基于 Snort 入侵检测系统的设计与实现①

Design and Realization of Snort-Based Intrusion Detection System

王 喆 (天津城市建设管理职业技术学院 天津 300134)

摘 要: 入侵检测技术是一种主动保护网络资源免受黑客攻击的安全技术。介绍了如何在 Windows 平台上以 Snort 为基础，在校园网络环境中搭建一个基于网络的入侵检测系统，帮助网管员及时发现网络入侵行为，有效地保护校园网络安全。

关键词: 入侵检测 Windows Snort 校园网 网络安全

1 引言

随着网络技术的发展，网络环境变得越来越复杂，单纯的防火墙技术暴露出明显的不足和弱点，有些攻击方式可以绕过防火墙，直接侵入到内部网络，使得网络安全受到威胁[1]。入侵检测系统(IDS-Intrusion Detection System)可以弥补防火墙的不足,其任务是用来识别针对计算机系统和网络系统，或者更广泛意义上的信息系统的非法攻击，包括检测外界非法入侵者的恶意攻击或试探及内部合法用户的超越使用权限的非法行动。它采用探测与控制(与其他系统如防火墙)相结合的技术，起着主动防御的作用，为网络安全提供实时的入侵检测及采取相应的防护手段[2]。

2 Snort简介

Snort 是一款轻量级的网络入侵检测系统[3],它能够在IP网络上进行实时流量分析和数据包记录。Snort 不仅能进行协议分析、内容检索、内容匹配，而且能用于侦测缓冲溢出、隐秘端口扫描、CGI 攻击、SMB 探测、操作系统指纹识别等大量的攻击或非法探测。Snort 使用灵活的规则去描述哪些流量应该被收集或被忽略，并且提供一个模块化的探测引擎[4]。该系统可以根据用户自己的需求开发和升级。

Snort 的工作原理是在基于共享网络上检测原始的网络传输数据，通过分析捕捉的数据包，匹配入侵行为的特征或者从网络活动的角度检测异常行为，进而采取入侵的预警和记录。从检测模式而言，Snort 属于误用检测，即对已知攻击的特征模式进行匹配。从本质上来说 Snort 是基于规则的入侵检测工具[5]。该入侵检测系统如果只有 snort 的可执行程序，而没有规则文件，那么 snort 就不能真正实现入侵检测功能，不能识别任何攻击。snort 规则文件就是该系统的核心，是 snort 检测攻击的知识库。

3 基于snort入侵检测系统的部署

我校建立基于网络的入侵检测系统，入侵检测系统的中心服务器作为一个单独的个体接入到核心交换机上。部署网络入侵检测系统的关键是应当保证系统的监听网卡所连接的设备端口能够监听到监控网段的全部网络流量。在共享式网络中是不涉及到这个问题，但在交换式网络中由于交换机的每个端口拥有自己的冲突域，因此无法捕获除广播和组播之外的网络流量，这就要求交换机提供监控端口。由于我校核心交换机没有直接提供监控端口，所以本文利用核心交换机中的 mirroring-group 命令来配置端口镜像组来实现。图 1 为我校入侵检测系统部署图。

4 基于snort入侵检测系统的实现

4.1 MySQL 数据库管理系统

入侵检测系统使用 MySQL 作为数据库主要是为了记录的警告信息的数据，便于今后进行分析，从而

① 收稿时间:2009-02-11

调整入侵检测系统的规则集。

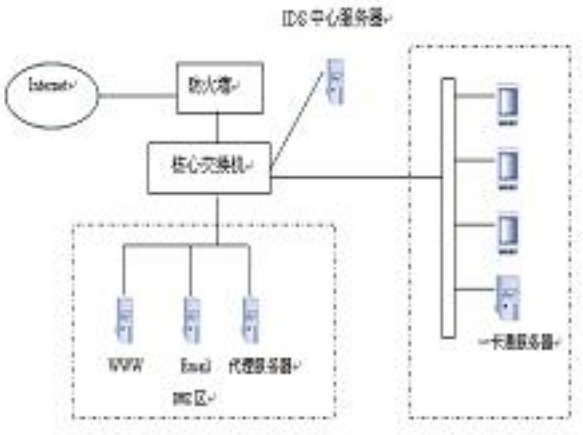

图 1　入侵检测系统部署图

4.2 Apache Web 服务器配置

入侵检测系统使用 Apache 作为 Web 服务器，主要是为了发布入侵检测分析控制台 ACID 。由于该台服务器在安装系统的时候，已经安装了 Windows 2000 Server 系统的组件 IIS Web Server，IIS Web Server 默认监听的端口是 80，该端口会与 Apache Web Server 监听的端口冲突，因此将 Apache 的监听端口配置成其它不常用端口，论文中使用的端口号为 8028。具体方法是修改 c:\Apache2\conf\httpd.conf 文件中 Listen 80 语句为 Listen 8028。配置完成后，在命令提示符下输入：c:\apache2\bin> apache－k install，从而启动 Apache 服务。

4.3 PHP 配置

由于 ACID 是基于 PHP 的开发的，所以要在 Apache Web Server 运行 ACID，就必须配置 Apache Web Server 对 PHP 的支持。同时，配置 PHP 对 MySQL 的支持。

入侵检测系统使用 PHP 5.0 版本，解压 php-5.1.1- Win32.zip 文件到 c:\php5 ，将 c:\php5\php5ts.dll 文件拷贝到 c:\WINNT\system32 下。然后将 c:\php5\php.ini-dist 文件拷贝到 c:\WINNT 下，并修改该文件名为 php.ini。同时，修改 php.ini 文件中的内容，将文件中“;extension=php_mysql.dll”语句中的“;”去掉即可。然后拷贝 c:\php5\extension\php_mysql.dll 文件至 c:\WINNT，此时，从而完成 PHP 对 MySQL 支持的配置。

配置 Apache Web Server 对 PHP 的支持，需要修改 C:\Apache2\conf\httpd.conf 文件，在该文件的最后加入以下内容：

PHPIniDir "C:\php5"

LoadModule php5_module "c:\php5\php5apache2.dll"

AddType application/x-httpd-php.php

然后重新启动 Apache 服务，完成 Apache Web Server 对 PHP 支持的配置。

4.4 Winpcap 配置

Winpcap(Windows Packet capture)是 UNIX 下的 Libpcap 移植到 Windows 下的产物，是 Windows 平台下一个免费、公共的网络访问系统。入侵检测系统使用 Winpcap 主要是用来进行网络数据包截取的驱动程序。

4.5 ADODB 库和 jpgrapg 库配置

ADODB(Active Data Objects Data Base)库是为 PHP 提供数据库接口，便于 ACID 访问 MySQL 数据库。入侵检测系统构建过程中解压 adodb465.tar 文件到 c:\Apache2\ htdocs\adodb 目录下，完成 ADODB 库的安装。

jpgrapg 库是 PHP 下面的图形库。入侵检测系统构建过程中解压 jpgraph-2.0.tar.tar 文件到 c:\Apache2\ htdocs\ jpgraph 目录下，同时修改 c:\Apache2\ htdocs\ jpgraph\scr 目录下的 jpgraph.php 文件中 DEFINE("CACHE_DIR","")语句为 DEFINE("CACHE_DIR", "/ tmp/jpgraph_cache/")，完成 jpgrapg 库的配置。

4.6 Snort 配置

在 snort 的配置过程中，首先在 MySQL 建立 snort 必须使用的 snort 库和 snort 用户，并且为 snort 用户设置密码和分配相关权限，具体实现的命令如下：

mysql>create database snort;

mysql>grant usage on *.* to "snort"@"localhost" identified by "snort";

mysql>grant select,insert,update, delete, create,alter on snort .* to "snort"@"localhost";

mysql> set password for "snort"@"localhost"= password ('111111');

4.6.1 建立 snort 运行必须的数据表

将 C:\snort\contrib 下的 create_mysql 文件拷

贝到 c:\Program Files\MySQL\MySQL Server 4.1\bin 目录下，运行命令：

mysql>source create_mysql;

完成在 snort 数据库下建立 snort 运行必须的数据表。此时在 snort 数据库下一共建立了 16 个数据表，这些数据表包括：data 表、detail 表、encoding 表、event 表、icmphdr 表、iphdr 表、opt 表、reference 表、reference_system 表、schema 表、sensor 表、sig_class 表、sig_reference 表、signature 表、tcphdr 表、udphdr 表。

4.6.2 配置 snort.conf 文件

配置 c:\snort\etc\snort.conf 文件，首先修改“include classification.config” 语句为“include:c:\snort\etc\classification.config”,“includere ference.config” 语句修改为“include c:\snort\etc\reference.config”，完成 classification.config 文件和 reference.config 绝对路径的配置。

同时为 snort 定制规则集，修改“var RULE_PATH ../rules” 语句为“var RULE_PATH c:/snort/rules”，为 snort 定制规则的绝对路径。目前在 snor 下一共包含了 48 个规则文件。

4.6.3 配置 snort.conf 文件

通过语句“output database: alert, Mysql, host=localhost port=3306 dbname=snort user=root password=wangjiji1225 sensor_name=n encoding=ascii detail=Full” 完成该设置。

4.7 配置入侵检测分析控制台 ACID

入侵检测分析控制台(Analysis Console Intrusion Detection—ACID)是一个基于 PHP 技术的分析引擎，用于搜索和处理由各种 IDS、Firewall、网络监视工具生成的存储在数据库中的安全事件。ACID 可以搜索和处理基于 Snort 开放源码的 IDS 生成的存储在 MySQL 数据库中安全事件[6]。修改 acid_conf.php 文件，进行 acid 的配置，具体配置内容如下：

```
$DBlib_path="c:\Apache2\ htdocs\adodb";
$alert_dbname="snort";
$alert_host="localhost";
$alert_port="3306";
$alert_user="snort";
$alert_password="111111";
/* Archive DB connection parameters */
$archive_dbname="snort ";
$archive_host="localhost";
$archive_port="3306";
$archive_user="snort";
$archive_password="111111";
$ChartLib_path"c:\apache2\htdocs\jpgrap h\src";
```

同时，把 c:\Apache2\htdocs\acid 目录下的 create_acid_tbls_mysql.txt 的内容拷到 create_mysql 文件中，再一次运行命令“mysql>source create_mysql;”，从而向 MYSQL 的 snort 数据库中增加了 ACID 所用到的 4 个表：acid_ag、aicd_ag_alert、acid_event 和 acid_ip_cache。

5 入侵检测系统控制台的测试

5.1 入侵检测系统控制台的运行

在 IDS 的中心服务器的浏览器中输入地址：http://localhost:8028/acid 就可以看到入侵检测系统控制台的运行情况，如图 2 所示为入侵检测系统控制台主页面。

图 2　入侵检测系统控制台

该界面里显示的信息包括：触发安全规则的网络流量中各种协议所占的比例、警报的数量、入侵主机和目标主机的 IP 地址及端口号等。同时该控制台还提供强大的搜索功能，用户可根据时间、IP 地址、端口号、协议类型以及数据净荷等多种条件的灵活组合在入侵事件数据库中进行查询。另外应用该控制台提供的制图功能可以直观地对网络入侵事件进行分析，而

(下转第 195 页)

(上接第 103 页)

生成的图表可以进一步丰富网管人员编制的报告。

5.2 入侵检测系统控制台的测试

为了测试入侵检测系统的入侵检测效果，论文对公共服务器子网的入侵检测系统进行了测试。由于公共服务器子网处于防火墙的 DMZ 区域，该区域存在允许被内部网络和外部网络同时访问的应用服务器，该区域可能同时面临内部网络和外部网络攻击，所以该区域能够比较好的反映出入侵的检测效果。

由于攻击者要确定攻击的目标，或者确定要攻击的目标系统是否存在可攻击的漏洞或服务端口等信息，最好的方法就是通过扫描。为了检测入侵检测系统的效果，本文利用 X-Scan v3.2 GUI 扫描软件对目标主机进行了扫描测试，得到了目标主机的系统信息和漏洞，同时发现入侵检测系统能够比较好的完成对大部分扫描攻击的检测。表 1 为入侵测试的结果。

表 1　入侵检测结果

扫描次数	检测到的攻击次数	成功率	漏报率
2662 次	2633 次	98.91%	1.09%

6　总结

在校园网络环境下搭建的基于 snort 的入侵检测系统，有效的弥补了防火墙被动防御的不足，对系统或网络资源进行实时检测，及时发现闯入系统或网络的入侵者，对网络起到了主动防御的作用。

参考文献

1 Ptacek TH, Newsham T. Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection, Secure Networks Inc., 1998:47－52.

2 马力,焦李成,卢涛,等.一种基于代理的分布式入侵检测系统结构设计,通信和计算机, 2005,2(6):55－58.

3 http://hx007.blogdriver.com/hx007/index.html

4 http://www.cnpaf.net/Class/hack/200610/16001.html

5 郭宏刚.入侵检测系统在校园网中的应用研究[硕士学位论文].武汉:华中科技大学, 2005.

6 方贤进.校园网环境下入侵检测系统的研究与实现[硕士学位论文].合肥:安徽大学, 2005.