Redes de computares

Prof. Dr. Bruno da Silva Rodrigues

Bruno.rodrigues@mackenzie.br

Analisando uma transferência TCP do seu computador para um servidor remoto usando Wireshark

Introdução

Neste laboratório, investigaremos detalhadamente o comportamento do protocolo TCP. Faremos isso analisando um traço dos segmentos TCP enviados e recebidos ao transferir um arquivo de 150KB (contendo o texto de Lewis Carrol's Alice's Adventures in Wonderland) do seu computador para um servidor remoto. Estudaremos o uso da TCP de números de seqüência e reconhecimento para fornecer transferência confiável de dados; veremos o algoritmo de controle de congestionamento da TCP - início lento e evasão de congestionamento - em ação; e analisaremos o mecanismo de controle de fluxo anunciado pelo receptor da TCP. Também consideramos brevemente a configuração da conexão TCP e investigaremos o desempenho (throughput e round trip trip) da conexão TCP entre o seu computador e o servidor.

*Experiência de uso do software Wireshark – esta experiência foi proposta por Kurose**

Procedimento

1. *Abra o navegador e acesse:* http://gaia.cs.umass.edu/ethereal-labs/alice.txt
2. *Salve o texto do livro Alice no país das maravilhas num arquivo Alice.txt (ou copie e cole o texto num bloco de notas).*
3. *Abra o wireshark e inicie a captura de pacotes*
4. *Acesse o site:* http://gaia.cs.umass.edu/ethereal-labs/TCP-ethereal-file1.html
5. *Após acessar o site, selecione o arquivo alice.txt" para carregar o arquivo para o servidor gaia.cs.umass.edu*

Objetivos da atividade:

- Estudar o protocolo TCP usando wireshark analisando segmentação, *transferência confiável de dados e controle de congestionamento*

Bibliografias

KUROSE, J. F. e ROSS, K. W. Redes de Computadores e a Internet – Uma Nova Abordagem – Pearson

Internet Engineering Task Force. Disponível em: https://www.ietf.org/rfc/rfc1035.txt

6. *Uma vez que o arquivo foi carregado, uma breve mensagem de parabéns será exibida na janela do navegador. Pare a captura de pacotes do Wireshark.*

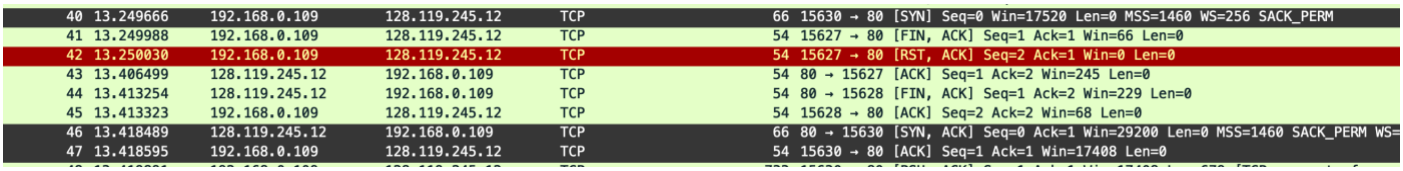
1. ***Responda as questões em negrito com fonte vermelha**.*

Sempre que possível, ao responder uma pergunta, você deve entregar uma impressão do (s) pacote (s) dentro do rastreamento que você usou para responder a pergunta

Após abrir o arquivo analise os pacotes e responda:

***Questão 1(1,5)**. Localize a sequência de pacotes trocados entre o cliente e o servidor gaia e responda:*

a) *localize o Three-way handshake (apresente um print).*



40	13.249666	192.168.0.109	128.119.245.12	TCP	66 15630 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM
41	13.249988	192.168.0.109	128.119.245.12	TCP	54 15627 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66 Len=0
42	13.250030	192.168.0.109	128.119.245.12	TCP	54 15627 → 80 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
43	13.406499	128.119.245.12	192.168.0.109	TCP	54 80 → 15627 [ACK] Seq=1 Ack=2 Win=245 Len=0
44	13.413254	128.119.245.12	192.168.0.109	TCP	54 80 → 15628 [FIN, ACK] Seq=1 Ack=2 Win=229 Len=0
45	13.413323	192.168.0.109	128.119.245.12	TCP	54 15628 → 80 [ACK] Seq=2 Ack=2 Win=68 Len=0
46	13.418489	128.119.245.12	192.168.0.109	TCP	66 80 → 15630 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=
47	13.418595	192.168.0.109	128.119.245.12	TCP	54 15630 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0

O three way handshake são os pacotes 40, 46 e 47

b) *Qual a função do Three-way Handshake? Descreva a função dos pacotes trocados no Three-way Handshake.*

O three way handshake é o processo de estabelecimento de conexão TCP entre dois dispositivos.

A primeira etapa é quando o dispositivo cliente envia um pacote SYN (synchronize) para o dispositivo servidor, pedindo para iniciar uma conexão TCP.

A segunda etapa é quando o dispositivo servidor responde com um pacote SYN-ACK (synchronize-acknowledge), indicando que está pronto para iniciar a conexão e confirmando o número de sequência recebido.

Por fim, a terceira etapa é quando o dispositivo cliente envia um pacote ACK (acknowledge), confirmando que recebeu a resposta do servidor e está pronto para estabelecer a conexão TCP.

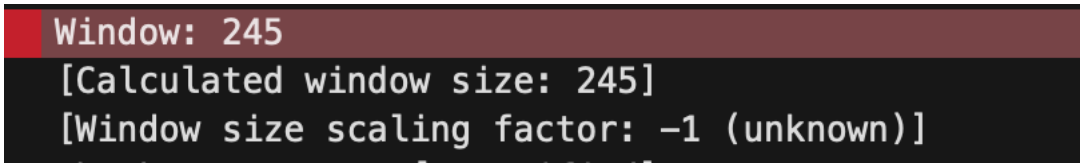
***Questão 2(1,5)**. Qual informação no cabeçalho do segmento identifica se o segmento é SYN ou SYNACK? Apresente um print das informações que serviram como base para sua resposta.*

Questão 3(2,0). *Essa foi uma transmissão segura? Como você chegou a essa conclusão? Observe que segura não é a mesma coisa que confiável. Apresente a tela que justifique sua resposta.*

Como pode ser observado no print da questão anterior, a transmissão não é considerada segura pois não é criptografada, uma vez que ocorre na porta 80 e não 443 (ssl - seguro).

Questão 4(2,0). *Qual o tamanho da janela de recepção do servidor gaia?*

a) *Apresente a tela com um círculo de onde você tirou essa informação.*



b) *Qual a função da janela de recepção?*

A janela de transmissão é uma área da memória do computador que armazena os pacotes de dados que ainda não foram reconhecidos pelo receptor. Ela funciona como um buffer para o tráfego de rede, permitindo que o transmissor continue a enviar dados mesmo se o receptor não puder receber todos os pacotes imediatamente. A janela de transmissão é ajustada dinamicamente com base na taxa de transmissão e no feedback do receptor.

Questão 5(1,5). *O que é maximum segment size (MSS)? Qual o MSS nessa comunicação?*

a) *Apresente um print da tela de onde você tirou essa informação (não esqueça de indicar na imagem onde está a informação).*

O MSS pode ser visto no final da linha (MSS = 1460)

b) *Qual a função do MSS?*

A função do Maximum Segment Size (MSS) é permitir que o transmissor e o receptor de dados em uma conexão TCP acordem sobre o tamanho máximo de dados que podem ser transmitidos em um único segmento TCP.

Questão 6(1,5). *Ao analisar o cabeçalho TCP temos a informação de iRTT (inicial RTT) e RTT. Apresente o segmento onde o iRTT foi determinado. Compare com as respostas ACK e verifique se o RTT aumentou ou diminuiu. Apresente os valores e as telas onde as informações foram retiradas*

Nota: *O Wireshark possui um recurso agradável que permite traçar o RTT para cada um dos segmentos TCP enviados. Selecione um segmento TCP na janela "listagem de pacotes capturados" que está sendo enviada do cliente para o servidor gaia.cs.umass.edu. Em seguida, selecione:* ***Estatísticas-> Gráfico de fluxo TCP> Gráfico de tempo de viagem***.