

Ćwiczenie 8 Łamanie zabezpieczeń w systemie Windows 2000

1. Zalogować się jako Administrator, uruchomić *regedit* i zmienić wartość klucza: *ScreenSaveTimeOut* na wartość 30 (sekund) - (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 wygaszacz 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 (można wykorzystać program *whoami* z *Resorce Kit*);
B. Uruchomić konsolę *lusrmgr.msc* i wypróbować możliwości:
 - zmiany hasła dla konta Administrator,
 - utworzenia nowego konta użytkownika,
 - zmiany składu grup Administrators.
C. Uruchomić program *explorer.exe* i zbadać możliwości wykorzystania *Narzędzi administracyjnych*.
D. Zamknąć konsolę.
4. Zainstalować program do audytu haseł - LC4 (**lc4setup.exe**). Zainstalować bibliotekę *WinPcap 2.3 (WinPcap_2_3.exe)*.
Z katalogu systemowego *\winnt\system32* skopiować pliki: **packet.dll** i **wpcap.dll** do katalogu instalacyjnego programu LC4. Do katalogu instalacyjnego LC4 skopiować pliki: *LC4-patch.exe* oraz *N-GeN.info*. Uruchomić program *LC4-patch*.
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).
A. 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).
B. Przeprowadzić próbę typu *Brute force* dla kont **konto3**, **konto5** wybierając rozszerzony zestaw znaków (**A-Z, 0-9, !@#\$\$%^&*()-_+=**). Dla konta **konto8** wykonać atak z wykorzystaniem 2 komputerów (wykorzystać opcję *Save Disributed* z menu *File*). Jeżeli próba nie powiedzie się w ciągu 15 min. należy przerwać ćwiczenie. Zarejestrować czasy odgadywania haseł.

- 5.2. Przeprowadzić próby pozyskania haseł poprzez sniffing w sieci laboratoryjnej. Zadanie wykonać w zespołach dwuosobowych (komputery **A** i **B**).
 - 5.2.1. Zalogować się na komputerze **A** jako Administrator, utworzyć folder **Passw** i udostępnić go pod tą samą nazwą dla wybranego użytkownika z prawem dostępu *Read*.
 - 5.2.2. Na komputerze **A** uruchomić program LC4 i w oknie *Get Encrypted Passwords* wybrać opcję *Retrieve by sniffing ...*. Określić atak typu *Brute Force* z zastosowaniem podstawowego zbioru znaków (A-Z, 0-9). Uruchomić sniffer.
 - 5.2.3. Z komputera **B** odwołać się do zasobów komputera **A**:
\\A\PASSW - podając konto i hasło wybranego użytkownika,
\\A\Admin\$ - podając konto i hasło Administratora komputera **A**.
 - 5.2.4. Obserwować działanie sniffera, określić czas ataku.
- 5.3. Przetestować możliwość pozyskania haseł z komputera zdalnego (zadanie wykonać jak w poprzednim punkcie (na komputerach **A** i **B**):
 - 5.3.1. Na komputerze **A** uruchomić program PWDUMP3 z konsoli CMD:
PWDUMP3 <Nazwa_komputera_B> <plik_wyjściowy> <konto>, a następnie podać hasło dla wybranego konta komputera **B**. W razie niepowodzenia uruchomić PWDUMP3 podając konto Administratora.
 - 5.3.2. Na komputerze **A** uruchomić program LC4, zamknąć okno kreatora, otworzyć nową sesję, wybrać *Import* → *Import From PWDUMP File ...* oraz 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;
 - 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 dyskietki:
 - wskazać właściwą partycję, zawierającą własną instalację systemu,
 - wskazać plik z bazą **sam** (standardowo *%systemroot%\system32\config\sam*),
 - nie wyłączać domyślnej dla Windows 2000 opcji szyfrowania postaci hash haseł (SYSKEY),
 - wpisać nowe hasło dla użytkownika Administrator.
 - 6.4. Uruchomić ponownie własną instalację W2K. Dokonać próby załogowania się na konto administratora podając zmienione hasło.
7. Zainstalować program **Iris** (Iris380Demo.exe). Dokonać próby przechwycenia i zdekodowania dowolnej sesji (pop3, telnet, ftp) między komputerami. Należy wykorzystać filtrowanie portów i dekodowanie sesji.
8. Sprawdzić możliwości odgadywania haseł wykorzystywanych w dostępie do zasobów w systemie Windows 98/Me. Próby przeprowadzić za pomocą wskazanego narzędzia tylko po uzyskaniu odpowiednich informacji od prowadzącego.

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 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.