HTTPS in Wireshark and Stratoshark

This exercise uses the files 3_https_packets.pcapng and 3_https_syscalls.scap. In these files, we will examine an HTTPS request and its response from Apache.

1. Open 3_https_packets.pcapng
    a. Look at the TCP handshake in the first 3 frames.
        i. Write down the 4-tuple of this connection (source IP address, source port, destination IP address, and destination port)

192.168.64.1, 53946, 192.168.64.3, 443

        ii. In each direction, what is the Maximum Segment Size (MSS)?

Client -> Server, 1460 | Server -> Client, 1460

        iii. In each direction what is the Window Scaling factor?

Client -> Server, 6 | Server -> Client, 7

        iv. Are there any other TCP options used in either direction?

SACK is enabled and TCP Timestamps are enabled in both directions

    b. Look at the TLS Client Hello and Server Hello.
        i. What TLS version is this conversation?

TLS 1.3

        ii. The Client Hello lists all supported cipher suites, and the server picks one to use. What is the negotiated cipher suite?

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

        iii. What is the TCP payload length of the entire Client Hello?

517 bytes

iv. What is the TCP payload length of the entire Server Hello?

1329 bytes

c. What is the initial round trip time of this conversation?

0.000365000 seconds (365 microseconds)

2. Open 3_https_syscalls.scap
   a. Build the expected connection filename. It's typically formatted [source IP address]:[source port]->[destination IP address]:[destination port]

192.168.64.1:53946->192.168.64.3:443

   b. Create a display filter using this connection name: fd.name eq <your connection name here>. Apply it using the Find tool in Stratoshark (Ctrl+F/Cmd+F). In which event does the Apache accept the network connection from the OS?

73

   c. Using what you know about the Client Hello from Part 1 of this exercise, in which event does the OS send the Client Hello to Apache?

100

   d. Using what you know about the Server Hello from Part 1 of this exercise, in which event does Apache send the Server Hello to the client?

131

   e. Create a filter for all read and write calls (sysdig.event_name in {}). Between the connection acceptance and Server Hello, are any cryptography-related files accessed during the TLS setup?

/dev/urandom - pseudorandom bits used as a seed for encryption keys

f. After the Server Hello is sent, the client sends an HTTP request, and the server sends a response. What file contains the information the client is requesting?

/var/www/html/index.html