Arnaldo Torres

HW 0

7/14/20

8) WHAT IS THE FULL PATH OF DocumentRoot DIRECTORY ON YOUR WINDOWS 10 VM?

C:/xampp/htdocs

9) WHAT IS THE IP ADDRESS OF YOUR HOST COMPUTER (the lab computer), and HOW DID YOU FIND THIS INFORMATION?

192.168.56.1 // I went through the control panel, network settings, then view network connections, went to the active connection, and then went to details and there was the ip address.

10) Open WireShark inside the Windows 10 VM and start a new capture.

11) From the host machine, refresh (or re-browse) to http://192.168.56.101

12) Stop the WireShark capture, and use it to answer the following questions…

13) IN THE TCP THREE-WAY HANDSHAKE THAT BEGINS THE EXCHANGE OF THIS WEB PAGE, WHICH IP ADDRESS INITIATES COMMUNICATION (sends the first packet)? Hence, we will refer to this as packet 0. (Hint: The TCP Three-Way Handshake can be identified from the TCP Flags used in the first 2 packets… SYN, SYN/ACK)

192.168.56.1

14) WHAT ARE THE INITIAL TCP SEQUENCE NUMBERS USED BY EACH SIDE OF THE WEB PAGE EXCHANGE?

0

15) HOW MANY PACKETS INTO THE CONVERSATION (how many packets after “packet 0”) IS THE PACKET WHICH CONTAINS THE TEXT OF THE WEB PAGE index.html?

8th packet on wireshark, but since we are starting from packet 0 and wireshark counts from 1, it would be the 7th packet.

16) a. WHAT IS THE FIRST LINE OF THE HTTP HEADER IN THE PACKET WHICH CONTAINS THE TEXT OF THE WEB PAGE index.html?

HTTP/1.1 200 OK\r\n

b. DOES THIS LINE OF THE HEADER INDICATE SUCCESS OR FAILURE?

It indicates success.

17) a. HOW MANY PACKETS INTO THE CONVERSATION CONVERSATION (how many packets after "packet 0") IS THE PACKET WHICH CONTAINS THE GET REQUEST FROM THE Host Computer TO THE Windows 10 VM?

Number 7 is where the get request, so that would make it 5 packets after the initial packet 0

b. WHAT IS THE FIRST LINE OF THE GET REQUEST HTTP HEADER (starts with the word "GET")? c. WHAT TEXT IS IN THE "User-Agent" FIELD OF THIS HEADER? (What do you think this User-Agent field indicates?)

GET / HTTP/1.1\r\n

18) WHICH SIDE (Host Computer or Windows 10 VM) IS THE FIRST TO SIGNAL AN END TO THE CONVERSATION (in other words, sends the TCP Fin flag)?

Windows 10 VM sends the TCP Fin flag

19) WHAT ARE THE TCP FLAGS OF THE LAST PACKET SENT IN THE CONVERSATION? WHICH COMPUTER (Host or VM) SENDS THIS PACKET?

ACK acknowledging the Fin flag. And ACK was sent by the host computer

20) NOW THAT THE Windows 10 VM IS ON THE "INTERNAL NETWORKING," OPEN A BROWSER INSIDE THE VM AND ACCESS http://www.csun.edu DOES THIS SUCCEED? WHY OR WHY NOT?

It fails, because the VM has been set on virtual host only adapter, meaning it networks only between the host and itself.