Cel:

Celem laboratorium nr 3 jest wykorzystanie dostarczonych informacji do otrzymania dostępu do danych poufnych z wykorzystaniem oprogramowania Packet Tracer.

Pytania i odpowiedzi:

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

Zaszyfrowana wiadomość nie ujawnia tekstu jawnego i nie można z pliku nic odczytać oprócz informacji o dekrytpowaniu

Jaki jest rezultat odszyfrowania wiadomości?

Account Information:

Mary

Username= mary

Password= cisco321

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

Została użyta metoda AES czyli Advanced Encryption Standard. W 2001 roku został przyjęty jako standard.

AES jest oparty na algorytmie, którego autorami są belgijscy kryptografowie, Joan Daemen i Vincent Rijmen. Zaprezentowali oni swoją propozycję szyfru Instytucji NIST w ramach ogłoszonego konkursu. Rijndael jest rodziną szyfrów o różnych długościach klucza oraz różnych wielkościach bloków.

Klucz jest wymagady do szyfrowania i do odszyfrowania wiadomości.

Klucz można pozyskać używając hasła użytkownika. W ogólnym znaczeniu hasło zdobywa się od nadawcy zaszyfrowanej wiadomości dlatego metoda ta należy do bezpiecznych, bez klucza nie uzyskamy dostępu do zaszyfrowanej wiadomości.

Jakie inne podstawowe zasady tworzenia haseł są Tobie znane?

Używanie więcej niż 8 znaków w tym cyfry, litery, znaki specjalne w różnych kombinacjach lub/i używanie generatorów trudnych haseł jak np. KeePass.

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

Hasło do szyfrowania Mary to: maryftp123
Dane do serwera FTP: username: mary, password: cisco123

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

209.165.201.3

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

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

Zaszyfrowany plik txt z wiadomością gdzie ją odszyfrować.

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

Hasło do szyfrowania Boba to: bobftp123
Dane do serwera FTP: username: bob, password: ninja123

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

Tym razem wybieramy prywatny adres IP serwera FTP czyli: 10.44.1.254 ponieważ jesteśmy w sieci prywatnej.

Co warto sprawdzić w celu poszukiwania klucza?

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

Wnioski:

Warto używać szyfrowania AES wraz z kluczem do odszyfrowania wiadomości jeżeli posiadamy poufne dane i chcemy przekazać komuś je w internecie w bezpieczny sposób. Warto także klucze przechowywać na innych nośnikach niedostępnych online lub podawać je np. w połowie drogą mailową drugą połowę telefonicznie lub w innych kombinacjach np. używając komunikatorów Signal bądź Telegram.