网络扫描原理的研究

黄家林,姚景周,周 婷
(中南大学 信息科学与工程学院,湖南 长沙 410083)

摘 要:安全扫描是在网络安全领域中非常重要的一种技术手段。使用扫描,可以发现网络信息,甚至进行攻击。分析了网络安全扫描的原理,对扫描中使用的主要技术进行了分类,并阐述了每种技术的原理及协议特性。给出了常见平台上的有代表性的工具,并针对其特点进行了比较。指出网络扫描中存在的一些性能和安全上的问题,提出了一些使之完善化的建议。

关键词:ping;端口扫描;操作系统探测;弱点探测;防火墙探测
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)06-0147-04

Research on Network Scanning Principles

HUANG Jia-lin, YAO Jing-zhou, ZHOU Ting
(College of Information Science & Engineering, Central South University, Changsha 410083, China)

Abstract: Network scanning is very important in security field. It is used to get the information of the target network, even to launch attack. Analyzes the principles of network security scan, categories the techniques used in a scan process, presents the concept and protocols each technique derives from. Also introduces some utilities on common OS platforms, discusses their characteristics separately. At last, points out some performance and security problems existing in network scanning and gives some suggestions for improvement.

Key words: ping; port scan; OS detection; vulnerability detection; firewalking detection

0 引 言

收集目标网络和主机的信息,是维护网络安全的第一步。在网络安全人员看来,只有收集到了足够、有效的信息,才有可能防止潜在的攻击行为。正如安全专家所做的那样,黑客也会尽可能地收集信息,看系统是否存在漏洞或者弱点以实施攻击。双方攻防的第一步,主要集中在网络安全扫描领域。

网络扫描,是基于 Internet 的探测远端网络或主机信息的一种技术,也是保证系统和网络安全必不可少的一种手段。网络扫描,是对计算机主机或者其它网络设备进行安全性检测,以找出安全隐患和系统漏洞。但是,网络扫描软件事实上也是一把双刃剑:入侵者利用它来寻找对系统发起攻击的途径,而系统管理员则利用它来有效防范黑客入侵。通过网络扫描,扫描者能够发现远端网络或主机的配置信息、TCP/UDP端口的分配、提供的网络服务、服务器的具体信息等。网络扫描可以划分为 ping 扫描、端口扫描、操作系统探测、弱点探测、防火墙规则探测五种主要技术,运用的原理各不相同。

收稿日期:2006-09-08

作者简介:黄家林(1952-),男,湖南长沙人,研究员,研究方向为计算机网络安全和网络管理技术。

1 扫描技术及原理

1.1 ping 扫描

ping 扫描的目的,就是确认目标主机的 IP 地址,即扫描的 IP 地址是否分配了主机。对没有任何预知信息的黑客而言,ping 扫描是进行网络扫描及入侵的第一步,也是必不可少的一步;对已经了解网络整体 IP 划分的网络安全人员来讲,也可以借助 ping 扫描,对主机的 IP 分配有一个精确的定位。大体上,ping 扫描是基于 ICMP 协议的,因此把发现目的网络或主机的一类基于 ICMP 协议的扫描称为 ping 扫描。其主要思想,就是构造一个 ICMP 包,发送给目标主机,从目标主机生成的响应来进行判断。

1.1.1 ECHO 扫描

给目标 IP 地址发送一个 ICMP ECHO REQUEST (ICMP type 8)的包,等待是否收到 ICMP ECHO REPLY(ICMP type 0)[1]。如果收到了 ICMP ECHO REPLY,就表示目标 IP 上存在主机,否则就说明没有主机。同时扫描多个 IP 地址,就叫 ping 扫描。

此外,如果向子网的网络地址或广播地址发送 ICMP ECHO REQUEST,则子网中的 unix 主机会响应该请求,而 windows 主机不会生成响应,这也可以用来进行操作系统探测。

1.1.2 non-ECHO 扫描

向目的 IP 地址发送 ICMP TIMESTAMP REQUEST(ICMP type 13),或 ICMP ADDRESS MASK REQUEST(ICMP type 17),根据是否收到响应,可以确定目的主机是否存在。当防火墙配置为阻止 ICMP ECHO 流量时,则可以用 non-ECHO REQUEST 来进行主机探测。

1.2 端口扫描

ping 扫描确定了目标主机的 IP 地址,接下来就可以通过端口扫描,探测主机所开放的端口。因为端口扫描通常只做最简单的端口联通性测试,不进行更进一步的数据分析,因此比较适合进行大范围的扫描:对指定 IP 地址进行某个端口值段的扫描;或者指定端口值对某个 IP 地址段进行扫描。然后基于端口扫描的结果,进行操作系统探测和弱点扫描。端口扫描大体上分为 TCP 扫描和 UDP 扫描两类。

1.2.1 TCP 扫描

TCP 建立连接分三步,也称三次握手:

1)请求端发送一个 SYN 包,指明客户打算连接的目的端口。

2)观察目的端返回的包:

返回 SYN/ACK 包,说明目的端口处于侦听状态;

返回 RST/ACK 包,说明目的端口没有侦听,连接会重置。

3)若返回 SYN/ACK 包,则请求端向目的端口发送 ACK 包完成 3 次握手,连接建立。

●TCP 全连接和半连接扫描。

全连接扫描,就是和目的主机建立一个 TCP 连接,而目的主机的 log 文件中会生成记录。半连接扫描,也称为 TCP SYN 扫描,则违反了 TCP 三次握手的规则。此扫描发送 SYN 包开始三次握手并等待目的主机的响应。如果收到 SYN/ACK 包,则说明端口处于侦听状态,扫描者马上发送 RST 包,中止连接。因为半连接扫描并没有建立连接,目的主机的 log 文件中可能不会记录此扫描[2]。

●TCP 隐蔽扫描。

RFC793 指出,处于关闭状态的端口,在收到探测包时会响应 RST 包,而处于侦听状态的端口则忽略此探测包。根据发送探测包的不同,TCP 隐蔽扫描又分为 SYN/ACK 扫描、FIN 扫描、XMAS(圣诞树)扫描和 NULL 扫描四种。

SYN/ACK 扫描和 FIN 扫描:这两类扫描均绕过 TCP 三次握手过程的第一步,直接给目的端口发送 SYN/ACK 包或者 FIN 包。因为 TCP 是有连接的,它知道在第一步中应该发送的 SYN 包没有送出,从而认为此连接过程出错,发送一个 RST 包以拆除连接。而这正是我们想要的——只要有响应,就说明目标系统存在,且目标端口处于关闭状态[3]。

XMAS扫描和 NULL 扫描:这两类扫描正好相反,XMAS 扫描设置 TCP 包中所有标志位(URG, ACK, RST, PSH, SYN, FIN),而 NULL 扫描则关闭 TCP 包中的所有标志位。

1.2.2 UDP 端口扫描

UDP 协议是数据包协议,为了要发现正在服务的 UDP 端口,通常的扫描方式是构造一个内容为空的 UDP 数据包送往目的端口。若目的端口上有服务正在等待,则目的端口返回错误的消息;若目的端口处于关闭状态,则目的主机返回 ICMP 端口不可达消息。UDP 端口扫描的速度很慢,因为 UDP 端口扫描软件要计算传输中丢包的数量,而且扫描结果也不太准确[4]。

1.3 操作系统探测

在网络结构中的服务器,有两层含义:一是指网络上管理网络资源的主机或设备,如文档服务器等;二是指向其它计算机程序提供数据/服务的计算机程序。从而,在操作系统探测中,其目的也是双重的:得到所扫描的目标主机的 OS 具体信息,以及提供服务的计算机程序的具体信息。比如操作系统探测的结果是:OS 是 Windows XP sp2,服务器平台是 IIS 4.0[5]。为简便起见,统称为操作系统(OS)探测。

1.3.1 二进制信息探测

这是最简单的 OS 探测技术,等于是 OS 泄漏了自己的具体信息。

从图 1 可以看出,在 telnet 连上 FTP 服务器后,服务器返回的标语(banner)已经提供了 server 的信息,在执行 ftp 的 syst 命令后可得到更具体的信息。

```
C: \ telnet ftp. netscape. com 21
Trying 207. 200. 74. 26…
Connected to ftp. netscape. com.
Escape character is '^]'.
220 ftp29 FTP server (UNIX(r) System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

图 1 二进制信息

1.3.2 HTTP 响应分析

在和 HTTP 建立连接后,可以分析服务器的响应得出 OS 类型,响应包经分析如图 2 所示。

```
HTTP/1.0 200 OK
Date:Sun,25 Jan 2004 20:00:02 GMT
Server:Apache/1.3.26(Unix) mod_gzip/1.3.19.1a
mod_perl/1.27
Last-Modified:Mon, 19 Jan 2004 03:11:10 GMT
```

图 2　响应包分析

1.3.3　栈指纹分析

网络上的所有主机都会通过 TCP/IP 或类似的协议栈来互通互联。由于 OS 开发商不唯一,系统架构多样,甚至是软件版本的差异,都导致了协议栈具体实现上的不同。对错误包的响应,默认值等都可以作为区分 OS 的依据。

1)主动栈指纹探测。

主动栈指纹探测是主动向主机发起连接,并分析收到的响应,从而确定 OS 类型的技术。

(1)FIN 探测。跳过 TCP 三次握手的顺序,给目标主机发送一个 FIN 包。RFC793 规定,正确的处理没有响应,但有些 OS,如 MS Windows, CISCO, HP/UX 等会响应一个 RST 包。

(2)Bogus 标志探测。某些 OS 会设置 SYN 包中 TCP 头的未定义位(一般为 64 或 128),而某些 OS 在收到设置了 Bogus 位的 SYN 包后,会重置连接。

(3)统计 ICMP ERROR 报文。RFC1812 中规定了 ICMP ERROR 消息的发送速度。Linux 设定了目标不可达消息上限为 80 个/4 秒。OS 探测时可以向随机的高端 UDP 端口大量发包,然后统计收到的目标不可达消息。用此技术进行 OS 探测时时间会长一些,因为要大量发包,并且还要等待响应,同时也可能出现网络中丢包的情况。

(4)ICMP ERROR 报文引用。RFC 文件中规定,ICMP ERROR 消息要引用导致该消息的 ICMP 消息的部分内容。例如对于端口不可达消息,某些 OS 返回收到的 IP 头及后续的 8 个字节,Solaris 返回的 ERROR 消息中则引用内容更多一些,而 Linux 比 Solaris 还要多。

2)被动栈指纹探测。

被动栈指纹探测是在网络中监听,分析系统流量,用默认值来猜测 OS 类型的技术,包括 TCP 初始窗口尺寸, Don't Fragment 位等。

(1)TCP 初始化窗口尺寸。分析响应中的初始窗口大小。这种技术比较可靠,因为很多 OS 的初始窗口尺寸不同。比如 AIX 设置的初始窗口尺寸是 0x3F25,而 Windows NT5、OpenBSD、FreeBSD 设置的值是 0x402E。

(2)Don't Fragment 位。为了增进性能,某些 OS 在发送的包中设置了 DF 位,可以从 DF 位的设置情况中做大概的判断。

(3)TCP ISN 采样。建立 TCP 连接时,SYN/ACK 中初始序列号 ISN 的生成存在规律,比如固定不变、随机增加(Solaris, FreeBSD 等),真正的随机(Linux 2.0.*),而 Windows 使用的是时间相关模型,ISN 在每个不同时间段都有固定的增量。

1.4　弱点扫描

弱点扫描是端口扫描和操作系统探测的后续,也是网络安全人员和黑客收集网络或主机信息的最后一步。从对黑客攻击行为的分析和收集的弱点类型来看,弱点扫描绝大多数都是针对特定操作系统所提供的特定的网络服务,也就是针对操作系统中某一个特定端口的。弱点扫描使用的技术主要有基于弱点数据库和基于插件两种[6]。

1.4.1　基于弱点数据库

此方法的关键在于其所使用的弱点数据库。首先建立分析的环境模型,对网络系统存在的弱点、过往黑客攻击案例和系统管理员的网络安全配置进行综合分析;基于分析的结果,生成一套标准的网络/主机弱点数据库,与此同时构造相应的匹配模式,由扫描程序自动进行弱点扫描工作。从而进行弱点扫描的准确性就取决于弱点数据库的完整性及有效性。

1.4.2　基于插件

插件是由脚本语言编写的子程序模块,扫描程序可以通过调用插件来执行弱点扫描。添加新的功能插件就可以使弱点扫描软件增加新的功能,也可以添加新的扫描插件增加扫描软件可扫描弱点的数量,还可以升级扫描插件来更新弱点的特征信息,从而得到更为准确的扫描结果。插件技术使弱点扫描软件的升级维护变得相对简单,而专用脚本语言的使用也简化了编写新插件的编程工作,使弱点扫描软件具有很强的扩展性。

1.5　防火墙规则探测

目的在于扫描后的入侵或再次开始扫描的顺利进行。这种技术采用类似于 traceroute 的 IP 数据包分析方法,来测定是否可以发送一个特定的包给位于过滤设备后的主机。可以测定防火墙上打开或允许通过的端口,并且测定带有各种控制信息的包是否能通过防火墙。更进一步,可以探测到位于数据包过滤设备后的路由器。

2　常见的扫描工具

扫描一个复杂的多层结构系统,工具的选择是相当重要的。通常,扫描者会考虑工具的操作平台、所运

用的原理、易用性、准确性等等。在作出决策时,扫描工具的可用性是最重要也是最基本的,但是扫描过程的可控性和扫描结果分析的准确性同样不容忽视。常见的扫描工具如表 1 所示。

表 1 常见扫描工具

工具类型	名称	平台	特点介绍
ping 扫描	Hping2	Unix/Linux	能自定义发送 ICMP/UDP/TCP 包到目标地址并且显示响应信息
	icmpush& icmpquery	Unix/Linux	可以完全定制 ICMP 包的结构以及种类
	Pinger	Windows	速度很快,能同时发送多个 ICMP ECHO REQUEST 并且显示响应信息
端口扫描	Fport	Windows	能扫描目标主机上所有打开的 TCP/UDP 端口,并显示端口所属的进程
	SuperScan	Windows	能进行 TCP 全连接扫描、ping 扫描,并且可以解析域名
OS 探测	XProbe2	Unix/Linux	基于 ICMP 协议,通过与配套的签名数据库进行模糊匹配来确定 OS 类型
	THC-Amap	Unix/Linux	通过分析端口响应的应用程序指纹数据来确定应用程序及服务
弱点扫描	Whisker	Unix/Linux	能扫描出大量的 HTTP 服务器弱点,并且可以扩充其程序库,创建自己的 HTTP 扫描器
	Nessus	Unix/Linux	应用了多线程和基于插件的技术,速度快,并可以对扫描出的弱点提出解决方案
	GFI LANguard	Windows	对目标主机可以作出较完整的安全测试,并生成可自定义的安全报告
防火墙规则探测	Firewalk	Unix/Linux	分析 IP 包的响应,从而测定网关的 ACL 并且绘制出网络拓扑图

3 结 论

一般而言,扫描者并不是孤立地、单纯地使用某种扫描技术,而是综合地应用一系列的扫描方法。而如果大范围地进行某种扫描,反复高速地发出特定的连接请求,所造成的结果就是目标主机上存在大量等待的 TCP 连接,目标网络中充斥着许多无用的数据包,最终网络拥塞,主机无法正常使用,这正是 DoS 的表现。因此若要防范网络扫描以及可能的 DoS 攻击,要做到以下三点:

(1) 在防火墙及过滤设备上采用严格的过滤规则,禁止扫描的数据包进入系统。

(2) 主机系统除了必要的网络服务外,禁止其它的网络应用程序。

(3) 对于只对内开放的网络服务,更改其提供服务的端口[7]。

此外,网络扫描时发送的数据或多或少都会含有扫描者自身相关信息,从而也可以抓取扫描时的数据包,对扫描者进行反向追踪,这也是一个值得研究的方向。

参考文献:

[1] Stevens W R. TCP/IP 详解卷一:协议[M]. 北京:机械工业出版社,2000:50-60.

[2] Afkin O. Network Scanning Techniques-Understanding how it is done [EB/OL]. 1999-11-01[2005-06-11]. http://www.sys-security.com.

[3] Fyodor. The Art of Port Scanning[EB/OL]. 1997-09-06 [2005-11-12]. http://www.insecure.org/nmap/nmap_doc.html.

[4] 王 灏,王换招. 端口扫描与反扫描技术[J]. 微机发展,2001,11(5):60-63.

[5] Fyodor. Remote OS detection via TCP/IP stack Fingerprinting[EB/OL]. 1998-10-18[2006-02-01]. http://insecure.org/nmap/nmap-fingerprinting-article.txt.

[6] 洪 宏,张玉清,胡予濮,等. 网络安全扫描技术研究[J]. 计算机工程,2004,30(10):54-56.

[7] 丁常福,方 敏,徐 亮. 端口扫描技术及防御分析[J]. 微机发展,2003,13(6):7-12.

(上接第 146 页)

hardware implementation based on Montgomery's algorithm [J]. Journal of Shanghai Jiaotong University,2002,E-7(1):46-49.

[2] Rivest R L,Shamir A,Adleman L M. A Method for Obtaining Digital Signatures and Public-key Cryptosystems[J]. Communication of the ACM,1978,21(2):120-126.

[3] Montgomery P L. Modular multiplication without trial division [J]. Mathematics of Computation,1985,44(170):519-521.

[4] 王金荣,陈 勤,丁 宏. 大数模乘算法的分析与研究[J]. 计算机工程与应用,2004,40(24):70-72.

[5] Welschenbach M. Kryptographie in C and C++ weite, überarbeitete und erweiterte Auflage[M]. 北京:电子工业出版社,2003:54-80.

[6] 孔凡玉,于 佳,李大兴. 一种改进的 Montgomery 模乘快速算法[J]. 计算机工程,2005(8):1-3.

[7] Dusse S R,Jr Kaliski B S. A Cryptographic Library for the Motorola DSP56000[C]// Advances in Cryptology- EUROCRYPT 90. [s.l.]:Springer-Verlag,1990:230-244.

[8] Walter C D. Montgomery Exponentiation Needs No Final Subtractions[J]. Electronic Letters,1999,35(21):1831-1832.