广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(2):80~81,84
Vol. 23,No. 2 May 2007

防火墙与入侵检测系统(IDS)互动模型的构建
Construction of Interactive Model for Fire Wall and Intrusion Detection System(IDS)

梁 骥
LIANG Ji

(广西计算中心,广西南宁 530022)
(Computing Center of Guangxi,Nanning,Guangxi,530022,China)

摘要:通过建立基于误用的入侵检测系统(IDS)的特征库,并采用VC++语言建立防火墙与入侵检测系统之间的开放接口,构建防火墙与入侵检测系统互动模型。通过互动模型,防火墙可以利用入侵检测系统及时地发现其策略之外的攻击行为,入侵检测系统也可以通过防火墙阻断来自外部网络的攻击行为,能有效互动地构成较为有效的安全防护体系,大大提高网络整体的防护性能。该模型能解决传统信息安全技术的弊端和原先防火墙的粗颗粒防御与检测系统只发现,难响应的问题。

关键词:互动模型 防火墙 入侵检测
中图法分类号:TP39 **文献标识码**:A **文章编号**:1002-7378(2007)02-0080-02

Abstract:Interactive Model for Fire Wall and Intrusion Detection System(IDS) is constructed on the basis of misuse of feature database for IDS. The model is capable of overcoming the defects of traditonal information security technology and the problems that are difficult for coarse particle defense and detection system of fire wall to respond to.

Key words:interactive model,firewall,intrusion detection system(IDS)

从狭义上讲,防火墙是两个网络之间访问控制的一个或一系列网络设备,是安装了防火墙软件的主机、路由器或多机系统;从广义上讲,防火墙还包括整个网络的安全策略和安全行为,是一整套保障网络安全的手段[1]。防火墙与目前应用的很多网络安全设备,如代理服务器、过滤器、加密器、口令验证器等都采用的是静态安全技术,这些静态安全技术都需要人工来实施和维护,不能主动地跟踪入侵者。近年来,入侵检测作为一种积极主动的安全防护技术得到了广泛的重视,被认为是防火墙之后的第二道安全闸门。入侵检测被定义为对计算机和网络资源上的恶意行为进行识别和响应的处理过程。入侵检测系统收集计算机网络系统中的若干关键点信息,并分析这些信息,从而检查网络中是否有违反安全策略的行为或遭到袭击。入侵检测系统从网络安全立体纵深、多层次防御的角度出发,对防范网络恶意攻击及误操作提供了主动的实时保护,从而能够在网络系统受到危害之前拦截和响应[2]。入侵检测系统(IDS)使用动态安全技术,它能够主动地检测网络中的易受攻击点和安全漏洞,能较快地探测到危险行为[1]。本文通过建立基于误用的入侵检测系统的特征库,并采用VC++语言建立防火墙与入侵检测系统之间的开放接口构建防火墙与入侵检测系统互动模型。

收稿日期:2007-04-10

作者简介:梁 骥(1972-),男,助理工程师,主要从事网络安全研究工作。

1 互动模型原理

防火墙与入侵检测系统互动模型是在对防火墙系统和入侵检测系统的功能和优缺点进行仔细的研究之后,建立的一个基于入侵检测系统和防火墙系统的互动模型,实现二者功能上的互补。模型是在防火墙或者入侵检测设备上开放一个接口供对方调用,按照一定的协议进行通信,传输警报,从而防火墙可以使用它的第一层防御功能——访问控制;入侵检测系统可以行使它的第二层的防御功能——检

测入侵,丢弃恶意通信,确保这次通信不能达到目的地,并通知防火墙进行阻断[3]。防火墙与入侵检测系统互动模型的逻辑示意图,如图 1 所示。

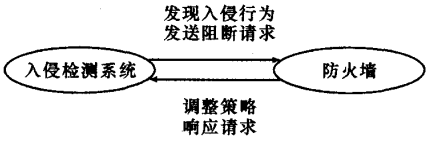

图 1　防火墙与入侵检测系统互动模型的逻辑示意

2　互动模型的构建

2.1　编写基于误用的入侵检测系统特征库

基于误用的入侵检测系统的误报警率低,而且对一些已知的常用的攻击行为特别有效。为了使该入侵检测系统实现我们所期望的功能,就必须将一些规则编写至特征库中。通常规则划分为两个逻辑部分:规则头和规则选项。规则头包含了规则动作、协议、ip 源地址和目的地址、子网掩码以及源端口和目标端口值等信息。而规则选项则包含警报信息,以及用于确定是否触发规则响应动作而需检查的数据包区域位置信息[3]。在编写特征库前必须先仔细分析所要保护的网络经常或可能遭受的攻击例如,

(1)对任何来自外部网络地址的数据包生成警报信号。

Alert tcp ! 58. 59. 136. 0/8 any －＞ 58. 59. 136. 0/8 any

(2)记录来自任意端口且目标端口为 1～1024 的 udp 数据包。

Log udp any any －＞58. 59. 136. 0/8 1:1024

(1)规则中的 ip 地址表示任意一个来自外部网络而目的地址为本地网络地址的 tcp 数据包。

2.2　防火墙与入侵检测系统的接口

经过比较,我们认为将入侵检测系统与防火墙通过开放接口来实现互动的方法要比紧密结合方法要好,因为系统越复杂其自身的安全问题就越难以解决,所以我们通过 VC＋＋语言来实现防火墙与入侵检测系统之间的接口。具体步骤如下。

(1)初始化通信连接时,一般由入侵检测系统向防火墙发起连接;

(2)建立正常连接后,当入侵检测系统产生需要通知防火墙的安全事件时,可以通过发送约定格式的数据包,来传递必要的互动信息;

(3)防火墙收到互动信息后,可以实施互动行为,并将结果(成功与否)以约定格式的数据包反馈给入侵检测系统。

防火墙端建立通信服务的代码如下。

```
Init openSSL();// 初始化通讯环境
CreateServer(char * ip, char * port);//建立服务(其中 ip 为防火墙的 ip 地址,端口为通讯的端口)
SetRevCallbacd(void * ApRecvFunc);// 设立接收的回调函数,处理接收数据
SetAcceptClallback(void * ApacceptFunc);// 设立接收的回调函数
RunServer();//运行服务
Send(char * ApBuf, int AnBuflen);//向 IDS 发送反馈信息;
StopServer();//停止服务
```

通信数据包结构代码如下。

```
Typedef struct _Packet
{Unsigned char srcip[16];// 源 ip 地址
Unsigned char dstip[16];//目的 ip 地址
Unsigned char sensorip[16];//IDS 引擎 ip 地址
Unsinged int duration;//阻断时间
Unsinged int srcport;// 源端口
Unsinged int dstport;// 目的端口
Unsinged int protocol;// 协议
Unsinged int mode;//阻断模式
Unsinged int version;//版本号
Unsinged int echo;//回应标识
Unsinged int reserver;//保留字段
}Packet;
```

3　结束语

通过防火墙与入侵检测系统互动模型,防火墙就可以通过入侵检测系统及时地发现其策略之外的攻击行为,入侵检测系统也可以通过防火墙对来自外部网络的攻击行为进行阻断。入侵检测系统与防火墙地有效互动构成了较为有效的安全防护体系,可以大大提高整体防护性能,解决了传统信息安全技术的弊端和原先防火墙的粗颗粒防御与检测系统只发现,难响应的问题。我们将此模型大胆地应用在某市政务网络中,大大提高了该网络的安全防护水平,取得了良好的效果。相信经过进一步的研究与开

(下转第 84 页)

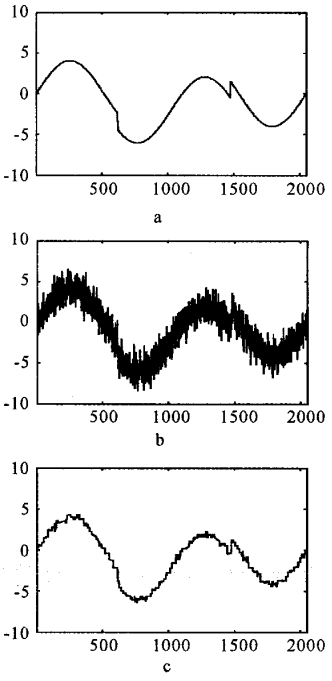

图1 Haar小波对一维信号消噪

a.原始信号;b.含噪信号(信噪比为3);c.Haar小波去噪后的信号

图2 Haar小波对二维图像消噪

a.原始图像;b.含噪图像;c.Haar独立阈值消噪图像;d.平滑后的图像

理,并对处理后的图形进行离散取样,然后将其平滑.图2中a为一灰度图像,b为a的加噪图像,将b用Haar小波进行消噪处理得到c所示的图像.虽然取出了大部分高频噪声,但是得到的图像有些模糊,消噪效果并不是特别理想.那么再将c进行平滑化,得到d所示的结果.经过平滑处理更有利于消除噪声信号,消噪的效果比较理想.

4 结束语

将Haar小波离散化后进行小波变换的方法,应用于信号及图像的消噪处理当中,取得了满意的结果.因此将Haar小波离散化后进行小波变换是一种有效的方法,具有一定的实用价值.

参考文献:

[1] 杨福生.小波分析的工程分析与应用[M].北京:科学技术出版社,1999.

[2] 谭剑,陈祥训,郑健超.连续小波变换在使用中应满足的条件[J].电工技术学报,1998,13(5):57-60.

[3] 崔锦泰.小波分析导论[M].程正兴,译.西安:西安交通大学出版社,1995.

[4] 徐晨,赵瑞珍,甘晓冰.小波分析:应用算法[M].北京:科学出版社,2004.

[5] 刘贵忠,邸双亮.小波分析及其应用[M].西安:西安电子科技大学出版社,1992.

[6] 胡昌华,李国华,刘涛,等.基于MATLAB 6.x的系统分析与设计——小波分析[M].西安:西安电子科技大学出版社,2004.

[7] 曹志刚,钱亚生.现代通信原理[M].北京:清华大学出版社,2002.

[8] 王应生,徐亚宁.信号与系统[M].北京:电子工业出版社,2003:12-17.

(责任编辑:韦廷宗)

(上接第81页)

发,今后这种防火墙与入侵检测系统互动模型将会有更多、更广泛的应用。

参考文献:

[1] 丁志芳,徐梦春.评说防火墙和入侵检测[J].网络安全技术与应用,2002,4(4):37-41.

[2] 薛立.防火墙和入侵检测系统在企业信息网络中的应用[J].中原工学院学报,2003,14(3):67-69.

[3] 冯洪亮.IDP让防火墙与IDS走向统一[EB/OL].(2003-04-15)[2007-04-20].http://tech.ccidnet.com/art/232/20030415/43670-1.html.

(责任编辑:凌汉恩 邓大玉)