Como ler um log TCP/HTTP do Wireshark

Nesta leitura, você aprenderá a ler um log TCP/HTTP do Wireshark para tráfego de rede entre os visitantes do site do funcionário e o servidor web da empresa. A maioria das ferramentas de protocolo de rede/analisador de tráfego usadas para capturar pacotes fornecerá essas mesmas informações.

Número e hora da entrada do log

No.	Tempo
47	3.144521
48	3.195755
49	3.246989

Esta seção de log TCP do Wireshark fornecida a você começa na entrada de log número (nº) 47, que é três segundos e 0,144521 milissegundos após a ferramenta de registro ter iniciado a gravação. Isso indica que aproximadamente 47 mensagens foram enviadas e recebidas pelo servidor web nos 3,1 segundos após o início do log. Essa alta velocidade de tráfego é o motivo pelo qual a ferramenta registra o tempo em milissegundos.

Endereços IP de origem e destino

Fonte	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

As colunas de origem e destino contêm o endereço IP de origem da máquina que está enviando o pacote e o endereço IP de destino pretendido do pacote. Neste arquivo de log, o endereço IP 192.0.2.1 pertence ao servidor web da empresa. O intervalo de endereços IP em 198.51.100.0/24 pertence aos computadores dos funcionários.

Tipo de protocolo e informações relacionadas

Protocolo	Informações
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...

A coluna Protocolo indica que os pacotes estão sendo enviados usando o protocolo TCP, que está na camada de transporte do modelo TCP/IP. No arquivo de log fornecido, você notará que o protocolo eventualmente mudará para HTTP, na camada de aplicação, assim que a conexão com o servidor web for estabelecida com sucesso.

A coluna Info fornece informações sobre o pacote. Ela lista a porta de origem seguida por uma seta ⟶ apontando para a porta de destino. Neste caso, a porta 443 pertence ao servidor web. A porta 443 é normalmente usada para tráfego web criptografado.

O próximo elemento de dados fornecido na coluna Info faz parte do processo de handshake triplo para estabelecer uma conexão entre duas máquinas. Neste caso, os funcionários estão tentando se conectar ao servidor web da empresa:

- O pacote [SYN] é a solicitação inicial de um visitante funcionário que tenta se conectar a uma página web hospedada no servidor web. SYN significa “sincronizar”.
- O pacote [SYN, ACK] é a resposta do servidor web à solicitação do visitante de concordância com a conexão. O servidor irá recursos do sistema de reserva para a etapa final do aperto de mão. SYN, ACK significa “sincronizar reconhecimento”.
- O pacote [ACK] é a máquina do visitante confirmando a permissão de conexão. Esta é a etapa final necessária para estabelecer uma conexão TCP bem-sucedida. ACK significa "reconhecimento".

Os próximos itens na coluna Informações fornecem mais detalhes sobre os pacotes. No entanto, esses dados não são necessários para concluir esta atividade. Se você quiser saber mais sobre as propriedades dos pacotes, visite Introdução da Microsoft à Análise de Rastreamento de Rede.

Tráfego normal do site

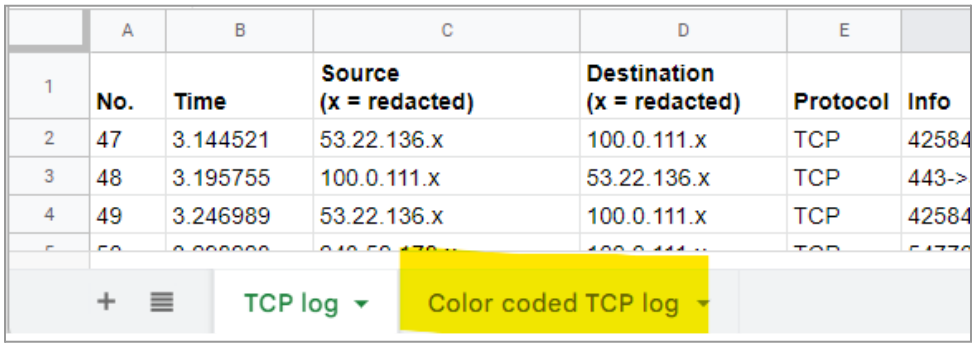
Uma transação normal entre um visitante de um site e o servidor web seria assim:

No.	Tempo	Fonte	Destino	Protocolo	Informações
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)

Observe que o processo de handshake leva alguns milissegundos para ser concluído. Em seguida, você pode identificar o navegador do funcionário que está solicitando a página sales.html usando o protocolo HTTP no nível do aplicativo do modelo TCP/IP. Em seguida, o servidor web responde à solicitação.

O Ataque

Como você aprendeu anteriormente, Atores maliciosos podem tirar vantagem do protocolo TCP inundando um servidor com solicitações de pacotes SYN para a primeira parte do handshake. No entanto,se o número de solicitações SYN for maior que os recursos do servidor disponíveis para lidar com as solicitações, o servidor ficará sobrecarregado e não conseguirá responder às solicitações. Trata-se de um ataque de negação de serviço (DoS) em nível de rede, chamado de **ataque de inundação SYN**, que visa a largura de banda da rede para reduzir o tráfego. Um ataque de inundação SYN simula uma conexão TCP e inunda o servidor com pacotes SYN. **Um ataque direto DoS tem origem em uma única fonte**. Um ataque de negação de serviço distribuído (DDoS) tem origem em múltiplas fontes, geralmente em locais diferentes, dificultando a identificação do(s) invasor(es).



Há duas abas na parte inferior do arquivo de log. Uma delas é chamada de "Log TCP codificado por cores". Se você clicar nessa aba, encontrará as interações do servidor com o endereço IP do invasor (203.0.113.0) marcadas em vermelho (e a palavra "vermelho" na coluna A).

Cor como texto	Não.	Tempo	Fonte (x = redigido)	Destino (x = redigido)	Protocolo	Informações
vermelho	52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	53	3.441926	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
vermelho	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...
vermelho	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...
vermelho	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	OBTER /vendas.html HTTP/1.1
vermelho	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, a solicitação SYN do invasor é respondida normalmente pelo servidor web (itens de log 52 a 54). No entanto, o invasor continua enviando mais solicitações SYN, o que é anormal. Nesse ponto, o servidor web ainda consegue responder ao tráfego normal de visitantes, que é destacado e marcado em verde. Um visitante funcionário com o endereço IP 198.51.100.14 conclui com sucesso um handshake de conexão SYN/ACK com o servidor web (itens de log n.º 55, 56 e 58). Em seguida, o navegador do funcionário solicita a página sales.html com o comando GET e o servidor web responde (itens de log n.º 60 e 62).

Cor como texto	Não.	Tempo	Fonte	Destino	Protocolo	Informações
verde	63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0

						Win-5792 Len=120...
vermelho	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...
vermelho	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...
vermelho	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...
vermelho	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	OBTER /vendas.html HTTP/1.1
vermelho	72	6.229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
amarelo	73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win-5792 Len=120...
vermelho	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...
vermelho	76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
amarelo	77	7.330577	192.0.2.1	198.51.100.5	TCP	Tempo limite do gateway HTTP/1.1 504 (texto/html)
vermelho	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...
amarelo	80	7.340773	192.0.2.1	198.51.100.7	TCP	443->42584 [RST, ACK] Seq=1 Win-5792 Len=120...
vermelho	81	7.340778	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermel	82	7.340783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0

ho						Win=5792 Len=0...
vermelho	83	7.439658	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...

Nas próximas 20 linhas, o log começa a refletir a dificuldade que o servidor web está enfrentando para acompanhar o número anormal de solicitações SYN que chegam em ritmo acelerado. O invasor envia várias solicitações SYN a cada segundo. As linhas destacadas e marcadas em amarelo indicam falhas de comunicação entre visitantes legítimos do site de funcionários e o servidor web.

Os dois tipos de erros nos logs incluem:

- Uma mensagem de erro HTTP/1.1 504 Gateway Time-out (texto/html). Esta mensagem é gerada por um servidor gateway que estava aguardando uma resposta do servidor web. Se o servidor web demorar muito para responder, o servidor gateway enviará uma mensagem de erro de tempo limite ao navegador solicitante.
- Um pacote [RST, ACK], que seria enviado ao visitante solicitante caso o pacote [SYN, ACK] não fosse recebido pelo servidor web. RST significa reset, reconhecimento. O visitante receberá uma mensagem de erro de tempo limite no navegador e a tentativa de conexão será interrompida. O visitante pode atualizar o navegador para tentar enviar uma nova solicitação SYN.

Cor como texto	Não.	Tempo	Fonte (x = redigido)	Destino (x = redigido)	Protocolo	Informações
vermelho	119	19.198705	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	120	19.521718	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
amarelo	121	19.844731	192.0.2.1	198.51.100.9	TCP	443->4631 [RST, ACK] Seq=1 Win=5792 Len=0...
vermelho	122	20.167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	123	20.490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	124	20.81377	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
vermel	125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0

ho						Win=5792 Len=0…
vermelho	126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	130	22.751848	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	131	23.074861	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	132	23.397874	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	133	23.720887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	134	24.0439	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	135	24.366913	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	136	24.689926	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	137	25.012939	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	138	25.335952	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	139	25.658965	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	140	25.981978	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	141	26.304991	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	142	26.628004	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…
vermelho	143	26.951017	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0…

vermelho	144	27.27403	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	145	27.597043	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	146	27.920056	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	147	28.243069	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	148	28.566082	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	149	28.889095	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	150	29.212108	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	151	29.535121	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
vermelho	152	29.858134	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

Ao percorrer o restante do log, você notará que o servidor web para de responder ao tráfego legítimo de visitantes de funcionários. Os visitantes recebem mais mensagens de erro indicando que não conseguem estabelecer ou manter uma conexão com o servidor web. A partir do item de log 125, o servidor web para de responder. Os únicos itens registrados neste ponto são do ataque. Como há apenas um endereço IP atacando o servidor web, você pode presumir que se trata de um ataque direto de DoS SYN flood.