

SPRAWOZDANIE Z ZAJĘĆ LABORATORYJNYCH CYBERBEZPIECZEŃSTWO

Lab 09 Ochrona komunikacji

Tomasz Mroczko, 266604

1 Konfiguracja śrowdowiska

Adresy IP



Maszyna używana jako server posiada IP 172.16.96.2. Maszyna używana jako klient posiada IP 172.16.96.3.

Plik client.ovpn

```
kali@kali:/etc/openvpn

File Actions Edit View Help

(kali@kali)-[/etc/openvpn]

sudo vim client.ovpn
[sudo] password for kali:

(kali@kali)-[/etc/openvpn]

cat client.ovpn| grep 172.16.96.2

remote 172.16.96.2 1194

(kali@kali)-[/etc/openvpn]

sss
```

Modyfikacja pliku "client.ovpn".

Nawiązanie połączenia z serverem VPN

```
File Actions Edit View Help

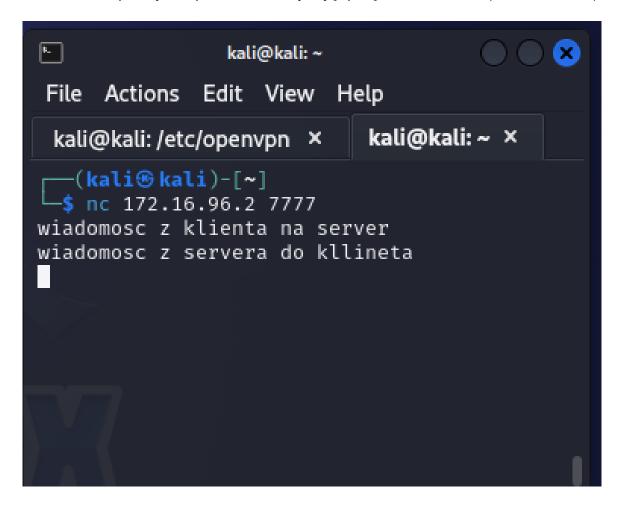
(kali@kali:/etc/openvpn)

$ sudo openvpn — config /etc/openvpn/client.ovpn
2023-12-07 14:35:22 WARNINO: file 'clientA.key' is group or others accessible
2023-12-07 14:35:22 WARNINO: file 'ta.key' is group or others accessible
2023-12-07 14:35:22 UBPNY 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2023-12-07 14:35:22 Library versions: OpenSSL 3.0.11 19 Sep 2023, LZO 2.10
2023-12-07 14:35:22 DCO version: M/A

2023-12-07 14:35:22 UDPY4 link local: (not bound)
2023-12-07 14:35:22 UDPY4 link local: (not bound)
2023-12-07 14:35:22 [Server] Peer Connection Initiated with [AF_INET]172.16.96.2:1194
2023-12-07 14:35:22 [Server] Peer Connection Initiated with [AF_INET]172.16.96.2:1194
2023-12-07 14:35:22 tilly/TAP device tun0 opened
2023-12-07 14:35:22 net_iface_mu_set: mtu 1500 for tun0
2023-12-07 14:35:22 net_iface_mu_set: tun0 up
2023-12-07 14:35:22 net_iface_mu_set: tun0 up
2023-12-07 14:35:22 net_iface_mu_set: tun0 up
2023-12-07 14:35:22 net_iface_mu_set: mtu 1500 for tun0
2023-12-07 14:35:22 net_iface_mu_set: tun0 up
2023-12-07 14:35:22 net_iface_mu_set: mtu 1500 for tun0
2023-12-07 14:35:20 mtu_set: mtu 1500 for
```

2 Zadania

Zadanie 2.1



Zadanie 2.2

Przchwycony ruch sieciowy podczas tej wymiany

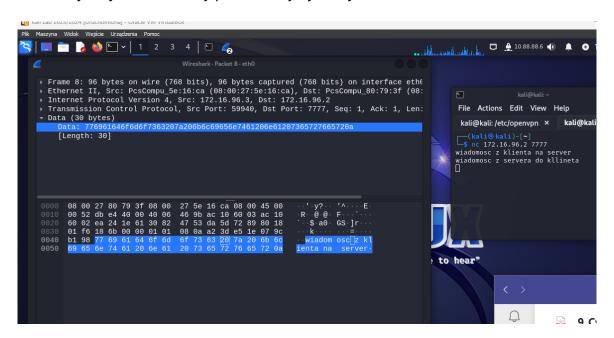


Figure 1: Przechwycona ramka z klienta na server.

Wiadomość przesłana z klienta na server została przechwycona. Widoczny jest adres IP źródła, adres IP celu oraz przede wszystkim treść wiadomości.

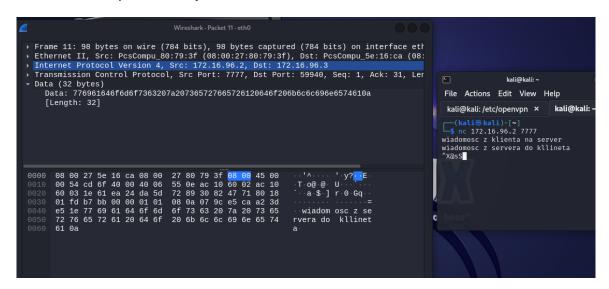
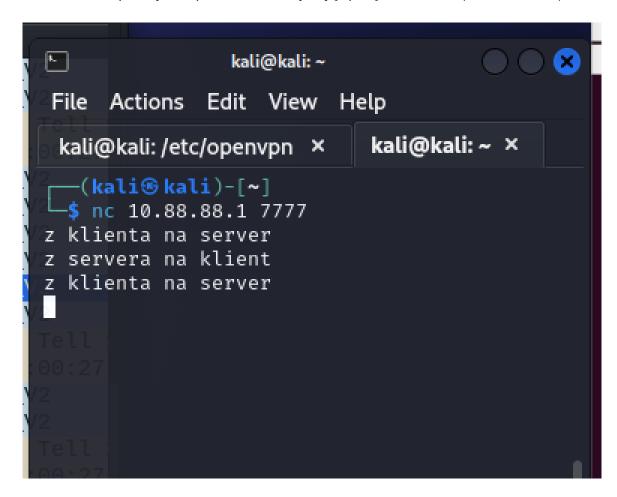


Figure 2: Przechwycona ramka z servera do klienta.

Wiadomość z servera do klienta również została przechwycona i ukazuje nam treść wiadomośći.

Zadanie 3.1

Wiadomości przesyłane przez netcat używając połączenia VPN (10.88.88.0/24)



Zadanie 3.2

Przchwycony ruch sieciowy podczas tej wymiany

```
Wireshark · Packet 40 · eth0
▶ Frame 40: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on inter
▶ Ethernet II, Src: PcsCompu_5e:16:ca (08:00:27:5e:16:ca), Dst: PcsCompu_80:79:3f
▶ Internet Protocol Version 4, Src: 172.16.96.3, Dst: 172.16.96.2
▶ User Datagram Protocol, Src Port: 53330, Dst Port: 1194
▶ OpenVPN Protocol
         08 00 27 80 79 3f 08 00
                                               27 5e 16 ca 08 00 45 00
                                                                                       9c 20 ac 10 60 03 ac 10
             7c 86 2a 40 00 40 11
         00
         60 02 d0 52 04 aa 00 68
                                               18 a0 48 00 00 00 <mark>00 00</mark>
              24 8c ab a9 08 34 da
                                               5d 3c fd 47 d3 ea 7d 8f
                                               2f cb cd bb 64 95 08 44
f6 d9 45 41 2c 5d ec b4
54 68 fc c1 f9 b0 f6 31
         bd 40 98 b0 4d 12 0b 93
28 4f 7a c3 40 3d 6d 02
11 d8 7d 3c 2d b4 30 7a
0040
                                                                                        (Oz⋅@=m⋅ ⋅⋅EA,]
0060
                                                                                        H<sup>*</sup>····· F··/·Z
                                               46 03 fa 2f ee 5a b0 a8
0070
0080
          a3 51 8f 94 3d 9d 69 9f
```

Figure 3: Ramka z klienta na server przy połączeniu VPN

Treść wiadomości nie jest czytelna z przechwyconej ramki.

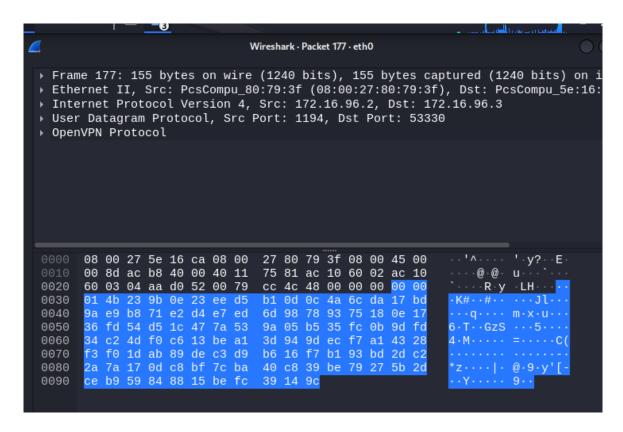


Figure 4: Ramka z servera do klienta przy połączeniu VPN

Ponownie treść wiadomości nie jest czytelna z przechwyconej ramki.

Pytanie 3.5

Czy można odczytać wiadomość wysłaną przez netcat?

Interfejs fizyczny

W przypadku użycia kanału komunikacji bez zabezpieczeń łatwe jest przechwycenie ramek, zawierających nadawcę, odbiorcę oraz treść wiadomości w niezaszyfrowanej postaci. Przechwycenie i odczytanie wiadomości nie było problematyczne. Przechwycone były ramki TCP, a ich zawartość łatwa do odczytania.

W przypadku korzystania z VPN, przechwytone zostały tylko ramki OpenVPN. Treść wiadomości była zaszyfrowana.

Interfejs VPN (tun0)

Podczas połączenia za pomocą netcat, na adres VPN (10.88.88.0/24), przechwycone były ramki TCP, podobnie jak dla komunikacji bez szyfrowania VPN. Można było odczytać treść ramek oraz nadawców i odbiorców (10.88.88.0/24).

Pytanie 3.6

Jaka jest charakterystyka przechwyconego ruchu na interfejsie sieci VPN i interfejsie hosta?

· Podczas połączenia VPN

W przypadku połączenia VPN, ruch na interfejsie VPN był minimalistyczny. Jedyne ramki

nadawane tym interfejsem to komunikaty TCP nadane przez netcat. Posiadały one prywatne adresy IP (z puli 10.88.88.0/24). Ich treść nie była szyfrowana wewnątrz kanału.

Ruch na interfejcie fizycznym (hosta) był dużo większy. Zamiast komunikatów TCP z treścią wiadomości netcat, nadawane były komunikaty OpenVPN, z zaszyfrowaną treścią wiadomości. Występował duży ruch protokołów takich jak ARP. Treść wiadomości nie była możliwa do odczytania.

Bez połączenia VPN

W przypadku braku połączenia VPN, ruch na interfejsie VPN(tun0), zgodnie z oczekiwaniami, nie występował wcale.

Jeśli chodzi o ruch na interfejsie fizycznym, to możliwe było przechwycenie wszystkich wiadomości netcat,

Pytanie 3.7

Jakie istotne informacje można zobaczyć analizując ruch w obu przypadkach?

Podczas połączenia VPN

Podczas połączenia VPN, na interfejsie VPN, przechwycić można było zarówno adresy nadawcy oraz odbiorcy (wewnątrz sieci VPN), jak i treść wiadomości. Interfejs fizyczny jednak wysyłał zaszyforwane ramki OpenVPN, które nie pozwalały na przechwycenie treści komunikatów.

Bez połączenia VPN

Jeśli chodzi o interfejs VPN, to oczywiście nie przepływały przez niego informacje. Interfejs fizyczny dawał możliwość przechwycenia wielu przydatnych infromacji, takich jak adres nadawcy, odbiorcy oraz treść wiadomości.