Redes de Computadores

1Q2023

Prof. Gustavo Sousa Pavani

Universidade Federal do ABC (UFABC)

Aula Prática 3

Wireshark

- Wireshark é um analisador de protocolos (*sniffer*), distribuído gratuitamente, a partir do endereço http://www.wireshark.org.
  - Ele pode ser executado em diversas plataformas, incluindo sistemas Unix e Windows.
- Capturando pacotes:
  - Abra o Wireshark e ative a captura de pacotes (*Capture* > *Interfaces*).
    - ★ Na opção *Interfaces*, escolha a interface Ethernet (eth0).
    - ★ Em *Options*, selecione a opção "enable network name resolution".
    - ★ Clique em *Start* para iniciar a captura.
    - ★ Pare a captura de pacotes clicando no botão *Stop* da janela de captura.
- A interface do Wireshark é dividida em três partes:
  - A primeira contém uma relação dos pacotes capturados, um por linha.
  - A segunda contém informações sobre o pacote que está selecionado, onde cada linha contém um protocolo, na ordem em que eles são empilhados. Dentro de cada protocolo, são mostrados os campos do seu cabeçalho.
  - A terceira parte contém a carga útil do pacote, que é apresentada no formato hexadecimal e o seu correspondente para ASCII.

Roteiro – Instruções

- Relatório individual ou em dupla discutindo o que foi feito nas aulas práticas 3 e 4, o qual deve incluir as saídas dos programas.
  - Incluir os códigos fontes implementados, caso aplicável, e o relatório em um arquivo zip, que deve seguir o formato `RA_2.zip` ou `RA1_RA2_2.zip`.
  - Prazo de entrega: 19/04, conforme tarefa no Moodle.
  - **Importante:** Entrega somente através do Moodle. Não serão aceitas outras formas de entrega.

Roteiro – *Hypertext Transfer Protocol* (HTTP)

1 Interação básica HTTP.

1.1 Acesse a página http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html e aplique o filtro HTTP para ver apenas os pacotes do protocolo HTTP. Observe os pacotes capturados e identifique:

1.1.1 Versão do HTTP do navegador e do servidor web acessado.

1.1.2 Línguas que o navegador aceita.

1.1.3 IP do seu computador e do servidor.

1.1.4 Código de status retornado do servidor para o navegador.

1.1.5 HTTP persistente ou não persistente.

1.1.6 Última modificação do arquivo HTML do servidor.

1.1.7 Número de bytes de conteúdo retornado ao navegador.

1.2 Analise os dados (*raw data*) do pacote e descreva o que é possível observar.

Roteiro – *Hypertext Transfer Protocol* (HTTP) - cont.

2 GET Condicional.

- 2.1 Limpe o cache do seu navegador e acesse a página http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html.
- 2.2 Verifique o conteúdo da primeira requisição GET. É possível ver `IF-MODIFIED-SINCE'` no HTTP GET?
- 2.3 Verifique a resposta do servidor. O servidor retorna o conteúdo do arquivo?
- 2.4 Faça uma segunda requisição GET e verifique a resposta do servidor. É possível ver `IF-MODIFIED-SINCE` no HTTP GET? Explique.
- 2.5 Verifique a resposta do servidor ao segundo GET. O servidor retorna o conteúdo do arquivo? Explique.

Roteiro – *Hypertext Transfer Protocol* (HTTP) - cont.

3 HTML com objetos.

- 3.1 Acesse a página http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html.
- 3.2 Quantas requisições HTTP GET foram feitas pelo navegador? Para qual endereço IP estas requisições foram feitas?
- 3.3 Identifique se o navegador fez o *download* das imagens (objetos) de maneira serial ou paralela. Explique.

4 Autenticação HTTP.

- 4.1 Acesse a página http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html com nome de usuário: `wireshark-students` e senha: `network`.
- 4.2 Qual a resposta do servidor ao HTTP GET inicial do navegador?
- 4.3 Na segunda mensagem GET do navegador, qual novo campo é incluído na mensagem GET?
- 4.4 É possível visualizar o nome de usuário e senha no pacote capturado pelo wireshark? Discuta sobre a segurança desta autenticação HTTP.

Roteiro – *Domain Name System* (DNS)

5 Resolução de nomes.

- 5.1 Acesse o site do Pudim e filtre as mensagens DNS.
- 5.2 O protocolo DNS usa TCP ou UDP?
- 5.3 Identifique a porta de destino da mensagem `query` DNS e a porta de origem da mensagem de resposta do DNS.
- 5.4 Identifique o endereço IP para qual a mensagem de `query` do DNS foi enviada.
- 5.5 Examine a resposta DNS. Quantas "respostas" foram dadas? Qual o conteúdo destas respostas?
- 5.6 Aplique os filtros necessários e considere o pacote TCP SYN subsequente enviado pelo navegador. O IP de destino do pacote TCP SYN corresponde ao endereço IP fornecido pela mensagem de resposta DNS?
- 5.7 Esta página contém imagens. Antes de requisitar cada imagem, seu *host* faz novas *queries* DNS?

Roteiro – *Domain Name System* (DNS) - cont.

6 Usando nslookup.

- 6.1 Execute o comando `nslookup www.mit.edu`.
- 6.2 Identifique a porta de destino da mensagem de *query* DNS e a porta de origem da mensagem de resposta do DNS.
- 6.3 Identifique o endereço IP para qual a mensagem de *query* DNS foi enviada.
- 6.4 Examine a resposta DNS. Quantas "respostas" foram dadas? Qual o conteúdo destas respostas?
- 6.5 Execute o comando `nslookup www.aiit.or.kr google-public-dns-a.google.com`.
- 6.6 Identifique o endereço IP para qual a mensagem de query do DNS foi enviada. Este endereço IP é o mesmo do seu servidor DNS local? Caso contrário, esse endereço IP corresponde a que servidor?
- 6.7 Examine a resposta DNS. Quantas "respostas" foram dadas? Qual o conteúdo destas respostas?