Universidade Federal do Rio Grande do Norte - UFRN
Centro de Ensino Superior do Seridó - CERES
Departamento de Computação e Tecnologia - DCT

Curso: Bacharelado em Sistemas de Informação
Disciplina: DCT2102 – Redes de Computadores
Professor: João Borges
Data: 14 de janeiro de 2025

Atividade em Dupla

Análise de Captura de Pacotes de Tráfego de Redes

ATENÇÃO 1: Só serão aceitos trabalhos em **Dupla** ou **Individual**, mais do que isso invalidará o trabalho;

ATENÇÃO 2: Não serão permitidos plágios entre os grupos, sendo punidos, ambos os grupos que tiverem seus trabalhos iguais, com nota 0 (zero).

1 Introdução

1. Esta atividade consiste na tarefa de implementação e análise de tráfegos de redes capturados e armazenados em formato PCAP (*Packet Capture*)[1].

[1] `https://en.wikipedia.org/wiki/Pcap`

2. A análise de pacotes de rede é uma etapa importante para entender o tráfego em uma rede, permitindo extrair informações valiosas dos pacotes capturados e realizar análises avançadas.

3. O PCAP é um formato binário de arquivos que é utilizado para armazenar um tráfego de pacotes de redes, permitindo sua posterior análise[2].

4. O formato PCAP pode ser aberto firetamente por aplicativos como o Wireshark, ou pode ser manipulado utilizando-se a API de uma biblioteca de programação.

5. Neste trabalho, será utilizada a biblioteca Scapy[3]

2 Análise de tráfego com Scapy

A biblioteca Scapy permite tanto a captura de pacotes quanto a análise de pacotes previamente capturados.

A seguir está uma breve introdução com as principais funcionalidades da desta biblioteca a serem utilizadas neste trabalho.

Para mais detalhes e aprofundamento, verificar estes endereços:

- Site Oficial: `https://scapy.net/`
- Documentação: `https://scapy.readthedocs.io/en/latest/`

[2] `https://www.ietf.org/archive/id/draft-gharris-opsawg-pcap-01.html`

[3] `https://scapy.net/`

- Scapy em 20 minutos: `https://github.com/secdev/scapy/blob/master/doc/notebooks/Scapy%20in%2015%20minutes.ipynb`
- Analyzing Packet Captures with Python: `https://vnetman.github.io/pcap/python/pyshark/scapy/libpcap/2018/10/25/analyzing-packet-captures-with-python-part-html`

Outras fontes podem ser facilmente encontradas.

2.1 Instalação

Para utilizar a biblioteca Scapy, é preciso realizar a sua instalação. Em ambientes Debian Linux, o pacote a ser instalado é o `python3-scapy`.

Também há alternativas para outras versões e sistemas operacionais. Verifique a sua versão e efetue a instalação.

2.2 Analisando um arquivo PCAP

O primeiro passo é importar a funcionalidade da biblioteca:

```
from scapy.all import *
```

Para abrir um arquivo de captura .pcap:

```
packets = rdpcap("captura1.pcap")
```

A variável `packets`, agora, armazena uma lista com todos os pacotes desta captura, na ordem em que foram capturados pela interface de rede.

Para exibir a quantidade de pacotes capturados:

```
print(f"Número de pacotes capturados: {len(packets)}")
```

Para exibir um sumário dos pacotes capturados:

```
for packet in packets:
    print(packet.summary())
```

2.3 Analisando os cabeçalhos de um pacote

Para verificar se um determinado pacote possui um determinado cabeçalho, e exibir os seus campos:

```
packet = packets[1]
if packet.haslayer("IP"):
    print(f"Origem: {packet['IP'].src}")
    print(f"Destino: {packet['IP'].dst}")
```

Observe a sintaxe desta verificação, com o método `packet.haslayer` Outros cabeçalhos podem ser verificados, como TCP, UDP, ICMP, etc.

Um vez identificando que há determinado cabeçalho no pacote, é possível acessar os campos por cabeçalho.

Para exibir mais detalhes sobre um pacote, e verificar os nomes de seus campos:

```
packet.show()
```

2.4 Estatísticas de um pacote

Para obter estatísticas e contabilizar certas informações úteis dos pacotes, pode-se utilizar contadores da biblioteca `collections`.

```
from collections import Counter
```

Esta biblioteca permite a criação de contadores e a contabilização dos valores utilizando os próprios campos como chaves do contador:

```
# inicializando os contadores
src_ips = Counter()
dst_ips = Counter()

# iterando pelos pacotes e contabilidando informações de l
for packet in packets:
    if packet.haslayer("IP"):
        src_ips[packet['IP'].src] += 1
        dst_ips[packet['IP'].dst] += 1

# exibindo IPs de origem e destino e suas quantidades
print("IPs de origem:")
for ip, count in src_ips.items():
    print(f"{ip}: {count} pacotes")

print("IPs de destino:")
for ip, count in dst_ips.items():
    print(f"{ip}: {count} pacotes")
```

Observe que os IPs de origem e destino são usados como chave dos contadores e origem e destino, sendo incrementado seus valores quando identificados nos pacotes.

Por fim, utilizam-se os itens dos contadores para exibir seus valores.

Agora, com base nestes fundamentos básicos de manipulação dos pacotes, é possível realizar a atividade que está descrita na próxima seção.

3 Descrição da Atividade

A atividade a ser desenvolvida nesta tarefa corresponde em responder questões solicitadas pelo professor, com base na análise de diferentes arquivos de captura PCAP. Para cada questão, devem ser realizadas duas etapas:

1. Implementar um código em Python para analisar um arquivo de captura PCAP, e
2. Descrever a análise, demonstrando suas descobertas e justificativas para as respostas, em um relatório.

Abaixo segue a descrição e requisitos das questões das atividades a serem realizadas neste trabalho.

Questão 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.

Questão 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.

Questão 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) Apresente 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. Qual são as portas de origem e de destino antes e após a tradução do NAT.

iii. Justifique suas respostas apresentando suas observações e descobertas.

Cada uma destas questões devem ser realizadas pelo grupo, devendo ser enviado tanto o código-fonte utilizado em cada análise quanto as respostas em um relatório final.

Os códigos-fonte e o texto deverão ser enviado na tarefa do SIGAA como um único arquivo compactado, até a data estabelecida pelo professor na tarefa cadastrada no sistema.