**Universidade Federal do Ceará**

**Disciplina: Redes de Computadores** **Profa Atslands Rocha**

**Capturando o 3 Way Handshaking do TCP (Fonte: Kurose 6/7, colaboração parte 1: Profª Nídia Campos)**

**Objetivo:**

- Analisar as mensagens de estabelecimento de conexão do protocolo TCP.

**TAREFA 1 - Detectar o endereço IP do seu host**

**PASSO 1.** Use o comando **ipconfig** para descobrir seu endereço IP da conexão local ou conexão sem fio.

**<<<<<<<<<<<<cole aqui a saída deste comando>>>>>>>>>>>>>>>>>>>>>>**

**TAREFA 2 - Detectar o endereço IP do servidor de destino**

**PASSO 1.** Escolha um site web para você abrir no navegador.

**PASSO 2.** Execute o comando **nslookup** para descobrir o endereço IP do servidor web. O servidor deve ter apenas um endereço IP.

**<<<<<<<<<<<<cole aqui a saída deste comando>>>>>>>>>>>>>>>>>>>>>>**

**TAREFA 3 - Usar o navegador web para se estabelecer conexão TCP**

**PASSO 1** - Desabilite todas as interfaces de rede do seu host, exceto a interface de rede que possui o endereço IP registrado na Tarefa 1.

**PASSO 2** - Configure o Wireshark para capturar mensagens.

**PASSO 3** - No navegador web, abra o site escolhido.

**PASSO 4** - Pare o Wireshark e salve o trace da captura em um arquivo .pcap.

**TAREFA 4 - Analisar as três mensagens de estabelecimento de conexão do TCP**

**PASSO 1** - Na captura do Wireshark, filtre todas as mensagens que possui o IP do servidor web. Use o filtro ip.addr== ENDEREÇO_IP_DO_SERVIDOR_WEB

**PASSO 2** - Localize a mensagem HTTP Request solicitando o site que você escolheu. As mensagens de apresentação do TCP (*Three-Way Handshake*) se encontram antes desse HTTP Request.

**PASSO 3 -** Capture a tela desses 3 pacotes expandidos no Wireshark, mostrando todos campos de endereço IP Origem e Destino. Enfatize nessas capturas de tela as seguintes informações do TCP para cada um dos três segmentos: **Source Port, Destination Port, Sequence Number e Acknowledgment Number**.

**<<<<<<<<<<<<cole aqui as três capturas de telas>>>>>>>>>>>>>>>>>>>>>>**

**PASSO 4 -** Preencha os campos abaixo usando as informações dos pacotes capturados.

| Primeiro Segmento TCP | Segundo Segmento TCP | Terceiro Segmento TCP |
|---|---|---|
| Source port:_____ | Source port:_____ | Source port:_____ |
| Destination port:_____ | Destination port:_____ | Destination port:_____ |
| Sequence Number: _____ | Sequence Number: _____ | Sequence Number: _____ |
| ACK Number: _____ | ACK Number: _____ | ACK Number: _____ |
| Marque com um X as flags que foram habilitadas: | Marque com um X as flags que foram habilitadas: | Marque com um X as flags que foram habilitadas: |
| ____ ACK | ____ ACK | ____ ACK |
| ____ Push | ____ Push | ____ Push |
| ____ Syn | ____ Syn | ____ Syn |
| ____ Fin | ____ Fin | ____ Fin |

**QUESTÃO EXTRA**

Neste laboratório, vamos investigar o comportamento do protocolo TCP analisando um rastro dos segmentos TCP enviados e recebidos na transferência de um arquivo de 150KB (contendo o texto de Lewis Carrol's – Aventuras de Alice no País das Maravilhas) do seu computador para um servidor remoto.

**1. Capturando uma transferência TCP em massa do seu computador para um servidor remoto**

Antes de começar nossa exploração do TCP, precisamos usar o Wireshark para obter um rastreamento de pacotes da transferência TCP de um arquivo do computador para um servidor remoto. Você fará isso acessando uma página da Web que permitirá que você digite o nome de um arquivo armazenado em seu computador (que contém o texto ASCII de Alice no País das Maravilhas) e, em seguida, transfira o arquivo para um servidor Web usando o HTTP POST. Estamos usando o método POST em vez do método GET, pois gostaríamos de transferir uma grande quantidade de dados do computador para outro computador.

Faça o seguinte:

• Inicie o seu navegador web. Vá para http://gaia.cs.umass.edu/wireshark-labs/alice.txt e recupere uma cópia ASCII de Alice no País das Maravilhas. Armazene este arquivo em algum lugar no seu computador.

• Em seguida, vá para http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html .

• Na página, utilize o botão Procurar deste formulário para introduzir o nome do arquivo (nome completo do caminho) no computador que contém Alice no País das Maravilhas (ou fazê-lo manualmente). Não pressione o botão "Carregar arquivo alice.txt".

• Agora inicie o Wireshark e comece a captura de pacotes (Capture-> Start) e pressione OK na tela Wireshark Packet Capture Options (não precisaremos selecionar nenhuma opção aqui).

• Voltando ao seu navegador, pressione o botão "Carregar arquivo alice.txt" para carregar o arquivo para o servidor gaia.cs.umass.edu. 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.

**2. Um primeiro olhar para o trace capturado**

- Antes de analisar o comportamento da conexão TCP em detalhes, filtre os pacotes exibidos na janela do Wireshark digitando "tcp" na janela de especificação do filtro de exibição na parte superior da janela do Wireshark.

**Pergunta:** Você deve ver é uma série de mensagens TCP e HTTP entre seu computador e gaia.cs.umass.edu. Você deve ver o handshake inicial de três vias contendo uma mensagem SYN. Você deve ver uma mensagem HTTP POST. Além disso, o que há de diferente da primeira experiência acima?

Responda às seguintes perguntas:

1. Qual é o endereço IP e o número de porta TCP usado pelo computador cliente (origem) que está transferindo o arquivo para gaia.cs.umass.edu?
2. Qual é o endereço IP de gaia.cs.umass.edu? Em que número de porta está enviando e recebendo segmentos TCP para essa conexão?
3. Qual é o endereço IP e o número da porta TCP usado pelo computador cliente (origem) para transferir o arquivo para gaia.cs.umass.edu?

Nota: Uma vez que este laboratório é sobre TCP em vez de HTTP, vamos mudar a janela "listagem de pacotes capturados" do Wireshark para que mostre informações sobre os segmentos TCP contendo as mensagens HTTP, em vez de sobre as mensagens HTTP. Para que o Wireshark faça isso, selecione Analisar-> Protocolos habilitados. Em seguida, desmarque a caixa HTTP e selecione OK.

4. Qual é o número de sequência do segmento TCP SYN que é usado para iniciar a conexão TCP entre o computador cliente e gaia.cs.umass.edu? O que é no segmento que identifica o segmento como um segmento SYN?
5. Qual é o número de sequência do segmento SYNACK enviado por gaia.cs.umass.edu para o computador cliente em resposta ao SYN? Qual é o valor do campo Reconhecimento no

segmento SYNACK? Como gaia.cs.umass.edu determinou esse valor? O que é no segmento que identifica o segmento como um segmento SYNACK?

6. Qual é o número de sequência do segmento TCP que contém o comando HTTP POST? Observe que, para encontrar o comando POST, você precisará digitar no campo de conteúdo de pacote na parte inferior da janela Wireshark, procurando um segmento com um "POST" dentro de seu campo DATA.
7. Considere o segmento TCP contendo o HTTP POST como o primeiro segmento na conexão TCP. Quais são os números de sequência dos primeiros seis segmentos na conexão TCP (incluindo o segmento que contém o HTTP POST)? Em que horário foi enviado cada segmento? Quando foi recebido o ACK para cada segmento?
8. Qual é o comprimento de cada um dos seis primeiros segmentos TCP?
9. Existem segmentos retransmitidos no ficheiro de rastreio? O que você verificou (no rastro) para responder a esta pergunta?

Nota: Veja sobre o RTT: Wireshark tem um recurso interessante que permite traçar o RTT para cada um dos segmentos TCP enviados. Selecione um segmento TCP na janela "lista de pacotes capturados" que está sendo enviada do cliente para o servidor gaia.cs.umass.edu. Em seguida, selecione: Statistics-> TCP Stream Graph-> Round Trip Time Graph.