Co-funded by the Erasmus+ Programme of the European Union

Moduł treningowy InCyT

Bezpieczeństwo informacji dla pracowników **Dział 3, Tydzień 5** **Moduł: Bezpieczeństwo podczas podróży służbowych**	
Zajęcia edukacyjne	❑ **Webinar** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑ **Prezentacja** ❑ **Inne**
Odpowiedzialni za zajęcia	• Mirosław Mazurek • Paweł Dymora
Cele aktywności edukacyjnej	1. Sieci bezprzewodowe 2. VPN 3. Szyfrowanie poczty email
Umiejętności do zdobycia	• **TS3** • **SS2**
Czas trwania okresu edukacyjnego	2 tygodnie
Wymagania wstępne	***Co jest potrzebne?***
	• Dostęp do Internetu • Przeglądarka Internetowa • MS Office365

Co-funded by the Erasmus+ Programme of the European Union

Krótka informacja o module

Opis
Ogólny zarys tego modułu to przedstawienie pewnych teoretycznych i praktycznych zagadnień związanych z bezpieczeństwem wiedzy i praktycznych umiejętności podczas wyjazdów służbowych. Będzie można zabezpieczyć sieć bezprzewodową oraz korzystać z zabezpieczonych sieci bezprzewodowych z uwzględnieniem idei VPN. Moduł obejmie również sposób bezpiecznego wysyłania wiadomości e-mail z wykorzystaniem darmowego protokołu PGP do szyfrowania wiadomości, których nikt nie może odszyfrować bez Twojej zgody.

Treść materiałów dydaktycznych

1. Wprowadzenie do sieci bezprzewodowych. Podstawy teoretyczne: zasada działania, protokoły szyfrujące.

Wcześniej do zabezpieczania sieci bezprzewodowych stosowano protokoły WEP i WPA, ale nie były one odporne na ataki hakerów. Wprowadzenie protokołu WPA2 pozwoliło zapewnić wystarczający poziom bezpieczeństwa, ale i tak nie zapewnia on pełnego bezpieczeństwa. Dostępnych jest wiele topologii sieci, protokołów dostępu bezprzewodowego oraz technik akwizycji dostępu do sieci, a do akwizycji kluczy sieciowych wykorzystuje się zarówno architektury obliczeniowe CPU (Central Processing Unit) jak i GPU (Graphics Processing Unit) [1,2].

WEP (Wired Equivalent Privacy) jest jednym z najstarszych standardów szyfrowania sieci bezprzewodowych IEEE 802.11. Zapewnia on ochronę informacji w oparciu o wykorzystanie algorytmu RC4. Ma wiele znanych luk w zabezpieczeniach i dlatego był wielokrotnie łamany. Jest jednym z najstarszych standardów zabezpieczania sieci WLAN (powstał w 1997 roku). Nie wymaga dużej mocy obliczeniowej zainstalowanych urządzeń. Wykorzystuje dwie metody uwierzytelniania użytkowników: Open Authentication oraz Shared Key Authentication. Dodatkowo umożliwia weryfikację użytkowników na podstawie fizycznych adresów MAC z wykorzystaniem listy ACL (Access Control List). Istnieje 64-bitowy wariant WEP (oparty na 40-bitowym kluczu i 24-bitowym wektorze inicjalizacyjnym) oraz 128-bitowy wariant WEP (oparty na 104-bitowym kluczu). Niektórzy producenci wprowadzili również 256-bitowy standard WEP [1,2].

WPA (Wi-Fi Protected Access) to kolejny standard szyfrowania sieci bezprzewodowych IEEE 802.11. Został wprowadzony w celu podniesienia poziomu bezpieczeństwa sieci WLAN, zastępując znane luki w standardzie WEP. Opiera się na wykorzystaniu protokołów: TKIP (Temporal Key

Integrity Protocol) i EAP (Extensible Authentication Protocol), standardu 802.1x oraz mechanizmu MIC (Message Integrity Check). Standard ten oparty jest na algorytmie RC4. Został wprowadzony jako rozwiązanie przejściowe pomiędzy standardem WEP a obecnym najbezpieczniejszym standardem szyfrowania sieci bezprzewodowych 802.11i. Zapewnia on pracę w dwóch trybach, do których należą: Enterprise (wykorzystujący serwer RADIUS zarządzający przydzielaniem kluczy użytkownikom) oraz Personal (wykorzystujący współdzielony klucz PSK) [1,2].

WPA2 (Wi-Fi Protected Access 2) to aktualnie najmocniej rozbudowany standard szyfrowania dla sieci bezprzewodowych (znanych także jako 802.11i). Zapewnia on ochronę informacji w oparciu o wykorzystanie standardu AES (Advanced Encryption Standard). Został wprowadzony w celu zwiększenia poziomu bezpieczeństwa sieci WLAN, zastępując znane luki w standardzie WEP i przejściowym standardzie WPA. Implementuje protokół 802.1x usprawniający kontrolę dostępu użytkowników do sieci. Zapewnia pracę w dwóch trybach, do których należą: Enterprise (wykorzystujący serwer RADIUS zarządzający przydzielaniem kluczy użytkownikom) oraz Personal (wykorzystujący współdzielony klucz PSK) - często stosowany obecnie w rozwiązaniach domowych [1,2].

Algorytm WEP jest najmniej bezpiecznym standardem szyfrowania dla sieci bezprzewodowych IEEE 802.11. Był on wielokrotnie łamany różnymi metodami ze względu na wiele znanych obecnie luk w zabezpieczeniach algorytmu. Do głównych wad standardu należą[3]:

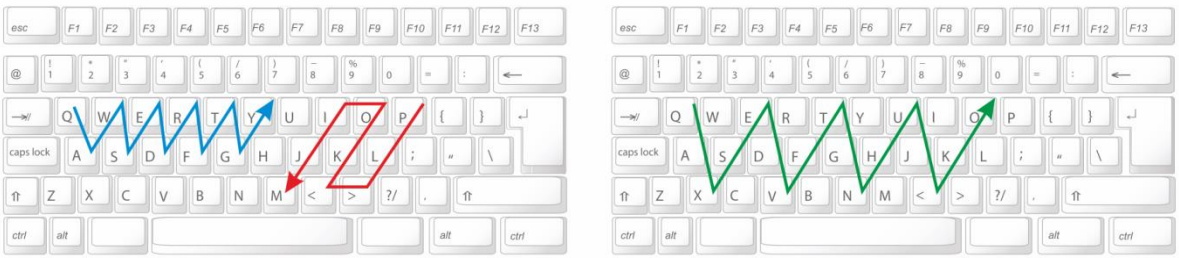
- Brak zdefiniowanego systemu zarządzania kluczami (często jeden klucz sieciowy jest używany przez wszystkie węzły sieci bezprzewodowej);
- Niewystarczający rozmiar bitowy klucza sieciowego (pierwsza wersja standardu WEP wprowadza klucze 40-bitowe);
- Niewystarczający rozmiar bitowy wektora inicjalizacyjnego IV (standard WEP wprowadza 24-bitowy wektor inicjalizacyjny, który okazuje się niewystarczający i ze względu na stosunkowo duże prawdopodobieństwo kolizji przy niewielkiej liczbie odebranych pakietów istnieje możliwość ataku kryptograficznego w celu uzyskania wartości klucza WEP);
- Słaba suma kontrolna ICV oparta na funkcji liniowej CRC-32 (istnieje możliwość niezauważalnej modyfikacji informacji przesyłanej w sieci);
- Słaby algorytm szyfrowania informacji RC4 (istnieje zbyt wiele zależności pomiędzy kluczem sieciowym a wynikiem szyfrowania informacji);
- Niewystarczający system uwierzytelniania użytkowników (istnieje możliwość fałszowania komunikatów uwierzytelniających).
- Na podstawie przedstawionych słabości algorytmu WEP powstało wiele narzędzi do przeprowadzania ataków testujących poziom bezpieczeństwa sieci WLAN. Do najpopularniejszych ataków na WEP należą:
- Atak FMS - atak statystyczny (opracowany przez Fluhrera, Mantina i Shamira) na algorytm RC4 stosowany w standardzie szyfrowania WEP;
- Atak KoreK - atak statystyczny (opracowany przez osobę o pseudonimie KoreK) wykorzystujący kilka kolejnych (w porównaniu do ataku FMS) zależności procesu szyfrowania algorytmu RC4;

- Atak Chopchop - atak interaktywny, przeprowadzany w kierunku uzyskania dostępu do sieci poprzez stopniowe odszyfrowywanie jednego z odebranych pakietów;
- Atak PTW - to atak statystyczny (opracowany przez Pyshkina, Tewsa i Weinmanna) na algorytm RC4, który dzięki kolejnym zależnościom procesu szyfrowania danych znacznie zwiększa prawdopodobieństwo uzyskania wartości klucza przy stosunkowo niewielkiej liczbie odebranych pakietów.

Innym często stosowanym rodzajem ataku jest atak słownikowy. Jest to jedna z metod brute-force pozyskiwania np. wartości kluczy kryptograficznych w bezprzewodowych sieciach komputerowych. W celu uzyskania wartości kluczy WPA/WPA2 metoda ta opiera się na jednokierunkowym szyfrowaniu i porównywaniu haseł w słowniku z informacjami zawartymi w przechwyconej 4-way handshake sequence. Ataki słownikowe przeprowadzane są z zamiarem skrócenia czasu uzyskania wartości klucza w porównaniu z metodą brute-force. Proces pobierania wartości klucza trwa do momentu uzyskania pozytywnego wyniku (tj. gdy wpis w słowniku okaże się poprawną wartością klucza) lub do momentu porównania wszystkich wpisów w słowniku z wynikiem negatywnym. Wynik negatywny może wskazywać na wysoki stopień skomplikowania wartości klucza i konieczność zastosowania metody brute-force[3].

Warunkiem powodzenia tego ataku jest dobór odpowiedniego słownika. Słownik to plik tekstowy wykorzystywany w przypadku ataków słownikowych w celu uzyskania np. wartości klucza kryptograficznego. Zawiera on listę odpowiednio przygotowanych elementów, które mogą stanowić poszukiwaną wartość klucza. Zastosowanie słowników w przypadku ataków siłowych pozwala na znaczne ograniczenie zbioru badanych wartości, co może skutkować przyspieszeniem procesu pozyskania wartości klucza kryptograficznego. Zawartość słowników budowana jest np. na podstawie przedstawionych pozycji[3]:

- lista słów występujących w słownikach krajowych i zagranicznych;
- połączenia wyrazów z dużymi i małymi literami, wyrazy pisane wspak (czyli palindromy);
- kombinacje haseł słownikowych z wyciętymi samogłoskami lub spółgłoskami;
- kombinacje wielokrotnych powtórzeń wybranych imion, nazwisk, haseł słownikowych;
- kombinacje słów z wartościami liczbowymi, znakami specjalnymi itp;
- lista haseł i loginów najczęściej używanych przez użytkowników;
- lista popularnych firm, organizacji, terminów technicznych, nazw własnych itp;
- wycieki informacji (tj. loginy, pseudonimy, hasła) z różnych portali internetowych;
- kombinacje sąsiadujących ze sobą znaków klawiatury dla wybranych wzorców (rys. 1).



Rys. 1. Schemat przedstawiający przykłady wzorców tworzenia kluczy sieciowych

Klucz sieciowy odgrywa kluczową rolę w badaniu odporności sieci. Jest to ciąg znaków wykorzystywany przez użytkowników sieci w procesie uwierzytelniania. Proces uwierzytelniania jest ważnym krokiem w ochronie dostępu do usług wspólnych i zasobów sieciowych przed nieuprawnionymi użytkownikami. Klucze sieciowe są często tworzone i zarządzane przez administratorów sieci i mogą stanowić najsłabsze ogniwo bezpieczeństwa sieci komputerowej. Wartości kluczy, które okazują się stosunkowo czasochłonne lub niemożliwe do złamania metodami brute-force w realistycznym czasie, powinny być generowane na przykład w oparciu o przedstawione reguły [3]:

- Każda sieć bezprzewodowa zarządzana przez administratora powinna być zabezpieczona przy użyciu innego klucza sieciowego;
- Każdy użytkownik sieci powinien korzystać z indywidualnego klucza sieciowego;
- Klucze sieciowe powinny być budowane w oparciu o odpowiednią liczbę znaków;
- Generowanie kluczy powinno opierać się na maksymalnej dostępnej przestrzeni znaków;
- Klucze nie powinny być generowane z wykorzystaniem informacji korporacyjnych i osobistych;
- Generowanie kluczy nie powinno opierać się na liście pozycji w publicznie dostępnych słownikach;
- Klucze sieciowe powinny być budowane na podstawie losowych ciągów znaków;
- Klucze sieciowe powinny być okresowo aktualizowane;
- Obecnie używane wartości kluczy nie powinny być kojarzone z wartościami kluczy, które nie są już używane.

2. VPN – wirtualne sieci prywatne. Podstawy teoretyczne: rodzaje, architektura, zasada działania, protokoły szyfrujące. Instalacja programu Open VPN (konfiguracja, adresowanie, dobór parametrów, generowanie kluczy).

Wirtualna sieć prywatna to tunel, przez który prywatny ruch sieciowy przepływa między nadawcą a odbiorcą przez sieć publiczną. Skrót VPN oznacza "Virtual Private Network" (wirtualna sieć prywatna). Sieć VPN szyfruje wszystkie działania w Internecie, ukrywa adres IP, chroniąc tożsamość użytkownika sieci. Połączenie VPN oferuje bezpieczny dostęp do aplikacji, stron internetowych i platform rozrywkowych z dowolnego miejsca na świecie. Istnieje możliwość opcjonalnej kompresji lub szyfrowania przesyłanych danych w celu zapewnienia lepszej jakości lub wyższego poziomu bezpieczeństwa, chroniąc tym samym prywatność w sieci [4].

Bezpieczny tunel jest tworzony przez pierwsze uwierzytelnienie klienta z serwerem VPN. Następnie serwer stosuje protokół szyfrowania do wszystkich danych, które są wysyłane i odbierane. Aby zapewnić bezpieczeństwo każdego pakietu danych, VPN umieszcza go w zewnętrznym pakiecie, który następnie jest szyfrowany przez enkapsulację. Zapewnia ona

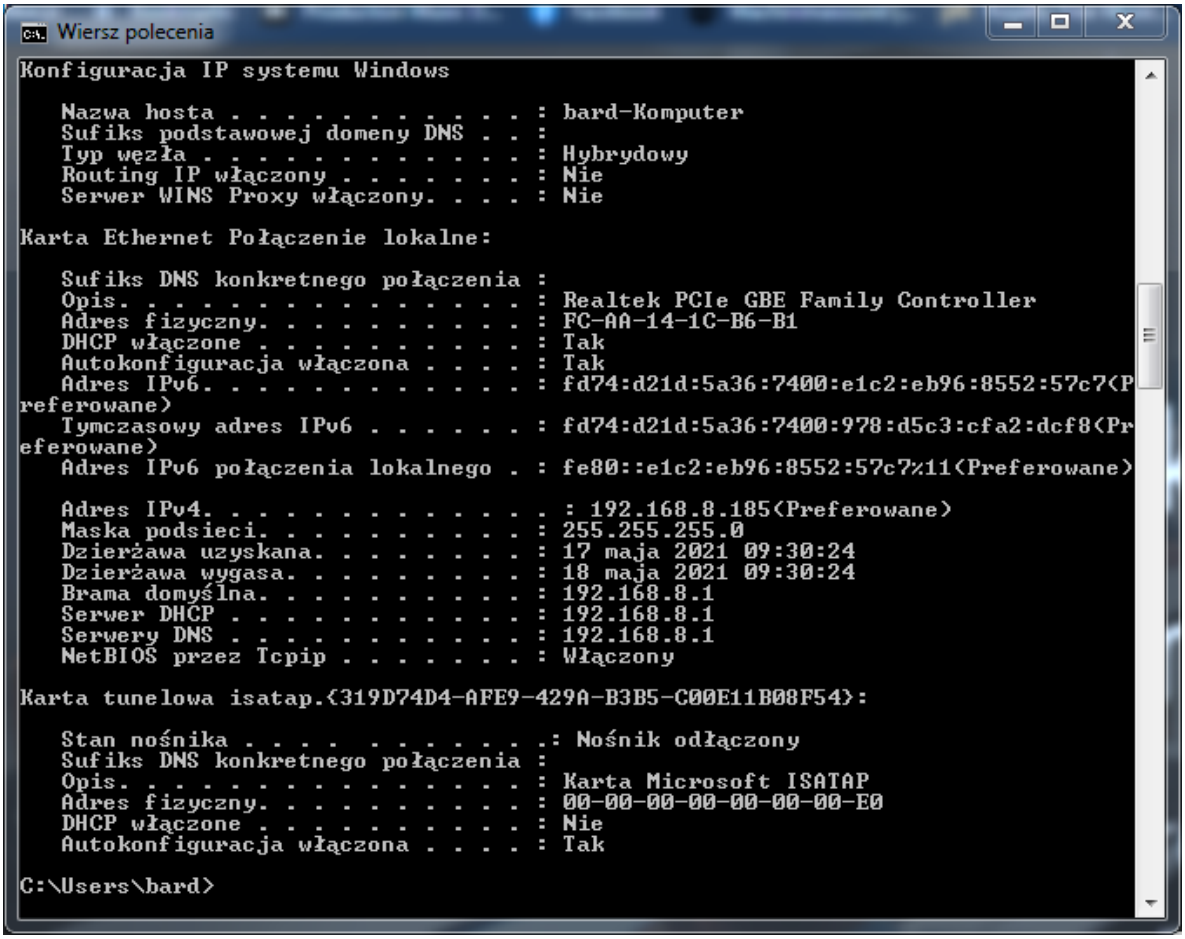
bezpieczeństwo danych podczas transmisji i jest podstawowym elementem tunelu VPN. Po dotarciu danych do serwera, pakiety zewnętrzne są usuwane w procesie deszyfrowania [4].

Sieci VPN można podzielić na dwie główne kategorie [5]:

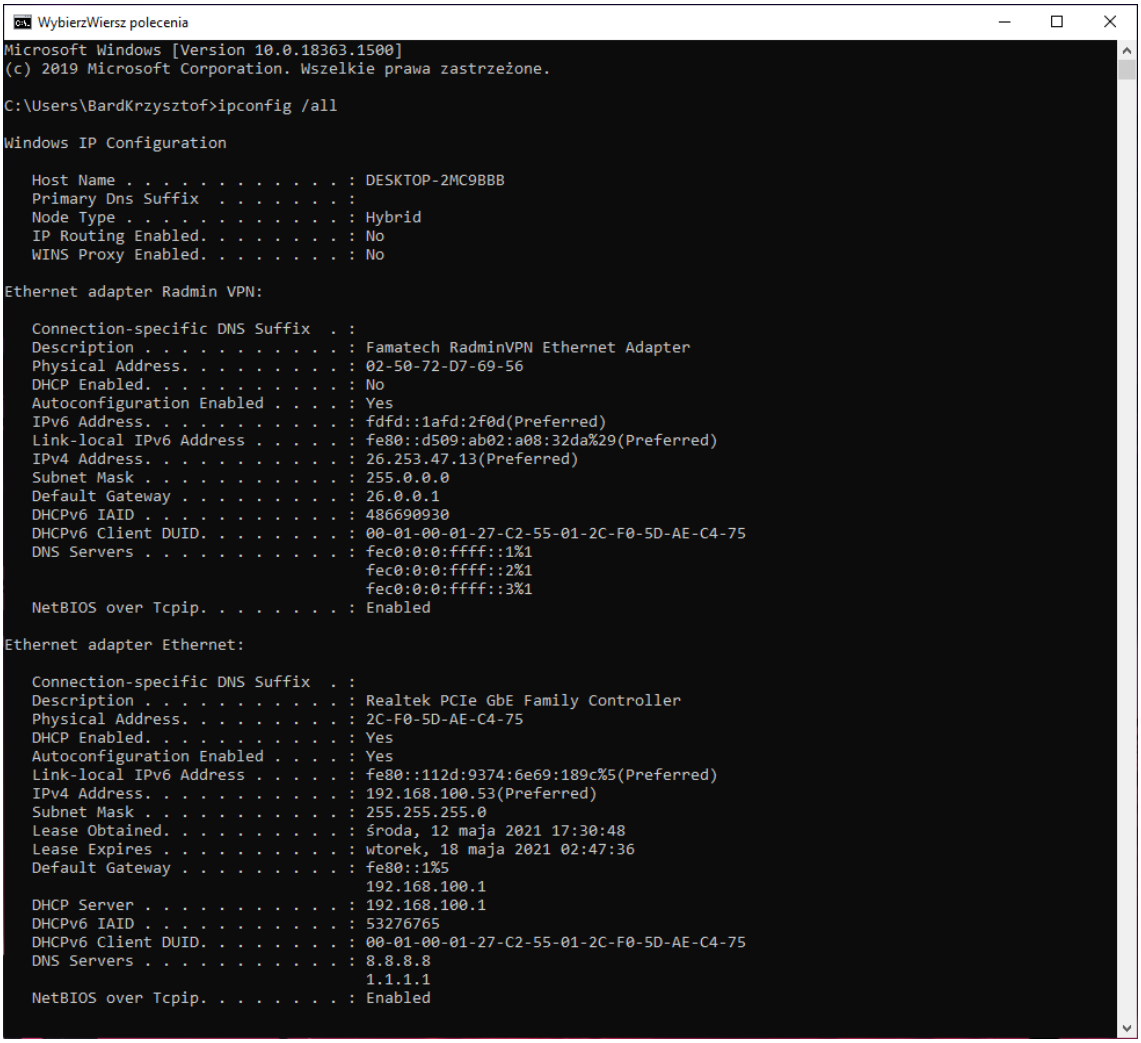
- VPN zdalnego dostępu, który pozwala użytkownikom łączyć się ze zdalną siecią, zwykle za pomocą specjalnego oprogramowania.
- Site-to-site Sieci VPN wykorzystywane przez firmy, zwłaszcza duże korporacje. Pozwalają użytkownikom w wybranych lokalizacjach na bezpieczny dostęp do sieci innych użytkowników.

Przykładem dedykowanego oprogramowania do tworzenia VPN jest **RadminVPN**. W większości przypadków do zestawienia tunelu VPN nie jest konieczne posiadanie statycznego adresu IP w sieci lokalnej. Po pobraniu odpowiedniego oprogramowania stworzy ono odpowiednią sieć ze statycznym adresem komputera [6].

Radmin VPN pozwala na połączenie się z dwoma komputerami w dwóch różnych sieciach. Przykładowa konfiguracja została przedstawiona poniżej. Dla łatwiejszego zrozumienia działania kanału VPN na rys. 2 i 3 przedstawiono wstępną konfigurację komputerów, pomiędzy którymi ma zostać utworzony bezpieczny kanał.



Rys. 2. Wstępna konfiguracja komputerów.

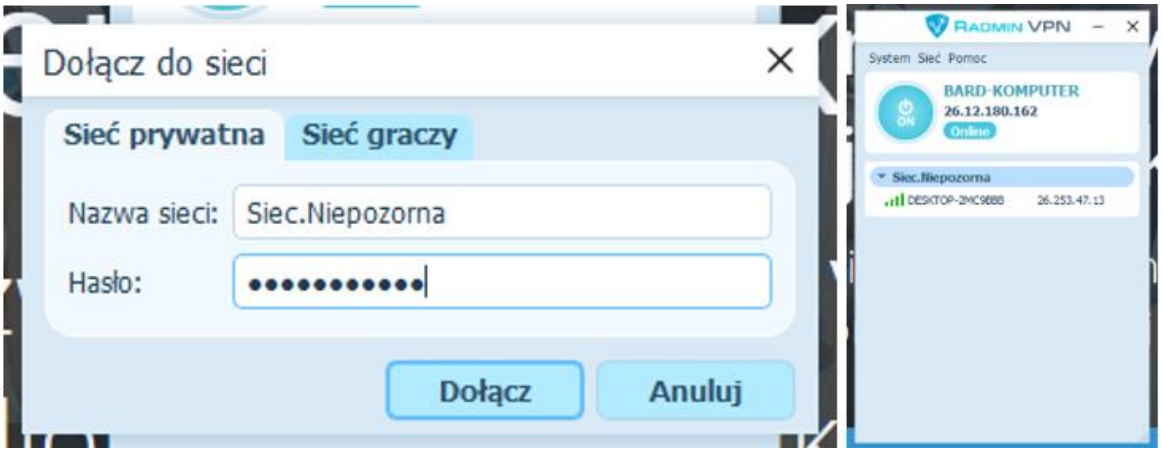


Rys. 3. Wstępna konfiguracja komputerów

Jak widać, adresy bram są zupełnie inne, więc komputery nie mają fizycznego ani logicznego połączenia ze sobą. Aby utworzyć kanał, zainstaluj RadminVPN na obu komputerach. Na jednym z nich musisz zacząć od utworzenia własnej sieci.

Rys. 4. Widok ekranu głównego aplikacji (lewy obraz - konfiguracja komputera 1, prawy obraz - komputer 2).

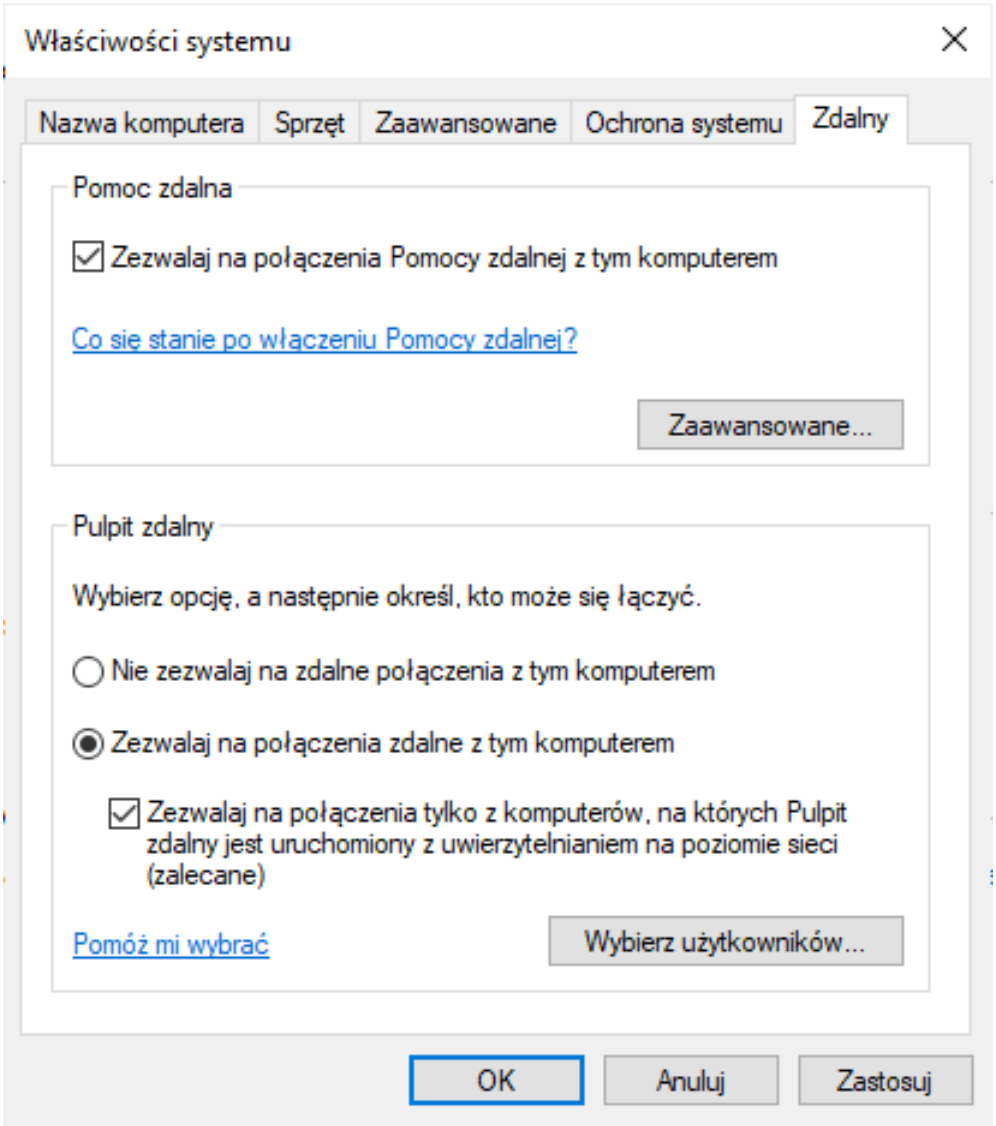
W celu utworzenia sieci należy w oknie aplikacji wybrać opcję **Utwórz sieć**, podać nazwę i hasło sieci oraz zatwierdzić przyciskiem Utwórz. Na drugim komputerze tak utworzoną sieć należy dodać, klikając przycisk Dołącz do sieci, podając nazwę i hasło właśnie utworzonej sieci.



Rys. 5. a) widok okna połączenia sieciowego; b) stan połączenia.

Po pomyślnym połączeniu się z siecią oba komputery powinny znaleźć się w widoku połączenia sieciowego (jak na rysunku 5b). W tym przypadku widać nazwę i adres komputera po drugiej stronie tunelu. Tak samo będzie na drugim komputerze. Próba połączenia na tym etapie nie powiedzie się,

ponieważ do działania systemu wymagany jest Radmin Server. W aplikacji pojawi się informacja o instalacji, którą należy wykonać na obu komputerach i ponownie uruchomić. Po zakończeniu całego procesu instalacji komputery będą mogły się komunikować, ale nie będzie możliwe przejęcie kontroli przez jeden nad drugim. Aby móc się wzajemnie kontrolować należy skonfigurować systemowy pulpit zdalny w systemie Windows (Panel sterowania->System i po prawej stronie wybrać Zaawansowane ustawienia systemu).



Rys. 6. Ustawienia sekcji Remote Desktop.

Pojawi się okno Właściwości systemu. Następnie wybierz zakładkę Remote i sekcję Remote Desktop zaznaczając Allow remote connections to this computer (Rys. 6). Po zatwierdzeniu zmian na obu komputerach należy utworzyć użytkownika o danych prawach dostępu. W tym celu należy uruchomić RadminServer i z pól po prawej stronie wybrać Uprawnienia, a następnie opcję

Permissions. W oknie uprawnień należy zaznaczyć opcję Pełny dostęp i utworzyć użytkownika (należy nadać mu nazwę i hasło). W ten sposób kończy się proces konfiguracji kanału VPN. Utworzony tunel jest dwukierunkowy i można go łatwo wykorzystać do kontrolowania komputerów z obu stron.

3. Szyfrowanie poczty elektronicznej. Podstawy teoretyczne: rodzaje szyfrowania (symetryczne i asymetryczne), bezpieczeństwo, protokoły, klucze. Instalacja i konfiguracja programu OpenPGP. Instalacja i konfiguracja klienta poczty elektronicznej.

Jednym z najczęściej używanych kanałów komunikacji jest poczta elektroniczna (e-mail), która coraz częściej staje się celem ataków hakerskich. Ochrona tego elementu jest ważną częścią pakietu rozwiązań cyberbezpieczeństwa. Ochrona poczty elektronicznej i szyfrowanie załączników to dwie bardzo ważne kwestie związane z bezpieczeństwem online. Szyfrowanie poczty elektronicznej nie tylko minimalizuje ryzyko wycieku poufnych danych, ale zapobiega ich nieautoryzowanemu przechwyceniu. Poczta elektroniczna i jej załączniki nie są domyślnie zabezpieczone protokołami SSL i TLS, a wszystkie wiadomości są wysyłane jako zwykły tekst [8].

Algorytmy szyfrowania, podobnie jak kryptografia, dzielą się na dwie kategorie:

- algorytmy szyfrowania symetrycznego;
- algorytmy szyfrowania asymetrycznego;

Główną różnicą między tymi dwoma metodami szyfrowania jest liczba używanych kluczy. Szyfrowanie symetryczne wykorzystuje jeden klucz, natomiast szyfrowanie asymetryczne wykorzystuje dwa różne, ale powiązane ze sobą klucze. Jeden z kluczy to klucz prywatny, a drugi to klucz publiczny. Algorytmy szyfrowania symetrycznego wykorzystują ten sam klucz do realizacji funkcji szyfrowania i deszyfrowania. Asymetryczny algorytm szyfrowania wykorzystuje jeden klucz do szyfrowania danych, a drugi do ich odszyfrowania. Oznacza to, że jeśli chcemy wysłać komuś zaszyfrowaną wiadomość, szyfrujemy ją kluczem publicznym odbiorcy, a odbiorca używa swojego klucza prywatnego do jej odszyfrowania.

Kolejnym kryterium podziału szyfrowania jest kryterium długości klucza. Długość klucza jest bezpośrednio związana z poziomem bezpieczeństwa zapewnianym przez każdy z algorytmów kryptograficznych. Im dłuższy klucz, tym bezpieczniejsze dane. W algorytmach symetrycznych klucze są wybierane losowo, a ich długość wynosi zazwyczaj 128 lub 256 bitów, w zależności od wymaganego poziomu bezpieczeństwa. W przypadku szyfrowania asymetrycznego, aby nastąpiło szyfrowanie i deszyfrowanie, musi istnieć matematyczna zależność pomiędzy kluczem publicznym i prywatnym (w postaci jakiegoś unikalnego wzoru matematycznego).

Ze względu na większą szybkość, szyfrowanie symetryczne jest szeroko stosowane do ochrony informacji w wielu współczesnych systemach komputerowych, np. Advanced Encryption Standard (AES) używany przez rząd USA do szyfrowania poufnych i tajnych informacji. AES zastąpił

wcześniejszy standard szyfrowania danych (DES).

Szyfrowanie asymetryczne jest stosowane w systemach, w których wielu użytkowników może wymagać dostępu zarówno do szyfrowania, jak i deszyfrowania wiadomości lub zestawu danych. Przykładem może być szyfrowanie poczty elektronicznej, gdzie klucz publiczny może być użyty do zaszyfrowania wiadomości, a klucz prywatny do jej odszyfrowania.

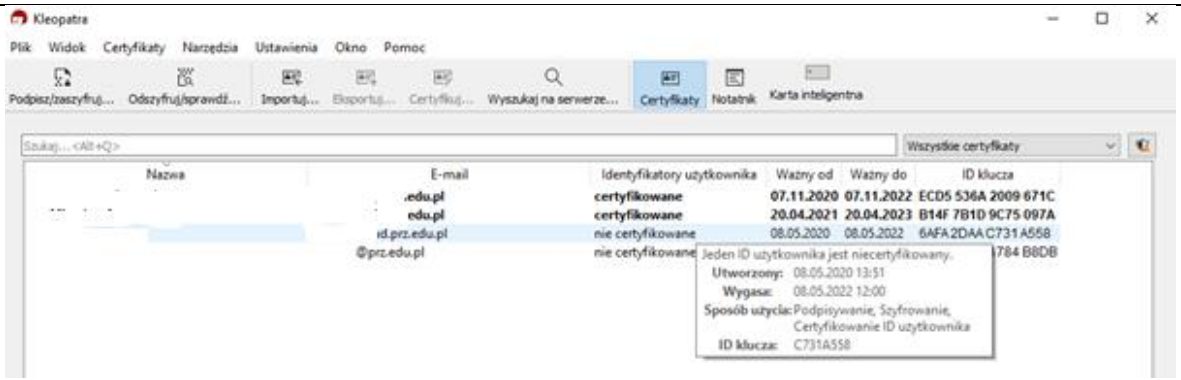
Jednym z rozwiązań jest standard OpenPGP. Definiuje kryptograficzne rozszerzenia poczty elektronicznej - szyfrowanie i podpisy cyfrowe. Standard został oparty na istniejącym programie PGP. Obecnie istnieje wiele różnych implementacji. Standard został zdefiniowany w dokumencie RFC 4880. Często w procesie wysyłania wiadomości e-mail użytkownicy korzystają z klienta poczty elektronicznej Thunderbird. Klient ten umożliwia wysyłanie i odbieranie zaszyfrowanych i cyfrowo podpisanych wiadomości e-mail przy użyciu standardu OpenPGP. Ta funkcja jest powszechnie znana jako szyfrowanie end-to-end (e2ee) i sprawia, że komunikacja jest bardziej bezpieczna i mniej prawdopodobne jest, że będzie szpiegowana przez osoby trzecie. Thunderbird 78 ma wbudowaną obsługę dwóch standardów szyfrowania - OpenPGP i S/MIME.

Poprzednie wersje Thunderbirda (v68 i wcześniejsze) miały wbudowaną obsługę S/MIME, a obsługę OpenPGP można było dodać za pomocą dodatku Enigmail i oprogramowania GnuPG. Dodatek Enigmail nie jest już dostępny dla Thunderbirda 78, chyba że chodzi o pomoc jego byłym użytkownikom w migracji do OpenPGP w Thunderbirdzie 78 lub uzyskanie wskazówek, jak przywrócić swoje reguły "Junior Mode" z Enigmaila. Można zaktualizować ustawienia Thunderbirda ze starszej wersji (np. 68.x) do wersji 78.x. Przed pierwszym użyciem Thunderbirda 78 zaleca się jednak wykonanie kopii zapasowej profilu Thunderbirda, ponieważ po aktualizacji profil nie może być już używany z Thunderbirdem 68.

Enigmail używał GnuPG do przechowywania i zarządzania wszystkimi kluczami i zaufanymi ustawieniami. Możesz dokonać migracji, a Enigmail odczyta stare klucze z GnuPG i zaimportuje je. Thunderbird 78 używa innych ustawień niż Enigmail. W Enigmailu można było włączyć OpenPGP dla konta pocztowego, ale pozwolić mu automatycznie wybrać klucz do użycia. Thunderbird 78 łączy te ustawienia. Aby włączyć OpenPGP dla konta e-mail, musisz jawnie określić klucz, który ma być użyty.

Do szyfrowania zostanie wykorzystane oprogramowanie GPG4win. Jest to zestaw zaawansowanych narzędzi do szyfrowania danych. Umożliwia ochronę przed nieautoryzowanym dostępem nie tylko poczty elektronicznej, ale także plików i folderów. Praca z Gpg4win opiera się na szyfrowaniu asymetrycznym, czyli na podstawie dwóch kluczy - prywatnego i publicznego. Pierwszy z nich służy do szyfrowania danych, drugi powinien trafić do odbiorców wiadomości, którzy mogą uzyskać do nich dostęp. Klucz prywatny należy przechowywać w bezpiecznym miejscu.

W skład pakietu wchodzą takie elementy jak narzędzie szyfrujące GnuPG, menedżer certyfikatów Kleopatra (rys. 7), alternatywny menedżer certyfikatów GPA, klient poczty elektronicznej Claws Mail, a także dwie wtyczki umożliwiające integrację z Microsoft Outlook (w wersjach 2003, 2007, 2010 i 2013) oraz Eksploratorem Windows.

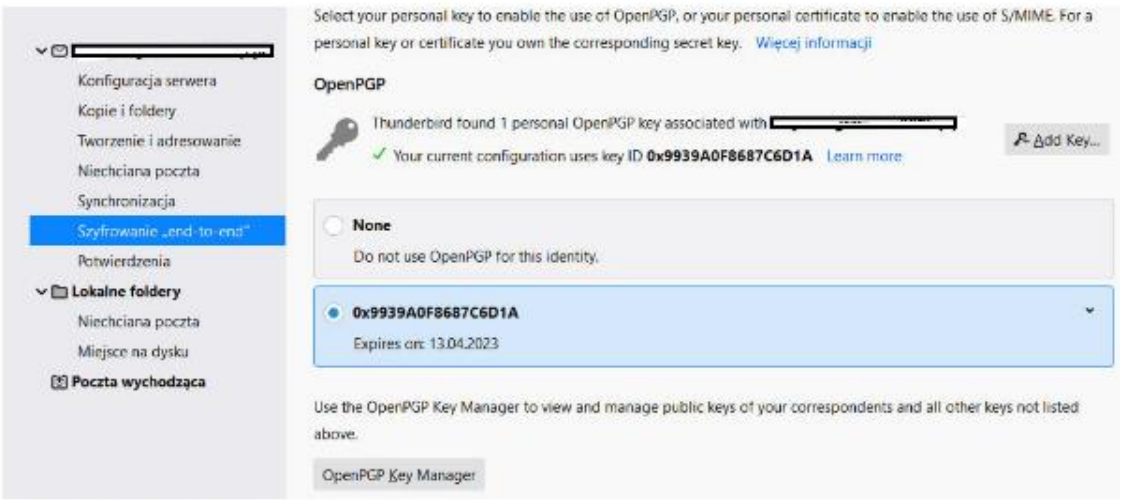


Rys. 7. Menedżer certyfikatów - Kleopatra.

Gpg4win obsługuje standardy OpenPGP i S/MIME (X.509), tworząc domyślnie certyfikaty przy użyciu kluczy 2048-bitowych. Standardowym algorytmem szyfrowania i podpisywania jest RSA. Dodatkowo pakiet umożliwia również generowanie i weryfikację sum kontrolnych SHA1, SHA256 i MD5.

Konfiguracja środowiska szyfrowania wiadomości.

Po przypisaniu kont pocztowych do programu GPG4WIN należy wygenerować parę kluczy. Para kluczy składa się z klucza prywatnego i klucza publicznego. Klucz prywatny jest przypisany do konkretnego konta. Osoba, która chce wysłać zaszyfrowaną wiadomość na to konto musi posiadać klucz publiczny odbiorcy.



Rys. 8. Ustawienia sekcji Remote Desktop

Po skonfigurowaniu kont w Cleopatrze, możesz bezpośrednio używać Thunderbirda do wysyłania i odbierania zaszyfrowanych wiadomości bez użycia zewnętrznego programu. Pamiętaj o przesłaniu swojego klucza publicznego przy wysyłaniu pierwszej wiadomości do nowego odbiorcy (Rys. 8). Przykładowa zaszyfrowana wiadomość została przedstawiona na Rys. 9.

```
-----BEGIN PGP MESSAGE-----

wcDMA0r5u59RHK/uAQv/cvK0XliobGKfmQ25IcGe4kxtcXan9oDhQ0HODeAQyLSfpPFYOitt4LpF
Kc2aae3ayqRN+0bhTESVFaxttCw76E5wszkM9cK8UdxYzrX9PuaujtzYj8kSx3m0skfXrdglYnM8
llIYNETSgTnFSZ4jHKQLVIHVw9ZMztoo/ibLVJY3TTd7aKn7+cYyepNasrPPzoxcSGjJ1pQCkJ6t
SGtm8HDBfekKbK6qTKefYdGrCDBS4sAsuszwaX5QtSn50LAE2FkXCiKzTh6DkdFxQQ7yk/rUTs93
MkRwRtjteDqO7KC1yNPBim+KVLVG20EibD1FrdFIsbaEaPIl3Y06LhmjBMrUOUaMhPJpYDM1Ki8u
gqGHOQmqISQU1y6/poyGDmOfSPOFchWaTB+9fjzpmEb32mK10D1JOM2llut5AtmZH8W1lKpy4cdC
XygSXMkJ4as+p9/MtICdESyFkDXamESbtI04Ay5Xj+YrBnQ+Wk0lHOeLfSFg+cj7fwUuasRvEIe0
wcDMA3pK1foZRRoWAQv/UVilR5h++k8Tq8uk/IeUchC3Si832Li8Ro++dGxy65Gomjlzg+oxbOoj
0u1kZGs5QbCywv5+vlo7CxpGSeMcBbj1T5jV/cKk1An9bdCjADXFLw4sEWCtqTR47OFqArvqi2gm
2iOW4g6Zcnd21cfGe5kmeyRKt8OmHL6LDaZXSnJCJkhNRwr3GKHh8gJeT00bn+72M9TbBKXxLe3T
bnGw2ypPIQJ55k2x+ZbgkjDnQQDogsHpB1ip7K5yYArf+rI4uPqbYQgSU3NYYAUsmOtI2yesouvV
gFic/0TE9xq0qhciE2bTWPxH5ikxCMwLQa33E8+hngsSDfoyoRdolSEwjhI8KHthzddXzPNSkdgn
Q4pdGUljFaDivtLc7cNs3SFKoZBiZcQaHRTABVNDMQgRqgoG6F0Ditu03vXCh5aR8/zUVS6moGT8
2sh/VWvryEAHKLSUPZulgwaZlD5hxosUMuwzGibLzaCApbilNdzm4zaDz2KdGBwmvyGkC7oT4lvj
0sMwAbnd2f3Hz+AuXFajZ6uO8m6ibKMtJRM3EXggkNhue0rIU4KLchp9U9jLAt6GMQjPFKmgGqEj
U7/QPiVbJ8DjbmhYH90JwYH8hJCx1rq4AtXOxJgz8w0B+MOe6maKxDaDqS9gQj/n9N/Hvj8btZKz
turb54Y8MxZXXXoNxLAVZr1HHcbQoweHIx0EXanoMsxEwT3ugAiQetwBzXnR9DOzxTkzeOMK1ooS
6jnVTQy454q1+w6fNWAfBbpYY73Lt1NifD7mHoqe1G3oWhgzj/uUs67TJ1DjLfqzhxqw0TnfXyNM
+457fZCj+iYwdV8DhfDb4dyfYmDjA8LLP8Uw7gLtkFxDldsaLf7/xQ5g98eKhz/4INI0xL+5Znno
x4SnkX++hy4z/nRKBNQcIupW7KuG1SOABTIhQWx3mtxyte0mxBRxiApfC5HfNzQM+vtmhJK8mlHK
Osc3kVw6kTodafSTi/qLghcOh2R7h8hL7qRc56ig7i4nPY5bnsPpfyyPYAuUDJQUz5z4tFrdEX/+
gw/gH3O8hTS17VSfgya0BUwJvMnlbS1+VZ7zomF405ne8hrFsT5j/dnjP7NgGS3CVMDLyEDtQA7k
Vbru0EN4JTsCu3T7rMnRrGtXlkfsTXBLayhcpbaMyHojMKw60p41o2gvTn5fw/+GJHGQdsZ3HJ+g
fr9EWKLQzQX6PSLsJ5OexLRkMtHXV4jBoSRyTzFTwprBkNNKZu2aRYa17BBFuVc5RTf8rSVWq7Eq
rKrXGOP+GgqGGTxoD8zfFtp0YJ+mP28L0DtuPnmG9IzxdbXO/JG6sT6hzPEA6MIlaW6Y++94Jpg2
XEKsGOdW9IHx9613FwjPtj6HKC8GtN5s8dgSAm3tw5KUWfchtKIOZYiynxuRnwIMN0UM0G2QFKYr
pU+50ba8rdui9D2YFzEcbw9a3meaWksO3Zvd8obQfwGFMX9DwV5VPEcmASHEUMULGBUO3KIUtaxU
Sdg9qmehxPMkkH3bB3x+G79WmV0ss0G9r+uVk/XhzxckqUI0w++q2PmWsXAIP2NsyX7W1BHyZ5J0
HhUwUllGtpl3gv/WwOxTyoEz2oeQucK5Eq91vEwaudCnip7STqK2WpboGvAQ54ZIZRFbm/4sOd/W
4kH6xyeYBTsIf3ft7LyvoB6Xq91A1xOFe94CcAqty90FynvF26Da7QRsNQalhfhfB1bnaEQIgf+7
J9fpMYQEcC4tT8RW9vtozQurNpgZnZS9sjWjke6/j3XV7paxOW7OG8nc+1r09LQMMtVjvI5Zd1FV
JyAtr1EsoF/9MzFfofn6eCtU8VvXiS8+cIDjTqrb2EKS68Rpu9Z8LCgz
=MjYk
-----END PGP MESSAGE-----
```

Rys. 9. Przykład zaszyfrowanej wiadomości.

Thunderbird automatycznie deszyfruje wiadomości i wysyłane z nimi załączniki. Pamiętaj, że przed wysłaniem zaszyfrowanej korespondencji musisz znać klucze publiczne odbiorców. Szyfrowanie za pomocą dodatku GPG chroni nie tylko treść, ale również załączniki. Bez znajomości klucza odbiorcy nie jesteśmy w stanie wysłać zaszyfrowanej wiadomości. Dodatkowo Thunderbird pozwala na synchronizację kilku kont pocztowych.

Pytania:

Pytania na forum dyskusyjnym, na które należy odpowiedzieć z krótkim uzasadnieniem. Odpowiedzi zostaną omówione z mentorem podczas sesji mentorskich.

1. Czym jest sieć VPN?
2. Jak można korzystać z rozwiązania VPN?
3. Czy można wysłać komuś swój klucz prywatny do szyfrowania poczty elektronicznej PGP?

Pytania do samooceny. Po udzieleniu odpowiedzi uczeń może zobaczyć wyniki i porównać je z tymi zapisanymi na platformie

1. Metoda bezpiecznego dostępu do Twoich danych z dostępu zdalnego
2. Metody zabezpieczania konwersacji e-mailowych

Załączniki:

1. Prezentacja
2. Materiały wideo

Referencje:

1. Rana, Muhammad Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam. (2021). Common Security Protocols for Wireless Networks: A Comparative Analysis. 10.2991/ahis.k.210913.080.
2. Habibi Lashkari, Arash & Sendón Varela, Juan & Samadi, Behrang. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). 10.1109/ICCSIT.2009.5234856.
3. Kumkar, Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne, Seema. (2012). Vulnerabilities of Wireless Security protocols (WEP and WPA2). International Journal of Advanced Research in Computer Engineering & Technology. 1.
4. Costa, Luís & Fdida, Serge & M. B. Duarte, Otto Carlos. (2000). An Introduction to Virtual Private Networks: Towards D-VPNs.
5. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/
6. https://www.radmin-vpn.com
7. https://www.fortinet.com/resources/cyberglossary/pgp-encryption