CES-35 – Redes de Computadores e Internet

Laboratório número 1
Conhecendo protocolos - Wireshark

1. Baixe e instale o software Wireshark: http://www.wireshark.org/download.html

2. Inicie o seu navegador (browser). Inicie o Wireshark e selecione a interface onde vai capturar pacotes que deve ter acesso a Internet. Inicie a capture (Start).

3. Acesse a URL do site do Kurose: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html no navegador. Pare a captura (Stop)

   Você pode salvar esta captura para ir respondendo as perguntas abaixo em diferentes momentos. Para salvar File→ Save as → salve no formato próprio do wireshark que usa a biblioteca pcapng. Não se esqueça de outras vezes que tiver que trabalhar com esta mesma captura de abri-lo
4. Responda as perguntas gerais:

   4.A) Quais destes protocolos aparecem na lista de pacotes: TCP, QUIC, HTTP, DNS, UDP, TLS?

   4.B) Quanto tempo transcorreu desde quando a mensagem HTTP GET foi enviada até quando a resposta HTTP OK foi recebida? Observação: Por padrão, o valor da coluna "Time" (na janela de listagem de pacotes capturados) é a quantidade de tempo que passou (em segundos) desde que a captura de pacotes começou. Para exibir a hora do dia na coluna "Time", selecione a opção "Time Display Format" do menu "View" e, em seguida, selecione a opção "Time-of-day" no menu emergente.
   Tempo decorrido: _____

   4.C) Aponte para a mensagem que tem o GET e expanda a porção HTTP da mensagem. Olhando os detalhes do pacote, qual o tipo do web browser que emitiu o HTTP request? Vide o campo User-Agent e diga qual o navegador compatível (Mozilla, Safari e outros) e plataforma nativa (linux, windows…). Isto é informado ao servidor para que ele possa fornecer a página mais adequada à requisição.

   4.D) Aponte para a mensagem que tem o OK, ou seja, a resposta do HTTP GET.
   Escreva aqui o tamanho em bytes do cabeçalho de cada camada:
   Num. de Bytes do cabeçalho de Aplicação (HTTP): _____
   Num. de Bytes do cabeçalho de Transporte (TCP): _____
   Num. de Bytes do cabeçalho de Rede (Internet Protocol): _____
   Num. de Bytes do cabeçalho de Enlace (Ethernet): _____
   Assim, o total do número de bytes dedicados aos cabeçalhos foi _____.
   Dados "úteis"carregados pela resposta (a página de resposta): _____
   Portanto, do total de bytes transferidos nesta mensagem, quanto se refere aos dados úteis em porcentagem? _____

   4.E) Inclua no relatório o print das mensagens HTTP (GET e OK) referentes ao acesso feito em (3). Para isso, no wireshark selecione as mensagens, seleciona File→ Print, selecione "Selected Packet Only" e "Print as displayed" → Ok.

5. Para estudar superficialmente a Camada de Transporte, selecione a mensagem com o GET novamente e responda:

   5.A) Expandindo a porção TCP, qual o número da porta de destino para o qual a requisição HTTP foi enviada? Porta de destino: _____
   E qual o número da porta de origem? Porta de origem: _____

   5.B) Os protocolos criam sua maneira de conversar, por exemplo, através de bits ligados nas mensagens trocadas, os chamados flags. Há pacotes de controle do TCP que não carregam dados de aplicação. Estão nesta categoria 3 pacotes TCP anteriores ao pacote do HTTP GET. Estes pacotes formam o chamado 3-way handshake e são usados para estabelecer a conexão com o outro lado antes de fazer a requisição propriamente dita. Este handshake envolve os flags SYN e ACK no cabeçalho. Encontre 3 pacotes anteriores ao GET que usam as mesmas portas do item (5A). Em ordem do menor tempo para o maior. Preencha:
   Flag(s) de controle ligado(s) no primeiro pacote do handshake:_____
   Flag(s) de controle ligado(s) no segundo pacote:_____
   Flag(s) de controle ligado(s) no terceiro pacote: _____

Você vai entender melhor este mecanismo quando estudarmos o nível de transporte, por enquanto basta saber que há diversos pacotes trocados para controlar a conversa.

   5.C) No pacote HTTP OK quais são as portas envolvidas?
   Porta de origem: _____
   Porta de destino: _____

   5.D) Depois da transferência da página normalmente acontece a desconexão que envolve os flags FIN e ACK. Há pacotes ligados as mesmas portas do item (5A) com o bit FIN? Mencione o instante de tempo, os pacotes e os flags ligados nos pacotes encontrados depois da transferência.

6. O comando ifconfig (Linux) traz os endereços das suas interfaces de rede. Coloque aqui a saída do ifconfig. No Windows o comando equivalente é ipconfig.

7. Para estudar superficialmente a Camada de Rede, selecione a mensagem com o GET novamente e responda:
   7.A) Endereço IP de gaia.cs.umass.edu : _____
   Endereço IP de seu computador: _____
   O campo inet na saída do ifconfig é o mesmo do endereço IP que o wireshark mostrou? Espero que sim, pois o Sistema Operacional usa esta configuração ligada a sua placa de rede na hora de montar os pacotes que emite para a rede.

8. Para estudar superficialmente a Camada de Enlace, selecione a mensagem com o GET novamente. Na camada de enlace os endereços não se referem ao endereçamento mundial IP, mas ao endereço de sua placa de rede que será usado localmente. Responda:
   8.A) Endereço MAC de origem: _____
   Endereço MAC de destino _____
   O campo ether na saída do ifconfig é o mesmo do endereço de origem que o wireshark mostrou? Espero que sim, pois o Sistema Operacional usa esta configuração de sua placa de rede na hora de montar os pacotes que emite para a rede.

Note como, com um simples GET quanta coisa você aprendeu da relação entre os protocolos!
E tem muito mais pela frente!