Pontifícia Universidade Católica do Rio Grande do Sul
Escola Politécnica
Laboratório de Redes de Computadores

Monitoração de Protocolos de Aplicação

Objetivo

Monitorar pacotes de protocolos de aplicação e identificar a constituição do *header* do protocolo, o encapsulamento pelos demais protocolos da pilha e o fluxo de comunicação entre origem e destino.

Descrição

Utilize o *Wireshark* para capturar pacotes dos seguintes protocolos de aplicação:

- DNS
- HTTP / HTTPS
- DHCP

Para cada protocolo, identifique:

- Os campos do *header* protocolo de aplicação
- Como é o encapsulamento do protocolo pelos demais níveis da pilha TCP/IP
    - Observe se o protocolo é encapsulado por todos os demais níveis da pilha;
    - Observe se todo as informações do *header,* do protocolo de aplicação e dos demais níveis, podem ser acessadas em texto aberto ou estão criptografadas.
- O fluxo de mensagens entre origem e destino. Trace um diagrama de comunicação mostrando a conversa entre a origem e o destino, apresentando:
    - O endereço das portas de origem e destino (fim-a-fim) utilizadas no protocolo de transporte.
    - O endereço IPv4 (endereço fim-a-fim) da origem e do destino utilizado em cada datagrama do fluxo monitorado para cada protocolo de aplicação.
    - O endereço MAC (endereço ponto-a-ponto) da origem e do destino utilizado em cada datagrama do fluxo monitorado para cada protocolo de aplicação. Identifique as máquinas às quais o endereço MAC pertence.
- Para o protocolo HTTP, verifique também qual a versão do HTTP está em uso e qual o protocolo de transporte em uso.

Dicas

DHCP

- Se você estiver usando Linux, para gerar tráfego do protocolo DHCP utilize o comando *dhclient.* Exemplo:
    - *sudo dhclient -r* --- para liberar o IP atual
    - *sudo dhclient* -4 --- para solicitar um novo IPv4

Atenção! O comando sudo fará com que o dhclient seja executado com permissão de super usuário (root).

- Se você estiver usando Windows, para gerar tráfego do protocolo DHCP utilize o comando *ipconfig.* Exemplo:
  - *ipconfig /release*
  - *net stop dhcp*
  - *net start dhcp*
  - *ipconfig /renew*

Atenção! Faça isso com permissão de Administrador.

HTTP

- Acesse também páginas não seguras, ou seja, que não utilizam o protocolo HTTPS
- Exemplo: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

DNS

- Acesse um site utilizando a sua URL, utilizando o *browser* ou simplesmente executando um *ping* para este destino.

Resultado e Entrega

Entrega: Relatório com o resultado da monitoração.

Grupos: até 2 alunos.