# Como ler um log TCP\_HTTP Wireshark

Nesta leitura você irá aprender como ler um log TCP\_HTTP Wireshark para tráfego de rede entre os visitantes do site dos funcionários e o servidor web da empresa. A maioria das ferramentas de análise de protocolo/tráfego de rede usados para capturar pacotes providenciará esta mesma informação.

## Número de entrada de Log e tempo

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

Esta sessão do log TCP Wireshark fornecida a você começa no log de número (No.) 47, que aconteceu 3 segundos e 0.144521 milissegundos depois que a ferramenta de login começou a gravar. Isso indica que aproximadamente 47 mensagens foram enviadas e recebidas pelo servidor web nos 3.1 segundos após começar o log. Essa alta velocidade de tráfego é o porquê a ferramenta rastreia o tempo em milissegundos.

## Endereços de IP de origem e destino

|  |  |
| --- | --- |
| **Origem** | **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 contém o IP de origem da máquina que está enviando o pacote e o endereço de IP de destino pretendido do pacote. Neste arquivo de log, o endereço de IP 192.0.2.1 pertence ao servidor web da empresa. O range de endereços de IP 198.51.100.0/24 pertencem aos computadores dos funcionários.

## Tipos de protocolo e informações relacionadas

|  |  |
| --- | --- |
| **Protocolo** | **Informação** |
| 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 de Protocolo indica que os pacotes estão sendo enviados usando o protocolo TCP, que pertence à 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, uma vez que a conexão com o servidor web for estabelecida com sucesso.

A coluna Informação fornece informações sobre o pacote. Ali estão listados a porta de origem seguido por uma flecha -> apontando para a porta de destino. Neste caso, a porta 443 pertence ao servidor web. A porta 443 é geralmente usada para tráfego de rede criptografado.

O próximo elemento fornecido na coluna Informação é parte do processo de aperto de mão em três etapas, usado para estabelecer uma conexão entre duas máquinas. Neste caso, funcionários tentando se conectar ao servidor web da empresa:

* O pacote [SYN] é a exigência inicial para um funcionário tentando se conectar com uma página web hospedada no servidor web. SYN vem de “synchronize” (sincronizar).
* O pacote [SYN, ACK] é a resposta do servidor web para o pedido do visitante, concordando com a conexão. O servidor irá alocar recursos para a etapa final do aperto de mão. SYN ACK vem de “synchronize acknowledge.” (sincronizar reconhecimento).
* O pacote [ACK] é a máquina do visitante reconhecendo a permissão para conectar. Esta é a etapa final exigida para estabelecer com sucesso uma conexão TCP. ACK vem de “acknowledge” (reconhecimento).

Os próximos poucos itens na coluna Informação fornecem mais detalhes sobre os pacotes. No entanto, estas informações não são necessárias para completar esta atividade. Se você tem interesse em aprender mais sobre as propriedades dos pacotes, por favor visite a página [Microsoft’s Introduction to Network Trace Analysis](https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/introduction-to-network-trace-analysis-3-tcp-performance/ba-p/3737115).

## Tráfego normal no site

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Tempo** | **Origem** | **Destino** | **Protocolo** | **Informação** |
| 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) |

Note que o processo de aperto de mão leva milissegundos para concluir. Logo após, você pode identificar o browser do funcionário solicitando a página sales.html usando o protocolo HTTP na camada de aplicação no modelo TCP/IP. Seguido pelo servidor web respondendo ao pedido.

## **O ataque**

Como você aprendeu anteriormente, atacantes podem tirar vantagem dos protocolos TCP inundando um servidor com pedidos de pacotes SYN para a primeira etapa do aperto de mão. No entanto, se o número de solicitações de pacote SYN for maior que o número total que o servidor pode lidar, então o servidor ficará sobrecarregado e indisponível a responder as solicitações. Este é um ataque de negação de serviço (DoS) em nível de rede, chamado de ataque SYN flood, que mira a largura de banda da rede para diminuir o tráfego. Um ataque SYN flood simula uma conexão TCP e inunda o servidor com pacotes SYN. Um ataque DoS direto se origina de uma origem única. Um ataque distribuído de negação de serviço (DDoS) vem de múltiplas origens, geralmente em localizações diferentes, tornando mais difícil identificar o atacante ou atacantes.



Há duas tabelas de arquivos de log abaixo. Uma está rotulada como “Color coded TCP log”. Nesta tabela você encontra interações do servidor com o endereço IP do atacante (203.0.113.0) marcadas e destacadas em vermelho (com a palavra “red” na primeira coluna).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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, o pedido SYN do atacante é respondido normalmente pelo servidor web (log items 52-54). No entanto, o atacante continua mandando mais solicitações SYN, o que é anormal. Neste ponto, o servidor web ainda é capaz de responder a tráfego normal de visitante, que é destacado e rotulado em verde. Um funcionário visitante com o endereço de IP 198.51.100.14 completa com sucesso uma conexão de aperto de mão SYN/ACK com o servidor web (log item nos. 55, 56, 58). Então, o browser do funcionário solicita a página sales.html com o comando GET e o servidor web responde (log item no. 60 e 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... |

Nas próximas 20 linhas, o log começa a refletir a dificuldade que o servidor web está enfrentando com a quantidade anormal de solicitações SYN chegando. O atacante está enviando diversas solicitações SYN por segundo. As linhas destacadas e rotuladas em amarelo são comunicações falhas entre um funcionário visitante legitimo e o servidor web.

Dois tipos de erro nos logs incluem:

* Uma mensagem de erro HTTP/1.1 504 Gateway Time-out (text/html). Essa mensagem é gerada por um servidor gateway que está esperando pela resposta de um servidor web. Se o servidor web demora muito para responder, o servidor gateway vai mandar a mensagem de erro de timeout para o navegador solicitante.
* Um pacote [RST, ACK], deve ser enviado para um visitante solicitante se o pacote [SYN, ACK] não for recebido pelo servidor web. RST significa reset, acknowledge. O visitante vai receber uma mensagem de erro de timeout em seu browser e a tentativa de conexão é desfeita. O visitante pode atualizar seu browser para tentar enviar uma nova solicitação 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... |

Conforme você desce através do restante do log, notará que o servidor web para de responder ao tráfego de funcionários visitantes legítimos. Os visitantes recebem mais mensagens de erro indicando que eles não podem estabelecer ou manter uma conexão com o servidor web. Do número de item de log 125 em diante, o servidor web para de responder. Os únicos itens logados neste ponto são do ataque. Sendo que existe apenas um endereço de IP atacando o servidor web, você pode assumir que este é um ataque DoS direto de SYN flood.