Sieci komputerowe
Warsztaty 7

Mateusz Markiewicz

7 czerwca 2020

1 Pierwsze zadanie do zaprezentowania

Pierwszym etapem było stworzenie dwóch maszyn wirtualnych z dwiema kartami (NAT oraz sieć wewnętrzna). Następnie aktywowałem oraz skonfigurowałem interfejsy.

- V1#> dhclient -v enp0s3
- V1#> ip link set up dev enp0s8
- V1#> ip addr add 192.168.1.1/24 dev enp0s8

- V2#> dhclient -v enp0s3
- V2#> ip link set up dev enp0s8
- V2#> ip addr add 192.168.1.2/24 dev enp0s8

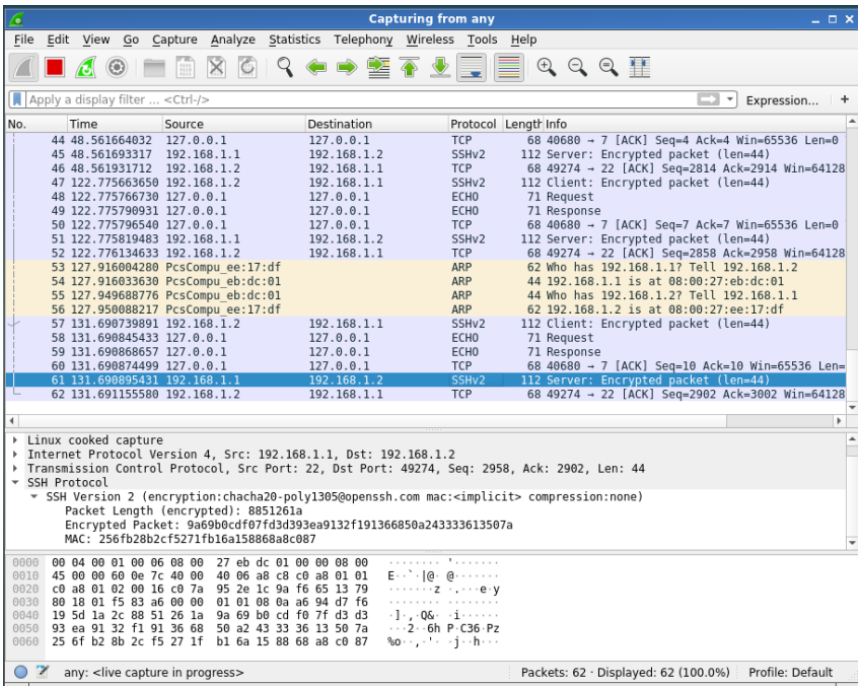
Następnie wykonałem pierwszy tutorial.
Na maszynie $Virbian2$ wykonałem polecenie:

V2$> ssh -N -L 7777 : *localhost* : 7 *user*@192.168.1.1

a po wpisaniu polecenia:

V2$> telnet localhost 7777

odpowiadał serwer echa maszyny $Virbian1$.
Następnie przyjrzałem się pakietom w Wiresharku na obu maszynach.



- Na maszynie *Virbian*2 strumień danych występuje w postaci niezaszyfrowanej jako pakiety przesyłane z :: 1 port 48492 do :: 1 port 7777, (IPv6)
- Pomiędzy maszyną *Virbian*2 a maszyną *Virbian*1 strumień danych występuje w postaci zaszyfrowanej jako pakiety przesyłane z 192.168.1.2 port 49274 do 192.168.1.1 port 22 (IPv4)
- Na maszynie *Virbian*1 strumień danych występuje w postaci niezaszyfrowanej jako pakiety przesyłane z *localhost* port 40680 do *localhost* port 7 (IPv4)

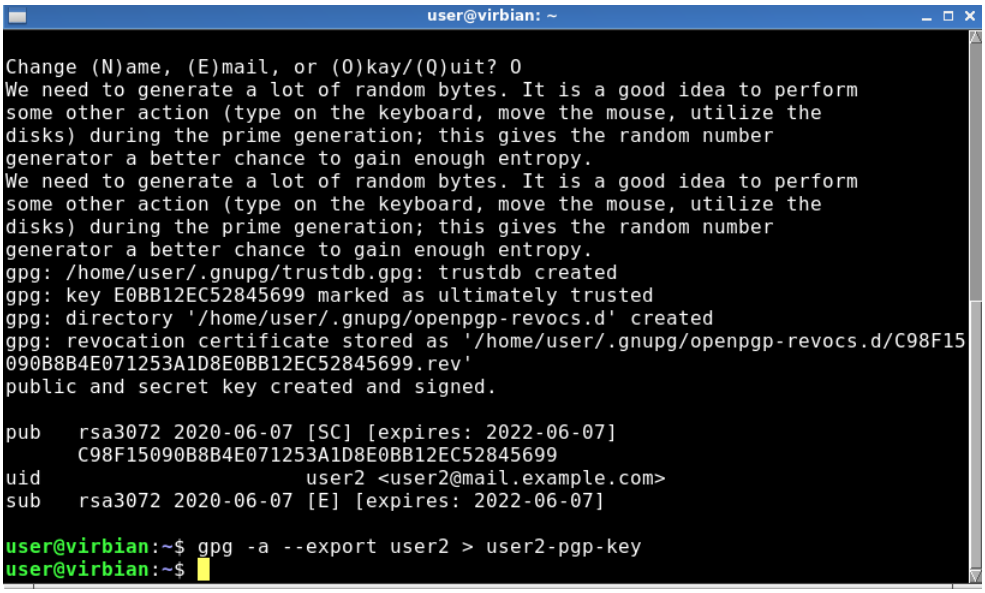
2 Drugie zadanie do zaprezentowania

Na maszynie *Virbian*1 zapisałem klucz publiczny użytkownika user1 za pomocą polecenia:

V1$> gpg -a –export user1 > user1-pgp-key

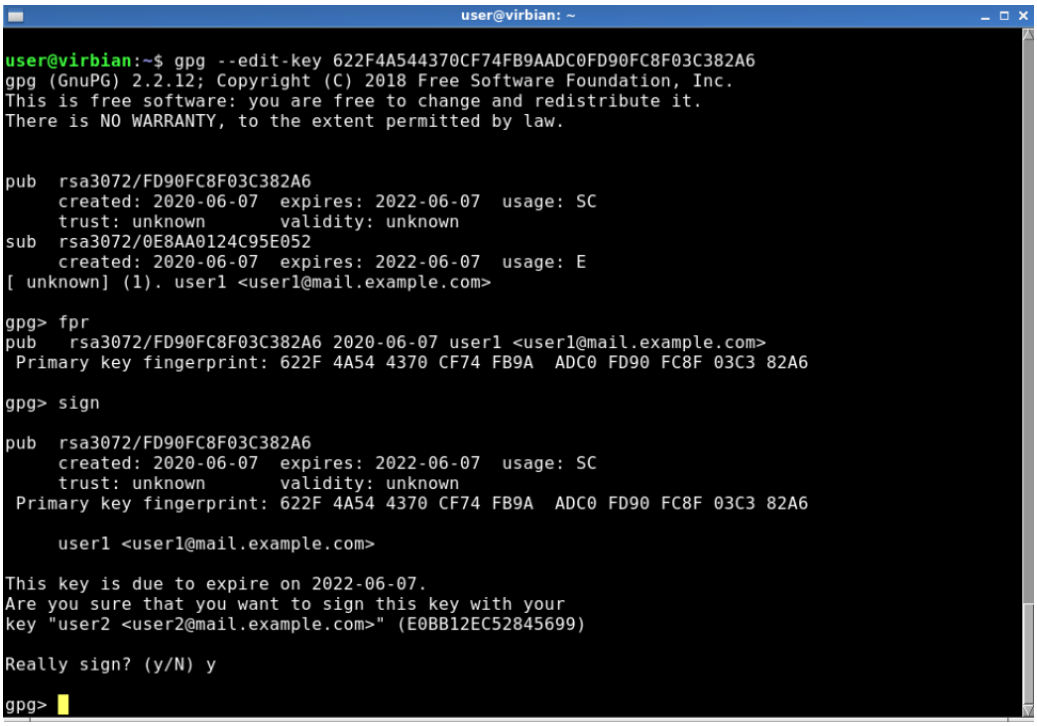
Następnie na maszynie *Virbian*2 wygenerowałem klucze dla użytkownika user2 i zapisałem go do pliku za pomocą poleceń:

- V2$> gpg –gen-key
- V2$> gpg -a –export user2 > user2-pgp-key



Następnie skopiowałem plik user1-pgp-key na maszynę *Virbian*2, a następnie zaimportowałem go do kluczy użytkownika user2 oraz podpisałem kluczem prywatnym użytkownika user2 za pomocą poleceń:

- V1$> scp user1-pgp-key 192.168.1.2 :user1-pgp-key
- V1$> gpg –import < user1-pgp-key
- V1$> gpg –edit-key identyfikator-klucza
- gpg> fpr
- gpg> sign
- gpg> quit



Powyższe działania powtórzyłem na drugiej maszynie.

Następnie na maszynie *Virbian*1 utworzyłem plik message z treścią message321, podpisałem go kluczem użytkownika user1 oraz zaszyfrowałem ją kluczem publicznym użytkownika user2. Następnie skopiowałem go na maszynę *Virbian*2 za pomocą poleceń:

- V1$> gpg -a -r user2 -se message
- V1$> scp message.asc 192.168.1.2:message.asc

```
user@virbian:~/Downloads$ touch message
user@virbian:~/Downloads$ vim message
user@virbian:~/Downloads$ cat message
message321
user@virbian:~/Downloads$ gpg -a -r user2 -se message
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   2  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   2  signed:   0  trust: 2-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2022-06-07
user@virbian:~/Downloads$ ls
message      user1-pgp-key  veracrypt.deb
message.asc  user2-pgp-key  veracrypt.deb.sig
user@virbian:~/Downloads$ scp message.asc 192.168.0.2:message.asc
user@192.168.0.2's password:
message.asc                                   100% 1329     1.7MB/s   00:00
user@virbian:~/Downloads$
```

Na maszynie *Virbian*2 otrzymany plik odszyfrowałem kluczem prywatnym użytkownika user2, a następnie wypisałem odszyfrowaną zawartość - była poprawna.

V2$> gpg -d message.asc > deciphered message

```
user@virbian:~$ ls
message.asc  user1-pgp-key  user2-pgp-key
user@virbian:~$ gpg -d message.asc > deciphered_message
gpg: encrypted with 3072-bit RSA key, ID 2D5D590CE9A13B64, created 2020-06-07
      "user2 <user2@mail.example.com>"
gpg: Signature made Sun Jun  7 18:16:14 2020 CEST
gpg:                using RSA key 622F4A544370CF74FB9AADC0FD90FC8F03C382A6
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 2022-06-07
gpg: Good signature from "user1 <user1@mail.example.com>" [full]
user@virbian:~$ cat deciphered_message
message321
```