Universidade Federal do Ceará (UFC) - Campus Quixadá
Disciplina: Redes de Computadores Período 2011.1
Profa. Atslands Rego da Rocha (atslands@ufc.br)
Data: 01/03/2011

02 AULA PRÁTICA – Hypertext Transfer Protocol: HTTP (WIRESHARK)

(Baseada nas Práticas do livro de James Kurose – 4Edição)

Nesta segunda aula prática usando o Wireshark, exploraremos os vários aspectos do protocolo HTTP: a interação básica GET/response, formatos de mensagens HTTP, recuperação de arquivos HTML grandes e arquivos HTML com objetos embutidos, além da autenticação e segurança HTTP.

A interação básica HTTP GET/response

Vamos começar realizando o download de um arquivo simples HTML que além de pequeno não contém objetos embutidos. Faça o seguinte:

1. Inicie o seu navegador (browser).
2. Inicie o Wireshark como descrito na prática anterior (mas não inicie a captura de pacotes ainda). Digite **http** na janela de filtro para mostrar somente pacotes HTTP capturados.
3. Inicie a captura de pacotes com o Wireshark.
4. Digite o endereço no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html. Seu navegador deve mostrar um arquivo HTML simples de uma única linha.
5. Finalize a captura de pacotes pelo Wireshark.

Sua interface deve estar similar a interface ilustrada na Figura 1.

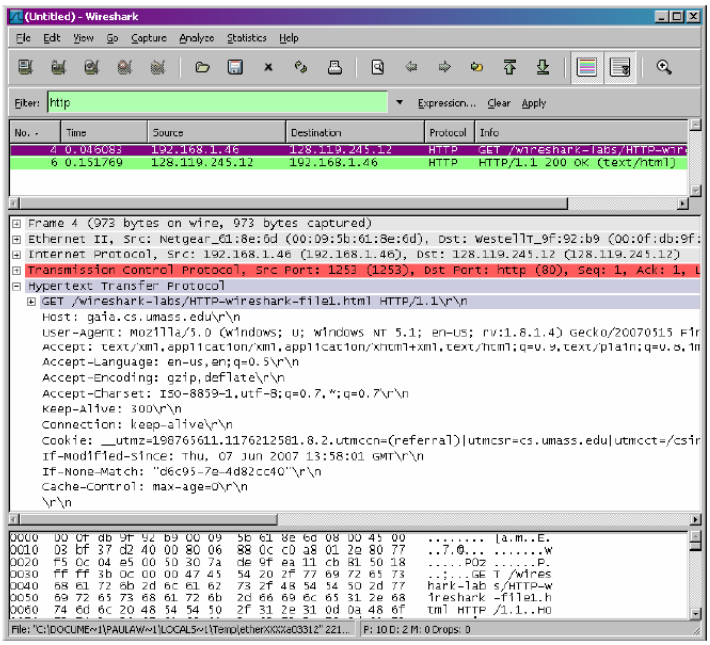

Figura 1. Wireshark após realização dos passos anteriores descritos

O exemplo na Figura 1 mostra duas mensagens HTTP na lista de pacotes: a mensagem GET (enviada do seu navegador para o servidor gaia.cs.umass.edu web) e a mensagem response do servidor para o seu navegador. O conteúdo dos pacotes mostram os detalhes de cada mensagem selecionada. Analisando esses dados das mensagens analisadas, responda às seguintes questões:

1. Seu navegador está executando qual versão do HTTP 1.0 ou 1.1? Qual versão do HTTP está sendo executada no servidor?
2. Qual o endereço IP do seu computador? E do servido gaia.cs.umass.edu?
3. Qual é o código de retorno da mensagem dado pelo servidor para o seu navegador?
4. Quando o arquivo HTML que você recuperou foi modificado pelo servidor?
5. Quantos bytes de conteúdo estão sendo retornados para o seu navegador?

A interação condicional HTTP GET/response

A maioria dos navegadores usam caching de objetos e assim desempenham um GET condicional quando recuperam um objeto HTTP. Antes de executar os passos abaixo, esteja seguro de que o cache do seu navegador está vazio. (Nota: Geralmente as configurações de cache do navegador estão na aba de "Opções" ou "Preferências". Após encontrar a opção, limpe o cache do navegador). Então continue:

• Inicie o navegador.
• Inicie o Wireshark.
• Digite a seguinte URL no navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html. Seu navegador mostrará um arquivo HMTL de cinco linhas.
• Digite rapidamente a mesma URL no seu navegador novamente (ou simplesmente selecione o botão "atualizar" do navegador).
• Finalize a captura de pacotes pelo Wireshark e digite **http** na janela de filtros do Wireshark para mostrar somente mensagens HTTP capturadas.

Responda às seguintes questões:

6. Inspecione os conteúdos da primeira mensagem HTTP GET enviada do seu navegador para o servidor. Você vê uma linha **IF-MODIFIED-SINCE** na mensagem HTTP GET?
7. Inspecione os conteúdos da resposta do servidor. O servidor retornou explicitamente os conteúdos do arquivo?
8. Agora inspecione o conteúdo da segunda mensagem HTTP GET enviada pelo seu navegador para o servidor. Você vê uma linha **IF-MODIFIED-SINCE** na mensagem HTTP GET? Se a resposta for **sim**, que informação esta linha contém?
9. Qual é o código de estado HTTP e a frase retornada pelo servidor em resposta à segunda mensagem HTTP GET? O servidor retornou explicitamente os conteúdos do arquivo? Explique.

Recuperando documentos HTTP longos

Nos exemplos anteriores, os arquivos HTML são simples e pequenos. Para ver o que ocorre quando realizamos o download de um arquivo longo HTML faça o seguinte:

• Inicie o navegador e esteja seguro de que o cache está limpo (como descrito anteriormente).
• Inicie o Wireshark.
• Digite a seguinte URL no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html. Seu navegador deve mostrar um documento que mostre "The US Bill of Rights" como título.

• Finalize a captura de pacotes pelo Wireshark e digite **http** na janela de filtros para que apenas as mensagens HTTP sejam mostradas.

Na lista de pacotes capturados, você deve ver a mensagem HTTP GET seguida de várias mensagens HTTP response. Isso ocorre porque a resposta é maior do que o campo da mensagem HTTP que recebe a página para retornar ao navegador (e mais longo que uma pacote TCP). Então, a mensagem HTTP response é quebrada em vários pedaços pelo TCP, com cada pedaço da mensagem sendo enviado por um segmento TCP separado. Cada segmento TCP é registrado pelo Wireshark como uma mensagem separada e de fato um único HTTP response foi fragmentado através de múltiplos pacotes TCP.

Responda às seguintes questões:

10.Quantas mensagens HTTP GET foram enviadas pelo seu navegador?
11.Quantos segmentos TCP contendo dados foram necessários para carregar uma única mensagem HTTP response?
12. Qual é o código de estado e a frase associada com a resposta para a mensagem HTTP GET?

Documentos HTML com objetos embutidos

Agora, vamos ver o que ocorre quando o navegador realiza o download de um arquivo HTML com objetos embutidos, ou seja, um arquivo que contenha imagens, por exemplo. Faça o seguinte:
• Inicie o navegador e esteja seguro de que o cache está limpo (como descrito anteriormente).
• Inicie o Wireshark.
• Digite a seguinte URL no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html. Seu navegador deve mostrar um documento HTML com duas imagens (que são referenciadas no documento HTML, mas que não estão inseridas nele como o habitual).
Nota: lembre que as imagens tem seu próprio URL que é referenciada no código HTML dentro do documento recuperado.
• Finalize a captura de pacotes pelo Wireshark e digite **http** na janela de filtros para que apenas as mensagens HTTP sejam mostradas.

Responda às seguintes questões:
13. Quantas mensagens HTTP GET foram enviadas pelo seu navegador? Para qual endereço da Internet as mensagens HTTP GET foram enviadas?
14. Você pode dizer se o seu navegador realizou o download das duas imagens de forma serial ou paralela? Explique.

Autenticação HTTP

Finalmente, vamos visitar um site que possua senha para ser acessado. Faça o seguinte:

• Esteja seguro de que o cache está limpo (como descrito anteriormente). Reinicie o navegador.
• Inicie o Wireshark.
• Digite a seguinte URL no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html. Digite o usuário e a senha. O usuário é **wireshark-students** e a senha **network.**

• Finalize a captura de pacotes pelo Wireshark e digite **http** na janela de filtros para que apenas as mensagens HTTP sejam mostradas.

Se desejar se aprofundar mais sobre autenticação HTTP, leia o material "HTTP Access Authentication Framework" em http://frontier.userland.com/stories/storyReader$2159 (em inglês!).

Responda às seguintes questões:
18. Qual é a resposta do servidor (código de estado e frase) na resposta para a mensagem inicial HTTP GET do seu navegador?
19. Que novo campo é incluído na mensagem HTTP GET?

O usuário (wireshark-students) e a senha (network) que você digitou são codificados em uma string de caracteres (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=) seguindo do cabeçalho "Authorization: Basic" na mensagem HTTP GET enviada pelo navegador. O usuário e a senha são apenas codificadas de uma forma simples (formato Base64) e não CRIPTOGRAFADAS! Vá para a URL http://www.motobit.com/util/base64-decoder-encoder.asp e digite a string codificada em base64 **d2lyZXNoYXJrLXN0dWRlbnRz**. Selecione a opção "decode the data from a Base64 string (base64 decoding)" e clique no botão "Convert the source data". Você pode ver o usuário decodificado rapidamente! Para ver a senha digite a outra parte da string **Om5ldHdvcms=** e decodifique. Ou seja, sites com esquemas de senhas simples como essa não são seguras!
Nota: Existem outras formas de enviar senhas pela WWW, ufa!

"Conte-me e eu esquecerei. Mostre-me e eu lembrarei. Envolva-me e eu compreenderei."
Provérbio Chinês