仿真环境下入侵检测系统测试①

何增颖

(湛江师范学院 实验教学管理处，湛江 524048)

摘 要：分析传统的入侵检测系统评测方法，提出了一种基于虚拟机技术的入侵检测系统性能评测方法。该方法利用 Vmwre 软件构建攻击仿真环境，并在模拟实验环境下实现攻击，对 IDS 的指标进行测试与比较，验证了该方案的可行性。

关键词：虚拟机；入侵检测系统；仿真；IDS 测试；攻击测试

Simulation Environment for Testing Intrusion Detection System

HE Zeng-Ying

(Deptement of Experimental Teaching Management, Zhanjiang Normal College, Zhanjiang 524048, China)

Abstract: This paper makes an abstract Analysis of traditional intrusion detection system evaluation method and proposes an intrusion detection system performance evaluation method based on virtual machine technology. The method is used to build attack Vmwre software simulation environment. And simulation environment to achieve attack, testing and comparison of indicators of IDS verify the feasibility of the program.

Keywords: virtual machine; intrusion detection system; simulation; IDS testing;attack testing

1 引言

随着对入侵检测技术研究的发展，出现了许多入侵检测系统，因此也产生了对各种入侵检测系统的功能和性能评估的需求。许多研究机构都进行了相应的研究，给出了自己的测试方法和测试结果[1]，1994 年加州大学戴维斯分校(UCD)的 Nicholas 和 J. Puketza 等人提出通过模拟被监测系统上用户的行为来测试 IDS 系统的方法，开创了对 IDS 评估系统研究的先河；IBM 苏黎世研究实验室在 1997 年也开展了入侵检测评测的相关研究；而受到广泛关注的是 1998、1999 年 MIT 的 Licoln laboratory 通过模拟美军空军基地的日常网络流量进行了 IDS 系统的两次测试，成为 IDS 综合测试的典范，也是目前为止学术界最有影响力的入侵检测评测研究；2000 年时，MIT 在测试数据中加入了对于 DDoS(Diskibuted Deny of Service)攻击的模拟；2001 年 Terrence Champion 等人专门对于 IDS 系统检测 DDoS 攻击的能力进行了测量，同时还考虑了 IDS 系统响应功能的评测。因此设计通用的 IDS 测试、评估方法和平台， 实现对多种 IDS 的检测， 已成为当前工研究与发展的另一重要领域。

2 测试方案目的

攻击平台是IDS测试平台的核心，同时也是对IDS进行测试的关键所在但是，在实际的应用环境中对 IDS 进行测试是最直接的办法，同时能获得最准确、全面的测评数据与结果。但存在以下问题[2]。1)被测产品的不足可能带来的高风险性；一旦 IDS 被攻破， 整个受保护系统将面临巨大的安全威胁。2) 真实网络流量中测试的数据中包括一些特征及隐私数据，通用性受限；3) 真实网络中的随机性大，测试种类可能不全面，许多数据并不能满足对 IDS 进行准确、全面测试的要求，而且不可重复。比较不同 IDS 的检测效果，这就失去了评测的重要意义。4)真实测试环境构建需要硬件设备的投入，测试投资较大，从使用者及开发者的角度考虑，实现起来代价都很大。

由于这些不足之处，在对 IDS 进行攻击测试时，

① 基金项目:湛江市科技攻关计划项目(湛科[2009]64 号);湛江师范学院自然科学项目(L0823)
收稿时间:2010-05-25;收到修改稿时间:2010-12-14

很少会把 IDS 放在实际运行的网络中，因而需要构建专用的攻击平台然而，基于这种考虑，本文给出了一种基于虚拟机技术的入侵检测系统性能评测方案，并对其进行了设计和实现对 IDS 进行攻击仿真测试，该方法利用虚拟机技术有效地构建入侵检测系统的测试环境，模拟背景流量和网络攻击现象，对入侵检测系统进行常规性能评测，从而作出性能评价。

该测试方案的目标主要包括两方面的内容：(1)攻击网段通过 Vmware 软件创建多台虚拟机对被测网段进行攻击，构建一个仿真程度较高的测试环境。(2)通过对攻击网段进行良性攻击，分析观察 IDS 受攻击前后系统资源占用率、检测的准确性、处理数据的性能等性能指标的变化。以证明该测试方案的可行性。

3 入侵检测系统测试方案

3.1 测试环境

测试环境是对 IDS 进行评估和测试的基础，因为它直接关系到测试的结果，也直接影响测试的真实性和客观性。无论何种类型的 IDS，其运行的真实环境总是一个具体的网络。建立的测试环境应该能够满足 IDS 测试中多样性的需要，使它不仅能对测试环境进行灵活的调整，又能在现实网络中使其流量要求与技术指标相符合[3]。

虚拟机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。

我们在测试方案中选择 vmware 作为构建攻击仿真环境的平台软件。Vmware 有强大的硬件模拟功能、支持多种操作系统且使用方便，是较为常用的虚拟机软件，用一台单主机可以模拟出一个完备的网络环境，在此虚拟网络环境中部署 IDS，然后再配合测试软件就可以进行 IDS 的测试。这种方法有一定的可行性，因为它的环境单一性使得测试人员能够方便地测试一些轻量级的 IDS 或者测试 IDS 某个特定的功能方面。参考 MIT 林肯实验室用于生成入侵检测评测数据集的实验网络，我们设计了如图 1 所示的网络的拓扑结构，从图中我们可以看出整个实验网络分为被测网段和攻击网段两个部分[4,5]。

被测网络由以下几部分组成:Windows 靶机:系统中保留常见的漏洞、后门；Linux 靶机:对外开放 WWW，FTP，Telnet，Finger 等服务；Smartbits:按照实际网络中各网络协议数据流量的比例，产生不同字节数和不同流量大小，模拟正常背景流量；Sniffer:用于抓取被测网络中的流量，进行攻击特征数据包分析。

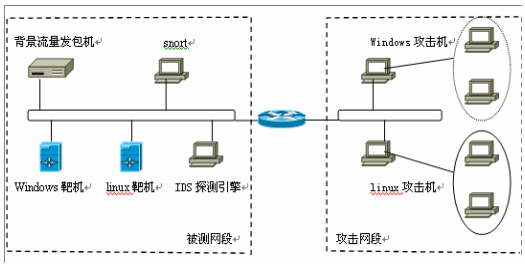

图 1 测试环境示意图

攻击网络由以下几部分组成:Windows 攻击机:虚拟出多台攻击机，预装多种攻击手段向靶机发起攻击；Linux 攻击机: 虚拟出多台攻击机，安装各种 Linux 攻击工具向靶机发起攻击。

在图 1 所示的攻击网段中，运行 Vmware 虚拟机软件的操作系统称为宿主机操作系统，在虚拟机里运行的操作系统叫做客户机操作系统，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。

3.2 测试过程

测试工作过程如下：由 Smartbits 流量产生器生成所需的网络背景流量，攻击网段的根据搜集到的攻击素材，由攻击机形成攻击数据流发送；对靶机以及待检测的 IDS 发起攻击，对 IDS 的运行情况进行记录，评估 IDS 的各种行为和对入侵事件的反应，最后对测试结果进行分析。

3.2.1 背景流量

网络背景流量对测试结果影响很大。网络背景流量中的各个数据包大小、内容、协议类型和流量大小等决定了 IDS 的处理方式，在很大程度上影响性能指标的有效性和真实性[6]。

背景流量的数据包大小。流量等于数据包大小和每秒数据包数的乘积。对于网卡和检测引擎，每秒能够处理的数据包是有限的，在一定的流量压力下，操作系统无法继续抓取数据包，IDS 检测引擎也开始丢包，无法重组会话，甚至遗漏关键特征数据包而漏报此攻击行为。

背景流量的数据包类型。数据包类型决定了 IDS 的处理方式，在很大程度上决定了性能指标的有效性和真实性。真实的网络流量包含了 HTTP、POP、SMTP、Finger、Telnet、FTP 等多种协议流，每种协议流都占有一定的比例，为了更加真实地反映 IDS 在实际应用中所表现出来的真实性能，在测试前我们使用 sniffer 来捕捉

实际网络流量，通过分析所捕捉到的实际流量，我们可以得到各类协议按时间的流量概率分布以及每类协议流中数据包按包长大小出现的概率分布。然后据此确定需要产生哪些协议流以及各类协议流所占的比例并在每类协议流中设置各长度的数据包所占的比例。

根据以上两点可知在模拟背景流量时，不仅需要考虑模拟的网络带宽大小，还需要考虑不同大小、不同协议类型的数据包在数据流中所占的比例。该项测试可以反映出在大负荷背景流量下，IDS 对各种攻击行为的检测性能，以及该 IDS 的负荷能力。本次测试使用 Smartbits 产生相应比例的 64，128，256，512，1024，1518 字节 10M，50M，80M 背景流量作为测试流量，每组背景流量产生相应比例的不同协议流。

3.2.2 攻击仿真

攻击仿真是整个测试过程的核心，也是测试结果是否合理的关键。攻击测试用例的选择应该尽可能的全面，但是由于各种攻击的数量过于庞大，不可能把每一种现有的攻击都进行仿真试验一遍，参考软件测试领域中的等价划分方法，先把所有的攻击按照某种标准进行划分，在所划分的每个子集里挑选若干个典型的攻击来完成测试。MIT 林肯实验室的数据就其可用性、全面性和权威性都得到了广泛的认可。1998 年，MIT LL 集前人研究之大成，提出了入侵检测系统数据集评测方法，不仅是 IDS 综合测试的典范，也是目前为止学术界最有影响力的入侵检测评测研究。目前 MIT LL 公开发布的评测数据集一共有 3 年,分别是 MIT'1998 、MIT'1999 和 MIT'2000。因此，考虑到数据集的公开性和定量的精确评测，在用合成的背景流量中加入 MIT 不同类型的攻击手段是比较合适的选择。这种方案既能较好地解决隐私问题,又能保留真实网络的特征。通过参考这些测试实验数据的，并通过虚拟机技术来实施具体的攻击。在主机上使用 vmware 软件仿真台多台虚拟机，每台虚拟机分别就是一个攻击测试域，在攻击网段机器上运行攻击测试程序发起攻击，其信息如表 1 所示[7]。

表 1 攻击类型信息表

操作系统	攻击类型	攻击手段
Window，linux	拒绝服务攻击	TCP /UDP flood， SYN flood，ICMP flood，
windows	远程攻击	Xscan，Hscan，
linux	后门	netcat、stcp shell

3.2.3 测试结果分析

在该环境对 snort 入侵检测系统进行了相应的测试，并在被测网段利用网络管理工具收集运行该 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， 得到的结果如下[8,9]：正常情况，CPU 占用率为 0%~5%，IDS 受攻击情况下，CPU 占用率提升至 60%~75%，内存占用率从 0%~5% 提升至 50%~65%；在正常情况下，终端系统几乎没有发生丢包的情况，而在系统受攻击的情况下，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。入侵检测系统的延迟时间随着背景流量的加大而逐渐增加，终端系统对服务请求的响应时间相应变慢，平均响应时间显著上升，可以看出通过该测试平台能正常开展 IDS 的测试工作，能够达到比较好的效果。在本实验搭建的仿真测试环境基础上可以进一步对入侵检测系统进行研究，对更多的性能指标进行测试对比，展开更多更丰富的后续研究。

4 结语

本文提出通过模拟现实的网络环境搭建软件平台进行 IDS 测试的方案。既考虑到测试的目的，又考虑了开发者的需要，尽量能够保证测试环境和开发环境的融合，该方法比较容易实现，可控制性强，能够满足 IDS 测试的多种需要，提供一种新的解决方法。随后的仿真测试说明该方法是有效的。

参考文献

1 史美林,钱俊,许超.入侵检测系统数据集评测研究.计算机科学,2006,8(33):1－8.
2 尹述峰,赵俊忠,郭银章.入侵检测系统评测数据集发展分析.计算机与数字工程,2009,4(37):108－110.
3 蔡林毅,田园,薛媛.基于环境模拟的入侵检测系统测试方法.现代电子技术, 2009,17:66－69.
4 李培.基于变化流量互补测试集的入侵检测系统测试.计算机科学,2009,3(36):97－99.
5 汪洋,龚俭.入侵检测系统评估方法综述.计算机工程与应用,2003,39(32):171－173.
6 张基温.基于应用环境的入侵检测系统测试方案.计算机工程与设计,2006,7(27):1220－1223.
7 王勇.一种 Windows 主机入侵检测实验系统.计算机工程,2006,10(32):132－134.
8 王汝传.基于虚拟机技术的人侵检测系统攻击仿真平台的研究和实现.电子与信息学报,2004,10(26):1668－1673.
9 王艳青.基于局域网的入侵检测系统测试平台设计与实现.计算机工程与设计,2008,9(29):2215－2232.