Universidade Federal do Ceará

Disciplina: Redes de Computadores **Fonte: Kurose – versão 6/7**

PARTE 1 - A Interação básica Request/Response HTTP

Material de apoio: Redes de Computadores e a Internet – uma abordagem top-down, 6/7ª edição, autores: James F. Kurose, Keith W. Ross, editora Pearson.

Entrega: Cada aluno ou dupla deve fazer o upload no site da disciplina de um arquivo .zip/.rar contendo o relatório e o arquivo **.pcap** desta prática (parte 1 e 2).

Objetivo:

- Conhecer a sintaxe e semântica de mensagens HTTP
- Conhecer a ordem de troca de mensagens HTTP

PASSOS

1. **PASSO 1** - Inicie o seu navegador web. Em seguida, inicie o Wireshark. Você irá inicialmente ver uma janela ainda sem nenhum dado nas suas janelas, dado que Wireshark ainda não começou a capturar pacotes. Para configurar a captura de pacotes, selecione o menu de captura (*Capture*) e selecione *Options*. Isto causará a apresentação da janela "Wireshark: Capture Options" (Opções de captura do Wireshark). Você poderá usar todos os valores *default* desta janela. As interfaces de rede (isto é, as conexões físicas) que o seu computador possui com a rede serão mostradas no menu de Interface no alto da janela de Opções de Captura. Caso o seu computador possua mais de uma interface de rede ativa (por exemplo, se você tiver tanto uma conexão sem fio como uma conexão cabeada), você deverá selecionar uma interface que esteja sendo usada para enviar e receber pacotes (provavelmente a interface cabeada). Depois de selecionar a interface de rede (ou usando a interface default escolhida pelo Wireshark), clique *Start*. Assim terá início a captura – todos os pacotes que forem transmitidos/recebidos para/pelo seu computador agora estará sendo capturado pelo Wireshark! Assim que você começar a captura de pacotes, aparecerá na janela principal o resumo da captura de pacotes. A captura é parada no menu Capture\Stop. Mas, ainda não pare a captura.

PASSO 2 - Inicie a captura de pacotes usando o Wireshark.

PASSO 3 - Enquanto o Wireshark estiver executando, Digite o endereço abaixo no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html e faça com que a página seja apresentada no seu browser. De modo a lhe apresentar esta página, o seu browser irá contactar o servidor HTTP em gaia.cs.umass.edu e trocar mensagens http com o servidor de modo a baixar esta página, como discutido no livro da disciplina.

PASSO 4 - Seu navegador deve mostrar um arquivo HTML simples de uma linha.

PASSO 5 - Interrompa a captura de pacotes. Salve a captura do Wireshark em um arquivo **.pcap**.

PASSO 6 - Digite http no campo **filter** da janela principal do programa (no alto da janela principal do Wireshark). Depois selecione *Apply* (à direita de onde você digitou http). Isto causará a apresentação apenas de mensagens http na janela de listagem de pacotes.

PASSO 7 - Na captura do Wireshark, localize a mensagem de **GET HTTP** e mensagem de **Response HTTP** e responda as perguntas abaixo:

1) Seu navegador está rodando a versão 1.0 ou 1.1 do HTTP? Qual versão do HTTP está executando no servidor?
2) Quais idiomas (se há algum) o seu navegador indica que deseja receber a página web solicitada do servidor?
3) Qual o seu endereço IP? Qual o endereço IP do servidor gaia.cs.umass.edu?
4) Qual o código de status retornado do servidor para o seu navegador?
5) Quando o arquivo HTML que você solicitou foi modificado pela última vez pelo servidor?
6) Quantos bytes de conteúdo são retornados para o seu navegador?
7) Inspecionando o payload (carga útil) da mensagem de resposta http: você vê algum cabeçalho de algum outro protocolo? Se sim, nomeie algum.

PARTE 2 - A interação CONDICIONAL Request/Response HTTP

PASSO 8 - Inicie seu navegador web e certifique-se que a cache do seu navegador está vazia.

PASSO 9 - Inicie a captura de pacotes usando o Wireshark.

PASSO 10 - Digite o seguinte endereço no seu navegador:

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

PASSO 11 - Rapidamente o botão atualizar do seu navegador.

PASSO 12 - Interrompa a captura de pacotes e salve sua captura em um arquivo **.pcap.** Digite "http" no campo filtro da janela principal do Wireshark para mostrar apenas as mensagens HTTP capturadas.

PASSO 13 - Responda as questões abaixo analisando as mensagens de requisição e resposta trocadas entre seu computador e o servidor gaia.cs.umass.edu:

1. Inspecione os conteúdos da primeira requisição HTTP GET enviada do seu navegador para o servidor. Você vê a linha "IF-MODIFIED-SINCE:" na requisição HTTP?
2. Inspecione o conteúdo da resposta do servidor . O servidor retornou explicitamente o conteúdo do arquivo? Como você pode afirmar isso?
3. Agora inspecione o conteúdo da segunda requisição HTTP GET da página HTTP-wireshark-file2.html enviada do seu cliente para o servidor. Você vê a linha "IF-MODIFIED-SINCE:" na requisição HTTP? Se sim, que informação segue o cabeçalho "IF-MODIFIED-SINCE:"?
4. Qual código e frase de status HTTP são retornados do servidor em resposta à segunda requisição HTTP? O servidor retornou explicitamente o conteúdo desse arquivo? Explique.

Questão Opcional (Entrega não obrigatória)

Se você realizou as questões da prática 01 e 02 facilmente, recomendo realizar a parte 3 opcional para aumentar o seu conhecimento.

Autenticação HTTP

O site a ser visitado nessa parte da prática é uma página web protegida por senha e examinaremos a sequencia de mensagens trocadas pelo HTTP para tal site. O usuário é **wireshark-students** e a senha é **network**.

PASSO 14 - Inicie seu navegador web e certifique-se que a cache do seu navegador está vazia.

PASSO 15 - Inicie a captura de pacotes usando o Wireshark.

PASSO 16 - Digite o seguinte endereço no seu navegador:

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

PASSO 17 - Digite o usuário e a senha requerida.

PASSO 18 - Interrompa a captura de pacotes e salve sua captura em um arquivo **.pcap.** Digite "http" no campo filtro da janela principal do Wireshark para mostrar apenas as mensagens HTTP capturadas.

Talvez você deseje saber mais a respeito da autenticação HTTP no material "HTTP Access Authentication Framework" em http://frontier.userland.com/stories/storyReader$2159

PASSO 19 - Responda as questões abaixo analisando as mensagens de requisição e resposta trocadas entre seu computador e o servidor gaia.cs.umass.edu:

1. Qual é a resposta do servidor (código e frase de estado) para a mensagem HTTP GET inicial do seu navegador?
2. Quando o seu navegador envia a mensagem HTTP GET pela segunda vez, qual novo campo é incluído na mensagem GET?

O nome de usuário (wireshark-students) e a senha (network) que você inseriu são codificados na sequência de caracteres (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms =) seguindo o cabeçalho "Autorização: Básico" na mensagem HTTP GET do cliente. Embora possa parecer que seu nome de usuário e senha são criptografados, eles são simplesmente codificados em um formato conhecido como formato Base64. O nome de usuário e a senha não são criptografados! Para ver isso, vá para http://www.motobit.com/util/base64-decoder-encoder.asp e digite a sequência codificada em base64 d2lyZXNoYXJrLXN0dWRlbnRz e decodifique. Voila! Você traduziu de codificação Base64 para codificação ASCII e, portanto, deve ver seu nome de usuário! Para visualizar a senha, digite o restante da string Om5ldHdvcms= e pressione decodificar. Uma vez que qualquer pessoa pode fazer o download de uma ferramenta como Wireshark e sniff de pacotes (não apenas seus próprios) passando por seu adaptador de rede, e qualquer pessoa pode traduzir de Base64 para ASCII (você acabou de fazê-lo!), Deve ser claro para você que senhas simples nas páginas Web não são seguros a menos que medidas adicionais sejam tomadas.

Não tenha medo! No Capítulo 8 do livro são apresentadas outras maneiras de tornar o acesso WWW mais seguro. No entanto, você já sabe que vamos precisar claramente de algo que vai além da estrutura básica de autenticação HTTP!