

书的赞誉

么购买本书

与方法

使用本书

示例捕获文件

科技基金会

与支持

章 数据包分析技术与网络基础

1.1 数据包分析与数据包嗅探器

1.1.1 评估数据包嗅探器

1.1.2 数据包嗅探器工作过程

1.2 网络通信原理

1.2.1 协议

1.2.2 七层 OSI 参考模型

1.2.3 OSI 参考模型中的数据...

1.2.4 数据封装

1.2.5 网络硬件

1.3 流量分类

1.3.1 广播流量

1.1.1 评估数据包嗅探器

当你选择一款数据包嗅探器时，需要考虑的因素很多，包括以下几点


支持的协议：数据包嗅探器对协议解析的支持范围是各不相同的，大部分通常都能解析常见的网络协议（如 IPv4 和 ICMP）、传输层协议（如 TCP 和 UDP），甚至一些应用层协议（如 DNS 和 HTTP）。然而，它们可能并不支持一些非传统的或新的协议（如 IPv6、SMBv2、SIP 等）。在选择一款探器时，需要确保它能够支持你所要用到的协议。

用户友好性：考虑数据包嗅探器的界面布局、安装的容易度，以及操作流程的通用性。你选择的嗅探器应该适合你的专业知识水平。如果你的数据包分析经验还很少的话，可能需要避免选择那些更高级命令行嗅探器，比如 Tcpdump；另一方面，如果你拥有丰富的经验，你可能会觉得这类命令程序更具有吸引力。在逐步积累数据包分析经验时，你甚至会发现组合使用多种数据包嗅探器软件将更有助于适应不同的应用场景。

费用：数据包嗅探器最突出的优点是拥有很多能够与任何商业产品相媲美的免费工具。商业产品与其他替代品之间的一个明显的区别是它们的报引擎，商业产品通常包括各种形式的花哨的报告生成模块，而在免费软件则通常缺乏。

技术支持：即使你已经掌握了嗅探软件的基本用法，但在遇到一些新题时仍需要技术支持。在评估技术支持时，你可以寻找开发人员文档、论坛和邮件列表。虽然对于一些像 Wireshark 这样的免费软件可能缺乏一开发人员文档，但使用这些应用软件的社区往往可以填补这些空白。使用和贡献者社区会提供一些讨论区、维基、博客，来帮助你获得更多关于数据包嗅探器的使用方法。

操作系统支持：不幸的是，并不是全部数据包嗅探器都支持所有的操作系统平台。你需要选择一款嗅探器，能够支持所有你将要工作的操作系统。如果你是一位顾问，有时要在大多数操作系统平台上进行数据包捕获和分析，那么你就需要一款能够在大多数操作系统平台上运行的嗅探器。你还要留意，有时你会在一台机器上捕获数据包，然后在另一台机器上分析它们。操作系统之间的差异，可能会迫使你在不同的设备上使用不同的嗅探软件。



Wireshark 数据包分析实战（第 3 版）
作者：[美]克里斯·桑德斯（Chris Sander...
6%

扫码下载知

