



Definição do Primeiro Trabalho

O trabalho consiste em desenvolver um monitor de rede para geração de estatísticas e alertas sobre o tráfego da rede. O monitor deve apresentar as informações sobre o tráfego através de uma interface textual ou gráfica. O usuário deve informar a interface que deseja monitorar ao iniciar a execução do monitor. A interface escolhida deve ser configurada para o modo promíscuo. O monitor deve ser implementado em C ou C++, usando socket raw, e deve implementar as seguintes funcionalidades:

- Geral
 - Apresentar min/max/média do tamanho dos pacotes recebidos
- Nível de Enlace
 - Quantidade e porcentagem de ARP Requests e ARP Reply
- Nível de Rede
 - Quantidade e porcentagem de pacotes ICMP
 - Quantidade e porcentagem de ICMP Echo Request e ICMP Echo Reply
 - Lista com os 5 IPs mais acessados na rede
- Nível de Transporte
 - Quantidade e porcentagem de pacotes UDP
 - Quantidade e porcentagem de pacotes TCP
 - Número de conexões TCP iniciadas
 - Lista com as 5 portas TCP mais acessadas
 - Lista com as 5 portas UDP mais acessadas
- Nível de Aplicação
 - Quantidade e porcentagem de pacotes HTTP
 - Quantidade e porcentagem de pacotes DNS
 - Quantidade e porcentagem para outros 2 protocolos de aplicação quaisquer
 - Lista com os 5 sites mais acessados

Resultados e Entrega

Grupos: individual ou em dupla.

Entrega: código-fonte e manual explicando o funcionamento do monitor.

Data Entrega e apresentação: 16/09/2016