**Engenharia de Computação - Redes de Computadores A**

**Atividade 6**

|  |  |
| --- | --- |
| **Participantes** | **RA** |
| Bruno Camilo Silvério | 16080293 |
| Bruno Vicente Donaio Kitaka | 16156341 |
| Marcelo Dib Coutinho | 16023673 |
| Rafael Fioramonte | 16032708 |

**Sumário**

* **Introdução ……………………………. 2**
* **Fundamentação Teórica ……………………………. 2**
* **Desenvolvimento ……………………………. 2**
* **Resultados ……………………………. 3**
* **Conclusão ……………………………. 17**

1. **Introdução**

O experimento possibilitou um estudo inicial e a familiarização com o Wireshark, para que possamos responder a todas as perguntas relacionadas a análise de pacotes.

Wireshark nos permite exibir os conteúdos das mensagens sendo enviadas/recebidas de/por protocolos em diferentes camadas da pilha de protocolos.

1. **Fundamentação Teórica**

As redes de computadores são constituídas por múltiplas máquinas (computadores) ligadas entre si de modo que possam trocar informações a partir dessa ligação, tais dados pode ser enviados *bit* a *bit* ou na forma de pacotes.

Os pacotes de dados são constituídos por uma sequência de bytes formatados de modo que possam ser transmitidos juntos e ao chegarem a seu destino possam ser reorganizados para montar a “mensagem” enviada.

O modelo utilizado pelas redes de computadores hoje em dia é o Modelo OSI (Open System Interconnection), padrão de comunicação onde elas são dividas em 7 camadas de abstração: camada física, camada de enlace de dados, camada de rede, camada de transporte, camada de sessão, camada de apresentação e camada de aplicação. Tais abstrações são feitas para que máquinas heterogêneas possam comunicar entre si e não importe a tecnologia utilizada.

O Wireshark é um programa que analisa o tráfego de rede, e o organiza por protocolos. Através desta aplicação é possível controlar o tráfego de uma rede e monitorar a entrada e saída de dados do computador, em diferentes protocolos, ou da rede à qual o computador está ligado.

Também é possível controlar o tráfego de um determinado dispositivo de rede numa máquina que pode ter um ou mais desses dispositivos. Se você estiver a rede local, com micros ligados através de um hub ou switch, outro usuário pode usar o Wireshark para capturar todas as suas transmissões.

1. **Resultados**
2. **Conclusão**

Com esse experimento nos foi apresentado uma ferramenta de análise de pacote chamada Wireshark. Após as instalações do Wireshark e leitura dos PDFs, fizemos a análise da aplicação funcionando, seguindo todas as etapas para melhor entender a ferramenta e para conseguir responder às perguntas propostas pelo professor.

As questões que nos foram propostas foi para testar nossa capacidade a executar o Wireshark e explorar algumas das capacidades dele. Utilizamos o Wireshark para investigar protocolos em operação, tais como protocolo HTTP: a interação básica GET/resposta do HTTP, formatos de mensagens HTTP. E observamos mais de perto o lado cliente do DNS.