Informacje

- **Kontakt:** katarzyna.mazur@umcs.pl
- **Konsultacje:** pokój 412 na 4 piętrze, przed konsultacjami proszę o wiadomość mailową
- **Zasady zaliczenia:** `https://kampus.umcs.pl/pluginfile.php/806844/mod_resource/content/1/zasady_zaliczenia_bsk_2022.pdf`
- **Materiały, aktualności, zmiany terminów zajęć:** `https://kampus.umcs.pl/course/view.php?id=20754`

Teoria

Kryptograficzne funkcje hashujące, zwane też funkcjami skrótu to algorytmy, które potrafią przekształcić dane dowolnej długości w krótki ciąg bajtów (zwykle, dla czytelności zapisywany w formacie szesnastkowym).

OpenSSL to wieloplatformowa, otwarta implementacja protokołów SSL (wersji 2 i 3) i TLS (wersji 1) oraz algorytmów kryptograficznych ogólnego przeznaczenia. Dostępna jest dla systemów uniksopodobnych (m.in. Linux, BSD, Solaris), OpenVMS i Microsoft Windows. OpenSSL zawiera biblioteki implementujące wspomniane standardy oraz mechanizmy kryptograficzne, a także zestaw narzędzi konsolowych (przede wszystkim do tworzenia kluczy oraz certyfikatów, zarządzania urzędem certyfikacji, szyfrowania, dekryptażu i obliczania podpisów cyfrowych). OpenSSL pozwala na używanie wszystkich zastosowań kryptografii.

Crunch jest jednym z najwygodniejszych narzędzi do tworzenia słowników z listami haseł. Pozwala on wygenerować wszystkie kombinacje, które możemy wykorzystać do testowania. Trzeba przygotować się na to, że wygenerowany przez crunch słownik będzie sporych rozmiarów.

John the Ripper został stworzony przez Solar Designer. Program na początku był opracowany dla systemu operacyjnego UNIX, aktualnie uruchamia się na piętnastu różnych platformach i obsługuję różne architektury sprzętowe. Jest to jeden z najpopularniejszych programów do łamania oraz testowania haseł. Jego fundamentalnym celem jest wykrycie słabych haseł będących najsłabszym ogniwem większości dzisiejszych serwerów. Dzięki temu narzędziu możemy zapobiec złamaniu słabego hasła przez intruza, nakazując danemu użytkownikowi, który posługuje się złamanym hasłem, jego zmianę z uwzględnieniem cech charakterystycznych mocnego hasła.

Base64 służy do kodowania ciągu bajtów za pomocą ciągu znaków. Kodowanie to przypisuje 64 wybranym znakom wartości od 0 do 63. Ciąg bajtów poddawany kodowaniu dzielony jest na grupy po 3 bajty. Ponieważ bajt ma 8 bitów, grupa 3 bajtów składa się z 24 bitów. Każdą taką grupę dzieli się następnie na 4 jednostki 6-bitowe, więc istnieją dokładnie 64 możliwe wartości każdej z tych jednostek. Jednostkom przypisywane są odpowiednie znaki na podstawie arbitralnie ustalonego kodowania (patrz tabela poniżej). Jeśli rozmiar wejściowego ciągu bajtów nie jest wielokrotnością liczby 3, to stosowane jest dopełnianie – na końcu wynikowego ciągu dodawana jest taka liczba symboli dopełnienia (ang. pad), aby ten miał długość podzielną przez 4.

Istnieje kilka różnych schematów uwierzytelniania, których można używać w systemach Linux. Najczęściej stosowanym i standardowym schematem jest przeprowadzanie uwierzytelnienia na ***/etc/passwd*** i ***/etc/shadow***. Ponieważ hasła użytkowników umieszczane są w pliku ***/etc/shadow***, konieczne jest połączenie obu plików w jeden. Użytecznym narzędziem łączącym oba te pliki jest narzędzie ***unshadow***.

/etc/passwd to plik, w którym informacje o użytkowniku (takie jak nazwa użytkownika, identyfikator użytkownika, identyfikator grupy, lokalizacja katalogu domowego, powłoka logowania, ...) są przechowywane podczas tworzenia nowego użytkownika.

/etc/shadow to plik, w którym ważne informacje (takie jak zaszyfrowana forma hasła użytkownika, dzień wygaśnięcia hasła, niezależnie od tego, czy hasło musi zostać zmienione, minimalny i maksymalny czas między zmianami hasła, ...) są przechowywane, gdy zostaje utworzony nowy użytkownik.

Zadania

1.1 Za pomocą narzędzia `rand` dostarczonego wraz z pakietem `OpenSSL`, wygeneruj 4 bitowe hasło i zakoduj go za pomocą Base64. Następnie, za pomocą narzędzia `OpenSSL`, wygeneruj hash MD5 tego hasła. Nie korzystaj z pomocniczych plików.

1.2 Korzystając z poleceń systemowych (np. `tr`, `head`, `cut`, `base64`) oraz pliku `/dev/urandom` wygeneruj bezpieczne hasło dla użytkownika (hasło ma mieć długość 16 znaków, nie może posiadać nie-alfanumerycznych znaków) a następnie wygeneruj, za pomocą narzędzia `OpenSSL`, funkcję skrótu MD5 dla wygenerowanego wcześniej hasła. Nie korzystaj z pomocniczych plików.

1.3 Korzystając z narzędzia `crunch`, wygeneruj do pliku listę haseł składających się z samych cyfr o długości 3 znaków. Zapisz je do pliku. Za pomocą narzędzia `OpenSSL` wygeneruj funkcje skrótu SHA-1 dla wszystkich wygenerowanych haseł.

1.4 Korzystając z narzędzia `crunch`, wygeneruj do pliku listę haseł o długości 5 znaków według wzoru, gdzie:

- pierwszy znak hasła to cyfra
- drugi znak hasła to mała litera *a*
- trzeci znak hasła to znak specjalny
- czwarty znak hasła to mała litera *b*
- piąty znak hasła to cyfra

Zapisz je do pliku. Za pomocą narzędzia `OpenSSL` wygeneruj funkcje skrótu SHA-3 dla wszystkich wygenerowanych haseł.

1.5 Korzystając z narzędzia `crunch`, wygeneruj do pliku listę haseł o długości 3 znaków według wzoru:

- pierwszy znak hasła to litera ze zbioru {`a, b, c`}
- drugi znak hasła to cyfra za zbioru {`4, 6, 8`}
- trzeci znak hasła to znak specjalny ze zbioru: {`?, %, :`}

Przykładowe hasła: `a4?, b6%, c8:, ....` Zapisz je do pliku. Za pomocą narzędzia `OpenSSL` wygeneruj funkcje skrótu SHA-3 dla wszystkich wygenerowanych haseł.

1.6 Za pomocą słownika `rockyou.txt` oraz programu JohnTheRipper, spróbuj złamać hash MD5 zapisany w pliku `hash16.txt`.

1.7 Za pomocą słownika `rockyou.txt` oraz programu JohnTheRipper, spróbuj złamać hash SHA-256 zapisany w pliku `hash17.txt`.

1.8 Ze strony `https://gparted.org/download.php` pobierz plik `gparted-live-1.3.1-1-amd64.iso`. Za pomocą `OpenSSL` sprawdź integralność pobranego pliku. (*Integralność polega na zapewnieniu, że przetwarzana informacja nie została w żaden sposób zmieniona. Zmiana taka może być przypadkowa (błąd podczas transmisji) jak i celowa (zmiana przez atakującego)*).

1.9 Napisz skrypt w języku Python, w którym wygenerujesz hash MD5 dowolnego ciągu znaków podawanego jako argument wywołania skryptu. Sprawdź poprawność wygenerowanego hasha porównując go z wynikiem otrzymanym przy pomocy `md5sum` lub `openssl`.

1.10 Napisz skrypt w języku Python, w którym wygenerujesz hash SHA-1 dowolnego pliku podawanego jako argument wywołania skryptu. Sprawdź poprawność wygenerowanego hasha porównując go z wynikiem otrzymanym przy pomocy `sha1sum` lub `openssl`.

1.11 Mając dany początkowy ciąg znaków zapisany w pliku `111.rand`, który następnie został zahashowany, określ, jaka funkcja skrótu została wykorzystana do utworzenia jego hasha, zapisanego w pliku `111.hash`.

1.12 Sprawdź, czy pliki `a.txt` oraz `b.txt` mają taką samą zawartość.

1.13 Wykonaj zadanie **1.6** za pomocą narzędzia `hashcat`.

1.14 Za pomocą słownika `rockyou.txt` oraz oprogramowania `JohnTheRipper` sprawdź jakie hasła mają użytkownicy `u1` i `u2` (plik `z2.shadow`). Hasła te mają charakter słów słownikowych.

1.15 Użytkownik ma hasło (plik `z5.shadow`) składające się z 3 dowolnych znaków. Jakie to hasło? Do rozwiązania zadania użyj oprogramowania `JohnTheRipper`.

1.16 Użytkownik ma hasło (plik `z6.shadow`) składające się z 5 dowolnych znaków. Jakie to hasło? Do rozwiązania zadania użyj oprogramowania `JohnTheRipper`.

1.17 W pliku `z7.shadow` jest wiersz z hasłem użytkownika `user1`. Hasło ma charakter słownikowy, przy czym jest zapisane w taki sposób, że niektóre litery zamienione są na cyfry i tak: każde wystąpienie małego ***a*** zamienione jest na ***@***, małego ***i*** na ***1***, małego ***e*** na ***3***. Ponadto hasło ma jeszcze na początku i na końcu znak ***#*** (hash). Do rozwiązania zadania użyj oprogramowania `JohnTheRipper`.

1.18 Wykonaj zadanie **1.14** za pomocą narzędzia `hashcat`.

1.19 Wykonaj zadanie **1.15** za pomocą narzędzia `hashcat`.

1.20 Wykonaj zadanie **1.16** za pomocą narzędzia `hashcat`.

1.21 Wykonaj zadanie **1.17** za pomocą narzędzia `hashcat`.

Linki

- https://pl.wikipedia.org/wiki/Potok_(Unix)
- https://manpages.ubuntu.com/manpages/impish/pl/man1/head.1.html
- https://manpages.ubuntu.com/manpages/impish/pl/man1/cut.1.html
- https://manpages.ubuntu.com/manpages/impish/pl/man1/base64.1.html
- https://manpages.ubuntu.com/manpages/impish/pl/man1/tr.1.html
- http://linuxwiki.pl/wiki/Tr
- https://linux.die.net/man/4/urandom
- https://unix.stackexchange.com/questions/324209/when-to-use-dev-random-vs-dev-urandom
- https://tools.kali.org/password-attacks/crunch
- https://www.openwall.com/john/
- https://www.openwall.com/john/doc/EXAMPLES.shtml
- https://www.openwall.com/john/doc/OPTIONS.shtml
- https://www.varonis.com/blog/john-the-ripper/
- https://www.soisk-me.pl/klasa-iii-linux/plik-passwd-i-shadow
- https://chameleonstales.blogspot.com/2019/04/co-to-jest-za-plik-etcpasswd-i-etcshadow.html
- https://docs.python.org/3/library/hashlib.html
- https://hashcat.net/hashcat/
- http://manpages.ubuntu.com/manpages/impish/man1/fcrackzip.1.html
- https://www.cyberpratibha.com/blog/add-kali-linux-repository/
- https://hashcat.net/wiki/doku.php?id=example_hashes
- https://miloserdov.org/?p=5477
- https://countuponsecurity.files.wordpress.com/2016/09/jtr-cheat-sheet.pdf