Universidade Federal de Mato Grosso do Sul

Faculdade de Computação

REDES DE COMPUTADORES

LABORATÓRIO

LAB -1

prof. Hana Karina Salles Rubinsztejn -
hana@facom.ufms.br

Conteúdo

- **packet sniffer** – Wireshark http://www.wireshark.org
- Exercício

Packet Sniffer

- Um 'farejador de pacotes'
- Passivo
  - Nunca envia pacotes
  - Captura pacotes enviados ou recebidos pelo computador
  - Recebe uma cópia dos pacotes que estão trafegando na rede

Sniffer

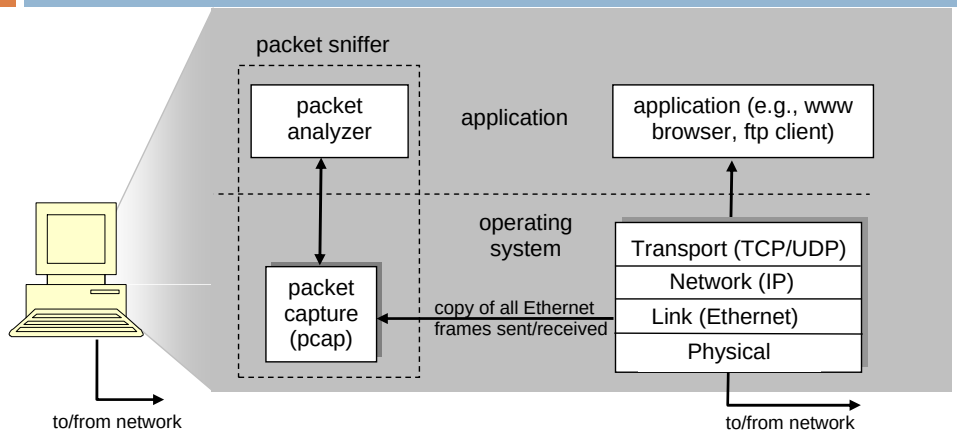

Figure 1: Packet sniffer structure

- A **biblioteca de captura de pacotes** recebe uma cópia de cada quadro Ethernet que é enviado ou recebido pelo seu computador.
- **analisador de pacotes,** que exibe o conteúdo de todos os campos dentro de uma mensagem do protocolo.

Wireshark

- Wireshark = *sniffer* de pacotes
  - http://www.wireshark.org
  - Sucessor do Ethereal
  - Disponível para Windows, Linux/Unix e Mac
    - Usa bibliotecas de captura Winpcap ou libpcap

Executando o Wireshark

- A melhor maneira de aprender sobre qualquer novo software é experimentá-lo!
- Vamos assumir que seu computador está conectado à Internet através de uma interface Ethernet com fio. Faça o seguinte:

1 - Inicie seu web browser favorito.

2 - Inicie o software Wireshark.

  - Você irá provavelmente ver uma janela ainda sem nenhum dado nas suas janelas, dado que Wireshark ainda não começou a capturar pacotes.

Executando o Wireshark

3 - Para começar a captura de pacotes, selecione o menu `Capture` e selecione `Options`. Isto fará com que a janela "*Wireshark: Capture Options*" seja exibida

4 - Você pode usar a maioria dos valores padrão nesta janela, mas desmarque a opção "`Hide capture info dialog`", em "opções de exibição".

Executando o Wireshark

4 – (cont...) As interfaces de rede (ou seja, as conexões físicas) que seu computador possui com a rede serão mostradas na parte superior da janela Opções de Captura.

- Caso o seu computador tenha mais de uma interface de rede ativa (por exemplo, se você tem tanto uma conexão Ethernet com e sem fio), você terá de escolher a interface que será usada para enviar e receber pacotes (muito provavelmente a interface com fio).

Depois de selecionar a interface de rede (ou usando a interface padrão escolhida pelo Wireshark), clique em Iniciar (***Start***).

A captura de pacotes começará agora - todos os pacotes enviados/recebidos a partir de/por seu computador serão capturados pelo Wireshark!

Executando o Wireshark

5 - Assim que começar a captura de pacotes, uma janela de resumo de captura pacotes será exibida.

- Esta janela resume o número de pacotes de diversos tipos que estão sendo capturados, e (importante!) contém o botão de parada "*Stop*" que vai permitir-lhe parar a captura de pacotes.
  - Você pode encerrar a captura de pacotes através da seleção menu *Capture* > *Stop*, ou através do atalho, Ctrl+E, ou clicando no quarto ícone da esquerda para a direita na barra de ferramentas principal.

Mas não pare de capturar pacotes ainda !

Executando o Wireshark

6 - Enquanto o Wireshark estiver rodando, entre a URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html e veja a página exibida no navegador.

- A fim de exibir esta página, o seu navegador irá se conectar ao servidor HTTP em `gaia.cs.umass.edu` e trocar mensagens HTTP com o servidor para download nesta página. Os quadros Ethernet contendo essas mensagens HTTP serão capturados pelo Wireshark.

7 - Após o seu browser exibir a página intro-wireshark-file1.html, pare a captura de pacotes do Wireshark, selecionando *parar* (*STOP*) na janela de captura do Wireshark (ou Ctrl+E).

Executando o Wireshark

7 – (Cont).

Isto fará com que a janela de captura do Wireshark desapareça e a janela principal do Wireshark mostre todos os pacotes capturados desde que começou a captura de pacotes.

Você tem agora pacotes reais que contêm todas as mensagens de protocolo trocadas entre o seu computador e outras entidades de rede! A troca de mensagens HTTP com o servidor web gaia.cs.umass.edu deve aparecer em algum lugar na listagem de pacotes capturados.

- Mas haverá muitos outros tipos de pacotes exibidos também (veja por exemplo, os diferentes tipos de protocolos mostrados na coluna *Protocol*).
- Mesmo que a única ação que você tomou foi o download de uma página da web, havia evidentemente, muitos outros protocolos em execução no computador que são desconhecidos para o usuário. Vamos aprender muito mais sobre estes protocolos com o progresso da matéria! Por agora, você deve apenas estar ciente de que muitas vezes há muito mais coisas acontecendo que o "que podemos ver“!

Executando o Wireshark

- 8 - Digite "http" (sem as aspas e em minúsculas - todos os nomes de protocolo estão em minúsculas no Wireshark) na janela de especificação do filtro de visualização no topo da janela principal. Em seguida, selecione Aplicar - *Apply* (à direita de onde você entrou "http"). Isto fará com que apenas mensagens HTTP sejam exibidas na janela de lista de pacotes.

Executando o Wireshark

- 9 - Selecione a primeira mensagem HTTP mostrada na janela de listagem de pacotes. Deve ser a mensagem GET do HTTP que foi enviada a partir do seu computador para o servidor HTTP gaia.cs.umass.edu.

  Quando você selecionar a mensagem GET, serão apresentadas na janela de cabeçalho dos pacotes, as informações dos cabeçalhos do quadro Ethernet, do datagrama IP, do segmento TCP e da mensagem HTTP. Clicando na caixas mais-e-menos no lado esquerdo da janela de detalhes do pacote, minimize a quantidade de informações apresentadas. *Maximize* a quantidade de informações apresentada sobre o protocolo HTTP.

Exercícios

- Responda às seguintes perguntas, baseado nos seus experimentos com o Wireshark:

  1. Liste os diferentes protocolos que aparecem na coluna de protocolo na janela de listagem de pacotes sem a filtragem do passo 7 acima.

  2. Quanto tempo passou desde que a mensagem GET do http foi enviada até que a resposta OK tenha sido recebida?
     - Por default, o valor da coluna de Tempo na janela de listagem de pacotes, é a quantidade de tempo, em segundos, desde que a captura do Wireshark teve início. Para apresentar o campo de Tempo no formado de hora do dia, selecione o menu de *View*, depois selecione o *Time Display Format*, então selecione *Time-of-day*.

Exercícios

3. Qual é o endereço Internet de gaia.cs.umass.edu (também conhecido como www-net.cs.umass.edu)? Qual é o endereço IP do seu computador?

4. Imprima duas mensagens HTTP apresentadas no passo 9 acima.
   - Para fazer isto, selecione *Print* do menu *File*, e selecione "*Selected Packet Only*" e "*Packet details: as displayed*" e depois clique *Print*.
   - Imprima para PDF

5. Há outras mensagens relacionadas a requisição ao site gaia? Se sim, o que é procurado e qual o retorno?

Referências

- Wireshark http://www.wireshark.org
- *Computer Networking: A Top- down Approach, 4rd edition.*