Zajęcia 12 Bezpieczeństwo haseł

Na tych zajęciach chciałbym żebyście Państwo zapoznali się ze sposobem zabezpieczania haseł na przykładzie haseł w systemie linuks. Będzie potrzebna:
dowolna dystrybucja linuksa oraz program john the ripper (https://www.openwall.com/john/ na wielu dystrybucjach linuksowych jest zainstalowany domyślnie, ale w razie czego instrukcja instalacji też jest na tej stronie)

Użytkownicy i hasła w linuksie
W linuksie żeby dodać nowego użytkownika możemy skorzystać z komendy
adduser nazwa_uzytkownika
hasło użytkownika możemy ustawić poprzez
passwd nazwa_uzytkownika
(będąc rootem, albo w zależności od dystrybucji dodając „sudo” na poczatku”)
informacja o nowym użytkowniku znajduje się w pliku /etc/passwd
...
test1:x:1001:1001:,,,:/home/test1:/bin/bash
…
drugie pole powinno zawierać hasło, ale dla bezpieczeństwa hasło jest przeniesione do pliku /etc/shadow:
test1:6gQiozw7Z$2XG1EJjVI6toQKpcCQwH/rslYq8jYDKWEOdQgbAGw1iyjlk8s2M6M./qsVuAFOnjQuXJurl3hpKlLn0MLSkDr0:18397:0:99999:7:::

hasło jest oczywiście zapisane tekstem niejawnym. Co więcej tworząc dwóch użytkowników i nadając im to samo hasło możemy zobaczyć, że zapisane hasło będzie wyglądało inaczej. To dlatego, bo proces zapisywania hasła polega na dodaniu do właściwego hasła tzw. soli (ang. salt), czyli losowej liczby z zakresu 0-4095 i potem policzenie funkcji skrótu (funkcja mieszająca, hash, to co mieliśmy na poprzednich zajęciach) hasła z solą. To właśnie ta funkcja skrótu jest zapisana i nie da się z niej w prosty sposób odtworzyć hasła.
Gdy użytkownik wpisuje hasło system dodaje do niego po kolei różne wartości soli: 0, 1, 2, … 4095 i sprawdza czy utworzony w ten sposób ciąg bajtów ma funkcję skrótu zgodną z tym co jest zapisane.

Sprawdzanie siły haseł
Ponieważ nie da się w prosty sposób odwrócić funkcji skrótu to jedynym sposobem na „złamanie” takiego hasła jest znalezienie hasła które ma taką samą funkcję skrótu. Zwykle powinno to być takie same hasło jakie wprowadził użytkownik, teoretycznie może zdarzyć się, że zupełnie inne hasło (z zupełnie inną solą) da taką samą funkcję skrótu a zatem również pozwoli dostać się do systemu, ale funkcje skrótu stosowane w kryptografii mają znikomo małe prawdopodobieństwo kolizji, więc nie musimy się tym zwykle martwić.

Żeby sprawdzić bezpieczeństwo haseł w systemie linuksowym próbujemy odgadnąć hasło i sprawdzić czy dla dowolnej soli zgadza się z zapisanym. Próbne hasła mogą być wybierane według trzech metod (które są używane również w programie John the Ripper):
1) „single crack” - hasło dobierane jest na podstawie danych o użytkowniku (np. różne kombinacje imienia, nazwiska, itd.)
2) metoda słownikowa – hasła wybierane są ze słownika, rozszerzeniem tej metody są przekształcenia które są stosowane na hasłach ze słownika (dopisanie czegoś, napisanie od tyłu, połączenie dwóch słów, …)
3) metoda „brutal force”, albo tryb inkrementacyjny – próbowanie wszystkich możliwości (czy słowa mają sens czy nie), ponieważ ta metoda jest bardzo wolna, to hasła dobierane są w sposób

optymalny, tj najpierw te przypominające prawdziwe słowa, a dopiero potem kompletnie losowe zbitki liter/cyfr.

John the ripper
żeby uruchomić program john the ripper potrzebujemy plik z hasłami
powinien mieć on format taki jak w pliku /etc/passwd, tylko, że na drugiej pozycji zamiast 'x' powinno być właściwe hasło (tak jak wyżej)
hasła można albo przekopiować ręcznie albo skorzystać z komendy
unshadow plik_passwd plik_shadow > hasla.txt

po czym sam program john the ripper uruchamiamy (w najprostszej opcji) przez
john hasla.txt

program ma różne opcje, najbardziej użyteczne to
--wordlist=slownik.txt zamienia domyślny słownik haseł na inny plik
--rules w przypadku dodania opcji –wordlist włącza testowanie przekształconych haseł
--fork=N liczy jednocześnie korzystając z N równoległych procesów
odnalezione hasła są wyświetlane na bieżąco, ale po wyjściu z programu można je wyświetlić ponownie przez opcję --show

Zadanie dla Państwa Część A do wykonania do 2020.06.03
Utworzyć 6 użytkowników o nazwach:
imie_nazwisko1
…
imie_nazwisko6
(gdzie „imie” i „nazwisko” to Państwa imię i nazwisko), wymyślić i nadać dla każdego hasło
po czym wyciągnąć z /etc/passwd informacje o użytkowniku i połączyć ją z hasłem z /etc/shadow

wynik dopisać do dokumentu google który dla Państwa przygotowałem
https://docs.google.com/document/d/1Rn7B6LdDNRG6gRCcNkKP9S2B5aJZjU08Mq9t1YjRwec/edit?usp=sharing

w dokumencie umieściłem dla Państwa kilku przykładowych użytkowników ode mnie, żebyście mogli Państwo potwierdzić format.

Uwaga: na wszelki wypadek proszę nie używać swoich prywatnych haseł, które są używane w innych miejscach.

Uwaga: wszyscy Państwo powinniście mieć prawo edycji tego dokumentu, więc proszę uważać żeby nie skasować przykładu ani nie skasować użytkowników wysłanych przez Państwa kolegów i koleżanki. Jeżeli ktoś boi się żeby jego użytkownicy nie zniknęli to przez „Plik->Historia zmian->Nazwij obecną wersję” może zaznaczyć wersję (proszę wpisać wtedy swoje imię i nazwisko) zaraz po swojej edycji, więc w razie czego będzie łatwo znaleźć zagubione linie.

Zadanie dla Państwa Część B do wykonania pomiędzy 2020.06.04 a 2020.06.07

W drugiej części zadania będziecie Państwo używać użytkowników i haseł przygotowanych przez Państwa kolegów i koleżanki, zatem może być ono wykonane dopiero po zakończeniu pierwszej części przez wszystkich.
Proszę ściągnąć z powyższego adresu listę wszystkich użytkowników z hasłami, zapisać ją do pliku tekstowego i przetestować bezpieczeństwo haseł korzystając z programu John the Ripper.
Proponuje uruchomić (i pozwolić pochodzić programowi przez jakiś czas) z domyślnymi opcjami, a potem zrobić to samo korzystając z własnoręcznie znalezionego słownika zawierającego polskie

wyrazy.

Uwaga: jeżeli hasło jest „mocne” to znalezienie go w ten sposób wymagałoby nierealistycznie długiego czasu obliczeniowego, więc proszę się nie martwić, że program będzie w stanie znaleźć tylko niektóre hasła. Generalnie im dłużej pozwolimy mu działać tym więcej haseł powinien znaleźć.

Wynik działania programu (czyli listę użytkowników i odpowiadających im haseł, może być w formacie takim jak zwraca john --show hasła.txt) proszę wysłać na mój adres e-mail:

Tytuł maila: Ochrona danych, grupa 2, 2020.06.01, IMIĘ NAZWISKO