



- 1.实验报告如有雷同,雷同各方当次实验成绩均以0分计。
- 2. 当次小组成员成绩只计学号、姓名登录在下表中的。
- 3.在规定时间内未上交实验报告的,不得以其他方式补交,当次成绩按0分计。
- 4.实验报告文件以 PDF 格式提交。

院系	计算机学院	班 级	<u>软件工程</u>	组长	梁冠轩
学号	<u>19335118</u>	193352	<u>58</u>		
学生	梁冠轩	余世龙			

Ftp 协议分析实验

一、打开"FTP 数据包"的"ftp 例 1.cap"文件,进行观察分析,回答以下问题(见附件)

题号						
1	FTP 客户端的 mac 地址是多少?					
答案	00:14:2a:20:12:96					
截图	<pre>V Ethernet II, Src: Elitegro_20:12:96 (00:14:2a:20:12:96), Dst: DigitalC_02:b7:57 (00:03:0f:02:b7:57) > Destination: DigitalC_02:b7:57 (00:03:0f:02:b7:57) > Source: Elitegro_20:12:96 (00:14:2a:20:12:96) Type: IPv4 (0x0800)</pre>					
分析	客户端向服务器发出连接请求,第一条 src 为客户端					
2	第 1、2、3 号报文的作用是什么?					
答案	ftp 客户端与 ftp 服务器的 21 号端口连接的三次握手					
截图	1 0.000000 172.16.39.73 172.16.28.58 TCP 62 1372 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 2 0.000340 172.16.28.58 172.16.39.73 TCP 62 21 → 1372 [SYN], ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 3 0.000385 172.16.39.73 172.16.28.58 TCP 54 1372 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0					
分析	Tcp 的连接的三次握手					
3	该数据包中共有多少个 TCP 流?					
答案	5个					
截图	1 0.000000 172.16.39.73 172.16.28.58 TCP 62 1372 + 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 2 0.000340 172.16.28.58 172.16.39.73 TCP 62 21 + 1372 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 15 31.309831 172.16.28.58 172.16.39.73 TCP 62 20 + 1377 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 172.16.39.73 172.16.28.58 TCP 62 1377 + 20 [SYN], ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 38 104.700884 172.16.28.58 172.16.39.73 TCP 62 20 + 1380 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 39 104.700924 172.16.39.73 172.16.28.58 TCP 62 1380 + 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 110 111.708455 172.16.39.73 172.16.28.58 TCP 62 1380 + 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 130 149.974402 172.16.39.73 TCP 62 20 + 1381 {SYN} Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 131 149.974402 172.16.39.73 TCP 62 20 + 1384 {SYN} Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 131 149.974402 172.16.39.73 TCP 62 20 + 1384 {SYN} Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 131 149.974402 172.16.39.73 TCP 62 20 + 1384 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 131 149.974402 172.16.39.73 TCP 62 1384 + 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 131 149.974402 172.16.39.73 TCP 62 1384 + 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 131 149.974402 172.16.39.73 TCP 62 1384 + 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1					
分析	五次 tcp 流的连接					
4	用什么用户和密码登录成功?					
答案	用户名: wlx2008 密码: wlx2008					
截图	6 17.542571 172.16.39.73 172.16.28.58 FTP 68 Request: USER wlx2008 7 17.543205 172.16.28.58 172.16.39.73 FTP 90 Response: 331 User name okay, need password.					



中山大學 SUN YAT-SEN UNIVERSITY 计算机网络实验报告

5 套 5 套 6 答 4 数 6 条 8 0 9 0 8 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 10 0 </th <th>User 和 password 该 FTP 的命令连接和数据连持 传输用户名和密码后的都是数</th> <th>文据连接,前面的 1CP 62 21 + 1372 + 21 1CP 52 11 + 1372 + 21</th> <th></th> <th>接</th>	User 和 password 该 FTP 的命令连接和数据连持 传输用户名和密码后的都是数	文据连接,前面的 1CP 62 21 + 1372 + 21 1CP 52 11 + 1372 + 21		接			
5 套 5 套 6 答 4 数 6 条 8 0 9 0 8 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 10 0 </th <th>该 FTP 的命令连接和数据连接输用户名和密码后的都是数</th> <th>文据连接,前面的 1CP 62 21 + 1372 + 21 1CP 52 11 + 1372 + 21</th> <th></th> <th>接</th>	该 FTP 的命令连接和数据连接输用户名和密码后的都是数	文据连接,前面的 1CP 62 21 + 1372 + 21 1CP 52 11 + 1372 + 21		接			
答 截 分 6 客 图 所 6 案 图 所 6 案 图 所 8 人 7 条 8 人 8 人 8 人 8 人 9 上 9 上 9 日 </th <th>传输用户名和密码后的都是数 10.0000000 172.16.39.73 172.16.28.58 20.000340 172.16.28.58 172.16.39.73 30.000385 172.16.28.58 172.16.39.73 40.003815 172.16.28.58 172.16.39.53 50.201287 172.16.39.73 172.16.28.58 617.542571 172.16.39.73 172.16.28.58 717.543205 172.16.39.73 172.16.28.58 817.670704 172.16.39.73 172.16.28.58 921.6176364 172.16.39.73 172.16.28.58</th> <th>文据连接,前面的 1CP 62 21 + 1372 + 21 1CP 52 11 + 1372 + 21</th> <th></th> <th></th>	传输用户名和密码后的都是数 10.0000000 172.16.39.73 172.16.28.58 20.000340 172.16.28.58 172.16.39.73 30.000385 172.16.28.58 172.16.39.73 40.003815 172.16.28.58 172.16.39.53 50.201287 172.16.39.73 172.16.28.58 617.542571 172.16.39.73 172.16.28.58 717.543205 172.16.39.73 172.16.28.58 817.670704 172.16.39.73 172.16.28.58 921.6176364 172.16.39.73 172.16.28.58	文据连接,前面的 1CP 62 21 + 1372 + 21 1CP 52 11 + 1372 + 21					
截 分 6 答 截 分 7 答 截 分 8 月 P </th <th>2 6.009346 172.16.28.58 172.16.39.73 3 0.000385 172.16.39.73 172.16.28.58 4 0.001815 172.16.28.58 172.16.39.73 5 0.201287 172.16.39.73 172.16.28.58 6 17.542571 172.16.39.73 172.16.28.58 7 17.543205 172.16.39.73 172.16.28.58 8 17.670704 172.16.39.73 172.16.28.58 9 21.637636 172.16.39.73 172.16.28.58</th> <th>TCP 62 21 → 1372 TCP 54 1372 → 21</th> <th></th> <th></th>	2 6.009346 172.16.28.58 172.16.39.73 3 0.000385 172.16.39.73 172.16.28.58 4 0.001815 172.16.28.58 172.16.39.73 5 0.201287 172.16.39.73 172.16.28.58 6 17.542571 172.16.39.73 172.16.28.58 7 17.543205 172.16.39.73 172.16.28.58 8 17.670704 172.16.39.73 172.16.28.58 9 21.637636 172.16.39.73 172.16.28.58	TCP 62 21 → 1372 TCP 54 1372 → 21					
分 6 答 截 分 7 答 截 分 7 答 截 分 8 人 8 人 8 人 8 人 8 人 9 上 9 上 9 上 9 上 9 上 9 上 9 上 9 上 9 上 9 日 </th <th>3 0.000385 177.16.39.73 172.16.28.58 4 0.003815 177.16.28.58 172.16.39.73 5 0.201287 172.16.39.73 172.16.28.58 172.16.39.73 172.16.28.58 6 17.542571 172.16.39.73 172.16.28.58 172.16.39.73 172.16.28.58 172.16.39.73 172.16.28.58 921.617670704 172.16.39.73 172.16.28.58 921.6176365 172.16.39.73 172.16.28.58</th> <th>TCP 54 1372 → 21</th> <th></th> <th>Len=0 MSS=1460 SACK_PERM=1 Win=16384 Len=0 MSS=1460 SACK_PERN=1</th>	3 0.000385 177.16.39.73 172.16.28.58 4 0.003815 177.16.28.58 172.16.39.73 5 0.201287 172.16.39.73 172.16.28.58 172.16.39.73 172.16.28.58 6 17.542571 172.16.39.73 172.16.28.58 172.16.39.73 172.16.28.58 172.16.39.73 172.16.28.58 921.617670704 172.16.39.73 172.16.28.58 921.6176365 172.16.39.73 172.16.28.58	TCP 54 1372 → 21		Len=0 MSS=1460 SACK_PERM=1 Win=16384 Len=0 MSS=1460 SACK_PERN=1			
6 答 6 客 8 A 7 C 8 A 9 D 9 D 9 D 9 D 9 D 9 D 9 D 9 D 10 D	11 21,733359 172,16,28,73 172,16,28,58 123,1,96502 177,16,39,73 172,16,28,58 133,3060179 172,16,28,58 172,16,29,73 1431,3060179 172,16,28,58 172,16,39,73 1531,306981 172,16,39,73 172,16,28,58 1531,306981 172,16,39,73 172,16,28,58 172,16,39,73 1631,3069891 172,16,28,58 172,16,39,73 1831,310890 172,16,28,58 172,16,39,73 1931,3108901 172,16,28,58 172,16,39,73 2031,310991 172,16,28,58 172,16,39,73 2031,310931 172,16,28,58 172,16,39,73 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,28,58 231,310931 172,16,39,73 172,16,39,58	TCP 54 1372 - 21 FTP 90 Response: FTP 90 Response: FTP 84 Response: FTP 84 Response: FTP 78 Request: FTP 78 Request: FTP 68 Request: FTP 69 Repuest: FTP 60 Repuest: FTP 78 Request: FTP 78 Re	[ACK] Seq-1 ACK-1 Min-1 220 Serv-U FTP Server v [ACK] Seq-3 ACk-50 Min- USER wix2008 331 User name okay, ne [ACK] Seq-15 ACk-66 Win- PASS wix2008 230 User logged in, pr [ACK] Seq-29 ACk-116 W. PORT 172,16,30,73,5,97 200 PORT Command success [USY] Seq-0 Min-65535 [SYM] Seq-0 ACk-1 Win-6 [ACK] Seq-2 ACk-1 Win-6	65335 Len-0 vc4. for kinSock ready =65486 Len-0 ed password. =65456 Len-0 oceed. iin-65420 Len-0 issful. Lene0 HSS-1460 SACK_PERM-1 kin-16344 Len-0 HSS-1460 SACK_PERM-1 data connection for /bin/lsl) =1 Win-65355 Len-0 =65431 Len-0 Ze Win-65431 Len-0			
答 基 查 基 方 条 基 基 T 3 基 基 D D P </th <th>数据连接端口为 20, 控制连</th> <th>接端口为 21</th> <th></th> <th></th>	数据连接端口为 20, 控制连	接端口为 21					
截分析 7 答 截分析 7 客 8 花 0 P P P E E	该 FTP 的连接模式是那种?	为什么?					
分析 主 7 客 截图 分析 8 3 4 U P P E E	主动模式						
7 年 答案 T	12 31.305692 172.16.39.73 172.16.28.58 FTP 78 Request: PORT 172,16,39,73,5,97						
答案 T	主动模式为 Port 方式						
截图 分析 T 8 6 7 8 6 8 8 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9	最后四个报文的作用是什么?						
截图 分析 T 8 6 7 8 7 8 8 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9	Tcp 连接释放						
8	208 168.026708 172.16.28.58 209 168.026762 172.16.28.58	.72.16.28.58 TC .72.16.39.73 TC .72.16.39.73 TC .72.16.28.58 TC	P 60 21 → P 60 21 →	→ 21 [FIN, ACK] Seq=248 Ack=1203 win=64333 Len=0 1372 [ACK] Seq=1203 Ack=249 win=65288 Len=0 1372 [FIN, ACK] Seq=1203 Ack=249 win=65288 Len=0 → 21 [ACK] Seq=249 Ack=1204 win=64333 Len=0			
有 U P. P. 服 答案	Tcp 连接释放的四次报文						
U P. P. 服 答案	该数据包中有多少个 ftp 的命令及应答,其含义分别是什么?						
R	有 15 个 ftp 的命令与应答: USER w1x2008 向服务器发送用户名 w1x2008 PASS wlx2008 向服务器发送密码 wlx2008 PORT 172,16,39,73,5,97 主动模式,服务器主动与客户端建立连接,客服端的端口号通告给服务器 NLST -I 让服务器给客户发送一份目录列表 XMKD jjj 创建目录 RNFR jjj 重新命名文件 RNTO ppp 该命令和 RNFR 命令完成对文件的重命名						



STOR xs2009-9.xls. 接收数据并且在服务器站点保存为文件

PORT 172,16,39,73,5,101 主动模式,服务器主动与客户端建立连接,客服端的端口号通告给服务器

NLST -I 让服务器给客户发送一份目录列表

RNFR xs2009-9.xls 重新命名文件

RNTO 888.xls 该命令和 RNFR 命令完成对文件的重命名

PORT 172,16,39,73,5,104 主动模式,服务器主动与客户端建立连接,客服端的端口号通告给服务器

RETR 888.xls 让服务器给客户传送一份在路径名中指定的文件的副本

QUIT关闭与服务器的连接

	No. Time	Source	Destination	Process 1	Length Info
	4 0.001815	172.16.28.58	172.16.39.73	FTP	103 Response: 220 Serv-U FTP Server v6.4 for WinSock ready
	6 17.542571	172.16.39.73	172.16.28.58	FTP	68 Request: USER wlx2008
	7 17,543205	172.16.28.58	172.16.39.73	FTP	90 Response: 331 User name okay, need password.
	9 21.617636	172.16.39.73	172.16.28.58	FTP	68 Request: PASS wlx2008
	10 21.618699	172.16.28.58	172.16.39.73	FTP	84 Response: 230 User logged in, proceed.
	12 31.305692	172.16.39.73	172.16.28.58	FTP	78 Request: PORT 172,16,39,73,5,97
	13 31,306179	172.16.28.58	172.16.39.73	FTP	84 Response: 200 PORT Command successful.
	14 31.308878	172.16.39.73	172.16.28.58	FTP	63 Request: NLST -1
	18 31.310880	172.16.28.58	172.16.39.73	FTP	107 Response: 150 Opening ASCII mode data connection for /bin/ls.
	25 31,484083	172,16,28,58	172.16.39.73	FTP	182 Response: 226-Maximum disk quota limited to 307200 kBytes
	27 42.200128	172.16.39.73	172.16.28.58	FTP	64 Request: XMKD jjj
	28 42.201268	172.16.28.58	172.16.39.73	FTP	85 Response: 257 "/jjj" directory created.
	30 54.715458	172.16.39.73	172.16.28.58	FTP	64 Request: RNFR jjj
	31 54.716541	172.16.28.58	172.16.39.73	FTP	112 Response: 350 File or directory exists, ready for destination name
	32 54.720019	172.16.39.73	172.16.28.58	FTP	64 Request: RNTO ppp
	33 54,723253	172.16.28.58	172.16.39.73	FTP	84 Response: 250 RNTO command successful.
	35 104.695575	172.16.39.73	172.16.28.58	FTP	79 Request: PORT 172,16,39,73,5,100
	36 104.696037	172.16.28.58	172.16.39.73	FTP	84 Response: 200 PORT Command successful.
Del.	37 104.698520	172.16.39.73	172.16.28.58	FTP	73 Request: STOR xs2009-9.xls
冬	41 104.701805	172.16.28.58	172.16.39.73	FTP	112 Response: 150 Opening ASCII mode data connection for xs2009-9.xls.
	105 104.814922	172.16.28.58	172.16.39.73	FTP	183 Response: 226-Maximum disk quota limited to 307200 kBytes
	107 111.703852	172,16,39,73	172.16.28.58	FTP	79 Request: PORT 172,16,39,73,5,101
	108 111.704411	172.16.28.58	172.16.39.73	FTP	84 Response: 200 PORT Command successful.
	109 111.707423	172.16.39.73	172.16.28.58	FTP	63 Request: NLST -1
	113 111.709282	172.16.28.58	172.16.39.73	FTP	107 Response: 150 Opening ASCII mode data connection for /bin/ls.
	120 111.822991	172.16.28.58	172.16.39.73	FTP	183 Response: 226-Maximum disk quota limited to 307200 kBytes
	122 131.649709	172.16.39.73	172.16.28.58	FTP	73 Request: RNFR xs2009-9.xls
	123 131.650613	172.16.28.58	172.16.39.73	FTP	112 Response: 350 File or directory exists, ready for destination name
	124 131.654130	172.16.39.73	172.16.28.58	FTP	68 Request: RNTO 888.xls
	125 131.657140	172.16.28.58	172.16.39.73	FTP	84 Response: 250 RNTO command successful.
	127 149.968452	172.16.39.73	172.16.28.58	FTP	79 Request: PORT 172,16,39,73,5,104
	128 149.968908	172.16.28.58	172.16.39.73	FTP	84 Response: 200 PORT Command successful.
	129 149.972714	172.16.39.73	172.16.28.58	FTP	68 Request: RETR 888.xls
	133 149.975126	172.16.28.58	172.16.39.73	FTP	121 Response: 150 Opening ASCII mode data connection for 888.xls (57856 Bytes).
1	202 150 112474	173 16 30 E0	172 16 20 72	ETD	103 Dacparca, 776 Maximum dick quata limited to 207700 kButoc
	133 149.975126	172.16.28.58	172.16.39.73	FTP	121 Response: 150 Opening ASCII mode data connection for 888.xls (57856 Bytes).
	203 150.113474	172.16.28.58	172.16.39.73	FTP	183 Response: 226-Maximum disk quota limited to 307200 kBytes
	205 168.024267	172.16.39.73	172.16.28.58	FTP	60 Request: QUIT
	206 168.024267	172.16.39.73	172.16.28.38	FTP	68 Response: 221 Goodbye!
	200 108.024673	1/2.10.20.30	1/2.10.39./3	FIP	oo kesponse. 221 doodbye:
1					
析					

二、打开 "FTP 数据包"的 "ftp 例 2.cap" 文件, 进行观察分析, 回答以下问题

题号	
1	FTP 服务器的 ip 是多少? FTP 客户端的 mac 地址是多少?
	Ip:172.16.3.240
答案	
	mac:00:14:2a:20:12:96



	3 0.006731 172.16.39.93 172.16.3.240 TCP 62 3995 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1					
截图	<pre> V Ethernet II, Src: Elitegro_20:12:96 (00:14:2a:20:12:96), Dst: DigitalC_02:b7:57 (00:03:0f:02:b7:57) > Destination: DigitalC_02:b7:57 (00:03:0f:02:b7:57) > Source: Elitegro_20:12:96 (00:14:2a:20:12:96) Type: IPv4 (0x0800) </pre>					
分析	服务器 ip 地址和客户端 mac					
2	该数据包中共有多少个 TCP 流?					
答案	9 个					
截图	3 0.006731 172.16.39.93 172.16.3.240 TCP 62 3995 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 4 0.009137 172.16.3.240 172.16.39.93 TCP 62 21 → 3995 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 4 5 54.561498 172.16.39.93 172.16.3.240 TCP 62 241 → 2418 [SYN, ACK] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 4 5 54.571096 172.16.3.240 172.16.39.93 TCP 62 21 → 4218 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 8 9 177.671981 172.16.3.240 172.16.3.240 TCP 62 4685 + 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 9 0 177.672313 172.16.3.240 172.16.3.240 TCP 62 1132 ≥ 1 [SYN], ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 132 267.933915 172.16.3.240 172.16.3.240 TCP 62 1132 ≥ 1 [SYN], ACK] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 172 346.347532 172.16.3.240 172.16.3.240 TCP 62 1132 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 172 346.347532 172.16.3.240 172.16.39.93 TCP 62 21 → 1132 [SYN], ACK] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 172 346.347532 172.16.3.240 172.16.3.240 TCP 62 11345 [SYN, ACK] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 172 346.34757 172.16.3.240 172.16.3.9.93 TCP 62 1545 454 [SYN, ACK] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 172 346.34757 172.16.3.240 172.16.3.9.93 TCP 62 1545 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 173 346.34757 172.16.3.240 172.16.3.9.93 TCP 62 1654 [SYN], Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 174 346.34757 172.16.3.240 172.16.3.9.93 TCP 62 1654 [SYN], Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 175 346.34757 172.16.3.240 172.16.3.240 TCP 62 1791 + 17113 [SYN], Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 175 346.340823 172.16.3.240 172.16.3.9.93 TCP 62 1654 [SYN], Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 175 346.340823 172.16.3.240 172.16.39.93 TCP 62 1791 + 17113 [SYN], Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 175 347 347 347 347 347 347 347 347 347 347					
分析	九次 tcp 流的连接					
3	最后用什么用户和密码登录成功?					
答案	用户: kjdown 密码: kjdown					
截图	205 388.431413 172.16.39.93 172.16.3.240 FTP 67 Request: USER Kjdown 206 388.508545 172.16.3.240 172.16.39.93 FTP 90 Response: 331 User name okay, need password. 207 388.508724 172.16.39.93 172.16.3.240 FTP 67 Request: PASS Kjdown 208 388.676690 172.16.3.240 172.16.39.93 TCP 60 21 → 1454 [ACK] Seq=698 ACk=27 Win=65509 Len=0					
分析	User 和 pass					
4	该 FTP 的命令连接和数据连接分别是什么?					
答案	命令连接端口号为 21 数据连接端口号为 2118					
截图	30.006731 172.16.3.9.93 172.16.3.240 TCP 62 3995 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 40.009137 172.16.3.240 172.16.39.93 TCP 62 21 → 3995 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 50.009192 172.16.3.9.93 172.16.3.240 TCP 54 3995 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 172.16.3.240 172.16.3.240 172.16.3.9.93 FTP-DA 1514 FTP Data: 1460 bytes (PASV) (SIZE ************************************					
分析	命令连接端口号和数据连接多口号					
5	哪几个报文是 FTP 数据连接的三次握手报文?					
答案	3, 4, 5					
截图	3 0.006731 172.16.39.93 172.16.3.240 TCP 62 3995 + 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 4 0.009137 172.16.3.240 172.16.39.93 TCP 62 21 + 3995 [SYN] ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 5 0.009192 172.16.39.93 172.16.3.240 TCP 54 3995 + 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0					
分析	三次握手					



6	哪几个报文是 FTP 数据连接的挥手报文(结束报文)?					
答案	629, 630, 631, 632					
截图	629 565.983884 172.16.3.940 TCP 54 1454 → 21 [FIN, ACK] Seq=375 Ack=1843 Win=65161 Len=0 630 565.988017 172.16.3.240 172.16.3.943 TCP 60 21 → 1454 [ACK] Seq=1843 Ack=376 Win=65161 Len=0 631 566.203149 172.16.3.240 172.16.3.93 TCP 60 21 → 1454 [FIN, ACK] Seq=1843 Ack=376 Win=65161 Len=0 632 566.203215 172.16.3.940 TCP 54 1454 → 21 [ACK] Seq=376 Ack=1844 Win=65161 Len=0					
分析	挥手报文					
7	该 FTP 的连接模式是那种? 为什么?					
答案	被动方式,数据连接端口不为 20, 使用了随机端口					
截图	332 523.336555					
分析	数据端口为 2118					

三、在线捕获数据包实验

- 1. 阅读教材 P64-69 内容, 熟悉 FTP 协议。
- 2. 完成 P51 的实例 2-1。

本次实验完成后,请根据组员在实验中的贡献,请实事求是,自评在实验中应得的分数。(按百分制)

学号	学生	<u>自评分</u>
<u>19335118</u>	梁冠轩	<u>100</u>
19335258	余世龙	<u>100</u>

【交实验报告】

上传实验报告: <u>ftp://172.18.187.1/</u> 用户名/口令: netjob/d502 截止日期(不迟于): 1 周之内 上传包括两个文件:

(1) 小组实验报告。上传文件名格式: 小组号_Ftp 协议分析实验.pdf (由组长负责上传)

例如:文件名" 10_F tp 协议分析实验.pdf"表示第 10 组的 Ftp 协议分析实验报告,,视频文件与小组文件相同,扩展名是 mp4

(2) 小组成员实验体会。每个同学单独交一份只填写了实验体会的实验报告。只需填写自己的学号和姓名。 文件名格式: 小组号 学号 姓名 Ftp 协议分析实验.pdf (由组员自行上传)

例如: 文件名 "10_05373092_张三_ Ftp 协议分析实验.pdf"表示第 10 组的 Ftp 协议分析实验报告。



注意:不要打包上传!