3.4.6 配置方案

章玩转捕获数据包

4.1 使用捕获文件

4.1.1 保存和导出捕获文件

4.1.2 合并捕获文件

4.2 分析数据包

4.2.1 保存和导出捕获文件

4.2.2 标记数据包

4.2.3 打印数据包

4.3 设定时间显示格式和相对参考

4.3.1 时间显示格式

4.3.2 数据包的相对时间参考

4.3.3 时间偏移

4.4 设定捕获选项

4.4.1 输入标签页

4.4.2 输出标签页

4.4.3 选项标签页

4.5 过滤器

4.5.1 捕获过滤器

4.5.2 显示过滤器

4.5.3 保存过滤器规则

4.5.4 在工具栏中增加显示过…

章 Wireshark 高级特性

5.1 端点和网络会话

5.1.1 查看端点统计

4.2.1 保存和导出捕获文件

如果想要找到符合特定条件的数据包,那么可以按 Ctrl-F 组合键打开 Find Packet 条形框,如图 4-4 方框内所示。这个条形框应该在过滤框和'列表窗口之间。

Pa	cket list	¥	Narrow & Wide	▼ Case sensiti	ve [Display filter	▼ tcp Find Cancel
No.		Time	Source	Destination	Protocol	Length	Info
Г	1	0	172.16.16.128	74.125.95.104	TCP	66	1606 → 80 [SYN] Seq=2082691767 Win=8192 Len=0 MSS=1460 WS=4 SACK
	2	0	74.125.95.104	172.16.16.128	TCP	66	80 → 1606 [SYN, ACK] Seq=2775577373 Ack=2082691768 Win=5720 Len=
	3	0	172.16.16.128	74.125.95.104	TCP	54	1606 → 80 [ACK] Seq=2082691768 Ack=2775577374 Win=16872 Len=0
	4	0	172.16.16.128	74.125.95.104	HTTP	681	GET / HTTP/1.1

图 4-4 在 Wireshark 中根据条件查找数据包——在这个案例中,只有数据包符号 达式 TCP 才会被显示出来

这个对话框为查找数据包提供了3个选项。

- Display filter 选项允许你通过输入表达式进行筛选,并只找出那些满足该达式的数据包,就像在图 4-4 中所使用的那样。
- Hex Value 选项使用你所输入的十六进制数,对数据包进行搜索。
- String 选项使用你所输入的字符串,对数据包进行搜索。你可以在搜索面上设置是否区分大小写和其他的格式。

表 4-1 给出了上述几种搜索类型的例子。

表 4-1 用来查找数据包的搜索类型

搜索类型	例子
Display Filter	not ip
	ip.addr==192.168.0.1
	arp
Hex value	00:ff
	ff:ff

4/29/2021

3.4.6 配置方案

章玩转捕获数据包

4.1 使用捕获文件

4.1.1 保存和导出捕获文件

4.1.2 合并捕获文件

4.2 分析数据包

4.2.1 保存和导出捕获文件

4.2.2 标记数据包

4.2.3 打印数据包

4.3 设定时间显示格式和相对参考

4.3.1 时间显示格式

4.3.2 数据包的相对时间参考

4.3.3 时间偏移

4.4 设定捕获选项

4.4.1 输入标签页

4.4.2 输出标签页

4.4.3 选项标签页

4.5 过滤器

4.5.1 捕获过滤器

4.5.2 显示过滤器

4.5.3 保存过滤器规则

4.5.4 在工具栏中增加显示过…

章 Wireshark 高级特性

5.1 端点和网络会话

5.1.1 查看端点统计

4.2.1 保存和导出捕获文件 - Wireshark 数据包分析实战(第 3 版) - 知乎书店

搜索类型	例子
	00:AB:B1:f0
String	Workstation1
	User8
	Domain

在确定选项并在文本框中输入搜索关键词之后,单击 Find,就会找到满足该关键词的第一个数据包。如果想要找到下一个匹配的数据包,则接 Ctrl-N 组合键;想要找到前一个,则按 Ctrl-B 组合键。