Universidade Federal do Ceará
Centro de Ciências
Departamento de Computação

Redes de Computadores I (CK0249) 2020.1 - PPE

Prof. Dr. Emanuel Bezerra Rodrigues

ATIVIDADE PRÁTICA I
CAMADA DE APLICAÇÃO

CONTEXTUALIZAÇÃO

Conforme visto na disciplina, os protocolos HTTP e DNS são essenciais para o funcionamento da Internet como conhecemos. Entre outras funções, eles atuam na requisição e fornecimento de páginas Web, fazendo com que aplicações cliente (*browsers*/navegadores) possam obter conteúdos hospedados em servidores, através da troca de pacotes.

Um tipo de software, os sniffers (farejadores), são utilizados para monitorar o tráfego em uma rede. De forma resumida, um sniffer captura os pacotes enviados e recebidos em uma interface de rede de um dispositivo e, dependendo do software, podem armazenar esses pacotes e/ou exibi-los para o usuário. Assim, o conteúdo das capturas pode ser analisado para fins de monitoramento, detecção de problemas, análise do comportamento de protocolos, dentre outros. O Wireshark é um dos mais conhecidos e utilizados sniffers de rede.

OBJETIVO

Analisar os pacotes envolvidos em uma requisição de página WEB, mais especificamente os relacionados aos protocolos HTTP e DNS.

FERRAMENTAS E RECURSOS

- Wireshark
- Browser
- Prompt do Sistema Operacional

AVISOS IMPORTANTES

- Ler a prática completa antes de começar a fazer pode ser útil.
- Certifique-se que seu computador está com conexão com a Internet.
- Evite que seu navegador esteja com outras páginas abertas além daquelas solicitadas no roteiro, pois pode interferir no resultado.

- É interessante manter o material para anotações durante o experimento.

ENTREGA

- Para fins de registro, ao final da prática, deverá ser anexado à tarefa no Google Classroom um documento, preferencialmente em formato PDF, contendo nome do aluno, matrícula e as respostas às perguntas feitas durante o roteiro da prática.

PREPARANDO O AMBIENTE

1. Baixe e instale o Wireshark em sua versão mais recente e compatível com seu SO.
    1. O download pode ser feito na página oficial https://www.wireshark.org/ .
    2. Caso haja dúvidas no processo de instalação, você pode assistir aos vídeos: https://youtu.be/I-T5-VW0CnU (SO Linux) ou https://youtu.be/fpeMCuCKgHA (SO Windows).

2. Limpe a cache do seu navegador.

    Cada navegador possui uma funcionalidade de limpar sua cache. Em geral, essa função encontra-se no menu configurações e está relacionado a "limpar cache e cookies".

3. Anote seu endereço IP e o gateway.

    Para saber o endereço IP do seu computador, você pode acessar as configurações de rede ou utilizar os comandos ipconfig, no Windows, ou ifconfig, no Linux, no prompt de comandos.

4. Limpe a cache DNS do seu computador. *Acesse o prompt e use o comando ipconfig /flushdns (Windows) ou ifconfig /flushdns (Linux).*

CAPTURA 1

1. Inicie seu navegador. Não acesse nenhuma página ainda!
2. Inicie o Wireshark e digite o filtro "ip.addr == seu_ip" (sem as aspas).

    Esse filtro vai fazer com que apenas sejam exibidos pacotes que tenham origem ou sejam destinados ao seu computador.
3. Inicie a captura de pacotes no Wireshark.
4. Vá ao navegador e digite o endereço:

    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

    Espere o site carregar completamente.

5. Vá no wireshark e pare a captura.
    a. Quantos pacotes foram capturados? Anexe um print da captura no relatório.

    Uma dica: Salve a captura.

6. No wireshark, na barra de filtros, digite o “ip.addr == seu_ip and http” (sem as aspas).
    Esse filtro vai exibir apenas os pacotes referentes ao protocolo HTTP.

7. Analise o primeiro pacote HTTP request. Anexe um print desse pacote no relatório. Responda:
    a) Qual tamanho do pacote?
    b) Qual o endereço IP de destino?
    c) Qual o método utilizado?
    d) Qual a versão do HTTP está sendo executada no seu navegador?
    e) Quais formatos de arquivos o seu navegador indica aceitar?
    f) Quais linguagens (se houver) o seu navegador indica ao servidor?
    g) O que contém a linha de requisição do HTTP?

8. Analise o primeiro pacote HTTP response. Anexe um print desse pacote no relatório. Responda:
    a) Qual a versão do HTTP executada no servidor?
    b) Qual o nome do servidor e seu sistema operacional?
    c) Qual linha informa a data e a hora do servidor?
    d) Qual a data em que o conteúdo solicitado foi modificado pela última vez?
    e) Qual o tamanho e tipo de conteúdo enviado na resposta HTTP?
    f) Qual o conteúdo retornado?

9. Na barra de filtros do Wireshark, digite o seguinte: “ip.addr == seu_ip and dns” (sem aspas).

Esse filtro vai fazer com que sejam exibidos apenas os pacotes referentes ao protocolo DNS.

10. Analise o pacote que contém a requisição de resolução de nome “gaia.cs.umass.edu”. Esse pacote está assinalado com query. Anexe um print desse pacote no relatório. Responda:
    a) Qual o tamanho do pacote?
    b) Qual o endereço IP de destino? A quem corresponde esse endereço?
    c) A requisição é do tipo recursiva ou iterativa? Qual linha indica isso?

11. Analise a resposta à requisição DNS. Ele está assinalado com query response. Responda:
    a) Qual o endereço do emissor desse pacote? É o mesmo do destinatário da requisição anterior? Por quê?

b) Qual o endereço do servidor autoritativo responsável pelo domínio “gaia.cs.umass.edu”?

12. **Responda**: *Analisando a captura de pacotes como um todo, quais pacotes vieram primeiro: HTTP ou DNS? Por quê?*

CAPTURA 2

1. Limpe a cache do seu navegador.
2. Inicie uma nova captura do Wireshark utilizando como filtro “ip.addr == seu_ip”.
3. No navegador, digite o endereço:

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

4. Espere a página carregar completamente e pare a captura no Wireshark.
5. No filtro do Wireshark, adeque para que sejam exibidos apenas os pacotes referentes ao protocolo DNS.
   a) Uma nova resolução DNS foi feita para o endereço solicitado? Por quê?
6. Modifique o filtro no Wireshark para exibir apenas os pacotes referentes ao protocolo HTTP. Anexe um print no relatório.
   a) Quantas requisições (GET request) foram feitas e para qual endereço foram enviadas? Explique.

7. Analise o segundo pacote GET request. Responda:
   a) Qual o conteúdo solicitado?
   b) Como o conteúdo é identificado na requisição HTTP?
   c) Quais os formatos indicados como aceitos?
8. Analise o pacote HTTP response que atende à requisição anterior. Responda:
   a) Qual o tamanho do conteúdo?
   b) Qual o formato do conteúdo?
   c) Qual sua data de modificação?

CONCLUSÃO

Apesar de simples, nesse laboratório podemos entender um pouco como acontecem as requisições a páginas Web e como os protocolos HTTP e DNS atuam nesse processo. Outros protocolos também estão envolvidos, mas iremos entender melhor à medida que descemos na pilha de protocolos TCP/IP.