Ćwiczenie 10 Audyt haseł w systemie Windows

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.
Sprawozdanie w postaci elektronicznej należy oddać prowadzącemu zajęcia przed opuszczeniem laboratorium.

Zadanie 1 Nieautoryzowany dostęp do komputera, z wykorzystaniem standardowego wygaszacza ekranu *logon.scr*

1. Zalogować się jako administrator, uruchomić program ***regedit*** i zmienić wartość klucza: *ScreenSaveTimeOut* na wartość 15 (sekund) oraz *ScreenSaveActive* na wartość 1. (*HKEY_USERS\.DEFAULT\Control Panel\Desktop*).
2. W katalogu *%systemroot%\System32* skopiować następujące pliki:
   logon.scr → na *logon.old.scr*
   cmd.exe → na *logon.scr*.
3. Wylogować się i odczekać około 15 sekund.
4. Po pojawieniu się konsoli (okna poleceń) wykonać następujące próby (uwaga: niektóre z nich należy powtórzyć kilkakrotnie, ograniczając do niezbędnego minimum ilość otwartych okien):
   A. Określić kontekst użytkownika (wykorzystać program *whoami z Resource Kit*);
   B. Uruchomić konsolę *lusrmgr.msc* i wypróbować możliwości:
      - zmiany hasła dla konta administratora,
      - utworzenia nowego konta użytkownika,
      - zmiany składu grup ***Administrators***.
   C. Po zamknięciu konsoli *lusrmgr.msc*, uruchomić program *explorer.exe* i zbadać możliwości wykorzystania *Narzędzi administracyjnych* (np. wyczyścić plik dziennika systemowego).
   D. Zamknąć okno poleceń.
5. Zalogować się jako administrator.
6. Przywrócić pierwotne wartości kluczy w rejestrze, zmienione podczas realizacji punktu 1.
7. Przywrócić pierwotny stan plików zmieniony podczas realizacji punktu 2.

Zadanie 2 Audyt haseł przy pomocy programu LC5

1. Utworzyć trzy konta użytkowników o nazwach: KONTO3, KONTO5, KONTO8 określając dla nich dowolne hasła odpowiednio 3-znakowe, 5-znakowe i 8-znakowe. Pozostałe atrybuty konta pozostawić bez zmian w stosunku do ustawień standardowych.
2. Zainstalować program do audytu haseł - LC5 (program ***lc5setup.exe***).
3. Przy pomocy programu LC5 wykonać następujące zadania:

   3.1. Dokonać próby pozyskania haseł z komputera lokalnego (wykorzystać opcję „*Retrieve from the local machine* ..” w kreatorze).
   Przeprowadzić dwa rodzaje ataku: słownikowy oraz słownikowy atak kombinowany (w kreatorze dla kroku *Choose Auditing Method* wybrać przycisk *Custom Options* i zaznaczyć opcje dotyczące odpowiednich metod). W przypadku braku powodzenia dokonać modyfikacji słownika. Zarejestrować czas przeprowadzenia prób.

3.2. Przetestować możliwość pozyskania haseł z komputera zdalnego:

3.2.1. Na swoim komputerze, z konsoli CMD uruchomić program PWDUMP3E:
PWDUMP3E <*nazwa_komputera_partnera*> <*plik_wyjściowy*> <*konto*>,
a następnie podać hasło dla wybranego konta na komputerze partnera. W razie niepowodzenia uruchomić program PWDUMP3E podając konto administratora komputera partnerskiego.

3.2.2. Na swoim komputerze uruchomić program LC5, zamknąć okno kreatora, otworzyć nową sesję, wybrać kolejno z menu pozycje: ***Import → Import From PWDUMP File …*** , wskazać plik utworzony w p. 3.2.1 (<*plik_wyjściowy*>), a następnie przeprowadzić próbę odgadnięcia haseł dowolną metodą.

Zadanie 3 Dekodowanie fazy uwierzytelniania sesji

Zainstalować analizator ruchu sieciowego IRIS. Dokonać przechwycenia (funkcja ***Capture***) i zdekodowania (funkcja ***Decode***) fazy uwierzytelnienia sesji dla dwóch dowolnych usług (*pop3, telnet, ftp, lub innych*). Po przechwyceniu pakietów należy wykonać funkcję ***Send Buffer to Decode***. W sprawozdaniu należy zamieścić obrazy okien, w których powinny być widoczne przesyłane nazwy i hasła użytkowników.