Cómo leer el registro TCP/HTTP de Wireshark

En esta lectura, aprenderás cómo leer el registro TCP/HTTP de Wireshark proporcionado para el tráfico de red entre visitantes del sitio web para empleados/as 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 tiempo de la entrada en el registro

No.	Time
47	3.144521
48	3.195755
49	3.246989

La sección de registro TCP de Wireshark que se te proporcionó comienza en el número de entrada de registro (Nº) 47, que es de tres segundos y 0,144521 milisegundos después de que la herramienta de registro comenzó 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 velocidad de tráfico rápida es la razón por la cual la herramienta registra el tiempo en milisegundos.

Direcciones IP de origen y destino

Source	Destination
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 de la máquina 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 las computadoras de los/las empleados/as.

Tipo de protocolo e información relacionada

Protocol	Info
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 Protocol indica que los paquetes se envían utilizando el protocolo TCP, que se encuentra en la capa de transporte del modelo TCP/IP. En el archivo de registro, notarás que el protocolo eventualmente cambiará a HTTP, en la capa de aplicación, una vez que la conexión con el servidor web se haya establecido correctamente.

La columna Info 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 que aparece en la columna Info es parte del 3-way handshake (protocolo de acuerdo de 3 vías) para establecer una conexión entre dos máquinas. En este caso, los/las empleados/as están tratando de conectarse al servidor web de la empresa:

- El paquete [SYN] es la solicitud inicial de un/a empleado/a visitante que intenta conectarse a una página web alojada en el servidor web. SYN significa “sincronización”.
- El paquete [SYN, ACK] es la respuesta del servidor web a la solicitud del/de la visitante que acepta la conexión. El servidor reservará recursos del sistema para el paso final del handshake (acuerdo de comunicación). SYN, ACK significa “acuse de recibo de la sincronización” (synchronize acknowledgement).
- El paquete [ACK] es el reconocimiento del permiso de conexión por parte de la máquina del/de la visitante. Este es el paso final requerido para realizar una conexión TCP con éxito. ACK significa “acuse de recibo”.

Los siguientes elementos de la columna Info proporcionan más detalles sobre los paquetes. Sin embargo, estos datos no son necesarios para completar esta actividad. Si deseas obtener más información sobre las propiedades de los paquetes, visita la Introducción al análisis de seguimiento de red de Microsoft.

Tráfico normal del sitio web

Una transacción normal entre el visitante de un sitio web y el servidor web podría ser así:

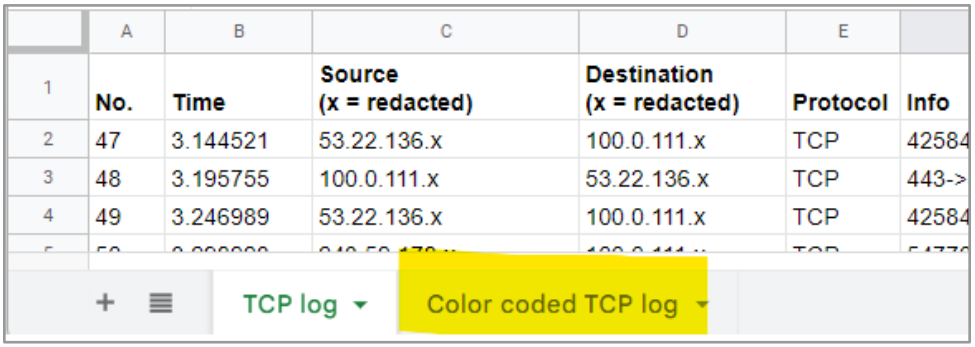
No.	Time	Source	Destination	Protocol	Info

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	GET /sales.html HTTP/1.1
51	3.349457	192.0.2.1	198.51.100.23	HTTP	HTTP/1.1 200 OK (text/html)

Ten en cuenta que el handshake tarda unos milisegundos en completarse. A continuación, puedes identificar el navegador del/de la empleado/a que solicita la página web sales.html mediante el uso del protocolo HTTP en el nivel de aplicación del modelo TCP/IP, seguido por el servidor web que responde a la solicitud.

El ataque

Como aprendiste anteriormente, los agentes de amenaza pueden aprovecharse del protocolo TCP inundando un servidor con solicitudes de paquetes SYN para la primera parte del handshake. Sin embargo, si el número de solicitudes SYN es superior a los recursos del servidor disponibles para atenderlas, el servidor se verá desbordado y no podrá responder a las solicitudes. Se trata de un ataque de denegación de servicio (DoS) a nivel de red, llamado ataque de inundación sincronizada (SYN), que se dirige al ancho de banda de la red para ralentizar el tráfico. Un ataque de inundación sincronizada (SYN) simula una conexión TCP e inunda el servidor con paquetes SYN. Un ataque directo DoS se origina desde una única 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 atacantes.



[TEXTO ALTERNATIVO: Hay dos pestañas en la hoja de cálculo de registro: registro TCP y registro TCP codificado por colores]

Hay dos pestañas en la parte inferior del archivo de registro. Una está etiquetada como “Registro TCP codificado por colores”. Si haces clic en esa pestaña, encontrarás las interacciones del servidor con la dirección IP del (203.0.113.0) marcadas con resaltador rojo (y la palabra “rojo” en la columna A).

Color as text	No.	Time	Source (x = redacted)	Destination (x = redacted)	Protocol	Info
red	52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	53	3.441926	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
red	54	3.493160	203.0.113.0	192.0.2.1	TCP	54770->443 [ACK Seq=1 Win=5792 Len=0...
green	55	3.544394	198.51.100.14	192.0.2.1	TCP	14785->443 [SYN] Seq=0 Win-5792 Len=120...
green	56	3.599628	192.0.2.1	198.51.100.14	TCP	443->14785 [SYN, ACK] Seq=0 Win-5792 Len=120...
red	57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	58	3.730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK] Seq=1 Win-5792 Len=120...
red	59	3.795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
green	60	3.860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
red	61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
green	62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)

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

Color as text	No.	Time	Source	Destination	Protocol	Info
green	63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0

						Win-5792 Len=120...
red	64	4.176295	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
green	65	4.255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win-5792 Len=120...
red	66	4.256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	67	5.235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK] Seq=1 Win-5792 Len=120...
red	68	5.236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	69	5.236955	198.51.100.16	192.0.2.1	TCP	32641->443 [SYN] Seq=0 Win-5792 Len=120...
red	70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	71	6.228728	198.51.100.5	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
red	72	6.229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow	73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win-5792 Len=120...
red	74	6.330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	75	6.330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
red	76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow	77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
red	78	7.331323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	79	7.340768	198.51.100.22	192.0.2.1	TCP	6345->443 [SYN] Seq=0 Win=5792 Len=0...
yellow	80	7.340773	192.0.2.1	198.51.100.7	TCP	443->42584 [RST, ACK] Seq=1 Win-5792 Len=120...
red	81	7.340778	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	82	7.340783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	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 cómo el servidor web está luchando para mantener el ritmo frente al número anormal de solicitudes SYN que llegan a gran velocidad. La/el atacante está enviando varias solicitudes SYN cada 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 de tiempo de espera de la puerta de enlace HTTP/1.1 504 (texto/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/a la visitante solicitante si el paquete [SYN, ACK] no es recibido por el servidor web. RST significa reiniciar, reconocer. La/el visitante recibirá un mensaje de error de tiempo de espera en su navegador y se abandonará el intento de conexión. La/el visitante puede actualizar su navegador para intentar enviar una nueva solicitud SYN.

Color as text	No.	Time	Source (x = redacted)	Destination (x = redacted)	Protocol	Info
red	119	19.198705	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	120	19.521718	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow	121	19.844731	192.0.2.1	198.51.100.9	TCP	443->4631 [RST, ACK] Seq=1 Win=5792 Len=0...
red	122	20.167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	123	20.490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	124	20.81377	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red	125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

red	127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	130	22.751848	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	131	23.074861	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	132	23.397874	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	133	23.720887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	134	24.0439	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	135	24.366913	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	136	24.689926	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	137	25.012939	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	138	25.335952	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	139	25.658965	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	140	25.981978	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	141	26.304991	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	142	26.628004	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	143	26.951017	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	144	27.27403	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	145	27.597043	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	146	27.920056	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	147	28.243069	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0

						Win=5792 Len=0...
red	148	28.566082	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	149	28.889095	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	150	29.212108	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	151	29.535121	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	152	29.858134	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

A medida que te desplaces por el resto del registro, observarás que el servidor web deja de responder al tráfico legítimo de empleados/as visitantes. Las/los visitantes reciben más mensajes de error que indican que no pueden establecer o mantener una conexión con el servidor web. A partir del número de elemento de registro 125, el servidor web deja de responder. Los únicos elementos registrados en ese punto proceden del ataque. Como solo hay una dirección IP que ataca el servidor web, puedes asumir que se trata de un ataque directo de inundación DoS SYN.