第50卷 第S1期
2004年10月

武汉大学学报(理学版)
J. Wuhan Univ. (Nat. Sci. Ed.)

Vol. 50 No. S1
Oct. 2004, 079～082

文章编号:1671-8836(2004)S1-0079-04

针对NIDS的分布式攻击评估技术研究

马恒太[1,2], 蒋建春[1,2], 黄 菁[1,2], 文伟平[1,2]

(1. 中国科学院 软件研究所,北京 100080;2. 中国科学院信息安全技术工程研究中心,北京 100080)

摘 要:对网络入侵检测系统本身的一些安全问题,如可靠性和生存健壮性等进行了研究,针对网络入侵检测系统——Snort,利用分布式协同攻击技术对NIDS的可靠性和生存健壮性进行了测试.实验结果显示,当前的NIDS是脆弱的.

关 键 词:网络入侵检测系统;生存健壮性;拒绝服务攻击;消息传送接口

中图分类号:TP 309 **文献标识码**:A

0 引 言

随着社会网络化程度的增加,对网络的依赖越来越大,网络安全问题也日益明显.最近几年,网络攻击技术迅速发展.其发展趋势主要表现为攻击自动化程度增高、攻击工具复杂程度提高、不对称威胁加大和攻击渗透性增强等[1].

攻击者为了实现攻击目的,逃避或利用安全保障系统,针对网络入侵检测系统(NIDS)使用各种方法试图逃避NIDS的检测[2].由于NIDS对网络安全的重要性,国外特别重视NIDS评测技术的研究,美国高级研究计划局(DARPA)特别关注入侵检测技术发明创新及应用研究[3,4],资助了20多个项目,用于IDS测试评估费用高达上千万美元.麻省理工学院Lincoln实验室开发了非实时的IDS性能评估工具[5],该工具能够动态地加速重放大量的数据,迅速产生所需测试数据.IBM公司Zurich研究实验室也开发了一套IDS测评工具[6].Fred Cohen博士从理论上探讨了攻击IDS若干方法[7].英国的NSS小组也专门就IDS进行了攻击测试[8],已在网络上公布了相关的技术资料.此外,还有一些黑客工具软件也可用作IDS攻击测试.

NIDS的生存健壮性是系统评价的重要指标,它主要体现在两个方面:一是系统本身在各种网络环境下都能正常工作;二是系统各个模块之间的通信不被破坏和仿冒.通过对NIDS健壮性的评测,可以更好地做好网络安全防范工作.不仅保证系统的安全性,还可极大地促进入侵检测技术的发展.

本文主要针对NIDS处理数据包的能力,研究快速制造大量测试数据包的技术,有效干扰系统的正常运行,测试其在极端环境下的生存能力.

本文的第1部分简要介绍了NIDS-snort;第2部分详细介绍了测试数据包的构造方式和对应的实验方案;第3部分是实验,并给出了实验结果及分析;第4部分是结束语.

1 网络入侵检测系统——Snort

1.1 入侵检测技术

入侵检测技术[9]自20世纪80年代提出以来得到了极大的发展,国内外一些研究机构及厂商已开发出了应用于不同操作系统的多种IDS.入侵检测方法主要分为两种:

一是异常检测.假定所有入侵行为都与正常行为不同.建立系统正常行为轮廓,理论上可把所有与正常轮廓不同的系统状态视为可疑.异常阈值与特征的选择是异常发现技术的关键.该方法的局限是并非所有的入侵都表现为异常,而且系统的轮廓也比较难于量化计算和及时更新.

二是误用检测.假定所有入侵行为都能表达为一种模式或特征,那么入侵可以用匹配的方法发现.

收稿日期:2004-07-05

基金项目:国家信息与网络安全保障持续发展计划基金资助(2001-研3-006);国家863高技术研究发展计划资助项目(2003AA144030);中科院软件所基础研究基金资助项目(CXK45634)

作者简介:马恒太(1970-),男,工程师,博士,现从事信息安全方面的研究. E-mail: mht@ercist.iscas.ac.cn

误用检测的关键是如何准确有效地描述入侵的模式.该方法的优点是误报少,局限是只能发现已知攻击,对未知攻击无能为力.

目前的方法都有不足之处,因此现在的IDS一般都融合多种检测技术,互相补充不足.

1.2 Snort

按数据来源分,IDS可分为基于主机型、基于网络型和混合型.Snort是一个网络型入侵检测系统,本文就是针对它进行讨论.当然,在此讨论的相关技术对其它NIDS同样适用.

Snort是一个轻量级实时NIDS,具有很好的扩展性和可移植性.Snort通过协议分析、内容检测及匹配来检测不同的攻击行为,如缓冲区溢出、端口扫描、CGI攻击、SMB探测、操作系统指纹特征探测等.

Snort包括包捕获和解析子系统、规则分析和检测子系统、日志和报警子系统及插件与预处理器4部分.

从网络上捕获到数据包后,进入包捕获和解析子系统,解析完成后,数据被记入日志,然后传到预处理器并进入检测模块.检测模块读取规则与数据包内容进行比较,匹配则激发相应的报警和日志动作.

Snort使用一种非常灵活且功能强大的规则描述语言.规则分为规则头和规则选项两部分,规则头包含规则的动作、协议、源和目标IP地址与网络掩码,及源和目标端口信息;规则选项部分包含报警消息内容和要检查包的具体部分.Snort规则文件的基本语法如下:

规则动作 协议类型 IP地址端口号→协议类型 IP地址端口号(规则选项).

Snort规则库是文本文件,每次启动时,由规则翻译器对规则库文件进行预处理,生成可供检测程序高效检索的二维链表(图1).二维链表生成后,就进入检测过程.检测引擎以数据包为参数,在规则链表中逐条匹配,从"左"到"右"遍历规则链表,从"上"到"下"遍历规则选项.

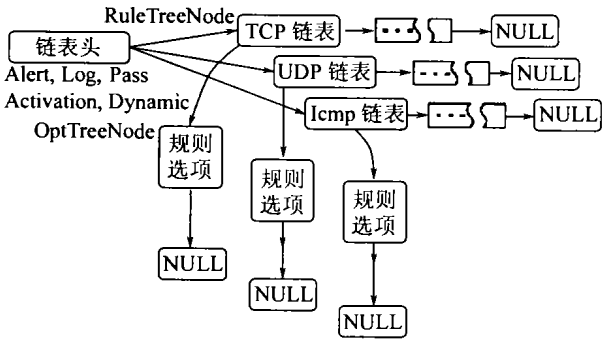

图1 规则在程序内部表示

2 测试数据构造和评估方案设计

测试数据要能明显降低NIDS的性能或形成拒绝服务,且易于构造.本文采用两种方法构造测试数据,虽然构造过程差异很大,但攻击测试效果相当相似.

2.1 基于NIDS报警机制获取数据

本方法是利用NIDS自身报警机制产生测试数据.误用检测引擎会准确地按照规则检测可疑行为,通过修改NIDS误用检测处理部分,可顺序记录网络可疑数据包,形成逼真的测试数据.

本文以公开源码NIDS-Snort为研究对象,进行相应处理,形成测试数据.由于NIDS的检测方法和目标是一致的,因此,对一个NIDS有效测试数据,对其它NIDS同样有效.通过实验,作者也证实了这一点,由Snort产生的测试数据,对Realsecure等加速重放测试可产生极其相似的评估效果.

攻击测试程序利用已获取的测试数据,重新构建数据包,加速发送到目标主机所在网段(如图2).

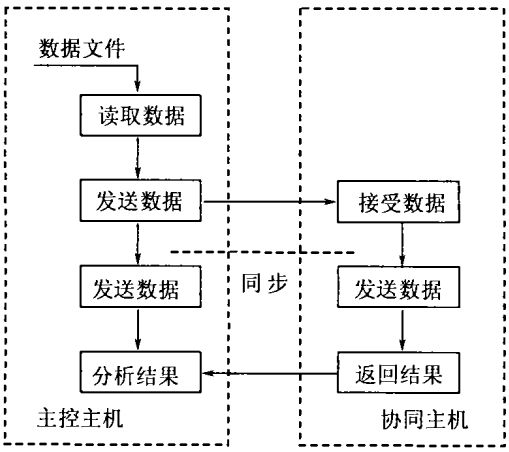

图2 分布式攻击测试流程(1)

主控程序流程:

1)初始化分布环境和网络接口;

2)读取指定文件数据,发送给各节点主机;

3)将数据包插入环状链表;

4)各节点主机同步,从环状链表读取数据包,加速发送;

5)收集、分析测试统计结果;

6)释放环状链表.

协同程序流程:

1)、3)、4)、6)与主控流程同,2)接收测试数据

包,5) 将测试统计结果发送回主控机.

2.2 基于 Snort 规则文件构造测试数据

通过对 Snort 规则进行分析,依据 Snort 的规则描述来构建测试数据. 只要数据包内容符合某一规则动作是 alert 的规则描述,而 Snort 又配置了相应检测规则,该数据包就能触发其报警.

测试数据包构造过程如下:

a) 根据数据包协议,初始化 TCP、UDP、ICMP 首部内容;

b) 根据规则内容修改数据包相应域;

c) 计算 IP 首部 16 位校验和.

该方法的测试数据是在协同主机中构造的,主机间通信量较少. 测试数据构造完成后,各测试主机进行同步,同时加速发送测试数据. 工作流程如图 3 所示.

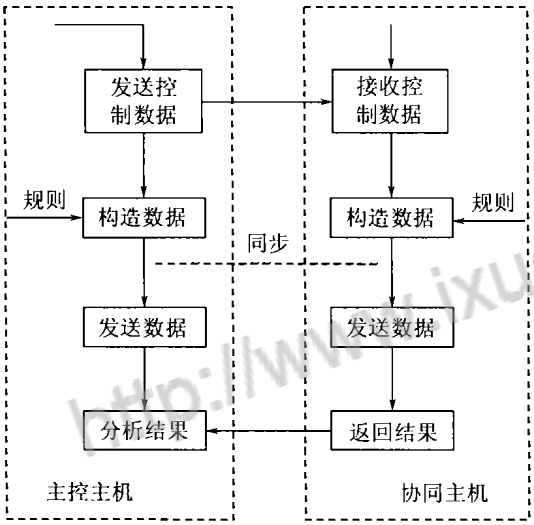

图 3　分布式攻击测试流程(2)

3 实验及效果分析

测试实验环境选用消息传递接口[10](MPI)实现各主机间的通信与任务同步. MPI 广泛应用于并行机,为消息传递建立了一个实际的、可移植的和灵活有效的标准.

实验环境如图 4 所示,192.168.0.2、192.168.0.3 和 192.168.3.2 构成分布式攻击环境,作为攻击测试主机,192.168.0.2 是主控主机. 192.168.3.3 装有 Snort,做为测试目标主机.

实验分两组,第 1 组是利用 NIDS 报警机制获取的数据进行测试;第 2 组是利用基于 Snort 规则文件构造的数据进行测试. 分别记录各主机的攻击时间、发包数量、发包长度等数据. 结果显示,两组实验测试效果很相似,都可以明显影响目标主机,表 1 是第 2 组实验的统计结果.

表2是基于规则攻击评估的数据统计:(其中

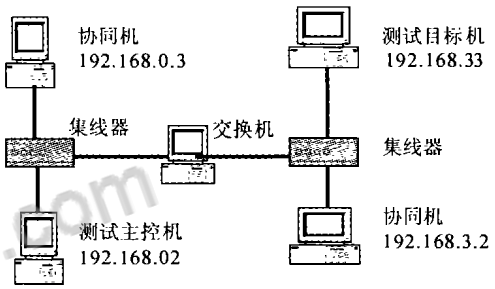

图 4　实验环境拓扑图

表 1　测试实验结果

攻击主机	发包数量	发包长度/B	发包时间/s	发包速率/MB·s^{-1}
192.168.3.2	1540078	113965772	10	10.87
192.168.0.3	924535	68415590	10	6.52
192.168.0.2	1518273	112352202	10	10.71

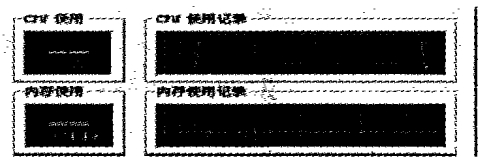

表 2　基于规则攻击网络入侵检测系统的统计数据表

攻击次数	发送规则条数	发送时间/s	接受规则数	消耗磁盘空间/kB	文件数
1	100	0.035634	43	372	43
2	200	0.046085	55	444	55
3	1000	0.123724	134	1100	134
4	2000	0.219417	189	1500	189
5	4000	0.416121	436	3400	436
6	8000	0.809960	765	6000	765
7	10000	1.024153	965	7600	965
8	40000	4.089581	3187	25000	3187
9	100000	10.752189	6825	58000	6825
10	1000000	103.95639	33264	256000	33264

规则是随机抽取的,攻击测试主机数目为一台).

从以上实验结果分析可知:

● 攻击对 CPU 的占用有着很大影响.多台主机攻击时,时间稍长就会使目标主机当机;

● 发包速率对测试效果有决定作用.由于测试数据预先生成,测试程序本身负荷小,发包速率可达 10 MB/s;

● 实验对被测主机内存使用情况有一定影响,但不明显,这正是无状态 NIDS 的特点;

● 实验对硬盘的占用有很大影响,由于 NIDS 将日志信息写入硬盘,大量报警数据使日志文件在短短的几分钟内达到上百兆;

● 攻击测试同时也消耗网络带宽.具体表现为丢包率增高.

4 结束语

近年来,入侵检测技术逐渐成为网络安全研究的热点之一,入侵检测系统作为网络系统的安全预警器,越来越受倚重.对 NIDS 进行攻击性评估是促进系统自身安全改进行之有效的方法.

NIDS 生存健壮性评估是对其网络安全保障能力的测试.本实验对 Snort 的数据处理能力和生存健壮性进行了有效测试.作者认为,NIDS 是脆弱的,大流量网络下其可用性值得怀疑,要实现实时检测和响应,还需要在体系结构、攻击判别方法和生存健壮性等方面进行重大改进.

对 RealSecure 等 NIDS 进行同样测试,得到类似实验结果和相同结论.同时还对 NIDS 的检测能力进行了评测,如可避过 NIDS 检测的缓冲区溢出攻击、隐蔽通道攻击、分布式网络扫描等,相关工作将另文发表.

参考文献:

[1] Houle K, Weaver G, Long N, *et al*. Trends in Denial of Service Attack Technology [DB/OL]. *http://www.cert.org/archiue/pdf/Dostrends.pdf*. 2001-10.

[2] Ptacek H, Newsham N. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection [DB/OL]. *http://secinf, net/info/ids/idspaper/idspaper.html*. 1998.

[3] Zhang K. A Methodology for Testing Intrusion Detection Systems[D]. University of California at Davis, May 1993.

[4] Wang C X, Knight C. Towards Survivable Intrusion Detection[DB/OL]. *http://www.cert.org/research/isw/isw2000/papers/38.pdf*. 2000-12.

[5] John M. Testing Intrusion Detection Systems: a Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory[A]. *ACM Transactions on Information and System Security (TISSEC)*[C]. 2000, **3**: 262-294.

[6] Dębar H, Dacier M, Wespi A, *et al*. A Workbench for Intrusion Detection Systems[R]. IBM Zurich Research Laboratory, Ruschlikon, Switzerland, Mar. 1998.

[7] Fred C. 50 ways to Defeat Your Intrusion Detection System[DB/OL]. *http://all.net/*. 1997-12.

[8] The NSS Group. Intrusion Detection Systems Group Test (Edition 2)[DB/OL]. Oakwood House, Wennington, Ambridgeshire, England, Dec. 2001. *http://www.nss.co.uk/ids/*. 2001-12.

[9] Clifford K, Porras A, Chen S, *et al*. A Common Intrusion Detection Framework, The Open Group SRI UC Davis ISI. July 15, 1998.

[10] Message Passing Interface Forum, MPI-2: Extensions to Message Passing Interface[DB/OL]. *http://www.mpi-forum.org/*. 1997-07.

Distributed Attack and Test Technology for Evaluating NIDS

MA Heng-tai[1,2], JIANG Jian-chun[1,2], HUANG Jing[1,2], WEN Wei-ping[1,2]

(1. Software Institute, Chinese Academy of Sciences, Beijing 100080, China;
2. Engineering Research Center for Information Security Technology, Chinese Academy of Sciences, Beijing 100080, China)

Abstract: Aiming at lately popular NIDS, this paper tries to test the survivability and robustness of the SNORT with DDOS attack technology. According to the result and analysis of the experiment, NIDS is vulnerable.

Key words: NIDS; survivability and robustness; DDOS; MPI(Message-Passing Interface)