ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.4, April 2006, pp.885−897
DOI: 10.1360/jos170885

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

层次化网络安全威胁态势量化评估方法*

陈秀真[1+], 郑庆华[1], 管晓宏[1,2], 林晨光[1]

[1](西安交通大学 网络化系统与信息安全研究中心 制造系统工程国家重点实验室,陕西 西安 710049)

[2](清华大学 智能与网络化系统研究中心,北京 100084)

Quantitative Hierarchical Threat Evaluation Model for Network Security

CHEN Xiu-Zhen[1+], ZHENG Qing-Hua[1], GUAN Xiao-Hong[1,2], LIN Chen-Guang[1]

[1](State Key Laboratory of Manufacturing System, Center for Networked Systems and Information Security, Xi'an Jiaotong University, Xi'an 710049, China)

[2](Center for Intelligent and Networked Systems, Tsinghua University, Beijing 100084, China)

+ Corresponding author: Phn: +86-29-82663939, Fax: +86-29-82664233, E-mail: chenxz@sjtu.edu.cn

Chen XZ, Zheng QH, Guan XH, Lin CG. Quantitative hierarchical threat evaluation model for network security. *Journal of Software*, 2006,17(4):885−897. http://www.jos.org.cn/1000-9825/17/885.htm

Abstract: Evaluating security threat status is very important in network security management and analysis. A quantitative hierarchical threat evaluation model is developed in this paper to evaluate security threat status of a computer network system and the computational method is developed based on the structure of the network and the importance of services and hosts. The evaluation policy from bottom to top and from local to global is adopted in this model. The threat indexes of services, hosts and local networks are calculated by weighting the importance of services and hosts based on attack frequency, severity and network bandwidth consumption, and the security threat status is then evaluated. The experiment results show that this model can provide the intuitive security threat status in three hierarchies: services, hosts and local networks so that system administrators are freed from tedious analysis tasks based on the alarm datasets to have overall security status of the entire system. It is also possible for them to find the security behaviors of the system, to adjust the security strategies and to enhance the performance on system security. This model is valuable for guiding the security engineering practice and developing the tool of security risk evaluation.

Key words: network security; threat evaluation model; threat index; intrusion detection system; threat situation

摘 要: 安全评估是贯穿信息系统生命周期的重要管理手段,是制定和调整安全策略的基础和前提.只有充分识别系统安全风险,才能有针对性地采取有效的安全防范措施.基于 IDS(intrusion detection system)海量报警信息和网络性能指标,结合服务、主机本身的重要性及网络系统的组织结构,提出采用自下而上、先局部后整体评估策略的层次化安全威胁态势量化评估模型及其相应的计算方法.该方法在报警发生频率、报警严重性及其网

* Supported by the National Natural Science Foundation of China under Grant No.60243001 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2001AA140213 (国家高技术研究发展计划(863)); the National Outstanding Young Investigator of China under Grant No.6970025 (国家杰出青年基金)

Received 2004-06-09; Accepted 2005-07-11

络带宽耗用率的统计基础上,对服务、主机本身的重要性因子进行加权,计算服务、主机以及整个网络系统的威胁指数,进而评估分析安全威胁态势.实验表明,该系统减轻了管理员繁重的报警数据分析任务,能够提供服务、主机和网络系统 3 个层次的直观安全威胁态势,使其对系统的安全威胁状况有宏观的了解.而且,可以从安全态势曲线中发现安全规律,以便调整系统安全策略,更好地提高系统安全性能,为指导安全工程实践、设计相应安全风险评估和管理工具提供了有价值的模型和算法.

关键词: 网络安全;威胁评估模型;威胁指数;入侵检测系统;威胁态势
中图法分类号: TP393 文献标识码: A

连续运行的入侵检测系统(intrusion detection system,简称 IDS)报警量常常达到 G 数量级,据统计,最多的时候有 99%以上是无关报警[1].报警量大、不相关报警多,使安全管理员面对大量报警信息很难了解系统的安全威胁状况,不能及时采取合适的响应措施[2].为此,安全报警的管理分析成为网络安全领域的研究热点,涉及入侵事件归约、融合关联分析、安全评估等工作.而且,近几年的安全会议和权威性期刊中大量文献报道了攻击可视化、报警关联分析和复杂攻击建模 3 方面的研究工作.然而,评估网络系统安全威胁状况的研究工作开展得还很少,只停留在对单个攻击事件可能给系统造成威胁的评估上,不能提供切实有用的态势信息,不能为网络管理人员决策系统的安全状况提供帮助[3].网络安全威胁态势评估是一个比较年轻的课题,研究难度大,进展缓慢.

本文利用 IDS 报警信息和网络性能指标进行网络安全的定量威胁评估,根据网络系统的组织结构,基于服务、主机本身的重要性,提出一种层次化网络安全威胁态势评估模型及相应的量化计算方法,该模型从服务、主机及网络系统 3 个层次评估安全威胁态势,即提供一段时间内的安全威胁演化.这样,一方面,把管理员从海量的日志分析中解放出来,提供一种直观的安全威胁态势图,使管理员对系统的安全威胁状况有宏观的了解;另一方面,可从态势图中发现系统安全趋势和规律,以便调整系统的安全策略,更好地提高网络系统的安全性能.

本模型作为国家 863 计划项目“集成化网络安全防卫系统 Net-Keeper”中的一部分,属于网络安全监控系统的上层分析,采用 HoneyNet 和 CNSIS 数据进行测试,无论是在有效性还是正确性方面,均取得良好的评估效果.

1 相关工作

网络安全态势评估的研究按照数据源分为基于系统配置信息和基于系统运行信息两大类.前者是指系统设计、配置状况,包括服务设置、系统中存在的漏洞等;后者是指系统所受攻击的状况,主要来自于 IDS 日志库.

基于系统配置信息的安全评估是目前网络安全态势评估的重要部分.Ortalo 和 Deswarte 基于 COPS 提供的数据,采用权限图理论建模系统漏洞,使用马尔科夫模型计算攻击者击败系统安全目标可能付出的平均代价,以定量度量系统安全,给出系统安全的演化[4].肖道举等人基于服务在系统中所占的比重和漏洞威胁度给出一个综合评估模型,评估目标系统所提供服务的风险,定量分析目标系统的安全状况[5].冯登国研究员对信息安全风险评估领域的安全模型、评估标准、评估方法、评估工具等进行了综述,但主要集中在通过漏洞扫描等技术手段、依据评估标准或依赖量化脆弱性因素的评估指标进行的安全风险评估上[6].

基于系统运行信息的安全态势评估工作,目前只停留在单个事件给系统造成威胁的评估上.Bass 提出应用多传感器数据融合建立网络空间态势意识的框架,通过推理识别攻击者身份、攻击速度、威胁性和攻击目标,进而评估网络空间的安全意识[7],但没有实现具体原型系统.Information Extraction & Transport 开发 SSARE 用于广域的计算机攻击检测和态势、响应评估[8],但通过调查问卷的方式获得信息.Porras 提出基于系统任务影响的报警优先级评估方法,结合报警造成的严重后果、系统相关性和攻击目标的关键性等因素,评估报警流中每个报警的威胁程度[9].该方法只是孤立地分析每个报警、评估其威胁程度,不能提供直观的攻击态势曲线.Salim Hariri 等人基于网络性能度量指标,评估分析网络攻击对系统安全的影响[10],但这种方法只适用于分析拒绝服务(denial of service,简称 DoS)类攻击对系统安全的影响,不能评估权限提升类攻击对系统安全的威胁.对策理论被应用到安全威胁评估领域,实现实时定量的安全风险评估,但该方法依赖于专家经验确定策略矩阵[11];Blyth 提出通过观察黑客的攻击足迹,进而定性评估其安全威胁,但该方法不能给管理员提供全局的安全

威胁趋势状况[12].

结合已有研究成果,基于 IDS 取样数据和网络带宽占用率实现网络安全威胁态势的定量评估,即利用 IDS 日志库和系统资源使用,根据系统过去遭受攻击的记录情况,结合服务、主机自身的重要性,按照网络系统组织结构,提出一种层次化安全威胁态势定量评估模型及相应的量化计算方法,从服务、主机、局域网系统 3 个层次进行安全威胁态势评估,并使用 HoneyNet 和 CNSIS 数据进行实验测试.

2 安全威胁态势评估体系

2.1 层次化安全威胁评估模型

实际网络系统按规模和层次关系可分解为系统、主机、服务 3 层,而且大多数攻击是针对系统中主机上某一服务的.本文利用系统分解技术[13],根据网络系统组织结构,提出一个如图 1 所示的层次化网络系统安全威胁态势量化评估模型.从上到下分为网络系统、主机、服务和攻击/漏洞 4 个层次,采取“自下而上、先局部后整体”的评估策略.以 IDS 报警和漏洞信息为原始数据,结合网络资源耗用,发现各个主机所提供服务的威胁情况,在攻击层统计分析攻击严重程度、发生次数以及网络带宽占用率,进而评估各项服务的安全威胁状况.在此基础上,综合评估网络系统中各主机的安全状况.最后,根据网络系统结构评估整个局域网系统的安全威胁态势.

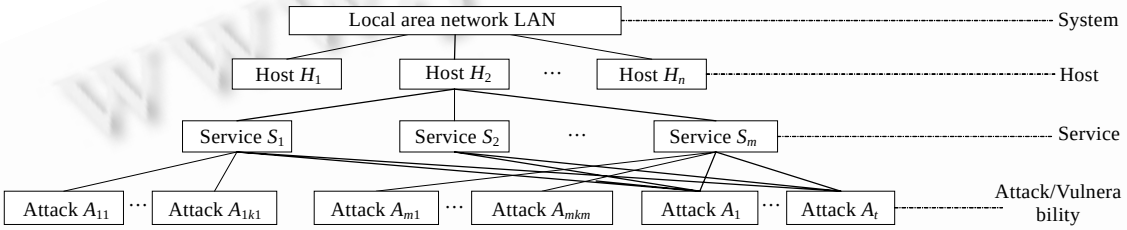

Fig.1 Hierarchical threat evaluation model for computer networks

图 1 层次化网络系统安全威胁态势评估模型

图 1 中,攻击层包含常见网络 IDS 能够检测到的攻击,主要有探测、权限提升和 DoS 三大类[14].其中,DoS 攻击(A_1,…,A_t)利用协议设计上的缺陷,通过向目标主机连续发送大量数据报耗尽网络资源,造成服务不可用,即 DoS 攻击威胁系统所有服务的安全.为叙述方便,本文定义以下概念:

定义 **1**. 攻击 A.引发 IDS 产生报警的黑客攻击行为,表示为 A={*Name*,*Time*,*Type*,*SIP*,*DIP*,*SP*,*DP*,*Pro*,*Priority*}.其中,*Name*,*Time*,*Type* 表示攻击特征、发生时间以及类型;*SIP*,*DIP* 代表源和目的地址;*SP*,*DP* 代表源和目的端口;*Pro* 表示协议类型;*Priority* 代表攻击威胁级别.

定义 **2**. 服务威胁指数 R_S.服务器上具有一定重要程度的服务在遭受一定数量的攻击时,其对应安全策略被违反的程度.

定义 **3**. 主机威胁指数 R_H.多个不同重要程度的服务在某时刻受到的威胁对服务器安全策略的违反程度.

定义 **4**. 网络系统威胁指数 R_L.多个遭受不同威胁程度的服务器对网络系统安全策略的总体违反程度.

2.2 安全威胁指数的定量计算

本文对定义的服务威胁指数 R_S、主机威胁指数 R_H和网络系统威胁指数 R_L 提出相应的量化计算方法,下面详细介绍各个层次安全威胁指数的定量计算.

2.2.1 服务级

攻击对服务的安全威胁与服务的正常访问量、威胁强度和攻击严重程度相关,而且,不同时段内服务的正常访问量不同,即同一攻击在不同时段内对服务造成不同的影响.给定分析时间窗口Δt,定义 t 时刻服务 S_j 的威胁指数为

$$R_{S_j}(t)=f(\vec{\theta},\vec{C}_j(t),\vec{D}_j(t),\vec{N}(t),\vec{D}_D)=\vec{\theta}\cdot(\vec{C}_j(t)\cdot 10^{\vec{D}_j(t)}+100\vec{N}(t)\cdot 10^{\vec{D}_D}) \quad (1)$$

其中:

(1) $\vec{\theta}=(\theta_1,...,\theta_h)$ 为正常访问量向量,h 为把一天划分的时段数,这里把一天分为 3 个时段:Δt_1=*Night*(0:00−8:00),Δt_2=*OfficeHour*(8:00−18:00),Δt_3=*Evening*(18:00−24:00),即 h=3, $\vec{\theta}=(\theta_1,\theta_2,\theta_3)$. $\vec{\theta}$ 的元素初值由系统管理员根据被保护网络系统不同时段的正常平均访问量 F_i(i=1,…,h)进行定量赋值,分别用 1,2,3,4,5 表示访问量:非常低、低、中、高、非常高,其取值越大,表示平均访问量越大.然后,对此进行归一化处理,得到 $\vec{\theta}$ 的元素值,即

$$\theta_i=\frac{F_i}{\sum_{t=1}^{h}F_t} \quad (2)$$

(2) $\vec{D}_j(t)=(\vec{D}_{1j},...,\vec{D}_{hj})$, $\vec{C}_j(t)=(\vec{C}_{1j},...,\vec{C}_{hj})$ 分别为 t 时刻攻击严重程度和发生次数向量,其元素 $\vec{D}_{ij}=(D_{ij1},...,D_{iju})$, $\vec{C}_{ij}=(C_{ij1},...,C_{iju})$ (i=1,…,h)为第 i 个时段内从 t 至 $t+\Delta t$ 时刻,针对服务 S_j 的各种攻击的严重程度和发生次数,u 为 Δt 时间内攻击种类数,u 和 $\vec{C}_{ij}$ 的取值通过统计攻击事件日志数据库得到.

(3) 为了提高评估的合理度,本文对不同严重等级的入侵事件的威胁指数的等效性进行了调查,大多数安全研究人员普遍认同:100 次严重度为 1 的事件威胁指数与 10 次严重度为 2 的事件威胁指数、1 次严重度为 3 的事件威胁指数是等效的.为此,本文把 $\vec{C}_{ij}\cdot\vec{D}_{ij}$ 修正为 $\vec{C}_{ij}\cdot 10^{\vec{D}_{ij}}$, $10^{\vec{D}_{ij}}$ 运算定义为 $10^{\vec{D}_{ij}}=(10^{D_{ij1}},...,10^{D_{iju}})$,以突出评价指标值中较小者的作用[15],即突出攻击严重度在威胁指数计算中的比重,避免威胁指数计算结果在一些特殊情况下与实际情况存在偏差.比如,根据对入侵事件威胁指数等效性的调查结果,3 次严重度为 1 的攻击事件对系统造成的实际危害比 1 次严重度为 3 的攻击事件要小,但使用 $\vec{C}_{ij}\cdot\vec{D}_{ij}$ 的威胁指数计算方法有(3)·(1)=3=(1)·(3),显然与实际情况不符,而采用 $\vec{C}_{ij}\cdot 10^{\vec{D}_{ij}}$ 有(3)·$10^{(1)}$=30<(1)·$10^{(3)}$=1000,与实际情况相符.

(4) $\vec{N}(t)=(\vec{N}_1,...,\vec{N}_h)$, $\vec{D}_D=(\vec{D}_{D_1},...,\vec{D}_{D_h})$ 分别为网络带宽占用率和 DoS 攻击的威胁等级向量,其元素 $\vec{N}_i=(N_{i1},...,N_{iv})$, $\vec{D}_{D_i}=(D_{D_{i1}},...,D_{D_{iv}})$ (i=1,…,h)为第 i 个时段内各个时间窗的网络带宽占用率和 DoS 攻击的威胁等级,v 为第 i 个时段内的分析时间窗口数.$100\vec{N}(t)$ 的系数 100 是为了把网络带宽占用率转为整数,进而评估 DoS 攻击的威胁.

(5) R_{S_j} 值越大,表示威胁程度越高,应该引起管理员的高度重视.而且,计算 R_{S_j} 的意义在于计算出一段连续时期内的安全威胁值,将这些值进行比较,从而判断出服务 S_j 的安全威胁趋势.

2.2.2 主机级

在时刻 t 主机 H_k 的威胁指数为

$$R_{H_k}(t)=f(\vec{R}_S(t),\vec{V})=\vec{V}\cdot\vec{R}_S(t) \quad (3)$$

其中:

(1) $\vec{R}_S(t)=(R_{S_1},...,R_{S_m})$ 为 t 时刻主机 H_k 的服务安全威胁向量,元素 R_{S_i} ($i=1,...,m$) 为根据式(1)计算出来的服务 S_i 的安全威胁指数,m 为主机 H_k 开通的服务数.

(2) $\vec{V}=(v_1,...,v_m)$ 为服务在主机开通的所有服务中所占权重向量,其元素取值根据主机 H_k 提供服务的重要性 IM_i(i=1,…,m)来确定,分别用 1,2,3 表示服务的重要程度:低、中、高.然后,对重要性 IM_i 进行归一化处理得到向量 $\vec{V}$ 的元素值,即

$$v_i=\frac{IM_i}{\sum_{t=1}^{m}IM_t} \quad (4)$$

(3) 威胁指数 R_{H_k} 取值越大,表示主机 H_k 威胁程度越高,其意义还在于计算出一段连续时期内 R_{H_k} 值,并进行比较,从而判断主机 H_k 在这一段时期内的安全威胁趋势.

2.2.3 网络系统级

在时刻 t 网络系统 LAN 的威胁指数为

$$R_L(t)=f(\vec{R}_H(t),\vec{W})=\vec{W}\cdot\vec{R}_H(t) \tag{5}$$

其中:

(1) $\vec{R}_H(t)=(R_{H_1},...,R_{H_n})$ 为 t 时刻网络系统内主机的安全威胁向量,元素 $R_{H_l}(l=1,...,n)$ 为根据式(3)计算出来的主机 H_l 的威胁指数,n 为网络系统内的主机数.

(2) $\vec{W}=(w_1,...,w_n)$ 为主机在被评估局域网中所占重要性的权重向量,其元素取值根据各主机在局域网中的地位 $ST_i(i=1,\ldots,n)$来确定.

(3) 网络系统威胁指数 R_L 取值越大,表示危险程度越高,其含义也在于计算出一段连续时期内 R_L 的值,并进行比较,进而判断这段时期网络系统的安全威胁趋势.

2.3 参数确定

在服务、主机和网络系统 3 个层次的威胁指数计算中,需确定攻击的威胁严重度、网络带宽占用率、服务重要性权重和主机重要性权重 4 个参数,下面分别加以详细介绍.

2.3.1 威胁严重度

攻击的威胁严重度既与攻击可能带来的后果有关,也与攻击的有效性相关.IDS 报警日志中包含一些不相关的无效攻击尝试,这些信息只表示黑客存在攻击企图.因此,为提高评估结果的合理性,避免在发生大量无效的攻击尝试、成功攻击次数很少的情况下,安全威胁态势图存在一定的误导.本文在 Snort 用户手册提供的攻击优先级划分基础上,关联漏洞评估数据和 IDS 报警信息,降低无效攻击的威胁度[14].该方法使无效攻击对应的威胁指数成为一个较小的值,这提示管理员威胁存在,但危险很小.其算法如下:

首先,根据 Snort 用户手册攻击分类与优先级划分来确定攻击的严重度[16],其根据攻击类别把严重度划分为高、中、低 3 个等级,分别用 3,2,1 表示.表 1 是从 Snort 用户手册中摘录的部分攻击类别及其对应的严重度.

Table 1 Attack types and severities

表 **1** 攻击类别与严重度

Attack types	Attack description	Severity
Attempted-Admin	Attempt to gain administrator privilege	High
Attempted-User	Attempt to gain ordinary user privilege	High
Attempted-Dos	Attempt to denial of service	Medium

其次,对无效尝试攻击的威胁度进行降级处理,即把攻击事件 A 依赖的特定条件 T 与目标系统漏洞信息集 I 不符的事件的威胁级别降为低,表达为

$$[A,(A_{.DIP}=IP_l\in K)\cap(A_{.DP}\in Z_l)\cap(T\notin I)]\Rightarrow A_{.Priority}=low \tag{6}$$

其中:$K=\{IP_1,\ldots,IP_d\}$为系统的合法地址集,d 为主机数;$Z_l=\{Port_1,\ldots,Port_b\}$为主机 IP_l 开放的端口集,b 为主机 IP_l 开放的端口数;$I=\{V_1,\ldots,V_g\}$为系统漏洞信息,g 为系统漏洞数.

2.3.2 网络带宽占用率

基于攻击次数的威胁分析,难以客观反映 DoS 攻击时的状态.本文结合常见 DoS 攻击的原理:通过消耗网络带宽致使拒绝服务[17],提出使用网络带宽占用率指标,度量 DoS 攻击发生时的威胁.网络带宽占用率定义为

$$N_{ij}=\begin{cases}\dfrac{NB'}{NB_{\max}}\times 100\%, & \dfrac{NB'}{NB_{\max}}\geq N_t\\ 0, & \dfrac{NB'}{NB_{\max}}<N_t\end{cases} \tag{7}$$

其中,NB',$NB_{\max}$ 分别为当前网络带宽占用和最大可用网络带宽;N_t 为网络带宽占用率阈值,即可接受的运行模式下最大的网络带宽占用率,需结合实验统计分析和专家经验确定.这里,确定 N_t 为 0.7,当 $N_{ij}\geq 0.7$ 时,使用网络带宽占用率度量其威胁,不统计 DoS 攻击引发的报警.

2.3.3 服务重要性权重

服务重要性的确定是一种动态、多变量、人为因素起主要作用的评估,不确定因素多、逻辑关系复杂,而且这些因素动态变化,难以建立服务重要性评估模型.本文结合客观统计信息和主观经验知识——主流服务的用户数目越多、访问频率越大,服务的重要性越高,制定表 2 所示的服务重要性判断原则.其中主流服务为布尔变量:取值为 1 表示是主流服务;反之为非主流服务.

Table 2 Determination principles of service importance degree

表 **2** 服务重要性判断原则

Numbering	Mainstream service	Number of users	Access frequency (times/day)	Service importance degree
1	1	[0,20)	[0,50)	Medium
2	1	[20,50)	[50,100)	Medium
3	1	[50,∞)	[100,∞)	High
4	1	[0,20)	[50,100)	Medium
5	1	[0,20)	[100,∞)	Medium
6	1	[20,50)	[0,50)	Medium
7	1	[20,50)	[100,∞)	High
8	1	[50,∞)	[0,50)	Medium
9	1	[50,∞)	[50,100)	High
10	0	[0,20))	[0,50)	Low
11	0	[20,50)	[50,100)	Medium
12	0	[50,∞)	[100,∞)	Medium
13	0	[0,20)	[50,100)	Low
14	0	[0,20)	[100,∞)	Medium
15	0	[20,50)	[0,50)	Low
16	0	[20,50)	[100,∞)	Medium
17	0	[50,∞)	[0,50)	Medium
18	0	[50,∞)	[50,100)	Medium

2.3.4 主机重要性权重

主机重要性取决于服务器类型、服务器中数据的重要性等许多因素,仍然是一个动态、多变量、人为因素起主要作用的评估,没有通用的用于评估主机重要性的准则.本文基于主机中各个服务的重要性信息:各个重要级别的服务数,并根据直观经验知识:重要程度高的服务数越多,主机在局域网中的地位越高,定义主机在局域网中的地位为

$$ST_i=k_hN_h+k_mN_m+k_lN_l \tag{8}$$

其中,N_h,N_m 和 N_l 分别为主机 H_i 上高、中、低 3 个重要程度的服务数目;k_h,k_m 和 k_l 分别为高、中、低 3 个重要程度对应的量化分值,其取值基于表 2 提供的重要性判断原则信息,确定如下:

(1) 定义服务 S_j 的主流性 ms,用户数目 un,访问频率 af 对应的量化值分别为

$$V_{ms}=\begin{cases}0, & ms=0\\ 10, & ms=1\end{cases},\quad V_{un}=\begin{cases}4, & un\in[0,20)\\ 8, & un\in[20,50)\\ 12, & un\in[50,\infty)\end{cases},\quad V_{af}=\begin{cases}4, & af\in[0,50)\\ 8, & af\in[50,100)\\ 12, & af\in[100,\infty)\end{cases}.$$

(2) 在服务重要性判断中,基于安全管理人员的专家经验知识:服务的主流性所占比重最大,用户访问频率和用户数目占有同等比重,定义服务重要性的量化值为

$$IV=\frac{1}{2}V_{ms}+\frac{1}{4}V_{un}+\frac{1}{4}V_{af} \tag{9}$$

(3) 根据表 2 中的规则,结合式(9),可以确定高、中、低 3 个重要程度的服务对应的量化值区间 $[IV_{h_a}, IV_{h_b}]$,$[IV_{m_a}, IV_{m_b}]$,$[IV_{l_a}, IV_{l_b}]$,由此得到

$$k_h=\frac{IV_{h_a}+IV_{h_b}}{2}, k_m=\frac{IV_{m_a}+IV_{m_b}}{2}, k_l=\frac{IV_{l_a}+IV_{l_b}}{2} \tag{10}$$

然后,对主机重要性 ST_i 进行归一化处理,得到向量 $\vec{W}$ 的元素值,即主机重要性权重:

$$w_i = \frac{ST_i}{\sum_{t=1}^{n} ST_t} \tag{11}$$

3 实验分析

为衡量无效攻击的威胁度降级方法在提高安全威胁态势图的指导意义的有效性,定义误导抑制率(decreased misleading rate,简称 DMR)为

$$DMR = \frac{R_S{}^b - R_S{}^a}{Rs^b} \times 100\%, \qquad DMR \in [0,1) \tag{12}$$

其中 R_S^b, R_S^a 为对无效攻击的威胁度降级前、后的服务威胁指数.误导抑制率 DMR 越大,对系统危害大的攻击在态势图中得以明显体现,安全威胁态势图的指导意义越大.

下面详细介绍使用 HoneyNet 和 CNSIS 数据进行的实验,以验证层次化安全威胁态势评估模型的有效性.

3.1 实验1

采用 HoneyNet 组织收集的黑客攻击数据集(简称 HoneyNet 数据[18])作为实验数据,包含扫描、rpc.statd 和 ftp 缓冲区溢出攻击 3 类[19].该数据集用于实现“分析过去、预测未来”,反映出黑客的行为模式特征,有助于发现安全趋势和规律.

以 2000 年 11 月份数据为例进行安全威胁态势评估,分析这一个月内系统、主机及主机上运行服务的安全威胁状态演化.由于 HoneyNet 组织没有提供网络拓扑结构及主机的服务信息,给安全威胁态势评估系统的分析带来了困难.本文从报警信息中构建仅有关键服务器的简化网络拓扑,通过分析报警数据的目的 IP 和目的端口,得出如图 2 所示的 HoneyNet 网络系统层次化安全威胁态势评估模型.

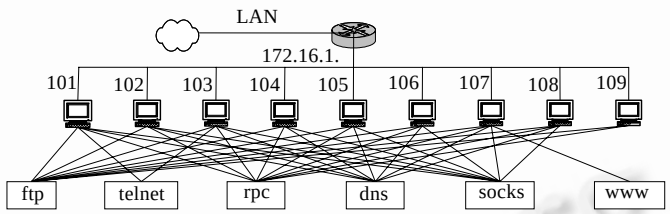

Fig.2 Hierarchical threat evaluation model in HoneyNet network

图 2 HoneyNet 网络系统层次化安全威胁态势评估模型

设定Δt 为 1 天,对 *Night*,*OfficeHour*,*Evening* 三个时段的 F_i 赋以 1,3,2,分别表示访问量:非常低、中、低,归一化处理得到 $\vec{\theta} = (0.167, 0.5, 0.333)$.系统内主机、服务及其重要性信息见表 3.

Table 3 Information about hosts, running services and their importances in HoneyNet network

表 3 HoneyNet 网络内主机、服务及其重要性

IP	Running services	Degree of service importance	Weights of service importance	Degree of host importance	Weights of host importance
101	{ftp, telnet, rpc, dns, socks}	{3, 1, 3, 3, 2}	(0.25, 0.083, 0.25, 0.25, 0.167)	40.5	0.122
102	{ftp, rpc, dns, socks}	{3, 3, 3, 2}	(0.273, 0.273, 0.273, 0.181)	38	0.114
103	{ftp, telnet, rpc, dns, socks}	{3, 1, 3, 3, 2}	(0.25, 0.083, 0.25, 0.25, 0.167)	40.5	0.122
104	{ftp, rpc, dns, socks}	{3, 3, 3, 2}	(0.273, 0.273, 0.273, 0.181)	38	0.114
105	{ftp, rpc, dns, socks}	{3, 3, 3, 2}	(0.273, 0.273, 0.273, 0.181)	38	0.114
106	{ftp, rpc, dns, socks}	{3, 3, 3, 2}	(0.273, 0.273, 0.273, 0.181)	38	0.114
107	{ftp, rpc, dns, socks, www}	{3, 3, 3, 2, 1}	(0.25, 0.25, 0.25, 0.25, 0.167, 0.083)	40.5	0.122
108	{ftp, rpc, dns, socks}	{3, 3, 3, 2}	(0.273, 0.273, 0.273, 0.181)	38	0.114
109	{ftp, rpc}	{3, 3}	(0.5, 0.5)	21	0.063

利用第 2 部分介绍的网络系统安全威胁评估计算方法,分析图 2 所示的模型,得到如下实验结果:

(1) HoneyNet 系统服务级安全威胁态势(以 IP107 主机 ftp,www,rpc 服务为例)

图 3 直观地给出 ftp, rpc 和 www 三个服务的安全威胁态势.利用 HoneyNet 系统中主机的默认配置信息[19]分析报警数据,没有发现一些不相关的无效攻击尝试,这与 BlackHat 黑客组织的技术水平有关.因此,在这个实验中不进行误导抑制率的分析.图 3 给管理员提供以下直观信息:1) 系统中开通的 rpc 服务受到频繁攻击,说明 rpc 服务可能存在较多或较容易攻破的漏洞,值得管理员对这个服务的设置情况进行检查;2) 2000 年 11 月 3 日~4 日、11 月 6 日~7 日、11 月 10 日~13 日和 11 月 19 日~22 日是攻击比较密集的时间段,这些时段为周末前后.这一方面说明周末相对于平时来说,更容易遭受黑客攻击,需要更加小心防范;另一方面说明可能不是全职黑客,在周末不上班时发动攻击,便于缩小黑客范围.

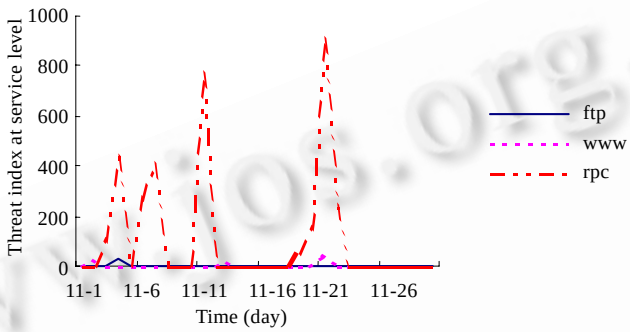

Fig.3 Threat situation at service level on IP107 host

图 3 IP107 主机的服务级安全威胁态势图

(2) HoneyNet 系统中主机级的安全威胁态势(以主机 IP101, IP104, IP107 为例)

图 4 给出 HoneyNet 系统中主机级的威胁态势图,提供了以下直观信息:1) 类似于图 3 给出的信息,在周末前后主机容易受到攻击,因此在周末前后时段中,网络系统中主机的安全应该更加重视;2) 对于某一主机而言,通常它在前后 2~3 天中持续危险程度比较高.因此,对于系统管理员而言,当某天发现某一主机遭受了攻击,在随后几天内,仍应该对该主机保持高度重视,黑客可能还会对它进行攻击,或者利用它作为跳板来攻击其他主机.

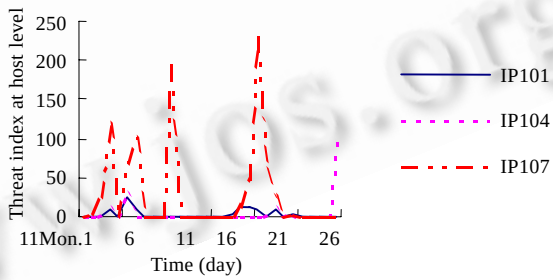

Fig.4 Threat situation of IP101, IP104 and IP107 hosts

图 4 IP101,IP104,IP107 主机的安全威胁态势图

(3) HoneyNet 系统级安全威胁态势

图 5 给出整个系统的威胁态势图,提供了以下信息:1) 类似于图 3、图 4 所给出的,网络系统在周末前后的危险指数明显高于非周末时期,这提示系统管理员必须对周末时期的系统安全更加重视;2) 通常系统会在连续几天中,威胁指数持续偏高.这提示系统管理员一旦发现系统受到比较明显的攻击,在之后的几天需要继续保持注意,因为随后这几天系统遭受攻击的可能性比较高.

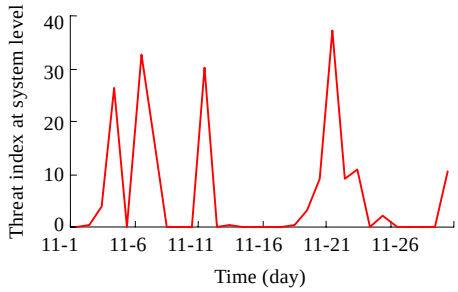

Fig.5 Threat situation of HoneyNet network

图 5 HoneyNet 网络系统的安全威胁态势图

在图 3~图 5 中,威胁指数值越大,说明越不安全,对系统安全策略的违反程度越大.从安全威胁态势曲线中,可以清晰地看出一个月内服务、主机、网络系统的安全威胁态势以及系统的安全威胁演化规律.

3.2 实验2

测试环境为 CNSIS 局域网,100M 局域网网段 192.168.1.0/24 共享一个 C 类地址 202.117.14.189 联入 Internet.受保护服务器的操作系统有 Red Hat Linux 6.2 和 7.2,在内网的 mail 服务器、ftp 服务器和 samba 服务器分别布置 Snort 2.0.2,XJTU Sensor 和 Snort 2.1.0.每个 IDS 产生的事件存入数据中心,作为安全威胁态势评估数据源.3 个受保护服务器的配置信息、根据服务重要性判断原则确定的各个主机的服务重要性权重向量以及根据式(8)确定的局域网中主机的重要性权重向量见表 4.

Table 4 Configuration information of three servers in CNSIS

表 4 服务器配置信息

IP address (192.168.1.)	Operation system	Service	Version information of the server	Degree of service importance	Weights of service importance	Degree of host importance	Weights of host importance
243 (mail server)	Red Hat Linux (7.2)	mail	imapc-2000c-15	High	0.375	26	0.302
		ftp	wu-ftpd-2.6.1-18	Medium	0.25		
		rpc	nfs-utils-0.3.1-13	Medium	0.25		
		telnet	telnet-0.17-20	Low	0.125		
24 (ftp server)	Red Hat Linux (6.2)	ftp	wu-ftpd-2.6.0 (1)	High	0.3	32.5	0.378
		mail	sendmail-8.9.3-20	Medium	0.2		
		dns	bind-8.2.2	Medium	0.2		
		telnet	telnet-0.16-6	Medium	0.2		
		rpc	nfs-utils-0.1.6-2	Low	0.1		
251 (samba server)	Red Hat Linux (7.2)	samba	samba-2.2.1a-4	High	0.375	27.5	0.32
		telnet	telnet-0.17-20	High	0.375		
		www	apache-1.3.20	Medium	0.25		

基于表 4,建立如图 6 所示的 CNSIS 局域网层次化安全威胁态势评估模型.管理员根据 *Night*,*OfficeHour* 和 *Evening* 三个时段的平均正常访问量大小,对 $F_i(i=1,2,3)$分别赋值为 2,5,4 表示访问量:低、非常高、高,经过归一化处理得到 $\vec{\theta}=(0.18, 0.45, 0.37)$.

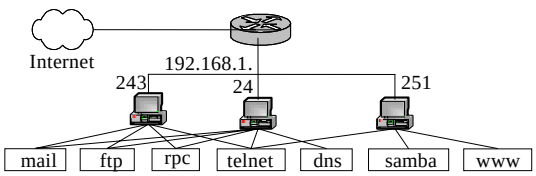

Fig.6 Threat evaluation model in CNSIS

图 6 CNSIS 局域网层次化安全威胁态势评估模型

安排学生模拟黑客,在指定时间和主机上对 3 个受保护服务器发起扫描、缓冲区溢出、DoS 等攻击,而且包含无效的攻击尝试和有效攻击,实验时间长达 1 天.分析 IDS 报警日志以及网络资源的使用,进一步获取各个时期的安全威胁状况.设定Δt 为 1 分钟,使用提出的层次化安全威胁态势评估模型及其相应的计算方法,得出服务、主机和系统 3 个层次的安全威胁演化.分析结果如下:

(1) CNSIS 服务级安全威胁态势(以 ftp 服务器的 ftp 和 mail 服务为例)

图 7、图 8 给出 ftp 服务器的两个服务在降级前后的安全威胁态势.实验中,17:59 分 47 次 serv-u directory traversal 攻击的威胁等级进行了降级处理,从中级别降为低,这主要因为其针对 Windows 系统 serv-u 软件的 Unicode 实现错误漏洞[20],而目标主机为 Linux 系统.此时,降级前、后的威胁指数分别为: R^b_{FTP} = (0.18,0.45, 0.37)·(0,(4,50,0)·$10^{(1,2,3)}$)=2268, R^a_{FTP} =(0.18,0.45,0.37)·(0,(51,3,0)·$10^{(1,2,3)}$,0)=364.5,误导抑制率为 DMR = 83.93%. 在 17:38,17:58 分别发起一次成功的 wu-ftp 缓冲区溢出攻击,统计引发的报警信息,得出威胁指数: R'_{FTP} =(0.18, 0.45,0.37)·(0,(0,77,1)·$10^{(1,2,3)}$,0)=3915.比较 R^b_{FTP} , R^a_{FTP} 和 R'_{FTP} ,可以看出,对系统危害大的攻击,在态势图中得以明显体现,威胁态势图具有很大的指导意义.另外,图 7 和图 8 给管理员提供了 ftp 服务遭受攻击比较频繁的信息,值得管理员检查有关 ftp 服务的配置和漏洞信息.

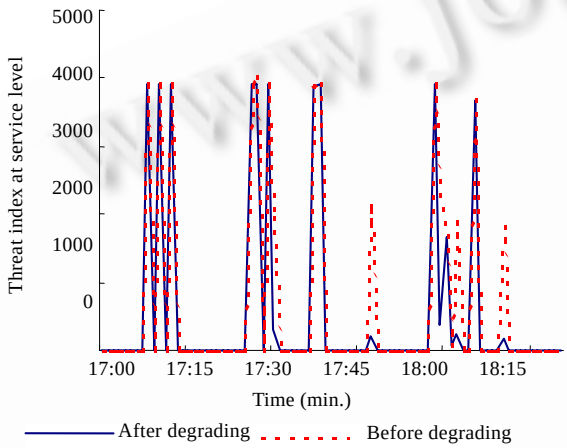

Fig.7 Threat situation of ftp service on ftp server

图 7 ftp 服务器的 ftp 服务安全威胁态势

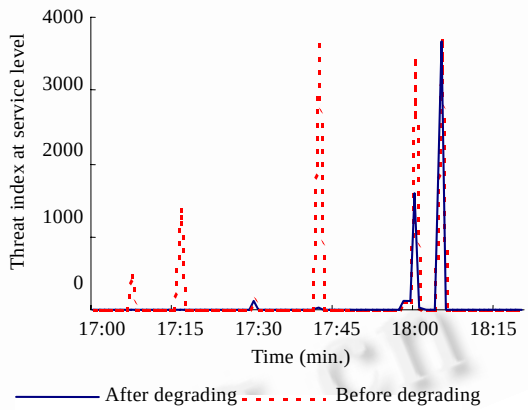

Fig.8 Threat situation of mail service on ftp server

图 8 ftp 服务器的 mail 服务安全威胁态势

实验过程中,网络带宽占用率的演化如图 9 所示.在 18:05 发起的 ping flood 攻击引起网络带宽占用率迅速增加,致使 2 个服务的安全威胁指数增大(如图 7 和图 8 所示).

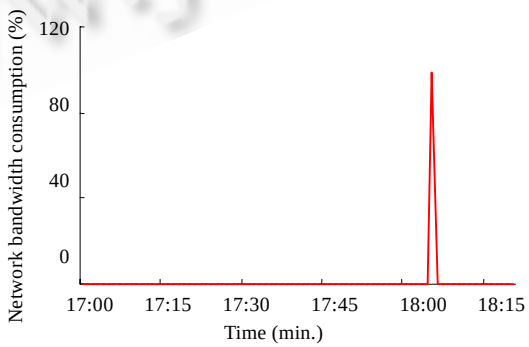

Fig.9 Network bandwidth consumption of ftp server

图 9 ftp 服务器的网络带宽占用率

(2) 主机 CNSIS 级安全威胁态势

图 10 给出 CNSIS 主机级安全威胁态势,分析该图可以清晰地看出 CNSIS 局域网内 3 个服务器的安全威胁指数演化,samba 服务器在 17:35~17:45 的威胁指数连续偏高,值得管理员尽快查找威胁指数增大的原因.

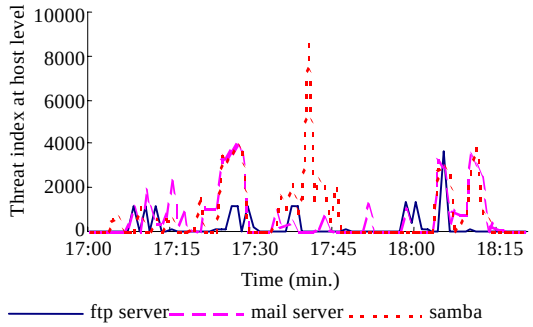

Fig.10 Threat situation at host level

图 10 主机级安全威胁态势

(3) CNSIS 系统级安全威胁态势

从图 11 可以直观地发现 CNSIS 局域网系统的安全威胁状况,系统在 17:24~17:28,18:04~18:05,18:10~18:12 安全威胁指数很大,说明系统运行状况很差,应引起管理员高度重视,尽快分析系统日志,查找遭受攻击的信息.

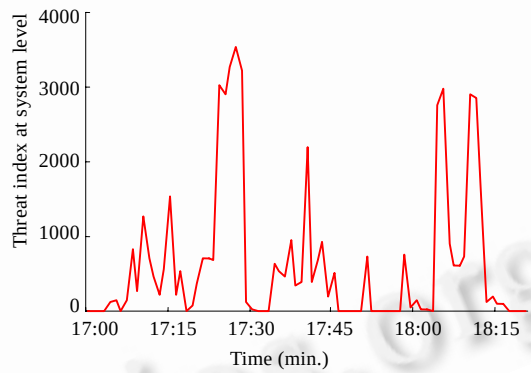

Fig.11 Threat situation at CNSIS system level

图 11 CNSIS 系统级安全威胁态势

以上两个实验测试表明:

(1) 提出的层次化安全威胁态势评估模型具有合理性,各个级别的安全威胁指数与所受攻击的严重性、攻击强度和攻击目标的重要性紧密相关,是一个整体性的综合评价值;

(2) 结合网络带宽占用率评估 DoS 攻击的威胁,使得评估结果更加合理;

(3) HoneyNet 数据分析表明:较大的统计分析时间窗口可以提供宏观的安全威胁态势图.从长时期的安全威胁态势曲线中可以发现安全规律,确定黑客范围(全职黑客、业余黑客),以便更好地进行安全防范;

(4) CNSIS 数据分析表明:选用较小的统计分析时间窗口,可以提供微观的系统安全威胁态势图,实现系统安全威胁的动态监控.实验测试还表明,关联漏洞评估数据对无效尝试攻击的威胁度进行降级处理的方法,提高了威胁态势图的指导意义.而且,无效攻击尝试的次数越多、威胁度越大,降级前后的威胁指数相差越大,安全威胁态势图的误导抑制率也越大.

4 结论及工作展望

实验表明,提出的层次化网络安全威胁态势定量评估模型能够直观地给出整个网络系统、主机和服务 3 个层次的安全威胁态势,使网络管理员能够及时了解系统安全动态,查找安全变化的原因,调整安全策略,保证系统安全最大化.而且,从长时期的安全威胁态势曲线中可以发现安全威胁演化规律.该系统在 Net-Keeper 系统中得到很好的应用,能够合理评估常见网络攻击对系统安全的威胁,将管理员从繁重的报警数据分析任务中解脱出来.

目前,安全威胁态势评估系统的实验分析基于网络入侵检测传感器报警日志和网络带宽占用率,但这些信息还不能全面反映黑客的攻击行为,诸如获取系统权限后执行的命令操作.进一步工作的重点是:(1) 研究融合 NIDS(network-based IDS)和 HIDS(host-based IDS)报警日志等多源信息的方法,结合用户以及文件访问行为信息,进一步提高安全威胁态势评估精度;(2) 研究适合于多网段的局域网和大规模网络系统的安全威胁评估模型.

致谢 在此,我们向对本文的工作给予支持和建议的专家表示感谢.

References:

[1] Cuppens F, Miège A. Alert correlation in a cooperative intrusion detection framework. In: IEEE Symp. on Security and Privacy. Oakland, 2002. 12−15. http://ieeexplore.ieee.org/iel5/7873/21681/01004372.pdf?tp=&arnumber=1004372&isnumber=21681

[2] Qin XZ, Lee WK. Statistical causality analysis of INFOSEC alert data. In: Proc. of the 6th Int'l Symp. on Recent Advances in Intrusion Detection. Pittsburgh, 2003. 73−93. http://www.springerlink.com/media/c5jhqhlrukegjxhpyddj/contributions/u/t/m/h/utmhwugc5lwjnfh6_html/BodyRef/PDF/558_10953587_Chapter_5.pdf

[3] Bass T. Intrusion systems and multisensor data fusion: Creating cyberspace situational awareness. Communications of the ACM, 2000,43(4):99−105.

[4] Ortalo R, Deswarte Y, Kaâniche M. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Trans. on Software Engineering, 1999,25(5):633−651.

[5] Xiao DJ, Yang SJ, Zhou KF, Chen XS. A study of evaluation model for network security. Journal of Huazhong University of Science & Technology (Nature Science Edition), 2002,30(4):37−39 (in Chinese with English abstract).

[6] Feng DG, Zhang Y, Zhang YQ. Survey of information security risk assessment. Journal of China Institute of Communications, 2004,25(7):10−18 (in Chinese with English abstract).

[7] Bass T. Multisensor data fusion for next generation distributed intrusion detection systems. In: 1999 IRIS National Symp. on Sensor and Data Fusion. Laurel, 1999. 24−27.

[8] D'Ambrosio B, Takikawa M, Upper D, Fitzgerald J, Mahoney S. Security situation assessment and response evaluation. In: DARPA Information Survivability Conf. & Exposition II. Anaheirn, 2001. 387−394. http://ieeexplore.ieee.org/iel5/7418/20170/00932233.pdf?tp=&arnumber=932233&isnumber=20170

[9] Porras P, Fong M, Valdes A. A mission-impact-based approach to INFOSEC alarm correlation. In: Proc. of the 15th Int'l Symp. on Recent Advances in Intrusion Detection. Zurich, 2002. 95−114. http://www.springerlink.com/media/mh9xdpqyrr0wq6tvxceg/contributions/2/4/8/7/2487wb0an7qq8art.pdf

[10] Hariri S, Qu GZ, Dharmagadda T, *et al*. Impact analysis of faults and attacks in large-scale networks. IEEE Security & Privacy, 2003,1(5):49−54.

[11] Cohen F. Managing network security attack and defense strategies. 2004. http://www.blacksheepnetworks.com/security/info/misc/9907.html

[12] Blyth A. Footprinting for intrusion detection and threat assessment. Information Security Technical Report, 1999,4(3):43−53.

[13] Wang CX, Wulf WA. Towards a framework for security measurement. In: Proc. of the 20th National Information Systems Security Conf. Baltimore, 1997. 7−10. http://csrc.nist.gov/nissc/1997/proceedings/522.pdf

[14] Lippmann R, Webster S, Stetson D. The effect of identifying vulnerabilities and patching software on the utility of network intrusion detection. In: Proc. of the 15th Int'l Symp. on Recent Advances in Intrusion Detection. Zurich, 2002. 307−326. http://www.springerlink.com/media/320e3xk18j1vuwbe6k1p/contributions/w/2/6/5/w265fm4f77n2nm7a.pdf

[15] Guo YJ. Theory and Method of Comprehensive Evaluation. Beijing: Science Press, 2002 (in Chinese).

[16] Roesch M, Green C. Snort users manual, snort release 2.0.0. 2003. http://www.snort.org/docs/SnortUsersManual.pdf

[17] Qu GZ, Pakash J, Kishore R, Hariri S. A framework for network vulnerability analysis. 2003. http://www.ece.arizona.edu/~hpdc/projects/nvat/NV-framework.pdf

[18] Project H. Know your enemy: Statistics. 2002. http://www.honeynet.org/papers/stats/

[19] Project H. Scan 17. 2002. http://www.honeynet.org/scans/scan17/

[20] SecurityFocus™. Serv-U FTP directory traversal vulnerability. 2003. http://www.securityfocus.com/bid/2052

附中文参考文献:

[5] 肖道举,杨素娟,周开锋,陈晓苏.网络安全评估模型研究.华中科技大学学报(自然科学版),2002,30(4):37−39.

[6] 冯登国,张阳,张玉清.信息安全风险评估综述.通信学报,2004,25(7):10−18.

[15] 郭亚军.综合评价理论与方法.北京:科学出版社,2002.

陈秀真(1977–),女,山东聊城人,博士生,主要研究领域为计算机网络安全检测与评估.

管晓宏(1955–),男,博士,教授,博士生导师,主要研究领域为计算机网络信息安全,系统优化与调度.

郑庆华(1969–),男,博士,教授,博士生导师,主要研究领域为计算机网络信息安全,智能网络学习环境.

林晨光(1977－),男,硕士生,主要研究领域为计算机网络安全漏洞评估,入侵检测.