附录 A

延伸阅读

数据包分析工具不仅只有 Wireshark，还有一大堆好用的工具，可以在解决网络缓慢、网络安全等常规问题及分析无线网络问题时大显身手。本章列出了一些有用的数据包分析工具，以及其他数据包分析的学习资源。

A.1 数据包分析工具

除了 Wireshark 之外，还有一些实用的数据包分析工具。在这里，我会介绍一些我认为最有用的。

A.1.1 tcpdump 和 Windump

虽然 Wireshark 很流行，但它可能没有 tcpdump 使用广泛。考虑到一些人群对数据包捕获和分析的实际需求，tcpdump 是完全基于文本的。

尽管 tcpdump 缺少图形特性，但它处理海量数据时非常可靠。因为你可以用管道将它的输出重定向输入给其他命令，比如 Linux 的 sed 和 awk。随着对数据包分析的深入钻研，你会发现 Wireshark 和 tcpdump 都很有用。你可以从 http://www.tcpdump.org/下载 tcpdump。

Windump 只是 tcpdump 在 Windows 平台的版本而已。你可以从 http://www.winpcap.org/windump/下载到它。

A.1.2 Cain & Abel

第 2 章已经讨论过，Cain & Abel 是 Windows 平台上最好的 ARP 缓存中毒攻击工具之一。Cain & Abel 实际上是一个非常健壮的工具套件，你一定能发现其他用途。它可以从 http://www.oxid.it/cain.html 取得。

A.1.3 Scapy

Scapy 是一个非常强大的 Python 库，允许使用基于命令行脚本的方法创建、修改数据包。简单地说，Scapy 是已知最强大、最灵活的数据包操纵程序。你可以在 http://www.secdev.org/projects/scapy/读到更多有关 Scapy 的资料，也可以下载 Scapy 并浏览 Scapy 的示例脚本。

A.1.4 Netdude

如果你不需要像 Scapy 那样高级的工具，那么 Netdude 是 Linux 下一个好的替代品。虽然 Netdude 功能有限，但它提供了图形用户界面，因而出于研究目的，需要创建、修改数据包时，它显得极其方便。图 A-1 演示了使用 Netdude 的一个例子。你可以从 http://netdude.sourceforge.net/下载到 Netdude。

A.1.5 Colasoft Packet Builder

如果你是 Windows 用户，并且想要与 Netdude 类似的 GUI，那你可以考虑使用 Colasoft Packet Builder，一款超棒的免费工具。Colasoft 也提供了一个易用的用于数据包创建和修改的 GUI。你可以从 http://www.colasoft.com/packet_builder/下载到它。

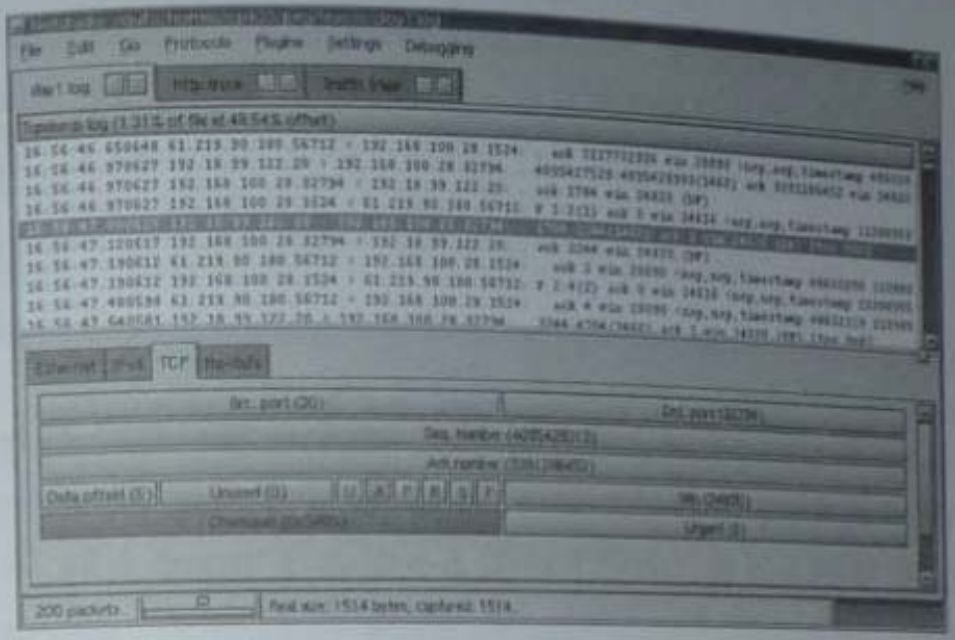

图 A-1　在 Netdude 上修改数据包

A.1.6 CloudShark

CloudShark（由 QA Café开发）是我最喜爱的工具之一，可以用它在线分享数据包捕获记录。如图 A-2 所示，CloudShark 网站可以在浏览器里以 Wireshark 的方式显示网络捕获文件。你可以上传捕获文件，并将链接发送给同事，以便共同分析。

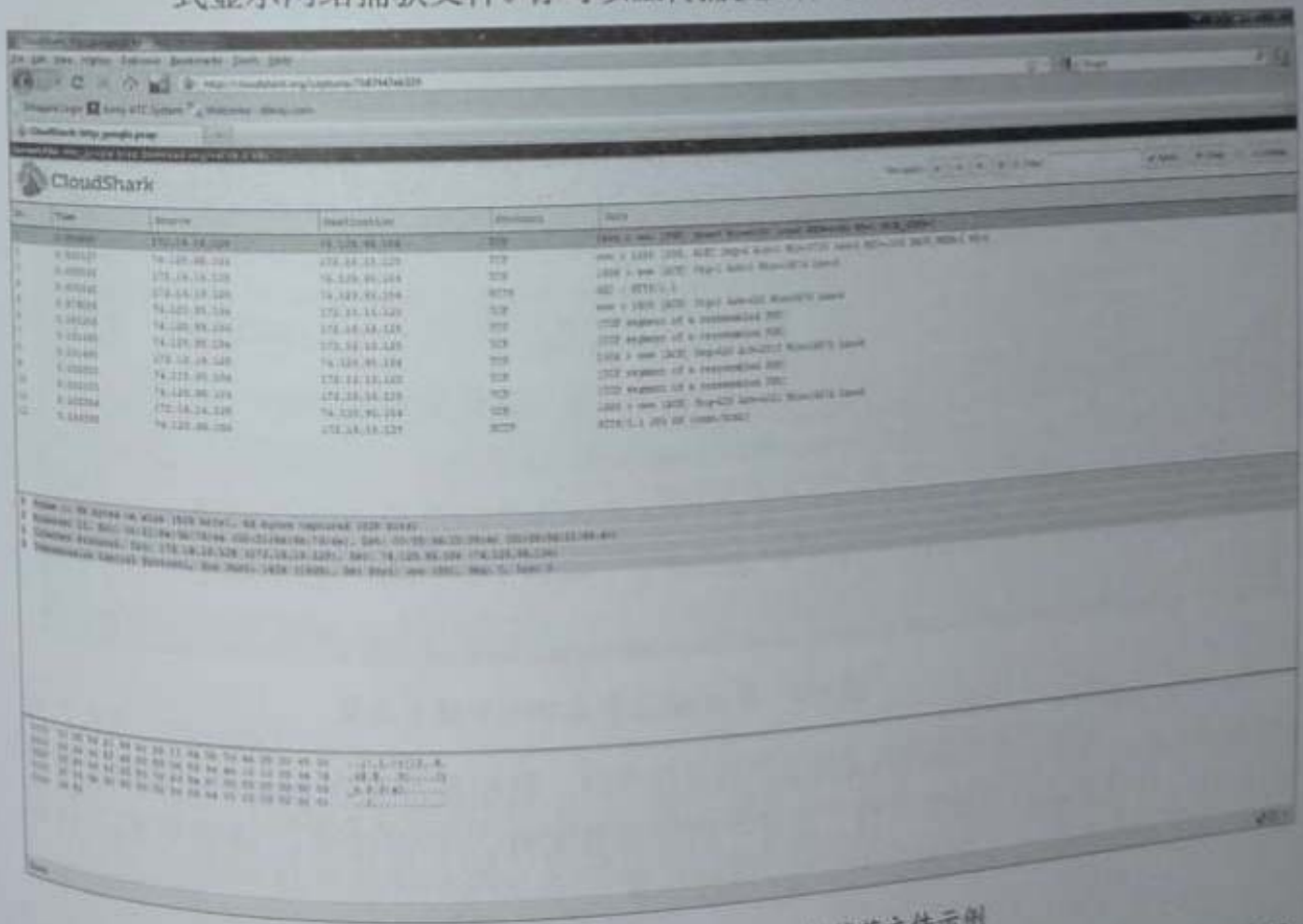

图 A-2　用 CloudShark 查看一个捕获文件示例

关于 CloudShark，我最赞赏的是它不需要注册，并能通过 URL 直接链接获取。这意味着，当我在博客上发布一个 PCAP 文件的链接时，其他人只需要单击就能查看数据包，而不需要下载文件后，再用 Wireshark 打开。

你可以通过 http://www.cloudshark.org/访问 CloudShark。

A.1.7 pcapr

pcapr 是 Mu Dynamics 的人创建的一个非常健壮的用于分享 PCAP 文件的 Web 2.0 平台。在撰写本文时，pcapr 包含了将近 3000 个 PCAP 文件，涉及 400 多种不同协议的例子。图 A-3 显示了 pcapr 上的 DHCP 流量捕获的例子。

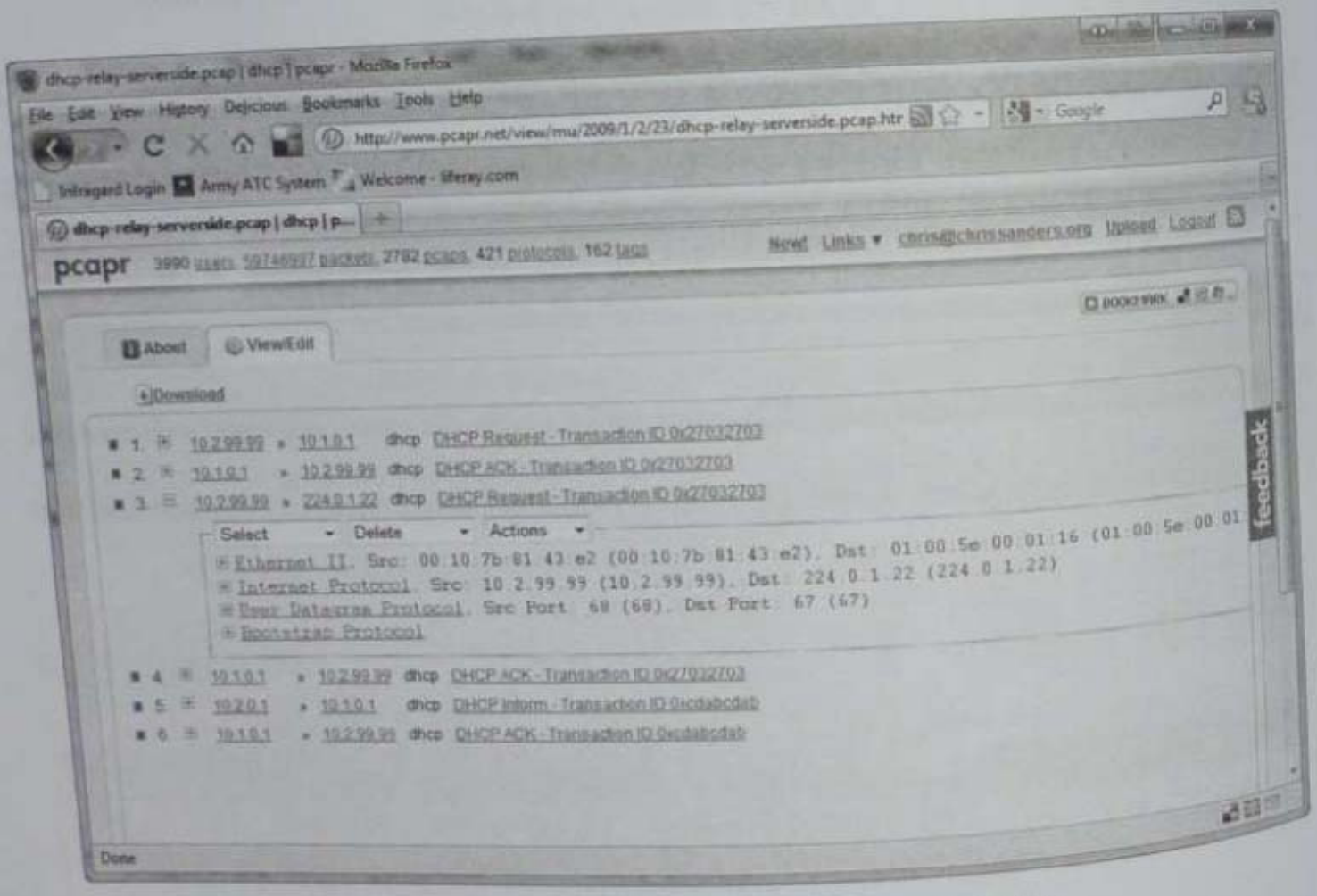

图 A-3 在 pcapr 上查看 DHCP 流量捕获

每次要查找某种确定类型的通信样例时，我都是首先在 pcapr 上搜索。如果你在自己的试验中创建了大量不同的捕获文件，不要犹豫，请将它们上传到 http://www.pcapr.net/，与 pcapr 社区分享。

A.1.8 NetworkMiner

NetworkMiner 是一款主要用于网络取证的工具，但我发现它在其他一些情形下也非常实用。尽管它也可以用来捕获数据包，但它的强项在于如何解析数据包。NetworkMiner 会检测 PCAP 文件中网络各端的操作系统类型，并将文件解析成主机间的会话。它甚至允许你直接从捕获记录中提取传输的文件。NetworkMiner 可以从 http:// networkminer.sourceforge.net/免费下载。

A.1.9 Tcpreplay

每当我有一堆数据包需要在线路上重传并观察设备如何响应它们时，我就用 Tcpreplay 来执行这个任务。Tcpreplay 专门设计用来重传 PCAP 文件里的数据包。可以从 http://tcpreplay.synfin.net/下载它。

A.1.10 ngrep

如果你熟悉 Linux，毫无疑问，你肯定用过 grep 搜索数据。Ngrep 与之非常相似，允许你在 PCAP 数据上执行特定搜索。当捕获和显示过滤器都无法实现目标，或者实现太复杂时，就使用 ngrep。你可以在 http:// ngrep.sourceforge.net/读到更多有关 ngrep 的信息。

A.1.11 libpcap

如果你计划开发一款应用程序，来进行一些高级的数据包解析，或是创建处理数据包，那你要对 libpcap 非常熟悉。简而言之，libpcap 是一个用于网络流量捕获的可移植的 C/C++库。Wireshark、tcpdump，以及其他大部分数据包分析工具都在一定层次上依赖于 libpcap。你可以在 http://www.tcpdump.org/读到更多有关 libpcap 的信息。

A.1.12 hping

hping 是你武器库中应有的“瑞士军刀”之一。hping 是一个命令行的数据包操纵和传输工具。它支持各种各样的协议，反应非常快且直观。你可以从 http://www.hping.org/下载 hping。

A.1.13 Domain Dossier

如果你需要查询域名或 IP 地址的注册信息，那 Domain Dossier 正合你意。它快速、简单、有效。你可以在 http://www.centralops.net/co/DomainDossier.aspx 访问到 Domain Dossier。

A.1.14 Perl 和 Python

Perl 和 Python 虽然不是工具，但却是值得留意的脚本语言。当你熟练于数据包分析时，你会遇到没有自动化工具满足要求的情况。在那些情况下，首选 Perl 和 Python 语言编写工具，以在数据包上做些有趣的事情。对于大部分应用程序，我通常使用 Python，但这只是个人选择。

A.2 数据包分析资源

从 Wireshark 的主页到教程、博客，有很多可用的数据包分析资源。我将在此列出我最喜欢的一些。

A.2.1 Wireshark 主页

与 Wireshark 有关的首要资源就是它的主页：http://www.Wireshark.org/。主页包括软件文档、一个非常有用的包含了捕获文件样例的 wiki，以及 Wireshark 邮件列表的注册信息。

A.2.2 SANS 安全入侵检测深入课程

作为一名 SANS 导师，我可能会有点偏袒，但我真不认为这个星球上有比“SANS SEC 503：Intrusion Detection In-Depth”更好的数据包分析课程。这个课程集中于数据包分析的安全方面。即便你不是重点关注安全，该课程前两天提供的对数据包分析和对 tcpdump 的介绍也是我所见最好的。

该课程由我的两位数据包分析英雄 Mike Poor 和 Judy Novak 讲授。它每年面授好几次。若你的旅行经费有限，没关系，该课程也通过基于 web 的点播格式在线讲授。

你可以在 http://www.sans.org/阅读到更多关于 SEC 503 和其他 SANS 课程的

信息。

A.2.3 Chris Sanders 的博客

我没有太多时间写博客，但偶尔也会在我的博客 http://www.chrissanders.org/ 上写一些有关数据包分析的文章。如果没有别的，我的博客就作为链接到我写的其他文章和书籍的门户，另外它也提供了我的联系方式。

A.2.4 Packetstan 博客

Mike Poor 和 Judy Novak 的博客是我目前最喜欢的与数据包相关的博客。他们的网站 http://www.packetstan.com/包含了一些有趣流量的分类，并且每一篇内容都是 A+级别的。Mike 和 Judy 在他们领域是做得最好的两位，给了我很大鼓舞。

A.2.5 Wireshark 大学

你会发现，Laura Chappell 是最多产的 Wireshark 布道者之一。她的网站包含了很多 Wireshark 使用技巧，以及她的著作 *Wireshark Network Analysis* 的信息和她教授的课程。在 http://www.Wiresharktraining.com/能找到更多相关信息。

A.2.6 IANA

互联网编号分配机构（Internet Assigned Numbers Authority，IANA）的网站是 http:// www.iana.org/，它负责监督为北美分配 IP 地址和协议号码。它的网站提供了一些有价值的参考工具，比如查找端口号、查看有关顶级域名的信息、以及浏览合作网站查阅 RFC 文档。

A.2.7 TCP/IPIllustrated（Addison-Wesley）

对生活在数据包层次的人而言，Richard Stevens 博士撰写的系列图书是书架上的主要书目，已被多数人奉为 TCP/IP 圣经。这是我最喜欢的 TCP/IP 书籍，也是我写作本书时经常参考的文献。

A.2.8 TheTCP/IP Guide（No Starch 出版社）

在 TCP/IP 领域里，我最喜欢的另一本书是 Charles Kozierok 写的。这本巨著厚达 1000 多页，内容非常详细，并且为视觉型学习者准备了大量很棒的图表。