网络监听与反监听

贺龙涛[1]　方滨兴[2]　云晓春[1]
[1](哈尔滨工业大学计算机科学与技术系,哈尔滨 150001)
[2](国家计算机网络与信息安全管理中心,北京 100031)
E-mail:hlt@hope.hit.edu.cn

摘　要　在网络安全领域,网络监听程序(sniffer)占有重要的地位。文章分析了网络监听的工作原理,防止被有效监听的方法,并分析了当前出现的检测监听程序(anti-sniffer)的工作原理。由此提出 sniffer 对抗 anti-sniffer 的办法:修改本机协议栈以及进行网络通信包伪装、检测网络负载并在负载剧增的时候停止监听。网络监听与反监听的对抗作为黑客攻击与网络安全斗争的重要方面,还将继续下去。

关键词　网络监听　检测监听　混杂模式

文章编号 1002-8331-(2001)18-0020-02　文献标识码 A　中图分类号 TP393.08

Network Sniffer and Anti-Sniffer

He Longtao[1]　Fang Binxing[2]　Yun Xiaochun[1]
[1](Department of Computer Science and Technology,Harbin Institute of Technology,Harbin 150001)
[2](National Computer Network and Information System Security Administration Center,Beijing 100031)

Abstract: Sniffer plays an important role in the field of network security.The principle of network sniffing and the methods to stop people from sniffing data are analyzed,and the principle of anti-sniffer is also analyzed.Then the method of anti-anti-sniffer is put forward that changing the protocol stack and spoofing network communications,detecting the network load then stopping sniffing when the load is increasing remarkably.Being an important aspect of the opposition of hacker attacking and network security,the opposition of sniffer and anti-sniffer will go on.

Keywords: Sniffer,Anti-Sniffer,Promiscuous Mode

1　引言

网络监听,即将网络上传输的数据捕获并进行分析的行为[1]。在网络安全领域,网络监听占有极其重要的作用。对于黑客攻击而言,网络监听是一种有效的信息(用户名、口令等)收集手段,并且可以辅助进行 IP 欺骗[2];对于安全管理而言,监听也是监控本地网络状况的直接手段,监听还是基于网络的入侵检测系统(NIDS)的必要基础[3]。近一段还出现了在交换网络进行主动监听的研究[4]。

为了防止网络数据被有效的监听,出现了网络分段以及网络交换技术;以及加密传输技术。

而针对网络监听的检测的研究,也一直在进行着[5,6]。虽然从理论上讲,完全检测监听程序是不可能的,因为它们基本上是被动的:只是进行数据包搜集,并不发送数据。然而,实际上,有时候还是可能检测到监听程序的。独立设计的硬件网络监听器并不向网网络发送任何数据,然而在一般的计算机上安装了监听程序之后,监听程序往往会产生数据通信,例如它可能会对所捕获包的 IP 地址进行反向域名查询。网络监听的检测正是依据这些网络监听程序固有的特点进行工作,从而尽量查找出本网段内进行监听的机器。

既然有了对网络监听的检测手段,就必然会有对反检测的研究,也就是依据对各种检测手段的特点分析,对网络监听程序进行改造,以逃避检测,甚至假冒别的正常主机的一些行为,使之被误检测为正在进行网络监听的主机。

2　网络监听原理

一般而言,网络监听都是在局域网络进行的。IEEE 的 802 标准委员会和 802 项目组定义了两种主要的局域网传输方法—以太网(Ethernet)和令牌环(Token Ring)网。当前最常用的局域网环境是以太网。所以文章只对以太网下的网络监听原理进行分析。

以太网的控制方法是所谓的带有冲突检测的载波侦听多路存取(CSMA/CD),CSMA/CD 要求所有网络结点在电缆上监听所有包的传输,也就是说,传统的以太网是基于广播形式的。以太网协议的工作方式为将要发送的数据包发往连在一起的所有主机。在包头中包含应该接收数据包的主机的地址(MAC 地址)。正常情况下,虽然数据包到达了所有主机的网卡,但是只有网卡 MAC 地址与数据包中目的 MAC 地址一致的那台主机的协议栈才能接收数据包。然而,当主机将网卡设置为混杂模式时,无论数据包中的目的 MAC 地址是什么,主机的协议栈都将接收。这样,主机上的处理程序就可以得到子网内别的机器间的网络数据,并进行分析处理,这就是网络监听。

基金项目:国防科技预研跨行业综合技术项目"计算机病毒及其预防技术"(编号:15.7.2)
作者简介:贺龙涛,男,博士研究生,研究方向:计算机网络与信息安全,网络应用技术。方滨兴,博士生导师,研究方向:计算机网络与信息安全,并行计算,体系结构。

3 防止被监听的手段

要防止主机间传输的网络数据或密码口令不被有效监听，可以从两个方面来考虑：

(1)使用手段防止网络数据被非法监听。也就是说使用技术手段使得除了应该接受指定网络数据的主机网卡能够接收该网络数据外，别的主机网卡根本就不能就接收到该网络数据。使用的方法包括网络分段和网络交换技术：

网络分段是保证安全的一项重要措施，同时也是一项基本措施，其指导思想在于将非法用户与网络资源相互隔离，从而达到限制用户非法访问的目的。对于 TCP/IP 网络，可把网络分成若干 IP 子网，各子网间必须通过路由器、路由交换机、网关或防火墙等设备进行连接，利用这些中间设备(含软件、硬件)的安全机制来控制各子网间的访问。

网络交换技术，也就是使用交换机将传统的广播以太网替换成交换以太网，从根本上讲局域网通信变成了真正的点对点通信，从而杜绝了第三方监听的可能。这种技术越来越流行。

(2)在不能阻止网络通信被监听到的情况下，可以使用手段使监听者不能有效的获得要监听的信息。也就是说，即使监听者可以得到所有的网络通信包，但是他仍然不能获得有用的信息，这就需要进行加密传输。当前的加密传输可以分为以下几类：

针对特定的单一应用的加密方法。例如应用于 WWW 的 SSL(Secure Sockets Layer)；应用于 Email 的 PGP(Pretty Good Privacy)和 S/MIME(Secure MIME)；应用于远程登陆的 SSH (secure shell)。这些加密协议的最大特点就是工作在应用层，只对特定应用，不对现有的协议作重大修改。

针对认证机制的加密方法。例如传统的 Kerberos5，它提供通用的强认证机制；smart cards，它使用一次性口令技术 还有 SMB/CIFS 用于文件共享；以及 Stanford 的 SRP (Secure Remote Password)用于增强 telnet 与 ftp 服务的安全性。这些认证协议的特点是完全针对认证机制的，一般并不对信息内容进行加密。

针对网络传输的虚拟专用网 VPN (Virtual Private Network)。VPN 技术的核心是采用隧道技术，将企业专网的数据加密封装后，透过虚拟的公网隧道进行传输，从而防止敏感数据的被窃。VPN 工作在 IP 层，对所有应用提供加密服务。

4 对监听程序的检测

单纯被动的使用交换技术或者加密技术来防止信息被监听，并不能知道本局域网内是否运行着网络监听程序，这对局域网安全是一个极大的隐患。因此对网络监听程序进行检测的研究势在必行，以下对运行着网络监听程序的主机的特点进行分析：

(1) 主机的协议栈会处理那些目的 MAC 地址不是本机 MAC 地址或者广播地址的以太包。在通常情况下，网卡过滤和丢弃掉那些以太包，而只是将目的 MAC 地址是本机 MAC 地址或者广播地址的以太包传递给内核协议栈进行处理。然而在网卡处于混杂模式时，它会将所有接收到的数据都向内核协议栈提交，而很多操作系统内核的协议栈并不对底层提交的以太包的目的 MAC 地址进行检查或者只进行简单的检查。例如多种 LINUX 内核以及 NETBSD 都不进行检查，而 WINDOWS95，98，NT 的绝大部分网卡驱动程序则只检查 MAC 地址的第一个字节是否为 0xff 来判断数据包是否为广播包，而不是标准的 ff:ff:ff:ff:ff:ff，所以当接收到一个目的 MAC 地址为 ff:00:00:00:00:00，目的 IP 地址为本机的 ARP 包或者 IP 包，这些主机就会进行响应。

(2)有些监听程序(包括 tcpdump，sniffit，esniff，linsniff 等)会对监听到的数据包的 IP 地址进行反向域名解析。在执行反向解析时，网络监听程序就从被动监听工具转变为主动网络工具。而那些没有监视网络数据的主机则不会去解析这些无关的 IP 地址。

(3)当主机运行了监听程序时，网卡处于混杂模式，则所有到达网卡的以太包都会产生硬件中断来请求网卡驱动程序的执行，另外，所有的以太包都要传递给用户态的监听程序处理。因此，在网络负载极重的情况下，运行监听程序会大大降低主机性能。这样，运行监听程序的主机的负载必然会与网络负载同步，即当网络负载加重时，该主机的负载也会加重。而没有运行监听程序的主机的负载则不会明显随网络负载变化而变化。由以上的分析，有以下三种检测方法来检测局域网内是否运行了监听程序：

(1)MAC 检测。由以上的分析 1 可知，只需在发送一个正常的 IP 包(可以是 ICMP 应答请求包，也可以是 TCP SYN 请求包)给被检测的主机的时候，其以太包头的目的 MAC 不使用该主机的网卡 MAC，而是使用 ff:00:00:00:00:00 (如图 1 所示)。这样，如果该主机没有处于混杂模式，其内核协议栈就不会收到这个 IP 包，也就不会进行回应；而当该主机处于混杂模式时，其内核协议栈就会收到这个 IP 包，且由上边的分析知道他会将其作为一个正常的 IP 包进行处理，并进行回应。这样就可以检测出来局域网内哪些主机的网卡是处于混杂模式的，考虑到网卡处于混杂模式的主机一般都是在运行网络监听程序，可以认为，对 MAC 检测进行回应的主机都运行了网络监听程序。

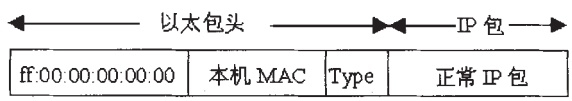

图 1 以目的 MAC 为 ff:00:00:00:00:00 发送 IP 包

(2)DNS 检测。这种检测就是引诱监听程序主动进行反向域名解析，同时检测者本身也监听本地网络，当发现有主机进行检测者指定的反向域名解析请求时，就认为它正在运行网络监听程序。具体来讲，就是向网络中不存在的主机发送 IP 包，同时监听本地网络的 DNS 请求来查看目标是否在请求解析那些不存在的主机 IP，从而发现运行监听程序的主机。

(3)负载检测。负载检测的技术难点在于如何远程检测系统反应时间。直接的选择是使用 ICMP 应答请求[7]，然而许多操作系统的 TCP/IP 协议栈总是对 ICMP 包尽快处理：一接收到 ICMP 应答请求包，系统就立即进行应答。这是由于 ICMP 处理模块处于 TCP/IP 协议栈的底层，执行的优先级较高，不存在被调度程序切换出去的可能，系统反应时间与系统的负载关系不明显。较好的选择是使用优先级比较低的 TCP 层以上的应用服务，比如 Telnet，Ftp 等进行反应时间检测。即对开放的 TCP 服务端口进行连接，并接收其第一次发送的数据包，然后纪录从发起连接到接收到数据包之间的时间，这个时间就基本能表征主机负载了。在实际实现中，可以使用往不存在的 IP 发送大量的 TCP 连接请求(SYN)包来加重网络负载(由于网络监听程序一般都是在接收到 SYN 包后初始化连接，所以 SYN 包也是加重监听程序负载的较好方法)，并比较大量发送 SYN 包时与

(下转 44 页)

成到 WEB 的 ASP 页面脚本中,进行用户请求处理及数据库访问工作。

3.2 数据交换技术

在系统中,数据交换是一个关键问题,在此,分两种情况分别处理:

(1)对只有查询功能的镜像站点:可以充分利用分布式数据库提供的数据复制功能,使用快照复制数据。Oracle 中的 snapshot 将主数据库中的源数据复制到多个目标,同时还能够以指定时间周期对目标数据进行刷新。快照可以是只读的,也可以是可更新的。在该系统的开发中,根据系统的实际情况,我们采用只读快照(其结构如图 5 示)方式将西安中心的数据复制到各镜像站点。具体步骤如下:

设计复制环境:确定要复制的数据对象;

建立快照站点的数据模式和数据库连接;

在主站建立必要的主站快照日志;

在快照站点建立快照;

创建快照站点的刷新组;

赋予应用程序必要的权限以访问快照。

(2)对于注册用户可以进行本地数据录入、维护的区域中心的镜像站点,以某个区域为数据交换中心,其他生产力中心定期上载本地数据,在数据交换中心通过交换程序将各区域的信息分类分文件存储,各区域再从数据交换中心下载不包含本地数据的交换文件,导入本地数据库。

4 结束语

该系统的开发建成,可以为全国上万家企业及个人提供信息服务,取得了明显的社会效益和经济效益。同时,该系统所采用的体系结构和技术,对于开发基于 Internet 的分布式应用系统也有很大的借鉴作用。(收稿日期:2001 年 4 月)

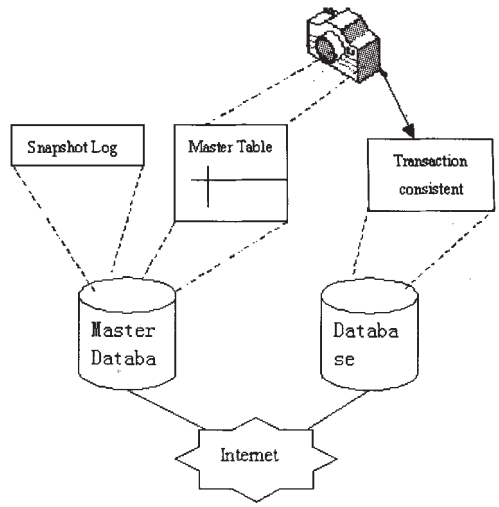

图 5 只读快照结构

参考文献

1.http://www.miscrosoft.com

2.Microsoft Corp.IIS ResourceKit 开发人员指南[M].北京希望电脑公司,1999

3.陈文博,夏长虹.DNA、组件对象模型与商务逻辑计算[N].计算机世界,1999.11

4.李晓军,李晓华,郑君等译.Oracle8 数据库管理员手册[M].机械工业出版社,1998

(上接 21 页)

不发送 SYN 包时的响应时间,当他们有显著差别时,则认为主机上运行了监听程序。

5 监听程序的反检测

上节提出的监测方法均是针对网络监听程序的某一特征的,这样,可以对网络监听程序进行改进,尽量消除自身特征,就可以逃避检测。以下对上节提出的检测方法,分别进行讨论:

(1)MAC 检测。MAC 检测攻击的不是监听程序本身,而是攻击监听程序所在主机的正常协议栈,也就是说,由于网卡混杂模式将所有到达本网卡的以太包都不加区分的向上层协议栈提交,这样当发现了这种包:以太包目的 MAC 地址不是本机 MAC 地址或广播地址,但该包的 IP 分片的目的 IP 却是本机 IP,协议栈会将这种包当作正常包一样处理,当检测者主机发送这种请求包时,就会收到网卡混杂模式的主机协议栈的回应。监听程序要防范检测,就应该在正常协议栈上做文章,可以在底层插入一个过滤模块,过滤掉所有非本 MAC 地址或者广播、组播的包,保证主机正常协议栈的运行。另外,既然监听程序可以捕获所有本广播网的包,就可以记录下所有本广播网的 MAC/IP 映射,在发现 MAC/IP 对异常的包时,就可以伪装这个发生异常的 IP(非本机 IP)回应,这就是说,监听程序可以对 MAC 检测进行欺骗。

(2)DNS 检测。这是由于网络监听程序将自身变为一个主动网络工具而导致的,只要将监听程序设计得不再进行反向域名解析就可以逃避检测。

(3)负载检测。既然监听程序一直在察看网络数据,则它可以实时计算网络负载,当发现负载急剧上升的时候(这正是负载检测方式的特征),监听程序可以将网卡设置为正常模式,并停止监听,睡眠一段时间后才重新进行监听并计算网络负载。这样,虽然监听程序丢失了部分网络数据,但是它可以在很大程度上避免被检测出来。

6 结束语

有了网络,就有了网络监听;有了网络监听,就有了加密传输来防止有效监听,以及检测监听程序;有了检测监听,就有了防止被检测到的监听程序。网络监听与反监听的对抗作为黑客攻击与网络安全斗争的重要方面,一直都在进行着,并将进行下去。(收稿日期:2001 年 4 月)

参考文献

1.Mark Taber.Maximum Security:A Hacker's Guide to Protecting Your Internet Site and Network[M].Macmillan Computer Publishing,1997

2.Brecht Claerhout.A short overview of IP spoofing[J].Phrack Magazine,1996,48(7)

3.Mark Crosbie,Gene Spafford.Defending A Computer System using Autonomous Agents.COAST Laboratory,1994

4.贺龙涛,方滨兴,云晓春等.利用 ARP 伪装在交换以太网捕包[J].网络安全技术与应用,2001(1):38-40

5.http://www.l0pht.com/antisniff/

6.David Wu,Frederick Wong.Remote Sniffer Detection[M].1998.12

7.http://www.securitysoftwaretech.com/antisniff/tech-paper.html