LAB 1 – Wireshark Setup

Name – Sati, Ankit Date – 9/14/2021

Section - 001

Total in points (Maximum 100 points)–

Professors Comments –

Affirmation of Independent Effort – Ankit Sati

Answers

1. Three Protocols that were visible in the packet-listing window are.
   a. Transmission control protocol (TCP)
   b. User Datagram Protocol (UDP)
   c. Internet Control Message Protocol (ICMP)
   d. Hypertext Transfer Protocol (HTTP)

2. The total amount of time between HTTP GET message and HTTP OK message was.
   - 2021-09-14 10:42:59.951111 GET /ncsi.txt HTTP/1.1
   - 2021-09-14 10:42:59.975880 HTTP/1.1 200 OK (text/plain)

   Total Time = 0.24,769 seconds

3. The required IP's are listed below.
   - gaia.cs.umass.edu – 128.119.245.12
   - My computer - 10.0.0.220

4. Please find the HTTP messages printed below (GET and OK).

   No. Time Source Destination Protocol Length Info
   188 2021-09-14 17:04:26.697684 10.0.0.220 128.119.245.12 HTTP 649 GET /wireshark-labs/INTRO-wireshark-file1.html
   HTTP/1.1
   Frame 188: 649 bytes on wire (5192 bits), 649 bytes captured (5192 bits) on interface \Device\NPF_{DEDD6F2D-6126-4990-A19F-6C341FF023AF}, id 0
   Ethernet II, Src: IntelCor_31:68:61 (f0:9e:4a:31:68:61), Dst: ARRISGro_1d:ae:80 (58:19:f8:1d:ae:80)
   Internet Protocol Version 4, Src: 10.0.0.220, Dst: 128.119.245.12
   Transmission Control Protocol, Src Port: 50413, Dst Port: 80, Seq: 1, Ack: 1, Len: 595
   Hypertext Transfer Protocol
   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
   Host: gaia.cs.umass.edu\r\n
   Connection: keep-alive\r\n
   Cache-Control: max-age=0\r\n
   DNT: 1\r\n
   Upgrade-Insecure-Requests: 1\r\n
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signedexchange;v=b3;q=0.9\r\n
   Accept-Encoding: gzip, deflate\r\n
   Accept-Language: en-US,en;q=0.9\r\n
   If-None-Match: "51-5cbee474338cd"\r\n

If-Modified-Since: Tue, 14 Sep 2021 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 193]

No. Time Source Destination Protocol Length Info
235 2021-09-14 17:04:29.978312 23.38.168.179 10.0.0.220 HTTP 233 HTTP/1.1 200 OK (text/plain)
Frame 235: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface \Device\NPF_{DEDD6F2D-6126-4990-A19F-6C341FF023AF}, id 0
Ethernet II, Src: ARRISGro_1d:ae:80 (58:19:f8:1d:ae:80), Dst: IntelCor_31:68:61 (f0:9e:4a:31:68:61)
Internet Protocol Version 4, Src: 23.38.168.179, Dst: 10.0.0.220
Transmission Control Protocol, Src Port: 80, Dst Port: 64032, Seq: 1, Ack: 125, Len: 179
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Content-Length: 14\r\n
Date: Tue, 14 Sep 2021 21:04:29 GMT\r\n
Connection: close\r\n
Content-Type: text/plain\r\n
Cache-Control: max-age=30, must-revalidate\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.028561000 seconds]
[Request in frame: 233]
[Request URI: http://www.msftncsi.com/ncsi.txt]
File Data: 14 bytes
Line-based text data: text/plain (1 lines)