

第 2 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 使用网络分流量

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

第 3 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

2.1 混杂模式

你需要一个支持混杂模式驱动的网卡，才可能在网络上嗅探数据包。混杂模式是什么呢？实际上它是一种允许网卡能够查看到所有流经网络线路数据包驱动模式。

正如你在第 1 章了解到的那样，由于在网络上有一类广播流量，因此对于客户端来说，接收到并非以它们的地址作为目标的数据包是很常见的。来对给定 IP 地址解析对应 MAC 地址的 ARP 协议（在任何网络上都是一个键组成部分）便是一个很好的例子，它能够说明有些网络流量并非是发往指定的目标地址。为了找到对应的 MAC 地址，ARP 协议会发送一个广播发出到广播域中的每个设备，然后期望正确的客户端将做出回应。

一个广播域（也就是一个网络段，其中任何一台计算机都可以无须经路由器，直接传送数据到另一台计算机）是由几台计算机组成的，但广播域中仅仅只有一台客户端应该对传输的 ARP 广播请求包感兴趣。而一旦网络上的每台计算机都处理和回应 ARP 广播包的话，那么网络的性能将变得非常的糟糕。

因此，其他网络设备上的网卡驱动会识别出这个数据包对于它们来说没有任何用处，于是选择将数据包丢弃，而不是传递给 CPU 进行处理。将标不是这台接收主机的数据包进行丢弃可以显著地提高网络处理性能，但对于数据包分析师来说并不是个好消息。作为分析师，我们通常需要看到网络上传输的每一个数据包，这样我们才不用担心会丢失掉任何关键的信息。

我们可以使用网卡的混杂模式来确保能够捕获所有的网络流量。一旦工作在混杂模式下，网卡将会把每一个它所看到的数据包都传递给主机的处理器，而无论数据包的目的地址是什么。一旦数据包到达 CPU，它就可以被一个数据包嗅探软件捕获并进行分析。

现在的网卡一般都支持混杂模式，Wireshark 软件包中也包含了 libpcap / WinPcap 驱动，这让你能够很方便地在 Wireshark 软件界面上将网卡直接切换到混杂模式上。（我们将在第 3 章里介绍更多的 libpcap / WinPcap 的内容。）

为了学习本书中的数据包分析技术，你必须要有个支持使用混杂模式的网卡与操作系统。在你只想看到发往你运行嗅探软件主机 MAC 地址的




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

12%

扫码下载知

知乎 书店	查看目录	上一章	下一章	图书详情	返回书架
在大多数操作系统（包括 Windows）上，要想使用一个混杂模式的网下，你就必须要提升用户权限到管理员级别。如果你不能在一个系统上合法地获得这些权限，那就不应该在这台系统上对所在网络进行任何方式的数据包嗅探。					
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…

12%

扫码下载知