网络深层防御体系模型的研究和实现

李 菲,乔佩利
(哈尔滨理工大学 计算机科学与技术学院,黑龙江 哈尔滨 150080)

摘 要:针对单一技术在安全防御上存在的缺陷,提出了一个基于三层防御机制的网络安全防御体系模型。该体系有机结合了防火墙、NIPS、基于异常的入侵检测、蜜罐等多种安全技术深层抵御入侵,各组件通过传递XML信息互相协作。首先对网络的安全和结构进行分析,在此基础上给出了体系模型并说明了模型的工作流程,对涉及的关键技术做了探讨,给出了蠕虫攻击实验测试系统的性能。实验结果证明该体系不仅能阻断已知攻击,对未知攻击也做到了有效防御。

关键词:防火墙;入侵检测;蜜罐;NIPS;XML
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)02-0159-04

Research and Implementation of Network Defense In-Depth System Model

LI Fei, QIAO Pei-li
(Computer Science and Technology College, Harbin Univ. of Sci. and Tech., Harbin 150080, China)

Abstract: Focusing on the defects of the single technology on security prevention, proposed a network defense system model based on the three-level defense mechanism. The model that organically joined firewall, NIPS, AIDS, honeypot and so on had resisted attack in-depth, components cooperated by transmiting XML message. Firstly, the design thought of the security prevention system was described in the paper, and based on the thought, the architecture and workflow of the model was presented, and then the relevant sore technology was discussed. Lastly the worm attack experiment was presented to test the performance of the system. The experiment proved that the model not only blocked the known attack but also achieved the effective defense to the unknown attack.

Key words: firewall; intrusion detection; honeypot; NIPS; XML

0 引 言

随着网络应用的不断深入和黑客攻击水平的日益提高,网络安全和可靠性成为人们关注的焦点。目前各研发企业对安全技术的研究也越来越深入,但研究重点都放在了某一个单独的技术上,却很少考虑如何对各种技术加以整合。然而单一的安全技术如防火墙、入侵检测技术、入侵防御技术不足以保护网络安全,它们存在着局限性。防火墙无法阻挡面向应用层的攻击;入侵检测系统只能检测攻击而不能及时采取响应措施;入侵防御系统因不能采取复杂的检测手段容易产生漏报(如果检测方法复杂会造成网络传输延迟)。安全不是孤立的问题[1],木桶原理形象说明了这一点。因此,只有在各种安全技术的研究基础上,制定具体的系统安全策略,通过设立多道的安全防线集成各种可靠的安全机制,建立完善的多层安全防御体系,才能抵御来自系统内外的入侵攻击,达到维护网络安全的目的。

基于上述思想,提出了综合防火墙、NIPS、异常入侵检测、蜜罐四种安全技术的网络深层防御体系模型,模型中各技术互相协作,层层抵御入侵。

1 网络深层防御体系模型的工作流程

数据包由外网进入内网的处理流程如图1所示。模型中把网络数据包划分为三类:正常数据包、已知入侵数据包、未知可疑数据包。处理流程为:(1)第一层防御。数据包首先经过外防火墙规则粗粒度的检测。若防火墙加载了对此数据包目的地址的重定向规则,则说明数据包为未知可疑数据包,将其转入蜜罐进行跟踪分析,并把记录下的攻击过程保存在远程日志服务器中,由规则分析器提炼出新的规则加入NIPS。若外防火墙没有加载该数据包的重定向规则,则数据包经过剩余规则检测后进入内网。(2)第二层防御。由

收稿日期:2007-07-11
基金项目:国家社会公益研究专项(2005DIB2J218)
作者简介:李 菲(1983-),女,山东德州人,硕士研究生,研究方向为网络安全;乔佩利,教授,研究方向为网络安全与电子政务。

NIPS采用误用检测技术对进入内网的数据包进行快速检测,若发现已知入侵数据包则立即阻断。(3)第三层防御。由于 NIPS 发现不了未知攻击,流量异常检测器对 NIPS 认为的可信数据流进行再次分析。若检测器发现异常流量,则收集重定向控制信息:攻击源、目的地址和重定向时长等传给外防火墙,由防火墙的 Sever 进程生成重定向规则把后续的未知可疑数据包转入蜜罐,从而保护了真正的受攻击主机。

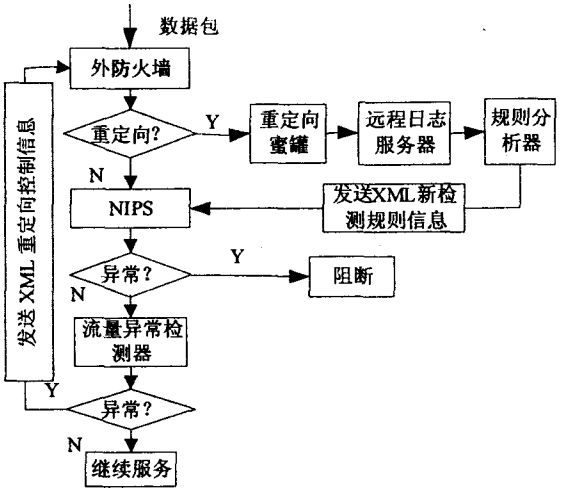

图 1 数据包处理流程图

2 深层防御体系各组成部分的设计和实现

如图 2 所示,体系模型由外防火墙、NIPS、流量异常检测器、蜜网、日志服务器和规则生成器组成。各部分的功能和实现如下:

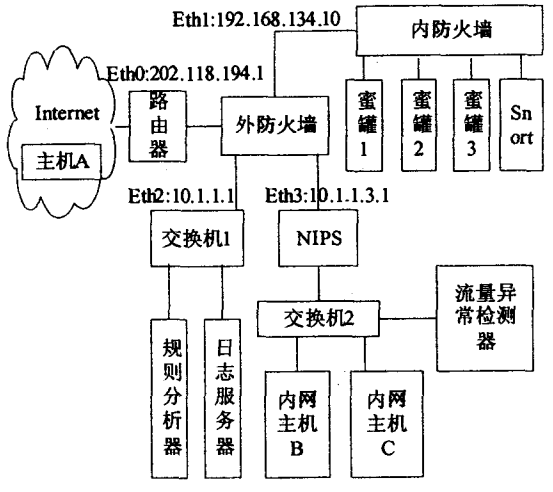

图 2 网络深层防御体系结构拓扑图

外防火墙是配有四块网卡的 Netfilter/iptables 防火墙主机,eth0 连接外网,eth1 连接蜜网,eth2 连接日志服务器,eth3 连接内网。防火墙对于外网进入内网和日志服务器的数据包采用"严进宽出"的配置策略,将一部分越权访问行为隔离。而对于外网进入蜜网的数据包则不配置访问限制功能,黑客可轻松进入刺探。此外,外防火墙和流量异常检测器基于 C/S 模式进行协作。防火墙主机中驻留着 Sever 进程,负责监听接收流量异常检测器传来的重定向控制信息,并根据信息生成重定向规则加入防火墙规则链中,实现了对可疑数据包的重定向。

NIPS 处于外防火墙和交换机之间,采用基于误用的检测技术阻断已知入侵数据包。本模型中 NIPS 是在 Netfilter/iptables 防火墙和 Snort 基础上进行集成开发的。NIPS 实现如下:(1)首先由 Netfilter/iptables 防火墙捕获数据包,并且通过设置 iptables 规则:iptables -A FORWARD -j QUEUE,将数据包发往用户空间队列。(2)修改 Snort 抓包程序,使用 Netfilter 提供的 libipq 库函数,不直接从链路层抓包,而是作为用户空间的应用程序从用户空间队列拷贝数据包进行检测。(3)修改 Snort 响应程序。将 Snort 规则匹配后的执行动作改为:pass,drop,reject。如果数据包匹配成功,响应程序中调用 libipq 库的 ipq_set_verdict 函数把执行动作传给防火墙,由防火墙对队列数据具体操作。

流量异常检测器:检测器与交换机相连,数据流通过交换机的 SPAN 端口镜像到检测器的采集模块 Sniffer 中。检测器采用基于异常的检测方法进行检测分析。检测器的实现过程:(1)确定可测度集,即准确反映流量的属性集[2]。本检测器定义了 18 项测度,分别是:HTTP,FTP,SMTP,POP3,ICMP 包的平均进出量和包长度,TCP 中 syn 与 syn+ack 的比率,udp 端口入出比率,ICMP 的 reguest/reply 比率。(2)建立流量模型。将过去 20 天每一天分为 24 个时段,采用基于正态分布的统计方法计算出各受保护主机在每个时段 18 个测度的阈值区间,从而建立一个正常的网络流量模型。(3)进行流量检测。计算各受保护主机当前时段的流量测度值并与正常模型比对[3],若超过了阈值,则判定为未知可疑行为发出警报,并且触发 Client 进程收集重定向控制信息发送给外防火墙。

蜜网:蜜网由三台蜜罐主机、内防火墙 Netfilter/iptables、Snort 组成。蜜网负责对重定向的可疑入侵进行跟踪分析,从而保护了真正的被攻击主机。蜜网主机各自使用了不同的操作系统,并且在不同系统平台上运行不同的系统软件,例如办公软件、MIS 等,从而使建立的网络环境看上去更加真实可信[4],并且蜜罐主机日志记录了黑客的详细攻击活动。为了防止黑客将蜜网作为跳板对其它系统发起攻击,必须制定一种访问策略限制蜜网向外连接。策略为:(1)限制连接数。例如,通过设置 iptables 规则制定某蜜罐每小时对外 TCP 连接数为 10,若超过 10,内防火墙阻断后续连

接。规则设置为:iptables -A FORWARD -s *.*.*.* -p tcp -m physdev -physdev-in eth1 -m state-state NEW -m limit -limit 10/hour -limit-burst 10 -j tcpHandler。(2)基于C/S模式的Snort与内防火墙联动阻断攻击。Snort若发现向外连接的攻击行为,产生报警并生成阻断控制信息,通知内防火墙阻断后续数据包。

日志服务器和规则生成器:日志服务器是对防火墙、Snort和蜜罐主机日志的备份。因为这些攻击日志对人们很重要但又易被黑客破坏[5],所以需要远程维护。本模型采用强访问控制的Linux系统存放远程日志。规则生成器采用人工智能推理的方法对相关日志进行融合分析,重建攻击场景,并采用LCS算法求取相同连接记录的最长公共子串,提炼出新的入侵规则,然后启动线程传送给NIPS。

3　网络深层防御体系模型关键技术的研究

此深层防御体系作为一种综合的安全机制,涉及到多个复杂技术的集成。下面介绍体系中所应用到的几个关键技术。

3.1　基于正态分布的统计建模技术

流量异常检测器采用基于正态分布的统计方法计算过去20天各受保护主机每天每个时间段18个测度的区间阈值,从而建立了一个正常的流量模型。以计算主机A在上午9:00-10:00时段Http包平均流入量的阈值为例说明建模方法。将这个时间段再等分 n 个时间片,$n=30$,对于每个时间片计算出Http包的平均流入量。中心极限定理认为无论研究的统计总体服从什么样的分布,样本平均值的分布均接近一个正态分布,正态分布的均值等于总体分布的均值,标准差等于总体分布的标准差除以样本大小的平方根。所以可认为每个时段Http包平均流入量是呈正态分布的,那么可基于定理计算出包平均流入量的置信区间。

假设 X_{n-1} 是时段中前 $n-1$ 个时间片Http包平均流入量的累加和,x_n 是第 n 个时间片的平均流入量,那么就有 n 个时间片流入量的累加和为 $X_n = X_{n-1} + x_n$。相应地,n 个时间片内数据包平均流入量为 $\bar{X}_n = X_n/n$,标准差为 $S_n = \sqrt{\frac{1}{n-1}(\sum_{i=1}^{n} X_i^2 - n\bar{X}_n^2)}$。根据概率理论,样本均值 $\bar{X}_n$ 的标准差为 $\frac{S_n}{\sqrt{n}}$,因此总体均值的置信度为 $(1-\alpha)$,置信区间为 $(\bar{X}_n - Z_{\frac{\alpha}{2}}\frac{S_n}{\sqrt{n}}, \bar{X}_n + Z_{\frac{\alpha}{2}}\frac{S_n}{\sqrt{n}})$。用如上方法计算出过去20天每天上午9:00-10:00时段的Http包平均流入量的置信区间,共得到20个置信区间,阈值下限取这20个区间的最小下限,阈值上限取20个区间的最大上限,这样就建立了检测阈值区间。检测时对主机A记录它在上午每个时间片(设为5~10秒)内流入的数据包个数,时间片用完后计算其平均流量值并与建立的检测阈值区间比较,若在此区间内,则认为正常,否则判定为异常。

3.2　入侵行为重定向技术

入侵行为重定向功能是通过外防火墙Netfilter/iptables的地址转换技术实现的。通过向防火墙添加针对该数据包的重定向规则即地址转换规则改变其目的地址,使其转入蜜罐主机。由于重定向规则是对未知可疑数据包采取的响应措施,规则在防火墙中应具有优先性和动态性:(1)优先性:防火墙本身提供了向规则头部插入新规则的选项(-I选项)功能,使用此选项插入规则,保证了新的重定向规则在防火墙规则链中编号为1,数据包到来后优先被此规则检测。例1,对于可疑行为:外网主机202.118.194.173总是试图连接telnet连接主机10.1.3.9,把telnet连接转入蜜罐主机192.168.134.13,则生成iptables地址转换规则:iptables -t nat -I PREROUTING -s 202.118.194.173 -d 10.1.3.9 -dport32 -i eth3 -j DNAT -to 192.168.134.13:32;(2)动态性:规则在防火墙中有生存时间,为了不影响攻击停止后正常的服务请求,须设立重定向时长,对于超过时长的规则利用防火墙删除规则选项(-D选项)删除指定编号的规则。

3.3　基于XML的数据封装技术

XML是具有数据描述功能的高度结构性及可验证性语言,它有可读性、灵活性、可扩展性、互操作性等特点,可作为不同系统或应用程序之间的数据交换格式。本模型中流量异常检测器与外防火墙、规则分析器与NIPS、Snort与内防火墙之间的交换信息都是使用XML封装后传递的。对于上述例子1,重定向控制信息使用XML封装为:

```
<response>
<action>Rediction</action>
<protocol>TCP</protocol>
<sip>202.118.194.173</sip>//源IP地址
<sport>32</sport>//源端口
<dip>10.1.3.9</dip>//目的IP地址
<dport>32</dport>//目的端口
<redip>192.168.134.13</redip>//重定向地址
<redport>32</redport>//重定向端口
<datetime>2007-6-26,9:20:20</datetime>
<during>3 hour</during>//重定向时长
</response>
```

4 实 验

以 Nimda 攻击为例测试体系对未知攻击的防御性能。实验环境见图 2。在 NIPS 和 Snort 删除对 Nimda 蠕虫攻击的检测规则,这样对于体系来说此攻击为未知攻击。

测试过程:在外网 IP 为 202.118.194.140 的主机 A 上启动 Tftp 服务器,监听 UDP/69 端口。然后使用 X-Scan 扫描器,选中"IIS 漏洞扫描模块",对 IP 为 10.1.3.9 的内网主机 B 的 80 端口进行扫描,发现有 IIS 漏洞,则使用 Tftp 命令将本地的 Admin.Dll 病毒文件传播给主机 B,并发送请求执行命令。

测试结果:由于 NIPS 规则库中无关于 Nimda 攻击的检测规则,它没有阻断攻击数据包。而流量异常检测器发出了报警声并弹出页面报警通知(见图 3),

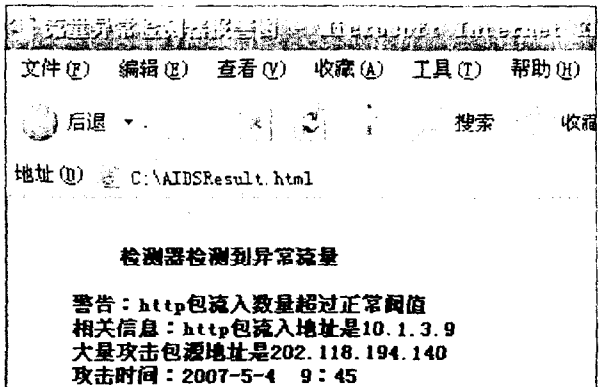

图 3 检测器检测到攻击-页面报警图

因为它发现主机 B 在这一时刻的 http 包平均流入量不在正常检测阈值区间 18769.3 包/秒~40321.8 包/秒,且这些大量 http 包来源于同一个地址 202.118.194.140。外防火墙的地址转换规则将这些可疑数据包重定向蜜罐 1:iptables -t nat -I PREROUTING -s 202.118.194.140 -d 10.1.3.9 -dport80 -i eth3 -j DNAT -to 192.168.134.13:80。数据包进入蜜网后,蜜罐主机 1 布置有 IIS 漏洞,不管主机 A"GET"什么都回应"200 OK"。打开蜜罐主机日志,发现了以下可疑信息:"GET/scr ipts/root.exe? /c+dir HTTP/1.0, GET/c/winnt/system32/cmd.exe? /c + dir HTTP/1.0, … GET/scripts/root.exe? /c + tftp -i 202.118.194.140,GET Admin.dll HTTP/1.0,GET/scripts/Admin.dll HTTP/1.0"。规则生成器根据这些记录采用 LCS 算法提炼出攻击特征生成了防御规则:"Drop tcp any any->any 80(msg:"Nimda WORM";flags:PA;content:"/root.exe? /c+dir";nocase;)"等。

在实验中本防御体系成功地保护了受攻击主机 B,并生成防御此攻击的检测规则。

5 结束语

文中提出的网络深层防御体系模型不仅能防御 2000 多种已知攻击,对于未知攻击(特别是蠕虫攻击和 DOS 攻击)也起到了实时抵制作用。模型中 NIPS 和流量异常检测器是基于软件开发的,整个架构成本低且功能强大,特别适合中小企业和普通学校使用。模型采用了基于误用和异常两种检测技术很好地解决了传统 NIDS 的漏报问题,但是误报问题还没有得到很好的控制,有可能会出现对合法请求的阻断。解决误报问题需要模型全方位地识别网络环境,减少错误报警。可以考虑加入漏洞扫描器实时评估网络系统弱点并与 NIPS 和异常检测器互动来印证报警是否属实,确定报警真实性之后系统再作出合理响应,具体的协作方案这是今后研究的一个重点。

参考文献:

[1] 程 渤,张新有.基于主动诱骗的电力网络安全提升策略设计与实现[J].电力系统自动化,2004,28(21):73-75.

[2] Goldman A. Anomaly Detection Based on an Iterative Local Statisticals Approach[J]. IEEE Signal Processing,2004,84(7):440-443.

[3] 宋连涛,庄为华.基于异常的入侵检测技术在 Snort 系统中的应用[J].计算机技术与发展,2006,16(6):136-138.

[4] 孙知信,杨家园.基于蜜罐的主动网络安全系统的研究与实现[J].电子与信息学报,2005,27(3):24-26.

[5] 熊 华,郭世泽.取证与蜜罐[M].北京:人民邮电出版社,2003:8-19.

(上接第 145 页)

(7):899-907.

[2] Workflow Management Coalition. Workflow reference model [EB/OL]. 1995-01. http://www.wfmc.org/standards/docs.

[3] 周 坤,邓保华,林齐圣,等.面向 WEB SERVICES 动态复合的流程自动化系统的研究与实现[J].计算机应用,2005,25(1):85-90.

[4] Blow M, Goland Y, Kloppmann M, et al. BPELJ: BPEL for Java, A Joint White Paper by BEA and IBM[EB/OL]. 2004. http://www.ibm.com/developerworks/cn/webservices/ws-bpelj/ws-bpelj.pdf.

[5] BEA. WEBLOGIC PLATFORM 的 BPM 开发与集成. [EB/OL]. 2005. http://searchwebservices.techtarget.com.cn/imagelist/05/08/sy3a6f1936yu.rar.

[6] 褚红伟,葛 玮.基于 Web Services 的分布式工作流的研究与实现[J].计算机应用研究,2005,22(8):49-51.