7	Windows XP	SQL Server 服务器

使用漏洞扫描工具对本文的实验网络进行扫描，得到实验网络的脆弱性数据。实验网络的脆弱性信息如表 7 所列。

表 7　主机脆弱性信息

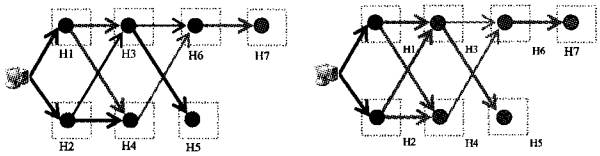
主机名	漏洞编号	漏洞信息	攻击成功概率
H1	V1	CVE-2004-0040	0.8
H2	V2	CVE-2006-2379	0.7
H3	V3	CVE-2003-0252	0.7
H4	V4	CVE-2004-0575	0.6
H5	V5	CVE-2006-2370	0.7
H6	V6	CVE-2004-1306	0.3
H7	V7	CVE-2004-0893	0.8

由扮演入侵者的实验人员发起攻击行为，入侵检测系统（IDS）实时检测并纪录网络中攻击行为，实验过程中记录的攻击行为如表 8 所列，为了便于了解攻防对抗过程，对应时间采取的防御行为也在该表中列出。

表 8　攻击行为

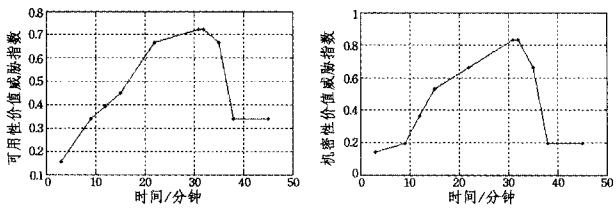
序号	时间	攻击源	攻击目标	漏洞信息	防御行为
1	01/12-14:02:58	H0	H1	CVE-2004-0040	无
2	01/12-14:09:08	H0	H2	CVE-2006-2379	无
3	01/12-14:11:51	H2	H3	CVE-2003-0252	无
4	01/12-14:15:26	H2	H4	CVE-2004-0575	无
5	01/12-14:22:37	H3	H6	CVE-2004-1306	无
6	01/12-14:31:51	H3	H5	CVE-2006-2370	无
7	01/12-14:32:32	H3	H5	CVE-2006-2370	限制 H3 主机对 H6 主机的访问
8	01/12-14:35:36	H3	H5	CVE-2006-2370	限制 H3 主机对 H5 主机的访问
9	01/12-14:37:51	H3	H5	CVE-2006-2370	限制 H2 主机对子网 2 的访问
10	01/12-14:45:05	H3	H5	CVE-2006-2370	无

根据主机的脆弱性信息、入侵检测系统的攻击纪录和防御行为纪录生成攻击路径图，如图 4 所示。

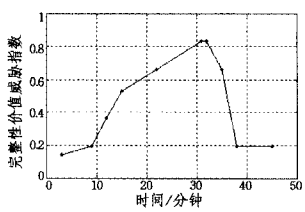


(a) 攻击路径图中的攻击行为　　(b) 攻击路径图中的防御行为

图 4



(a) 可用性价值威胁指数　　(b) 保密性价值威胁指数



(c) 完整性价值威胁指数

图 5

图 5 显示了遭受攻击后网络资产价值受到的威胁情况，当 H0 的攻击行为逐步成功后，网络的安全受到了越来越大的威胁。发现网络安全受到威胁后，通过修改防火墙 3 和防火墙 2 的访问策略，限制子网 1 到子网 2 的访问，阻断了 H0 的攻击路径，从而降低了 H0 主机对网络的威胁。

结束语　本文针对网络攻防对抗实时变化的特点，提出一种基于攻防对抗的网络安全动态评估方法。该方法对攻击过程和防御过程中网络设备的脆弱性状态变化进行量化评估，能较好地实现网络攻防过程的可视化。网络管理人员可以根据本文提供的结果直观、准确地了解当前的网络安全状态，从而为下一步采取的应对措施提供辅助决策支持。

参 考 文 献

[1] 韦勇，连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型[J]. 计算机学报，2009，32(4)：763-772

[2] Lau S. The spinning cube of potential doom[J]. Communications of the ACM，2004，47(6)：25-26

[3] 徐玮晟，张保稳，李生红. 网络安全评估方法研究进展[J]. 信息安全与通信保密，2009，50(4)

[4] 马俊春，王勇军，孙继银，等. 基于攻击图的网络安全评估方法研究[J]. 计算机应用研究，2012，29(3)

[5] Yu D，Frincke D. Improving the quality of alerts and predicting intruder's next goal with hidden colored Petri-net[J]. Computer Networks，2007，51(3)：632-654

[6] Aven T. A unified framework for risk and vulnerability analysis covering both safety and security[J]. Reliability Engineering and System Safety，2007，92(6)：745-754

[7] 廖年冬，易禹，胡琦. 动态实时网络安全风险评估研究[J]. 计算机工程与应用，2011，47(36)

[8] 陈锋，刘德辉，张怡，等. 基于威胁传播模型的层次化网络安全评估方法[J]. 计算机研究与发展，2011，48(6)：945-954

(上接第 198 页)

测试 2　在 KDDCUP99 入侵检测数据集中根据测试需要对网络流量进行分割，使得分割后的测试数据文件中只包含某一种特定的攻击。本测试从 4 大类典型攻击中随机选取以下 8 种特定攻击：Dos 类选取 pingofdeath 和 smurf；R2L 类选取 imap 和 named；U2R 类选取 overflow 和 Perl；PROBING 类选取 Nmap 和 IPsweep。

测试仍然采用进行 5 次再取其平均值的方式，测试结果如图 5 所示。

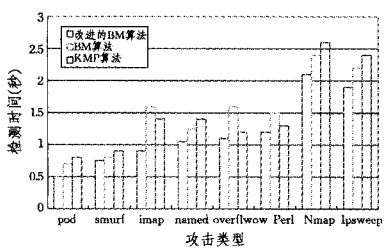


图 5　特定攻击检测

从本组测试结果可以看出：对于 imap 攻击、overflow 攻击和 Perl 攻击而言，KMP 算法的检测速度比 BM 算法分别快了 12.5%，24.8%，13.3%。而对于其它几种攻击，BM 算法的检测速度都比 KMP 算法快了近 7.6%～12.5%。而改进的 BM 算法对每一种攻击的时间性能都明显要优于其它两种算法。

结束语　Snort 的成功是建立在对源代码不断改进完善的基础之上的，因此本章提出了一种对 BM 的改进算法，增大了每轮匹配的移位量，并使用麻省理工学院林肯实验室的 KDD99 数据集作为数据源，对 3 种算法进行了离线的测试，针对混合类攻击和特定类攻击两方面的测试表明，采用本文的 BM 改进算法之后，Snort 的时间性能和空间性能都得到了优化，效率得到了一定的提升。

参 考 文 献

[1] 冉占军，姚全珠. 模式匹配算法在入侵检测中的应用[J]. 计算机应用技术，2011，21(12)：63-65

[2] 王新志，等. 一种面向软件行为可信性的入侵检测方法[J]. 中国科学技术大学学报，2011，41(7)：626-635

[3] 李雪莹，刘宝旭，许榕生. 字符串匹配技术研究[J]. 计算机工程，2011，30(22)：24-26

[4] 杨文君，魏占国，王玉平. 入侵检测系统中高效的模式匹配算法[J]. 小型微型计算机系统，2010，30(11)，2281-225

[5] Namjoshi K，Narlikar G. Robust and Fast Pattern Matching for Intrusion Detection [C]// IEEE Conference Computer Communications. Piscataway，2010：14-19

[6] Kim H J，Hong H，Kim H-S，et al. A Memory-Efficient Parallel String Matching for Inrusion Detection System [J]. IEEE Comunications Letters，2010，13(12)：1004-1006

[7] 郇正军. 基于 snort 的网络入侵检测系统研究[D]. 山东大学，2009：18-19

[8] 袁静波，郑吉森，丁顺利. 一种 BM 模式匹配算法的改进[J]. 计算机工程与应，2009，45(17)：105-107