网络监听攻击技术数据包扑捉与协议分析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/284/2021_2022__E7_BD_91_E7_BB_9C_E7_9B_91_E5_c101_284176.htm 在网络中，当信息进行传播的时候，可以利用工具，将网络接口设置在监听的模式，便可将网络中正在传播的信息截获或者捕获到，从而进行攻击。网络监听在网络中的任何一个位置模式下都可实施进行。而黑客一般都是利用网络监听来截取用户口令。比如当有人占领了一台主机之后，那么他要再想将战果扩大到这个主机所在的整个局域网话，监听往往是他们选择的捷径。很多时候我在各类安全论坛上看到一些初学的爱好者，在他们认为如果占领了某主机之后那么想进入它的内部网应该是很简单的。其实非也，进入了某主机再想转入它的内部网络里的其它机器也都不是一件容易的事情。因为你除了要拿到他们的口令之外还有就是他们共享的绝对路径，当然了，这个路径的尽头必须是有写的权限了。在这个时候，运行已经被控制的主机上的监听程序就会有大收效。不过却是一件费神的事情，而且还需要当事者有足够的耐心和应变能力。网络监听的原理 Ethernet（以太网，它是由施乐公司发明的一种比较流行的局域网技术，它包含一条所有计算机都连接到其上的一条电缆，每台计算机需要一种叫接口板的硬件才能连接到以太网）协议的工作方式是将要发送的数据包发往连接在一起的所有主机。在包头中包括有应该接收数据包的主机的正确地址，因为只有与数据包中目标地址一致的那台主机才能接收到信息包，但是当主机工作在监听模式下的话不管数据包中的目标物理地址是什么，主机都将可以接收到。

许多局域网内有十几台甚至上百台主机是通过一个电缆、一个集线器连接在一起的，在协议的高层或者用户来看，当同一网络中的两台主机通信的时候，源主机将写有目的的主机地址的数据包直接发向目的主机，或者当网络中的一台主机同外界的主机通信时，源主机将写有目的的主机IP地址的数据包发向网关。但这种数据包并不能在协议栈的高层直接发送出去，要发送的数据包必须从TCP/IP协议的IP层交给网络接口，也就是所说的数据链路层。网络接口不会识别IP地址的。在网络接口由IP层来的带有IP地址的数据包又增加了一部分以太祯的祯头的信息。在祯头中，有两个域分别为只有网络接口才能识别的源主机和目的主机的物理地址这是一个48位的地址，这个48位的地址是与IP地址相对应的，换句话说就是一个IP地址也会对应一个物理地址。对于作为网关的主机，由于它连接了多个网络，它也就同时具备有很多个IP地址，在每个网络中它都有一个。而发向网络外的祯中继携带的就是网关的物理地址。 Ethernet中填写了物理地址的祯从网络接口中，也就是从网卡中发送出去传送到物理的线路上。如果局域网是由一条粗网或细网连接成的，那么数字信号在电缆上传输信号就能够到达线路上的每一台主机。再当使用集线器的时候，发送出去的信号到达集线器，由集线器再发向连接在集线器上的每一条线路。这样在物理线路上传输的数字信号也就能到达连接在集线器上的每个主机了。当数字信号到达一台主机的网络接口时，正常状态下网络接口对读入数据祯进行检查，如果数据祯中携带的物理地址是自己的或者物理地址是广播地址，那么就会将数据祯交给IP层软件。对于每个到达网络接口的数据祯都要进行这个过程

的。但是当主机工作在监听模式下的话，所有的数据祯都将被交给上层协议软件处理。 当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网的时候，那么要是有一台主机处于监听模式，它还将可以接收到发向与自己不在同一个子网（使用了不同的掩码、IP地址和网关）的主机的数据包，在同一个物理信道上传输的所有信息都可以被接收到。
在UNIX系统上，当拥有超级权限的用户要想使自己所控制的主机进入监听模式，只需要向Interface（网络接口）发送I/O控制命令，就可以使主机设置成监听模式了。而
在Windows9x的系统中则不论用户是否有权限都将可以通过直接运行监听工具就可以实现了。 在网络监听时，常常要保存大量的信息（也包含很多的垃圾信息），并将对收集的信息进行大量的整理，这样就会使正在监听的机器对其它用户的请求响应变的很慢。同时监听程序在运行的时候需要消耗大量的处理器时间，如果在这个时候就详细的分析包中的内容，许多包就会来不及接收而被漏走。所以监听程序很多时候就会将监听得到的包存放在文件中等待以后分析。分析监听到的数据包是很头疼的事情。因为网络中的数据包都非常之复杂。两台主机之间连续发送和接收数据包，在监听到的结果中必然会加一些别的主机交互的数据包。监听程序将同一TCP会话的包整理到一起就相当不容易了，如果你还期望将用户详细信息整理出来就需要根据协议对包进行大量的分析。Internet上那么多的协议，运行进起的话这个监听程序将会十分的大哦。 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