## Cel:

Celem laboratorium nr.3 było wykorzystanie dostarczonych informacji do otrzymania dostępu do danych poufnych z wykorzystaniem oprogramowania Cisco PacketTracer.

## Pytania i odpowiedzi:

***1.Czy zaszyfrowana wiadomość ujawnia tekst jawny? Czy można coś z niej odczytać?***

Nie, nie możemy odczytać teksu ponieważ zaszyfrowana wiadomość nie ujawnia tekstu jawnego i nie możemy z tego pliku nic odczytać oprócz informacji o dekrytpowaniu

***2.Jaki jest rezultat odszyfrowania wiadomości?***

Account Information:
Mary
Username= mary
Password= cisco321

***3.Jaka metoda szyfrowania została wykorzystana? Dlaczego wymagany jest klucz? W jaki sposób możesz pozyskać klucz?***

W tym przykładzie została użyta metoda AES czyli AdvancedEncryption Standard.

AES sięga korzeniami do początku lat 70. Wówczas National Bureau of Standards (NBS, obecnie National Institute of Standards and Technology – NIST) rozpoczęło prace nad stworzeniem algorytmu szyfrowania, który stworzyłby standard uznany za bezpieczny. Algorytm ten miał zapewnić wysoki poziom bezpieczeństwa, dostępny dla wszystkich użytkowników oraz łatwy do zaadoptowania w różnego rodzaju aplikacjach. Miał być ponadto łatwy i ekonomiczny w implementacji sprzętowej. Szyfr, który spełnił te warunki, został opracowany na bazie algorytmu stworzonego na początku lat 70 przez IBM noszącego nazwę Lucipher.

***4. Jakie inne podstawowe zasady tworzenia haseł są Tobie znane?***

Np. używanie więcej niż 8 znaków w tym cyfry, małe i duże litery, znaki specjalne w różnych kombinacjach lub/i używanie generatorów trudnych haseł.

**5.Jakie hasło do zaszyfrowania wykorzystała Mary? Jakie dane logowania do serwera FTP posiada Mary**

Hasło Mary to: maryftp123

Serwera FTP: username: mary, password: cisco123

***6.Jakiego adresu IP należy użyć to połączenia się z serwerem FTP?***

209.165.201.3

***7.Na laptopie Mary znajdują się inne pliki textowe. Który plik (i dlaczego) jest poufny? Czy możesz odczytać zawartość? Czy znasz hasło odszyfrowujące?***

Zarówno plik clientinfo.txt i ftplogin.txt są szyfrowane i nie można ich odczytać bez klucza.

Klucz to: maryftp123

***8.Osoba podsłuchująca ruch sieciowy przechwyciła plik. Jaką treść zobaczy atakujący?***

Zaszyfrowany plik txt z wiadomością gdzie ją odszyfrować.

***9.Jakie hasło do zaszyfrowania wykorzystał Bob? Jakie dane logowania do serwera FTP posiada Bob?***

Hasło Boba to: bobftp123

Serwer FTP: username: bob, password: ninja123

***10.Analogicznie jak poprzednio połącz się z serwerem FTP. Jaki adres należy wybrać do połączenia?***

Wybieramy adres prywatny serwera FTP czyli: 10.44.1.254, ponieważ jesteśmy w sieci prywatnej.

***11.Co warto sprawdzić w celu poszukiwania klucza?***

Warto sprawdzać ukryte wiadomości zapisane w mailu lub notatkach lub/i plikach ukrytych.

## Wnioski:

Do szyfrowania warto używać systemu AES wraz z kluczem do odszyfrowania wiadomości, jeśli mamy poufne dane i nie chcemy, żeby dostały się w niepowołane ręce, a chcemy je przekazać komuś w internecie w bezpieczny sposób. Klucze zawsze warto trzymać/przechowywać na innych nośnikach danych niedostępnych online, lub nie podwać całego klucza jedną ścieżką kontaktową, np. mailem, tylko wykorzystać do tego celu jeszcze np. telefon komórkowy. Dobrą praktyką jest także korzystanie z aplikacji szyfrujących takich jak np. Signal.