# Cómo leer un registro TCP/HTTP de Wireshark

En esta lectura, aprenderá a leer un registro TCP/HTTP de Wireshark para el tráfico de red entre los visitantes del sitio web de los empleados y el servidor web de la empresa. La mayoría de las herramientas de análisis de tráfico/protocolo de red utilizadas para capturar paquetes proporcionarán esta misma información.

## Número y hora de entrada de registro

|  |  |
| --- | --- |
| **No.** | **Hora** |
| 47 | 3.144521 |
| 48 | 3.195755 |
| 49 | 3.246989 |

Esta sección de registro TCP de Wireshark que se le proporciona comienza en el número de entrada de registro (n.º) 47, que es tres segundos y 0,144521 milisegundos después de que la herramienta de registro comenzara a grabar. Esto indica que el servidor web envió y recibió aproximadamente 47 mensajes en los 3,1 segundos posteriores al inicio del registro. Esta rápida velocidad del tráfico es la razón por la que la herramienta realiza un seguimiento del tiempo en milisegundos.

## Direcciones IP de origen y destino

|  |  |
| --- | --- |
| **Fuente** | **Destino** |
| 198.51.100.23 | 192.0.2.1 |
| 192.0.2.1 | 198.51.100.23 |
| 198.51.100.23 | 192.0.2.1 |

Las columnas de origen y destino contienen la dirección IP de origen del equipo que envía un paquete y la dirección IP de destino prevista del paquete. En este archivo de registro, la dirección IP 192.0.2.1 pertenece al servidor web de la empresa. El rango de direcciones IP en 198.51.100.0/24 pertenece a los equipos de los empleados.

## Tipo de protocolo e información relacionada

|  |  |
| --- | --- |
| **Protocolo** | **Información** |
| TCP | 42584->443 [SYN] Seq=0 Win-5792 Len=120... |
| TCP | 443->42584 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| TCP | 42584->443 [ACK] Seq=1 Win-5792 Len=120... |

La columna Protocolo indica que los paquetes se envían mediante el protocolo TCP, que se encuentra en la capa de transporte del modelo TCP/IP. En el archivo de registro dado, notará que el protocolo eventualmente cambiará a HTTP, en la capa de la aplicación, una vez que la conexión con el servidor web se haya establecido con éxito.

La columna Información proporciona información sobre el paquete. Enumera el puerto de origen seguido de una flecha → que apunta al puerto de destino. En este caso, el puerto 443 pertenece al servidor web. El puerto 443 se utiliza normalmente para el tráfico web cifrado.

El siguiente elemento de datos proporcionado en la columna Información es parte del proceso de protocolo de enlace de tres vías para establecer una conexión entre dos máquinas. En este caso, los empleados están intentando conectarse al servidor web de la empresa:

* El paquete [SYN] es la solicitud inicial de un empleado visitante que intenta conectarse a una página web alojada en el servidor web. SYN significa "sincronizar".
* El paquete [SYN, ACK] es la respuesta del servidor web a la solicitud del visitante que acepta la conexión. El servidor reservará los recursos del sistema para el paso final del protocolo de enlace. SYN, ACK significa "sincronizar reconocimiento".
* El paquete [ACK] es la máquina del visitante que reconoce el permiso para conectarse. Este es el paso final necesario para realizar una conexión TCP exitosa. ACK significa "reconocimiento".

Los siguientes elementos de la columna Información proporcionan más detalles sobre los paquetes. Sin embargo, estos datos no son necesarios para completar esta actividad. Si desea obtener más información sobre las propiedades de los paquetes, visite [la Introducción al análisis de seguimiento de red de Microsoft](https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/introduction-to-network-trace-analysis-3-tcp-performance/ba-p/3737115).

## Tráfico normal del sitio web

Una transacción normal entre un visitante del sitio web y el servidor web sería como:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Hora** | **Fuente** | **Destino** | **Protocolo** | **Información** |
| 47 | 3.144521 | 198.51.100.23 | 192.0.2.1 | TCP | 42584->443 [SYN] Seq=0 Win=5792 Len=120... |
| 48 | 3.195755 | 192.0.2.1 | 198.51.100.23 | TCP | 443->42584 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| 49 | 3.246989 | 198.51.100.23 | 192.0.2.1 | TCP | 42584->443 [ACK] Seq=1 Win-5792 Len=120... |
| 50 | 3.298223 | 198.51.100.23 | 192.0.2.1 | HTTP | OBTENER /sales.html HTTP/1.1 |
| 51 | 3.349457 | 192.0.2.1 | 198.51.100.23 | HTTP | HTTP/1.1 200 OK (texto/html) |

Tenga en cuenta que el proceso de protocolo de enlace tarda unos milisegundos en completarse. A continuación, puede identificar el navegador del empleado que solicita la página web sales.html utilizando el protocolo HTTP en el nivel de aplicación del modelo TCP/IP. Seguido por el servidor web que responde a la solicitud.

## El ataque

Como aprendió anteriormente, los actores malintencionados pueden aprovechar el protocolo TCP inundando un servidor con solicitudes de paquetes SYN para la primera parte del protocolo de enlace. Sin embargo, si el número de solicitudes SYN es mayor que los recursos del servidor disponibles para manejar las solicitudes, el servidor se verá abrumado y no podrá responder a las solicitudes. Se trata de un ataque de denegación de servicio (DoS) a nivel de red, denominado ataque de inundación SYN, que se dirige al ancho de banda de la red para ralentizar el tráfico. Un ataque de inundación SYN simula una conexión TCP e inunda el servidor con paquetes SYN. Un ataque directo DoS se origina en una sola fuente. Un ataque de denegación de servicio distribuido (DDoS) proviene de múltiples fuentes, a menudo en diferentes ubicaciones, lo que dificulta la identificación del atacante o los atacantes.



Hay dos pestañas en la parte inferior del archivo de registro. Uno de ellos está etiquetado como "Registro TCP codificado por colores". Si hace clic en esa pestaña, encontrará las interacciones del servidor con la dirección IP del atacante (203.0.113.0) marcada con un resaltado rojo (y la palabra "rojo" en la columna A).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Color como texto** | **No.** | **Hora** | **Fuente (x = censurado)** | **Destino (x = censurado)** | **Protocolo** | **Información** |
| rojo | 52 | 3.390692 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 53 | 3.441926 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| rojo | 54 | 3.493160 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [ACK Seq=1 Win=5792 Len=0... |
| verde | 55 | 3.544394 | 198.51.100.14 | 192.0.2.1 | TCP | 14785->443 [SYN] Seq=0 Win-5792 Len=120... |
| verde | 56 | 3.599628 | 192.0.2.1 | 198.51.100.14 | TCP | 443->14785 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| rojo | 57 | 3.664863 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| verde | 58 | 3.730097 | 198.51.100.14 | 192.0.2.1 | TCP | 14785->443 [ACK] Seq=1 Win-5792 Len=120... |
| rojo | 59 | 3.795332 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win-5792 Len=120... |
| verde | 60 | 3.860567 | 198.51.100.14 | 192.0.2.1 | HTTP | OBTENER /sales.html HTTP/1.1 |
| rojo | 61 | 3.939499 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win-5792 Len=120... |
| verde | 62 | 4.018431 | 192.0.2.1 | 198.51.100.14 | HTTP | HTTP/1.1 200 OK (texto/html) |

Inicialmente, el servidor web responde normalmente a la solicitud SYN del atacante (elementos de registro 52-54). Sin embargo, el atacante sigue enviando más solicitudes SYN, lo cual es anormal. En este punto, el servidor web todavía puede responder al tráfico normal de visitantes, que está resaltado y etiquetado en verde. Un visitante empleado con la dirección IP 198.51.100.14 completa con éxito un protocolo de enlace de conexión SYN/ACK con el servidor web (elementos de registro n.º 55, 56, 58). A continuación, el navegador del empleado solicita la página web sales.html con el comando GET y el servidor web responde (elementos de registro n.º 60 y 62).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Color como texto** | **No.** | **Hora** | **Fuente** | **Destino** | **Protocolo** | **Información** |
| verde | 63 | 4.097363 | 198.51.100.5 | 192.0.2.1 | TCP | 33638->443 [SYN] Seq=0 Win-5792 Len=120... |
| rojo | 64 | 4.176295 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| verde | 65 | 4.255227 | 192.0.2.1 | 198.51.100.5 | TCP | 443->33638 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| rojo | 66 | 4.256159 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| verde | 67 | 5.235091 | 198.51.100.5 | 192.0.2.1 | TCP | 33638->443 [ACK] Seq=1 Win-5792 Len=120... |
| rojo | 68 | 5.236023 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| verde | 69 | 5.236955 | 198.51.100.16 | 192.0.2.1 | TCP | 32641->443 [SYN] Seq=0 Win-5792 Len=120... |
| rojo | 70 | 5.237887 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| verde | 71 | 6.228728 | 198.51.100.5 | 192.0.2.1 | HTTP | OBTENER /sales.html HTTP/1.1 |
| rojo | 72 | 6.229638 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| amarillo | 73 | 6.230548 | 192.0.2.1 | 198.51.100.16 | TCP | 443->32641 [RST, ACK] Seq=0 Win-5792 Len=120... |
| rojo | 74 | 6.330539 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| verde | 75 | 6.330885 | 198.51.100.7 | 192.0.2.1 | TCP | 42584->443 [SYN] Seq=0, Win=5792, Len=0... |
| rojo | 76 | 6.331231 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| amarillo | 77 | 7.330577 | 192.0.2.1 | 198.51.100.5 | TCP | HTTP/1.1 504 Tiempo de espera de puerta de enlace (texto/html) |
| rojo | 78 | 7.331323 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| verde | 79 | 7.340768 | 198.51.100.22 | 192.0.2.1 | TCP | 6345->443 [SYN] Seq=0 Win=5792 Len=0... |
| amarillo | 80 | 7.340773 | 192.0.2.1 | 198.51.100.7 | TCP | 443->42584 [RST, ACK] Seq=1 Win-5792 Len=120... |
| rojo | 81 | 7.340778 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 82 | 7.340783 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 83 | 7.439658 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0... |

En las siguientes 20 filas, el registro comienza a reflejar la lucha que tiene el servidor web para mantenerse al día con el número anormal de solicitudes SYN que llegan a un ritmo rápido. El atacante envía varias solicitudes SYN por segundo. Las filas resaltadas y etiquetadas en amarillo son comunicaciones fallidas entre los visitantes legítimos del sitio web de los empleados y el servidor web.

Los dos tipos de errores en los registros incluyen:

* Un mensaje de error HTTP/1.1 504 Gateway Time-out (text/html). Este mensaje es generado por un servidor de puerta de enlace que estaba esperando una respuesta del servidor web. Si el servidor web tarda demasiado en responder, el servidor de puerta de enlace enviará un mensaje de error de tiempo de espera al navegador solicitante.
* Un paquete [RST, ACK], que se enviaría al visitante solicitante si el servidor web no recibe el paquete [SYN, ACK]. RST significa reinicio, reconocimiento. El visitante recibirá un mensaje de error de tiempo de espera en su navegador y se interrumpirá el intento de conexión. El visitante puede actualizar su navegador para intentar enviar una nueva solicitud SYN.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Color**  **como texto** | **No.** | **Hora** | **Fuente**  **(x = censurado)** | **Destino**  **(x = censurado)** | **Protocolo** | **Información** |
| rojo | 119 | 19.198705 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 120 | 19.521718 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| amarillo | 121 | 19.844731 | 192.0.2.1 | 198.51.100.9 | TCP | 443->4631 [RST, ACK] Seq=1 Win=5792 Len=0... |
| rojo | 122 | 20.167744 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 123 | 20.490757 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 124 | 20.81377 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0... |
| rojo | 125 | 21.136783 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 126 | 21.459796 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 127 | 21.782809 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 128 | 22.105822 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 129 | 22.428835 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 130 | 22.751848 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 131 | 23.074861 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 132 | 23.397874 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 133 | 23.720887 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 134 | 24.0439 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 135 | 24.366913 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 136 | 24.689926 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 137 | 25.012939 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 138 | 25.335952 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 139 | 25.658965 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 140 | 25.981978 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 141 | 26.304991 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 142 | 26.628004 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 143 | 26.951017 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 144 | 27.27403 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 145 | 27.597043 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 146 | 27.920056 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 147 | 28.243069 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 148 | 28.566082 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 149 | 28.889095 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 150 | 29.212108 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 151 | 29.535121 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| rojo | 152 | 29.858134 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |

A medida que se desplaza por el resto del registro, notará que el servidor web deja de responder al tráfico legítimo de visitantes de empleados. Los visitantes reciben más mensajes de error que indican que no pueden establecer o mantener una conexión con el servidor web. A partir del elemento de registro número 125, el servidor web deja de responder. Los únicos elementos registrados en ese punto son del ataque. Como solo hay una dirección IP que ataca el servidor web, puede suponer que se trata de un ataque directo de inundación DoS SYN.