DOI:10.16208/j.issn1000-7024.2002.09.005

第23卷 第9期 计算机工程与设计 2002年9月
Vol.23 No.9 COMPUTER ENGINEERING AND DESIGN Sep. 2002

文章编号:1000-7024(2002)09-0015-03 中图分类号:TP393.07 文献标识码:A

网络端口扫描及其防御技术研究

唐小明[1], 梁锦华[2], 蒋建春[3], 文伟平[3]

(1. 广西地方税务局计算机信息管理中心, 南宁 530022; 2. 中国科技大学研究生院, 北京 100039;
3. 中国科学院信息安全技术工程研究中心, 北京 100080)

摘 要: 对当前的端口扫描及其防御技术进行了综述和归类分析, 详细地讨论了各种技术的优缺点, 并讨论了端口扫描技术的研究方向。

关键词: 端口扫描; 端口扫描检测

Research about technology of port scan and port scan detect

TANG Xiao-ming[1], LIANG Jin-hua[2], JIANG Jian-chun[3], WEN Wei-ping[3]

(1. Computer Information Management Center, Guangxi Local Tax Bureau, Nanning 530022, China; 2. Graduate School of the Chinese Academy of Sciences, Beijing 100039, China; 3. Engineering Research Center for Information Security Technology, Beijing 100080, China)

Abstract: This paper gives a summary and classification of the existing intrusion detection models and technologies, and their merits or shortcomings have been compared in detail. It also gives out the development for the future.

Key words: port scan; port scan detect

1 引 言

端口扫描是一种非常重要的预攻击探测手段,几乎是黑客攻击的必经之途。通过端口扫描,可以知道目标主机上开放了哪些端口,运行了哪些服务,这些都是入侵系统的可能途径。对端口扫描技术进行研究,可以在攻击前得到一些警告和预报,尽可能在早期预测攻击者的行为并获得一定的证据,从而对攻击进行预警。

2 端口扫描原理

一个端口就是一个潜在的通信通道,也就是一个入侵通道。端口扫描通过选用远程 TCP/IP 不同的端口的服务,并记录目标给予的回答。通过这种方法,可以搜集到很多关于目标主机的各种有用的信息,如发现一个主机或网络和正运行在这台主机上的服务,通过测试这些服务,发现漏洞。扫描器并不是一个直接的攻击网络漏洞的程序,它仅仅能帮助我们发现目标主机的某些内在的弱点。一个好的扫描器能对它得到的数据进行分析,帮助我们查找目标主机的漏洞,但它不会提供进入一个系统的详细步骤。

3 端口扫描技术分类

3.1 开放扫描

完全连接扫描利用 TCP/IP 协议的次握手连接机

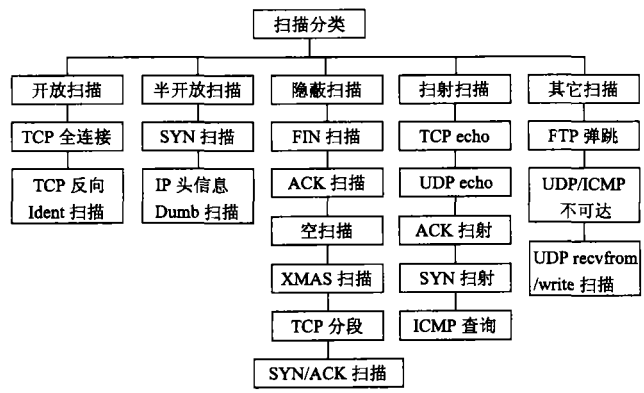

图 1 端口扫描分类

收稿日期: 2002-04-16

作者简介: 唐小明 (1970-), 男, 工程师, 研究方向为网络管理与信息安全。 梁锦华 (1973-), 男, 硕士研究生, 研究方向为计算机网络安全。

制，让源主机和目的主机的某个端口建立一次完整的连接。如果建立成功，则表明该端口开放。否则，表明该端口关闭。

技术实现的示意如下：

Client ——> SYN

Server ——> SYN/ACK

Client ——> ACK

表明客户端向目标主机发出连接请求后，目标主机回答ACK信息，表示可以提供连接。这说明，目标主机的该端口处于监听(LISTENING)状态。

如果目标主机返回RST信息，如下所示：

Client ——> SYN

Server ——> RST | ACK

Client ——> RST

表明原主机向目标主机的某个端口发出连接请求后，目标主机返回RESET信息，则表明此端口不处于监听状态。

3.2 半连接扫描

半连接扫描是指在源主机和目的主机的3次握手连接过程中，只完成前两次握手，而不是建立1次完整的连接。

3.2.1 SYN扫描

首先向目标主机发送连接请求，当目标主机返回响应后，立即切断连接过程，并查看响应情况。

Client ——> SYN

Server ——> SYN/ACK

当收到Server的ACK反馈后，立即切断连接，因为目标主机返回ACK信息，表示目标主机的该端口开放。

如果出现以下情况：

Client ——> SYN

Server ——> RST | ACK

因为目标主机返回RESET信息，表明该端口没有开放。

3.2.2 ID头信息扫描

这种扫描方法需要找一台第3方机器配合扫描，并且这台机器的网络通信量要非常少，即”dumb”主机。

首先由源主机A向”dumb”主机B发出连续的ping数据包，并且查看主机B返回的数据包的ID头信息。一般而言，每个顺序数据包的ID头的值会顺序增加1。然后由源主机A假冒主机B的地址向目的主机C的任意端口(1－65535)发送SYN数据包。这时，主机C向主机B发送的数据包有两种可能的结果：

(1)SYN|ACK

表示该端口处于监听状态。

(2)RST|ACK

表示该端口处于非监听状态。

那么，后续的PING数据包的响应信息的ID头信息可以看出如果主机C的某个端口是开放的，则主机B会返回A的数据包中，ID头的值不是递增1，而是大于1。如果主机C的某个端口是非开放的，则主机B会返回A的数据包中，ID头的值递增1，非常规律。

3.3 隐蔽扫描

隐蔽扫描是指能够成功的绕过IDS、防火墙和监视系统的阻挠，成功取得目标主机的端口信息的一种扫描方式。

3.3.1 SYN|ACK扫描

这种扫描方法时：由源主机向目标主机的某个端口直接发送SYN|ACK数据包，而不是先发送SYN数据包。由于这种方法不发送SYN数据包，目标主机会认为这是一次错误的连接，从而会报错。

如果目标主机的该端口没有开放，则会返回RST信息，如下所示：

client -> SYN|ACK

server -> RST

如果目标主机的该端口处于开放状态（LISTENING)，则不会返回任何信息，而直接将这个数据包抛弃掉，如下所示：

client -> SYN|ACK

server -> -

通过这种反馈信息的区别，可以成功地分辨出端口的开放情况。

3.3.2 FIN扫描

源主机A向目标主机B发送FIN数据包，然后查看反馈信息。如果端口返回RESET信息，则说明该端口关闭，如下所示：

client -> FIN

server -> RST

如果端口没有返回任何信息，则说明该端口开放，如下所示：

client -> FIN

server -> -

3.3.3 ACK扫描

这种方法首先由主机A向目标主机B发送FIN数据包，然后查看反馈数据包的TTL值和WIN值。开放端口所返回数据包的TTL值一般小于64，而关闭端口的返回值一般大于64。

开放端口所返回数据包的WIN值一般大于0，而关闭端口的返回值一般等于0。

3.3.4 NULL扫描

NULL扫描是指将源主机发送的数据包中的ACK、FIN、RST、SYN、URG、PSH等标志位全部置空。如果目标主机没有返回任何信息，则表明该端口是开放的。如果返回RST信息，则端口是关闭的。

3.3.5 XMAS扫描

XMAS扫描的原理和NULL扫描相同，只是将要发送的数据包中的ACK、FIN、RST、SYN、URG、PSH等头标志位全部置成1。如果目标主机没有返回任何信息，则表明该端口是开放的。如果返回RST信息，则端口是关闭的。

4 逃避检测的几种方法

4.1 改变检测的次序

将要扫描的IP地址和端口的次序打乱，可以躲避或降低检测的效率。

4.2 降低扫描速度

降低扫描速度能使当前大部分扫描检测系统不产生报警，即使对一些能够检测慢速扫描的系统来说，要分析相当长时间的网络连接，并要在更多的正常连接中找出扫描行为，增加了检测的难度。

4.3 扫描间隔随机化

确定的扫描时间间隔使得检测器能够比较高效地工作，随机化间隔能使之降低检测效率。

4.4 随机化不太重要的字段

扫描数据包中的序列号、ack号、IP序号、源端口号经常是一些较固定的值，很容易通过一些简单的运算产生，改变这些固有的数值会增加检测的难度。

4.5 假冒源地址

源地址是一个比较难以改变的部分，因为扫描者需要接收对方的反馈以确定端口是否开放。如果能够监视一个靠近目标的网络（如目标网络的ISP），就可以假冒一个源地址发送扫描的包，再从被监视的网络中获取回应的包。

4.6 分布式扫描

从许多不同位置的真实主机发起扫描，扫描的痕迹也被分散到不同的主机上，这使扫描检测变得更加复杂。大量的可发起拒绝服务攻击的代理可被用来实现分布式扫描。

5 当前端口扫描防御分析

5.1 NSM （The Network Security Monitor）

网络安全监测器，第一个网络入侵检测系统(NIDS),可以侦测任意IP地址和其它地址的连接。

5.2 GrIDS （The Graph Based Intrusion Detectiong System)

基于图形的入侵检测系统，通过建立节点之间的连接图表来代表网络中的主机的连接，这样来自同一个地址的扫描就被发现了。可以用很大的比例来进行图表查看，能发现随机性较强的扫描，但不能处理不正常和随机的数据包，所以不能检测秘密扫描。另外，其原型实现使用了Perl，相对较慢，不能适应现在的大型快速网络。

5.3 Snort预处理程序

原则：寻找在一定时间内从某一点发出的一定数量的TCP和UDP包。满足设定条件，则报告发生扫描。缺点是不能侦测分布式扫描、慢速扫描，不能处理分片。

5.4 Emerald

使用行为规则匹配和流量监控来发现扫描，缺点是不能侦测慢速扫描、分布式扫描和新的IP地址。

5.5 SPICE (Stealthy Probing and Intrusion Correlation Engine)

提出了一个分布式的端口扫描检测模型，理论上可以检测慢速扫描、分布式扫描等较为全面的功能。如果成功的话，这项技术不但可以侦测端口扫描，也可以检测拒绝服务攻击和蠕虫。

6 结束语

本文就端口扫描的原理、一些逃避检测的方法进行了阐述，对当前的扫描检测技术进行了分析，到目前为止还没有一个成熟、高效的端口检测技术。端口扫描检测面临着比较多的难题，对端口扫描的检测、过滤、诱骗、追踪等技术都有待进一步的研究和实现。

参 考 文 献：

[1] Fyodor. The Art of Scanning [EB/OL]. Phrack 51 www.phrack. com

[2] CERT Advisory CA-96.21: TCP SYN Flooding and IP Spoofing Attacks. 24 September 1996.

[3] Phrack .Port Scanning without the SYN flag / Uriel Maimon. Phrack 49-15.

[4] Stuart Staniford, Jams A. Hoagland ,et al. Practical Automated.