Universidade Federal do Rio Grande do Norte
Centro de Ensino Superior do Seridó
Departamento de Computação e Tecnologia
Bacharelado em Sistemas de Informação
Disciplina: Redes de Computadores
Docente:Prof. Dr. João Batista Borges Neto

Aluno:
Flávio Glaydson Guimarães Lopes - Matrícula: 20220046917

Relatório - Análise de Captura de Pacotes de Tráfego de Redes

1. QUESTÕES

1 - Implemente um código em Python, utilizando a biblioteca Scapy, para analisar o arquivo de captura captura1.pcap. Em seguida, responda:

a) De que se trata esta comunicação.
b) Quais são os endereços envolvidos.
c) Quantos pacotes são enviados neste tráfego de rede.

OBS: Justifique suas respostas por meio da ilustração dos prints da execução do seu código-fonte.

2 - Implemente um código em Python, utilizando a biblioteca Scapy, para analisar o arquivo de captura captura2.pcap. Em seguida, responda:

a) Descreva o que foi capturado neste tráfego de rede e apresente, por meio da sequência de pacotes, de que se trata esta captura.
b) Apresente estatísticas sobre a quantidade e tipo de pacotes capturados.

3 - Implemente um código em Python, utilizando a biblioteca Scapy, para analisar os arquivos de captura captura3-1.pcap e captura3-2.pcap. Em seguida, responda:

a) Apresenta estatísticas sobre os IPs de origem e destino das capturas.
b) Apresente estatísticas sobre as portas de origem e destino das capturas.
c) Estas capturas representam capturas de um tráfego de redes que passam por um roteador fazendo NAT (Network Address Translation). Estas são realizadas antes e depois do roteador. Com base nisto, responda:

i. Qual é o IP de origem e de destino antes e após a tradução do NAT.
ii. Quais são as portas de origem e de destino antes e após a tradução do NAT.
iii. Justifique suas respostas apresentando suas observações e descobertas.

2. RESULTADOS

1 - (A) - A análise do arquivo “captura.pcap1” indica que se trata de uma comunicação utilizando o protocolo *ICMP* (Internet Control Message Protocol). Este

protocolo é amplamente utilizado para testes de conectividade, como o comando *ping*. No cenário analisado, há uma troca de mensagens *echo-request* (pedido de eco) e **echo-reply** (resposta de eco) entre dois dispositivos na rede, conforme figura 1.

```
Resumo dos pacotes:
Ether / IP / ICMP 192.168.0.3 > 192.168.0.2 echo-request 0 / Raw
Ether / IP / ICMP 192.168.0.2 > 192.168.0.3 echo-reply 0 / Raw
Ether / IP / ICMP 192.168.0.3 > 192.168.0.2 echo-request 0 / Raw
Ether / IP / ICMP 192.168.0.2 > 192.168.0.3 echo-reply 0 / Raw
Ether / IP / ICMP 192.168.0.3 > 192.168.0.2 echo-request 0 / Raw
Ether / IP / ICMP 192.168.0.2 > 192.168.0.3 echo-reply 0 / Raw
```

Figura 1 - Resumo dos pacotes

A execução do código-fonte revela pacotes ICMP com mensagens de pedido e resposta de eco entre os endereços IP 192.168.0.3 e 192.168.0.2. Este comportamento é característico de um teste de ping.

(B)Os endereços IP envolvidos nesta comunicação são:

- **192.168.0.3**: Este endereço corresponde ao dispositivo que inicia a comunicação enviando os pacotes ICMP do tipo **echo-request**.
- **192.168.0.2**: Este endereço corresponde ao dispositivo que responde aos pacotes recebidos, enviando pacotes ICMP do tipo **echo-reply**.

```
Pacote 1:
  Origem: 192.168.0.3
  Destino: 192.168.0.2
Pacote 2:
  Origem: 192.168.0.2
  Destino: 192.168.0.3
Pacote 3:
  Origem: 192.168.0.3
  Destino: 192.168.0.2
Pacote 4:
  Origem: 192.168.0.2
  Destino: 192.168.0.3
Pacote 5:
  Origem: 192.168.0.3
  Destino: 192.168.0.2
Pacote 6:
  Origem: 192.168.0.2
  Destino: 192.168.0.3
```

Figura 2 - Endereços de origem e de destino

Conforme figura 2 e os resultados obtidos, cada pacote contém informações claras de origem e destino, identificando os IPs envolvidos na troca de mensagens ICMP.

(C) - No total, foram capturados **6 pacotes** nesta comunicação:

- **3 pacotes de echo-request**, enviados pelo endereço 192.168.0.3 para 192.168.0.2.
- **3 pacotes de echo-reply**, enviados pelo endereço 192.168.0.2 para 192.168.0.3.

O número total de pacotes foi contabilizado automaticamente pelo código desenvolvido, e o detalhamento de cada pacote foi apresentado no terminal.

```
PS C:\Users\SAMSUNG\Desktop\computer_network\tarefa02> python analise_captura1.py
WARNING: No libpcap provider available ! pcap won't be used
Número de pacotes capturados: 6
Resumo dos pacotes:
Ether / IP / ICMP 192.168.0.3 > 192.168.0.2 echo-request 0 / Raw
Ether / IP / ICMP 192.168.0.2 > 192.168.0.3 echo-reply 0 / Raw
Ether / IP / ICMP 192.168.0.3 > 192.168.0.2 echo-request 0 / Raw
Ether / IP / ICMP 192.168.0.2 > 192.168.0.3 echo-reply 0 / Raw
Ether / IP / ICMP 192.168.0.3 > 192.168.0.2 echo-request 0 / Raw
Ether / IP / ICMP 192.168.0.2 > 192.168.0.3 echo-reply 0 / Raw
Pacote 1:
  Origem: 192.168.0.3
  Destino: 192.168.0.2
Pacote 2:
  Origem: 192.168.0.2
  Destino: 192.168.0.3
Pacote 3:
  Origem: 192.168.0.3
  Destino: 192.168.0.2
Pacote 4:
  Origem: 192.168.0.2
  Destino: 192.168.0.3
Pacote 5:
  Origem: 192.168.0.3
  Destino: 192.168.0.2
Pacote 6:
  Origem: 192.168.0.2
  Destino: 192.168.0.3
PS C:\Users\SAMSUNG\Desktop\computer_network\tarefa02>
```

Figura 3 - Análise completa da captura 1

2 - (A) - A análise do arquivo **captura2.pcap,** conforme figura 4 revelou que o tráfego de rede capturado se trata de uma interação composta por duas etapas principais: resolução de nomes de domínio (DNS) e estabelecimento de uma conexão HTTP via TCP. Inicialmente, o dispositivo com endereço IP **192.168.0.3** realizou consultas ao servidor DNS para resolver o domínio **labepi.ufrn.br**. O servidor DNS respondeu às solicitações, fornecendo o endereço IP correspondente, **177.20.148.218**. Após a obtenção do endereço IP, foi iniciado o processo de conexão TCP entre o dispositivo cliente (**192.168.0.3**) e o servidor (**177.20.148.218**), utilizando a porta padrão HTTP (80). Durante essa conexão, foi observado o handshake inicial do protocolo TCP (SYN, SYN-ACK e ACK), seguido pela troca de dados e, posteriormente, o encerramento da comunicação com pacotes contendo a flag FIN-ACK.

```
PS C:\Users\SAMSUNG\Desktop\computer_network\tarefa02> python analise_captura2.py
WARNING: No libpcap provider available ! pcap won't be used
Resumo do tráfego:
Ether / IP / UDP / DNS Qry b'labepi.ufrn.br.'
Ether / IP / UDP / DNS Qry b'labepi.ufrn.br.'
Ether / IP / UDP / DNS Ans 177.20.148.218
Ether / IP / UDP / DNS Ans
Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http S
Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 SA
Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http PA / Raw
Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 A
Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 A / Raw
Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 PA / Raw
Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 PA / Raw
Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http FA
Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 FA
Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A

Estatísticas de tipos de pacotes:
Ether: 18 pacotes
PS C:\Users\SAMSUNG\Desktop\computer_network\tarefa02>
```

Figura 4 - Análise do arquivo captura 2

(B) - Foram capturados ao todo 18 pacotes, dos quais 4 correspondem ao tráfego UDP/DNS, sendo 2 consultas e 2 respostas, e os 14 pacotes restantes pertencem ao tráfego TCP. No contexto do tráfego TCP, identificaram-se pacotes relacionados tanto ao estabelecimento e término da conexão quanto à troca de dados durante a comunicação HTTP. Esses dados evidenciam que o tráfego capturado representa uma sequência típica de navegação na web, onde um cliente resolve o nome de domínio para um endereço IP e, em seguida, estabelece uma comunicação com o servidor para transferência de dados via HTTP.

3 -

I. As capturas analisadas mostram que, antes da tradução NAT, o endereço IP de origem era privado, como **192.168.1.100**, e, após a tradução, ele foi substituído por um IP público, como **71.192.34.104**. Essa substituição ocorre porque o NAT permite que dispositivos em uma rede privada se comuniquem com redes externas, utilizando o endereço público do roteador. O IP de destino permaneceu inalterado nas capturas, pois representa os servidores externos que estavam sendo acessados.

II. Em relação às portas, antes do NAT, as portas de origem são atribuídas pelas aplicações locais, podendo variar entre valores como **1028, 51554** ou **4331**. Após a tradução NAT, o roteador substitui essas portas por valores diferentes, como **4335** ou **57244**, para identificar de forma única cada conexão na tabela de NAT e permitir o retorno correto dos pacotes ao dispositivo de origem. Já as portas de destino permanecem inalteradas, geralmente representando serviços específicos nos servidores, como HTTP (porta 80) ou HTTPS (porta 443).

III. Essas mudanças são justificadas pela funcionalidade do NAT, que traduz os endereços e portas de origem para viabilizar a comunicação com a internet sem

expor diretamente os dispositivos privados. Isso também garante que múltiplas conexões simultâneas possam ser gerenciadas pelo roteador, preservando a segurança e a organização da rede interna.

```
PS C:\Users\SAMSUNG\Desktop\computer_network\tarefa02> python analise_captura3.py
WARNING: No libpcap provider available ! pcap won't be used
Estatísticas para a primeira captura:
IPs de origem:
192.168.1.100: 61
68.87.71.230: 5
74.125.91.113: 7
74.125.106.31: 18
69.183.241.120: 1
64.233.169.104: 40
IPs de destino:
10.119.240.64: 2
68.87.71.230: 5
192.168.1.100: 71
74.125.91.113: 9
74.125.106.31: 13
69.183.241.120: 1
64.233.169.104: 30
128.119.47.218: 1

Estatísticas para a segunda captura:
IPs de origem:
71.192.34.104: 61
68.87.71.230: 5
74.125.91.113: 7
74.125.106.31: 18
69.183.241.120: 1
169.254.247.145: 5
64.233.169.104: 40
73.160.28.1: 1
IPs de destino:
68.87.71.230: 5
71.192.34.104: 71
74.125.91.113: 9
74.125.106.31: 13
69.183.241.120: 1
224.0.0.252: 2
169.254.255.255: 3
10.119.240.64: 1
64.233.169.104: 30
255.255.255.255: 1
128.119.47.218: 1
85.218.105.47: 1

Comparação NAT:
IP de origem antes do NAT: ['192.168.1.100', '68.87.71.230', '74.125.91.113', '74.125.106.31', '69.183.241.120', '64.233.169.104']
IP de origem depois do NAT: ['71.192.34.104', '68.87.71.230', '74.125.91.113', '74.125.106.31', '69.183.241.120', '169.254.247.145', '64.233.169.104', '73.160.28.1']
Portas de origem antes do NAT: [1028, 51554, 53, 4330, 80, 58982, 4331, 15525, 49200, 4335, 57244, 4336, 4337, 4338, 60524]
Portas de origem depois do NAT: [51554, 53, 4330, 80, 58982, 4331, 15525, 53976, 50002, 137, 1028, 49200, 4335, 57244, 4336, 4337, 4338, 67, 60524]
PS C:\Users\SAMSUNG\Desktop\computer_network\tarefa02>
```

Figura 5 - Análise e estatísticas das capturas 3.1 e 3.2