

章 监听网络线路

2.1 混杂模式

2.2 在集线器连接网络中嗅探

2.3 在交换式网络中进行嗅探

2.3.1 端口镜像

2.3.2 集线器输出

2.3.3 使用网络分流器

2.3.4 ARP 缓存污染

2.4 在路由网络环境中进行嗅探

2.5 部署嗅探器的实践指南

章 Wireshark 入门

3.1 Wireshark 简史

3.2 Wireshark 的优点

3.3 安装 Wireshark

3.3.1 在微软 Windows 系统…

3.3.2 在 Linux 系统中安装

3.3.3 在 Mac OS X 系统中安装

3.4 Wireshark 初步入门

3.4.1 第一次捕获数据包

3.4.2 Wireshark 主窗口

3.4.3 Wireshark 首选项



Wireshark 数据包分析实战（第 3 版）
作者：[美] 克里斯·桑德斯（Chris Sander…

13%

扫码下载知

2.3.2 集线器输出

另一种在交换式网络中捕获目标设备通信流量的方式是集线器输出。用这种技巧，你需要将目标设备和分析系统分段到同一网络段中，然后把它们直接插入到一个集线器上。

许多人认为集线器输出根本就是一种作弊方法，不过，它在你不能过端口镜像但仍对目标设备接入的交换机有着物理访问的时候，真的是一个美的解决方案。为了进行集线器输出，你所需要的就是一个集线器和几根线。在你找齐了硬件之后，就可以按照如下操作步骤进行连接了。

- (1) 找到目标设备所连接的交换机，并将目标设备连接网线从交换机拔掉。
- (2) 将目标设备的网线插入到你的集线器上。
- (3) 使用另一根网线，将你的嗅探分析器也连接到集线器上。
- (4) 从你的集线器连接一根网线到交换机上，将集线器连接到网络上

现在你已经将目标设备和你的嗅探分析器连接到了同一个广播域中，有从你的目标设备流入流出的网络流量都将在集线器中广播，从而让你的探分析器可以捕获到这些数据包，如图 2-6 所示。

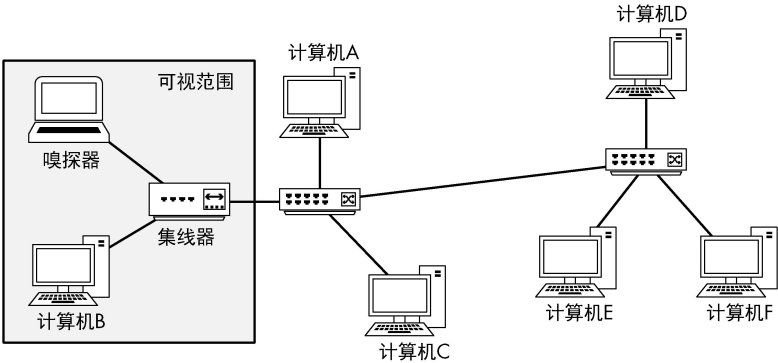


图 2-6 将你的目标设备通过集线器输出，与嗅探分析器连接在一起

在大多数情况下，集线器输出会将目标设备的全双工变成半双工。尽这种方法并不是进行网络线路监听最彻底的方法，但在交换机不支持端口像时它可能是你唯一的选择。但是，请记住的是，你的集线器同样需要一电源线连接，而某些情况下你却很难找到。


知乎 书店	查看目录	上一章	下一章	图书详情	返回书架
章 监听网络线路					
2.1 混杂模式					
2.2 在集线器连接网络中嗅探					
2.3 在交换式网络中进行嗅探					
2.3.1 端口镜像					
2.3.2 集线器输出					
2.3.3 使用网络分流器					
2.3.4 ARP 缓存污染					
2.4 在路由网络环境中进行嗅探					
2.5 部署嗅探器的实践指南					
章 Wireshark 入门					
3.1 Wireshark 简史					
3.2 Wireshark 的优点					
3.3 安装 Wireshark					
3.3.1 在微软 Windows 系统…					
3.3.2 在 Linux 系统中安装					
3.3.3 在 Mac OS X 系统中安装					
3.4 Wireshark 初步入门					
3.4.1 第一次捕获数据包					
3.4.2 Wireshark 主窗口					
3.4.3 Wireshark 首选项					

找到「真正的」集线器

当进行集线器输出时，你需要确保你使用的设备是一个真正的集线器，而不是虚假标记的交换机。有几家网络硬件厂商有着营销的坏习惯，会把一些低级别的交换机当作集线器进行出售。如果你使用的并不是一个可信的经过测试的集线器，那么你将只会看到你自己的流量，而不是目标设备的流量。

当你找到一个集线器时，需要对它进行测试，来确保它确实是一个集线器。如果是的话，它绝对是值得你收藏的了！确定一个设备是否真的是集线器的最好方法，就是连上两台电脑，然后看这两台电脑是否能嗅探对方与网络其他设备之间的网络通信。如果能监听到的话，那它就是一款真正的集线器了。

由于集线器已经是老古董了，因此它们早就不再被大规模生产了。你几乎不可能从市面上买到真正的集线器了。所以你需要发挥点创意来找到一个。一个很好的来源往往是在当地学校的二手交易市场。公立学校在处理老旧设备之前，都必须尝试进行二手拍卖交易，而他们经常有一些很古老的硬件设备。我曾经见过有人从二手交易市场上仅仅花了不到一顿快餐的钱就买到了好几台集线器。此外，eBay 也是一个集线器的良好来源，但你也需要留意，有可能你也会遇到将交换错误标识成集线器的情况。



Wireshark 数据包分析实战（第 3 版）

作者：[美]克里斯·桑德斯（Chris Sander…

13%

扫码下载知