ЛАБОРАТОРНА РОБОТА №8

ДОСЛІДЖЕННЯ АТАК НА ПАРОЛІ

Мета роботи:

1. Ознайомлення з принципами зберігання паролів у сучасних інформаційних системах.

2. Дослідження основних типів атак на паролі.

3. Отримання практичних навичок використання інструментів для відновлення паролів.

Інструменти та ПЗ: ВМ Kali Linux, hydra, john, hashcat, fcrackzip.

Теоретичні відомості

Основи зберігання паролів

У сучасних інформаційних системах паролі не зберігаються у відкритому вигляді. Замість цього використовується механізм хешування – одностороннього перетворення, яке перетворює пароль у фіксований рядок символів.

Хеш-функції мають такі властивості: вони є незворотними, детермінованими та чутливими до змін вхідних даних. Це означає, що навіть незначна зміна пароля призввдить до повністю іншого хешу.

У Linux-системах хеші паролів зберігаються у файлі /etc/shadow, доступ до якого мають лише привілейовані користувачі. Формат запису виглядає наступним чином:

```
username:$id$salt$hash
```

де $id визначає алгоритм хешування, salt – випадкове значення, а hash – результат обчилення.

Основні алгоритми, що використовуються:

1. MD5.
2. SHA-256.
3. SHA-512.

Salt – це випадкове значення, яке додається до пароля перед хешуванням. Використання sal дозволяє уникнути ситуації, коли однакові

паролі мають однакові хеші. Це значно ускладнює використання попередньо обчислених таблиць (rainbow tables).

Основні переваги використання salt:

1. Унікальність хешів навіть для однакових паролів.
2. Підвищення загальної стійкості системи автентифікації.

Типи атак на паролі

Атаки на паролі спрямовані не на злам криптографічного алгоритму, а на підбір правильного значення пароля.

Найбільш поширеними є наступні типи атак:

1. Dictionary attack (атака за словником) – використовує список найбільш поширених паролів і є швидкою та ефективною для слабких паролів.

2. Brute-force attack (повний перебір) – передбачає перебір усіх можливих комбінацій символів. Гарантує результат, але потребує значних обчислювальних ресурсів.

3. Mask attack – оптимізований варіант brute-force, який використовує шаблони для зменшення кількості варіантів.

Приклад маски:

?l?l?l?d?d – три малі літери та дві цифри.

Online та Offline атаки на паролі

Online атаки виконуються безпосередньо через сервіси автентифікації (наприклад, SSH або FTP). Вони обмежуються політиками безпеки, такими як блокування облікового запису або обмеження кількості спроб входу.

Offline атаки виконуються над отриманими хешами паролів. У цьому випадку відсутні обмеження на кількість спроб, що робить такі атаки значно ефективнішими.

Основні відмінності:

1. Online атаки легко виявляються системами безпеки.

2. Offline атаки не створюють записів у логах автентифікації.

3. Offline атаки дозволяють використовувати високопродуктивні обчислення (CPU/GPU).

Атаки на зашифровані файли

Файли, такі як ZIP-архіви та PDF-документи, можуть бути захищені паролем. У цьому випадку застосовується шифрування, яке робить вміст файлу недоступним без правильного ключа. Надійність такого захисту залежить переважно від складності пароля, а не від самого алгоритму шифрування.

Особливості атак на зашифровані файли:

1. Виконуються в offline режимі.
2. Не потребують взаємодії з сервером.
3. Ефективність залежить від довжини та складності пароля.

Слабкі паролі можуть бути відновлені за длопомогою словникових атак або перебору.

Інструменти для реалізації атак на паролі

Для реалізації атак на паролі використовуються спеціалізовані інструменти, які дозволяють виконувати як online, так і offline атаки. Вибір інструменту залежить від типу цілі (сервіс або хеш) та умов атаки.

Hydra

Hydra використовується для проведення online атак на мережеві сервіси шляхом підбору логіну та пароля.

Підтримувані сервіси:

1. SSH.
2. FTP.
3. HTTP/HTTPS (форми авторизації).
4. SMB.
5. Telnet.
6. RDP.
7. MySQL, PostgreSQL.

Загальний синтаксис:

```
hydra -l <login> -P <wordlist> <protocol>://<target>
```

Приклад використання:

1. Атака на SSH:

```
hydra -l admin -P passwords.txt ssh://192.168.1.10
```

2. Атака на FTP:

```
hydra -l user -P passwords.txt ftp://192.168.1.10
```

3. Атака на HTTP форму:

```
hydra -l admin -P passwords.txt 192.168.1.10 http-post-form
"/login:username=^USER^&password=^PASS^:F=incorrect"
```

Особливості інструмента Hydra:

1. Працює в режимі багатопоточності.
2. Може генерувати значний мережевий трафік.
3. Легко виявляється системами моніторингу.

John the Ripper

John the Ripper використовується для offline атак на хеші паролів та підтримує:

1. Хеші Linux.
2. ZIP, PDF тощо.
3. Різні алгоритми (MD5, SHA. bcrypt).

Загальний синтаксис:

```
john --wordlist=<wordlist> <hash_file>
```

Приклади використання:

1. Атака за словником:

```
john --wordlist=rockyou.txt hashes.txt
```

2. Перегляд знайдених паролів:

```
john --show hashes.txt
```

3. Інкрементальний (brute-force) режим:

```
john --incremental hashes.txt
```

Hashcat

Hashcat – це високопродуктивний інструмент для offline атак із підтримкою GPU.

Основні режими атак:

1. Dictionary attack.
2. Brute-force.
3. Mask attack.
4. Hybrid attack.

Загальний синтаксис:

```
hashcat -m <mode> -a <attack_mode> <hash_file> <wordlist>
```

Приклади використання:

1. MD5 (dictionary):

```
hashcat -m 0 -a 0 hashes.txt rockyou.txt
```

2. Brute-force:

```
hashcat -a 3 hashes.txt ?l?l?l?d?d
```

3. Hybrid attack:

```
hashcat -a 6 hashes.txt rockyou.txt ?d?d
```

Для детального ознайомлення з режимами хешів (-m) та типами атак рекомендується використовувати офіційну документацію Hashcat, яка містить повний перелік підтримуваних алгоритмів та їх ідентифікаторів.

Основне джерело: https://hashcat.net/wiki/doku.php?id=example_hashes

У цьому переліку наведені:

1. Типи хешів (MD5, SHA1, SHA256, bcrypt тощо).
2. Відповідні їм значення параметра -m.
3. Приклади хешів для тестування.

Наприклад:

1. -m 0 – MD5.
2. -m 1800 – SHA512 (Linux /etc/shadow).
3. -m 3200 – bcrypt.

Особливості використання Hashcat:

1. Дуже висока швидкість.
2. Підтримка GPU.
3. Велика кількість режимів хешів.

fcrackzip

fcrackzip використовується для підбору паролів до ZIP-архівів.

Синтаксис:

```
fcrackzip -u -D -p <wordlist> <archive.zip>
```

Приклад використання fcrackzip:

```
fcrackzip -u -D -p rockyou.txt secret.zip
```

Додатково (brute-force):

```
fcrackzip -u -b -c a1 -l 1-6 archive.zip
```

pdfcrack

pdfcrack використовується для відновлення паролів до PDF-документів.

Синтаксис:

```
pdfcrack -f <file.pdf> -w <wordlist>
```

Приклад використання pdfcrack:

```
pdfcrack -f file.pdf -w rockyou.txt
```

Brute-force:

```
pdfcrack -f file.pdf -n 4 -c abc123
```

Додаткові утиліти

Для підготовки хешів до подальшої атаки використовуються:

1. zip2john.
2. pdf2john.

Приклади використання:

```
zip2john archive.zip > hash.txt
pdf2john file.pdf > hash.txt
```

Ці утиліти дозволяють конвертувати захищені файли у формат, придатний для обробки в John the Ripper. Після отримання хешу наступним кроком є запуск атаки за словником або іншого типу атаки. Для цього отриманий файл з хешем передається у відповідний інструмент, наприклад:

```
john --wordlist=rockyou.txt hash.txt
```

Атака на паролі користувачів Linux за допомогою unshadow та Hashcat

У системах Linux паролі користувачів зберігаються у хешованому вигляді у файлі /etc/shadow, доступ до якого мають лише привілейовані користувачі. Для проведення атаки необхідно отримати відповідні файли конфігурації системи:

1. /etc/passwd – інформація про користувачів.
2. /etc/shadow – хеші паролів.

Оскільки інформація зберігається у розділеному вигляді, перед проведенням атаки необхідно об’єднати ці файли.

Інструмент **unshadow** використовується для об’єднання файлів /etc/passwd та /etc/shadow у формат, придатний для подальшої обробки інструментами для відновлення паролів.

Синтаксис команди unshadow:

```
unshadow passwd shadow > hashes.txt
```

У результаті створюється файл hashes.txt, який містить записи у вигляді:

```
username:$id$salt$hash
```

Після отримання хешів виконується офлайн-атака за допомогою інструменту Hashcat.

Для атак на хеші Linux (типу md5crypt або sha12crypt) використовується відповідний режим:

```
hashcat -m 500 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt
```

Де:

1. -m 500 – тип хешу (md5crypt, що використовується в /etc/shadow).
2. -a 0 – словникова атака.
3. rockyou.txt – словник паролів.

Завдання на лабораторну роботу:

Завдання 1. Локальна атака на хеші паролів ОС Linux.

1. Запустіть ВМ Kali Linux (збірка від Cisco).

2. Дізнайтеся IP-адресу вразливої машини Metasploitable2:

```
docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' metasploitable.vm
```

3. Підключіться до Metasploitable2 використовуючи SSH (логін/пароль: msfadmin/msfadmin):

```
ssh msfadmin@IP-адреса-Metasploitabe2
```

4. Після успішного підключення підвищіть рівень привілеїв до root шляхом виконання команди:

```
sudo su
# Пароль: msfadmin
```

5. Створіть нового локального користувача з **Вашим прізвищем** та паролем: **thunder515253ice**:

```
sudo adduser surname
```

6. Переконайтеся, що користувача створено:

```
cat /etc/passwd
```

7. Перегляньте файл /etc/shadow:

```
sudo cat /etc/shadow
```

8. Скопіюйте файли /etc/passwd та /etc/shadow в домашню директорію користувача msfadmin:

```
sudo cat /etc/shadow > /home/msfadmin/shadow
sudo cat /etc/passwd > /home/msfadmin/passwd
```

9. Відкрийте новий термінал в Kali Linux та виконайте завантаження файлів на локальну машину:

```
scp msfadmin@IP-адреса-Metasploitable2:/home/msfadmin/shadow .
scp msfadmin@ IP-адреса-Metasploitable2:/home/msfadmin/passwd .
```

10. Переконайтеся, що файли успішно завантажені (ls, cat).

11. Витягніть лише потрібні записи для подальшої реалізації атаки на пароль:

```
grep '^surname:' passwd > user_passwd
grep '^surname:' shadow > user_shadow
```

12. Об’єднайте отримані файли (user_passwd, user_shadow) у формат, придатний для підбору паролів, використовуючи інструмент **unshadow** (див. теоретичні відомості).

13. Виконайте словникову атаку на відновлення пароля із файлу з хешем, створеним у п. 12, використовуючи інструмент **hashcat** та наступні параметри:

- Параметр -m 500.
- Параметр -a 0.
- Файл із хешем, створений у п. 12
- Словник: **/usr/share/wordlists/rockyou.txt**.

14. Переконайтеся, що пароль новоствореного користувача успішно відновлено.

Завдання 2. Онлайн-атака на мережеві сервіси (кімната TryHackMe).

1. Увійдіть в обліковий запис на платформі TryHackMe та перейдіть до кімнати Hydra:

```
https://tryhackme.com/room/hydra
```

2. На ВМ Kali Linux підключіться до VPN (інструкція в ЛР№8).

3. Натисність “Join Room” для розблокування завдань та запустіть вразливу машину, натиснувши на “Start Machine”.

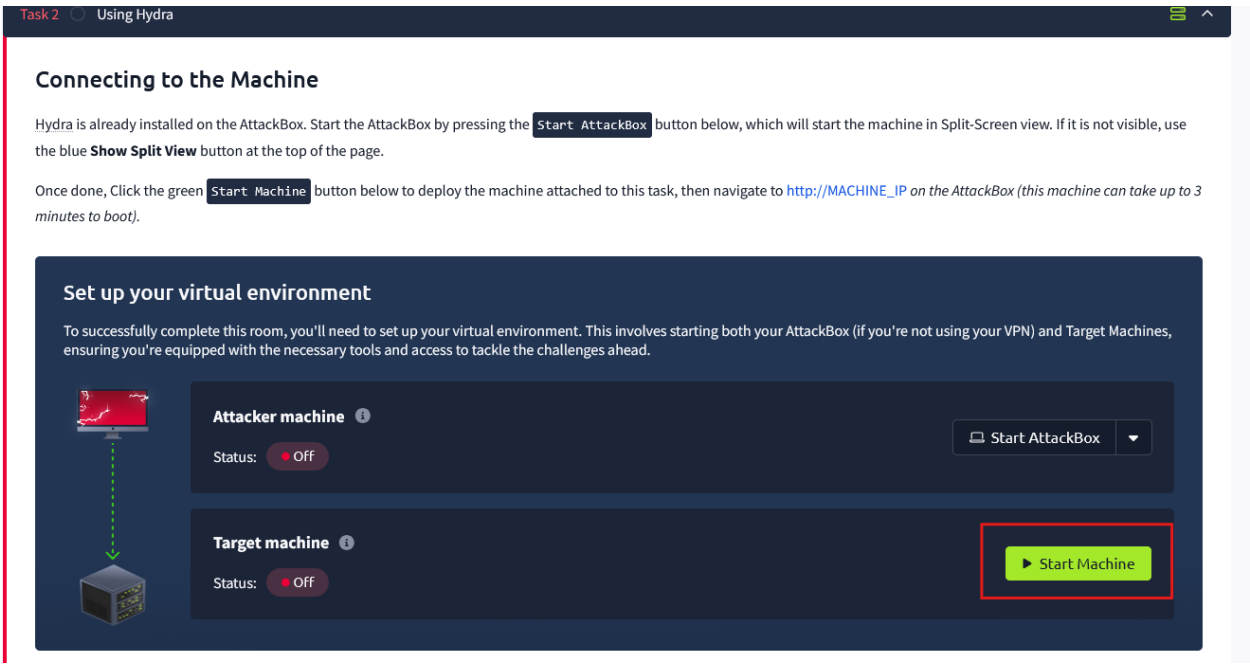

Рисунок 1 – Запуск вразливої машини

4. Ознайомтеся з теоретичною частиною кімнати.

5. Отримайте IP-адресу вразливої машини.

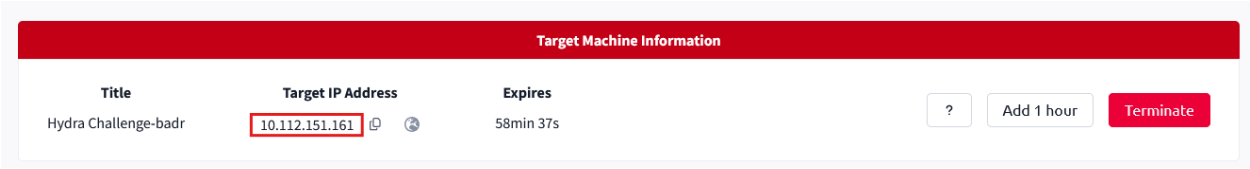

Рисунок 2 – Приклад отримання IP-адреси вразливої машини

6. Перевірте доступність IP-адреси вразливої машини шляхом виконання команди ping.

7. За допомогою браузера в Kali Linux перейдіть до вебсайту, використавши IP-адресу вразливої машини:

http://IP-адреса-машини

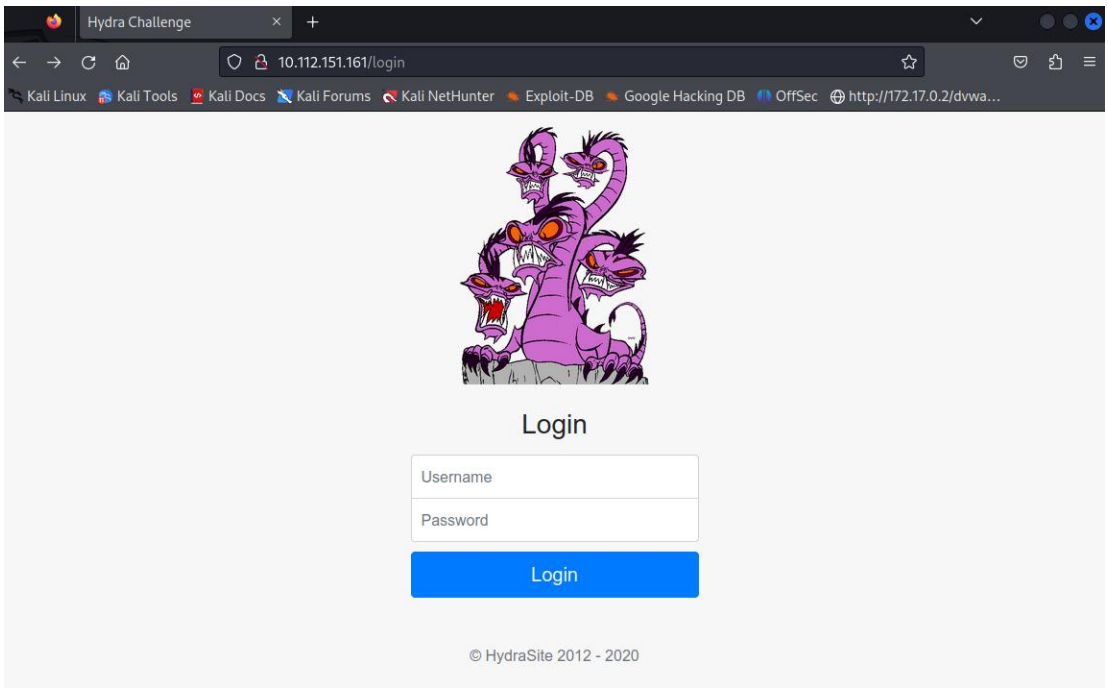

Рисунок 3 – Приклад вразливої вебсторінки

8. Виконайте розпакування словника rockyou.txt для подальшої реалізації атаки на пароль командою:

sudo gunzip /usr/share/wordlists/rockyou.txt.gz

9. Для виконання першого завдання на платформі TryHackMe та захоплення першого прапору реалізуйте атаку на форму логіну вебсторінки за допомогою інструмента Hydra, використовуючи наступні параметри:

- **Username:** molly

- **IP-адреса:** IP-адреса розгорнутої машини.

- **Словник:** /usr/share/wordlists/rockyou.txt

- **Параметр:** -t 50 – для збільшення кількості потоків та прискорення процесу підбору пароля.

10. Увійдіть в обліковий запис користувача molly на вебсайті, використовуючи пароль, отриманий в результаті виконання перебору.

11. Отримайте прапор №1 (THM{***}) та підтвердіть виконання першого завдання на платформі TryHackMe.

12. Для виконання другого завдання на платформі TryHackMe та захоплення другого прапору реалізуйте атаку на сервіс SSH за допомогою інструмента Hydra, використовуючи наступні параметри:

- **Username:** molly

- **IP-адреса:** IP-адреса розгорнутої машини.

- **Словник:** /usr/share/wordlists/rockyou.txt

13. Після успішного підбору пароля, підключіться до SSH вразливої машини, використовуючи логін **molly** та пароль, підібраний в результаті реалізації атаки (п. 12):

ssh molly@IP-адреса-машини

14. Після успішного підключення по SSH, перегляньте файли на сервері та виведіть вміст текстового файлу для отримання прапора №2.

15. Підтвердіть виконання другого завдання, скопіювавши прапор на платформу TryHackMe.

16. Вийдіть з SSH-сесії командою **exit**.

17. Залиште VPN-підключення активним для виконання завдання №3.

Завдання 3. Відновлення паролів зашифрованих файлів (кімната TryHackMe).

1. Перейдіть до кімнати Passwords - A Cracking Christmas на платформі TryHackMe:

https://tryhackme.com/room/attacks-on-ecrypted-files-aoc2025-asdfghj123

2. Натисність “Join Room” для розблокування завадань.

3. Запустіть вразливу машину, натиснувши “Start Machine”.

4. Дочекайтеся розгортання машини (1 хв). В результаті розгортання отримайте повну інформацію для підключення до машини з використанням SSH.

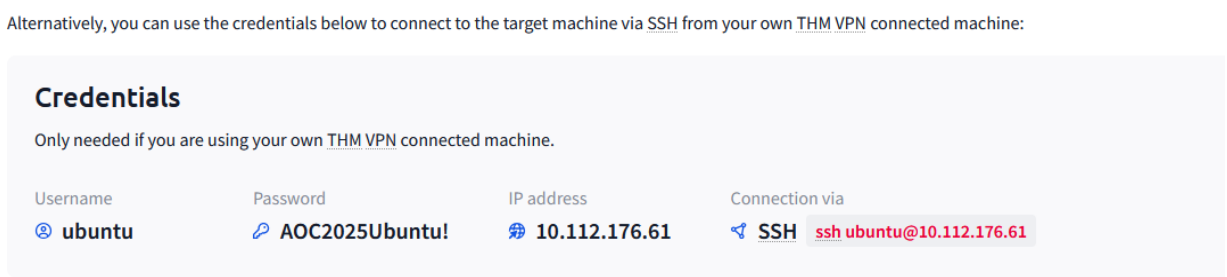

Рисунок 4 – Приклад інформації для підключення по SSH

5. Використовуючи термінал Kali Linux та дані з платформи TryHackMe, виконайте підключення до машини по SSH.

6. Ознайомтеся з теоретичною частиною кімнати.

7. В SSH-сесії перейдіть до каталогу **Desktop** та перегляньте його вміст за допомогою команди **ls**.

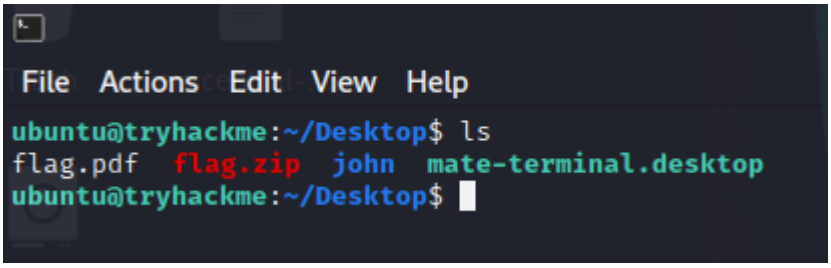

Рисунок 5 – Перелік файлів на сервері

8. Спробуйте відкрити PDF файл, використовуючи інструмент pdftotext та випадковий пароль (в даному випадку пароль – “test”):

```
pdftotext -upw "test" flag.pdf -
```

9. Реалізуйте перебір пароля для отримання доступу до вмісту PDF файлу, використовуючи інструмент **pdfcrack** та словник **/usr/share/wordlists/rockyou.txt**

10. Використайте підібраний пароль для отримання доступу до вмісту PDF файлу та захоплення прапора №1:

```
pdftotext -upw "підібраний-пароль" flag.pdf -
```

11. Скопіюйте прапор №1 на платформу TryHackMe для зарахування першого завдання.

12. Спробуйте розархівувати ZIP-архів flag.zip, використовуючи випадковий пароль:

```
7z x flag.zip
```

13. Використайте інструмент **zip2john** для отримання хешу ZIP-архіву (див. теоретичні відомості) та його запису в текстовий файл.

14. Переконайтеся, що хеш успішно додано до текстового файлу.

15. Реалізуйте атаку за словником на хеш, використовуючи інструмент **john** та отримайте підібраний пароль.

16. Розархівуйте ZIP-архів flag.zip, використовуючи підібраний пароль:

```
7z x flag.zip
```

17. В результаті успішного розархівування прочитайте вміст текстового файлу flag.txt для отримання прапора №2.

18. Скопіюйте прапор №2 на платформу TryHackMe для зарахування другого завдання.

19. Вийдіть з SSH-сесії командою **exit**.

20. Поясніть роль утиліти zip2john у процесі відновлення пароля. Чому інструмент john не може проводити атаку безпосередньо на файл .zip?

Контрольні запитання

1. Що таке хешування пароля?
2. Де в Linux зберігаються хеші паролів?
3. Яке значення має поле salt у хеші?
4. Який тип атаки використовує список готових паролів?
5. Яка атака передбачає перебір усіх можливих комбінацій?
6. Який інструмент використовується для онлайн атак?
7. Яка команда об’єднує файли /etc/passwd та /etc/shadow?
8. Який параметр у Hashcat відповідає словниковій атаці?
9. Що означає параметр -m 500 у Hashcat?
10. Який інструмент використовується для атаки на ZIP-архіви?
11. Яка команда використовується для підбору пароля в John the Ripper?
12. Який файл містить інформацію про користувачів у Linux?