第 26 卷第 10 期 电子与信息学报 Vol.26No.10
2004 年 10 月 Journal of Electronics & Information Technology Oct. 2004

基于虚拟机技术的入侵检测系统攻击仿真平台的研究和实现 [1]

王汝传 * ** 黄良俊 * 胡 涛 * 孙知信 *

*(南京邮电学院计算机科学与技术系 南京 210003)
**(信息安全国家重点实验室 中国科学院研究生院 北京 100039)

摘 要: 攻击仿真平台是入侵检测系统 (Intrusion Detectoin System, IDS) 测试平台的核心组成部分. 该文从攻击测试的角度, 提出了一种基于虚拟机技术的 IDS 攻击仿真平台. 首先介绍攻击仿真的测试目标和内容, 并提出了攻击仿真系统和仿真平台的设计和实现的详细方案; 同时, 在此基础上, 对该平台的设计和实现的 3 个关键技术: 测试数据的选择、攻击技术的分类研究、攻击测试域及其划分等进行了进一步的分析, 最后给出并分析了实验测试结果.

关键词: 入侵检测系统, 仿真平台, 虚拟机, 攻击测试
中图分类号: TP31, TN918 **文献标识码:** A **文章编号:** 1009-5896(2004)10-1668-07

The Research and Implementation of Attack Simulation Platform for Testing Intrusion Detection System Based on Virtual Machine Technology

Wang Ru-chuan* ** Huang Liang-jun* Hu Tao* Sun Zhi-xin*

*(*Dept. of Computer Science and Tech. Nanjing Univ. of Posts and Telecomunications, Nanjing* 210003, *China*)

**(*State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing* 100039, *China*)

Abstract Attack simulation plays a key role in testing Intrusion Detection System(IDS). From the viewpoint of attack testing, an attack simulation platform is put forward for testing IDS based on virtual machine technology. First of all, the testing aims and contents of attack simulation are proposed. Then, the design and implementation of the attack simulation platform are presented in detail. Under the platform, that the authors build, three key issues in realization of the platform :the choice of testing datum, the classification of attack technology, and the attack testing zones and their compartmentalization are discussed in detail. Finally, the test results are given.

Key words Intrusion Detection System(IDS), Simulation platform, Virtual machine, Attack testing

1 引言

近些年来, 网络安全事件不断发生, 信息安全越来越受到人们的重视, 各种各样的入侵检测系统 (Intrusion Detection System, IDS) 也应运而生, 并广泛用于社会生活的各个领域. IDS

[1] 2003-05-26 收到, 2003-09-29 改回
国家自然科学基金 (60173037 和 70271050), 江苏省自然科学基金 (BK2003105), 国家高科技项目 863 (2004AA776032) 和江苏省计算机信息处理技术重点实验室基金 (kjs03061 和 kjs04) 资助课题

产品的广泛应用，使得人们对 IDS 的可靠性、稳定性等性能指标提出更高的要求．与此同时，设计通用的 IDS 测试、评估方法和平台，实现对多种 IDS 的检测，已成为当前 IDS 研究与发展的另一重要领域 [1] ．

攻击仿真平台是 IDS 测试平台的核心，同时也是对 IDS 进行测试的关键所在 [2] ．但是，在对 IDS 进行攻击测试时，很少会把 IDS 放在实际运行的网络中，并且实际网络环境的专用性比较强，许多数据并不能满足对 IDS 进行准确、全面测试的要求，因而需要构建专用的攻击平台．然而，传统的攻击平台的构建需要硬件设备的投入，测试投资较大．基于这种考虑，我们提出了一种基于虚拟机技术的 IDS 攻击仿真平台，并对其进行了设计和实现．

对 IDS 进行攻击仿真测试，就是让 IDS 对进入受保护系统，包括受保护主机和受保护网络的数据进行检测，以检测 IDS 是否能够及时准确地发现这些攻击行为；同时由于 IDS 的特殊作用，使得 IDS 也成为入侵攻击的主要对象，一旦 IDS 被攻破，整个受保护系统将面临巨大的安全威胁，因此， IDS 本身的防护能力也越来越受到人们的关注．

基于对上述问题的考虑，我们的测试平台的攻击仿真主要包括两方面的内容： (1) 对受保护系统实施攻击，以测试 IDS 检测的准确性和处理数据的性能； (2) 对 IDS 本身进行良性攻击，以检测 IDS 自身的抗攻击能力，其中包括受攻击检测能力、系统资源占用率等性能指标．

2 攻击仿真平台的设计

2.1 攻击仿真系统结构

攻击仿真系统的结构框图如图 1 所示。在该系统中，控制中心负责调度测试策略和管理数据的产生，包括调度攻击数据产生模块和正常数据产生模块，并协调整个系统各个模块的工作．

测试策略是由若干测试规则组成，这些测试规则主要根据已验证的攻击手段的有效性来建立，同时负责管理对攻击手段的选择更新、攻击新技术的配置和正常数据流量的设置和数据流的产生时序等．

测试系统的测试结果将分别写入攻击日志文件和正常日志文件中．这两个日志文件主要用于记录测试实施使用的攻击手段、可利用漏洞、攻击目标、测试开始和结束时间、正常数据流量、正常数据产生手段等信息，供事后离线分析．

利用该系统中，我们可以同时对受保护系统和 IDS 本身进行攻击测试．

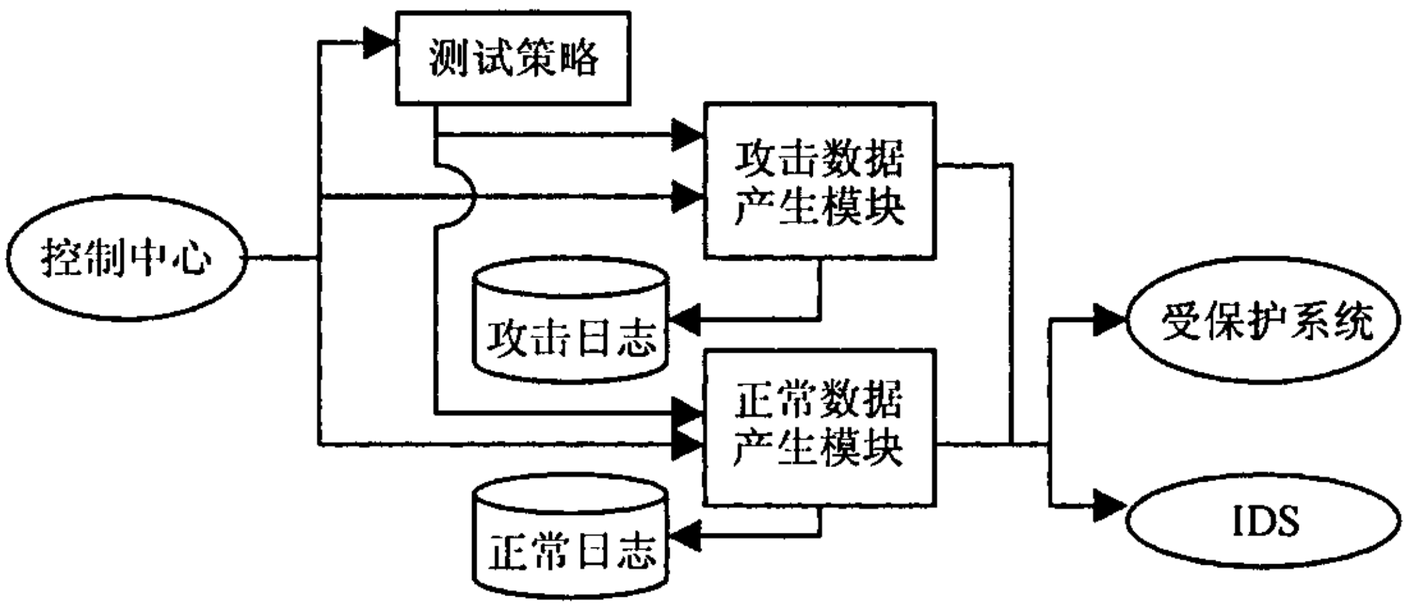


图 1　攻击仿真系统结构框图

2.2 构建在虚拟机上的攻击仿真平台

在对 IDS 进行攻击仿真时，我们往往需要两套或多套系统进行测试．一种方法是在两台或多台机器上分别安装不同的系统，这也是最简单的一种方法，但这种方法需要增加硬件设备投资．另一种方法是在一台计算机上安装多个操作系统，通常方式下，我们可以使用 Linux Lilo，Partition Magic 改变激活分区等多种安装引导方法，但这种方法需要在操作系统之间进行切换，这时只有重新启动计算机，这给我们的测试造成很大不便．而利用虚拟机技术可以很好地解决这样的问题。

虚拟机 (virtual machine) 是指利用软件技术实现同功能的硬件计算机. 利用虚拟机技术, 我们可以将一台计算机模拟成多台电脑, 同时运行不同的操作系统, 还可以将这几个操作系统连成一个虚拟网络. 虚拟机软件就是实现这个功能的软件. 这种方法给我们构建 IDS 测试平台提供了一种方便实用的途径. 目前, 较为常用的虚拟机软件有 VMWare 和 VirtualPC 等. 由于 VMWare 提供强大的硬件模拟功能、支持多种操作系统且使用方便, 因此, 我们选择 VMWare 作为构建攻击仿真环境的平台软件.

在图 2 所示的攻击仿真平台中, 运行虚拟机软件的操作系统称为宿主机操作系统 (Host OS), 在虚拟机里运行的操作系统叫做客户机操作系统 (Guest OS). 攻击仿真系统运行在每台虚拟机上, 同时, 这些系统通过计算机硬件平台可以连接成一个虚拟机网络, 并通过以太网与被测试的受保护系统和 IDS 相连.

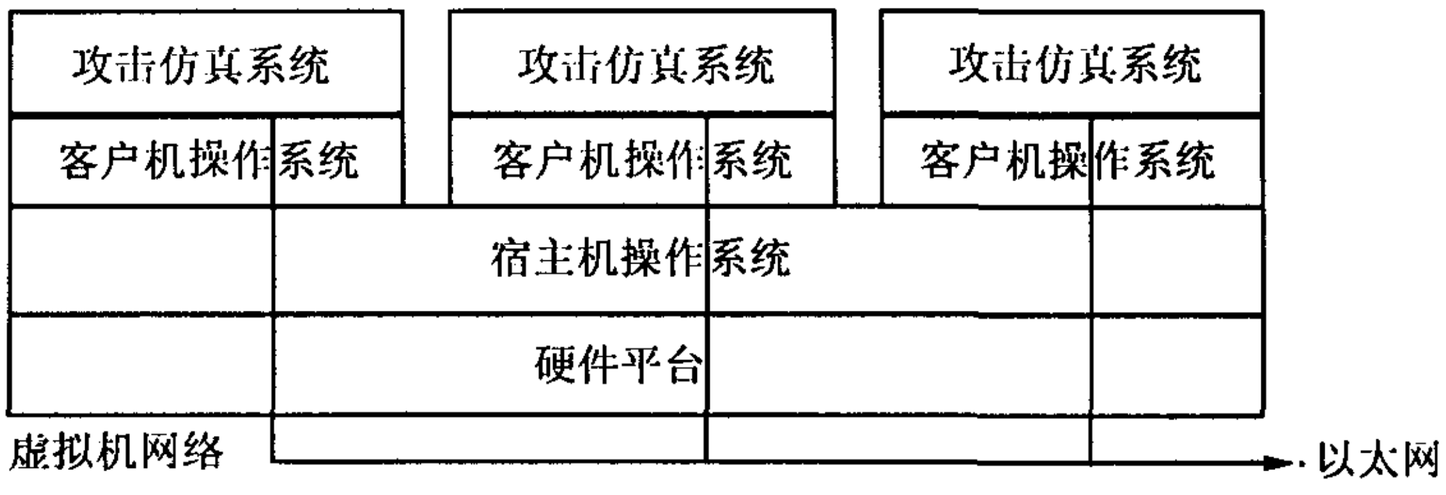


图 2 构建在虚拟机上的攻击仿真平台

3 攻击仿真的关键技术

3.1 测试数据的选择

测试数据的选择和生成对于测试 IDS 的性能起着重要的作用. 对 IDS 进行攻击测试的数据通常可分为正常数据和攻击数据两大类. 入侵行为在正常数据的掩护下, 被检测系统发现的几率会大大降低, 通过这种方式, 可以测试 IDS 的漏报率. 同时, IDS 也可能将正常的数据误判为攻击, 产生虚假报警, 由此, 我们可以测试 IDS 的误报率. 相应地, 在设计实现时, 如图 1 所示, 我们将数据产生划分为正常数据产生和攻击数据产生两大模块.

在选择生成测试数据时, 对于正常数据, 我们主要通过模拟用户的正常行为和网络正常访问来实现, 例如包括 Ftp, telnet, Web 访问等, 通过定时循环产生的方式自动生成这些数据; 对于攻击测试数据, 由于安全漏洞很多, 与之相应的攻击工具也很多, 同时新的攻击手段也层出不穷, 不可能对所有的攻击进行实现和测试. 因此, 我们先对攻击技术进行分类, 设计并实现了几种典型的、具有代表性的攻击工具例如 SYN Flood, UDP Flood 等, 并将其嵌入到我们的攻击测试系统当中.

3.2 攻击技术的分类

攻击数据产生模块是实现的重点, 而攻击手段的分类研究是设计该模块的关键所在. 对网络攻击手段的分类, 国内外不少研究机构或人员提出了许多分类方法, 其中包括以攻击技术手段进行的分类方法、结合攻击使用技术和攻击后果的分类方法、根据攻击实施操作顺序的分类方法等 [3]. 这些分类方法对于理解攻击利用的系统漏洞和攻击技术方法都大有帮助. 在这里, 我们根据攻击途径和攻击对象, 并结合应用实际将攻击技术分为基于用户行为的攻击、基于网络的攻击和针对 IDS 的攻击.

基于用户行为的攻击一般总是以获得 root 权限为目的. 如果用户可以在核心态运行他的程序, 那么该用户就可以获得一般账号没有的权限, 甚至比 root 权限更高级的权限. 攻击者通常通过执行特权的程序或者利用系统缓冲区溢出来获得超级用户的权利. 一个用户可以用登陆、shell 命令行执行或系统调用等来实现这样的攻击行为.

基于网络的攻击行为包括网络监听、对网络协议的弱点的攻击等攻击手段．其中在链路层上的主要攻击手段包括修改及重定向 ARP, proxy ARP, Internet ARP 数据包等； TCP/IP 层上攻击手段主要是针对现行的 TCP/IP 协议的一些安全漏洞进行的，包括利用 ICMP 重定向消息破坏路由表、拒绝服务攻击、碎片攻击等．

对 IDS 的攻击主要是针对 IDS 在分析数据时的弱点和漏洞进行的．上述拒绝服务攻击等手段也可以用于对 IDS 进行攻击．除此以外，对 IDS 实施攻击的模式还有另外两种 [4,5]： “插入式” 攻击和 “逃避式” 攻击． “插入式” 攻击的基本原理是向 IDS 系统发送经过精心设计的数据包，对于这种数据，运行 IDS 的终端系统会丢弃而 IDS 系统将接受并做出判断，这样会使 IDS 与终端系统得到不同的结论而实现攻击目的．而相对的， “逃避式” 攻击是产生 IDS 不会接受而终端系统却会做出处理的数据包，使得攻击数据能够逃脱 IDS 的检测．

我们选择上述几类攻击中具有代表性的攻击手段进行实现．利用这些攻击测试工具，既可以利用单一攻击手段进行测试，同时还可以实现多种攻击手段的并行攻击测试．

3.3 攻击测试域及其划分

在进行攻击测试过程中，难点在于模拟入侵攻击行为．综合目前的攻击事件，这些行为通常包括以下几个阶段： (1) 探测目标信息：对目标系统实施空间信息扫描、主机扫描及用户扫描，确定目标主机使用的操作系统类型及版本信息，并进行安全漏洞扫描，以确定目标系统有哪些漏洞可供利用，例如：利用 Finger 得到用户登录信息． (2) 实施攻击：针对目标系统的漏洞信息，确立攻击策略和攻击手段，发动攻击，包括 SYN 洪水攻击、 IP 分片攻击等． (3) 破坏目标系统：破坏目标系统的正常运作或获得目标系统 root 权限，修改、破坏目标系统文件． (4) 入侵痕迹：自动清除或手动清除入侵痕迹，保护自身不被发现；安装后门以及相关隐藏工具，为下一步攻击做准备． (5) 利用该系统作为跳板攻击其他机器．

为了更好地描述和模拟入侵行为，在攻击仿真平台中，我们提出攻击测试域的概念，如图 3 所示．攻击测试域可定义为一个四元组 Att=(M, S, P, t) ， 其中：

M ： 攻击主体集 $(m_1, m_2, \cdots, m_n)$, m_i 对应于参与该次攻击测试的一个虚拟机；

S ： 攻击手段集合；

P ： 攻击属性，即本次攻击测试所属的阶段．在我们的系统中，攻击属性可被设为 4 个不同的值，包括探测、攻击、破坏、清除等．

t ： 攻击时间点，用于表示攻击测试执行的时间序列．

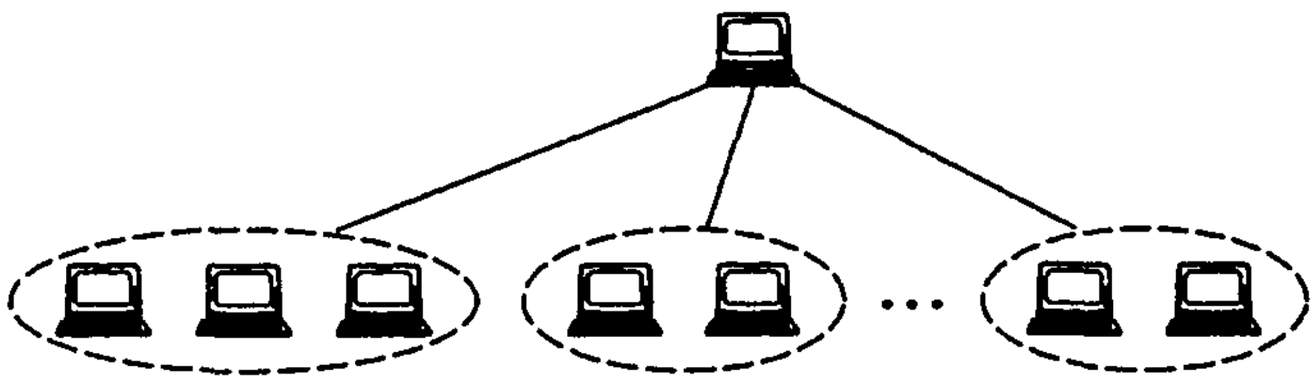


图 3　攻击测试域结构图

由该定义我们可以得知，攻击测试域具有以下一些性质：

性质 1　一个攻击主体 m_i 在不同时间点可以属于不同的攻击测试域；但在特定的某个时间点 t_i 只能属于一个攻击测试域；

性质 2　一个攻击主体域在某个特定时间点 t_i 的攻击属性 P 是唯一确定的；

性质 1 体现了攻击主体与攻击测试域的包含关系，性质 2 表明了一个攻击测试域在某个特定时刻的特定测试任务．

根据上述攻击测试域的定义和性质，我们可以制定出攻击测试的相应策略，并将测试策略在实施测试过程中动态地分配到各个不同的攻击测试域中来执行．

4 攻击测试的实施

4.1 网络拓扑结构及配置

攻击测试的网络拓扑结构如图 4 所示. 在攻击者机器上运行攻击测试仿真平台，其中 Host OS 使用 Redhat Linux7.3，在 Host OS 上使用 VMWare 仿真 3 台虚拟机 (Guest OS)，每台虚拟机分别就是一个攻击测试域，分别称为 Att1， Att2 和 Att3，其配置信息如表 1 所示.

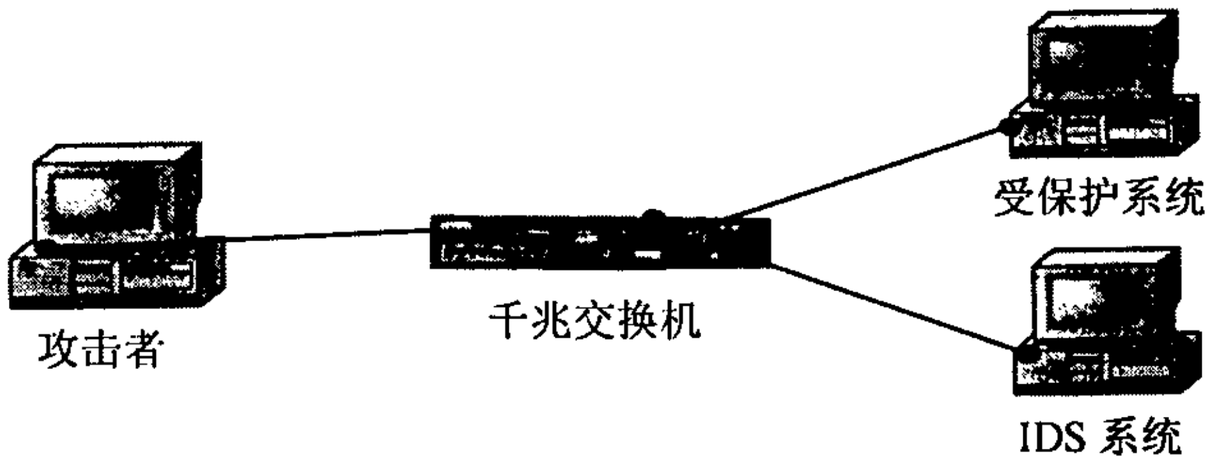


图 4 网络拓扑结构

表 1 攻击测试域配置信息

攻击测试域	使用的操作系统	测试手段	用途
Att1	Redhat Linux7.2	Syn flood, Udp Flood, Icmp Flood 等	发送各类攻击数据
Att2	Redhat Linux7.2	Udp Flood, Tcpreplay 等	制造背景流量
Att3	Windows 2000	telnet, ping, ftp 等	发送正常的服务请求数据包

4.2 实验结果及分析

我们在测试环境中，利用攻击测试仿真平台对受保护系统和我们设计的基于网络和主机调用的 IDS 系统同时实施攻击. 在测试过程中，我们使用了 SYN Flood, ICMP Flood, Stick 等攻击手段 [6,7]，并执行 ftp, telnet 和 ping 等正常服务请求；同时在受保护系统上运行 tcpdump 以捕获接收到的数据 [8]，并以这些数据作为我们计算的一个基准.

被测 IDS 系统的性能平均值如表 2 所示。一般的 IDS 系统在检测时会定义一个时间段，如果在这个时间段内发现超过某一预订值的连接次数，那么就判断为端口扫描，在测试过程中，我们通过提高端口的连接速度来使 IDS 系统发生误报. 另外，从该表中我们可以看出，被测 IDS 系统在检测能够检测到一般的攻击例如 SYN Flood, ICMP Flood 等洪水攻击；但对于躲避攻击发送的数据包，该 IDS 系统没有能够全部检测出来而发生漏报.

在对运行该 IDS 系统的终端系统进行测试时，我们测试正常情况下和在 IDS 系统受攻击情况下该 IDS 系统对主要资源 (CPU 和内存) 的占用率如表 3 所示. 从表 3 中我们看到，在一般的情况下， IDS 系统作为一个或多个实时监视进程运行，占用了系统很少的资源. 但是，当发生攻击行为时，快速的告警信息的产生使 IDS 耗费终端系统大量的资源，其资源占用率明显提高，甚至会出现死机现象。

表 2 被测 IDS 系统的性能平均值

Tcpdump 数据包 (个)	攻击数据包 (个)	正常数据包 (个)	IDS 误报率 (%)	IDS 漏报率 (%)
100	70.9	29.1	7.3	9.2

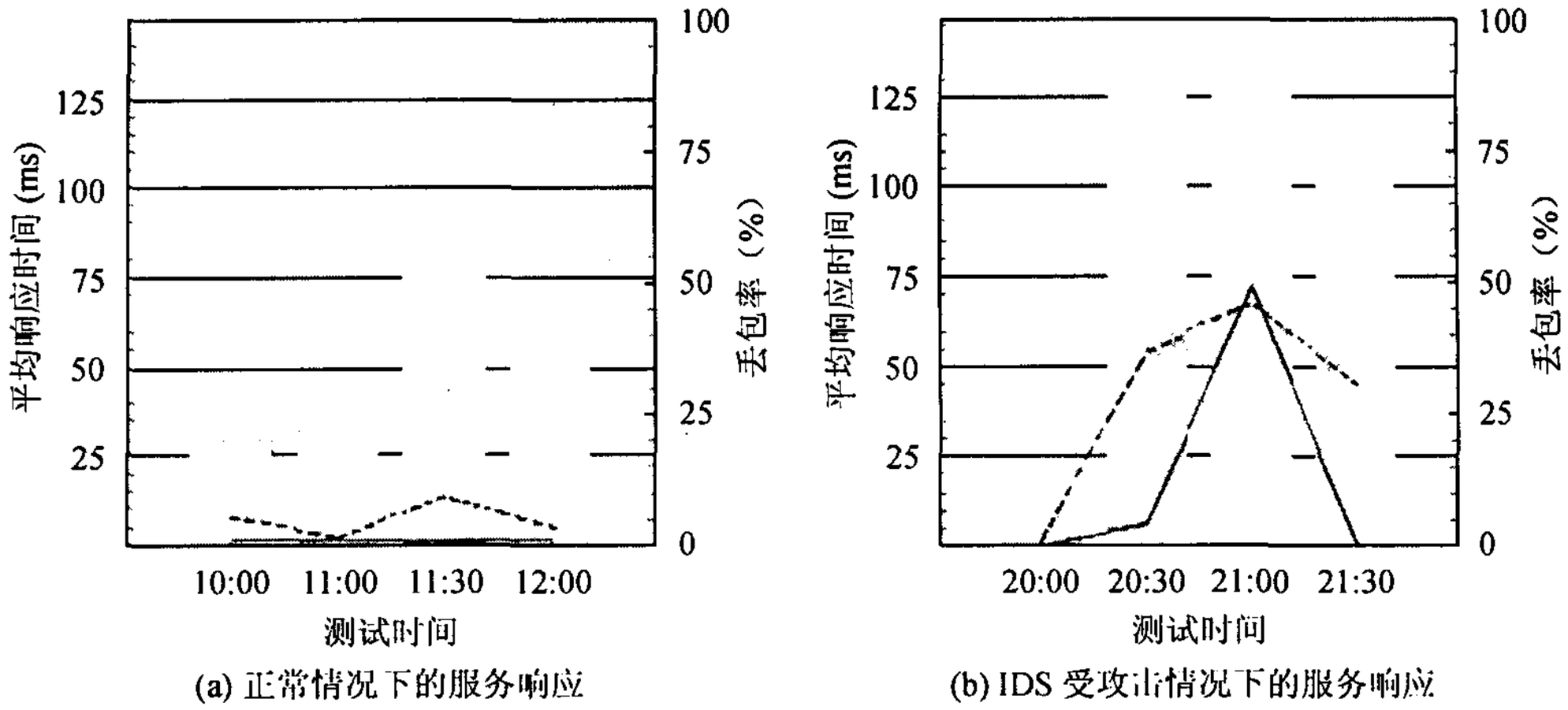
表 3 IDS 对系统主要资源占用率的比较

	正常情况下 (%)	IDS 受攻击情况下 (%)
CPU 占用率	1.3	69.2
内存占用率	1.8	53.7

同时，为了测试网络流量对 IDS 系统检测性能的影响，我们利用 UDP Flood 和 Tcpreplay 来分别制造 UDP 背景流量和 TCP 背景流量，同时，利用网络管理工具 SolarWinds 收集运行该 IDS 的终端系统在正常情况下和在 IDS 受攻击情况下的服务响应，并对此进行比较，得到的结果如图 5 所示，其中直方图为最长响应时间，虚线表示平均响应时间，实线表示丢包率.

从图 5 中，我们可以清楚地看到，在正常情况下，终端系统的丢包率接近于零；而在 IDS 系统受攻击的情况下，终端系统对服务请求的响应时间相应变慢，平均响应时间从 16.2 ms 上升到 68.4 ms . 由于背景流量数据和攻击数据的大量产生使得网络流量明显增加；同时，终端系统的丢包率也随之变大，提高到 50% 左右。

通过实验我们发现， IDS 是否会丢包以及丢包率的多少，主要取决于网络数据流量和 IDS 系统每秒的抓包数，如果网络数据流量超过 IDS 系统处理能力， IDS 就可能会丢包，从而不能正常检测出攻击. 另一方面，网络数据包的大小差异很大，每秒通过 IDS 系统的网络流量的差异也会很大，在相同抓包率的情况下，当网络数据包平均大小变小时，平均网络流量呈变大趋势，因此，提高 IDS 系统的抓包速率，也可以减少丢包率，从而提高其检测能力。



(a) 正常情况下的服务响应　　(b) IDS 受攻击情况下的服务响应

图 5　终端系统的服务响应曲线

5 结束语

该攻击仿真平台已经实现大部分攻击手段的自动化，为测试 IDS 检测的准确性和处理数据的性能、抗攻击能力等提供一套较为全面的测试策略和手段，其可用性和可靠性在实际测试中得到了验证，并且在实验中不断得到改进和修正。与传统的 IDS 测试方法相比，该平台具有实施方便，扩展性强等特点. 在该平台中，很多传统测试方法所使用的部分硬件设备可以用软件来代替，节省了用户投资.

同时，我们注意到，在用虚拟机构建攻击仿真平台时，对系统资源尤其是内存消耗很大，在一台计算机上同时运行多台虚拟机时，受计算机硬件资源的限制，在给受保护系统和 IDS 发送数据包时，发包速率与测试策略中设置的速率有些不同；同时，该系统的测试策略的规则相对简单，不能生成未知攻击的测试数据。

对于这些问题，我们将在以后的工作中不断改进；另外，测试策略和攻击数据产生模块的完善将成为我们下一步工作的重点，我们将对此进行更为深入的研究.

参　考　文　献

[1] Puketza N, *et al.*. A software platform for testing intrusion detection system. *IEEE Software Magazine*, 1997, 14(5): 43–51.

[2] 蔡忠闽，等. 入侵检测系统评估环境的设计与实现. 系统仿真学报， 2002, 14(3): 377–380.

[3] Eric Cole 著，苏雷，等译. 黑客——攻击透析与防范. 北京：电子工业出版社， 2002: 152–165.

[4] Miller I. Protection Against a Variant of the Tiny Fragment Attack, RFC3128 Singularis Ltd. 2001.

[5] 张铭来，等. 网络型入侵检测系统存在的漏洞及其对策研究. 计算机工程， 2002, 28(1): 172–174.

[6] Nash D A, Ragsdale D J. Simulation of self-similarity in network utilization patterns as a precursor to automated testing of intrusion detection systems. *IEEE Trans. on Systems, Man and Cybernetics: Part A*, 2001, SMC-A-31(4): 327–331.

[7] Erbacher R F, Walker K L, Frincke D A. Intrusion and misuse detection in large-scale systems. *IEEE Computer Graphics and Applications*, 2002, 22(1): 38–47.

[8] James Stanger, Patrick T Lane 著，钟日红，等译. Linux 黑客防范开放源代码安全指南. 北京：机械工业出版社， 2002: 176–190.

王汝传： 男， 1943 年生，教授，博士生导师，主要研究方向是计算机软件、计算机网络、信息安全、移动代理和虚拟现实等.

黄良俊： 男， 1979 年生，硕士生，目前研究方向是基于网络的计算机软件应用技术.

胡 涛： 男， 1980 年生，硕士生，目前研究方向是计算机软件在通信中的应用.

孙知信： 男， 1964 年生，博士，副教授，主要研究方向是软件工程理论、计算机网络.