1. A INTERAÇÃO BÁSICA GET HTTP/RESPOSTA HTTP

Vamos começar nossa exploração do HTTP acessando uma página HTML muito simples -

que é muita pequena e não contém objetos embutidos. Faça o seguinte:

1. Inicie o navegador web.

2. Inicie o Wireshark, conforme descrito no laboratório introdutório (mas NÃO inicie a captura ainda). Digite "http" (apenas o texto, sem aspas) no campo "filter", então apenas as mensagens HTTP serão exibidas na área de listagem de pacotes quando capturadas.

3. Espere um pouco mais que um minuto e então inicie a captura.

4. Digite o seguinte endereço no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

O seu navegador deverá exibir um arquivo HTML bem simples de apenas uma linha.

5. Pare a captura do Wireshark.

As mensagens HTTP que capturadas são a mensagem GET (do seu navegador para o servidor web gaia.cs.umass.edu) e a mensagem de resposta do servidor para o seu navegador. A área de exibição do conteúdo dos pacotes exibe os detalhes da mensagem selecionada (nesse caso a mensagem GET HTTP, que está destacada na área de listagem de pacotes capturados). Relembre que uma vez que a mensagem HTTP foi transportada dentro de um segmento TCP, que foi transportado dentro de datagrama IP, que foi transportado dentro de um quadro Ethernet, o Wireshark exibe as informações dos pacotes Frame, Ethernet, IP e TCP também.

Olhando as informações nas mensagens GET e resposta HTTP, responda as seguintes perguntas. Quando responder as perguntas, você deverá copiar as mensagens GET e resposta e indicar onde na mensagem você encontrou a informação que responde a questão.

1. O seu navegador está executando a versão 1.0 ou 1.1 do HTTP? E o servidor?
2. Quais idiomas (se houver) seu navegador indica que ele pode aceitar do servidor?
3. Qual o endereço IP do computador? E do servidor gaia.cs.umass.edu?
4. Qual o código de status retornado pelo servidor ao seu navegador?
5. Quando foi a última data de modificação do arquivo HTML que você está obtendo do servidor?
6. Quantos bytes de conteúdo estão sendo enviados para o seu navegador?
7. A INTERAÇÃO GET HTTP/RESPOSTA HTTP CONDICIONAL

A maioria dos navegadores web realizam cache de objetos e então faz um GET condicional quando solicita um objeto HTTP. Antes de seguir os passos abaixo, certifique-se que o cache do seu navegador está vazio.

1. Inicie o seu navegador web, e tenha certeza que o cache está limpo, conforme discutido acima.

2. Inicie o Wireshark.

3. Digite a seguinte URL no seu navegador:

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

O seu navegador exibirá um arquivo HTML muito simples de cinco linhas.

4. Rapidamente digite a mesma URL no seu navegador novamente (ou simplesmente clique no botão Atualizar no seu navegador).

5. Pare a captura do Wireshark, e digite "http" no campo "filter", assim apenas mensagens HTTP capturadas serão listadas.

Responda às seguintes perguntas:

g. Analise o conteúdo da primeira requisição GET HTTP do seu navegador para o servidor.

Você ver alguma linha "IF-MODIFIED-SINCE" nela?

h. Analise o conteúdo da resposta do servidor. O servidor, explicitamente, retornou o conteúdo do arquivo? Como você pode afirmar isso?

i. Agora analise o conteúdo da segunda requisição GET HTTP do seu navegador para o

servidor. Você ver alguma linha "IF-MODIFIED-SINCE" nela? Se sim, que informações ela possui?

j. Qual o código de status HTTP e frase retornaram do servidor em resposta ao segundo GET

HTTP? O servidor, explicitamente, retornou o conteúdo do arquivo?

1. OBTENDO DOCUMENTOS GRANDES

1. Inicie o navegador, e tenha certeza que o cache está limpo, conforme discutido acima.

2. Inicie o Wireshark.

3. Digite a seguinte URL no seu navegador:

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

Seu navegador deverá exibir a extensa "Bill of Rights" americana.

4. Pare a captura no Wireshark, e digite "http" no campo "filter", então somente mensagens

HTTP serão exibidas.

Na área de listagem de pacotes, você deverá ver sua mensagem GET HTTP, seguida por uma resposta com pacotes múltiplos para sua requisição A mensagem de resposta HTTP consiste de uma linha de status, seguida por linha de cabeçalho, seguidas por uma linha em branco, seguida por um corpo de entidade. No caso do nosso GET HTTP, o corpo de entidade na resposta HTTP é todo o arquivo HTML solicitado. No nosso caso aqui, o arquivo HTML é bastante longo, e 4500 bytes é muito grande para caber em um pacote TCP. Uma única mensagem de resposta HTTP é, portanto, dividida em vários pedaços pelo TCP, com cada pedaço a ser contido dentro de um segmento TCP em separado. Cada segmento TCP é registrado como um pacote separado pelo Wireshark, e o fato de que a resposta HTTP única foi fragmentado em vários pacotes TCP é indicado pela frase "continuation" exibida pelo Wireshark. OBS.: Não há nenhuma mensagem de "continuation" no HTTP!

Responda às seguintes perguntas:

k. Quantas mensagens de requisição GET HTTP foram enviadas pelo seu navegador?

l. Quantos segmentos TCP contendo dados foram necessários para carregar uma única resposta HTTP?

m. Qual é o código de status e frase associados com a resposta para a requisição GET HTTP?

1. DOCUMENTOS HTML COM OBJETOS EMBUTIDOS

1. Inicie seu navegador web, e tenha certeza que o cache está limpo, conforme discutido acima.

2. Inicie o Wireshark.

3. Digite a seguinte URL no seu navegador:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

O seu navegador deverá exibir um pequeno arquivo HTML com duas imagens. Estas duas imagens estão referenciadas no arquivo HTML. Isto é, as imagens em si não estão contidas no HTML; ao invés disso as URLs para o download das imagens estão contidas no arquivo HTML.

4. Pare a captura do Wireshark e digite "http" no campo "filter", assim apenas mensagens HTTP capturadas serão exibidas.

Responda às seguintes perguntas:

o. Quantas mensagens de requisição GET HTTP foram enviadas pelo seu navegador? Para qual endereço IP essas requisições GET foram enviadas?

p. Você pode dizer se o seu navegador baixou essas duas imagens em série, ou se elas foram baixadas dos dois sites web em paralelo?