Sean Blanchard

2/3/2021

COMP429

L02: Wireshark Lab

**tftp qanda**

1. ***What is the syntax for a RRQ or WRQ packet in TFTP?***

***The syntax for RRQ or WRQ packets in TFTP is a acknowledgement packet for write.***

2 bytes string 1 byte string 1 byte

------------------------------------------------

| Opcode | Filename | 0 | Mode | 0 |

------------------------------------------------

The file name is a sequence of bytes in netascii terminated by a zero byte. The mode field contains the string “netascii”, “octet”, or “mail”.

1. ***Which bytes contain the opcode for the RRQ in frame number 1 in the L02-tftp.pcapng file?***

00 01

Opcode: Read Request (1)

1. ***What is the name of the file for the RRQ in frame number 1?***

Rfc1350.txt

1. ***What are the three supported modes for RRQ/WRQ in TFTP?***

The three supported modes for RRQ/WRQ are strings “netascii”, “octet”, or “mail”, which can be either any combination of upper and lower case.

1. ***Which mode was used in the RRQ in frame number 1?***

netascii

1. ***What is the syntax for a DATA packet in TFTP?***

2 bytes 2 bytes n bytes

----------------------------------

| Opcode | Block # | Data |

----------------------------------

1. ***Explain the purpose of block numbers according to the RFC.***

The purpose of a block number is to restrict the allowed programs to use a single number to discriminate between new packets and duplicates. The block numbers on data packets begin with one and increase by one for each new block of data.

1. ***What would happen if a data block contained < 512 bytes?***

If the data block contained less than 512 bytes, it signals the end of the transfer. This packet is acknowledged by an ACK packet like all other DATA packets. The host acknowledges the final DATA packet may terminate its side of the connection on sending the final ACK.   
Essentially dallying is encouraged, this means that when the host sends the final ACK, the host will wait a certain time frame before terminating to retransmit the final ACK if it was lost. If the response is ACK, the transmission is successful. There is also cases where the transfer was unsuccessful, but long story short the connection has been closed.

1. ***What is the syntax of an ACK packet in TFTP?***

2 bytes 2 bytes

---------------------

| Opcode | Block # |

---------------------

1. ***Write down the frame number of one DATA packet and its coinciding ACK packet from the file transfer.***

Frame : 2

Block: 00 01

1. ***There are two IP addresses in this transaction, which one is the server and which one is the client?***

Server IP address : 192.168.19.1

Client IP address : 192.168.19.99

1. ***What port number is the server listening for a RRQ or WRQ on?***

Source Port: 51496

**ftp qanda**

1. ***Capture FTP traffic with Wireshark:***
   * ***Open Wireshark***
   * ***Begin capturing on the correct interface.***
   * ***In a browser, start an FTP connection***
     + ***You have to have ftp:// in the URL otherwise it will go over HTTP!***
     + ***ftp://ftp.gnu.org***
     + ***You have to have ftp:// in the URL otherwise it will go over HTTP!***
     + ***Hope that was clear.***
   * ***Download tree.json.gz (right click, "Save link as...")***
   * ***Stop the capture.***
   * ***Save capture file as L02-ftp.pcapng.***
2. ***What is the name of the user who logged into the FTP Server? Identify the request and responses using the frame number in your answer.***

USER anonymous

1. ***What is the IP address of you (client) and the IP address of the server?***

IP address of me (client): 2603:8001:a702:f900:5575:63f7:d648:fb1

IP address of server: 2001:470:142:3

1. ***Find a "PWD" request command sent by the client. Use a Wireshark filter to isolate the packet.***
   * ***What is the Wireshark filter you used?***
   * ***What frame numbers contain PWD requests?***
   * ***What is the filter to display PWD requests OR (hint: ||) ftp responses that contain code 257. Note: this filter should display the requests from the client and responses by the server.***

The Wireshark filter I used to find a “PWD” request command sent by client is “ftp.request.command==PWD”

Frame 218 contained PWD request. Also frame 605 requested PWD.

The Wireshark filter I used to display PWD requests or FTP responses that contain code 257 is “ftp.request.command==PWD||ftp.response.code==257”

1. ***What is the purpose of requesting PASV mode? (Mentioned in the lecture).***

A PASV request asks the server to accept a data connection on a new TCP port selected by the server. The server normally accepts PASV with code 227. Its response is a single line showing the IP address of the server and the TCP port number where the server is accepting connections.

1. ***Filter to display only the "PASV" requests and responses.***
   * ***What filter did you use?***
   * ***Find the response for the CWD / command, what port number is opened for the data to flow? (Wireshark tells you which response is for which command)***
   * ***Find the response for the SIZE tree.json.gz file, what port number is opened for the data to flow?***
   * ***Use the filter ftp-data to view the data being transferred. This will confirm your answers from above.***

The filter that I used to display only the “PASV” requests and responses is “[ftp.espv.ipv6](ftp://ftp.espv.ipv6)” since I am running an ipv6 connection.

I have two different PASV requests and responses. The first one

Frame: 229

Port number: 29423

Frame: 616

Port number: 22763

The response size of tree.json.gz file has a size of 587900 bytes. I found this number by looking directly under when the server requests the SIZE /tree,json.gz

The port number that is opened for the data to flow is 58225.