????????? ????????????? ???????

Получение легитимного доступа - доступ к системе без изменений системы, используя существующие учетные данные и способы доступа к системе.

Плюсы	Минусы
• Наименее заметный, так как в систему не вносится никаких изменений. • Может предоставлять доступ достаточно долго, если компрометация системы не обнаружена.	• При компрометации обычно меняют пароли и ключи доступа. • Лучше совмещать его с другими подходами, так как при обнаружении использования инвазивных методов закрепления теряется и данный способ закрепления. • Учетные данные могут быть изменены по воле оператора системы.

Способы получения легитимного доступа к системе:

- Извлечение паролей и ключей из доступных файлов в ОС
- Восстановление паролей из хешей
- Подбор паролей методом перебора
- Восстановление паролей и ключей из памяти процессов

Восстановление паролей из хэшей

JohnTheRipper

```
$ sudo cp /etc/shadow /tmp/shadow
$ sudo unshadow /etc/passwd /tmp/shadow > /tmp/unshadowed
$ john /tmp/unshadowed
```

Hashcat

Поддерживает MD5, SHA1, SHA256, bcrypt и т.д. Пример взлома MD5:

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

Параметры

-m 0	алгоритм хеширования MD5

-a 0	атака перебора
hash.txt	файл с хешами паролей
/usr/share/wordlists/rockyou.txt	используемый словарь для перебора паролей

Радужная таблица

Специальный вариант таблиц поиска для обращения криптографических хеш-функций, использующий механизм разумного компромисса между временем поиска по таблице и занимаемой памятью. Предварительно вычисляются радужные таблицы, которые затем используются для быстрого нахождения паролей, соответствующих хэшам. Подробнее тут.

Онлайн-сервисы

Подробнее

Подбор паролей методом перебора

Минус состоит в необходимости предустановить инструмент на машину для обеспечения большей скорости обращений, что с высокой долей вероятности будет заметно командой реагирования и отразится в журналах аудита.

Можно использовать nmap, patator или hydra, ... Лучше в виде портативных файлов для вашей версии ОС. Пример для patator:

```
patator ssh_login host=192.168.0.1 user=admin password=FILE0 0=/путь/к/файлу_с_паролями.txt -x ignore:fgrep='Permission denied'
```

Пример для nmap:

```
nmap --script ssh-brute --script-args userdb=usernames.txt,passdb=passwords.txt <target>
```

--script ssh-brute – указывает использование скрипта для перебора паролей ssh.
--script-args userdb=usernames.txt,passdb=passwords.txt – указывает на файлы, содержащие список пользователей и паролей соответственно.
<target> – целевой IP-адрес или диапазон адресов.

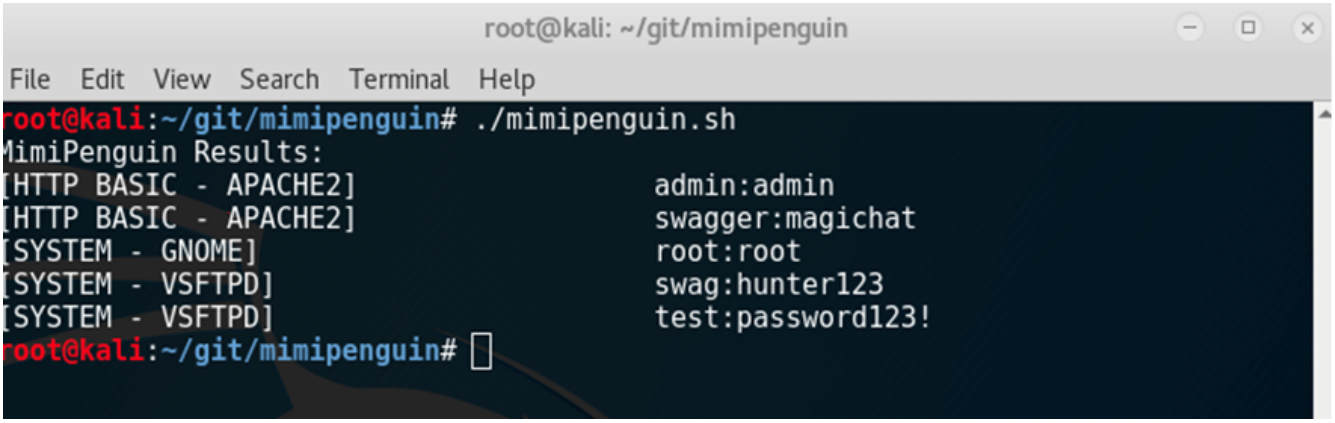
Прекомпилированный бинарный файл nmap тут.

Восстановление паролей и ключей из памяти процессов

В Linux сложнее чем в Windows.

Mimipenguin

Перехват паролей из памяти процессов на Linux-системе. Обычно используется для получения паролей, введенных пользователем в терминал, например, паролей от системы или приложений. После запуска Mimipenguin начнет мониторить процессы в системе и попытается извлечь пароли из памяти процессов. Пароли отображаются в терминале.



truffleproc

Инструмент для перехвата паролей из памяти любых процессов работающих в системе Linux, который ищет пароли и ключи API в процессах по регулярным выражениям выполняя выгрузку памяти процесса и анализируя ее. Ссылка на инструмент

Ручной способ

Нужно найти процесс аутентификации:

```
# ps -ef | grep "authenticator"
> root 2027 2025 0 11:46 ? 00:00:00 authenticator
```

Сделать дамп процесса (например, memory-dump) и поискать учетные данные в памяти:

```
# ./dump-memory.sh 2027
# strings *.dump | grep -i
```

Прочие подобные утилиты:

3snake – перехват паролей ssh, sudo и su (experimental)
SSHPry2.0 – перехват данных в терминале
Gimmecredz – дамп паролей в памяти (на основе bash)

Revision #2
Created 5 October 2025 18:31:09 by Admin
Updated 6 October 2025 15:26:36 by Admin