Kamil Michalak 299089

Sieci Komputerowe – Warsztaty 7

Zadanie 1

Na maszynie Virbian2 strumień danych występuje w postaci niezaszyfrowanej jako pakiety przesyłane z ::1:45910 (ipv6) do ::1:7777 (ipv6)

Pomiędzy maszyną Virbian2 a maszyną Virbian1 strumień danych występuje w postaci zaszyfrowanej jako pakiety przesyłane z 192.168.1.2:6008 do 192.168.1.1:22

Na maszynie Virbian1 strumień danych występuje w postaci niezaszyfrowanej jako pakiety przesyłane z 127.0.0.1:41560 do 127.0.0.1:7

Zadanie 2

- Wygenerowanie kluczy na Virbian2:
  - `V1$> gpg –gen-key`
- Przesłanie klucza
  - V1$> scp .ssh/user1-gpg-key 192.168.1.2:user1-gpg-key
- Edycja klucza
  - `V2$> gpg --edit-key user1@mail.example.com`
  - `gpg> fpr`
  - `gpg> sign`
  - `gpg> quit`
- Odszyfrowanie wiadomości

```
user@virbian:~$ gpg -d message.asc > deciphered_message
gpg: encrypted with 3072-bit RSA key, ID 6A10B007E46E4333, created 2020-06-09
      "user2 <user2@mail.example.com>"
gpg: Signature made Tue Jun  9 22:22:56 2020 CEST
gpg:                using RSA key 43FAF9AE533B872A0AD83273F7B7DA15538F4432
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   1  signed:   0  trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2022-06-09
gpg: Good signature from "user1 <user1@mail.example.com>" [full]
```

- Treść odszyfrowanej wiadomości się zgadza