基于裁减代价的入侵检测系统规则集优化研究和实现

孙成峰[1]，龚俭[1]，杨望[1]

（1.东南大学计算机科学与工程学院，南京，211189）

摘　要：目前大规模入侵检测系统存在大量的无关警报和误报，同时入侵检测效率也直接取决于用于检测的规则集质量，因此提出了基于裁减代价的入侵检测系统规则集最优化模型。依据入侵检测系统规则集的裁剪代价进行拆分，分为生成警报代价、漏报损失代价和误报损失代价三部分，依次对各部分代价进行分析并量化。再此基础上，进一步分析最优化模型，采用贪心算法的思想，将规则集的全局最优化模型转变为局部最优化模型，从而简化计算方案。最后对一个实际的网络入侵检测系统进行实验，表明方案的可行性，并在 2763 条规则中筛选出与僵尸网络相关规则 510 条。

关键词：优化；规则集；入侵检测系统；网络安全

Optimizing Rule Sets of Intrusion Detection System Based on Reduction Cost

Sun Chengfeng[1], Gong Jian[1], Yang Wang[1]

(1. School of Mechanical Engineering, Southeast University, Nanjing, 211189)

Abstract: It is well knonwn fact that a large number of irrelevant alerts and false positives commonly exist in large-scale intrusion detection system and the efficiency of intrusion detection is directly dependent on the quality of rule sets for the detection. So this paper proposes the optimization model of rule based on reduction cost. By split, the reduction cost of rule sets is divided into three parts, these are Generation Alert Cost, False Negative Damage Cost, and False Positive Damage Cost, which are analyzed and quantized. And then replace global optimization model with local optimization mode by further analysis of optimization models for simplifying calculation. Lastly, experiment on a practical system, showing the feasibility of the model, and filter 510 rules relation with botnet from 2763 rules.

Key words: Optimization; Rule Sets; Intrusion Detection System; Network Security

1　引言

过去几年里，每年主要类型的安全事件数量均近成倍增加[1]，网络的安全形势日趋严峻。僵尸网络(Botnet)由于为攻击者提供了隐匿、灵活且高效的一对多控制机制，得到了攻击者的青睐和进一步的发展，从而已成为因特网最为严重的安全威胁之一[2]。利用僵尸网络，攻击者可以轻易地控制成千上万台主机对因特网任意站点发起分布式拒绝服务攻击，发送大量垃圾邮件，从受控主机上窃取敏感信息或进行点击欺诈以牟取经济利益[3]。

入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。但是现有的滥用入侵监测系统，存在大量的无关警报和误警报，这使得安全管理员需要浪费大量的时间和精力。同时在规则集选取中，误裁剪一些相关规则，导致漏报一些攻击行为，加重了日益严峻网络的安全形势。而 Botnet 检测规则集作为入侵检测系统（IDS）进行 Botnet 攻击行为判别的基础核心部件，其设计的优劣对网络入侵检测系统的总体性能起着决定性的影响。因此，开展规则集的优化设计工作对解决入侵检测系统当前存在的一些问题，提高系统的检测效率将起到极大的帮助作用。

针对此现状，近年来有许多学者开展了针对入侵检测系统规则集优化的研究，常见的方法有基于攻击先验概率的规则集筛选[4]。但是对于这类优化

作者简介：孙成峰，（1988-），男，硕士研究生，E-mail：cfsun@njnet.edu.cn；龚俭，（1957-），男，教授、博士生导师，E-mail：jgong@njnet.edu.cn；杨望，（1979-），男，讲师，E-mail：wyang@njnet.edu.cn

方法，大多仅从优化目标入手，未能结合规则集的漏报、误报情况。本文提出了基于裁剪代价的入侵检测系统规则集最优化模型，结合了规则集本身信息和相应的警报信息，选取最优规则集。

本文第一节首先对网络安全背景和规则集优化现状进行了介绍，强调了入侵检测系统规则集优化的意义。第二节对规则集优化问题进行了研究，提出了基于裁剪代价的规则集最优化模型，并给出了规则集裁剪的具体算法。第三节对一个实际的网络入侵检测系统进行了实验，并从可行性角度对算法进行了验证。第四节为最后一节，对基于裁剪代价的规则集最优化模型进行了总结。

2 基于裁剪代价的规则集最优化模型

2.1 模型的基本原理

设入侵检测系统一共有 n 条规则，规则集为 $R=\{R_1,R_2,\cdots,R_n\}$。对于规则集 R，规则裁剪模型需要从 R 中选出最优规则集，该模型的关键是如何定义“最优”。

图 1.1 是一个矩阵，横坐标表示用户的行为，$1\sim n$ 表示 n 类攻击行为，横坐标 $n+1$ 表示正常行为；纵坐标表示 IDS 的检测结果，$1\sim n$ 表示对应的 n 类攻击行为，$n+1$ 表示正常行为。于是 (i,j) 表示：用户的行为是 i 并且相应的 1DS 检测结果为 j，则 IDS 的检测结果可以分为以下几类[5]：

（1） True Positive：对应集合 $\{(i,j)|i=j且i,j\in\{1,2,\ldots,n\}\}$，即图 1.1 中的 X 区域，它表示 IDS 正确检测到攻击行为。

（2） True Negative：对应点 $(n+1,n+1)$，即图 1.1 中的 O 区域，它表示 IDS 对正常行为的检测结果仍为正常行为。

（3） False Positive：对应集合 $\{(i,j)|i=n+1且j\in\{1,2,\ldots,n\}\}$，即图中的 U 区域，它表示 IDS 将正常行为当成攻击行为。

（4） False Negative：对应集合 $\{(i,j)|i=n+1且i\in\{1,2,\ldots,n\}\}$，即图 1.1 中的 Y 区域，它表示 IDS 将攻击行为当成正常行为。

（5） Misclassifled Hit：对应集合 $\{(i,j)|i\neq j且i,j\in\{1,2,\ldots,n\}\}$，即图 1.1 中的 Z 区域，它表示 IDS 将某一类型攻击行为当成其它类型攻击行为。

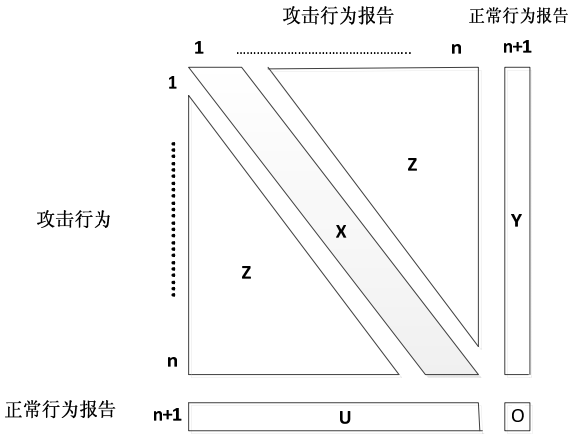

图 1.1 IDS 的检测结果的分类

由上述分析可以看出，对于 IDS 检测精确度由 False Positive、False Negative、Misclassifled Hit 三者所决定。由于基于滥用 IDS，规则集由厂商持续而专业的分析得到的，出现 Misclassifled Hit 的可能性可以忽略不计。

所以对于规则集 $R_1,R_2,\cdots,R_n$，系统的裁剪总代价 TCRC（Total Clipping Rule Cost），将从下面三个部分考虑：

（1） 生成警报代价 GAC（Generating Alert Cost）：即 IDS 检测到一次攻击事件时生成警报的代价。警报可能直接存放于本地服务器中，也可能通过邮件发送给管理员。

（2） 误报损失代价 FPDC（False Positive Damage Cost）：保留存在误报情况的规则所需付出的代价。对于一条规则，大部分不仅仅描述的是一种特定攻击行为，而是一类有共性的攻击行为，但因此也忽略了其中某些攻击行为所需要的其他特有的特征信息，会造成一些误报行为。同时，无关警报也会对造成系统资源的损耗和管理员时间和精力的浪费，因此也将归类于误报。

（3） 漏报损失代价 FNDC（False Negative Damage Cost）：裁剪某条规则而引发额外漏报所需付出的代价。裁剪掉某条规则，会将原来可以检测出的真实攻击行为给忽略，从而未能及时作出相应响应，会对目标主机和目标服务造成一定的损失。

通过以上分析，可以得到裁剪总代价的计算公式。在此，先给出一些变量的定义：

（1） 警报数 E_i：保留规则 R_i 时，IDS 所生成匹配此条规则的攻击事件数。

（2） 漏报率 α_i：裁剪规则 R_i 时，引发额外漏报数与警报数 E_i 的比率。也即为保留规则 R_i 时，IDS 正确检测攻击事件数与警报数 R_i 的比率。

（3） 误报率 β_i：保留规则 R_i 时，产生相关误报数与警报数 E_i 的比率。

（4） 裁剪值 x_i：

$$x_i = \begin{cases} 0 & \text{若裁剪规则} R_i \\ 1 & \text{若保留规则} R_i \end{cases}$$

x_i 的值表征了规则集的裁剪，利用 x_i 的值可以讨论最优化问题，即所谓的 0/1 规划问题。

很明显，对于任意的规则 R_i，漏报率 α_i 和误报率 β_i，存在下面的关系：

$$\alpha_i + \beta_i = 1 \tag{1}$$

得到裁剪总代价 TCRC 的计算公式：

$$TCRC(R,x) = \sum_{i=1}^{n} \{x_i E_i * GAC(R_i) + x_i \beta_i E_i * FPDC(R_i) + (1-x_i)\alpha_i E_i * FNDC(R_i)\} \tag{2}$$

因此，可以给出最优裁剪定义。

定义：设入侵检测系统的规则集为 $R=\{R_1, R_2, \cdots, R_n\}$，规则集裁剪值 $x=\{x_1, x_2, \ldots, x_n\}$ 满足：

$$OTCRC(R, x^*) = \min_x(TCRC(R, x)) \tag{3}$$

其中 $OTCRC$ 为最优裁剪总代价（Optimal Total Clipping Rule Cost），则称规则集裁剪值 x^* 为规则集 R 的最优裁剪。

基于裁剪代价的规则集最优化模型的基本思想就是：为规则集 R 从裁剪值 x 中找出最优裁剪，从而使该系统的裁剪总代价尽可能小。

2.2 模型代价量化

基于裁剪代价的规则集最优化模型的关键问题就是模型中各种代价的量化，其合理性直接影响到规则集最优化模型的合理性。

1.2.1 生成警报代价的量化

当一次攻击行为被检测到，IDS 需要将攻击警报保存在本地服务器，也可能保存在远处服务器上，甚至会发送邮件提醒管理员。但是这与误报损失代价相比，几乎可以忽略不计，因此可以假定对于任意一条规则 R_i 满足：$GAC(R_i)=0$。

1.2.2 漏报损失代价的量化

漏报损失代价与三个因素有关：攻击的致命性、攻击目标主机的重要性和攻击目标服务的重要性。其中攻击目标主机和攻击目标服务，可以统称为攻击目标。

（1） 攻击致命性的量化[5]

攻击的致命性衡量了攻击的危害程度，不同类型的攻击有着不同的危害程度。一般来说，取得超户权限的攻击要比取得普通用户权限的攻击严重，取得目标系统访问权限的攻击比对目标系统的拒绝服务攻击严重，而拒绝服务攻击比扫描攻击严重。

Wenke Lee 按照攻击的分类对攻击的致命性进行了量化，量化结果见表 1.1。其中，攻击的分类是依据 DARPA 的攻击数据，第一级分类按照攻击的后果，第二级分类按照攻击的技术，代价取值在 0 到 100 之间。表中的量化值并没有量纲，它的意义在于对不同攻击类型的致命性进行相对的比较，如表中所见，ROOT 类型攻击的致命性最为严重，R2L 类型和 DoS 类型攻击次之，而 PROBE 类型攻击的致命性最轻。

表 1.1 攻击致命性的量化

攻击一级分类	描述	攻击二级分类	描述	攻击致命性
ROOT	非法获取根权限	Local	通过先以合法用户登录再获取跟用户实现	100
		Remote	从远程主机直接获取根用户	100
R2L	从外界获得非法访问	Single	通过单一步骤实现	50
		Multiple	通过多步骤实现	50
DoS	拒绝服务	Crashing	通过单一事件实现	30
		Consumption	通过大量事件实现	30
PROBE	获取目标系统的信息	Simple	短时间内大量的扫描	2
		Stealth	分布式，并且慢速的扫描	2

（2） 攻击目标重要性的量化[5]

攻击目标也是衡量攻击损失代价的重要因素。在网络环境中，被攻击的对象可能为防火墙、路由器、DNS 服务器、Web 服务器、Mail 服务器、Unix 工作站、Windows 工作站等，不同的对象有着不同的重要性。通常，防火墙和路由器最为重要。DNS 服务器次之，Web 服务器和 Mail 服务器仅次于 DNS 服务器，Unix 工作站和 Windows 工作站的重要程度最低。对于同类型的攻击，若攻击目标非常重要，则该攻击的损失代价也相对较高。攻击目标重要性的量化需要管理员对管理域中的对象重要性作相对比较，然后给出统一的量化值，量化值在[0,1]范围内，1 表示重要程度最高。

（3） 漏报损失代价的计算

在对以上三个因素进行量化之后，规则 R_i 的漏报损失代价可以通过如下公式计算：

$$FNDC(R_i) = lethality(t) * criticality(a) \quad (4)$$

其中 t 为攻击类型，a 为攻击目标，$lethality(t)$ 为攻击类型 t 的致命性量化值，$criticality(a)$ 为攻击目标 a 的重要性量化值。

1.2.3 误报损失代价的量化

当 IDS 检测出一次攻击事件时，会采取一定的响应，以降低或消除攻击的威胁性，防止攻击目标造成大量的损失。但是对于一次误报行为，IDS 采取与正常警报相同的操作，会造成一定的损失。

误报损失代价与三个因素有关：响应操作代价、响应能耗代价、响应负面代价。

（1） 响应操作代价 ROC（Response Operation Cost）的量化

响应操作代价指的是杀死、挂起主机进程等轻量级响应方式所需要的代价，相对响应能耗代价、响应负面代价，可以几乎忽略不计。因此可以假定对于任意一条规则 R_i 满足：$ROC(R_i) = 0$。

（2） 响应耗源代价 RCC（Response Consumption Cost）的量化

响应耗源代价是指在对误报进行采取响应操作时，不可避免会占用系统系统资源，比如 CPU 时间、内存空间等。对于响应耗源代价，可以通过系统可用性的损失来衡量，而而这又可以转化为对该系统的 DoS 攻击的攻击损失代价的计算，因为 DoS 攻击的直接后果就是导致系统的可用性损失[5]。

（3） 响应负面代价 RNC（Response Negative Cost）

响应负面代价是指对本没有遭受攻击的正常用户造成的损失。响应操作，有封锁攻击源、封锁目标主机、封锁目标服务器等一些操作，造成了正常用户对某些服务不可用。而具体的响应操作要根据攻击的致命性、攻击目标重要性来选择，因此响应负面代价与漏报损失代价异曲同工之处。对于响应负面代价的量化，可以转化为漏报损失代价与响应负面代价比例因子 δ 的乘积。

（4） 误报损失代价的计算

在上述对影响误报损失代价的三个因素进行量化后，可以得到规则 R_i 的误报损失代价公式：

$$FPDC(R_i) = ROC(R_i) + RCC(R_i) + RNC(R_i) \quad (5)$$

其中 $ROC(R_i)=0$，$RCC(R_i)=lethality(DoS)$，$RNC(R_i)=\delta*\mathrm{FNDC}(R_i)$。

2.3 裁剪最优化分析

由定义，可知计算 $OTCPC$ 是最优化问题，但如何更有效的解决最优化问题，可以进一步分析。结合公式(2)，对定义进一步挖掘，发现可以采用贪心算法的思想来解决最优化问题。

记

$$f(R,x,i)=x_iE_i*GAC(R_i)+x_i\beta_iE_i*FPDC(R_i)+(1-x_i)\alpha_iE_i*FNDC(R_i) \tag{6}$$

则公式(6)可以转化为：

$$OTCPC(R,x^*)=\min_x\left(\sum_{i=1}^{n}f(R,x,i)\right)=\sum_{i=1}^{n}\left(\min_{x_i\in\{0,1\}}f(R,x,i)\right) \tag{7}$$

由于对于 $\forall i,j$，且 $i\neq j$，满足 $f(R,x,i)$ 与 $f(R,x,j)$ 相互独立，因此对于规则集 R，可以考虑局部最优解，单独判断具体某条规则 R_i 的裁剪代价，即 $f(R,x,i)$，选取最优的 x_i，使规则 R_i 的裁剪代价为最小。依次往复，对每条规则都考虑局部最优解，最后做出的裁剪抉择便是整体的最优解。

结合以上分析，对公式(6)进一步推导，得出：

$$f(R,x,i)=\beta_i*FNDC(R_i)+x_i*GAC(R_i)+x_i\beta_iE_i*FPDC(R_i)-x_i\alpha_iE_i*FNDC(R_i) \tag{8}$$

其中 $\alpha_i*FNDC(R_i)$ 为常数项，与 x_i 无关，$x_i*GAC(R_i)$ 为 0。

记 $\mathrm{g}(R,i)=\dfrac{FPDC(R_i)}{FNDC(R_i)}*\dfrac{\beta_i}{\alpha_i}$，则：

$$\min_{x_i\in\{0,1\}}f(R,x,i)=\begin{cases}f(R,0,i) & 若\mathrm{g}(R,i)>1\\ f(R,1,i) & 若\mathrm{g}(R,i)\le 1\end{cases} \tag{9}$$

其中 $\mathrm{CR}(R_i)=\dfrac{FPDC(R_i)}{FNDC(R_i)}$ 为误报漏报损失代价比，$\mathrm{PR}(R_i)=\dfrac{\beta_i}{\alpha_i}$ 为误报漏报率比，则若误报漏报损失代价比与误报漏报率比之积大于 1，裁剪此条规则；反之，则保留此条规则。

2.4 最优裁剪算法

设入侵检测系统一共有 n 条规则，则对于规则集 $R=\{R_1,R_2,\cdots,R_n\}$，依次对每条规则 R_i 进行如下操作：

（1） 计算漏报损失代价 $FNDC(R_i)$。分析规则 R_i，判定 R_i 所对应攻击的攻击类型 t 和攻击目标 a，从而进一步得到攻击致命性 $lethality(t)$ 和攻击目标重要性 $criticality(a)$，再由公式(4)计算出 $FNDC(R_i)$。

（2） 计算误报损失代价 $FPDC(R_i)$。首先计算响应操作代价 $ROC(R_i)$、响应耗源代价 $RCC(R_i)$、响应负面代价 $RNC(R_i)$，并由公式(5)得到误报损失代价 $FPDC(R_i)$。

（3） 对规则 R_i 对应的警报进行分析，总警报数为 E_i 条，其中误报数为 P_i 条，则计算出误报率 $\beta_i=\dfrac{P_i}{E_i}$，再由公式(1)，得到漏报率 $\alpha_i=1-\beta_i=1-\dfrac{P_i}{E_i}$。

（4） 由公式 $CR(R_i)=\frac{FPDC(R_i)}{FNDC(R_i)}$ 和公式 $PR(R_i)=\frac{\beta_i}{\alpha_i}$，分别计算得出误报漏报损失代价比 $CR(R_i)$ 和误报漏报率比 $PR(R_i)$，并计算 $g(R,i)=CR(R_i)*PR(R_i)$。

（5） 根据 $g(R,i)$ 的值和公式(9)，来抉择保留还是裁剪此条规则。

3 实验和结果分析

MONSTER 是 Monitor On Network Security and Tool for Emergency Response 的简称，它是在国家自然科学基金重大研究计划课题“面向大规模网络的分布式入侵检测与预警”（90104031）背景下，由江苏省计算机网络重点实验室设计开发的基于滥用检测的入侵检测和响应系统。该系统的监测对象是接入网络，它的设计的目标是实现一个集成报文过滤、入侵检测、协同和响应的入侵防范系统（Intrusion Prevention System）[6]。因此，针对对 CERNET 华东(北)地区网主干信道的 Botnet 检测，采用了上述的基于裁剪代价的规则集最优化模型，确定所需的 Botnet 规则集。

3.1 裁剪结果

本文所采用的规则集是基于 Snort 规则集转换得到的 Monster 规则集，共 2763 条；实验数据来自入侵检测系统 Monster3.0 对 CERNET 华东(北)地区网主干信道上报告的警报。

依据本文提出的裁剪代价的规则集最优化模型，对 Monster 规则集进行优化，将与 Botnet 无关规则和代价太大的规则裁剪掉，最终在 2763 条规则中选取出与僵尸网络相关的规则 510 条。

表 2.1 列举了四条具有代表性的规则的裁剪结果：

表 2.1 部分规则的裁剪结果

规则号	事件描述	事件数	是否裁剪
270000001	POLICY Suspicious .cn dns query	3877	是
110000015	MISC MS Terminal server request	813	是
600000012	DDOS mstream handler ping to agent	12	否
200000029	BACKDOOR neurotickat1.3 runtime detection - icq notification	3793	否

3.2 实验结果分析

为了验证本文提出的方法的可行性，需要验证两点：一是可裁剪性，是否所有的规则可以进行裁剪代价分析，因为本文是基于裁剪代价进行规则集优化，所以若存在规则不能进行裁剪代价分析，则方法不具备通用性；二是裁剪准确性，裁剪结果若不准确，则会存在大量的误报和漏报，无法正确起到优化规则集的目的。

对于方法可裁剪性，由裁剪结果来看，Monster 所有规则都可以进行裁剪，并且选取出 Botnet 检测规则集，满足可裁剪性要求。而对于裁剪准确性，下面将通过表 2.1 中四条具有代表性的规则进行直接的语义分析来进行验证：

（1） 规则 270000001，显示 IDS 检测到可疑的“.cn”域名请求。对于此规则检测，主要基于内容匹配监视 53 端口的报文。匹配的三个字段为，“|01 00 00 01 00 00 00 00 00 00|”、“|02|cn”、“/[\x05-\x20][bcdfghjklmnpqrstvwxyz]{5,32}\x02cn/i”。对于前两个字段，标识 dns 请求报文是“.cn”域名请求报文，而第三个字段用来检测僵尸网络域名。但是由于此字段过于简单，即使正常的“.cn”域名请求报文中也会有较高概率匹配该字段，所以会产生大量的误报行为。所以需要裁剪掉此条规则。这类规则虽然能够检测出 Botnet 相关攻击行为，但是由于其误报过多导致代价过高，因此需要裁剪。

（2） 规则 110000015，表明 IDS 检测到有攻击者想利用微软终端服务器的一个漏洞，进行 DoS 攻击。此条规则虽然对应的事件数比较多，但是由于描述的是非僵尸网络攻击，所以按照本文对误报的定义，则其误报率为 100%，需要裁减。这类规则的共性为，虽然能检测出大量的攻击行为，但是这类攻击的警报不是管理员所感兴趣的，为无关警报，同样需要裁剪。

（3） 规则 200000029，表明 IDS 检测到 Neurotickat 正在通过 HTTP 端口进行交互。其“Name=The Hosts port is”、“Name=Your Host is”等特有字符串，是平常报文中很难完全匹配，所以检测准确率高，需要保留。这类规则，能够比较精确的表示相关攻击特征，误报率低，需要保留。

（4） 规则 600000012，说明 IDS 检测到一次可能攻击者使用 mstream 攻击对主机进行扫描行为。由于其事件数过少，其规则支持度较小，从而其分析结果可能会出现较大的偏差，因此不进行裁减分析。但因为此规则可能与僵尸网络相关，则保留处理。这类规则，与 Botnet 攻击行为相关，但其警报数较少，默认做保留处理。

通过以上对四种不同类型的规则进行直接语义分析，验证了本文方法的裁剪准确性，表明了基于裁剪代价的规则集最优化模型能够很好的优化规则集，从而反映了方法的可行性。

4 结论

近年来，随着网络非法入侵的增长，入侵检测系统提供了积极保护作用，而作为基础核心部件的规则集，直接影响了入侵检测系统的性能。本文通过对规则集和警报进行分析，提出了基于裁剪代价的规则集最优化模型。根据代价，对规则保留、裁剪进行了比较，模型给出了规则误报、漏报损失代价的具体量化方法。通过响应操作代价、响应耗源代价和响应负面代价的计算转化为误报损失代价；而攻击类型威胁性和攻击目标重要性的量化组成了漏报损失代价。本文实验采用 CERNET 江苏省网主干下的实测警报数据进行分析，实验结果验证了该方法的对入侵检测系统的规则集优化的可行性。本文方法结合了警报的漏报、误报情况，具有比仅根据规则集本身信息进行优化准确，同时并基于裁剪代价进行分析，方法简单、容易计算等好处。

参考文献

[1] CNCERT/CC2007 年网络安全工作报告 [M].

[2] 诸葛建伟 等. 僵尸网络研究与进展[J]. Journal of Software, 19(3): 702-715.

[3] Geer D. Malicious bots threaten network security[J]. IEEE Computer, 2005,38(1): 18−20.

[4] 韩仲祥, 史浩山, 王元一. 实时入侵检测系统的优化问题研究[J]. 计算机工程与应用, 2004,29: 15-20.

[5] 丁勇. 自动入侵响应系统的研究[D]. Nanjing: Southeast University, 2004.

[6] 王韬. 高速网络环境下的报文监测[D]. 南京: 东南大学, 2004.