Wykrywanie ataków sieciowych - lab 1

Zadanie 2

W przypadku polecenia `ping` przechwycone zostały po dwa pakiety *request* i *reply*.

Request:

- typ: 8 (Echo (ping) request)
- kod: 0
- ttl: 64

Reply:

- typ: 0 (Echo (ping) reply)
- kod: 0
- ttl: 54

W przypadku polecenia `traceroute` wszystkie pakiety przekroczyły ttl.

W przypadku polecenia `nc` przechwycony został jeden pakiet *request*, nie została zwrócona odpowiedź `reply`

Request:

- typ: 8 (Echo (ping) request)
- kod: 0
- ttl: 50

Zrzut został zapisany w pliku `icmp.pcapng`

Zadanie 3

Zrzut został zapisany w pliku `tcp.pcapng`

Zadanie 4

Zrzut został zapisany w pliku `dns.pcapng`

Zadanie 5

Pakiety można wczytać poleceniem `tcpdump -qns 0 -X -r nazwa_zrzutu.pcapng`