

廈門大學



信息学院软件工程系

《计算机网络》实验报告

题 目 实验四 用 PCAP 库监听并解析 FTP 协议

班 级 软件工程 2018 级 2 班

姓 名 贺青卓

学 号 34520182201499

实验时间 2020 年 3 月 25 日

2020 年 3 月 30 日

1 实验目的

先用 Omnipcap 或 Wireshark 侦听并观察 TCP 报文段。观察其建立和撤除连接的过程，观察其报文段 ID、窗口机制和拥塞控制机制等。将其过程截图在报告中。

用 Omnipcap 或 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征，再总结出提取用户名密码的有效方法。基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。最终在文件上输出形如下列 CSV 格式的日志：

时间、源 MAC、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-

DD-7D-D5-72,192.168.33.2,student,software,SUCCEED

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-

DD-7D-D5-72,192.168.33.2,student,software1,FAILED

2 实验环境

Windows 10 、 C++

3 实验结果

步骤一：用 wireshark 侦听观察 TCP 报文段和 FTP 数据

(1) 如下，客户端 192.168.2.231（本机），经由端口号 60465，与 FTP 服务器 121.192.180.66（学院的 FTP 服务器），端口 21，经过三次握手建立连接

334	59.959811	121.192.180.66	192.168.2.231	TCP	54	60465 → 21 [ACK] Seq=32 Ack=162 Win=261888 Len=0
335	59.959875	192.168.2.231	121.192.180.66	TCP	54	60465 → 21 [ACK] Seq=32 Ack=162 Win=261888 Len=0
336	59.963574	121.192.180.66	192.168.2.231	TCP	66	21 → 60466 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE...
337	59.963697	192.168.2.231	121.192.180.66	TCP	54	60466 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
338	60.038210	121.192.180.66	192.168.2.231	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
339	60.038341	192.168.2.231	121.192.180.66	TCP	54	60466 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
340	60.038484	192.168.2.231	121.192.180.66	FTP	68	Request: USER student
341	60.105843	121.192.180.66	192.168.2.231	FTP	90	Response: 331 User name okay, need password.
342	60.105968	192.168.2.231	121.192.180.66	TCP	54	60466 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
343	60.106089	192.168.2.231	121.192.180.66	FTP	69	Request: PASS software

(2) FTP 服务器返回状态码 220, 表示服务就绪

334	59.959811	121.192.180.66	121.192.180.66	TCP	54 21 → 60465 [FIN, ACK] Seq=101 Ack=52 Win=0 Len=0
335	59.959875	192.168.2.231	121.192.180.66	TCP	54 60465 → 21 [ACK] Seq=32 Ack=162 Win=261888 Len=0
336	59.963574	121.192.180.66	192.168.2.231	TCP	66 21 → 60466 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE...
337	59.963697	192.168.2.231	121.192.180.66	TCP	54 60466 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
338	60.038210	121.192.180.66	192.168.2.231	FTP	103 Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
339	60.038341	192.168.2.231	121.192.180.66	TCP	54 60466 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
340	60.038484	192.168.2.231	121.192.180.66	FTP	68 Request: USER student
341	60.105843	121.192.180.66	192.168.2.231	FTP	90 Response: 331 User name okay, need password.
342	60.105968	192.168.2.231	121.192.180.66	TCP	54 60466 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
343	60.106089	192.168.2.231	121.192.180.66	FTP	69 Request: PASS software

(3) 登陆时输入用户名和密码 (学院 ftp, 用户名 student 密码 software)

向 FTP 服务器发送登陆用户名 student。用户名验证通过后, FTP 服务器返回状态码 331, 表示需要输入密码。输入登陆密码 software 发送给 FTP 服务器, FTP 服务器验证后返回状态码 230, 表示用户已经登陆。

340	60.038484	192.168.2.231	121.192.180.66	FTP	68 Request: USER student
341	60.105843	121.192.180.66	192.168.2.231	FTP	90 Response: 331 User name okay, need password.
342	60.105968	192.168.2.231	121.192.180.66	TCP	54 60466 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
343	60.106089	192.168.2.231	121.192.180.66	FTP	69 Request: PASS software
344	60.174092	121.192.180.66	192.168.2.231	FTP	84 Response: 230 User logged in, proceed.

(4) 分析过程

客户端确认服务器的返回信息, 选择以 UTF_8 的格式来显示字符。服务端确认客户端的设置并设置文件输出类型为 L8

373	62.035209	192.168.2.231	121.192.180.66	FTP	68 Request: opts utf8 on
374	62.103330	121.192.180.66	192.168.2.231	FTP	75 Response: 501 Invalid option.
375	62.103462	192.168.2.231	121.192.180.66	TCP	54 60467 → 21 [ACK] Seq=44 Ack=137 Win=261888 Len=0
376	62.105611	192.168.2.231	121.192.180.66	FTP	60 Request: syst
377	62.175791	121.192.180.66	192.168.2.231	FTP	73 Response: 215 UNIX Type: L8
378	62.175915	192.168.2.231	121.192.180.66	TCP	54 60467 → 21 [ACK] Seq=50 Ack=156 Win=261888 Len=0
379	62.176172	192.168.2.231	121.192.180.66	FTP	65 Request: site help

发送 PASV 解释

383	62.253168	192.168.2.231	121.192.180.66	FTP	59 Request: PWD
384	62.319775	121.192.180.66	192.168.2.231	FTP	85 Response: 257 "/" is current directory.
385	62.319880	192.168.2.231	121.192.180.66	TCP	54 60467 → 21 [ACK] Seq=66 Ack=219 Win=261888 Len=0
386	62.321934	192.168.2.231	121.192.180.66	FTP	62 Request: TYPE A
387	62.389860	121.192.180.66	192.168.2.231	FTP	74 Response: 200 Type set to A.
388	62.389966	192.168.2.231	121.192.180.66	TCP	54 60467 → 21 [ACK] Seq=74 Ack=239 Win=261888 Len=0
389	62.390238	192.168.2.231	121.192.180.66	FTP	60 Request: PASV

(5) 四次握手断开连接

75	6.670907	192.168.2.231	121.192.180.66	TCP	54 62053 → 21 [FIN, ACK] Seq=49 Ack=168 Win=261888 Len=0
76	6.688341				54 <Ignored>
77	6.739000	121.192.180.66	192.168.2.231	TCP	54 21 → 62053 [ACK] Seq=168 Ack=50 Win=66560 Len=0
78	6.739980	121.192.180.66	192.168.2.231	TCP	54 21 → 62053 [FIN, ACK] Seq=168 Ack=50 Win=66560 Len=0
79	6.740050	192.168.2.231	121.192.180.66	TCP	54 62053 → 21 [ACK] Seq=50 Ack=169 Win=261888 Len=0

步骤二：编程监听并观察 FTP，输出日志

```

D:\Winpcap\WpdPack_4_1_2\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe
1. rpcap://\Device\NPF_{E0B8ED22-D913-4A84-8760-005CDEE738A0} (Network adapter 'VMware Virtual Ethernet Adapter' on local host)
2. rpcap://\Device\NPF_{1C00CBE4-1E73-4B37-B029-B27C74FE17FE} (Network adapter 'Microsoft' on local host)
3. rpcap://\Device\NPF_{2C41BDA6-76D5-4D31-99B0-72374A7C6445} (Network adapter 'Microsoft' on local host)
4. rpcap://\Device\NPF_{4EFFEE40-6184-4769-82CC-B65F55502A2A} (Network adapter 'VMware Virtual Ethernet Adapter' on local host)
5. rpcap://\Device\NPF_{8F9C50C1-F1C0-49A8-96AD-8840DFC148CF} (Network adapter 'Microsoft' on local host)
6. rpcap://\Device\NPF_{A611FE67-05FE-4D7F-BD3D-5BEF95302533} (Network adapter 'Intel(R) Ethernet Connection I219-V' on local host)
Enter the interface number (1-6):5

listening on Network adapter 'Microsoft' on local host...
2020-03-30 12:03:55, 9E-75-0A-F5-1C-20, 192.168.2.231, 70-3A-D8-48-60-40, 121.192.180.66, anonymous, IEUser@, FAILED
2020-03-30 12:03:56, 9E-75-0A-F5-1C-20, 192.168.2.231, 70-3A-D8-48-60-40, 121.192.180.66, student, software, SUCCEED

```

4 实验总结

通过这次实验直观地观察到了服务端与 FTP 服务器建立连接的过程。了解了在 FTP 登陆过程中服务端和客户端，关于用户名、密码、格式方面的交流。直观地看到了三次握手连接，四次握手断开的过程。