JAK FUNGUJE

*SSHOLE

Ondřej Caletka | OpenAlt 2026 | listopad 2026

ANSWER TO THE ULTIMATE QUESTION OF LIFE, THE UNIVERSE, AND EVERYTHING

ALSO THE RESPONSE OF CRYPT(3) FUNCTION IN MUSL C LIBRARY FOR INVALID INPUT



0x 2A

2*16 + 10 = 42

0b 010 1010

JAK FUNGUJE PŘIHLAŠOVÁNÍ HESLEM

- Uživatel **zadá heslo**
- Heslo se předá do funkce **crypt(3)** knihovny jazyka C
- Výstup se porovná s hodnotou v **/etc/shadow**

POKROČILÉ HASHOVÁNÍ SE SOLÍ

- Heslo v /etc/shadow obsahuje preambuli s **označením algortimu** a **solí**
- Ověření hesla **dnes**:
  - Z /etc/shadow se vytáhne hash hesla
  - Funkce crypt(3) se zavolá s uživatelem zadaným heslem a hashem
  - Pokud je heslo správné, **funkce vrátí stejný hash**

JAK MŮŽE CRYPT(3) SELHAT?

- Hash hesla obsahuje **nepodporovanou hashovací** funkci (třeba 999)
- Uživatel zadá **velmi dlouhé heslo** (ochrana před DoS)

CO DĚLAT, KDYŽ CRYPT(3) SELŽE?

- Vrátit NULL
  - koncepčně čisté
  - ale aplikace neošetřující NULL spadne
- Vrátit **prázdný řetězec**
  - nebezpečné, mohlo by dojít k **nahodilé shodě**
- Vrátit **nárazníkovou hodnotu**, která nikdy nemůže být hash
  - * for musl
  - *0 pro glibc

JAK SSH ŘEŠÍ ZAMČENÉ ÚČTY

- **Dříve**
  - žádný hash, žádný přístup
- **Problém**
  - z trvání odpovědi lze zjistit, jestli účet **má hash** nebo ne
- **Nyní**
  - když účet nemá hash, půjčíme si hash z **jiného náhodného účtu**
  - takže to **trvá stejně dlouho**
  - výsledný hash **určitě nebude nikdy sedět**

JAK TO CELÉ FUNGUJE DOHROMADY

- Útočník se **přihlásí jako systémový účet** (nobody, daemon, …)
- SSH si půjčí hash z jiného účtu
- Funkce crypt(“dlouhé heslo”, “hash”) selže a vrátí “*”
- SSH porovná výstup s hodnotou **hashe systémového účtu**, která je taky “*”
- Systémový účet je **přihlášen**

CO PŘESNĚ SELHALO

- Rozhodnutí **nevracet** NULL, přestože je to standardní POSIXové chování
- Rozhodnutí použít “*” jako ***zaručeně neplatný hash***, který už se ale používá jako *zaručeně neplatný hash* s souboru /etc/shadow
- glibc později zavedlo nárazníkovou hodnotu “*0”

DÍKY ZA POZORNOST

ONDŘEJ CALETKA
HTTPS://ONDŘEJ.CALETKA.CZ
ONDŘEJ@CALETKA.CZ

Prezentace je už nyní k dispozici ke stažení