

WireShark Lab 2

Lab Example

Apply a display filter ... <Ctrl>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	129.2.205.242	129.2.205.242	FTP	183	Response: 220-FileZilla Server 0.9.53 beta
2	2.000005	129.2.205.242	129.2.205.242	FTP	52	Request: USER user1
3	5.350810	129.2.205.242	129.2.205.242	FTP	73	Response: 331 Password required for user1
4	15.927628	129.2.205.242	129.2.205.242	FTP	59	Request: PASS cyberskyline
5	15.927628	129.2.205.242	129.2.205.242	FTP	74	Response: 530 Login or password incorrect!
6	30.357654	129.2.205.242	129.2.205.242	FTP	46	Request: QUIT
7	33.742859	129.2.205.242	129.2.205.242	FTP	53	Response: 221 Goodbye
8	37.798867	129.2.205.242	129.2.205.242	FTP	183	Response: 220-FileZilla Server 0.9.53 beta
9	41.667673	129.2.205.242	129.2.205.242	FTP	52	Request: USER user1
10	43.882877	129.2.205.242	129.2.205.242	FTP	73	Response: 331 Password required for user1
11	46.768882	129.2.205.242	129.2.205.242	FTP	57	Request: PASS metropolis
12	49.966888	129.2.205.242	129.2.205.242	FTP	55	Response: 230 Logged on
13	52.665693	129.2.205.242	129.2.205.242	FTP	68	Request: PORT 129,2,205,242,207,243
14	58.078902	129.2.205.242	129.2.205.242	FTP	69	Response: 200 Port command successful
15	58.078902	129.2.205.242	129.2.205.242	FTP	46	Request: LIST
16	58.078902	129.2.205.242	129.2.205.242	FTP	95	Response: 150 Opening data channel for directory listing of "/"
17	58.078902	129.2.205.242	129.2.205.242	FTP-D...	364	FTP Data: 324 bytes (PORT) (LIST)
18	58.078902	129.2.205.242	129.2.205.242	FTP	74	Response: 226 Successfully transferred "/"
19	76.674135	129.2.205.242	129.2.205.242	FTP	55	Request: DELE bank.cap
20	76.674135	129.2.205.242	129.2.205.242	FTP	71	Response: 250 File deleted successfully
21	92.274162	129.2.205.242	129.2.205.242	FTP	68	Request: PORT 129,2,205,242,207,244
22	92.274162	129.2.205.242	129.2.205.242	FTP	69	Response: 200 Port command successful
23	92.274162	129.2.205.242	129.2.205.242	FTP	60	Request: STOR compcodes.zip
24	92.274162	129.2.205.242	129.2.205.242	FTP	112	Response: 150 Opening data channel for file upload to server of "/compcodes.zip"
25	92.274162	129.2.205.242	129.2.205.242	FTP-D...	1500	FTP Data: 1460 bytes (PORT) (STOR compcodes.zip)

> Frame 1: Packet, 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Raw packet data
> Internet Protocol Version 4, Src: 129.2.205.242, Dst: 129.2.205.242
> Transmission Control Protocol, Src Port: 21, Dst Port: 53233, Seq: 1, Ack: 1, Len: 143
> File Transfer Protocol (FTP)
[Current working directory:]

0000 45 00 00 b7 21 80 40 00 80 06 00 00 81 02 cd f2 E...f@:
0010 81 02 cd f2 00 15 cf f1 1b ec c9 a5 b8 1c 0d be 220-File
0020 50 18 00 20 ac ae 00 00 32 32 30 2d 46 69 6c 65 P... 220-File
0030 5a 69 6c 6c 61 20 53 65 72 76 65 72 20 30 2e 39 Zilla Se rver 0.9
0040 2e 35 33 20 62 65 74 61 0d 0a 32 32 30 2d 77 72 .53 beta -220-wr
0050 69 74 74 65 6e 20 62 79 20 54 69 6d 20 4b 6f 73 itten by Tin Kos
0060 73 65 20 20 74 69 6d 2e 6b 6f 73 73 65 40 66 69 se (tim.kosse@fi
0070 6c 65 7a 69 6c 6c 61 2d 70 72 6f 6a 65 63 74 2e lezilla- project
0080 6f 72 67 29 0d 0a 32 32 30 20 50 6c 65 61 73 65 org)-22 0 Please
0090 20 76 69 73 69 74 20 68 74 74 70 73 3a 2f 2f 66 visit h ttps://f
00a0 69 6c 65 7a 69 6c 6c 61 2d 70 72 6f 6a 65 63 74 ilezilla -project
00b0 2e 6f 72 67 2f 0d 0a .org/..

FTP.pcap Packets: 97 Profile: Default

Questions

Q1

What was the first username:password combination attempt made to log in to the server? (e.g. user:password)

user1:cyberskyline

Q2

What software is the FTP server running? (Include name and version)

FileZilla Server 0.9.53 beta

Q3

What is the first username:password combination that allows for successful authentication? (e.g. user:password)

user1:metropolis

Q4

What is the first command the user executes on the ftp server?

PORT

Q5

What file is deleted from the ftp server?

bank.cap

Q6

What file is uploaded to the ftp server?

compcodes.zip

Q7

What is the filesize (in bytes) of the uploaded file?

28183

Q8

What file does the anonymous user download?

compcodes.zip

Sources used to learn:

[~cengage](#)

[~~~~youtube](#)

[~~~~~trove.cyberskyline](#)