CES-35 – Redes de Computadores e Internet

FERNANDO DE MORAES RODRIGUES, COMP-22

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?

   TCP, HTTP, DNS, 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 (desde o início da captura): 5,981225s – 5,840723s = 0,140502s

   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.

   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36\r\n

   Navegadores Compatíveis: Mozilla, Chrome, Safari
   Plataforma Nativa: Windows

   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): 357 bytes
   Num. de Bytes do cabeçalho de Transporte (TCP): 20 bytes
   Num. de Bytes do cabeçalho de Rede (Internet Protocol): 20 bytes
   Num. de Bytes do cabeçalho de Enlace (Ethernet): 14 bytes
   Assim, o total do número de bytes dedicados aos cabeçalhos foi: 411 bytes
   Dados "úteis" carregados pela resposta (a página de resposta): (492–411) bytes = 81 bytes
   Portanto, do total de bytes transferidos nesta mensagem, quanto se refere aos dados úteis

em porcentagem? 100x(492-411)/492 = 16,46%

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.

```
No.     Time           Source                Destination           Protocol Length Info
    118 5.840723       192.168.0.58          128.119.245.12        HTTP     531    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 118: 531 bytes on wire (4248 bits), 531 bytes captured (4248 bits) on interface \Device\NPF_{1D374579-1415-4D24-929F-F7F038D8EEAB}, id
0
Ethernet II, Src: CompalIn_e0:3a:fb (7c:8a:e1:e0:3a:fb), Dst: HUMAX_ec:67:91 (e8:20:e2:ec:67:91)
Internet Protocol Version 4, Src: 192.168.0.58, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64993, Dst Port: 80, Seq: 1, Ack: 1, Len: 477
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    120 5.981225       128.119.245.12        192.168.0.58          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 120: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{1D374579-1415-4D24-929F-F7F038D8EEAB}, id
0
Ethernet II, Src: HUMAX_ec:67:91 (e8:20:e2:ec:67:91), Dst: CompalIn_e0:3a:fb (7c:8a:e1:e0:3a:fb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.58
Transmission Control Protocol, Src Port: 80, Dst Port: 64993, Seq: 1, Ack: 478, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

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: 80
E qual o número da porta de origem? Porta de origem: 64993

5.B) Os protocolos criam sua maneira de conversar, por exemplo, por meio 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: Syn (0x002)
Flag(s) de controle ligado(s) no segundo pacote: Acknowledgment, Syn (0x012)
Flag(s) de controle ligado(s) no terceiro pacote: Acknowledgment (0x010)
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: 80
Porta de destino: 64993

5.D) Depois da transferência da página normalmente acontece a desconexão que envolve os flags FIN e ACK. Há pacotes ligados às 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.

Instante de tempo: 11,182019s desde o início da captura

Pacotes: TCP

Flags Ligados: Acknowledgment, Fin (0x011)

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.

```
C:\Users\ferna>ipconfig

Configuração de IP do Windows


Adaptador Ethernet Ethernet:

   Sufixo DNS específico de conexão. . . . . :
   Endereço IPv6 . . . . . : 2804:14d:688c:8e9::1001
   Endereço IPv6 . . . . . : 2804:14d:688c:8e9:5844:87f0:bd1c:335b
   Endereço IPv6 Temporário. . . . . : 2804:14d:688c:8e9:8df7:cfa8:ff7:f33f
   Endereço IPv6 de link local . . . . . : fe80::5844:87f0:bd1c:335b%5
   Endereço IPv4. . . . . : 192.168.0.58
   Máscara de Sub-rede . . . . . : 255.255.255.0
   Gateway Padrão. . . . . : fe80::ea20:e2ff:feec:6791%5
                             192.168.0.1

Adaptador de Rede sem Fio Conexão Local* 1:

   Estado da mídia. . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Conexão Local* 10:

   Estado da mídia. . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . :

Adaptador Ethernet Ethernet 2:

   Estado da mídia. . . . . : mídia desconectada
   Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Wi-Fi:

   Sufixo DNS específico de conexão. . . . . :
   Endereço IPv6 . . . . . : 2804:14d:688c:8e9::1000
   Endereço IPv6 de link local . . . . . : fe80::5542:9966:22ba:cad7%19
   Endereço IPv4. . . . . : 192.168.0.69
   Máscara de Sub-rede . . . . . : 255.255.255.0
   Gateway Padrão. . . . . : 192.168.0.1
```

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: 128.119.245.12
   Endereço IP de seu computador: 192.168.0.58
   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 à sua placa de rede na hora de montar os pacotes que emite para a rede.

   Sim, são iguais (192.168.0.58).

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: 7c:8a:e1:e0:3a:fb
   Endereço MAC de destino: e8:20:e2:ec:67:91
   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.

   Sim, são iguais (7C-8A-E1-E0-3A-FB).

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