Подбор паролей. – Telegraph

telegra.ph/Podbor-parolej-06-28

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint June 28, 2024

Сегодня поговорим про подбор паролей. Существует два основных метода подбора: Brute-force и Password Spraying.

Брут-форс имеет много видов, но, в основном, это попытка использовать большое количество паролей с наименьшем количеством учетных записей или даже с одной учетной записью.

С другой стороны, Password Spraying представляет собой полную противоположность. Данная атака предполагает использование одного и того же пароля для взлома нескольких учетных записей. Испытав комбинации с одним паролем, злоумышленник переходит к другому. Такие атаки нередко бывают успешными, поскольку многие пользователи защищают свои аккаунты простыми паролями, которые несложно подобрать, например password, 123456 и так далее.

Во многих организациях действует политика блокирования учетной записи сотрудника после нескольких неудачных попыток входа. Использование одного пароля в комбинации с разными логинами позволяет избежать блокирования учетных записей, как в случае классического брутфорса, когда злоумышленник пытается войти в один аккаунт с разными паролями.

В цикле статей про OSINT мы писали о том, что много полезной информации о компании можно получить из открытых источников. Таким образом изучив профили сотрудников на LinkedIn, GitHub, X, и прочих социальных сетях, атакующий может составить список возможных пользователей по корпоративной модели, например firstname.lastname@companyname.com, и найти информацию об их интересах, которая может пригодиться для генерации словарей для Brute-force атаки.

После получения списка пользователей можно приступать к распылению паролей (конечно, учитывая парольную политику, пробуя одну попытку в некоторое время, во избежание блокировки учетной записи). Можно пробовать такие пароли:

Qq123456, Aa123456, Aa123456!@#;

!QA2ws3ed, !234Qwer, @WSX3edc;

P@ssw0rd, P@ssw0rd1, P@ssw0rd!;

Summer2024, Summer2023, June2024;

В большинстве случаев никто не использует эти простые пароли, но здесь работают законы теории вероятности – чем больше попыток (пользователей в списке), тем выше суммарная вероятность подобрать даже такой простой пароль.

Самый простой способ выполнить Password Spraying – применить инструмент CrackMapExec:

```
cme smb 192.168.1.101 -u /path/to/users.txt -p Summer2024 --continue-on-success
```

Данная команда проверит всех пользователей из списка "users.txt", подставив пароль "Summer2024". Параметр "--continue-on-success" отвечает за то, чтобы процесс не прервался после нахождения валидной пары.

Для проведения Brute-force атаки выполните команду:

```
cme smb 192.168.1.101 -u /path/to/users.txt -p /path/to/passwords.txt --local-auth
```

Данная команда проверит всех пользователей из списка "users.txt", подставив все пароли из списка "passwords.txt". Параметр "--local-auth" отвечает за прохождение аутентификации локально (не доменная учетная запись).

```
cme smb 192.168.1.101 -u /path/to/users.txt -p /path/to/passwords.txt --no-
bruteforce --continue-on-success
```

Данная команда проверит всех пользователей из списка "users.txt", подставив пароль соответствующий пароль из списка "passwords.txt". Параметр "--no-bruteforce" отвечает за установление соответствия между пользователем и паролем, таким образом можно легко найти валидные учетные данные из большого списка, когда одному пользователю принадлежит только один определенный пароль.

Вот еще несколько популярных инструментов для подбора паролей:

Metasploit - это многофункциональный инструмент для тестирования на проникновение, который имеет модули для подбора паролей и поддерживает различные протоколы и сервисы.

Hydra - мощный инструмент для атаки на пароли, который поддерживает различные протоколы, такие как HTTP, HTTPS, FTP, SMB и другие.

LEGBA - многопротокольный брутфорсер учетных данных на языке Rust.

Medusa - еще один инструмент для атаки на пароли, который также поддерживает различные протоколы.

Ncrack - инструмент для взлома паролей SSH, RDP, FTP и так далее. Имеет возможность многопоточного сканирования.