CES-35 - Redes de Computadores
Laboratório 1 - Sniffers e Sockets
Nicholas Scharan Cysne (PMG)

Questionário Sniffers

1. Liste 3 protocolos diferentes que aparecem na coluna protocolo da janela de listagem de pacotes capturados do Wireshark.

R: TCP, DNS, HTTP.

2. 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 columa “Time”, selecione a opção “Time Display Format” do menu “View” e, em seguida, selecione a opção “Time-of-day” no menu emergente.

R: 0,439 segundos.

3. Perguntas sobre HTTP:

    a. Que versão de HTTP está executando o seu navegador e o servidor?

R: HTTP/1.1

    b. Qual é o endereço IP do seu computador e do servidor gaia.cs.umass.edu?

R: Endereço de IP Local: 192.168.0.69, Endereço de IP do Servidor: 128.119.245.12.

    c. Qual é o código de status retornado do servidor para o seu navegador?

R: 200 OK.

    d. Quantos bytes de conteúdo estão sendo devolvidos para o seu navegador?

R: Tamanho de conteúdo de 128 bytes.

4. Perguntas sobre HTTP com GET condicional:

    a. Inspecione o conteúdo da primeira solicitação HTTP GET do seu navegador para o servidor. Você vê uma linha contendo "IF-MODIFIED-SINCE" na mensagem HTTP GET?

R: Não.

b. Inspecione o conteúdo da resposta do servidor da primeira solicitação do seu navegador (referente ao item a). O servidor retorna explicitamente o conteúdo do arquivo? Justifique sua resposta.

R: Sim, ele retorna um conteúdo text/html de 10 linhas que representa a página HTML mostrada no navegador.

c. Inspecione o conteúdo da segunda solicitação HTTP GET do seu navegador para o servidor. Você vê uma linha “IF-MODIFIED-SINCE:” na mensagem HTTP GET? Se a sua resposta é sim, quais são as informações que seguem o “IF-MODIFIED-SINCE”?

R: Sim, If-Modified-Since: Sun, 25 Sep 2022 05:59:01 GMT\r\n.

d. Qual é o código de status de HTTP e frase retornada do servidor em resposta à segunda solicitação HTTP GET (referente ao item iii)? O servidor retorna explicitamente o conteúdo do arquivo? Explicar.

R: 304 Not Modified. Não, ele utiliza o arquivo já em cache para retornar a resposta, falando que não houve alteração no arquivo que já está armazenado em cache.

5. Perguntas sobre recuperação de documentos longos em HTTP:

a. Quantas mensagens de solicitações HTTP GET seu navegador enviou? Qual é o número do pacote que contém a mensagem GET?

R: Apenas uma requisição GET. Pacote número 96.

b. Qual é o número do pacote que contém o código de status e a frase associada com a resposta ao pedido HTTP GET?

R: Pacote número 111.

c. Qual é o código de status e a frase na resposta?

R: Status 200 OK.

d. Quantos segmentos TCP (contendo os dados) foram necessários para transportar a resposta HTTP e o texto da Declaração dos Direitos dos Estados Unidos?

R: Foram necessários 2 segmentso TCP, tamanhos 4343 bytes e 517 bytes respectivamente.

6. Perguntas sobre documentos HTML com objetos incorporados:

    a. Quantas mensagens de solicitação HTTP GET seu navegador enviou? A quais endereços da Internet foram enviadas estas requisições?

R: Foram enviados 3 requisições GET. Para:

- http://gaia.cs.umass.edu//wireshark-labs/HTTP-wireshark-file4.html
- http://gaia.cs.umass.edu/pearson.png
- http://gaia.cs.umass.edu/8E_cover_small.jpg

    b. Você pode dizer se o navegador baixou estas duas imagens serialmente ou se elas foram baixadas de dois sites web em paralelo? Explicar

R: As imagens foram baixadas serialmente. Analizando os pacotes TCP enviados, é possível ver que a requisição da segunda imagem só começou após todos os pacotes da primeira terem chego.

7. Perguntas sobre DNS e Wireshark:

    a. Qual é a porta de destino para a mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta DNS?

R: A porta de destino para a mensagem de consulta DNS é a porta 53, a mesma porta de origem da mensagem de resposta.

    b. Para qual endereço IP a mensagem de consulta DNS é enviada? Use ipconfig para determinar o endereço IP do seu servidor DNS local. O endereço do IP do servidor que respondeu à consulta DNS e o mesmo do seu servidor DNS local?

R: A mensagem é enviada para o endereço 181.213.132.4. Não, o endereço que DNS local está associado à 127.0.0.53.

    c. Examine a mensagem de consulta DNS. Qual é o tipo (Type) da consulta DNS?

R: Tipo A.

    d. Examine a mensagem de resposta DNS. Quantas respostas “answers” são fornecidas? O que cada uma dessas respostas contém?

R: São fornecidas 3 respostas. A primeira apresenta a equivalência do endereço canônico www.ietf.org com o nome www.ietf.org.cdn.cloudflare.net, as outras duas apresentam dois endereços de IP possíveis para www.ietf.org.cdn.cloudflare.net.

    e. Localize o pacote TCP SYN (enviado pelo seu computador e posterior à mensagem de resposta DNS). O endereço IP de destino, do pacote SYN,

corresponde a qualquer um dos endereços IP fornecidos na mensagem de resposta DNS?

R: Sim.

f. A página web http://www.ietf.org contém imagens. Antes de recuperar cada imagem, o seu computador emite novas consultas DNS?

R: Não, pois ele já possui o endereço de IP do local que estão armazenados os arquivos HTML, Js, PNG, etc.

8. Perguntas sobre nslookup e Wireshark:

a. Para qual endereço IP a mensagem de consulta DNS foi enviada? É este o endereço IP do seu servidor DNS local? Se não, a quem corresponde este endereço IP?

R: A mensagem foi enviada para 184.26.161.64. O endereço pertence ao servidor DNS usw2.akam.net, responsável por me retornar o endereço IP de mit.edu.

b. Examine a mensagem de consulta DNS. Qual é o tipo (Type) desta consulta DNS? A mensagem de consulta contém alguma resposta (answers)?

R: Tipo A. A resposta apresenta a equivalência do nome canônico www.mit.edu com o nome real www.mit.edu.edgekey.net.

c. Fornecer um screenshot (captura de tela) que justifique as suas respostas.