软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(7):1638−1649 [doi: 10.13328/j.cnki.jos.004624]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于环境属性的网络威胁态势量化评估方法*

席荣荣, 云晓春, 张永铮

(中国科学院 信息工程研究所,北京 100093)

通讯作者: 云晓春, E-mail: yunxiaochun@cert.org.cn, http://js.caseducation.cn

摘 要: 传统的网络威胁态势评估方法主要是基于原始的警报信息,未结合目标网络的环境信息,使得方法的准确性受到很大的影响.提出了一种基于环境属性的网络威胁态势量化评估方法,该方法首先根据目标网络的环境属性对警报进行验证,判定引发警报的安全事件发生的可能性;然后,基于安全事件的风险级别及所针对的资产价值,分析安全事件发生后造成的损失;最后,基于安全事件发生的可能性及造成的损失量化评估网络的威胁态势.实例分析结果表明,该方法可以准确地量化评估网络的威胁态势.

关键词: 威胁态势量化评估;警报验证;环境属性;资产价值

中图法分类号: TP393

中文引用格式: 席荣荣,云晓春,张永铮.基于环境属性的网络威胁态势量化评估方法.软件学报,2015,26(7):1638−1649. http://www.jos.org.cn/1000-9825/4624.htm

英文引用格式: Xi RR, Yun XC, Zhang YZ. Quantitative threat situational assessment based on contextual information. Ruan Jian Xue Bao/Journal of Software, 2015,26(7):1638−1649 (in Chinese). http://www.jos.org.cn/1000-9825/4624.htm

Quantitative Threat Situational Assessment Based on Contextual Information

XI Rong-Rong, YUN Xiao-Chun, ZHANG Yong-Zheng

(Institute of Information Engineering, The Chinese Academy of Sciences, Beijing 100093, China)

Abstract: Traditional network threat situational assessment is based on primary alerts, however, its lack of access to contextual information compromises the accuracy of assessment. This paper proposes a method to quantitatively assess network threat situation based on not only alerts but also contextual information. The new method first verifies alerts along with contextual information to determine the successful possibility of events; then analyzes the loss caused by events according to the risk and the corresponding asset value of events; and finally quantitatively assesses network threat situation based on the successful possibility and the loss of events. Case studies show that the proposed method can evaluate network threat situations accurately.

Key words: threat situational assessment; alert verification; contextual information; asset value

网络的威胁态势是指网络面临的来自外部的各种恶意行为造成的危害和影响.网络威胁态势的分析,可以帮助安全管理人员准确、及时地把握网络安全状况及其发展趋势,为其提供决策支持.目前,网络威胁态势评估的主要方法之一是基于 IDS 产生的原始警报信息评估网络的威胁态势.如,Peng 等人[1−4]通过分析警报之间的逻辑关系对警报进行关联分析,基于关联结果分析网络的威胁态势.但是他们的研究假设所有的警报信息均代表成功的攻击行为,而在实际网络中,很大比例的警报为虚假警报或者不相关警报.文献[5]将 IDS 警报信息作为隐马尔可夫模型的观测序列,利用隐马尔可夫模型实时量化评估网络所处的安全状态.该方法可以有效评估网络的安全状态,但模型参数的合理设置存在很大的难度.文献[6]利用 IDS 警报,结合服务和主机的重要性构建了层次化网络安全威胁态势评估模型并提出了相应的量化计算方法,从而使该领域的研究推进了一大步,但其不

* 基金项目: 国家高技术研究发展计划(863)(2012AA012803, 2013AA014703); 国家科技支撑计划(2012BAH46B02); 国家自然科学基金(61070185); 中国科学院知识创新工程基金(XDA06030200)

收稿时间: 2013-08-20; 定稿时间: 2014-04-02

足在于未将警报信息与具体的网络环境信息相结合.基于上述研究中存在的问题,本文提出了一种基于环境属性的网络威胁态势量化评估方法.该方法首先根据目标网络的环境信息对警报进行验证,判定安全事件发生的可能性;然后,基于安全事件的风险级别及针对的目标资产价值分析安全事件发生后造成的损失,进而量化评估网络的威胁态势.

1 相关概念及描述

为了更加准确地描述网络威胁态势的评估,下面首先给出评估过程中的一些定义.

定义 1(警报(alert)). 警报是指由安全防护设备发出的、用于表明检测到可疑安全事件的通知,表示为

$$Alert=\{Name,Time,SIP,DIP,SP,DP,Description,Classification,Completion,Severity\},$$

其中,*Name* 表示警报的名称;*Time* 表示检测到警报的时间;*SIP* 和 *DIP* 表示警报的源 IP 和目的 IP;*SP* 和 *DP* 表示警报的源端口和目的端口;*Description* 表示警报的一些描述性信息,如警报所对应的操作系统等;*Classification* 表示警报的类型;*Completion* 表示警报所代表攻击完成的程度,即,攻击成功的概率;*Severity* 表示攻击的威胁严重度,即,攻击对目标系统造成的影响.

定义 2(警报验证(alert verification)). 警报验证是指将警报相关的信息和目标系统有关的配置信息进行匹配,以此来判定警报所代表的安全事件发生的概率.其中,

- 警报的相关信息是指警报的属性,如警报的名称 *Name*,警报的产生时间 *Time*,警报的源 IP、目的 IP,源端口,目的端口及警报的类型等属性;
- 目标系统的配置信息是指可对警报的分析提供辅助作用的所有目标网络信息,主要包括网络状态信息(stateinfo)和网络的脆弱性信息(vulninfo).

网络状态信息侧重描述网络中主机的信息,如主机类型、操作系统类型及版本、IP 地址、开放端口类型、提供服务类型等信息,可表示为

$$StateInfo=\{IP,Hostname,Role,State,OpenPort,PortState,Service,Ostype\},$$

其中,*IP* 表示系统状态监测信息所在主机 IP 地址;*Hostname* 表示主机名称;*Role* 表示主机的角色,如 router, switch,Web server,database 等;*State* 表示主机的状态,分为 Active 和 Inactive;*Openport* 表示主机上开放的端口;*PortState* 表示主机上开放端口的状态;*Service* 表示主机上运行的服务;*Ostype* 表示主机上运行的操作系统.

网络的脆弱性信息描述系统中存在的各种安全漏洞及漏洞的相关信息,表示为

$$VulnInfo=\{CVE\text{-}ID,IP,Port,Severity,Risk,Description\},$$

其中,*CVE-ID* 表示漏洞的 cve 编号,*IP* 表示发现该漏洞的主机 IP 地址,*Port* 表示漏洞所针对的主机端口号,*Severity* 表示该漏洞信息的严重程度,*Risk* 表示漏洞安全风险级别的高低,*Description* 表示漏洞的详细描述信息.

定义 3(环境属性相关度(contextual relevancy)). 环境属性相关度是指警报的相关信息与目标系统对应配置信息的匹配程度.匹配程度越高,相关性越强,引发警报的安全事件发生的可能性越高.

定义 4(资产价值(asset)). 资产价值是资产重要程度的表征.资产是指网络中有价值的信息或资源.资产的价值越高,资产对于网络安全性的影响越重要.

2 网络威胁态势量化评估方法

网络威胁态势不仅与网络受到的外部威胁有关,还与网络本身存在的脆弱性以及安全事件所针对的目标资产价值有关.基于外部威胁、内部脆弱性及资产价值这 3 个因素,威胁态势的评估流程如图 1 所示.

根据网络威胁态势评估原理图,本文提出了网络威胁态势量化评估方法.该算法首先通过分析警报与环境属性的相关度来评估引发警报的安全事件发生的可能性;然后,根据安全事件的风险级别及所针对的目标资产价值分析安全事件发生后所造成的损失;最后,基于安全事件发生的可能性及发生后造成的损失量化评估网络的威胁态势.

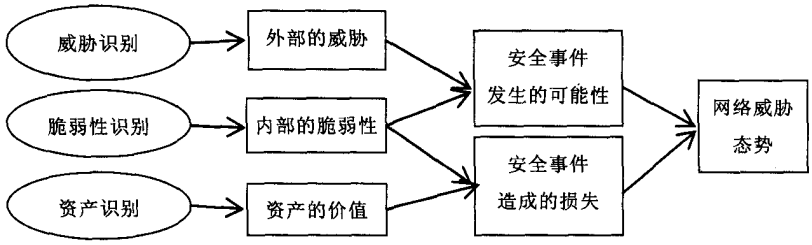


Fig.1 Diagram of network threat assessment

图 1 网络威胁态势评估原理图

2.1 安全事件发生的可能性

网络安全防护设备通常会产生海量的警报信息,但其中很大一部分恶意行为并没有发生,说明很多警报是与恶意行为无关的虚假警报或者是代表一个不成功事件的不相关警报[7].为了有效滤除虚假和不相关警报,更加准确地判定安全事件发生的可能性,本文提出了一种基于环境属性的入侵警报验证算法.该算法将警报相关的信息和目标网络的配置信息进行匹配,根据匹配程度判定引发警报的安全事件发生的可能性[8].

目前,大部分的警报验证方法主要是将安全事件所针对的漏洞与目标网络存在的漏洞相比较,确定警报与目标网络的相关性[9,10].即:警报验证方法只考虑了警报与目标网络漏洞的匹配,并没有考虑警报与其他环境信息的匹配,如操作系统、应用服务系统、安全配置等,在实际应用中存在一些局限性,主要有以下原因:(1) 存在漏洞并不代表安全事件一定发生,警报可能为虚假或者不相关警报;(2) 不是所有安全事件一定需要针对特定的漏洞才可以进行,如 DoS 攻击和 Probing 攻击就不需要目标网络存在明显的漏洞.因此,单纯依赖漏洞信息验证警报是不充分的.

基于环境属性的入侵警报验证算法解决了上述问题,它利用操作系统、应用服务、攻击漏洞、安全配置等多种目标网络环境信息进行警报验证,确定警报与目标网络的相关性,即,引发警报的安全事件发生的可能性.警报与目标网络环境信息匹配程度越高,表明警报与目标网络的相关性越强,引发警报的安全事件发生的可能性越高.将警报与目标网络的环境属性相关度,即,安全事件发生的可能性 P 定义为

$$P=\varpi_1 R_{OS}+\varpi_2 R_{Service}+\varpi_3 R_{Vulnerability}+\varpi_4 R_{Configuration} \tag{1}$$

(1) R_{OS} 表示警报与目标网络操作系统之间的相关度,操作系统为间接相关环境属性,相关度越高,安全事件发生的可能性越高;将操作系统与警报的相关度隶属函数定义为

$$R_{OS}=\begin{cases}1.0(A.DIP\in StateInfo.IP)\cap(StateInfo.state=Active)\cap(A.Description(OS)\subseteq StateInfo.Ostype)\\0.5(A.DIP\in StateInfo.IP)\cap(StateInfo.state=Active)\cap(A.Description(OS)=unknown)\\0(A.DIP\notin StateInfo.IP)\cup(StateInfo.state=Inactive)\cup(A.Description(OS)\notin StateInfo.Ostype)\end{cases}.$$

(2) $R_{Service}$ 表示警报与目标网络应用服务之间的相关度,应用服务为间接相关环境属性,相关度越高,安全事件发生的可能性越高;将应用服务与警报的相关度隶属函数定义为

$$R_{Service}=\begin{cases}1.0(A.DIP\in StateInfo.IP)\cap(StateInfo.State=Active)\cap\\\quad(A.DP\in StateInfo.OpenPort\cap(StateInfo.PortState=open)\\0.8(A.DIP\in StateInfo.IP)\cap(StateInfo.State=Active)\cap\\\quad(A.DP\in StateInfo.Open)\cap(StateInfo.PortState=unknown)\\0.6(A.DIP\in StateInfo.IP)\cap(StateInfo.State=Active))\cap(StateInfo.PortState=unknown)\\0.3(A.DIP\in StateInfo.IP)\cap(StateInfo.State=Active)\cap(A.DP=unknown)\\0(A.DIP\notin StateInfo.IP)\cap(StateInfo.State=Inactive)\cap(A.DP\notin StateInfo.Open)\end{cases}.$$

(3) $R_{Vulnerability}$ 表示警报与目标网络漏洞信息之间的相关度,漏洞信息为直接相关环境属性,匹配度越高,安全事件发生的可能性越高;将漏洞信息与警报的相关度隶属函数定义为

$$R_{Vulnerability}=\begin{cases}1.0(A.DIP\in VulnInfo.IP)\cap(A.Description(cve\text{-}id)\in VulnInfo.CVE\text{-}ID)\\0.5(A.Description(cve\text{-}id)=unknown)\\0(A.DIP\notin VulnInfo.IP)\cup(A.Description\notin VulnInfo.CVE\text{-}ID)\end{cases}.$$

(4) $R_{Configuration}$ 表示警报与目标网络安全配置信息之间的相关度,安全配置相关性则表现为对相关攻击的抑制或过滤防护作用,若其相关度越高,则安全事件发生的可能性越低.将安全配置信息与警报的相关度隶属函数定义为

$$R_{Configuration}=\begin{cases}1.0(StateInfo.Role\notin Securitymisc)\\0.5(StateInfo.Role=unkown)\\0(StateInfo.Role\in Securitymisc)\end{cases}.$$

(5) $W=[w_1,w_2,w_3,w_4]^T$ 为归一化权向量,表示各环境属性对安全事件发生的影响程度.本文采用优序图法确定权向量 W.优序图通过两两比较,分析各属性的重要程度.为了保证权向量的可靠性,本文对网络安全领域的50名专业人员进行了调查,针对每位专业人员的调查结果可构造如表1所示的优序图.将50张优序图中相应格的数字相加,汇总于表2.表2中,第 i 行 j 列的数字与第 j 行 i 列数字互补,互补值为参加调查的人数50,表明该优序图满足互补检验.把各行的数字横向相加,然后分别与总数 T 相除就可以得到各指标的权重值,其中,$T=n(n-1)m/2=4(4-1)50/2=300$.由表2可计算得到权向量 $W=[0.11,0.23,0.28,0.38]$.

Table 1 Precedence chart of one interviewee

表1 一名调查人员的优序图

	操作系统	服务	安全漏洞	防护措施
操作系统	■	0	0.5	0
服务	1	■	1	0
安全漏洞	0.5	0	■	0
防护措施	1	1	1	■

Table 2 Precedence chart of all interviewees

表2 所有调查人员的优序图汇总

	操作系统	服务	安全漏洞	防护措施	合计	权重
操作系统	■	8	11	15	**34**	**0.11**
服务	42	■	17.5	9	**69**	**0.23**
安全漏洞	39	32.5	■	12	**83**	**0.28**
防护措施	35	41	38	■	**114**	**0.38**

(6) 安全事件发生的可能性 $P\in[0,1]$,其取值越大,表示安全事件发生的可能性越大.

2.2 安全事件发生后造成的损失

不同的安全事件对网络造成的损失是不同的.例如,在 Internet 上非常普及的端口扫描行为,除了增加网络负荷外,并不会危及网络的安全性,表明探测类的安全事件的风险级别较低,该类安全事件造成的损失较小.而获得系统权限的攻击行为,利用系统级的漏洞造成缓冲区溢出,会完全攻陷网络系统,这表明获得系统权限类的安全事件的风险级别较高,该类安全事件会造成重大损失.

目前,对于安全事件造成的损失一般采用如下两种方式分析:

- 其一,通过与 IDS 的警报分级机制相结合量化评估安全事件造成的损失.

如,Snort 依安全事件对系统的影响程度将警报的优先级 Priority 分为高、中、低3级:Priority 为高,表示安全事件会造成严重的损失,如尝试获取管理员权限的攻击(attempted administrator privilege gain)、木马和网络应用程序攻击等;Priority 为中,表示安全事件造成的损失为中等,如 DoS 攻击、异常连接、可疑用户登录等;Priority 为低,表示安全事件会造成轻微的损失,包括网络扫描、ICMP 活动和一些普通协议命令的执行等.这种方法从安全事件的性质上来确定安全事件造成的损失,但安全事件只有高、中、低3个级别,对损失的量化不够精确.

- 其二,依据安全事件所针对的安全漏洞的风险级别量化评估安全事件造成的损失.

通用漏洞评分系统 CVSS(common vulnerability scoring system)是最著名和通用的方法,它已成为漏洞风险量化评估的标准.该方法基于安全事件所针对的安全漏洞的风险级别表征安全事件造成的损失,但是该方法存在一个局限性:对于不需要漏洞直接进行的攻击,无法量化安全事件造成的损失.

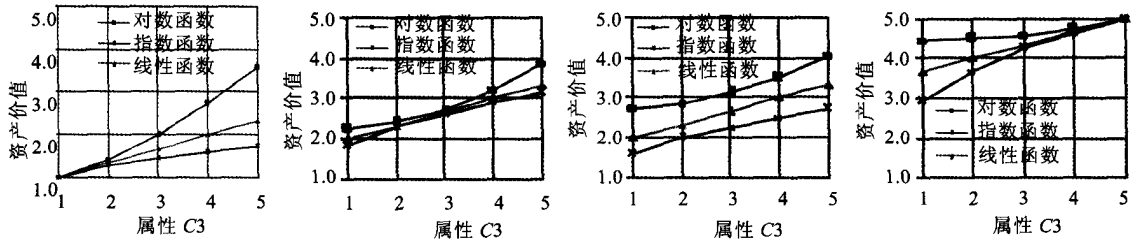
为解决不针对任何漏洞的安全事件的风险级别量化问题,本文对于不针对任何漏洞的安全事件,采用安全事件所属类别的风险值表征安全事件的风险级别,并结合安全事件针对的资产价值 *asset* 量化评估安全事件造成的损失,定义安全事件造成的损失 L 为

$$L=severity\times asset \tag{2}$$

(1) *Severity* 表示安全事件的风险级别:若安全事件是针对某个漏洞的,则采用相应的安全漏洞风险级别表征安全事件的风险级别;若安全事件不是针对某个漏洞的,则采用安全事件所属类别 classification 的风险值表征安全事件的风险级别.为了实现安全事件到其所属类别的映射,本文根据 IDS 的规则库构建了一个映射数据库.当采集到安全事件引发的警报信息时,通过查阅映射数据库,可直接将安全事件映射到其相应的类别.安全事件所属类别的风险值由该类别中所有可利用漏洞风险级别的平均值表征.依据通用漏洞评分系统CVSS的评分标准[11],$Severity\in[0,10]$,取值越大,表示安全事件的风险级别越高.

(2) *Asset* 表示安全事件所针对的资产价值.保密性、完整性和可用性是评估资产价值的 3 个安全属性.风险评估中,资产的价值不是以资产的经济价值来衡量的,而是由资产在这 3 个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的.不同的安全属性达成程度使得资产具有不同的价值,而资产面临的威胁、存在的脆弱性以及已采用的安全措施都将对资产安全属性的达成程度产生影响.根据资产在安全属性上的不同要求,将每个安全属性分为 5 个不同的等级,分别用 1,2,3,4,5 表示[12],对应资产在该属性缺失时对整个网络安全性的影响.

3 个安全属性对资产价值的影响并不是呈线性增加的,而是随着取值的增加,影响逐渐增强;且取值越高,对资产价值的影响越大.为了量化分析安全属性对资产价值的影响,本文采用常用的 3 种函数——线性函数、指数函数和对数函数分别对 3 种安全属性值的 125 种组合方式生成的资产价值进行了分析,其中,部分资产价值的分布趋势如图 2 所示.



(a) $C1=1$, $C2=1$ (b) $C1=2$, $C2=3$ (c) $C1=4$, $C2=1$ (d) $C1=5$, $C2=5$

Fig.2 Impact of security attributes for asset value

图 2 安全属性取值对资产价值的影响

图 2 中的 4 个子图分别表示当属性 1,2 取值确定时,随着属性 3 的变化,资产价值的变化趋势.图 2 表明:3 种函数都可以刻画随着安全属性取值的增加对资产价值的影响逐渐增大的特点;但是对于取值越高对资产价值影响越大的特点,只有对数函数的效果最佳.因此,本文采用对数函数量化安全属性对资产价值的影响,将资产价值 *asset* 确定为

$$asset = Round2\left(\log_2\left(\frac{w_1 2^{Conf} + w_2 2^{Int} + w_3 2^{avail}}{3}\right)\right) \tag{3}$$

其中,*Conf*,*Int*,*Avail* 分别表示资产在保密性、完整性和可用性上的安全等级,等级越高,表示该属性的缺失对网络安全性的影响越大;$\mathrm{Log}_2(\cdot)$表示取以 2 为底的对数;*Round*2(·)表示保留两位小数.

另外,由于网络对 3 种安全属性的需求有所不同,因此在计算资产价值时,本文引入了不同的权值 $W=[w_1,w_2,$

w_3],分别表示 3 种安全属性对资产价值的影响程度.根据文献[13]的调查,对于一般的应用网络,85%的被调查者认为可用性是最重要的,62%的被调查者认为完整性是 3 个属性中对资产价值影响最小的因子.采用层次分析法分析 3 个属性对资产价值的影响,求解得到 W=[0.26,0.1,0.64].

$asset$∈[1,5],取值越大,表示资产越重要,资产的安全属性被破坏后对网络造成的损失越严重.

(3) 安全事件造成的损失 L∈[0,50],取值越大,表示安全事件造成的损失越严重.

2.3 网络威胁态势的量化评估

根据计算出的安全事件发生的可能性 P 及安全事件造成的损失 L,量化评估网络的威胁态势值 R[14,15].

$$R=\frac{1}{n}\sum_{i=1}^{n}P[i]\times L[i] \tag{4}$$

其中,n 表示在采样周期内采集到的警报数目;R∈[0,50]表示网络的威胁态势值,值越大,表示网络受到的威胁越强,网络的安全性越低.

3 实验分析

为了描述算法融合数据的能力及算法对网络威胁态势值的调整作用,本文提出两个指标——数据约简率和误差修正值.

(1) 数据约简率(data reduction ratio,简称 DRR).

$$DRR=\frac{No.\ of\ validation\ alerts}{Total\ No.\ of\ alerts}\times 100\% \tag{5}$$

DRR 衡量原始警报的约简数目占所有已监测警报的比值,DRR 的值越小,表明算法的数据融合能力越强.

(2) 误差修正值(error correction value,简称 ECV).

$$ECV=|R^a-R^b| \tag{6}$$

误差修正值 ECV 用于描述对系统误差进行补偿的程度,在一定意义上表示误差减少的程度.ECV 的值越大,表明对系统的修正程度越高,修正方法的效果越明显.当然,由于系统误差不能完全获知,修正之后,系统误差会比修正之前减小,但不可能为 0,即,修正值只能对系统误差进行有限程度的补偿.

其中,R^a 表示与环境属性相关之后,根据本文算法计算所得的网络威胁值;R^b 表示未与环境属性相关之前所得到的风险值,同样由安全事件发生的可能性和造成的损失决定.但是,安全事件的可能性只考虑警报与漏洞信息的匹配程度,未结合其他环境属性,即,$P=R_{Vulnerbility}$;安全事件造成的损失由安全事件所针对的漏洞优先级决定,未结合安全事件的分类及所针对的资产价值,即,$L=Severity$.

3.1 实验1

据我们所知,目前还没有任何公开测试数据集评估网络的威胁态势.为了验证本文算法的有效性,我们构造了一个实验网络.实验网络的拓扑图如图 3 所示,其中,入侵检测系统 Snort[16]用于监测攻击,产生警报信息,OpenVAS[17]和 Nmap[18]采集网络系统中的环境信息.

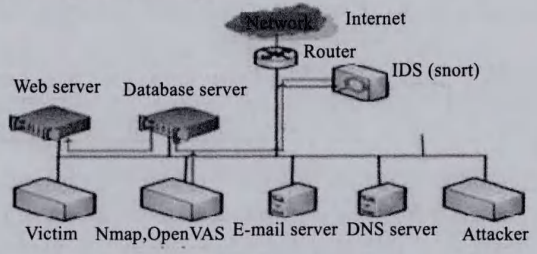


Fig.3 Topology of test network

图 3 实验网络的拓扑结构图

网络中关键设备的环境信息和主要的资产信息分别见表 3 和表 4.

Table 3 Contextual information of critical device in test network

表 3 实验网络中关键设备的环境信息

IP 地址 (192.168.158.)	操作系统	端口	漏洞	角色
80 (Web)	Ubuntu9.04	80, 8080	CVE-2009-0360, CVE-2012-0956, CVE-2012-4551	Server
110 (E-mail)	Redhat 7.2 Linux	110, 25	CVE-2011-5263, CVE-2012-4932, CVE-2013-0257	Server
53 (DNS)	Redhat 7.2 Linux	53	CVE-2012-4334, CVE-2012-3517	Server
50 (DataBase)	Ubuntu9.04	3306, 1521	CVE-2012-3328, CVE-2012-6355, CVE-2013-0880, CVE-2013-0911, CVE-2013-0676	Server
10 (Nmap, OpenVAS)	Ubuntu9.04	21, 80, 139, 3306	CVE-2012-4201, CVE-2012-4195, CVE-2013-0747	Host
9 (Victim)	Windows XP	21, 80, 135, 139, 443, 445, 1027, 1110, 3306, 8009, 8080, 19780	CVE-2010-5173, CVE-2012-2287, CVE-2012-2530, CVE-2012-4774, CVE-2012-2529, CVE-2013-1265 CVE-2013-1272, CVE-2013-0648, CVE-2013-2552, CVE-2013-1313	Host

Table 4 Asset in test network

表 4 网络中主要的资产信息

资产编号	资产名称	IP 地址	资产角色	安全属性			资产价值
				保密性	完整性	可用性	
NET_01	广域网路由器	192.168.158.1	网络设备	1	4	5	**4.06**
NET_02	入侵检测设备	192.168.158.40	安全设备	1	3	4	**3.12**
NET_03	Web 服务器	192.168.158.80	网络服务	2	3	4	**3.22**
NET_04	E-mail 服务器	192.168.158.110	网络服务	2	3	4	**3.22**
NET_05	DNS 服务器	192.168.158.53	网络服务	2	3	4	**3.22**
NET_06	Database 服务器	192.168.158.50	存储设备	2	1	4	**2.87**
NET_07	网络信息采集器	192.168.158.10	应用设备	1	2	4	**2.87**
NET_08	攻击主机	192.168.158.5	主机设备	1	1	1	**1.00**
NET_09	受害主机	192.168.158.9	主机设备	1	1	1	**1.00**

实验网络采集从 2013 年 3 月 18 日 13:30~3 月 22 日 13:30 的数据作为测试数据.数据被汇入数据库作为威胁态势评估的数据源.其中,模拟攻击的详细信息如下:

- 攻击场景 1:模拟扫描攻击,2013 年 3 月 19 日从 9:30~10:05,主机 Attacker 192.168.158.5 使用 Nmap, X-Scanner,ISS 对子网 192.168.158.0/24 执行 SYN 扫描、FIN 扫描和 UDP 扫描;
- 攻击场景 2:模拟 DoS 攻击,2013 年 3 月 20 日从 11:30~12:10,主机 Attacker 192.168.158.5 对主机 Victim192.168.158.9 发起 SYN flood 攻击.

下面将基于上述攻击场景产生的 IDS 报警日志以及网络的环境和资产信息,采用本文提出的算法分析网络威胁态势值的变化趋势.首先分析警报验证机制的数据融合能力,设定采样周期Δt为 5min,分别从正常的网络流量、攻击场景 1 和攻击场景 2 提取两个采样周期的数据分析算法的数据融合能力,结果见表 5.

Table 5 DRR of alert verification algorithm

表 5 警报验证算法的数据约简率

	背景		场景 1		场景 2	
	周期 1	周期 2	周期 3	周期 1	周期 2	周期 3
原始警报数目	365	298	1 656	1 678	1 735	1 806
有效警报数目	86	78	258	263	249	275
DRR	23.6%	26.2%	15.6%	15.7%	14.4%	15.2%

结果表明,警报验证机制具有数据融合能力.通过约简警报数目,使得管理员可以从海量警报信息中提取出具有代表性的警报信息,专注于真正的攻击行为.另外,结果还表明:正常网络流量时,DRR 的近似值为 25%;而在攻击情景 1 和情景 2 时,DRR 的近似值为 15%.表明,当具有攻击行为时,警报验证机制具有更好的融合能力.同样采用上述 6 个采样周期的数据,分析算法对于误差修正值的影响,结果见表 6,其相应的柱状图如图 4 所示.

Table 6 ECV of network threat assessment algorithm

表 6 网络威胁态势评估算法的误差修正值

	背景		场景 1		场景 2	
	周期 1	周期 2	周期 3	周期 4	周期 5	周期 6
R^b	18.35	14.3	22.3	21.05	30.6	31.45
R^a	17.25	11.95	28.1	27.1	36.2	37.9
ECV	1.1	2.35	5.8	6.05	5.6	6.45

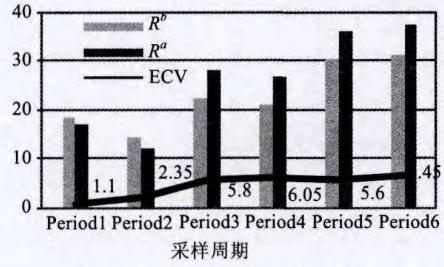
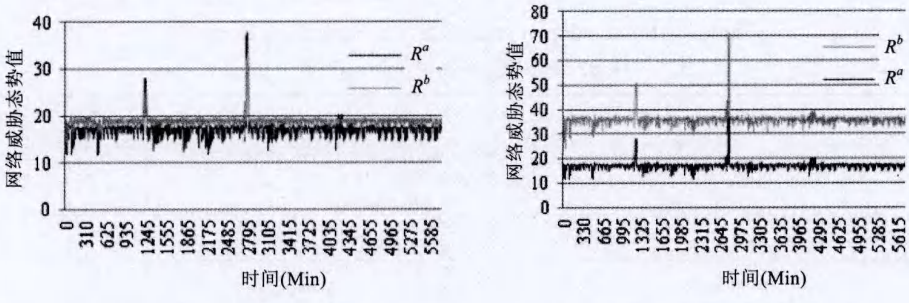


Fig.4 Distribution of ECV

图 4 误差修正值的分布图

图 4 表明:在正常网络流量时,即,在采样周期 1 和周期 2 期间,二者的相差幅度比较小,在 2.5 之下;而在网络具有攻击行为时,即,在采样周期 3~周期 6,相对于 R^b,R^a 增加的幅度更为明显,这表明,R^a 对于攻击行为的刻画更加准确.图 4 说明,采用警报验证机制和资产价值后所得到的网络威胁态势值 R^a 比之前的态势值 R^b 能够更加准确地描述网络安全状态的变化趋势.

最后计算在所有采样周期内的网络威胁态势值 R^a 和 R^b,结果如图 5 所示.



(a) 网络威胁态势值的折线图 (b) 网络威胁态势值的堆积折线图

Fig.5 Trend of network threat value

图 5 网络威胁态势值的变化趋势

图 5(a)表明:R^a 和 R^b 具有一致的网络安全态势变化趋势,即,在 1 200min 时都出现了小幅的波峰,说明在这一时段网络的安全状态发生了变化,出现了某种威胁,而模拟的扫描攻击正好发生在这个时段;在 2 760min 时,R^a 和 R^b 的值都出现了一个骤升的过程,说明在该时段网络安全状态急速恶化.根据模拟攻击场景的描述,在这个时间段,DoS 攻击正在进行.图 5(b)表明:相对于 R^b,R^a 能够更加明显地表征网络中的攻击行为.如图 5(b)所示,在 2 760min 时,R^b 的值从正常的 19.35 骤升至 31,而 R^a 的值则由 17 骤升至 36,具有更加明显的变化幅度.上述分析表明,本文提出的算法可以更加准确地反映网络安全态势的变化趋势.

3.2 实验2

为了对比分析算法的有效性,采用与文献[6]相同的数据集作为实验数据,即,采用 Honeynet 组织采集的

2000 年 11 月份的黑客攻击数据作为数据源,量化评估网络威胁态势的变化趋势.

Honeynet 组织的拓扑结构图如图 6 所示.

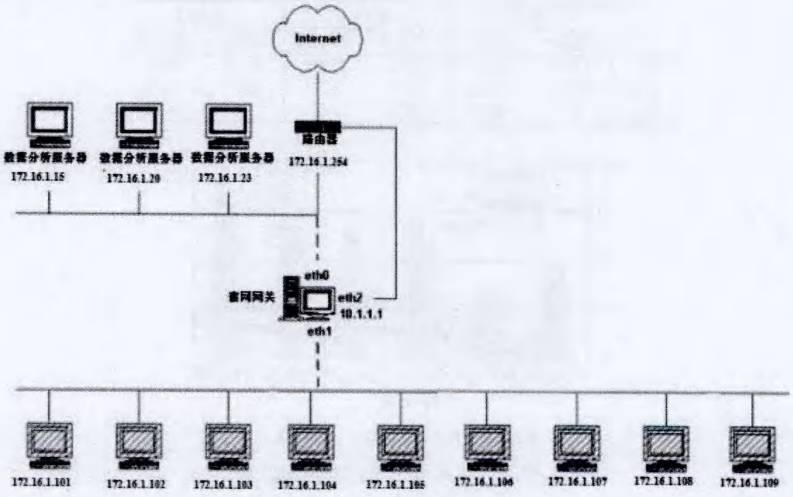


Fig.6 Topology of Honeynet collect hacking data

图 6 Honeynet 采集黑客攻击数据的拓扑结构图

Honeynet 组织构建的蜜网作为一种安全资源,其价值在于被扫描、攻击和攻陷,所以假设蜜网中攻击行为对应的端口是开放的;攻击对应的漏洞是存在的.基于上述两点假设,结合警报信息构建蜜网中关键设备的环境信息和资产信息,见表 7.

Table 7 Information of critical device and asset in Honeynet

表 7 Honeynet 中的关键设备信息和资产信息

IP 地址 (172.16.1.)	操作系统	端口	漏洞	角色	安全属性			资产价值
					C	I	A	
101	SunMicroSystems2.6	21, 23, 53, 111	CVE-1999-0789, CVE-1999-0073, CVE-1999-0696, CVE-2000-1042, CVE-2000-0508	Host	1	2	3	2.22
102	Windows98	21, 23, 111	CVE-1999-1544, CVE-2000-0666, CVE-1999-0208	Host	1	2	2	1.74
103	SunMicroSystems2.6	21, 23, 53, 111	CVE-1999-0219, CVE-1999-0218, VE-1999-0265, CVE-2000-1042	Host	1	2	3	2.22
104	Redhat 6.2 Linux	21, 23, 111	CVE-2000-0040, CVE-1999-0733, CVE-1999-0974, CVE-2000-0666	Host	1	2	2	1.74
105	Windows98	21, 53, 111	CVE-2000-1194, CVE-1999-0875, CVE-1999-0003, CVE-1999-0208, CVE-1999-1058	Host	1	2	2	1.74
106	Windows NT SP4	21, 53, 111	CVE-1999-1544, CVE-1999-0510, CVE-1999-0704, CVE-1999-0977	Host	1	2	2	1.74
107	Redhat 6.2 Linux	21, 23, 53, 80, 111, 1080	CVE-1999-0607, CVE-1999-0219, CVE-1999-1058, CVE-1999-0798, CVE-1999-0974, CVE-2000-0666	Server	2	3	5	3.87
108	SunMicroSystems2.6	21, 23, 111	CVE-1999-1544, CVE-2000-0733, CVE-1999-0696	Host	1	2	2	1.74
109	Windows98	21, 111	CVE-2000-1035, CVE-1999-0704	Host	1	1	1	1.00

由于 Honeynet 提供的警报数据已经过初步处理,因此实验中不再分析数据约简率.另外,层次分析法和环境属性法采用的是完全不同的算法,所以实验中也不对误差修正值进行分析.设定采样周期Δt 为 1 天,基于 Honeynet 提供的警报信息和构建的网络环境和资产信息,利用第 2 节介绍的算法量化评估网络的威胁态势值,得到的实验结果如图 7 所示.

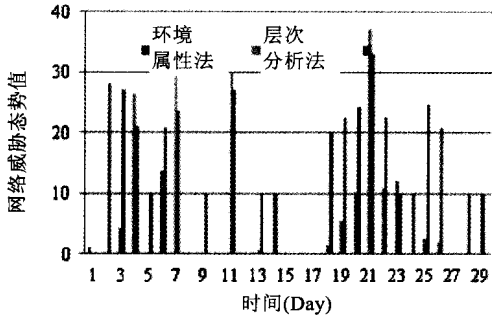


Fig.7 Trend of network threat value

图 7 网络威胁态势值的变化趋势

上述实验结果表明:

(1) 11 月 2 日,只产生了针对 WWW 服务的 CGI phf attempt 警报信息,环境属性法生成的威胁态势值为 28.2,而层次分析法的威胁态势值近似为 0.这主要是由于环境属性法对于 11 月 2 日产生的 CGI phf attempt 警报信息,根据警报相应的漏洞信息 CVE-1999-0607 及资产信息 172.16.1.107 量化分析网络的威胁态势值;而层次分析法将 CGI phf attempt 警报信息相应的 WWW 服务的权重值设置为 0.083,相对于 rpc 和 ftp 服务 0.25 的权重值,WWW 服务对于网络威胁态势值的影响极小,所以出现了威胁态势值近似为 0 的情况;

(2) 11 月 5 日、9 日、13 日、14 日以及 24 日、28 日和 29 日,环境属性法生成的威胁态势值为 10.14,而层次分析法生成的威胁态势值为 0.环境属性法对于黑客采集信息过程中产生的 portscan 警报信息,会根据引发警报的安全事件的风险级别及所针对的资产价值定量分析网络的威胁态势值;而层次分析法依据服务判定网络的威胁态势值,portscan 警报没有针对本文设定的 rpc 和 ftp 服务,所以层次分析法自动过滤了 portscan 警报信息表示的潜在威胁;

(3) 11 月 4 日、7 日、11 日以及 21 日,相对于环境属性法,层次分析法生成的威胁态势值变化幅度更加明显.上述采样周期内产生的警报信息主要是针对主机 172.16.1.107 的 rpc 和 ftp 服务的,层次分析法对 rpc 和 ftp 服务设置了 0.25 的较高权重值,而且对主机 172.16.1.107 设置了 40.5 的主机重要程度,所以层次分析法生成的风险值变化幅度更加明显.

上述分析表明:层次分析法对于已知的针对特定服务和目的主机的网络威胁进行量化评估,具有更高的准确性;而环境属性法对于未知的针对不确定服务和目的主机的网络威胁进行量化评估,准确性更高.

3.3 讨 论

完备的网络环境属性信息的获取是保证该方法有效性的关键,而衡量网络环境属性信息完备性的重要标准就是获取的网络环境属性信息是否能够准确反映网络安全态势的变化趋势.已知系统的脆弱性、外部威胁以及系统的资产价值这 3 个基本要素决定网络安全态势的变化趋势[12],且其相互之间的关系如图 8 所示.

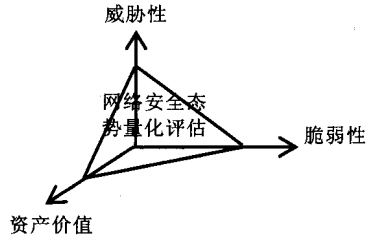


Fig.8 Basic elements of the network security situation assessment

图 8 评估网络安全态势的基本要素

基于网络安全态势评估的3个基本要素,本文对网络环境属性信息的获取主要从以下3个层面进行:

- 网络自身的脆弱性,它是造成系统被攻破的根本原因(内因).本文获取的 Vulnerability,OS,Service, Configuration 可从不同的角度描述系统自身的脆弱性;
- 外部威胁,它是造成系统被攻破的必要原因(外因).本文获取的 Alert 可用于描述系统的外部威胁;
- 系统资产价值,资产价值的重要程度是确定系统出现安全事故后可能造成的影响大小的必要指标.本文对资产价值的量化可准确衡量资产的重要程度.

上述分析表明:本文获取的网络环境属性信息涵盖了网络安全态势评估的各个方面,可提供完备的网络态势评估信息.

4 小 结

本文提出了一种基于环境属性的网络威胁态势量化评估方法,该方法首先结合目标网络的环境信息对警报进行验证,判定引发警报的安全事件发生的可能性;然后,基于安全事件的风险级别及所针对的目标资产价值分析安全事件发生后造成的损失,进而量化评估网络的威胁态势值.实例分析表明:该方法可以准确地反映网络威胁态势的变化趋势.但该方法还存在一些局限性,例如,本文对资产安全属性的赋值主要是基于网络资产的分类,但是资产分类中存在不全面或者相交的问题,导致资产价值的量化存在不确定性.另外,该方法对于安全事件的分类主要是基于映射数据库,而数据库的构建存在一定的主观性,限制了方法的应用.因此,下一步工作主要集中在这两个方向上.

References:

[1] Peng N, Cui Y, Reeves DS. Constructing attack scenarios through correlation of intrusion alerts. In: Proc. of the 9th ACM Conf. on Computer and Communications Security. ACM Press, 2002. 245−254. http://dl.acm.org/citation.cfm?doid=586110.586144

[2] Peng N, Xu D, Healey CG, St. Amant R. Building attack scenarios through integration of complementary alert correlation methods. In: Proc. of the 11th Annual Network and Distributed System Security Symp. 2004. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.60.4412

[3] Mohamed AB, Idris NB, Shanmugum B. Alert correlation framework using a novel clustering approach. In: Proc. of the 2012 Int'l Conf. on Computer & Information Science (ICCIS). IEEE, 2012. 403−408. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6297279&tag=1

[4] Bateni M, Baraani A, Ghorbani A. Using artificial immune system and fuzzy logic for alert correlation. Int'l Journal in Network Security, 2013,15(3):190−204.

[5] Li WM, Lei J, Dong J, Li ZT. An optimized method for real time network security quantification. Chinese Journal of Computers, 2009,32(4):793−804 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00793]

[6] Chen XZ, Zheng QH, Guan XH, Lin CG. Quantitative hierarchical threat evaluation model for network security. Ruan Jian Xue Bao/Journal of Software, 2006,17(4):885−897 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/885.htm

[7] Tian ZH, Wang BL, Zhang WZ, Ye JW, Zhang HL. Network intrusion detection method based on context verification. Journal of Computer Research and Development, 2013,50(3):498−508 (in Chinese with English abstract).

[8] Kruegel C, Robertson W. Alert verification determining the success of intrusion attempts. In: Proc. of the 1st Workshop the Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA 2004). 2004. 25−38. https://eldorado.tu-dortmund.de/handle/2003/22772

[9] Gula R. Correlating IDS alerts with vulnerability information. Technical Report, Tenable Network Security, 2011. https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/uploads/documents/whitepapers/va-ids-new.pdf

[10] Desai N. IDS correlation of VA data and IDS alerts. 2003. http://www.securityfocus.com/infocus/1708

[11] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system. IEEE Security & Privacy Magazine, 2006,4(6):85−89. [doi: 10.1109/MSP.2006.145]

[12] GB/T 20984-200, Information Security Technology—Risk Assessment Specification for Information Security. GB, 2007 (in Chinese).

[13] Fruhwirth C, Mannisto T. Improving CVSS-based vulnerability prioritization and response with context information. In: Proc. of the 2009 3rd Int'l Symp. on Empirical Software Engineering and Measurement. IEEE Computer Society, 2009. 535–544. [doi: 10.1109/ESEM.2009.5314230]

[14] Standards Australia and Standards. AS/NZS 4360: 2004 risk management. 2004.

[15] Xi RR, Yun XC, Jin SY, Zhang YZ. Network threat assessment based on alert verification. In: Proc. of the 12th Int'l Conf. on Parallel and Distributed Computing, Applications and Technologies (PDCAT). IEEE, 2011. 30–34. [doi: 10.1109/PDCAT.2011.57]

[16] Snort—The open source network intrusion detection system. 2013. http://www.snort.org

[17] OpenVAS—Open vulnerability assessment approach. 2013. http://www.openvas.org/

[18] Nmap—Free security scanner for network. 2013. http://nmap.org/

附中文参考文献:

[5] 李伟明,雷杰,董静,李之棠.一种优化的实时网络安全风险量化方法.计算机学报,2009,32(4):793–804. [doi: 10.3724/SP.J.1016.2009.00793]

[6] 陈秀真,郑庆华,管晓宏,林晨光.层次化网络安全威胁态势量化评估方法.软件学报,2006,17(4):885–897. http://www.jos.org.cn/1000-9825/17/885.htm

[7] 田志宏,王佰玲,张伟哲,叶建伟,张宏莉.上下文验证的网络入侵检测模型.计算机研究与发展,2013,50(3):498–508.

[12] GB/T 20984-2007,信息安全技术信息系统的风险评估规范.中华人民共和国国家标准,2007.

席荣荣(1979－),女,山西洪洞人,博士,助理研究员,CCF 会员,主要研究领域为网络安全,网络安全态势感知.

云晓春(1971－),男,博士,研究员,博士生导师,CCF 会员,主要研究领域为信息安全,计算机网络.

张永铮(1978－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为网络安全.