Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente con confianza media

Imagen que contiene Tabla

Descripción generada automáticamente

Explicación de los mensajes

Este mensaje es una captura de un paquete TCP enviado desde la dirección IP 1.1.1.1 hacia la dirección IP 192.168.1.6.

499 51.155381 1.1.1.1 192.168.1.6 TCP 66 853 → 52817 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK\_PERM WS=8192:

499: es el número de secuencia del mensaje.

51.155381: es el tiempo en el que se capturó el mensaje.

1.1.1.1: es la dirección IP del host emisor.

192.168.1.6: es la dirección IP del host receptor.

TCP: es el protocolo de capa de transporte utilizado en esta conexión.

853: es el número de puerto de origen utilizado en esta conexión.

52817: es el número de puerto de destino utilizado en esta conexión.

[SYN, ACK]: son los flags establecidos en este mensaje. SYN indica que se está iniciando una nueva conexión, y ACK indica que se está confirmando la recepción del mensaje anterior.

Seq=0: indica el número de secuencia utilizado en este mensaje.

Ack=1: indica el número de reconocimiento utilizado en este mensaje.

Win=64240: indica el tamaño de la ventana de recepción.

Len=0: indica la longitud del campo de datos.

MSS=1440: indica el tamaño máximo de segmento.

SACK\_PERM: indica que la opción Selective Acknowledgment (SACK) está habilitada.

WS=8192: indica el tamaño de la escala de ventana utilizada.

2///////////////////////////////////////////////////////////////////////////////////////////////////

498 51.101059 192.168.1.6 1.1.1.1 TCP 66 52817 → 853 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM

Este mensaje de captura de Wireshark es una solicitud de conexión SYN (sincronizar) enviada por la dirección IP local 192.168.1.6 al puerto de destino 853 en la dirección IP 1.1.1.1. Esta solicitud contiene la secuencia de inicio de la conexión, que es un número aleatorio seleccionado por el remitente, y también indica que la ventana de recepción del remitente es de 64.240 bytes. Además, especifica que el valor máximo de segmento (MSS) para la conexión es de 1460 bytes y que se ha habilitado la negociación selectiva de acuse de recibo (SACK). La ventana de escala (WS) se establece en 256 para permitir una ventana de recepción más grande.

3////////////////////////////////////////////////////////////////////////////////////////////////////

500 51.155430 192.168.1.6 1.1.1.1 TCP 54 52817 → 853 [ACK] Seq=1 Ack=1 Win=263424 Len=0

Este mensaje es una confirmación de que el servidor remoto (1.1.1.1) ha respondido al mensaje SYN enviado por el cliente local (192.168.1.6) en el puerto de destino 853. El mensaje del cliente fue recibido correctamente, por lo que el servidor responde con un ACK. La secuencia de envío (Seq) se establece en 1, lo que indica que el mensaje ACK es el primer mensaje enviado por el cliente. La secuencia de recepción (Ack) se establece en 1, lo que indica que el servidor remoto ha recibido correctamente el mensaje SYN enviado por el cliente. El campo de longitud (Len) se establece en 0, lo que significa que el mensaje no contiene datos adicionales.

4////////////////////////////////////////////////////////////////////////////////////////////////////

501 51.155647 192.168.1.6 1.1.1.1 TLSv1.3 646 Client Hello

Este mensaje de captura corresponde a un cliente que está intentando establecer una conexión segura con un servidor utilizando el protocolo TLS versión 1.3. El mensaje "Client Hello" indica que el cliente está enviando una solicitud al servidor para iniciar el proceso de negociación de TLS.

Por lo general, este mensaje es el primer paso en el proceso de negociación de TLS y sirve como una forma de iniciar una conexión segura con el servidor.

5////////////////////////////////////////////////////////////////////////////////////////////////////

502 51.178381 1.1.1.1 192.168.1.6 TCP 60 853 → 52817 [ACK] Seq=1 Ack=593 Win=65536 Len=0

En este mensaje, el servidor (1.1.1.1) está confirmando la recepción del paquete anterior enviado por el cliente (192.168.1.6). El servidor envía un paquete TCP con la bandera ACK establecida, indicando que ha recibido todos los datos que se le enviaron hasta ese momento y confirma que el siguiente número de secuencia esperado del cliente es 593. El campo Win indica el tamaño de la ventana de recepción del servidor, que indica la cantidad de datos que el servidor está dispuesto a recibir sin enviar confirmaciones adicionales. En este caso, la ventana es de 65536 bytes, lo que significa que el servidor puede aceptar 65536 bytes de datos sin necesidad de enviar una confirmación adicional. El campo Len indica la longitud del paquete, que en este caso es cero.

6////////////////////////////////////////////////////////////////////////////////////////////////////

503 51.178381 1.1.1.1 192.168.1.6 TLSv1.3 241 Server Hello, Change Cipher Spec, Application Data\

En esta captura de Wireshark, se puede observar lo siguiente:

51.178381: Este es el tiempo transcurrido desde el inicio de la captura hasta que se capturó este paquete.

1.1.1.1: Es la dirección IP del servidor con el que se está comunicando.

192.168.1.6: Es la dirección IP del cliente que está iniciando la comunicación.

TLSv1.3: Es el protocolo de seguridad que se está utilizando para la comunicación.

241: Este es el tamaño en bytes del paquete capturado.

Server Hello: Es un mensaje que indica que el servidor está respondiendo a la solicitud del cliente, confirmando que se establecerá una conexión segura.

Change Cipher Spec: Es un mensaje que indica que se cambiará la forma en que se cifrará la información que se intercambia entre el cliente y el servidor.

Application Data: Es un mensaje que indica que se empezará a enviar información de aplicación (por ejemplo, datos de una página web) de forma segura y cifrada.

7////////////////////////////////////////////////////////////////////////////////////////////////////

504 51.178707 192.168.1.6 1.1.1.1 TLSv1.3 60 Change Cipher Spec

En el paquete 504, se muestra un mensaje de "Change Cipher Spec" enviado desde el cliente (IP: 192.168.1.6) al servidor (IP: 1.1.1.1) a través del protocolo TLSv1.3. Este mensaje indica que el cliente está cambiando la forma en que cifra los datos para la comunicación segura. En este punto, el cliente y el servidor han acordado un cifrado para la comunicación y ahora el cliente está indicando que cambiará su cifrado para usar el acordado. Este mensaje es importante porque garantiza que el cliente y el servidor estén utilizando la misma forma de cifrado para la comunicación segura.

8////////////////////////////////////////////////////////////////////////////////////////////////////

505 51.178842 192.168.1.6 1.1.1.1 TLSv1.3 128 Application Data

El paquete número 505 es una trama de la capa de protocolo TLSv1.3 que contiene datos de aplicación. En la comunicación TLS, después de que se realiza el intercambio de saludos y se acuerda el cifrado, se pueden transmitir datos de aplicación cifrados de forma segura. En este paquete, el cliente envía datos de aplicación al servidor, aunque no es posible saber qué tipo de datos son, ya que están cifrados.

En resumen, este paquete representa la transmisión de datos cifrados de la aplicación por parte del cliente al servidor.

9////////////////////////////////////////////////////////////////////////////////////////////////////

508 51.200752 1.1.1.1 192.168.1.6 TCP 60 853 → 52817 [ACK] Seq=188 Ack=781 Win=65536 Len=0

En este paquete, el servidor (1.1.1.1) está enviando un mensaje de confirmación (ACK) al cliente (192.168.1.6), confirmando la recepción de datos anteriores. El número de secuencia es 188 y el número de reconocimiento (ACK) es 781, lo que significa que el servidor espera recibir el siguiente segmento de datos desde el cliente empezando desde el byte 781. Además, el tamaño de la ventana (Win) es de 65536, lo que indica que el servidor tiene suficiente espacio en su buffer para recibir más datos del cliente.

10////////////////////////////////////////////////////////////////////////////////////////////////////

509 51.202369 1.1.1.1 192.168.1.6 TLSv1.3 996 Application Data, Application Data

Este paquete es un flujo de datos cifrados enviado por el servidor a la dirección IP 192.168.1.6 (el cliente). El flujo de datos es parte de una conexión segura TLSv1.3 establecida previamente entre el cliente y el servidor.

El paquete contiene 996 bytes de datos de aplicación cifrados. No se puede leer el contenido real de los datos, ya que están cifrados. Sin embargo, podemos observar que el servidor está enviando datos de aplicación al cliente, lo que indica que la conexión está en curso y funcionando correctamente.

11////////////////////////////////////////////////////////////////////////////////////////////////////

653 61.384457 1.1.1.1 192.168.1.6 TCP 60 853 → 52817 [FIN, ACK] Seq=5462 Ack=1320 Win=65536 Len=0

Este paquete es una respuesta de finalización de la conexión TCP. El servidor (1.1.1.1) está enviando un mensaje de cierre a la dirección IP de la máquina cliente (192.168.1.6). El paquete incluye la bandera FIN, que indica que el servidor ha terminado su transmisión de datos y está cerrando la conexión. Además, también incluye la bandera ACK, lo que indica que el servidor ha recibido todos los datos enviados por la máquina cliente hasta el momento. El campo Seq indica el último número de secuencia recibido por el servidor, y el campo Ack indica el último número de secuencia esperado por el servidor. El campo Win muestra el tamaño de ventana que el servidor está dispuesto a aceptar para la transmisión de datos. En este caso, el servidor ha recibido 1320 bytes de datos de la máquina cliente y ha enviado 5462 bytes de datos.

12////////////////////////////////////////////////////////////////////////////////////////////////////

654 61.384490 192.168.1.6 1.1.1.1 TCP 54 52817 → 853 [ACK] Seq=1320 Ack=5463 Win=263424 Len=0

En este paquete (654) vemos la confirmación del cliente del cierre de la conexión, ya que el servidor ha enviado un paquete (653) indicando el FIN de la comunicación. El cliente envía un paquete con el flag ACK activado para confirmar que ha recibido el paquete FIN y está cerrando la conexión correctamente.

13////////////////////////////////////////////////////////////////////////////////////////////////////

655 61.384725 192.168.1.6 1.1.1.1 TCP 54 52817 → 853 [FIN, ACK] Seq=1320 Ack=5463 Win=263424 Len=0

Este paquete es una respuesta del cliente al paquete anterior enviado por el servidor (número 653). El cliente envía un paquete con la bandera FIN, ACK para indicar que ha terminado su sesión de comunicación y ya no enviará más datos al servidor. El campo Seq es igual al último número de secuencia recibido del servidor (5463) y el campo Ack es igual al último número de secuencia recibido más uno (5463 + 1 = 5464). El campo Win indica la cantidad de espacio disponible en el búfer del cliente para recibir datos.

14////////////////////////////////////////////////////////////////////////////////////////////////////

656 61.407468 1.1.1.1 192.168.1.6 TCP 60 853 → 52817 [ACK] Seq=5463 Ack=1321 Win=65536 Len=0

Este paquete es una confirmación del servidor de que ha recibido correctamente el paquete de finalización enviado por el cliente en el paquete 655. Tiene la información de la secuencia y el número de reconocimiento, donde Seq=5463 indica que el servidor ha recibido 5463 bytes de datos del cliente y Ack=1321 indica que el servidor espera recibir 1321 bytes de datos del cliente en el futuro. El campo Win=65536 indica el tamaño actual de la ventana de recepción del servidor. Además, el campo Len=0 indica que el paquete no contiene datos.

El filtro tcp.port == 853 significa que se están filtrando solo los paquetes que usan el puerto 853. En este contexto específico, este puerto se refiere al servicio DNS-over-TLS (DoT), que proporciona una forma segura de comunicarse con un servidor DNS utilizando el protocolo TLS.

Después de ver todos los paquetes, podemos concluir que se estableció una conexión segura entre el cliente DNS (192.168.1.6) y el servidor DNS (1.1.1.1) utilizando el protocolo DNS-over-TLS (DoT). Los paquetes 498 y 499 son los paquetes de inicio de la conexión TCP, seguidos del paquete 501 que contiene un "Client Hello" (solicitud de conexión TLS) del cliente y el paquete 503 que contiene un "Server Hello" (confirmación de conexión TLS) del servidor. Luego, se intercambian paquetes cifrados usando TLS (paquetes 504, 505 y 509). Finalmente, la conexión se cierra de manera segura mediante los paquetes 653, 654 y 655.