**Wrocław 01.10.2024**

**CYBERBEZPIECZEŃSTWO**

LabORATORIUM NR 9

**Ochrona** **komunikacji**

# Wstęp.

W tym ćwiczeniu będziemy zajmować się bezpieczną transmisję sieciową. Kwestie bezpieczeństwa omówione w laboratorium dotyczą komunikacji SSH, sieci VPN i wydajności ich algorytmów szyfrowania, uwierzytelniania TLS / SSL (OpenSSL) i konfiguracji zapory. W IT bezpieczna transmisja oznacza przesyłanie danych, takich jak informacje poufne lub zastrzeżone, za pośrednictwem bezpiecznego kanału. Wiele metod bezpiecznej transmisji wymaga użycia algorytmów szyfrowania.

Przypomnij sobie następujące pojęcia:

**Uwierzytelnianie** - to proces potwierdzania deklarowanej tożsamości podmiotu zaangażowanego w proces komunikacji. Celem uwierzytelnienia jest uzyskanie pewności, że dany podmiot jest tym, za którego się podaje.

**Autoryzacja** - celem autoryzacji jest kontrola dostępu, która potwierdza, że ​​podmiot jest uprawniony do korzystania z żądanego zasobu.

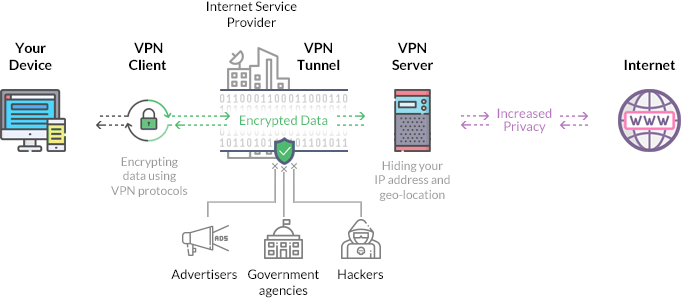
**Szyfrowanie** - to transformacja danych w taki sposób, że stają się one nierozpoznawalne bez znajomości konkretnego klucza. Pozwala to na ochronę danych podczas ich przesyłania w sieci.

**Integralność** - właściwość, która potwierdza, że ​​dane nie zostały naruszone lub zmienione w nieautoryzowany sposób. Jeśli osoba trzecia przechwytuje i modyfikuje Twoje dane, należy to zauważyć.

**Poufność** - to ochrona przed nieautoryzowanym dostępem, przy jednoczesnym zapewnieniu upoważnionym użytkownikom dostępu do zasobów bez przeszkód. Poufność zapewnia, że ​​dane nie są celowo lub nieumyślnie ujawniane nikomu bez ważnej potrzeby wiedzy.

**SSH, Secure Shell -**  to popularne, wydajne, programowe podejście do bezpieczeństwa sieci. Za każdym razem, gdy dane są wysyłane przez komputer do sieci, SSH automatycznie je szyfruje. Następnie, gdy dane dotrą do zamierzonego odbiorcy, SSH automatycznie je odszyfrowuje. Rezultatem jest przeźroczyste dla klienta szyfrowanie: użytkownicy mogą normalnie pracować, nie wiedząc, że ich komunikacja jest bezpiecznie szyfrowana w sieci. Poza tym protokół SSH wykorzystuje nowoczesne, bezpieczne algorytmy szyfrowania i jest na tyle skuteczny, że można go znaleźć w aplikacjach o znaczeniu krytycznym w dużych korporacjach.

**VPN** to skrót od „wirtualnej sieci prywatnej”. Krótka i bezpośrednia definicja jest taka, że ​​VPN jest mechanizmem do ustanowienia bezpiecznego połączenia zdalnego dostępu w sieci pośredniej, często w Internecie. Sieci VPN umożliwiają zdalny dostęp, zdalne sterowanie i wysoce bezpieczną komunikację w sieci prywatnej. Sieci VPN wykorzystują szyfrowanie i uwierzytelnianie w celu zapewnienia poufności, integralności i ochrony prywatności w komunikacji sieciowej. Przykładowy schemat sieci VPN:



Rysunek VPN – <https://www.rossco.org/SecureOffice_Images/how-does-a-vpn-work-diagram.png>

Na rynku dostępnych jest wiele produktów VPN, zarówno komercyjnych, jak i open source. Prawie wszystkie VPN można podzielić na następujące cztery kategorie:

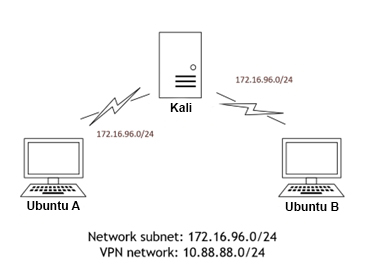
* VPN definiowany przy użyciu protokołu PPTP,
* VPN definiowany przy użyciu protokołu IPSec,
* VPN definiowany przy użyciu protokołu SSL,
* OpenVPN,

W naszym laboratorium używany jest OpenVPN. OpenVPN jest często nazywany siecią VPN opartą na SSL, ponieważ wykorzystuje protokół SSL / TLS do zabezpieczenia połączenia. Jednak OpenVPN wykorzystuje również HMAC w połączeniu z algorytmem skrótu (lub haszowania) w celu zapewnienia integralności dostarczanych pakietów. Można go skonfigurować tak, aby używał kluczy wstępnych, a także certyfikatów X.509. Te funkcje nie są zazwyczaj oferowane przez inne sieci VPN oparte na SSL.

SSL/TLS to protokół zapewniający poufność i integralność transmisji danych, a także uwierzytelnianie serwera, a czasem klienta. Opiera się na szyfrowaniu asymetrycznym i certyfikatach X.509. SSL jest używany przez przeglądarki internetowe i serwery do przesyłania poufnych informacji. SSL jest częścią ogólnego protokołu znanego jako Transport Layer Security (TLS). SSL i jego następca TLS korzystają z urzędów certyfikacji. Gdy przeglądarka żąda bezpiecznej strony internetowej, „s” jest dodawany do HTTP w adresie URL przeglądarki, która wysyła klucz publiczny i certyfikat, sprawdzając, czy certyfikat pochodzi od zaufanej strony komunikacji, która jest aktualnie ważna i ma związek z witryną, z której pochodzi. Najbardziej znanym zastosowaniem TLS jest zabezpieczenie transakcji online. TLS może być również używany do celów bezpieczeństwa na serwerach, takich jak poczta, baza danych lub katalog. Wirtualna sieć prywatna wykorzystuje protokół TLS do szyfrowania połączenia między urządzeniem użytkownika a siecią, do której uzyskuje się dostęp.

# Konfiguracja środowiska.

Aby skonfigurować środowisko, musisz pobrać trzy obrazy maszyn wirtualnych. Wszystkie niezbędne pliki można znaleźć na portalu w załącznikach do tego laboratorium. Dwie maszyny wirtualne (VM) są skonfigurowane jako klienci. Trzeci to serwer VPN i firewall. W pakiecie znajduje się również zestaw certyfikatów i plików konfiguracyjnych dla sieci VPN. Topologia sieci jest skonfigurowana w następujący sposób:



Rysunek 2 Topologia sieci VPN

1. Uruchom Virtualbox i zaimportuj obrazy maszyn wirtualnych.

2. Zaloguj się do Ubuntu (login:student, hasło: student).

3. Zaloguj się do Kali (login: stud, pass: stud).

**Konfiguracja serwera (Kali):**

1. Sprawdź, czy plik konfiguracyjny istnieje w */etc/openvpn/server* i wyświetl zawartość server.conf.
2. W */etc/openvpn/server* powinny znajdować się następujące pliki:

* server.crt - certyfikat serwera,
* server.key - klucz serwera,
* ta.key - podpis HMAC - uwierzytelnianie TLS,
* ca.crt - certyfikat CA,

1. Aby uruchomić serwer VPN, uruchom:

**sudo systemctl start openvpn-server@server.service**

Aby sprawdzić status usługi VPN, uruchom:

**sudo systemctl status openvpn-server @ server.service**

**Konfiguracja klienta (Ubuntu):**

1. Sprawdź, czy plik konfiguracyjny istnieje w */home/student/Desktop/VPN/client*/ i zweryfikuj zawartość client.ovpn.
2. W */home/student/Desktop/VPN/client*/ powinny znajdować się następujące pliki:

* client1.key - klucz klienta,
* client1.crt - certyfikat klienta,
* ta.key - podpis HMAC - uwierzytelnianie TLS
* client.ovpn - plik konfiguracyjny,
* ca.crt - certyfikat CA

Pozostałe certyfikaty i klucze znajdują się w katalogu w katalogu “~/VPN/client others”.

1. Dostosuj plik client.ovpn.

* Sprawdź adres IP (Rysunek 3) serwera. W tym celu uruchom polecenie ifconfig na serwerze i sprawdź adres IP interfejsu sieciowego, adres powinien pochodzić z podsieci NAT określonej w VirtualBox. W proponowanym przykładzie z 172.16.96.0/24.
* Skopiuj adres IP serwera i wklej go w pliku client.ovpn– wiersz:

**remote X.X.X.X 1194**

zamiast X.X.X.X.

Uwaga: aby edytować plik użyj edytora nano, w tym celu niezbędne są uprawnienia root’a, np .:

**sudo nano /home/student/Desktop/VPN/client/client.ovpn**

Aby zapisać plik, naciśnij Crtl + X, wpisz „Tak” i naciśnij Enter.

A computer screen with white text

Description automatically generated

Rysunek Sprawdzenie adresu IP

1. Pamiętaj o zmianie nazwy certyfikatu klienta i klucza w pliku client.ovpn dla dwóch instancji klienta Ubuntu A oraz Ubuntu B.
2. Aby rozpocząć połączenie VPN, wpisz:

**cd /home/student/Desktop/VPN/client**

**sudo openvpn --config /home/student/Desktop/VPN/client/client.ovpn**

# TLS

Punkt ma na celu analizę komunikacji TLS 1.2 / TLS 1.3. Zapoznaj się z TLS / SSL w wersjach 1.2 i 1.3, znajdź zalety i wady każdej wersji.

## Zadanie:

### Przechwytywanie ruchu sieciowego na fizycznym interfejsie sieciowym (zwykle nazwa zaczyna się od en…),

### Filtruj tylko rekordy dla komunikacji TLS / SSL. Wyrażenie filtru dla TLS / SSL w Wireshark: ssl.record.version == 0x0303,

### Szczegółowo przestudiuj rekordy TLS / SSL.

## Pytania:

### Czy TLS i SSL to ten sam protokół?

### Co to jest TLS/SSL handshake?

### Co zapewnia protokół TLS/SSL, podaj przykłady jego zastosowań (przynajmniej 2)?

### Które wersje protokołu są obecnie najpopularniejsze?

### Która wersja zapewnia większe bezpieczeństwo i dlaczego?

### Która wersja zapewnia wyższą wydajność?

Na podstawie przechwyconego ruchu przeanalizuj zarejestrowany ruch TLS / SSL.

### Która wersja protokołu została przechwycona?

### Z jakiego rodzaju wiadomości składa się uzgadnianie (nawiązanie połączenia)?

### Od czego zależy wersja używanego protokołu?

Zrób zrzut ekranu pokazujący, jaki typ szyfrowania został użyty do szyfrowania i umieść go w raporcie.

# OpenVPN.

Netcat to narzędzie służące do przesyłania danych między klientami, poniżej przykładowa konfiguracja:

* Przesyłanie wiadomości tekstowej
  + **Kali A**:
    - uruchom*:* ***nc -l -p 7777***,
  + **Kali B**:
    - uruchom*:* ***nc X.X.X.X 7777*** (X.X.X.X – to adres IP klienta A, 7777 to port używany do komunikacji Netcat),
    - wpisz tekst w terminalu,
* **Przesyłanie pliku**,
  + **Kali A**:
    - ***nc -l -p 7777 > file\_name***
  + **Kali B**:
    - ***cat ./file\_name | nc X.X.X.X 7777***

Wireshark służy do przechwytywania ruchu na interfejsach sieciowych.

## Zadania:

### Przechwytywanie ruchu sieciowego na interfejsie sieciowym VPN (zwykle nazwa to tun0, sprawdź za pomocą polecenia ifconfig).

### Wyślij kilka wiadomości za pomocą netcata między klientami A i B.

### Obserwuj i analizuj proces komunikacji w Wireshark.

### Znajdź i zweryfikuj dane przesłane przez netcata w Wireshark. Czy można odczytać wiadomość wysłaną przez netcata? Zrób zrzut ekranu danych zawartych w pakietach.

## Zadania:

### Przechwytywanie ruchu sieciowego na fizycznym interfejsie sieciowym (zwykle nazwa zaczyna się od en…)

### Wysłać kilka wiadomości za pomocą netcata między klientami A i B.

### Obserwuj i analizuj proces komunikacji w Wireshark.

### Znajdź i zweryfikuj dane przesłane przez netcata w Wireshark. Zrób zrzut ekranu danych zawartych w pakietach.

**Pytania do zadania 2 i 3**:

### Czy można odczytać wiadomość wysłaną przez netcat?

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

### Jakie istotne informacje można zobaczyć analizując ruch w obu przypadkach?

## Zadania:

### Przechwytywanie ruchu sieciowego na fizycznym interfejsie sieciowym (zwykle nazwa zaczyna się od en…),

### Prześlij plik z wykorzystaniem narzędzia netcat. Plik zlokalizowany jest na pulpicie w katalogu FILE ( ścieżka do pliku /home/kali/Desktop/FILES/ubuntu.iso ~900MB)

### Prześlij plik 4 razy, za każdym razem zmień algorytm szyfrowania i uwierzytelniania. Edytuj pliki **client.ovpn** na systemie clientA oraz clientB i zmień następujące parametry:

1. Setting 1
   1. cipher AES-256-GCM,
   2. auth SHA512,
2. Setting 2
   1. Cipher AES-128-CBC,
   2. Auth SHA1,
3. Setting 3
   1. Cipher DES-EDE-CBC,
   2. Auth MD5,
4. Setting 4
   1. Cipher DES-CBC,
   2. Auth MD5,

* Obserwuj i analizuj proces komunikacji w Wireshark.
* Zmierz czas transferu danych.

## Pytania:

### Czy istnieje różnica w czasach przesyłania danych? Co może na nich wpłynąć?

### Co możemy powiedzieć o zastosowanych algorytmach szyfrowania i uwierzytelniania?

### Który zestaw ustawień jest najgorszy, a który najlepszy pod względem bezpieczeństwa?