网络嗅探与监听围堵局域网中“ 耳朵 ”思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_BD_91_E7_BB_9C_E5_97_85_E6_c101_644307.htm 所谓“ 监听 ”技术，就是在互相通讯的两台计算机之间通过技术手段插入一台可以接收并记录通讯内容的设备，最终实现对通讯双方的数据记录。一般都要求用作监听途径的设备不能造成通讯双方的行为异常或连接中断。 一。 谁偷看了我的网络日记 检察员小洁从小就有写日记的习惯，毕业后上了工作岗位也不曾改变，无论工作多忙多累，每天晚上临近睡觉前她总会把今日发生的事情记录进日记本里，例如一些工作问题、心情想法、同事和上级的事情等等。小洁使用的是一个网站提供的网络日记本服务，她很喜欢那个宁静简洁的文字界面，偶尔没任务要忙或者心情不好的时候，她就会用院里的网络上去看自己以前写的日记。 这天小洁和往常一样来到办公室，却发现气氛不同往常了：同事们面对她的时候笑容很不自然，有几个女同事还偷偷对她指指点点的，小洁看过去时她们却又不说话了，她只好竖起耳朵偷听，隐隐约约听到一句“ …… 连别人还欠着50元没还她都写上去，这个人真…… ”，小洁的脸瞬间变得煞白：这不是她某天的日记内容吗?…… 究竟是谁把小洁的日记偷看了呢?你正在使用的局域网，又能真的很安全吗?小洁不知道，大院的局域网里，有一双耳朵正在悄悄的记录着她的电脑上发送和接收的一切信息…… 这双耳朵的名词被称为“ 网络嗅探 ”(Network Sniffing)或“ 网络监听 ”(Network Listening)，它并不是最近才出现的技术，也并非专门用在黑道上的技术，监听技术作为一种辅助手段，在协

助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用，因此一直倍受网络管理员的青睐并逐渐发展完善，所谓“ 监听 ”技术，就是在互相通讯的两台计算机之间通过技术手段插入一台可以接收并记录通讯内容的设备，最终实现对通讯双方的数据记录。一般都要求用作监听途径的设备不能造成通讯双方的行为异常或连接中断等，即是说，监听方不能参与通讯中任何一方的通讯行为，仅仅是“ 被动 ”的接收记录通讯数据而不能对其进行篡改，一旦监听方违反这个要求，这次行为就不是“ 监听 ”，而是“ 劫持 ”(Hijacking)了。 看了以上对于“ 监听 ”概念的描述，有人也许已经跃跃欲试了：我有网络，也有电脑，还有网络嗅探工具，那我能不能把某个收费电影站甚至国防部网站的账号密码记录下来呢?当然这也不是不可能，但是前提是你有足够能力在相关站点实体服务器的网关或路由设备上接入一个监听设备，否则凭一台你自己家里的计算机是无法实现的。这就是“ 监听 ”的弱点：它要求监听设备的物理传输介质与被监听设备的物理传输介质存在直接联系或者数据包能经过路由选择到达对方，即一个逻辑上的三方连接。能实现这个条件的只有以下情况： 1. 监听方与通讯方位于同一物理网络，如局域网 2. 监听方与通讯方存在路由或接口关系，例如通讯双方的同一网关、连接通讯双方的路由设备等 因此，直接用自己家里的计算机去嗅探国防部网站的数据是不可能的，你看到的只能是属于你自己领域的数据包，那些害怕自己在家里上网被远方的入侵者监听的朋友大可以松口气了(你机器上有木马的情况除外)，除非入侵者控制了你的网关设备，但这需要入侵者具有高级的入侵技术，而一个有高级技术的入侵者

会稀罕普通家庭用户是的一台计算机吗? 不可否认，“ 监听 ”行为是会对通讯方造成损失的，一个典型例子是在1994年的美国网络窃听事件，一个不知名的人在众多的主机和骨干网络设备上安装了网络监听软件，利用它对美国骨干互联网和军方网窃取了超过100000个有效的用户名和口令，引发了重大损失，而“ 监听 ”技术，就是在那次事件以后才从地下走向公开化的。 下面，我们来更深入一层了解如今最常见的网络监听。 二。 活跃在局域网里的“ 耳朵 ”们 由于前面说过的原因，嗅探技术不太能在公共网络设备上使用(仅指入侵行为的安装方式，因为网络管理员要在某个路由设备上设置监听是简单的事情)，所以当今最普遍的嗅探行为并不是发生在Internet上的，而是各个或大或小的局域网，因为它很显然满足监听技术需要的条件：监听方与通讯方位于同一物理网络。 1.写在前面：局域网内计算机通讯的概念和寻址 要发生监听事件，就必须有至少两台计算机处于通讯状态，而监听的实质也是数据的传输，这就要求窃听者自身也处于通讯网络中，而实现局域网通讯的基础是以太网模型(Ethernet)，它包括物理上的数据传输设备如网卡、集线器和交换机等，除此之外还需要逻辑上的软件、网络协议和操作系统支持，如网卡驱动程序、TCP/IP协议、NetBIOS协议、多种寻址和底层协议等，具备了这些条件，计算机才可以实现完整的通讯过程。 那么局域网内的计算机通讯是怎么进行的呢?计算机系统要传输数据时，是严格按照IEEE802.3标准的局域网协议进行的，而且还要结合 TCP/IP和OSI模型7层规范实施，所以数据是经过打包封装的，从高层到低层被分别加上相关数据头和地址，直至物理层把其转化为电平信号传送出去，而另一台

计算机则是通过逆向操作把数据还原的，这就引发了一个问题：寻址问题。 在局域网里，计算机要查找彼此并不是通过IP进行的，而是通过网卡MAC地址(也被称为以太网地址)，它是一组在生产时就固化的全球唯一标识号，根据协议规范，当一台计算机要查找另一台计算机时，它必须把目标计算机的IP通过ARP协议(地址解析协议)在物理网络中广播出去，“ 广播 ”是一种让任意一台计算机都能收到数据的数据发送方式，计算机收到数据后就会判断这条信息是不是发给自己的，如果是，就会返回应答，在这里，它会返回自身地址，这一步被称为“ ARP寻址 ”。当源计算机收到有效的回应时，它就得知了目标计算机的MAC地址并把结果保存在系统的地址缓冲池里，下次传输数据时就不需要再次发送广播了，这个地址缓冲池会定时刷新重建，以免造成数据老旧和错误。当前活动的ARP表可以使用arp a命令查看。 话题回到数据被打包成为比特流的最后两层，在这里有一个关键部分被称为“ 数据链路层 ”，数据在网络层形成IP数据报，再向下到达数据链路层，由数据链路层将IP数据报分割为数据帧，增加以太网包头，再向下一层发送。以太网包头中包含着本机和目标设备的MAC地址，也就是说，链路层的数据帧发送时，是依靠以太网地址而非IP地址来确认的，网卡驱动程序不会关心IP数据报中的目标地址，它所需要的仅仅是MAC地址，而MAC地址就是通过前面提到的 ARP寻址获得的。简单的说，数据在局域网内的最终传输目标地址是对方网卡的MAC地址，而不是IP地址，IP地址在局域网里只是为了协助系统找到MAC 地址而已。 而就是因为这个寻址结构，最终导致了监听实现的发生。 那么，发生在Internet上的监听又

是怎么进行的呢?Internet并不采用MAC地址寻址，因此不可能发生类似局域网内的监听案例，实际上，Internet上的监听是因为数据必须通过的路由网关路由设备被做了手脚，不属于本文讨论范围。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com