

Łamanie haseł w Windows 2000

Grzegorz Orzechowski
orzechq@o2.pl

W Windows 2000 do otrzymywania hashy (nieodwracalnych skrótów haseł) wykorzystywany jest algorytm MD4 (tworzący skróty o długości 128 bitów). W procesie potwierdzania tożsamości użytkownika, z podanego hasła otrzymuje się wyciąg (hash), który następnie porównywany jest z zawartością przechowywaną na serwerze. Jeśli ciągi znaków są jednakowe, można przyjąć, że zostało wprowadzone prawidłowe hasło. Niestety okazało się, iż metoda ta nie zapewnia odpowiedniego poziomu bezpieczeństwa.

Jak włamywacz może uzyskać dostęp do pliku z hasłami?

Hashe przechowywane są w pliku %SYSTEMROOT%\SYSTEM32\CONFIG\SAM (co w przypadku normalnej instalacji Windows 2000 oznacza WINNT\SYSTEM32\CONFIG\SAM). Pierwotne dane tego pliku znajdują się w kluczu rejestru HKEY_LOCAL_MACHINE\SAM.

Włamywacz nie będzie miał bezpośredniego dostępu do tego pliku, podczas działania systemu (błąd współdzielenia pliku – ang. sharing violation). Jednak kopię pliku SAM może on znaleźć w katalogu \WINNT\REPAIR, jeśli tworzono w systemie dyski ratunkowe.

Gdy pilny administrator wykonuje swoje obowiązki i tworzy dyski awaryjne to włamywacz znajdzie tam skompresowaną kopię pliku SAM. Tutaj uwaga dla nieostrożnych administratorów – warto usuwać plik sam._. Najłatwiej przed możliwością pobrania sam._ można zabezpieczyć się odbierając użytkownikom prawa do katalogu \WINNT\REPAIR.

Aby uzyskać pełen dostęp do każdego pliku w systemie NTFS, włamywacz może wykorzystać narzędzie zwane NTFSDOS (albo dyskietkę startową z Linuksa z dostępem do NTFS). Może ono zostać użyte przez dowolną osobę z dyskietką startową i dostępem fizycznym do komputera. NTFSDOS wyszukuje dyski NTFS i daje do nich pełny dostęp (tylko w pełnej wersji, bezpłatna wersja daje dostęp tylko do odczytu). Do tego celu można także użyć linuksowego boot dysku z obsługą NTFS.

Włamywacz może jeszcze wyjąć dysk systemowy i podłączyć do innego komputera z zainstalowanym systemem Windows 2000 lub NT, co umożliwi mu odczytanie wszystkich plików i co najważniejsze - pliku SAM.

Obsługa i polecenia NTFSDOS

/L:... – ustawia literę dysku, od której ma zacząć montowanie NTFS 'a

/C: – ustawia rozmiar bufora XMS w KB (pozwala na nadpisanie domyślnego bufora XMS)

/N – wyłącza wspomaganie dla skompresowanych plików, wykorzystywane do optymalizacji poboru pamięci NTFSDOS 'a

/X – wyłącza wspomaganie dodatkowego przerwania INT13 w przypadku, gdy mamy problemy z BIOS'em

/V – podaje więcej informacji na temat dysków

Przykład:

```
NTFSDOS /L:GE /C:1024
```

Powyższe polecenie wymusza przypisanie litery G dla pierwszej partycji NTFS jaką znajdzie program NTFSDOS, a literki E dla drugiej partycji. Jeśli litera jest w danej chwili używana, partycja się nie podmontuje i pojawi się błąd. Dodatkowo, po tej komendzie program stworzy 1MB bufora XMS.

Co dalej z uzyskanym plikiem?

Mając plik z hasłami włamywacz będzie potrzebował wyciągnąć z niego hashe. W tym celu może posłużyć się narzędziem SAMDUMP, a uzyskane hashe "potraktować" narzędziem L0phtCrack. Warto jednak wiedzieć, że oba te zadania wykona LC w wersji 3.0, który wyciąga hash bezpośrednio z bazy SAM.

Wraz z wydaniem drugiego Service Pack'a firma Microsoft wzmocniła 56-bitowe szyfrowanie bazy SAM na 128-bitowe, aplikując systemowi narzędzie zwane SYSKEY (System Key Encryption of Password Information). Narzędzie to pozwala chronić klucze za pomocą 128-bitowego kodowania i odpierać dzięki temu ataki za pomocą takich programów jak PWdump, czy L0pht. Trzeba jednak wiedzieć, że już druga wersja PWdump (PWdump2) autorstwa Todda Sabina, potrafi sobie poradzić z zaawansowanym szyfrowaniem SYSKEY.

SYSKEY dotyczy następujących komponentów:

```
%systemroot%\system32\config\SAM
```

```
HKEY_LOCAL_MACHINE\SAM
```

```
%systemroot%\system32\config\security
```

```
HKEY_LOCAL_MACHINE\Security
```

Pwdump2 działa w trybie konsoli Windows 2000, wykonując zrzut hashy haseł z rejestru (również zdalnie), jednak tylko administrator ma prawo do korzystania z niego. Jeśli włamywacz miałby jego prawa i mógłby uruchomić program, to wykona zrzut do dowolnego pliku w formacie haseł UNIX (format zgodny z plikiem /etc/passwd), po czym wykorzysta go w programie L0phtCrack i złamie. PWdump2 stosuje ponadto (w przeciwieństwie do pierwszej wersji) tzw. 'zastrzyk DLL'.

L0phtCrack zyskał sobie największą sławę, spośród pokrewnych mu narzędzi pod Windows NT/2000, głównie dzięki specyficznej strategii działania. Ale warto zapoznać się z innym przedstawicielem programów z tej dziedziny - Advanced NT Security Explorer. Ten rosyjski program może pracować w Windows 9x i Me, ale tylko w systemach NT, 2000 oraz XP potrafi sam pozyskiwać skróty haseł, potrzebne do ich złamania.

L0phtCrack, który może skanować sieć, pod tym względem zdecydowanie przewyższa omawiany program. ANTEp potrafi wydobywać skróty z pamięci, ale musi wówczas pracować z uprawnieniami administratora. W przypadku korzystania z rejestru funkcja SYSKEY musi być wyłączona. Warto dodać, że program (podobnie jak L0pht) wykorzystuje pliki wygenerowane przez PWdump.