УДК 004.056.5

Букатка С. – ст. гр. СБс-32, Тимощук В. – ст. гр. КТ-21
*Тернопільський національний технічний університет ім. І. Пулюя*

# ХЕШ-АЛГОРИТМ ШИФРУВАННЯ ПАРОЛІВ КОРИСТУВАЧІВ ОС LINUX

Науковий керівник: Тимощук Д. І.

Bukatka S., Tymoshchuk V.
*Ternopil Ivan Puluj National Technical University*

# HASH ALGORITHM FOR ENCRYPTING PASSWORDS OF LINUX OS USERS

Supervisor: D. Tymoshchuk

Ключові слова: хеш-алгоритм, шифрування, Linux, пароль, операційна система.
Keywords: hash algorithm, encryption, Linux, password, operating system.

Шифрування паролів користувачів є важливою частиною безпеки операційної системи Linux. Для цього використовується алгоритм хешування, що перетворює пароль у набір символів.

У сучасних версіях операційних систем Linux, для хешування паролів користувачів використовуються алгоритми з хеш-функціями. Linux підтримує хеш-алгоритми MD5, SHA-256, SHA-512, Yescrypt, Blowfish та інші у своїй криптографічній бібліотеці. Проте, найбільш стійкими та безпечними є SHA-512 та Blowfish.

Blowfish працює з блоками даних фіксованого розміру (64 біти) за один раз, використовуючи режим шифрування Electronic Code Book (ECB) або інші режими, такі як Cipher Block Chaining (CBC) тощо, для захисту довільних розмірів даних. Довжина ключа може бути до 448 біт, що робить його стійким до атак на взлом.

SHA-512 є криптографічно стійким алгоритмом хешування, що забезпечує високий рівень захисту паролів. Він генерує фіксований хеш-код довжиною 512 біт (64 байти), який є унікальним для кожного вхідного паролю.

У хешуванні паролів, salt-механізм є важливою складовою для забезпечення безпеки паролів. Коли користувач створює новий пароль, система генерує випадкову послідовність символів, яка додається до пароля, що робить хеш-значення унікальним, навіть якщо два користувача використовують однакові паролі[1].

В Linux процес хешування паролю користувача відбувається в кілька етапів:

*1-й етап*: при створенні облікового запису користувача, система випадково генерує послідовність символів, яка додається до пароля перед його хешуванням;

*2-й етап*: введений пароль передається алгоритму хешування;

*3-й етап:* алгоритм обчислює хеш-значення пароля, додаючи до нього послідовність випадкових символів, створену на 1-ому етапі і виконуючи кілька ітерацій;

*4-й етап:* отримане хеш-значення пароля зберігається в файлі /etc/shadow;

*5-й етап:* під час наступного входу в систему, користувач знову вводить свій пароль, який проходить через той самий алгоритм хешування, що і при створенні облікового запису. Отримане хеш-значення пароля порівнюється зі збереженим в системі (якщо вони співпадають, користувачу надається доступ до системи).

Зашифровані паролі та інша інформація, наприклад, інформація про закінчення терміну дії пароля, зберігається у файлі /etc/shadow. Запис тіньового файлу показано на рисунку 1.

testuser:$y$j9TkBL8.2ofze0LeuOMUgg8v1$hJeNgoZRTTPC7yUSneFWUljgzw3q7qcp0o4Ub7YQ6l7:19407:0:99999:7:::

Рисунок 1 – Зразок із файлу /etc/shadow

1. testuser – ідентифікатор користувача.
2. **$y** – префікс алгоритму шифрування, який використовується для цього пароля (в даному випадку Yescrypt).
3. $**j9TkBL8.2ofze0LeuOMUgg8v1** – salt, яка використовується для шифрування пароля та вибирається випадковим чином.
4. $**hJeNgoZRTTPC7yUSneFWUljgzw3q7qcp0o4Ub7YQ6l7** – хеш-значення salt + пароль користувача "testuser".
5. :19407 – дата останньої зміни пароля (у форматі днів з 1 січня 1970 року).
6. :0 – мінімальна довжина пароля.
7. :99999 – максимальна дата, до якої пароль є дійсним (у форматі днів з 1 січня 1970 року).
8. :7 – кількість днів, після яких користувачеві потрібно змінити пароль.
9. ::: – роздільники, які вказують, що відсутня інформація про кількість днів введення невірного пароля, дату відключення або блокування користувача [2].

Незважаючи на те, що вихідний код для шифрування легкодоступний, не було виявлено (і оприлюднено) жодної методики зміни зашифрованого пароля назад у вихідний пароль. Таке розшифрування може навіть бути неможливим. Як наслідок, єдиний відомий спосіб подолати безпеку паролів Linux – це атака грубою силою або атака за словником. Атака за словником здійснюється шляхом вибору ймовірних паролів, як зі словника, їх шифрування та порівняння результатів із значенням, що зберігається в системі. Цей підхід до злому криптографічного шифру також називають пошуком ключа або зломом пароля [3].

Linux системи використовують алгоритм хешування, який використовує випадковість та одноразовість, що забезпечує неможливість відновлення вихідного пароля з хеш-значення. Цей підхід дозволяє зберігати паролі користувачів у захищеному вигляді та забезпечує безпеку облікових записів користувачів в системах. Однак, слабкий пароль може бути відгаданий або підібраний, навіть якщо його хеш-значення збережено у захищеному вигляді. Тому важливо використовувати складні паролі та регулярно змінювати їх, щоб уникнути можливості злому облікових записів користувачів через атаки на хеш-значення їх паролів.

**Список використаних джерел:**

1. How are passwords stored in Linux (Understanding hashing with shadow utils). slashroot.in // URL: https://www.slashroot.in/how-are-passwords-stored-linux-understanding-hashing-shadow-utils (дата звернення: 04.04.2023).
2. Understanding Linux /etc/shadow File Format. 2DayGeek // URL: https://www.2daygeek.com/understanding-linux-etc-shadow-file-format/ (дата звернення: 04.04.2023).
3. What is a dictionary attack? And how you can easily stop them. CSO Online // URL: https://www.csoonline.com/article/3568794/what-is-a-dictionary-attack-and-how-you-can-easily-stop-them.html (дата звернення: 05.04.2023).