识别操作系统的方法、原理及其防范技术*

张焕明[1], 宋振锋[2]
(1. 暨南大学网络中心, 广东 广州 510632;
2. 中国农业银行广东省分行, 广东 广州 511430)

摘 要: 分析和探讨了识别远程操作系统类型的方法和原理, 重点介绍了高效识别操作系统的协议特征信号技术, 并探讨了如何防范操作系统被识别的手段。

关键词: 识别技术; 信息反馈技术; 协议特征信号
中图分类号: TP393.08 文献标识码: A 文章编号: 0529-6579 (2002) S1-0049-04

1 问题的提出

分析众多网络攻击事件, 黑客大多先要识别被攻击操作系统的类型, 进而尝试利用该操作系统某种服务漏洞进行攻击。例如, 攻击者通过某种技术探知远程网关 CISCO 的 IOS 版本号, 就能很快的利用该版本 IOS 的漏洞并实施攻击; 如果攻击者通过某些方法得知目标主机使用的操作系统是 win2000 server, 并开放了远程终端访问服务, 进而就有可能通过“输入法漏洞”获取超级管理员权限。如果攻击者无法准确地探知目标主机的类型, 就无从下手, 因此从黑客的角度来说, 能否准确识别目标系统的类型对于入侵的成功与否是至关重要的。

作为在 internet/intranet 上的重要主机和设备, 如何防止或伪装操作系统的类型, 对于减少网络攻击次数, 增加黑客攻击难度是很重要的。

2 识别操作系统的方法

识别操作系统技术按照识别技术的本质划分, 主要包括信息反馈技术和协议特征信号技术两大类。

信息反馈技术包括旗标攫取技巧、特殊端口识别方法。该技术是检测操作系统以及所运行服务的相关版本号的简易可行的方法。

旗标攫取主要是通过 telnet、ftp、pop 等服务返回的信息来识别远程系统类型的一种技巧。当访问远程服务时, 不同的系统、不同的服务返回的信息是不同的。比如使用 ftp 访问远程系统, 通过判断返回信息的差异就可以很方便地识别出远程操作系统的类型。

特殊端口识别方法是指利用某些系统在默认安装时开放特殊端口的这一特性来识别远程操作系统的一种技巧。比如 tcp 端口 3389 (远程终端访问服务) 是 win2000 server 所特有的开放端口, 如果通过扫描发现远程系统打开该端口, 那么可以断定该系统运行的是 win 2000 server; 又如通过扫描知道远程系统只打开了 TCP 23 端口 (telnet 服务), 那么该系统极有可能是一台路由器。

协议特征信号技术是利用不同的操作系统在实现 TCP/IP 协议时的细微差别, 来识别操作系统类型的一种技术。协议特征信号技术高效强大, 将在下面分析。

有些人把协议特征信号技术进一步划分为主动特征探测和被动特征探测, 主动特征探测是指有针对性的向系统发一些精心构造的包, 进而分析系统返回的包来识别操作系统类型; 被动特征探测是基于嗅探远程系统上的通信对应不同的信息包的数据库, 来识别操作系统类型。但是我们认为两者遵循相同的概念, 本质上是一样的 (都是根据远程系统在处理 tcp/ip 协议的差异来识别操作系统类型)。

3 协议特征信号原理、技术

3.1 协议特征信号技术概述

协议特征信号方法是一个极其强大的识别技

* 收稿日期: 2002-03-21
作者简介: 张焕明 (1973-), 男, 助教; E-mail: zhm@jnu.edu.cn

术，能够以很高的概率迅速确定远程系统的类型。从原理上讲，不同厂家在编写自己的TCP/IP协议栈实现存在许多细微差别，也就是说各个厂家在编写自己的TCP/IP协议栈时，通常对确定的RFC指导作出不同的解释。因此通过探测这些差异，我们就能对目标系统所用的准确操作系统明智地加以猜测。

3.2 协议特征信号技术实现的工具

通过后面介绍的技术，读者可以根据原理写出工具，也可以使用现成工具来实现，这些工具有：nmap、snort、sniffer和queso等。这里有必要作些说明，这些工具并不是专门为识别操作系统而设计的，nmap是一个高效的端口扫描器，snort是一个入侵检测工具，而sniffer是实现网络侦听的工具总称。我们利用这些工具的技巧来识别操作系统类型。

nmap的O选项就是利用这种技术来识别操作系统的，以下是一个例子：

[root@abc /root] #nmap -O 12.12.12.12

Starting nmap V.2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)

Warning: No ports found open on this machine, OS detection will be MUCH less reliable

No ports open for host (12.12.12.12)

Remote OS guesses: Linux 2.0.27-2.0.30

Nmap run completed - 1 IP address (1 host up) scanned in 1 second.

从这个例子，可以看到目标主机(12.12.12.12)并没有开放任何端口，但是nmap仍然可以猜测到目标主机操作系统是Linux 2.0.27-2.0.30。值得一提的是，使用信息反馈方法无法识别没有开放任何端口的主机。

3.3 协议特征信号技术分析

在上面的例子中，nmap是怎么样准确猜测目标主机的操作系统呢？事实上nmap综合了多种协议特征信号。以下是协议特征信号使用的技术：

(1) 伪标志位探测。其原理是在一个SYN数据包TCP头中设置未定义的TCP“标记”(64或128)，低于2.0.35版本的Linux内核会在回应包中保持这个标记，而其它操作系统则没有这个问题。

(2) FIN探测。通过发送一个FIN数据包(或任何未设置ACK或SYN标记位的数据包)到一个打开的端口，并等待回应。RFC793定义的标准行为是“不”响应，但诸如MS Windows、BSDi、CISCO、HP/UX、MVS和IRIX等操作系统会回应一个RESET包。

(3) TCP ISN取样。其原理是通过在操作系统对连接请求的回应中寻找TCP连接初始化序列号的特征。目前可以区分的类别有传统的64K(旧UNIX系统使用)、随机增加(新版本的Solaris IRIX、FreeBSD、Digital UNIX、Cray和其它许多系统使用)、真正“随机”(Linux2.0*及更高版本、OpenVMST和新版本的AIX等操作系统使用)等。Windows平台(还有其它一些平台)使用“基于时间”方式产生的ISN会随着时间的变化而有着相对固定的增长。不必说，最容易受到攻击的当然是老式的64K方式。而最受我们喜爱的当然是“固定”ISN。确实有些机器总是使用相同的ISN，如某些3Com集线器(使用0x83和Apple Laser Writer打印机)。

(4) “无碎片”标记位。许多操作系统逐渐开始在它们发送的数据包中设置IP“不分片(无碎片)”位。

这对于提高传输性能有好处。但并不是所有操作系统都有这个位置，或许并不总是使用这个设置，因此通过留意这个标记位的设置可以收集到关于目标主机操作系统的更多有用信息。

(5) TCP初始化“窗口”。就是检查返回数据包的“窗口”大小。以前的探测器仅仅通过RST数据包的非零“窗口”值来标识为“起源于BSD4.4”。而象queso和nmap会记录确切的窗口值，因为该窗口随操作系统类型有较为稳定的数值。这种探测能够提供许多有用的信息，因为某些系统总是使用比较特殊的窗口值(例如，目前为此AIX是惟一使用0x3F25窗口值的操作系统)。而在声称“完全重写”的NT5的TCP堆栈中，Microsoft使用的窗口值总是0x402E。这个数值同时也被OpenBSD和FreeBSD使用。

(6) ACK值。也许你认为ACK值总是很标准的，但事实上操作系统在ACK域值的实现也有所不同。例如，假设向一个关闭的TCP端口发送一个FIN|PSH|UPG包，许多操作系统会将ACK设置为ISN值，但Windows和某些打印机会设置为seq+1。如果向打开的端口哪送SYN|FIN|URG|PSH包、Windows的返回值就会非常不确定。有时seq序列号值，有时是S++，而有时

回送的是一个似乎很随机性的数值。

(7) ICMP 错误信息查询。有些操作系统根据 RFC1812 的建议对某些类型的错误信息发送频率作了限制。例如，Linux 内核（在 net/ipv4/icmp.h）限制发送“目标不可到达”信息次数为每 4 秒 80 次，如果超过这个限制则会再减少 1/4 秒。一种测试方法是向高端随机 UDP 端口发送成批的数据包，并计算接收到“目标不可到达”数据包的数量。在 nmap 中只有 UDP 端口扫描使用了这个技术。这种探测操作系统方法需要稍微长的时间，因为需要发送大量的数据包并等待它们的返回。这种数据包处理方式也会对网络性能造成某种程度的影响。

(8) ICMP 信息引用。RFC 定义了一些 ICMP 错误信息格式。如对于一个端口不可到达信息，几乎所有操作系统都只回送 IP 请求＋8 字节长度的包，但 Solaris 返回的包会稍微长一点，Linux 则返回更长的包。checkpoint 防火墙在处理一些拒绝的包时，一种方法是使用 drop，将非法包完全抛弃，另一种方法是使用 reject，返回源地址一个端口不可达或目地的不可达的 icmp 包，通过这种细微区别就可以知道目标系统被防火墙隔开，并且该防火墙有可能是 checkpoint 防火墙。

(9) ICMP 错误信息回完整性。我们在前面已谈到，机器必须接收到数据包返回“端口不可到达”(如果确实是这样) 数据包。有些操作系统会在初始化处理过程中弄乱了请求头，这样当你接收到这种数据包时会出现不正常。例如，AIX 和 BSDi 返回的 IP 包中的“总长度”域会被设置为 20 字节（太长了）。某些 BSDI、FreeBSD、OpenBSD、ULTRIX 和 VAX 操作系统甚至会修改请求头中的 IP ID 值。另外，由于 TTL 值的改变导致校验和需要修改时，某些系统（如 AIX、FReeBSD 等）返回数据包的检验和会不正确成为 0。有时这种情况也出现在 UDP 包检验和。

(10) TCP 选项。这是收集信息的最有效的方法之一。其原因是：①它们通常真的是“可选的”，因此并不是所有的操作系统都使用它们；②向目标主机发送带有可选项标记的数据包时，如果操作系统支持这些选项，会在返回包中也设置这些标记；③可以一次在数据包中设置多个可选项，从而增加了探测的准确度。

3.4　一个利用协议特征信号识别技术的例子

这里介绍一个利用 ICMP 包请求的特性来探测 SUN 操作系统的一个例子。

对于 ICMP 地址掩码请求，只有少数操作系统会产生相应的应答，这些系统包括 ULTRIX OpenVMS，Windows 95/98/98 SE/ME，NT below SP 4，和 SUN Solaris 机器。但其中 SUN 机器对碎片 ICMP 地址掩码请求（fragmented ICMP Address Mask Requests）的应答不一样，通过这种方法就能鉴定 SUN 主机操作系统。

下面的实现要使用到 SING（http://sourceforge.net/projects/sing）工具，该工具可对 SUN SOLARIS2.7 机器进行正常的地址掩码请求：

```
#./sing -mask IP-Address
SINGing to IP-Address (IP-Address): 12 data bytes
12 bytes from IP-Address: icmp-seq=0 ttl=236 mask=255.255.255.0
12 bytes from IP-Address: icmp-seq=1 ttl=236 mask=255.255.255.0
--- IP-Address sing statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
```

操作系统会回答一个 ICMP 的地址掩码请求并带有其响应的网络地址掩码。

接着发送一些碎片请求，下面的例子是通过发送 8 字节的 IP 数据碎片到同样上面操作的 SUN SOLARIS2.7 机器上，就可以看到操作系统响应的和刚才的不一样了（-c 2 是允许 SING 发送两个 ICMP 地址掩码请求）：

```
#./sing -mask -c 2 -F 8 IP-Address
SINGing to IP-Address (IP-Address): 12 data bytes
12 bytes from IP-Address: icmp-seq=0 ttl=241 mask=0.0.0.0
12 bytes from IP-Address: icmp-seq=1 ttl=241 mask=0.0.0.0
--- IP-Address sing statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
```

这样你就可以看到 SUN SOLARIS 回应的网络地址掩码是 0.0.0.0，其它系统不会有这样的回应。

4　防护系统被识别的方法

从识别操作系统的技术不难分析出防护系统

被识别的方法。

防范基于信息反馈技术的识别技术比较简单并且有效。只要有意改变服务 (如：TELNET, FTP 等) 的信息显示，不让有关操作系统的信息回显就能阻止旗标攫取识别方法。管理员基至可以提供虚假的信息，蒙蔽攻击者。通过伪装开放的端口也可轻易挫败特殊端口识别技术。防范基于协议特征信号的识别技术打补丁是最有效的方式，然而这不是一个容易解决的问题。通过修改操作系统源代码或改动某个操作系统参数来达到改变单个独特的协议信号的目的是可能的，但是这么做可能对操作系统的功能造成不利影响。

防范基于协议特征信号识别的另一种技术是使用健壮的安全代理或防火墙，使用安全代理或防火墙来关掉主机的 ICMP 响应，过滤外界的 ICMP 请求等其它有害的扫描和探测。当然安全代理或防火墙可处于网关的位置，也可成为主机的一个软件或模块。

5 总 结

信息反馈方法简单易用，对使用者的技术要求不高，不需要借助于工具或编程实现，但是如果被识别系统的管理员伪装旗标或欺骗服务端口，则运用该方法很容易被愚弄，得到完全错误的判断。

协议特征信号技术综合应用了多种技术，能以较高的效率判断远程系统类型。随着操作系统不断地增加新特性，会有更多的特征信号被黑客挖掘。但该技术要求使用者熟悉相关工具的使用技巧或会编程实现，并善于理解和判断操作系统返回信息的含意，对使用者技术水平要求较高。

参考文献：

[1] RICHARD W S. TCP/IP Illustrated Volume 1.
[2] 网络信息安全技术基础[M]. 北京：电子工业出版社.
[3] http://www.sys—security.com.
[4] http://www.securityfocus.com
[5] http://www.insecure.org

Method and Principle of Identifying Operating System and Its Protective Technology

ZHANG Huan ming[1], *SONG Zhen feng*[2]
(1. Network Center, Jinan University, Guangzhou 510632, China;
2. Guangdong Branch of Agricultural Bank of China, Guangzhou 511430, China)

Abstract: This article analyses and delves into the method and principle of identifying the operating system. It also discuss the protocol character signal technology which is widely used, and the protective technology is given.

Key words: identifying technology; information feedback technology; protocol character signal