MONASH University

Time left 1:19:31

Question 1

Not yet answered

Marked out of 93.00

Network Traffic Analysis using Wireshark

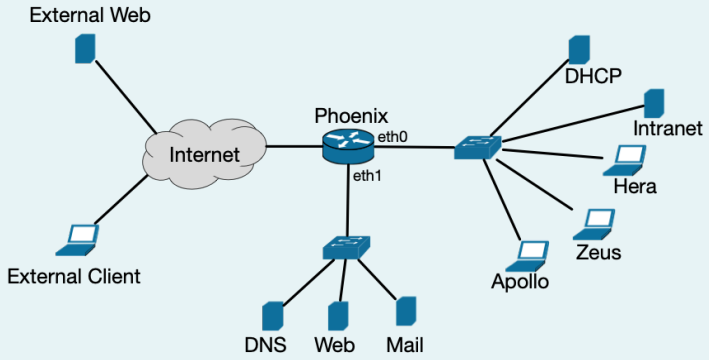
To complete this part of the quiz you need to download the following packet capture file which is available via google drive. Please note that you must be logged in with your Monash email account on the browser you are using for this quiz to access the google drive. Make sure you are logged out of all your personal google accounts if you encounter a request access page.
Link to Apollo Node PCAP file

Important Note: Various parts of the process of creating the PCAP files are randomised. Any name, domain, and/or IP address similarity is coincidental.

Scenario

The provided PCAP file for Apollo node contains the network traffic sent and received by this node for a period of time. During this time a user on this node has visited the web server of the organisation (the node named Web in the diagram), the intranet server (the node named Intranet in the diagram), and the external web server (the node named External in the diagram). The user Sepehr has sent an email to another user within the organisation and has used `ping` command to test the connection with nodes

Zeus and Hera. The network connectivity is shown in the following diagram.



Task 1: Data Link Layer

Using the information contained in the PCAP file identify the MAC addresses of the following nodes.
Note: Include colon (:) as the separator for all MAC addresses (e.g. AA:BB:CC:DD:EE:00)

MAC address of Apollo: [5 Mark(s)]

MAC address of Zeus: [5 Mark(s)]

MAC address of DHCP: [5 Mark(s)]

Task 2: Network Layer

IP address of Apollo: [5 Mark(s)]

IP address of Hera: [5 Mark(s)]

IP address of Phoenix_eth0: [5 Mark(s)]

IP address of DNS: [5 Mark(s)]

Task 3: Transport and Application Layers

Visiting a Web Server

Identify the frames of the Apollo's visit to the organisation web server (node named Web in the diagram) and fill out the following fields.

a) Identify the first frame that initiates the connection. Enter the frame number: [ ] **[2 Mark(s)]**

The client port number: [ ] **[2 Mark(s)]**

The 32-bit raw sequence number in hex: [ ] **[2 Mark(s)]**

This is sent from client to server:
○ True ○ False
[2 Mark(s)]

This message will consume one sequence number:
○ False ○ True
[2 Mark(s)]

b) Identify the second frame of the three-way handshake. Enter the frame number: [ ] **[2 Mark(s)]**

The 32-bit raw sequence number in hex: [ ] **[2 Mark(s)]**

c) Identify the third frame of the three-way handshake. Enter the frame number: [ ] **[2 Mark(s)]**

The 32-bit raw sequence number in hex: [ ] **[2 Mark(s)]**

The 32-bit raw acknowledgement number in hex:
[ ] **[2 Mark(s)]**

d) Identify the frame of the GET request for the default HTML page. Enter the frame number: [ ] **[2 Mark(s)]**

Enter the full request URI: [ ]
[2 Mark(s)]

Enter the size of application layer message in bytes as an integer number: [ ] **[2 Mark(s)]**

e) Identify the frame of the server response containing the HTML page. Enter the frame number: [ ] **[2 Mark(s)]**

Enter the size of the application layer message in bytes as an integer number: [ ] **[2 Mark(s)]**

Enter the size of the application layer user data (application layer message without application layer header): [ ] **[2 Mark(s)]**

The HTML page content has a 16-digit hex value as a flag. Enter the flag: [ ] **[2 Mark(s)]**

f) The page contains an image. Identify the GET request for the picture. Enter the frame number: [ ] **[2 Mark(s)]**

Enter the full request URI:
[ ] **[2 Mark(s)]**

Enter the size of application layer message in bytes as an integer number: [ ] **[2 Mark(s)]**

g) Identify the frame of the server response containing the picture. How many TCP segments was required to download this picture:
[ ] **[2 Mark(s)]**

Enter the size of the picture: [ ] **[2 Mark(s)]**

The picture has a 16-digit hex value as a flag. Export the picture to view this flag. Enter the flag: [ ] **[2 Mark(s)]**

Sending an email

Identify the frames of the email sent from Apollo using the Mail server.

a) Identify the first frame that initiates the connection. Enter the frame number: [ ] **[1 Mark(s)]**

The client port number: [ ] **[1 Mark(s)]**

The 32-bit raw sequence number in hex: [ ] **[1 Mark(s)]**

This is sent from client to server:
○ False ○ True
[1 Mark(s)]

This message will consume one sequence number:
○ True ○ False
[1 Mark(s)]

b) Identify the second frame of the three-way handshake. Enter the frame number: [ ] **[1 Mark(s)]**

The 32-bit raw sequence number in hex: [ ] **[1 Mark(s)]**

c) Identify the third frame of the three-way handshake. Enter the frame number: [ ] **[1 Mark(s)]**

The 32-bit raw sequence number in hex: [ ] **[1 Mark(s)]**

The 32-bit raw acknowledgement number in hex:

[ ] **[1 Mark(s)]**

d) Find the frame that contains the email of the recipient. Enter the receiver's email address (without < and >):

[ ]

[1 Mark(s)]

d) Find the frame that gives the queue ID of this email on the server. Enter the queue id: [ ] **[1 Mark(s)]**