Ćwiczenie 6 Łamanie haseł w systemie Windows 2000

1. Zalogować się jako administrator, uruchomić program *regedit* i zmienić wartość klucza: *ScreenSaveTimeOut* na wartość 30 (sekund) oraz *ScreenSaveActive* na wartość 1. (*HKEY_USERS\.DEFAULT\Control Panel\Desktop*).

2. Utworzyć trzy konta użytkowników o nazwach: **konto3**, **konto5**, **konto8** określając dla nich hasła odpowiednio 3-znakowe, 5-znakowe i 8-znakowe.

3. Dokonać próby nieautoryzowanego dostępu do własnego komputera, wykorzystując standardowy wygaszasz ekranu *logon.scr*.

   Zalogować się na jedno z kont lokalnego komputera. W katalogu *%systemroot%\System32* zmienić nazwy następujących plików:
   logon.scr → na *logon.old.scr*
   cmd.exe → na *logon.scr*.
   Wylogować się i odczekać około 30 sekund.

   Po pojawieniu się konsoli (okna poleceń) wykonać następujące próby:
   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. Uruchomić program *explorer.exe* i zbadać możliwości wykorzystania *Narzędzi administracyjnych*.
   D. Zamknąć okno poleceń.

4. Zainstalować program do audytu haseł - LC4 (**lc4setup.exe**).

5. Przy pomocy programu LC4 wykonać następujące zadania:

   5.1. Dokonać próby pozyskania haseł z rejestru 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 *Custom Options* ..). W przypadku braku powodzenia dokonać modyfikacji słownika.
   Sprawdzić możliwości pozyskania haseł w kontekście zwykłego użytkownika oraz przy braku autoryzacji (wg scenariusz opisanego w pkt. 2). Zarejestrować czas przeprowadzenia prób. Przywrócić pierwotne nazwy plików (z pkt. 2).

   5.2. Przetestować możliwość pozyskania haseł z komputera zdalnego:

   5.2.1. Na swoim komputerze, z konsoli CMD uruchomić program PWDUMP3:
   PWDUMP3 <*nazwa_komputera_partnera*> <*plik_wyjściowy*> <*konto*>,
   a następnie podać hasło dla wybranego konta na komputerze partnera. W razie niepowodzenia uruchomić program PWDUMP3 podając konto administratora komputera partnera.

5.2.2. Na swoim komputerze uruchomić program LC4, zamknąć okno kreatora, otworzyć nową sesję, wybrać kolejno z menu pozycje: ***Import → Import From PWDUMP File …*** , wskazać plik utworzony w p. 5.2.1 (<*plik_wyjściowy*>), a następnie przeprowadzić próbę odgadnięcia haseł dowolną metodą.

6. Przygotować w systemie W2K dyskietkę umożliwiającą resetowanie hasła dowolnego użytkownika w trybie *off-line* (z systemu Linux):
   6.1. Utworzyć dodatkowe konto administracyjne – włączyć je do grupy ***Administrators***.
   6.2. Uruchomić program *rawrite2.exe*, włożyć sformatowaną dyskietkę do napędu, a następnie podać nazwę pliku zawierającego binarny obraz dyskietki (bd011022.bin).
   6.3. Uruchomić komputer z przygotowanej dyskietki:
   - wskazać właściwą partycję, zawierającą **własną instalację** systemu,
   - wskazać katalog z bazą **SAM** (standardowo *winnt\system32\config*),
   - nie wyłączać domyślnej dla Windows 2000 opcji szyfrowania postaci *hash* haseł (SYSKEY),
   - wpisać nowe hasło dla użytkownika ***Administrator***
   - Na pytania: *Write hive files?* oraz *About to write file(s) back?* odpowiedzieć twierdząco (*y*).

   6.4. Uruchomić ponownie własną instalację W2K. Dokonać próby załogowania się na konto administratora podając zmienione hasło.

7. Zainstalować program **Iris** (*Iris380Demo.exe*). Dokonać przechwycenia i zdekodowania fazy uwierzytelnienia dwóch dowolnych sesji (*pop3, telnet, ftp, lub innych*). Należy wykorzystać filtrowanie portów i dekodowanie sesji.

8. Sprawdzić możliwości odgadywania haseł wykorzystywanych w dostępie do zasobów w systemie Windows 98. Próbę przeprowadzić za pomocą programu PQWAK, po uzyskaniu odpowiednich informacji od prowadzącego. W czasie eksperymentu dokonać przechwycenia (*sniffingu*) pakietów wymienianych pomiędzy programem PQWAK a systemem Windows 98. Określić rodzaje pojawiających się pakietów i sytuacje w jakich się pojawiają.

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie zawierające opis wszystkich wykonanych czynności i uzyskanych wyników. W sprawozdaniu należy zamieścić również obrazy okien wynikowych. Wyniki prób przedstawić w sprawozdaniu wraz z ich z uzasadnieniem.
W sprawozdaniu powinny znaleźć się też informacje o niepowodzeniach, tzn., próbach, które nie dały rezultatu. Należy wyjaśnić przyczyny niepowodzenia.
Sprawozdanie powinno zawierać też spostrzeżenia i wnioski końcowe.

Sprawozdanie w postaci elektronicznej należy oddać prowadzącemu zajęcia przed opuszczeniem laboratorium.