Shane McDonough
Kadejha Jones
Shawn Ching

Lab 3 Question 1 Answers

Link to the file

Task 1:

1. How many unique message types do we see in this transaction?
   a. We see 3 different types of messages. They are read request, data, and acknowledgement.
2. What is the default block size for TFTP?
   a. The default block size is 512 bytes.
3. What is the block size used in this transaction?
   a. 1337 bytes.
4. Which frame numbers contain read requests, if any?
   a. Frame 1 contains a read request.
5. Which frame numbers contain write requests, if any?
   a. There are no write requests.
6. Is a file being transferred from the server or being sent to the server? How do you know?
   a. It is being transferred to the client because there is a read request being made
7. Given your answer to number 6, which IP address represents the server?
   a. 192.168.254.15 represents the server.
8. How does the client/server know the file transfer is complete?
   a. The last data packet sent by the server is smaller than all the other ones showing that the transfer is complete.

Task 2:

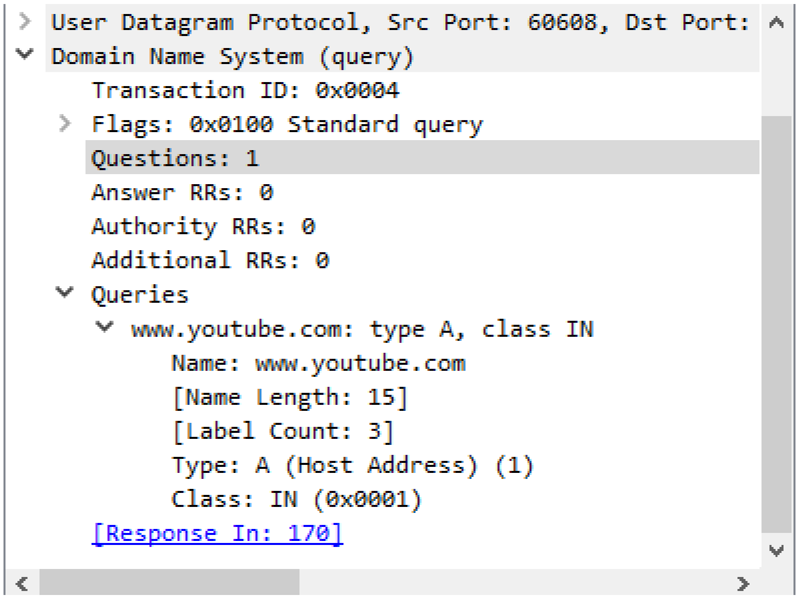
1. What are the three main parts of an IRC client message?
   a. The three main parts of the IRC client message are the “prefix”, the “command”, and the “parameters”
2. What is the maximum number of parameters allowed in an IRC message?
   a. There is a maximum of 15 parameters.
3. What must all messages end with?
   a. All messages must end with two characters, the carriage return (“\r” / %x0D) and the line feed (“\n” / %x0A).
4. Do any of the requests in the packet capture contain a prefix? If so, which are they? (list of frame numbers)
   a. Though our findings none of the requests contained prefixes.
5. Do any of the responses in the packet capture contain a prefix? If so, which are they? (list of frame numbers)
   a. The frame numbers that correspond to requests with prefixes are 8, 9, 10, 11, 13, 15,17, 19, 22, and 24.
6. To chat in a channel, the client sends a PRIVMSG command. What would the message look like if user kscrivs sent the message "workin' on the lab…" to channel lab two.

    a. “PRIVMSG #lab2 :workin' on the lab...\r\n”

7. IRC responses are numerical for the most part. What is the number range for responses to commands.
    a. The number range is 200 to 399.
8. What is the number range for responses that are error messages.
    a. The number range is 400 to 599.
9. Write a Wireshark filter to find all the normal responses (not errors) to commands.
    a. “irc.response.command >= 200 && irc.response.command <= 399”
10. Because of the message ending characters, more than one message can be present in a frame. List a frame that has this quality.
    a. One frame that has this quality is number 4.

Task 3:

1. Write a filter to display only DNS traffic (hint: it is simply the name of the protocol). Write down the filter
    a. “dns”
2. Save the capture as a pcapng file, but only save the filtered DNS traffic.
    a.
3. Write a filter to display only one of your DNS requests (req)
    a. “dns.qry.name == "www.youtube.com" && dns.qry.type == 1 && dns.flags == 0x0100”
4. DNS is a request (req) and response (resp) protocol. Design a filter to find DNS responses where the length of the data is longer than 10 characters.
    a. “dns.resp.len > 10”
5. DNS responses contain the number of questions asked. What is the filter to find the count of that value?
    a.



```
> User Datagram Protocol, Src Port: 60608, Dst Port:
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.youtube.com: type A, class IN
        Name: www.youtube.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 170]
```

Task 4:

1. Imagine if TFTP were an ASCII based protocol, reasonably translate three unique messages from this lab into this new imaginary version
    a. “\0\1file\0netascii\0blksize\01337\0” -> “readreq\nfile\nnetascii\nblksize\n1337:”
    b. “\0\6blksize\01337\0” -> “conf\nblksize\n1337:”
    c. “\0\4\0\0” -> “ack:”
2. Imagine if IRC were a binary based protocol, reasonably translate three unique messages from this lab to this new imaginary version
    a. “NICK kscrivs” -> “\0\1kscrivs\0”
    b. “NOTICE AUTH :*** looking up your hostname\r\n” -> “\0\2*** looking up your hostname\0”
    c. “USER kscriv 0 * kscrivs” -> ”\0\3kscriv 0 * kscrivs\0”