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

2012,28(2):178~180
Vol. 28,No. 2 May 2012

基于Snort传感器的分布式入侵检测系统在校园网络中的实验测试

Test and Analysis of Snort Based Distributed Intrusion Detection System on Campus Network

余思东[1,2],陈 华[1]
YU Si-dong[1,2],CHEN Hua[1]

(1.广西大学计算机与电子信息学院,广西南宁 530004;2.广西农业职业技术学院,广西南宁 530007)
(1. College of Computer Science and Electronic Information, Guangxi University, Nanning, Guangxi, 530004, China; 2. Guangxi Agriculture Vocational and Technical College, Nanning, Guangxi, 530007, China)

摘要:在校园网中部署基于Snort传感器的分布式入侵检测系统,并进行后门木马Bdoor攻击实验测试,以检测系统是否能主动、实时地全面防范一系列的网络攻击。实验测试结果显示,基于Snort的分布式入侵检测系统可以有效检测出校园网络中由于网络攻击带来的安全问题。

关键词:校园网络 入侵检测 Snort
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2012)02-0178-03

Abstract: An intrusion detection system based on Snort is employed and tested in campus network configuration. By constructing simulation experiment environment detection and postern Trojan Bdoor attack experiment, the effectiveness of intrusion detection system is analyzed. The results show that Snort intrusion detection system can effectively detect the security issues from network attack in campus network.

Key words: campus network, intrusion detection, Snort

入侵检测系统(简称IDS)通过计算机网络中的关键点收集信息[1],然后对收集到的信息进行分析,从而判断网络中是否有违反安全策略的行为和被攻击的迹象。分布式入侵检测系统(简称DIDS)一般用于部署大型网络环境下的入侵检测系统,以监视整个网络环境的安全状态。它可以提高单个独立IDS的处理能力,也可以增加IDS数量并使它们协同分工同时进行工作。

Snort是一种以开放源代码形式发布的轻量级网络入侵检测系统,支持多种系统软件和硬件平台(Windows,Linux等)。它采用基于规则的工作方式,通过对数据包内容进行规则匹配来检测多种不同的入侵行为和探测活动。例如缓冲区溢出,隐藏端口扫描、CGI攻击、SMB探测等等[2]。Snort经过若干年的发展,已经成为一个稳定、高效的IDS,是一个基于winpcap或者libpcap的网络数据包捕获器和日志记录工具。Snort可以执行协议分析,内容过滤,规则匹配,也可以用作探测器来检测攻击。

基于Snort平台,可以将分布式入侵检测系统分为数据管理中心、传感器、管理决策中心[3],符合三层架构。(1)传感器主要作用是全面收集被监控的网络的数据,它作为DIDS中最主要的构成部件,一般都分布式部署在要求实施监控的网段上。它把收集好的数据简单处理后,把入侵事件以日志方式记录在数据管理中心。数据管理中心根据日志,利用模式匹配和协议分析两种技术结合的方式进一步检测入侵行为[4]。(2)管理决策中心的作用是负责汇总和分析报警信息,以图形化的方式显示数据报

收稿日期:2012-03-06
修回日期:2012-04-22
作者简介:余思东(1979-),男,讲师,主要从事计算机网络安全研究。

警信息,根据汇总分析的结果修改传感器的配置,使传感器更适应网络的需求。另外,管理决策中心可以根据分析检测的结果做出响应,从而帮助网络管理员做出判断和决策,提高系统的检测效率和准确度。(3)传感器由 Snort 实现。在 Windows 环境下需要事先安装多种软件,构建支持环境才能使用 Snort,需要安装的相关软件有:Snort、winpcap、mysql、ACID(控制分析系统)、adodb、apache、php、jpgragh 等[5]。

校园网络是学校信息化的重要硬件平台,它是我们实现现代化教学与网络化管理的重要保障,在管理水平以及教学质量上都发挥重要作用。随着校园网用户的增多和应用服务的多样化,校园网的安全问题日趋严峻。因为它不但要应对校园网外部的攻击,还要重点防御来自内部网络的占大多数的攻击行为。分布式入侵检测系统对校园网络安全有重要作用[6]。本文在校园网中部署基于 Snort 传感器的分布式入侵检测系统,并进行后门木马 Bdoor 攻击实验测试,以检测系统是否能主动、实时的全面防范一系列的网络攻击。

1 基于 Snort 的分布式入侵检测系统在校园网络的配置方案

本文涉及的校园网络采用光纤技术、结构化布线技术、高速交换网络技术、互联网技术等关键技术。根据校园网络结构拓扑(图 1),为了更全面地收集信息,我们将 Snort 传感器在校园网中分布式的部署位置如下:(1)在防火墙的 DMZ 区放置 Snort 传感器,用于收集来自外网的入侵行为。(2)在校园网内部的核心交换机上部署 Snort 传感器用于收集信息,主要是为了保护网络中的各类业务及教育应用服务器。(3)在教工宿舍和学生宿舍网内安装 Snort 传感器用于收集信息。(4)在校内的办公区域网络中安装 Snort 传感器。

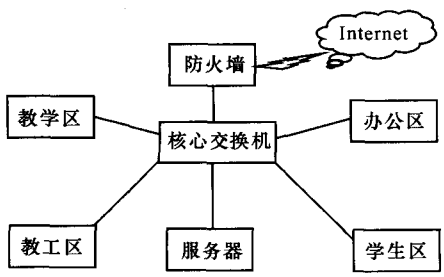

图 1 校园网络结构拓扑

Snort 传感器的作用是捕获网络中的数据包,并对发现的入侵行为进行分析和预处理。为了保护传感器自身的安全,一般会设置两个网络端口,也就是在配置有 Snort 系统的主机上安装两块网卡,一个接口用于捕获被监控网络的数据包,另一个接口用于与上层进行信息传递。进行信息传递的接口需要配置 IP 地址,而用于捕获数据包的接口不需要配置 IP 地址,这样可以使攻击者无法发现它的具体位置,降低其成为攻击对象的可能性。而且为了实现收集网络数据包的目的,需要将网卡设置成为混杂模式,这样才能够捕获网络中传播的数据包。

2 基于 Snort 的分布式入侵检测系统在校园网络的实验测试

2.1 构建模拟实验环境

我们在校园网的办公区域构建模拟实验环境(图 2),在实验环境测试入侵检测系统中模式匹配算法的性能。

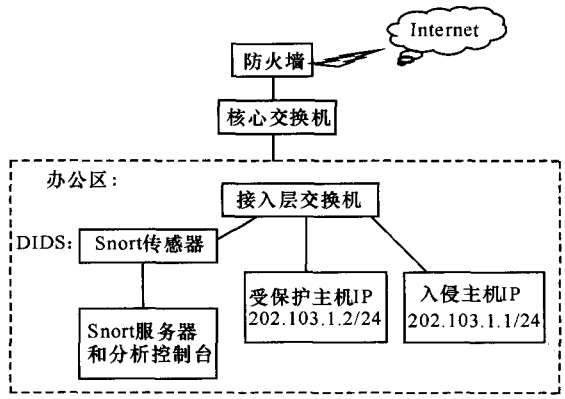

图 2 模拟的办公区网络结构

在模拟实验环境中,我们给主机设置的 IP 地址网络前缀为/24,说明这一网络可以同时有 254 台电脑主机进行网络通信,我们设计的 DIDS 将检测出所有网络地址为 202.103.1.0 这一整个网络的攻击行为。因此在这一网络中使用两台电脑主机(一台作为受保护主机,另一台作为入侵主机)所得出的实验结果完全可以代表整个网络区域的入侵检测效果。

2.2 后门木马 Bdoor 攻击实验

后门木马 Bdoor 是在 Windows 平台下开发的,攻击的操作系统也是 Windows 操作系统。它通过将进程写入 explore 进程从而实现隐藏,篡改注册表实现自动运行。木马入侵成功后,会自动安装并开放"肉鸡"的 5010 端口。入侵者就可以利用 telnet 协议从该商品远程登录,并且拥有复制、查询、修改、删除等权限。

本文编写针对后门木马 Bdoor 入侵攻击的

Snort 规则如下：

alert tcp $HOME_NET 5010 -> $EXTERNEL_NET any (msg:"Discover Bdoor activing"; flow:from_server,established;cont:"dir";no case; classtype:trojan-activity;sid:1111111;rev:1;)

规则设置完成后，我们通过实验验证，从 ACID 的分析控制台上，可能看到测试结果(图 3)。

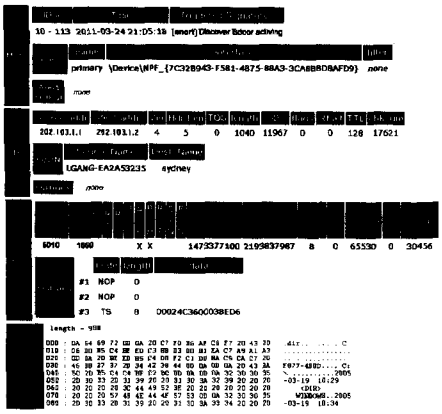

图 3 实验验证结果

由图 3 可以看到，报警信息 Meta 标签上，记录着报警时间、报警内容、发出警报传感器名和对应接口名称。在 IP 报头上，可以知道攻击源地址主机(202.103.1.1)以及被攻击主机(202.103.1.2)，从负载区中可以看到，攻击的特征串为"dir"。

在规则编写完成之后，我们进行 200 次针对后门 Bdoor 木马攻击的检测实验，从检测结果(表 1)可知，该规则可以有效检测后门木马 Bdoor 攻击。

表 1 后门木马 Bdoor 攻击的检测实验结果

测试时间	攻击次数	检测到的次数	检测率(%)
进行规则编写前	10	0	0
进行规则编写后	200	196	98

将实验分析结果扩展到校园网各个区域，即修改 Snort 规则库后使用后门木马 Bdoor 攻击软件，分别对防火墙的 DMZ 区、核心交换机、教工及学生宿舍区和教学办公区进行 20 次实验攻击，发现报警率均为 100%，说明基于 Snort 分布式入侵检测系统的实际应用效果非常明显。

3 结束语

在本文构建的模拟实验环境中，入侵主机使用 Bdoor 木马攻击对受保护主机进行多次攻击检测实验，经过修改和编写 Snort 规则后得出检测结果。根据检测结果可以看出：基于 Snort 分布式入侵检测系统可以有效检测出校园网络中由于网络攻击带来的安全问题。但是，在进行规则编写后对于后门木马 Bdoor 攻击的检测还是存在少量的漏报，还需要不断修改 Snort 规则以及特征库，以提高检测成功率。

参考文献：

[1] 唐正军. 入侵检测技术导论[M]. 北京：机械工业出版社，2004.

[2] 黄刚. 入侵防御系统关键技术研究[J]. 网络安全技术与应用，2008，5：13-14.

[3] 钟嘉鸣. 校园网安全平台的规划与设计[J]. 中国科技信息，2007，2：5-6.

[4] 陈添杰. 分布式 Snort 的研究与应用设计[D]. 广州：广东工业大学，2005.

[5] 李小平，王意洁，王勇军. 入侵防御系统的研究与设计[J]. 微计算机信息，2006，10：45-47.

[6] 黄梅珍. 基于分布式入侵检测系统的校园网络安全解决方案[J]. 计算机与信息技术，2006，08：101-103.

(责任编辑：陈小玲)