基于Snort检测端口扫描攻击规则的探讨

丁佳
（山东维平信息安全测评技术有限公司 山东济南 250101）

摘 要：Snort是一个轻量级的开源网络入侵检测系统，其作为入侵检测工具在入侵防范方面得到了广泛的应用。针对当前服务器容易受到不被日志机制、监测系统和入侵检测系统捕捉的隐蔽端口扫描攻击，文章基于Snort入侵检测系统，分析了端口扫描的基本特征，进行自定义Snort规则，以达到对隐蔽端口扫描攻击的检测和报警效果，更加促进应用层实现安全过滤。

关键词：Snort入侵检测；端口扫描；入侵防范
中图分类号： D918 **文献标识码：**A

Discussion on the rules of snort detection port scan attack

Ding Jia
(*Shandong Weiping Information Security Evaluation Technology Co., Ltd., Shandong Jinan 250101*)

Abstract: Snort is a lightweight open source network intrusion detection system, which is widely used as an intrusion detection tool in intrusion prevention. In view of the fact that the current server is vulnerable to hidden port scanning attacks that are not captured by the log mechanism, monitoring system and intrusion detection system, this paper analyzes the basic characteristics of port scanning based on Snort Intrusion detection system, carries out custom snort rules, achieves the detection and alarm effect of hidden port scanning attacks, and promotes the application layer to achieve security filtering.

Key words: snort intrusion detection; port scanning; intrusion prevention

1 引言

端口扫描是一种收集信息型的网络攻击，以向目的主机TCP/IP服务端口发送探测数据包的方式进行初步测试，再通过分析目的主机响应的数据包获取服务端口状态、服务器版本、用户漏洞等重要信息，并可通过端口扫描捕获目的主机流出的IP数据包监视其运行情况。端口扫描技术作为恶意攻击的前奏，当这些重要信息泄露，将会严重威胁用户的网络，并且随着端口扫描技术的发展，端口扫描越来越隐蔽，难以发现，再加上检测过滤产品由于应用环境的复杂性，客观上常难以满足实际应用环境的需要。因此，针对服务器环境的需要来配置对端口扫描的检测和防护是有必要的，通常可基于经典入侵检测工具Snort，结合针对性的规则实现。

Snort入侵检测功能是基于它的规则库，规则库中通过一种简单的规则描述语言，记录网络攻击表现的一些特征。根据鉴别的数据包是否匹配规则描述的特征判断是否是攻击行为，结合基于Snort检测机制，达到检测防范效果。

2 端口扫描特征分析及演示

2.1 特征分析

互联网上大多数应用是基于TCP/IP协议，故对端口扫描的特征分析需基于TCP/IP协议，从分

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

析TCP连接“三次握手”“四次挥手”以及相关数据包为出发点，了解端口扫描基本特征。

TCP连接只存在请求和响应，请求和响应都是对应的数据报文。报文包含一些重要字段用于表示连接状态，有SYN、ACK、FIN、RST、URG、PSH。SYN用于初始化连接；ACK可以确认收到的数据；FIN作为断开连接标志；RST用于重新建立连接；URG指示数据时紧急数据，应立即处理；PSH用于强制将数据压入缓冲区[1]。故“三次握手”就是在客户端和服务端之间三次TCP报文交换的过程，如图1所示；“四次挥手”就是结合客户端和服务端双方的状态来阐明链接释放的过程，如图2所示。

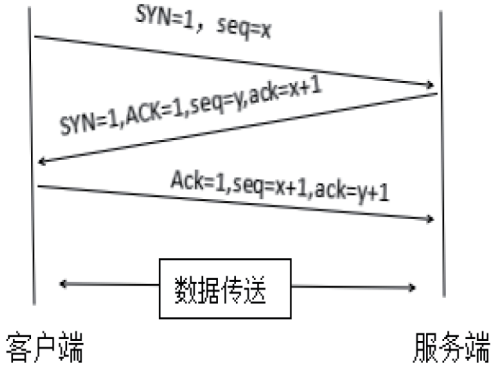

图1 三次握手

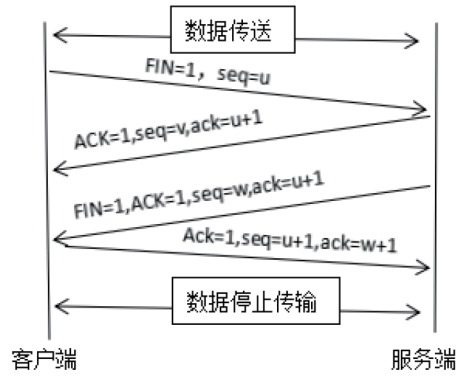

图2 四次挥手

基于以上信息，对以下端口扫描方式进行特征分析有几点。

（1）TCP content()扫描。此扫描尝试与每一个TCP端口进行“三次握手”通信（SYN、SYN/ACK和ACK），会产生大量的连接请求以及错误信息。若能够成功建立连接，表明端口开放，反之端口关闭。

（2）TCP SYN 扫描。此扫描不需要建立一个完全的TCP连接但需要Root权限，是一个半开放的扫描。其通过扫描器发送一个SYN包，当目标主机端口返回一个SYN/ACK信息时，表明该端口处于侦听状态，若返回一个PRST则反之。当收到一个SYN/ACK，扫描器需返回一个RST关闭该连接，一般情况下可避免在目标主机上留下扫描痕迹[2]。

（3）TCP FIN扫描。此扫描方式不依赖“三次握手”的过程，而是利用TCP连接“FIN”结束标志位。主机端口关闭时会用适当的RST回复FIN数据包，而开放的端口则会对这种可疑的数据报不加理睬并将其丢弃，此扫描是基于该思想来进行，该类扫描相关报文常包含大量的“FIN”结束位标志。该方式可用于通过被一些防火墙和包过滤器进行监视的指定端口。

（4）Xmas-Tree扫描。正常情况下，TCP数据包中的ACK、FIN、RST、SYN、URG、PSH标志位并不能被同时设置。该扫描便是向目标端口发送一个含有FIN（结束）、URG（紧急）和PUSH（弹出）标志的分组，对于关闭的端口，目标系统会返回RST标志，而在目标端口开放的情况下，目标主机将不返回任何信息，利用该特征从而判断端口开放情况。

（5）TCP空扫描。该扫描方式与Xmas-Tree扫描原理相同，但发送的数据包不同，该扫描向目标端口发送一个不包含任何标志位的分组，目标端口关闭的端口应该会返回RST标志位。

（6）IP段扫描。此扫描并不是直接发送TCP数据包，而是通过将数据包拆分成两个较小的IP段，把一个TCP头分成几个数据包，从而绕过滤器探测。

（7）TCP反向ident扫描。该扫描是应用第三方计算机向目标主机发送SYN包，并使第三方主机对目标主机返回的SYN|ACK回应RST，对RST不做回应。而利用第三方计算机进行扫描时，本地计算机进行的是对第三方计算机连续Ping的操作，通过查看第三方计算机机返回的Echo响应的ID字段，确定目标主机上端口开放或是关闭状态。

2.2 使用Nmap工具进行端口扫描

Nmap是一种常用于网络发现和审计的扫描

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

器，它可用于发现网络上的主机，可进行端口扫描、应用和版本侦测、OS检测以及与脚本进行脚本交互，是一种能够枚举和测试网络的工具，下列是Nmap一些常用扫描命令参数。

（1）-sT：TCP connect()扫描。

（2）-sS：TCP SYN扫描。

（3）-sF：TCP FIN扫描。

（4）-sX：Xmas-Tree扫描。

（5）-p：指定端口号扫描。

（6）-v：显示扫描过程。

（7）-F：快读扫描。

（8）-Pn：在目标主机禁止Ping连接情况下，能够绕过主机发现的过程进行端口扫描。

（9）-A：包括探测操作系统及版本，扫描脚本以及进行路径跟踪等全面扫描系统的扫描方式。

在安全测评工作当中，Nmap是常用的端口扫描工具之一，利用Nmap探测检测主机或Web服务器上开放多余的端口，在该类端口还未造成影响时进行及时弥补。Nmap扫描应用有两部分演示。

（1）检测TCP端口，如图3所示。由图结果可知端口80、3306、3389开放，端口23关闭以及检测出端口所对应的服务。

（2）对目标主机（39.96.38.215）进行Xmas-Tree扫描，命令指令为Nmap -sX 39.96.38.215,利用Wrieshark抓取目标主机的网络数据包，如图4所示。分析发现数据包的TCP标志位包含FIN、PSH、URG，符合Xmas-Tree扫描的主要特征。

3 检测端口扫描Snort规则拟定

在进行规则拟定之前，先对规则结构进行基本说明。Snort每条规则在逻辑上分为两部分：规则头和规则选项[3]。规则头包括四个部分：规则动作、协议、源信息、目的信息。规则动作有五种，分别为Alert〔生成告警、记录（Log）包〕、Log（记录包）、Pass（丢弃包）、Activate（Alert并且激活另一条Dynamic规则）、Dynamic（先保持空闲后作为规则执行）。协议有四种，为TCP、UDP、ICMP和IP[3]。源信息和目的信息包括IP地址端口等。规则选项组成了规则的核心，包含报警信息以及规则触发时提供给管理员的参考信息。具体作用是在规则头信息的基础上进一步分析，确定复杂的攻击。Snort规则选项用分号“；”隔开，规则选项关键字和其参数用冒号“：”分开，由于规则选项及其参数数量过多，这里便不做详细叙述。Snort规则结构大体如图5描述所示。

基于以上规则结构，结合前章端口扫描特征分析，规则拟定如下：

alert tcp ![39.96.38.215/32] any ->39.96.38.215/32 any

//规则头，匹配除主机外任意(any)源IP和端口到主机和和其任意端口的TCP数据包发送告警消息，检测非主机的IP地址发送的tcp协议包

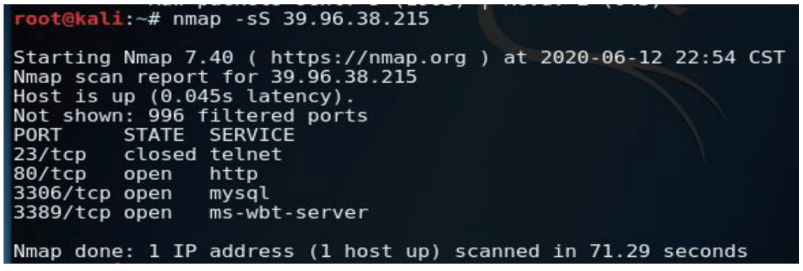

图3 TCP SYN扫描

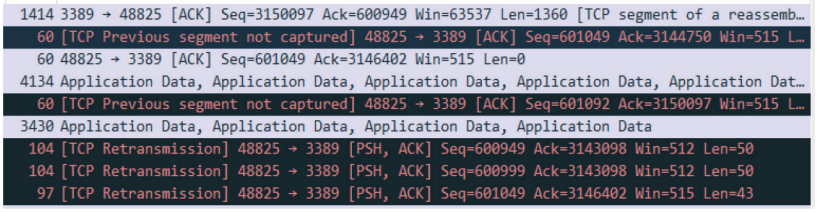

图4 Xmas-Tree扫描

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

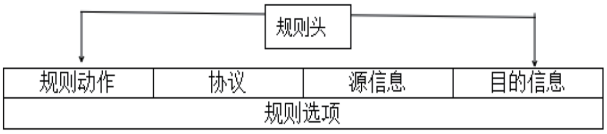

图5 Snort规则结构

(//规则选项

msg:”PortScan”;//在报警和包日志中打印的消息内容

flow:to_server,established;//检测向服务器发送方向的报文

dsize:<300;//应用层负载包长度小于300

flags:FPU;//TCP flags值

content:"|03|"; nocase; offset:4; depth:1;

//nocase指定对content字符串不区分大小写，offest设定开始搜索位置为4，depth设定搜索的最大深度为1，即负载偏移4取1的值为03

content:"select|20|geometryn|28|0x0000000000700000001";distance:10;

within:50;

//相对于上面的03特征向后偏移10个字节之后再取50个字节

//50个字节里边包含select|20|geometryn|28|0x00000000000700000001

sid:1000001;//规则编号，用户自行编写规则的编号在1000000以上

rev:1;)//版本信息。

通过该条规则，能够将除了本地主机IP之外的任意源IP的任意端口发向本主机端口的TCP数据包按照要求进行检测，若检测到端口扫描，则会报警记录到日志文件中。

4 实验与结果分析

4.1实验环境

Window Server；Linux虚拟机；WinPcap 4.1.3；Snort 2.9.11.1。

4.2 实验步骤

（1）绝对路径配置。将编写完成的规则保存至Snort的Rules路径下local.rules文件中并将Snort.conf中的相关相对路径改成绝对路径，在Snort运行时才会加载自定义的规则文件。

（2）运行Snort，命令：snort -A full -c "C:\Snort\etc\snort.conf" -l "C:\Snort\log" -A full 为默认的报警机制，snort.conf是规则集文件，当检测的数据包和规则集中某一规则成功匹配，Snort采取相应行动并记录至指定输出目录（C:\Snort\log）中。

（3）通过Nmap工具进行Xmas-Tree扫描。

（4）查看报警信息：

[**][1:1000001:0]PortScan [* *]

[Classification: Detectionof aNetwork Scan] [Priority: 0]

06/19-19:24:57.564404 192.168.197.129:3389->39.96.38.250:7599

TCP TTL:128 TOS:0x0 ID:55250 IpLen:20 DgmLen:1692 DF

[**][1:1000001:0]PortScan [* *]

[Classification: Detection of a Network Scan] [Priority: 0]

06/19-19:25:00.564449 192.168.197.129:3389-> 39.96.38.250:7599

TCP TTL:128 TOS:0x0 ID:55250 IpLen:20 DgmLen:1692 DF。

4.3 结果分析

实验表明，当主机受到Xmas-Tree扫描时，运行Snort的主机能够捕获网络上的数据包，在进行预处理之后，将包被送到检测引擎，检测引擎通过规则文件（即local.rules）中的规则选项来对每个包的特征和包信息进行单一、简单的检测。由报警信息可知，基于编写规则选项下，Snort能够成功检测出关于端口扫描的数据包，并能够详细地记录攻击源IP（192.168.197.129）、攻击类型（PortScan）、攻击目标（39.92.38.250）、攻击时间（6/19），实现防范端口扫描攻击。

4.4 实验总结

基于规则的检测操作简单且工作可靠，其工作过程精确，易调整配置及优化，减少误报率。

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

根据实际应用的需要进行规则编写，能够有针对性地提出防范措施。

实验中的主机基于防范端口扫描攻击的需要，对端口扫描原理及常用技术进行解析，以Xmas-Tree隐蔽端口扫描技术为攻击实例，提取其报文中FIN、PSH、URG标志位的特征，编写规则选项中的内容，结合Snort的灵活性，完成相应的端口扫描攻击防范。

5 结束语

依新发布的网络安全等级保护2.0标准，国家针对网络边界及计算环境提出入侵防范要求，能够对入侵行为进行检测并提供报警是主要要求之一。而Snort作为一个入侵检测工具，通过添加有效检测入侵行为的规则，能够成为防火墙的重要补充及构建安全区域边界和安全计算环境的组成部分。因此，针对作为入侵攻击前奏的端口扫描攻击来探讨Snort的规则，对实现入侵防范具有一定的促进作用。

本文以TCP/IP协议为基础，详细说明端口扫描行为特征以及常用的端口探测技术，通过Nmap工具讲述端口扫描实现方式，从而拟定相应的检测规则，从实际操作方面，探讨自定义Snort规则实现防在范端口扫描及在入侵防范方面的促进作用。Snort规则是Snort入侵检测系统检测入侵行为的知识库，在计算机网络不断受到网络攻击威胁和破坏的情况下，必须及时添加新的规则，提高Snort的检测能力。

本文的Snort规则基于端口扫描攻击行为特征进行编写，而网络攻击不仅包括端口扫描攻击，还包含SQL注入、XSS、拒绝服务等多种攻击方式，需要对攻击方式进行深入研究，根据应用环境要求，举一反三，编写出能够完成入侵防范效果的规则。

参考文献

[1] James F. Kurose,Keith W. Ross ,陈鸣译.计算机网络（第4版）[M].北京：机械工业出版社,2009.

[2] 王国栋.端口扫描技术的研究与实现[J].软件（教育现代化）,2013.

[3] Snort中文手册[Z].https://www.docin.com/p-981478311.html

[4] 赵艳华.基于Snort的检测方法研究与分析[D].衡阳:南华大学,2017.

作者简介：

丁佳（1984-），男，汉族，山东烟台人，北京化工大学，本科，山东维平信息安全测评技术有限公司，工程师；主要研究方向和关注领域：网络安全、等保测评、风险评估。

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net