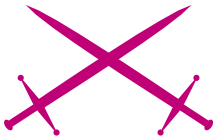


Wykorzystywanie tęczowych tablic do łamania haseł

Paweł Maziarz

stopień trudności

Znanym od dawna sposobem łamania haseł była metoda brute-force. Przy odpowiednio długim haśle była ona jednak co najmniej niepraktyczna. Jakiś czas temu Philippe Oechslin przedstawił nowe spojrzenie na łamanie pewnej grupy haseł, wprowadzając przy tym nowe narzędzie – tęczowe tablice (ang. Rainbow Tables).

Żeby zrozumieć istotę tęczowych tablic, trzeba wyjaśnić sobie kilka pojęć. Dziś w wielu systemach hasło użytkownika zapisywane jest jako jego skrót (tzw. hash), uzyskany poprzez użycie na haśle funkcji skrótu (ang. *hash function*). Funkcja skrótu to taka funkcja, która z dowolnie długiej wiadomości utworzy pewien ciąg znaków (zwykle o stałej długości), będący jej skrótem. Funkcje skrótu do zastosowań kryptograficznych powinny spełniać następujące kryteria:

- brak możliwości odtworzenia wiadomości (hasła) ze skrótu,
- brak możliwości wygenerowania dwóch różnych wiadomości o takim samym skrócie (brak kolizji),
- zmiana jednego bitu wiadomości powinna istotnie zmienić jej skrót.

Najbardziej popularne funkcje skrótu używane do przechowywania haseł to: SHA1, MD-2, MD-4, MD-5, LM, NTLM, MySQL-SHA1, RIPEMD-160, Cisco PIX. Za pomocą tych algorytmów hasła zapisywane są między innymi w bazie użytkowników MySQL, w systemie Windows, routerach Cisco oraz wielu aplikacjach. W ramce obok przedstawionych jest kilka hashy różnych funkcji skrótu z hasła hakin9.

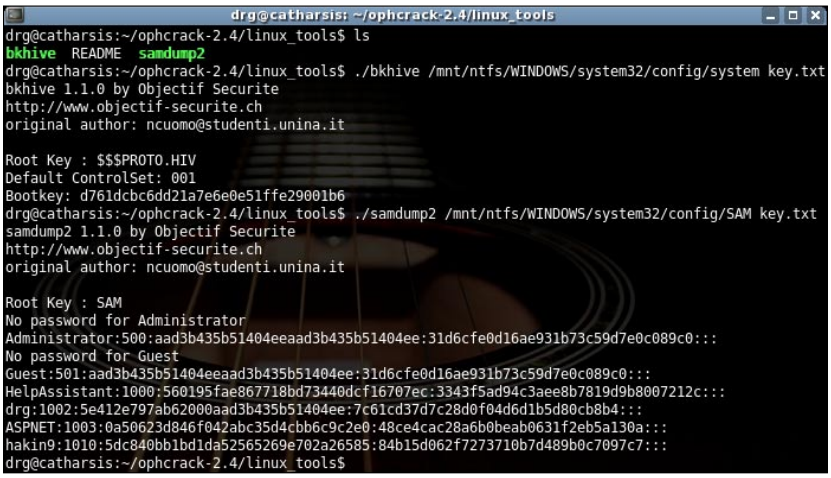
Druga funkcja leżąca u podstaw tęczowych tablic, o której należy wspomnieć, to funkcja redukcyjna. Działa ona niejako odwrotnie do funkcji skrótu, ponieważ z hasha tworzy ona hasło w czystym tekście (zawierające tylko określony zestaw znaków, np. tylko małe litery i cyfry). Uzyskane za jej pomocą hasło z hasha nie może być oczywiście hasłem, które dało określony hash (co wynika z własności funkcji skrótu), ale dzięki niej będą tworzone kolejne kombinacje hasła, które znowu zostaną potraktowane funkcją skrótu i porównane z hashem łamanego hasła.

Z artykułu dowiesz się

- co to są tęczowe tablice,
- jak dzięki nim złamać hasło do konta Windows, MySQL, Cisco PIX etc.

Co powinieneś wiedzieć

- powinieneś wiedzieć trochę o hasłach i metodach ich szyfrowania.



Rysunek 1. *Eksport zahashowanych haseł systemu Windows*

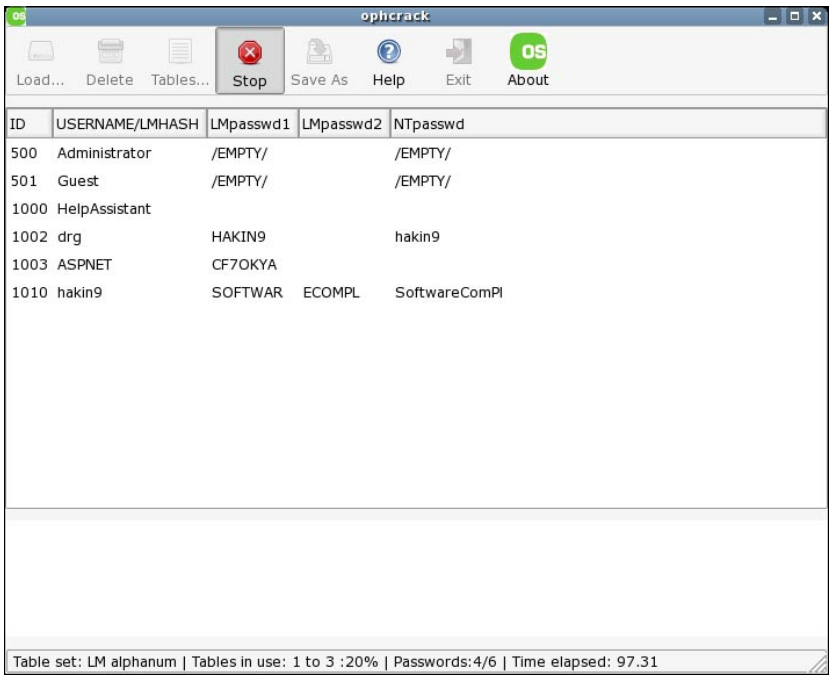
Tęczowe tablice – zasada działania

Jak zostało napisane wcześniej, funkcja skrótu użyta na haśle przedstawionym w postaci czystego tekstu, zwróci w wyniku jego hash. Na podstawie hasha nie jesteśmy w stanie odtworzyć hasła, a więc by złamać hasło musimy brać po kolei wszystkie możliwe hasła, pobierać ich skrót (hash), a następnie porównywać go z hashem hasła, które chcemy złamać. By skrócić czas takiego postępowania, można by zapisywać do pliku tak stworzone hashe i używać ich do łamania następnych haseł - jednak nietrudno ocenić, że plik zawierający taką tablicę haseł i ich hashy byłby ogromny, technicznie nie do pomieszczenia na dzisiejszych nośnikach danych.

Kompromisem między wykorzystaniem wcześniej przygotowanych hashy, a oszczędnością miejsca na dyskach są właśnie tęczowe tablice. Składają się one z łańcuchów (ang. *chains*) złożonych z haseł oraz ich hashy. Dla każdego łańcucha generowane jest hasło, z którego następnie wyliczany jest jego hash za pomocą funkcji skrótu. W następnym kroku, z tak otrzymanego hasha, za pomocą funkcji redukcyjnej tworzone jest kolejne hasło. Z tego hasła znów generowany jest hash, z hasha kolejne hasło. I tak dalej. W tęczowych tablicach zapisywany jest jednak tylko pierwszy i ostatni element łańcucha (hasło i ostatni hash), dzięki czemu tak stworzone tablice bez problemu mieszczą się na dzisiejszych dyskach twardych.

W celu odzyskania hasła, wczytywane są z tęczowych tablic hashe, następnie szukany jest w nich hash hasła, które chce się złamać. Jeżeli nie znaleziono, generowane jest hasło z łamanego hasha za pomocą funkcji redukcyjnej, z którego uzyskuje się następnie hash za pomocą funkcji skrótu i wraca do kroku poprzedniego znów porównując hashe. Kiedy hash zostaje w końcu znaleziony, brane jest początkowe hasło z łańcucha, w którym hash się znajdował, a następnie redukowane jest i skracane, aż uzyska się parę złożoną z hasła oraz jego skrótu w postaci szukanego hasha. Metoda ta jest równie prosta, co skuteczna.

Istnieje jednak jeden problem, który – paradoksalnie jako niepożądany przy funkcjach skrótu – zwiększa bezpieczeństwo generowanych hashy w kontekście tęczowych tablic. Chodzi o wspominane wcześniej kolizje, czyli sytuacje, kiedy wiele różnych wiadomości (haseł) daje w wyniku funkcji skrótu taki sam hash. W przypadku tęczowych tablic mogłoby się więc okazać, że łańcuchy, które zaczynają się różnymi hasłami, w okolicznościach wystąpienia kolizji w pewnym momencie zaczynają się pokrywać i w konsekwencji kończą się takim samym hashem. Mogą też wystąpić zapętlenia w przypadku, gdy hash został zredukowany do hasła, które zostało już otrzymane gdzieś wcześniej w danym łańcuchu. Problem ten został rozwiązany poprzez zastosowanie różnych funkcji redukcyjnych na całej drodze od początku łańcucha do jego końca. Dzięki temu, problem kolizji hashy w różnych łańcuchach został znacznie ograniczony, ponieważ w przypadku wystąpienia kolizji – o ile nie jest to kolizja w tej samej kolumnie – w kolejnym kroku hash zostanie zredukowany



Rysunek 2. *Łamanie haseł programem Ophcrack*

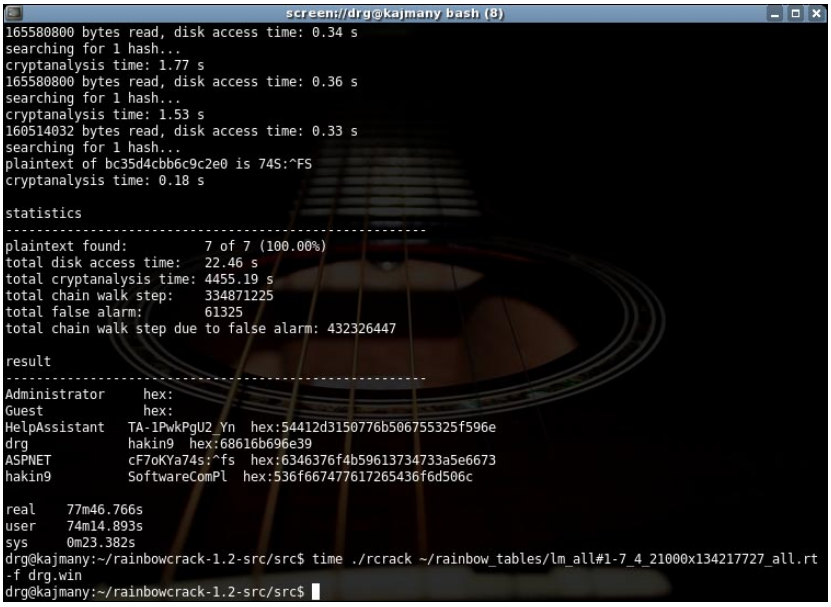
wany do innego hasła. Został tym samym wyeliminowany problem zapętleń wewnątrz jednego łańcucha, bo w każdym kroku hash redukowany jest inną funkcją.

Ten sposób rozwiązania omówionych problemów przyczynił się też do nazwy owych tablic. Jeżeli każdą funkcję redukcyjną w danym kroku oznaczyć innym kolorem, powstałaby wielka pionowa tęcza, a więc określenie tęczowych tablic jest zupełnie na miejscu.

Ophrack

Pierwszym narzędziem, które zostanie omówione jest program Ophrack napisany przez Philippe Oechslina. Jest to cracker haseł windowsowych działający w oparciu o tęczowe tablice. Jest on dostępny na platformy Windows, Linux oraz Mac. Potrafi łamać hasła zaszyfrowane algorytmami LM oraz NTLM. Dostępne za darmo są do niego tęczowe tablice zawierające hasła złożone z liter i cyfr dla algorytmu LM, bardziej wyszukane tablice można kupić na stronie projektu. Ciekawy jest fakt, że w oparciu o dystrybucję SLAX Linux stworzono *Ophrack LiveCD*, czyli dystrybucję Linuksa startującą wprost z napędu CD, która po wystartowaniu sama odnajdzie partycję z Windowsem, znajdzie i wyeksportuje sobie hasła użytkowników, po czym natychmiastowo zacznie je łamać, nie zostawiając po sobie żadnych śladów. Nie potrzeba znać hasła administratora Windows, ani mieć specjalnej wiedzy, wszystko robi się samo – wystarczy zbootować komputer z płyty CD.

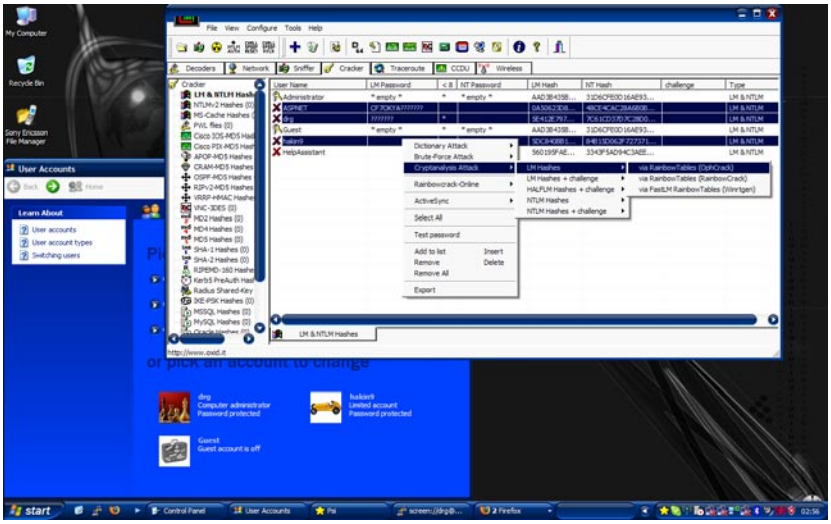
Uruchamiając program pod Windowsem i posiadając uprawnienia administratora, Ophrack pozwala wyeksportować hasła z bazy. W przeciwnym wypadku trzeba je uzyskać samemu poprzez użycie dołączonych poleceń *bkhive* oraz *samdump2* (Rysunek 1). Przykładowa sesja programu Ophrack, podczas której w niespełna kilkadziesiąt sekund poradził sobie z hasłami złożonymi z małych i dużych liter oraz cyfr, przedstawiona jest na Rysunku 2.



Rysunek 3. *Skomplikowane hasła złamane programem RainbowCrack*

RainbowCrack

Kolejnym ciekawym narzędziem jest aplikacja *RainbowCrack*. Jest to konsolowe narzędzie działające pod systemami Linux oraz Windows. Dzięki niemu można złamać hasła zahashowane algorytmami LM, MD5, SHA1 oraz dowolnym innym w miarę potrzeb, ponieważ łatwo można dodać obsługę własnego algorytmu. Oprócz właściwego crackera (*rcrack*), *RainbowCrack* posiada jeszcze narzędzia do tworzenia własnych tęczowych tablic (*rtgen*, *rtsort*, *rtdump*). Chociaż program nie ma graficznego interfejsu, używa się go szalenie łatwo – narzędzie wymaga dwóch parametrów: ścieżki do tęczowej tablicy oraz hashy do crackowania, które można podać wprost w linii komend (przełącznik -h), jako plik z listą hashy (-l) lub jako zrzut pliku z hasłami użytkowników (-f). Program w trakcie działania (z tęczowymi tablicami złożonymi z haseł zawierających małe i duże litery, cyfry oraz znaki specjalne) przedstawia Rysunek 3.



Rysunek 4. *Cain & Abel w akcji*

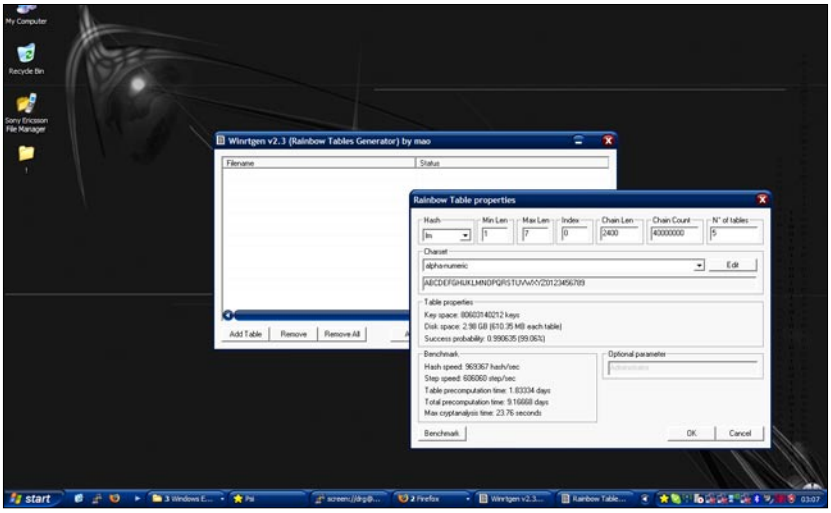
Cain & Able

Cain jest dobrze znanym narzędziem dla systemu Windows służącym do przywracania zapomnianych haseł za pomocą różnorakich technik – podsłuchiwania sieci, crackowa-

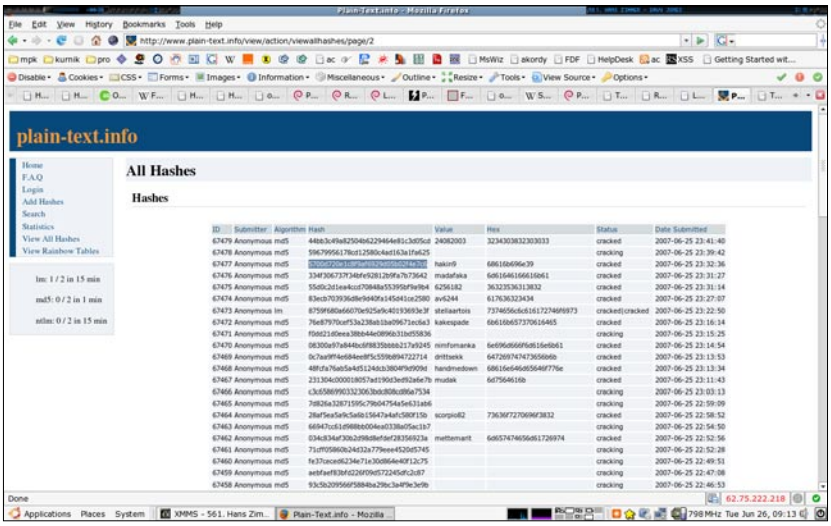
nia metodą brute-force, słownikową. Posiada on jeszcze wiele ciekawych funkcji, jednak w kontekście tego artykułu interesuje nas fakt, że potrafi łamać hasła korzystając z kryptoanalizy, między innymi używając tęczowych tablic. Program potrafi korzystać z tablic przeznaczonych zarówno dla programu *Ophrack*, jak i *RainbowCrack*. Jego użycie jest bardzo proste, sprowadza się tylko do wybrania użytkowników, dla których trzeba złamać hasło oraz zdefiniowania, z jakich tęczowych tablic chce się korzystać. W zależności od rodzaju tablic oraz stopnia skomplikowania samych haseł, w ciągu kilkudziesięciu sekund powinny ukazać się odszyfrowane hasła. Działanie programu przedstawione jest na Rysunku 4.

Przykładowe hashe hasła hakin9

- MD2: 6c335ceafc1ca2d9b701c0a503ebe29f,
- MD4: 60a6ba1557c83ffd6d40bbafa633963b,
- MD5: 5700d720e1c8f9af6929d05b02f4e7c6,
- SHA-1: c0132641f8f1acb0a74b249f441e0ebac18be386,
- SHA-2 (256): 42daba7642566324b9344c7e5a83a97da3fc5fa145fd6358132a-18804530de64,
- RIPEMD-160: 678e478a15637c67933731633ae73322b472aec2,
- LM: 5e412e797ab62000,
- NT: 7c61cd37d7c28d0f04d6d1b5d80cb8b4,
- MySQL-323: 42e0696a62ac975f,
- MySQL-SHA1: d6a98da6247cbaa40c436155203d104ef2865191,
- Cisco PIX: yvigbue7izydod6j.



Rysunek 5. *Generowanie tęczowych tablic za pomocą winrtgen*



Rysunek 6. *Łamanie hasła w serwisie plain-text.info*

Skąd wziąć tęczowe tablice?

Tęczowe tablice można pozyskać na 3 sposoby. Po pierwsze, można je wygenerować samemu. Służy do tego między innymi konsolowe narzędzie *rtgen* z wcześniej wspomnianego projektu *RainbowCrack* oraz okienkowy program pod systemy Microsoft o nazwie *winrtgen*. Uruchamiając ten pierwszy bez żadnych parametrów, uzyskamy dokładną informację o sposobie użycia wraz z kilkoma przykładami, drugi natomiast, posiadając bardzo przyjemny i przejrzysty interfejs (Rysunek 5), nie nastręczy trudności w generowaniu tablic nawet mało zaawansowanym użytkownikom.

Następny sposób na pozyskanie tęczowych tablic to ściągnięcie ich z Internetu. Jest kilka serwisów, które udostępniają je za darmo, na przykład *http://lasecwww.epfl.ch/~oechslin/projects/ophcrack/* (dwie podstawowe tablice dla programu *Ophrack*), *http://www.freerainbowtables.com/*, *http://rainbowtables.shmoo.com/*, *http://wired.s6n.com/files/jathias/*.

Ostatnim sposobem jest ich kupienie poprzez takie serwisy jak *http://www.rainbowcrack-online.com/*, *http://www.rainbowtables.net/* czy stronę projektu *Ophcrack* oraz wiele innych.

Łamanie haseł online

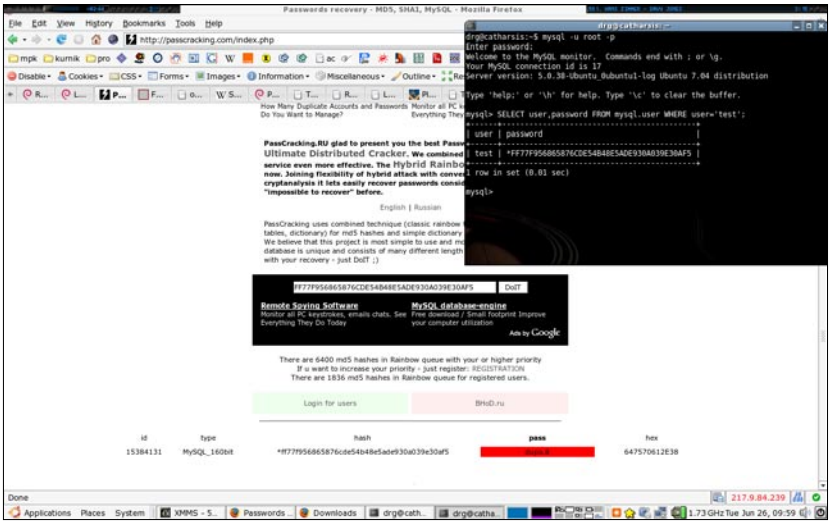
Tęczowe tablice są dziś już bardzo popularne, dlatego nikogo nie dziwi fakt powstania wielu serwisów internetowych umożliwiających łamanie hasła online. Istnieje wiele komercyjnych stron, które – po wniesieniu odpowiedniej opłaty – wykorzystując algorytm tęczowych tablic potrafią

odzyskać hasła kont windowsowych, użytkowników MySQL, routerów Cisco czy też zabezpieczonych dokumentów pakietu Microsoft Office. Istnieją też serwisy niekomercyjne, w których – ku uciesze wielu – można łamać hasła zupełnie za darmo, często z zupełnie zadowalającą skutecznością.

Jednym z takich serwisów jest plain-text.info. Dzięki niemu można odszyfrować hasło zakodowane algorytmami MD5, LM oraz NTLM. System wprawdzie przyjmuje po 2 hashe LM i NTLM co 15 minut oraz 2 MD5 co minutę, jednak w chwili pisania artykułu limity te są zupełnie nieodczuwalne przy łamaniu pojedynczych haseł. Po dodaniu hashy do serwisu i określeniu algorytmu, w jakim zostały utworzone, system wyszukuje czy hash został wcześniej złamany, jeżeli nie – tęczowe tablice idą w ruch i rozpoczyna się łamanie. Pozostaje już tylko co kilkanaście sekund odświeżać podstronę z wynikami (*View All Hashes*) i wypatrywać złamanego hasła w czystym tekście. Należy jednak pamiętać, że tak złamane hasła są widoczne przez wszystkich internautów, a więc również i my możemy zobaczyć hasła innych, co może mieć spore walory edukacyjne (Rysunek 6).

Kolejnym serwisem jest passcracking.com. Dzięki niemu można złamać hash MD5, SHA-1 oraz hasła użytkowników MySQL (MySQL-SHA1 i starszy MySQL-323). Po podaniu hasha system najpierw sprawdza, czy istnieje on już w bazie. Jeżeli istnieje, od razu zostanie wyświetlone hasło (tak jak na Rysunku 7), jeżeli nie, po kliknięciu przycisku *Send My md5 hash to Rainbow Cracker,* hash zostanie dodany do kolejki obliczeń. Na dzień dzisiejszy można dodawać do kolejki tylko hashe md5.

Inne serwisy łamiące hashe online bez opłat to między innymi *http://www.milw0rm.com/cracker/* oraz *http://md5crack.it-helpnet.de/.* Istnieje jeszcze wiele innych i wiele będzie jeszcze się tworzyć (a także znikać), dlatego najlepszym pomysłem jest wyszukanie ich dopiero wtedy, kiedy zajdzie taka potrzeba.



Rysunek 7. *Złamane hasło Mysql na passcracking.com*

W Sieci

- *http://lasecwww.epfl.ch/~oechslin/publications/crypto03.pdf* – idea tęczowych tablic opisana przez Philippe Oechslin-a,
- *http://kestas.kuliukas.com/RainbowTables/* – bardziej przyjazny opis tego tematu,
- *http://ophcrack.sourceforge.net/* – strona programu Ophcrack,
- *http://www.antsight.com/zsl/rainbowcrack/* – projekt RainbowCrack,
- *http://www.oxid.it/cain.html* – strona programu Cain & Abel.

O autorze

Autor jest właścicielem i jednocześnie jednym z głównych programistów firmy tworzącej między innymi oprogramowanie sieciowe. Na przełomie ostatnich lat współpracował z kilkoma firmami w charakterze Security Specialist. W wolnych chwilach gra w golfa, na gitarze klasycznej oraz spuszcza się na linie z budynków.
Kontakt z autorem: *pawel.maziarz@intersim.pl*

Podsumowanie

Jak widać, przechowywanie haseł w postaci ich hashy, powstałych w wyniku użycia funkcji skrótu, nie jest wcale tak bezpieczne, jak się to kiedyś wydawało. Dzięki tęczowym tablicom ich łamanie staje się całkiem szybkie, do tego coraz więcej firm (oraz niekomercyjnych grup) tworzy coraz to większe zbiory tęczowych tablic, które radzą sobie z haszami jeszcze szybciej. Jedną z metod obrony przed takimi atakami jest dodanie do hasła pewnej nadmiarowej, losowej informacji zwanej solą (ang. *salt*) i zapisanie jej w takiej postaci, by algorytm porównywania hasha z bazy z hashem hasła użytkownika ją uwzględnił. I tak na przykład podczas dodawania użytkownika do bazy, obok hasła mógłby zostać zapisany czas jego utworzenia i doklejony do końca hasła, więc hasło hakin9 zostałoby zapisane jako np. hash tekstu *hakin91182850495*. Przy logowaniu natomiast brane byłoby pod uwagę hasło podane przez użytkownika, do którego doklejana byłaby odpowiednia sól z bazy i dopiero wtedy hashowane. Ten prosty zabieg znacznie utrudniłby łamanie hasła, a w miarę zwiększania i komplikowania owej soli, nawet proste hasła mogłyby się okazać praktycznie niemożliwe do złamania metodami `brute-force` czy przy zastosowaniu tęczowych tablic. ●