Autor: Mateusz Kiebała 359758

1. Chronione wartości:
   - Hasło i login użytkownika.
   - Dostęp do wszystkich usług wymagających uwierzytelnienia.
   - Prywatne dane użytkownika.

2. Atakujący: doświadczona osoba lub grupa, która ma dostęp do specjalistycznego sprzętu, ma doświadczenie i duże zasoby organizacyjne, jest osobą zewnętrzną lub wewnętrzną w stosunku do organizacji, która obsługuje laboratorium komputerowe.

3. Drzewa ataku:

I
. (OR) Zdobycie dostępu do wszystkich usług wymagających uwierzytelnienia.
1. (OR) Zdobycie hasła i loginu.
1.1 (OR) Wykorzystanie połączenia podczas korzystania z protokołu POP3.
1.1.1 (OR) Podsłuchiwanie połączenia.
1.1.1.1 (OR) Użytkownik loguje się korzystając z „User/Pass Authentication”.
1.1.1.1.1 (OR) Przechwycenie loginu i hasła w postaci niezaszyfrowanej.
1.1.1.2 (AND) Użytkownik loguje się korzystając z „APOP Authentication”.
1.1.1.2.1 (OR) Przechwycenie loginu i hasła w postaci zaszyfrowanej.
1.1.1.2.2 (OR) Odszyfrowanie loginu i hasła za pomocą decryptora (np. MD5).
1.2 (AND) Szantaż użytkownika.
1.2.1 (OR) Znalezienie powodów do szantażu.
1.2.1.1 (AND) Zmuszenie szantażem użytkownika do podania hasła i loginu.
1.2.1.1.1 (OR) Nawiązanie anonimowego kontaktu z użytkownikiem.
1.2.1.1.2 (OR) Wymuszenie podania loginu i hasła przy użyciu gróźb.
1.3 (OR) Zmuszenie siłą użytkownika do podania loginu i hasła.
1.4 (OR) Złamanie hasła metodą brute force.
1.5 (AND) Wirus wysyłający login i hasło do osoby atakującej.
1.5.1 (OR) Brak zainstalowanego oprogramowania antywirusowego.
1.5.2 (OR) Wgranie wirusa na serwer.
1.5.2.1 (AND) Zdalne wgranie.
1.5.2.1.1 (OR) Wysłanie wirusa do administratora jako załącznik do e-mailu.
1.5.2.1.2 (OR) Ściągnięcie załącznika na komputer.
1.5.2.1.3 (OR) Zainstalowanie wirusa na komputerze.
1.5.2.2 (OR) Wgranie wirusa w laboratorium przez administratora.
1.5.2.2.1 (OR) Szantaż administratora.
1.5.2.2.1.1 (OR) Znalezienie powodów do szantażu.
1.5.2.2.1.2 (AND) Zmuszenie szantażem administratora do wgrania wirusa.
1.5.2.2.1.2.1 (OR) Nawiązanie anonimowego kontaktu z administratorem.
1.5.2.2.1.2.2 (OR) Wymuszenie wgrania wirusa przy użyciu gróźb.
1.5.2.2.2 (OR) Zmuszanie administratora siłą.
1.5.2.2.3 (OR) Przekupienie administratora.
1.5.2.3 (AND) Wgranie wirusa w laboratorium przez atakującego.
1.5.2.3.1 (OR) Pozyskanie hasła administratora metodami opisanymi w tym drzewie.
1.5.2.3.2 (OR) Znalezienie się w laboratorium.
1.5.2.3.3 (OR) Uzyskanie dostępu do komputera.
1.5.2.3.4 (OR) Zainstalowanie wirusa jako administrator.
1.5.3 (OR) Wysłanie loginu i hasła do atakującego.
1.5.3.1 (OR) Podczas tworzenia konta użytkownika.
1.5.3.2 (OR) Podczas korzystania z POP3 przy wpisywaniu loginu i hasła.
1.5.3.3 (OR) Podczas logowania użytkownika na komputer.
1.6 (OR) Podpatrzenie podczas wpisywania.

1.7 (OR) Podsłuchanie podczas wpisywania.
1.8 (AND) Wykradnięcie kartki z zapisanymi hasłami.
1.8.1 (OR) Znalezienie się w pobliżu użytkownika.
1.8.2 (OR) Zaobserwowanie gdzie trzyma kartkę z loginem i hasłem.
1.8.3 (OR) Zabranie kartki z zaobserwowanego miejsca.
1.9 (AND) Zdobycie loginu i hasła wykorzystując informacje o użytkowniku.
1.9.1 (OR) Obserwacja użytkownika.
1.9.2 (OR) Wykorzystanie informacji do złamania hasła, np. data urodzin, imię żony.
1.10 (OR) Pozyskanie loginu i hasła poprzez fałszywą stronę.
1.10.1 (AND) Zmiany w tabeli DNS.
1.10.1.1 (OR) Stworzenie strony przypominającej oryginalną.
1.10.1.2 (OR) Zalogowanie się na serwer jako administrator.
1.10.1.2.1 (OR) Podpatrzenie loginu i hasła podczas wpisywania.
1.10.1.2.2 (OR) Podsłuchanie loginu i hasła podczas wpisywania.
1.10.1.2.3 (OR) Przekupienie administratora.
1.10.1.2.4 (OR) Wykradnięcie kartki z zapisanymi hasłami.
1.10.1.2.5 (OR) Zmuszenie siłą administratora do podania loginu i hasła.
1.10.1.2.6 (AND) Szantaż administratora.
1.10.1.2.6.1 (OR) Znalezienie powodów do szantażu.
1.10.1.2.6.2 (AND) Zmuszenie szantażem administratora do zalogowania się.
1.10.1.2.6.2.1 (OR) Nawiązanie anonimowego kontaktu z administratorem.
1.10.1.2.6.2.2 (OR) Wymuszenie zalogowanie się przy użyciu gróźb.
1.10.1.3 (OR) Zmiana tabeli DNS i pamięci podręcznej DNS, tak żeby użytkownik wpisując adres strony był kierowany na podstawioną przez atakującego stronę.
1.10.1.4 (OR) Użytkownik loguje się na stronę za pomocą loginu i hasła.
1.10.1.5 (OR) Przesłanie loginu i hasła do osoby atakującej.
1.10.2 (AND) Zmiana hasła przez użytkownika na podstawionej stronie.
1.10.2.1 (OR) Stworzenie standardowej strony do zmiany hasła.
1.10.2.2 (OR) Wysłanie e-mailu do konieczności zmiany hasła, z linkiem do fałszywej strony.
1.10.2.3 (OR) Próba zmiany hasła przez użytkownika.
1.10.2.4 (OR) Przesłanie loginu i hasła do osoby atakującej.
1.10.3 (AND) Zalogowanie się użytkownika podczas próby połączenia z WiFi w laboratorium.
1.10.3.1 (OR) Włamanie się do routera WiFi.
1.10.3.1.1 (AND) Router ma ustawienia domyślne.
1.10.3.1.1.1 (OR) Zalogowanie się do routera przez domyślne hasło.
1.10.3.1.2 (AND) Router chroniony hasłem.
1.10.3.1.2.1 (OR) Pozyskanie hasła od administratora.
1.10.3.1.2.1.1 (OR) Podpatrzenie hasła podczas wpisywania.
1.10.3.1.2.1.2 (OR) Podsłuchanie hasła podczas wpisywania.
1.10.3.1.2.1.3 (OR) Przekupienie administratora.
1.10.3.1.2.1.4 (AND) Szantaż administratora.
1.10.3.1.2.1.4.1 (OR) Znalezienie powodów szantażu.
1.10.3.1.2.1.4.2 (AND) Zmuszenie siłą administratora do zalogowania się.
1.10.3.1.2.1.4.2.1 (OR) Nawiązanie anonimowego kontaktu z administratorem.
1.10.3.1.2.1.4.2.2 (OR) Wymuszenie hasła przy użyciu gróźb.
1.10.3.1.2.1.5 (OR) Wykradnięcie kartki z zapisanymi hasłami.
1.10.3.1.2.1.6 (OR) Zmuszenie siłą administratora do podania hasła.
1.10.3.2 (OR) Stworzenie fałszywej strony, na której użytkownik logując się, potwierdza swoją przynależność do uczelni i dzięki temu uzyskuje dostęp do WiFi.
1.10.3.3 (OR) Zmiana ustawień routera, że przy próbie połączenia się z WiFi, użytkownik przenoszony jest na fałszywą stroną autoryzującą, a następnie po jego zalogowaniu się, łączy użytkownika z WiFi.
1.10.3.4 (OR) Zalogowanie się użytkownika.
1.10.3.5 (OR) Przesłanie loginu i hasła do serwera osoby atakującej.

II

. (OR) Odczytanie prywatnych danych użytkownika.

1. (AND) Zdobycie loginu i hasła użytkownika metodami opisanymi w drzewie nr I.
   1.1. (OR) Zalogowanie się na wybraną usługę.
2. (OR) Wykorzystanie POP3.
   2.1. (AND) Wykorzystanie połączenia podczas korzystania z protokołu POP3.
      2.1.1. (OR) Podsłuchiwanie połączenia.
      2.1.2. (OR) Użytkownika korzysta z komend RETR lub TOP.
      2.1.3. (OR) Przechwytywanie e-maili ściąganych przez użytkownika w formie tekstowej.
   2.2. (AND) Odczytanie e-maili ściągniętych na komputer.
      2.2.1. (OR) Skorzystanie użytkownika z POP3 i ściągnięcie e-maili na komputer.
      2.2.2. (OR) Nieskasowanie e-maili po odczytaniu.
      2.2.3. (OR) Pozostawienie zalogowanego użytkownika na komputerze.
      2.2.4. (OR) Odczytanie e-maili.