Trabalho 1 de LabRedes - Monitor de Rede

Integrantes: Lucas Antunes e Henrique Xavier

Para executar o programa basta rodar `sudo python3 sniffer.py`, o programa irá analisar os pacotes e atualizar o terminal em tempo real com estatísticas sobres os pacotes.

Exemplo de saída do sniffer:

```
Packet Sizes
min: 42
max: 1514
mean: 296.09011670852414

Data link
arp_request: 18.72% (1267)
arp_reply: 0.13% (9)

Network
ipv4: 49.71% (3365)
icmp: 19.94% (1350)
icmpecho_request: 0.12% (8)
icmpecho_reply: 0.12% (8)
ipv6: 30.68% (2077)
icmpv6: 1.26% (85)
icmpv6echo_request: 0.12% (8)
icmpv6echo_reply: 0.12% (8)

Transport
udp: 38.87% (2631)
tcp: 18.38% (1244)
Most used ports: [443, 44701, 9993, 60632, 53]

Application
http: 1.09% (74)
https: 32.24% (2182)
dns: 7.33% (496)
dhcp: 0.09% (6)
ssh: 0.90% (61)
```

Implementação

O módulo principal é o `sniffer.py`. Foi utilizado um socket raw para o monitoramento dos pacotes. Para cada pacote é chamada a função `process_packet`. Essa função analisa os protocolos no pacote e passa o resultado da análise para o módulo de estatísticas.

Os pacotes são analisados por meio de uma "escadinha" de funções `handle_*`, onde `*` é o nome de um protocolo. `process_packet` começa chamando `handle_network` para analisar o pacote, pois ele possui um pacote da camada de rede. `handle_network` então lê os headers do pacote e descobre em qual protocolo o corpo do pacote está, com isso ele então chama a função `handle_*` apropriada (`handle_ipv4`, por exemplo).

Cada handler de protocolo vai chamar um handler do nível acima até chegar ao nível de aplicação, que é o último. Essa cascata de chamadas monta ao final uma lista de nomes de protocolos, por exemplo, `['ipv6', 'tcp', 'from_port:443', 'to_port:40822', 'https']`. Note que existem entradas `'from_port:443'` e `'to_port:40822'`, que não correspodem à nenhum protocolo. Isso é uma informação extra que é adicionada à lista para depois podermos calcular as portas mais e menos utilizadas.

Essa lista de protocolos e metadados é então enviada ao módulo `stats.py` para ser processada e contabilizada nas estatísticas.