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

Trabalho Final
Monitor de Tráfego de Rede em Tempo Real

Objetivo

O objetivo geral deste trabalho é desenvolver uma ferramenta para monitoramento de tráfego de rede em tempo real utilizando raw sockets. A ferramenta deve ser capaz de capturar, interpretar e classificar pacotes de rede, além de fornecer uma interface do usuario simples para visualizar contadores e estatísticas de tráfego de rede e ao mesmo tempo escrever um histórico dos pacotes recebidos em um arquivo de log.

Os objetivos específicos incluem:

- Desenvolvimento de uma aplicação usando sockets raw;
- Estudo do funcionamento dos protocolos de rede e do relacionamento entre as camadas;
- Entender como os pacotes de dados são estruturados e como eles podem ser interpretados para extrair informações uteis;
- Entender o tráfego de uma rede local e os tipos de protocolos normalmente trafegados.

Descrição

O monitor de tráfego de rede em tempo real a ser desenvolvido deve ser capaz de identificar e classificar diferentes tipos de pacotes de dados que passam pela rede. Isso inclui identificar protocolos de rede como Ethernet, IPv4, IPv6, ARP, TCP, UDP, ICMP, ICMPv6, etc, bem como origem, destino e tamanho dos pacotes. O programa a ser desenvolvido deve possuir uma interface modo texto que apresenta contadores para cada tipo de pacote recebido. Para cada protocolo, deve apresentar um conjunto de informações que serão mantidos em arquivos de log do tipo .csv, para as camadas 2, 3 e 4 da pilha de protocolos TCP/IP.

O arquivo de log para camada de enlace (camada2.csv) deve ter as seguintes colunas:

- Data e hora que o quadro foi capturado (ex: 2023-06-05 20:43:10);
- Endereço MAC de origem (ex: 02:42:d3:0c:8a:3e);
- Endereço MAC de destino;
- Protocolo que o quadro carrega (EtherType) no formato hexadecimal (ex: 0x0800 – IPv4);
- Tamanho total do quadro em bytes.

O arquivo de log para o protocolo IP na camada de rede (camada3.csv) deve ter as seguintes colunas:

- Data e hora que o pacote foi capturado;
- Nome do protocolo (ex: IPv4 ou IPv6);

- Endereço IP de origem (ex: 100.114.7.75, fe80::ad3e:46fc:abf7:55c9);
- Endereço IP de destino;
- Número identificador do protocolo que está sendo carregado no pacote;
- Tamanho total do pacote em bytes.

O arquivo de log para camada de transporte (camada4.csv) deve ter as seguintes colunas:

- Data e hora que o pacote foi capturado;
- Nome do protocolo (ex: TCP, UDP, etc.);
- Endereço IP de origem;
- Porta de origem (ex: 443 - HTTPS);
- Endereço IP de destino;
- Porta de destino;
- Tamanho total do pacote em bytes.

Os arquivos de log devem ser atualizados em tempo real e a qualquer momento deve ser possível dar um "cat" para visualizar o que foi capturado até o momento.

Resultado e Entrega

Grupo: grupos de até 3 alunos.

Data de entrega: **23/06** no Moodle

Apresentação: 23/06 e 30/06

Observações Gerais: É importante que **todos os integrantes dos grupos estejam aptos a apresentarem o trabalho** a partir do início da aula. Para a entrega, é esperado que apenas um dos integrantes envie pelo Moodle, até a data e hora especificadas, um **arquivo .zip com os nomes dos integrantes**, contendo **o código fonte completo do projeto** e **um relatório descrevendo a implementação e os testes realizados**.

IMPORTANTE: Não serão aceitos trabalhos entregues fora do prazo. Trabalhos que não compilam ou que não executam não serão avaliados. Todos os trabalhos serão analisados e comparados. Caso seja identificada cópia de trabalhos, todos os trabalhos