Instituto Federal de Educação, Ciência e Tecnologia do RN
Câmpus Currais Novos
Curso: Tecnologia em Sistemas para Internet
Disciplina: Aplicações de Redes de Computadores (TEC.1032)

Atividade Prática em Laboratório (Roteiro) :: Análise de Tráfego TCP

A atividade consiste em proporcionar ao aluno o contato com a técnica de análise de tráfego de redes a partir do uso de ferramentas que manipulam arquivos .pcap (arquivos com pacotes capturados de um tráfego de rede), com foco na análise da camada de transporte (segmentos TCP) e inferiores (rede = datagramas IP e enlace = quadros ethernet).

1) Baixe o arquivo de captura **`tcp01.pcap`** para realizar a análise.

```
https://www.segurancaderedes.com.br/arc/tcp01.pcap
```

2) Acesse o site da ferramenta online Packet Safari Analyzer (atividade também pode ser feita usando o aplicativo Wireshark)

```
https://app.packetsafari.com
```

3) Faça o upload do arquivo tcp01.pcap para iniciar a análise (botão Upload PCAP) e responda:

4) Análise das camadas de rede e enlace:

4.1) Qual o protocolo utilizado nos dois primeiros pacotes capturados? Explique o que foi solicitado no pacote 01 e o que foi respondido no pacote 02.

4.2) Qual o endereço MAC e endereço IP do host de origem (que iniciou a conexão)? E o endereço MAC e endereço IP do host de destino?

5) Análise do estabelecimento da conexão TCP (3-Way-Handshake):

5.1) Quais os pacotes relacionados ao procedimento 3-Way-Handshake (estabelecimento de conexão TCP)?

5.2) Qual a porta TCP utilizada pelo host de origem? Qual a porta TCP utilizada pelo host de destino?

5.3) Qual o número de sequência enviado pelo host de origem no estabelecimento da conexão?

5.4) Quantos bytes tem o cabeçalho do segmento enviado pelo host de origem no estabelecimento da conexão?

5.5) Qual o tamanho da janela de recepção informada pelo host de origem no estabelecimento da conexão?

5.6) Qual o valor (em hexadecimal) do Checksum calculado pelo host de origem no estabelecimento da conexão?

5.7) Quantos bytes tem o campo 'Options' do cabeçalho TCP informado pelo host de origem no estabelecimento da conexão?

5.8) Dentro do campo 'Options' do cabeçalho TCP informado pelo host de origem no estabelecimento da conexão, foi informado o tamanho máximo que pode ter o segmento (MSS = Maximum Segment Size). Qual é esse tamanho?

5.9) Qual o número de reconhecimento enviado pelo host de destino em resposta ao estabelecimento da conexão?

5.10) Qual o número de sequência enviado pelo host de destino em resposta ao estabelecimento da conexão?

5.11) Qual o tamanho da janela de recepção informada pelo host de destino em resposta ao estabelecimento da conexão?

5.12) Qual o número de sequência enviado pelo host de origem completando o estabelecimento da conexão?

5.13) Qual o valor (em hexadecimal) do Checksum calculado pelo host de origem no segmento que completa o estabelecimento da conexão?

5.14) Qual o tamanho da janela de recepção informada pelo host de origem no segmento que completa o estabelecimento da conexão?

6) Análise (parcial) do tráfego da camada de aplicação:

6.1) Qual o protocolo de aplicação utilizado nesta conexão?

6.2) Qual a 'mensagem' enviada pelo cliente ao servidor no primeiro pacote transmitido com dados da aplicação?

6.3) Qual a 'mensagem' enviada pelo servidor ao cliente no pacote de resposta transmitido na camada de aplicação?

7) Análise do encerramento da conexão TCP:

7.1) Quais os pacotes relacionados ao procedimento de encerramento da primeira sessão (conexão TCP)?

7.2) Quem iniciou o processo de finalização da conexão (cliente ou servidor)?

8) Análise complementar:

8.1) Quais os pacotes relacionados ao segundo procedimento de 3-Way-Handshake (estabelecimento de conexão TCP)?

8.2) Quais os pacotes relacionados ao encerramento da segunda sessão (conexão TCP)?