Politechnika Świętokrzyska
Cyberbezpieczeństwo

Cyberbezpieczeństwo- Laboratorium 3

Dostęp do plików poufnych

Prowadzący: mgr inż. Sebastian Wójtowicz

Politechnika Świętokrzyska
Cyberbezpieczeństwo

Device	Private IP	Public IP	Subnet mask	Site
FTP/Web Server	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Mary	10.44.3.101	N/A	255.255.255.0	Healthcare at Home
Bob	10.44.1.3	N/A	255.255.255.0	Metropolis Bank HQ

Cele

Część 1: Zlokalizuj dane logowania na konto FTP dla komputera Mary
Część 2: Wyślij poufne dane wykorzystując FTP
Część 3: Zlokalizuj dane logowania na konto FTP dla komputera Boba
Część 4: Pobierz poufne dane wykorzystując FTP
Część 5: Odszyfruj zawartość pliku *clientinfo.txt*

W tym zadaniu, otrzymasz dostęp do zaszyfrowanych zawartość plików tekstowych. Wykorzystasz przesyłanie przez Internet do scentralizowanego serwera FTP. Inny użytkownik pobierze następnie pliki z serwera FTP i odszyfruje ich treść.

Część 1: Zlokalizuj dane logowania na konto FTP dla komputera Mary

Krok 1: Dostęp do dokumentu tekstowego na laptopie Mary.

W **Healthcare at Home** wybierz laptop Mary i odszukaj plik textowy o nazwie **ftplogin.txt**.

Krok 2: Odszyfruj informacje o koncie FTP Mary.

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

Mary pozostawiła informację o stronie szyfrującej w swoim pliku txt. Przejdź do strony i odszyfruj zaszyfrowaną wiadomość.

...

Pytanie: Jaki jest rezultat odszyfrowania wiadomości?

Krok 2a: Odgadnij hasło użytkownika

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

Załóżmy, że Mary stosuje podstawowe metody zabezpieczeń konta.
1. Unikalne hasło dla nowego konta
2. Minimum 8 znaków
3. W kombinacja musi się być minimum jedna cyfra

Pytanie: Jakie inne podstawowe zasady tworzenia haseł są Tobie znane?

Biorąc pod uwagę powyższe informacje sprawdź:
mary1234, 1234mary, password1, passwordftp, maryftp1, maryftp12, maryftp123,123maryftp,ftpmary123, i inne kombinacje jakie przychodzą Ci na myśl.

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

Część 2: Wyślij poufne dane wykorzystując FTP

Krok 1: Zobacz dokument poufny na laptopie Mary.

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

Krok 2: Zdalnie połącz się z serwerem FTP.

Wykorzystaj **Wiersz poleceń i komendę ftp <IP>** aby podłączyć się do serwera **FTP / WWW** w **Metropolis Bank HQ.** Pytanie: Jakiego adresu IP należy użyć to połączenia się z serwerem FTP?

Krok 3: Prześlij plik na serwer FTP.

Wykorzystaj **Wiersz poleceń i komendę put <file>** w celu umieszczenia plików na serwerze FTP/WWW

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

Część 3: Zlokalizuj dane logowania na konto FTP dla komputera Boba.

Krok 1: Otwórz dokument tekstowy na komputerze Boba.

Postępuj analogicznie jak w części 1 aby odszukać plik textowy na komputerze Boba.

Krok 2: Odszyfruj informacje o koncie FTP Boba.

Postępuj analogicznie jak w części 1 aby odszyfrować informacje o koncie Boba. Pytanie: Jakie hasło do zaszyfrowania wykorzystał Bob? Jakie dane logowania do serwera FTP posiada Bob?

Część 4: Pobierz poufne dane przy użyciu FTP

Krok 1: Zdalnie połącz się z serwerem FTP.

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

Krok 2: Pobierz plik do komputera Boba.

Korzystając z komendy **get <file>** pobierz plik **clientinfo.txt.** Czy znasz już hasło do odszyfrowania wiadomości? Jeśli nie udało Ci się odgadnąć jeszcze hasło wypisz hasła (minimum 10) jakie przychodzą Ci do głowy, czasem odpowiedź mamy dosłownie „przed sobą”... Jeśli się nie uda przejdź do części 5.

Część 5: Odszyfruj zawartość pliku clientinfo.txt

Krok 1: Odszukaj klucz deszyfrujący.

Masz dostęp do komputera Boba który znajduje się w sieci Metropolis Bank HQ. Pytanie: Co warto sprawdzić w celu poszukiwania klucza? Sprawdzając mail pamiętaj o przyciskach funkcyjnych w symulacji PT.

Krok 2: Odszyfruj zawartość pliku clientinfo.txt.