Więcej niż 8 znaków

Jak słabe hasła i małe błędy w kodzie potrafią zdradzić nasze sekrety

Michał Komendera

Disclaimer

1. Opinie wyrażane podczas warsztatów to opinie moje własne - **nie** są to opinie mojego pracodawcy.

2. Treści ukazywane w czasie trwania warsztatów służą **tylko** celom edukacyjnym. Autor nie bierze **żadnej** odpowiedzialności za ewentualne wykorzystanie zdobytej przez uczestników wiedzy w sposób nieprawidłowy / niezgodny z prawem.

Tematyka

- Hasła
  - Co to jest hasło?
  - Jak przechowywane są hasła?
    - Przykład praktyczny
  - Omówienie metod wykorzystywanych do łamania haseł
    - Przykład praktyczny
- Analiza oprogramowania z wykorzystaniem inżynierii wstecznej
  - ASM - wprowadzenie
  - Wyjaśnienie zagadnienia przeprowadzania analizy złośliwego oprogramowania
    - Przykład praktyczny (CTF)

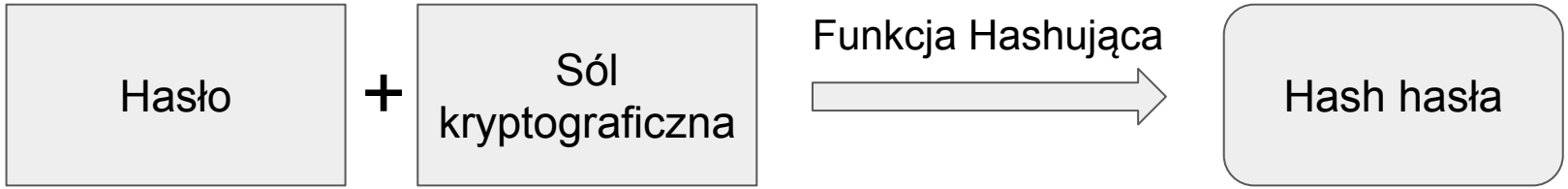
Część 1

Hasła

Wstęp teoretyczny

Hasło - (zazwyczaj krótki) ciąg znaków służący do uwierzytelnienia danego użytkownika w systemie/usłudze.

W klasycznym modelu (+salt):



Trochę soli, trochę pieprzu

Sól kryptograficzna - wartość (generowana losowo) dodawana do hasła (jeszcze jako tekst jawny) w celu zmniejszenia prawdopodobieństwa, że wynikowy hash hasła zostanie znaleziony we wcześniej przygotowanej tablicy tęczowej (rainbow table). Sól kryptograficzna przechowywana jest razem z wynikowym hashem (np. /etc/shadow).

Pieprz kryptograficzny - wartość (zazwyczaj generowana losowo) dodawana do hasła przed operacją hashowania w celu zmniejszenia ryzyka odgadnięcia hasła. Pieprz nie jest przechowywany z wynikowym hashem (implementation specific).

WebApp Auth

- Password stored in the Database
  - Hasła przechowywane są w postaci zahashowanej w bazie danych wykorzystywanej przez daną aplikację. Możliwe wykorzystanie soli i pieprzu kryptograficznego.
- Identity & Access Management (IAM)
  - Często zewnętrzny dostawca usług, który realizuje zadanie identyfikacji i uwierzytelnienia użytkownika na podstawie podanych danych. Przykładowy model przechowywania haseł: baza danych Active Directory.
- \+ Passwordless
  - Uwierzytelnienie bez hasła, przez posiadany przedmiot / dane biometryczne

Local OS Pass - Windows vs Unix-Like

- Windows
  - Hasła przechowywane są w rejestrze SAM (Security Account Manager) w postaci zaszyfrowanych hashów.
    Klucz do ich odszyfrowania znajduje się w rejestrze SYSTEM (jest nim wartość bootkey).

- Unix-Like (Linux)
  - Hasła przechowywane w pliku /etc/shadow w postaci hashów.
    Wcześniej można było je znaleźć w pliku /etc/passwd

Zadanie praktyczne #1

Zadanie praktyczne #1 - Windows

Zapis rejestru SYSTEM:

reg.exe save HKLM\SYSTEM systemRegDump.txt

Zapis rejestru SAM:

reg.exe save HKLM\SAM samRegDump.txt

Zadanie praktyczne #1 - Mac

Wygenerowanie UID użytkownika:

dscl localhost -read /Search/Users/<username> | grep GeneratedUID | cut -c15-

Odczyt hashu hasła:

cat /var/db/shadow/hash/<UID> | cut -c169-216

Metody wykorzystywane do łamania haseł

- Metoda Brute-Force
- Metoda Słownikowa
- Metoda tablic tęczowych (Rainbow Table)

Brute-Force

Polega na podstawianiu kolejnych znaków i rozszerzaniu powstałego ciągu aż do momentu znalezienia hasła.

Potencjalnie metoda brute-force jest w stanie złamać **każde** możliwe hasło.

Metoda Słownikowa

Polega na systematycznym przeszukiwaniu słownika - pliku, który zawiera w sobie określoną ilość haseł.

Rozmiary przeciętnych słowników wahają się od kilkuset MB, do kilkudziesięciu GB (ekstremalnie duże słowniki haseł mogą osiągać rozmiary liczone w setkach GB / terabajtach).

Metoda Tablic Tęczowych

Polega na systematycznym przeszukiwaniu tablicy tęczowej - pliku, który zawiera w sobie określoną ilość prekomputowalnych łańcuchów hashów i skorelowanych z nimi ciągów znaków.

Rozmiary przeciętnych tablic tęczowych wahają się od kilku GB, do nawet kilkuset GB.

Zadanie praktyczne #2

Część 2

Analiza oprogramowania z wykorzystaniem inżynierii wstecznej

Wstęp teoretyczny

Inżynieria wsteczna - proces badania działania oprogramowania / urządzenia w celu zdobycia informacji (np. o szczegółach implementacji).

W celu utrudnienia inżynierii wstecznej oprogramowania, twórcy mogą skorzystać z różnych metod obfuskacji kodu źródłowego, lub samego programu.

CTF?

Capture The Flag - zawody polegające na zdobyciu jak największej ilości ‘flag’ przez uczestników w przygotowanych wcześniej zadaniach (rozwój przez rywalizacje).

Flaga jest ciągiem znaków, którego znajomość informuje, że uczestnik zawodów był w stanie (złamać zabezpieczenie / wykorzystać podatność / bug w oprogramowaniu) == rozwiązać zadanie.

Zadanie praktyczne #3

Nic ciężkiego...

Malware - złośliwe oprogramowanie, które zostało stworzone w celu wykonania szkodliwej akcji w systemie informatycznym ofiary (pojedynczy komputer / sieć).

Dlaczego większość malware'u pisane jest w językach niższego poziomu, takich jak na przykład C/C++? -> Środowisko Uruchomieniowe

ASM

Assembly Language (ASM) - język programowania niskiego poziomu, nazywany inaczej symbolicznym kodem maszynowym.

Zadanie praktyczne #4

EOF

Q&A - jeśli mamy czas