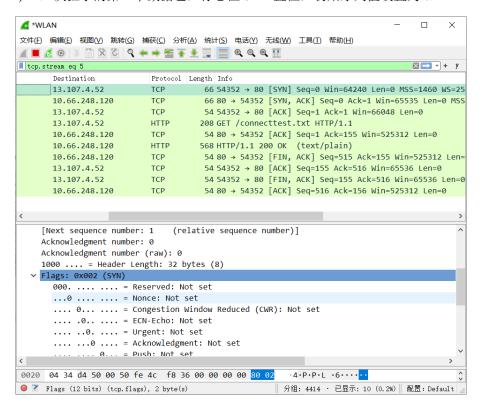
实验名称: TCP 协议分析 实验台号: 实验时间: 实验小组:张楷 实验目的: •了解 TCP 报文段的结构; •掌握 TCP 数据流追踪的方法; •理解 TCP 三次握手的基本过程; •理解 TCP 连接终止的基本过程; •认识 TCP 重置: •理解 TCP 可靠数据传输的基本原理。 实验环境说明: PC 实验过程、步骤(可另附页、使用网络拓扑图等辅助说明)及结果: 一、TCP 的连接。 1) 用 Wireshark 过滤显示 SYN ACK 置位数据包。从源端口为 80 可见是 HTTP 流。 *WLAN 文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H) 🛾 📕 👩 🔞 间 🖺 🛣 🧗 🤇 🧢 👄 🖺 🛜 💆 📃 🗨 🔍 Q Q 🗨 🎹 tcp. flags. syn ==1 && tcp. flags. ack==1 No. Time Destination Protocol Length Info Source 119 24.409992 66 443 → 54351 [S' 96.6.229.57 10.66.248.120 187 32,548101 10.66.248.120 66 80 → 54352 [SYI 13,107,4,52 TCP 66 443 → 54354 [S' 573 77.871721 40.81.31.55 TCP 10,66,248,120 597 78.090153 52.114.133.60 10.66.248.120 66 443 → 54353 [S' TCP 601 78.158186 104.68.76.183 10.66.248.120 TCP 66 443 → 54355 [S' 604 78,249544 10.66,248,120 66 443 → 54356 [S 204.79.197.200 TCP 607 78.311449 52.114.133.60 10.66.248.120 TCP 66 443 → 54357 [S' 617 78.374130 104.68.76.183 10.66.248.120 TCP 66 443 → 54358 627 78.483812 66 [TCP Out-Of-Or 104.68.76.183 10.66.248.120 66 [TCP Retransmi 650 78.719484 104.68.76.183 718 80.925349 183.3.225.78 10.66.248.120 TCP 66 36688 → 54359 > Frame 187: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF > Ethernet II, Src: Hangzhou_3a:4d:1e (74:25:8a:3a:4d:1e), Dst: IntelCor_9b:f0:00 (24:ee:9a:9b: > Internet Protocol Version 4, Src: 13.107.4.52, Dst: 10.66.248.120 > Transmission Control Protocol, Src Port: 80, Dst Port: 54352, Seq: 0, Ack: 1, Len: 0 \$ · · · · · t% · : M · · · E ·

分组: 1771 · 已显示: 46 (2.6%) │ 配置: Default

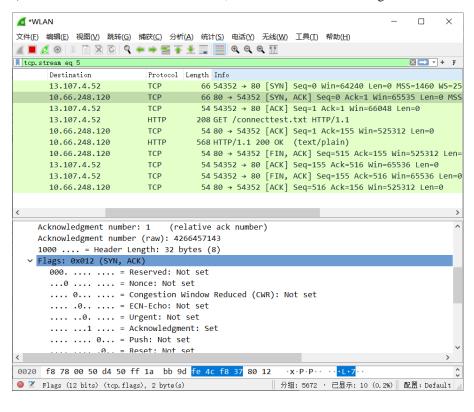
0000 24 ee 9a 9b f0 00 74 25 8a 3a 4d 1e 08 00 45 00

O 🕜 Acknowledgment: Boolean

2) 三次握手的第一个数据包,标志位 SYN 置位,初始序列值设置为 0.



3) 三次握手的第二个数据包, SYN,和 ACK 置位, Acknowledgment number 为 seq+1=1



4) TCP 三次握手的第三个数据包,标志位 ACK 置位, seq+1. П 文件(E) 编辑(E) 视图(Y) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H) tcp.stream eq 5 Destination Protocol Length Info 13.107.4.52 TCP 66 54352 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25 10.66.248.120 TCD 66 80 → 54352 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS 13,107,4,52 TCP 54 54352 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0 13.107.4.52 HTTP 208 GET /connecttest.txt HTTP/1.1 10.66.248.120 TCP 54 80 → 54352 [ACK] Seq=1 Ack=155 Win=525312 Len=0 10.66.248.120 HTTP 568 HTTP/1.1 200 OK (text/plain) 10.66.248.120 TCP 54 80 → 54352 [FIN, ACK] Seq=515 Ack=155 Win=525312 Len= 13.107.4.52 TCP 54 54352 → 80 [ACK] Seq=155 Ack=516 Win=65536 Len=0 13.107.4.52 TCP 54 54352 → 80 [FIN, ACK] Seq=155 Ack=516 Win=65536 Len=0 TCP 10.66.248.120 $54.80 \rightarrow 54352$ [ACK] Seq=516 Ack=156 Win=525312 Len=0 [Next sequence number: 1 (relative sequence number)] Acknowledgment number: 1 (relative ack number) Acknowledgment number (raw): 4279942046 0101 = Header Length: 20 bytes (5) ∨ Flags: 0x010 (ACK) 000. = Reserved: Not set ...0 = Nonce: Not set \dots 0 \dots = Congestion Window Reduced (CWR): Not set

二、TCP 的终止

.....0..... = ECN-Echo: Not set
.....0.... = Urgent: Not set
.....1 = Acknowledgment: Set
.....0... = Push: Not set

0020 04 34 d4 50 00 50 fe 4c f8 37 ff 1a bb 9e 50 10

■

✓ Flags (12 bits) (tcp.flags), 2 byte(s)

1) 过滤标志位 Fin 置位的包。服务器向客户机发送一个 Fin 包,标志位 ACK 和 FIN 置位,客户机也很快发送一个确认包,标志为 ACK 置位,ack 为 Fin 包的 seq+1.

·4·P·P·L ·7····

|| 分组: 7226 · 已显示: 10 (0.1%)|| 配置: Default |

