对操作系统指纹的研究与探讨

Discussion and Research on Fingerprint of Operating Systems

摘　要：本文对操作系统指纹进行了深入的研究与探讨。阐明了操作系统指纹的存在，介绍了若干指纹识别技术和操作系统指纹正反两方面的利用，即进行网络拓扑发现和被黑客所利用。并探讨了操作系统指纹的消除方法，最后还指出了操作系统指纹和防火墙自身安全性的关系，给出了一种自身安全性高的防火墙系统的设计思想。

关键词：操作系统指纹　利用　消除　防火墙

郭锡泉　张会汀　方 山（广州暨南大学电子系　510632）

1 引言

不同的网络操作系统在处理网络信息时是不完全相同的，存在着各自的特点，这些特点就称为系统的“指纹”。通过识别这些指纹就可以实现网络系统的识别。操作系统指纹的存在是一把双刃剑。一方面可以利用它进行网络拓扑的主动发现，辅助管理人员对整个网络的监控、管理，提高效率和管理水平；另一方面，操作系统指纹泄漏了自己的“身份”——操作系统类型和版本号，为网络安全埋下了极大的隐患。对于一个黑客来说，知道了网络上一台主机的操作系统类型和版本号，那么攻破这台主机只是时间上早一点或迟一点的问题！因此，研究和关注操作系统指纹对从事计算机网络安全的工作人员来说是不可忽视的问题，也很有必要性和迫切性。

2 操作系统指纹效应的存在

作为网络操作系统，究其实质，系统指纹实际上来源于TCP/IP协议栈。不同的操作系统，如WINDOWS、LINUX，还有各种类型的UNIX系统，它们的TCP/IP协议栈是各不相同的，对各种类型的数据包的响应也有所不同。而再精明的管理员都不太可能去修改系统底层的网络的堆栈参数，这样，借助一个好的扫描软件（如NMAP），我们常常很轻易就确定了网络上某台主机的操作系统类型和版本号。

现在，随着ADSL的普及，以及大量校园网用户的存在，种种因素都促使计算机在线时间的延长。另一方面，黑客软件很容易获取，各类扫描软件唾手可得，这意味着网络上主机面临的安全风险越来越大。操作系统指纹效应被不正当利用，由此引起的后果是极其严重的。

3 指纹识别技术

利用操作系统指纹，需要掌握TCP/IP协议栈指纹的识别技术。目前常用的指纹识别技术包括：

3.1 FIN 探测

这种技术的方法是发送一个FIN包(或任何其他不带ACK或SYN标记的包)到一个打开的端口并等待回应。正确的RFC793(最新的)中规定系统将不予响应,但许多有问题的实现例如MSWINDOWS，BSDI，CISCO，HP/UX，MVX和IRIX会发回一个RESET。正是这些问题的存在,使得可以区分一部分操作系统。

3.2 是否设置分段位

许多操作系统开始设置不分段位,从而增进系统的一些性能，但也促进了操作系统的识别。

3.3 TCP 初始窗口大小

这个方法简单地说是检查返回包的窗口大小。有些操作系统可以简单地用这种方法精确的识别。例如AIX使用的窗口大小为16165。

3.4 ACK 值

许多操作系统的ACK值是不标准的，带有自己的特征。

3.5 ICMP 出错信息的频率

一些操作系统按照RFC1812，限制了出错ICMP包的发送频率。

3.6 ICMP 消息引用

基金项目：广东省科技计划项目“基于专用协议栈的流过滤网络防火墙研制”（2003C101038）

RFC(最新的)规定ICMP错误消息可以引用一部分引起错误的源消息。对一个端口不可达消息，几乎所有操作系统只送回IP请求头外加8字节。然而，SOLARIS送回的稍多，而LINUX更多。这使得甚至在对方没有监听端口的情况下认出LINUX和SOLARIS主机。

3.7 TOS

有些系统在返回ICMP端口不可达信息时，TOS值不为0。

3.8 分段的处理

一些系统在处理重复的IP分段信息时采用的方法是不同的。

3.9 TCP 选项

不同的操作系统对于TCP选项的支持是不同的。有的多些，有的少些。且在处理返回时存在着格式和顺序的不同。这些可以很好的用于识别系统。

3.10 SYN 洪泛

一些操作系统当接收较多的孤立SYN包时，会停止接收新的连接，从而保证系统的稳定。所以可以发送一定数量(典型8个)的SYN包来根据系统的处理方式区别系统。

仅仅依据一两种方法来认定某台主机用的是什么操作系统，这样的结果是不可信的。但综合上述方法一起使用，使用的方法越多，得出的结果越可信。当然，远程主机开放的端口越多，指纹识别结果的准确度也越高。

4 操作系统指纹的利用

4.1 网络拓扑发现

网络拓扑发现技术是一项很有实用价值的技术，方便了网络系统的维护和管理，成为现有网络管理系统的一个很好的补充。其基本过程为：信息采集->区分设备（路由器、多目主机、主机）->构造拓扑->系统识别。其中，系统识别部分就是利用TCP/IP协议栈的指纹识别技术来识别主机采用的操作系统。将各个设备的系统区分出来，如主机采用的操作系统和路由设备的类型等，这样就能给网络管理人员更加全面的网络整体结构的认识。

4.2 被黑客利用

操作系统指纹效应的存在是一把双刃剑。它也有被黑客、被不正当利用的可能。对黑客来说，进行攻击前首要的问题是确定目标主机的操作系统类型和版本，信息越准确，攻击的成功率越高。众所周知，常用的操作系统都有很多安全漏洞。而许多安全漏洞不仅与操作系统的类型有关，还与其版本有关。因此，确认了目标主机的操作系统类型和版本之后，黑客可以查找相应的安全漏洞对目标主机进行攻击。与对训练有素而又富有耐性的黑客而言，弄清了目标的操作系统类型和版本，那么攻破目标只是时间上迟早的问题！

快速且准确的识别远程操作系统是十分重要的。假设黑客在进行一次侵入式的测试中发现port 139是开放的，如果这是一个有弱点的Bind，那么只有一次攻击的机会，如果失败就会造成这个服务器无法运作。用一个好的TCP/IP的指纹识别工具，可以很快的发现这台机器正在运行的操作系统和版本，据此可调整使用的shell code。令人担心的是这样的工具太多了，也太容易被一般人得到。

5 操作系统指纹的消除

在国内外的文献中，鲜见有文章对操作系统指纹进行系统的研究，尤其在如何消除操作系统指纹的问题上。本人结合搜集到的资料和实践中的体会，谈谈对这个问题的看法，也希望能起到抛砖引玉的作用。

从“治本”的角度说，操作系统指纹既然来源于操作系统本身，那么它的彻底消除应该依赖于操作系统的开发商。一方面，如果操作系统开发商对操作系统指纹的负面效应有充分认识的话，他们在技术上完全有可能消除系统指纹，至少可以大大减少指纹效应。另一方面，如果RFC文档对TCP/IP协议的实现有非常标准的、统一的要求，那么操作系统开发商设计出来的系统对网络信息的响应都一样，这样的话上述TCP/IP协议栈指纹识别技术就不再有意义了，也就没有操作系统指纹这一问题了。

从“治标”的角度说，可以采取如下措施“掩盖”系统指纹：

5.1 采用一些对抗扫描、对抗指纹识别的软件

有一个叫inflog的软件（http://www.rootshell.com/）可以对抗NMAP等软件的扫描，而且还是免费软件。

5.2 采用防火墙

扫描软件的准确性是靠获取尽可能多的有关目标主机TCP/IP协议栈的信息来保证的，防火墙能或多或少地影响扫描软件的准确性。对个人用户，装一个个人防火墙并设置得当的话，可以极大地减少操作系统的指纹效应；对公司集团用户，最好使用带NAT（网络地址转换）功能的防火墙网关或代理型的防火墙网关。

5.3 系统管理员要注意修改应用程序的banner

像FTP、TELNET和微软的IIS服务等应用层软件，其默认的banner都会把操作系统的类型和版本显示出来。在网络安全问题极其严峻的今天，聪明的系统管理员一定要注意修改这些banner，而且不妨来个“弄虚作假”以起到迷惑作用。

6 操作系统指纹与防火墙网关自身的安全性

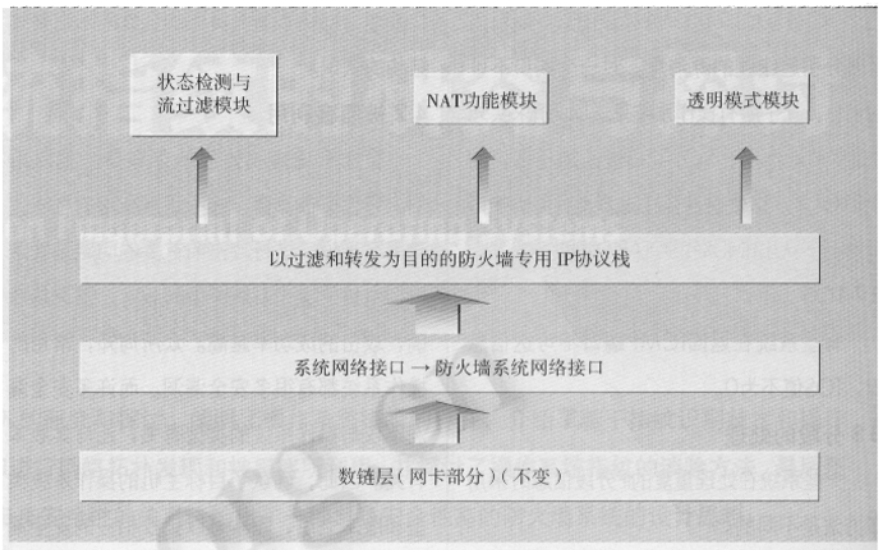
由上述可知，防火墙网关是对抗扫描软件的一个有力措施。如果一家公司的内部网络有专用的防火墙系统保护，那么内网的主机是比较安全的，因为防火墙的存在使外网的扫描软件难以识别内网主机操作系统的信息。但是，这时候扫描软件实际上是在对防火墙的TCP/IP协议栈进行扫描。而国内有不少防火墙产品都是在通用操作系统上加载自己的防火墙软件来做的，如果黑客通过扫描

协议栈指纹来获得具体的操作系统类型和本号的话，那么他们就可以通过系统漏洞来攻破防火墙！由此可见，操作系统指纹与防火墙自身的安全性也有密切的联系。

对于在通用操作系统上构建的防火墙，其安全性既与自身设计有关，也与操作系统有关。对于防火墙来说，自身安全性应该是第一位的，不能保证自己的安全，何来对别人的保护？操作系统指纹是防火墙自身安全性的极大隐患，而市面上不少防火墙软件都忽略了这个根本问题，因此形势是相当严峻的。有没有解决这个问题的方法？答案是肯定的。如果我们能屏蔽操作系统所有的网络操作，只保留防火墙软件的网络操作，那么就能消除操作系统指纹。这时扫描软件只能扫描到防火墙的TCP/IP协议栈，这样，防火墙安全性基本上只与自身设计有关，而与操作系统无关。这是在通用操作系统上构建防火墙问题上的一个进步。如果防火墙软件设计得好，那么其安全性就高。

众所周知，WINDOWS的源代码是不公开的。在WINDOWS上构建防火墙时要彻底屏蔽掉系统的其他网络操作，这恐怕难以实现（Windows下的防火墙对某些系统数据包是屏蔽不掉的）。而LINUX的源代码是公开的，有利于研究和开发。我们对LINUX（Redhat 7.3）内核（版本号是2.4.18-3）网络部分进行了深入的研究，通过模块加载动态地修改了网卡的中断处理乃至系统的整个网络流程，彻底屏蔽了系统的所有网络操作，消除了系统协议栈的指纹效应，极大地提高了防火墙的安全性。系统的框架如下：

扫描软件（如NMAP）或通过数据包生成器定制数据包对该防火墙扫描，都得不到正确的结果。更重要的是，由于本防火墙构建了一个以过滤和转发为目的的TCP/IP专用协议栈，主要目的是过滤和转发，而不是交给应用层，因此受攻击的可能性很小。黑客不能通过协议栈指纹获取操作系统的类型及版本号，一般不会贸然攻击该系统，因为他无法选择相应的攻击方法。使用不恰当的攻击方法的话将会给系统管理员留下相当多的线索，这是黑客的大忌。该防火墙系统自身安全性高，功能也比较完善，再则LINUX是免费软件，系统的成本低廉。故该系统对于中小型企业有一定的应用价值。



7 小结

本文深入研究操作系统指纹的存在、识别与利用，并探讨了操作系统指纹的消除方法，最后还指出了操作系统指纹和防火墙自身安全性的关系，给出了一种自身安全性高的防火墙系统的设计思想。本文对想了解操作系统指纹的读者和网络安全方面的研究人员、工作人员有一定的参考价值。

参考文献

1 向剑伟、孙晓，网络安全评估所涉及的关键技术与原理[j]，株洲工学院学报，2002,7。

2 张勇、张德运、李钢，网络拓扑发现的主动探测技术的研究和实现[j]，小型微型计算机系统，2000,8。

3 Farrow, Rik . System Fingerprinting with Nmap[j]. Network Magazine. Nov2000, Vol. 15。

4 McClure, Stuart, Scambray, Joel . TCP fingerprinting solutions for Linux offer another way to gather security data[j]. InfoWorld. 1998,10,26, Vol. 20 。

5 方山，网络防火墙状态检测技术的研究与实现[z]，暨南大学，2003。