Отчёт о выполнении индивидуальный проект Этап 3””

Использование Hydra

Акондзо Жордани Лади Гаэл

Содержание

# Цель работы

Научиться основным способам тестирования веб приложений

# Задание

* Найти максимальное количество уязвимостей различных типов.
* Реализовать успешную эксплуатацию каждой уязвимости.

# Теоретическое введение

**Hydra** — это мощный инструмент для атаки методом перебора (грубой силы) на различные сервисы, включая веб-формы HTTP. В этом этапе мы будем использовать Hydra для проверки безопасности формы аутентификации в приложении **DVWA**.

# Выполнение лабораторной работы

## Подготовка: Список Паролей

* Для выполнения атаки Hydra необходим список паролей.
* **rockyou.txt** — один из самых популярных списков паролей в Kali Linux: (рис. 1).

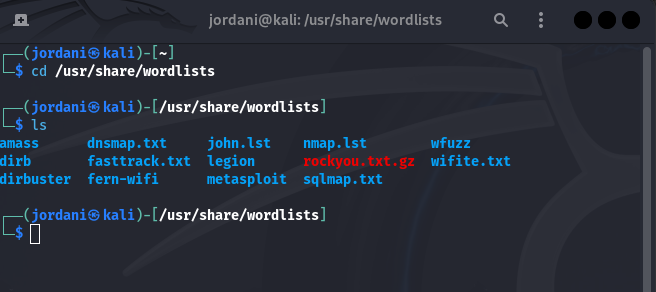


Рис. 1: Подготовка списока Паролей

* Сначала распаковал файл (рис. 2).

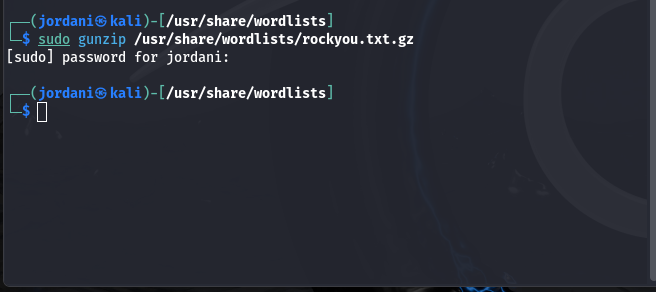


Рис. 2: Подготовка списока Паролей

## Команда Hydra для Атаки на HTTP Форму

* Для выполнения атаки на форму аутентификации DVWA использовал следующую команду (рис. 3).

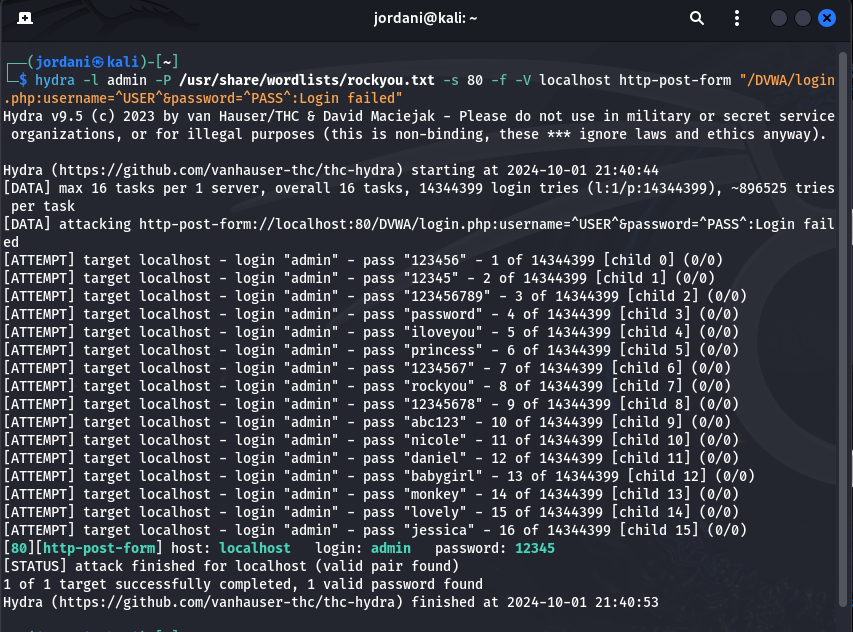


Рис. 3: Команда Hydra для Атаки на HTTP Форму

## Пояснение аргументов:

* -l admin: Имя пользователя для атаки (в данном случае — “admin”).
* -P /usr/share/wordlists/rockyou.txt: Файл со списком паролей.
* -s 80: Порт, на котором работает веб-сервис (обычно порт 80).
* -f: Остановить атаку после нахождения правильной комбинации.
* -V: Подробный режим, отображающий каждую попытку.
* localhost: Адрес сервера (в данном случае — локально установленное DVWA).
* http-post-form: Указывает, что это форма HTTP, использующая метод POST.
* “/DVWA/login.php:username=USER&password=PASS:Login failed”:
  + Путь к форме.
  + Шаблон для отправки имени пользователя и пароля.
  + Строка “Login failed” как индикатор неудачной попытки.

## Анализ Результатов

* После выполнения команды Hydra получим результат, который может выглядеть так:

[80][http-post-form] host: localhost login: admin password: 12345  
[STATUS] attack finished for localhost (valid pair found)

### Проверка Найденного Пароля

* Чтобы убедиться, что найденная комбинация действительно работает, выполнил следующие действия (рис. 4) и (рис. 5).
  + Ручная проверка:
    - Открыл браузер и перешёл на страницу входа в DVWA: http://localhost/DVWA/login.php.
    - Ввел имя пользователя admin и пароль 12345.
    - Если вход выполнен успешно, это подтверждает, что Hydra нашла правильный пароль.

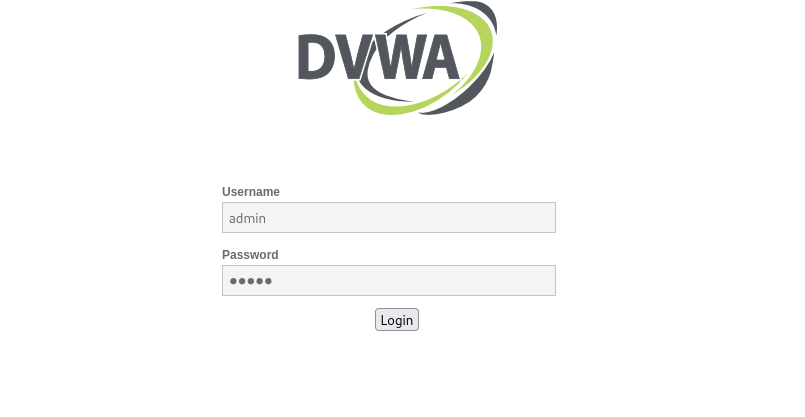


Рис. 4: Проверка Найденного Пароля

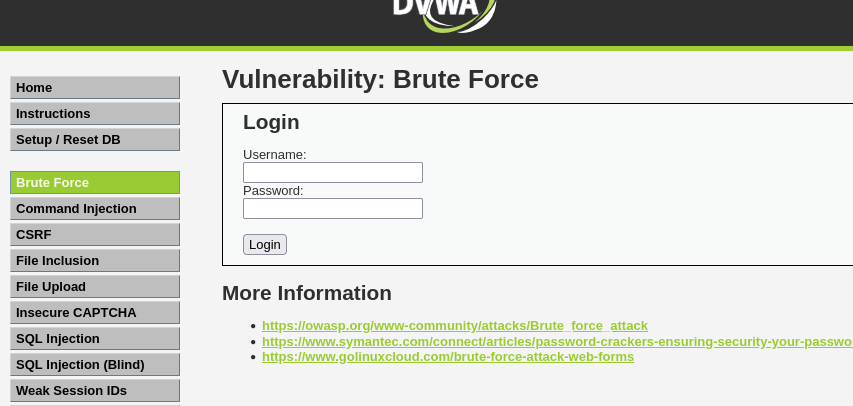


Рис. 5: Проверка Найденного Пароля

* Проверка с помощью curl:
  + Можно тоже использовать команду curl, чтобы проверить результаты в терминале (рис. 6):
* curl -X POST -d "username=admin&password=12345&Login=Login" http://localhost/DVWA/login.php -v

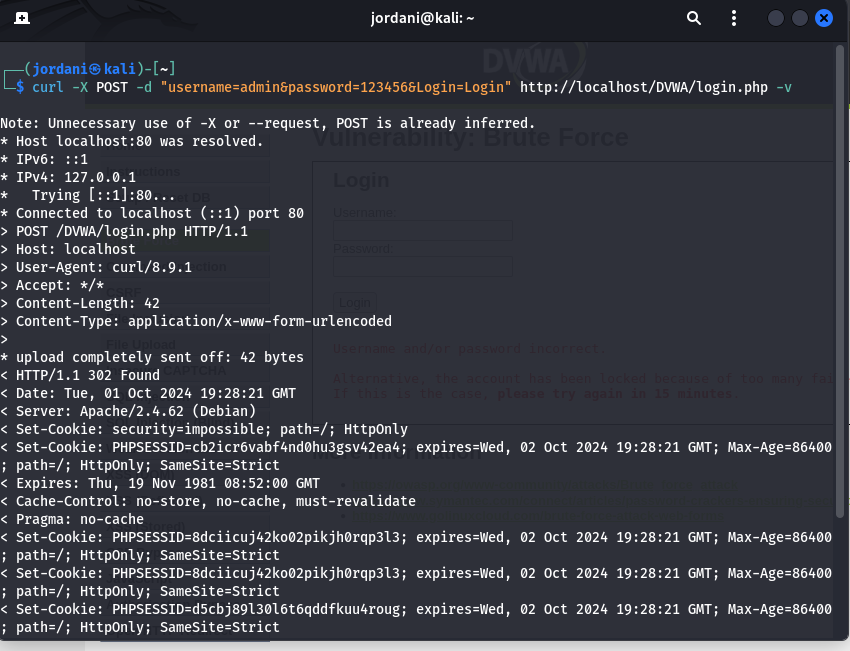


Рис. 6: Проверка Найденного Пароля

* Команда -v покажет ответ сервера, что поможет подтвердить успешность аутентификации.

# Выводы

На этом этапе я научилисся использовать **Hydra** для атаки методом грубой силы на форму входа в **DVWA** и проверять результаты атаки. Этот опыт демонстрирует, насколько важно использовать сложные пароли, чтобы предотвратить подобные атаки, и показывает, как инструменты автоматизации могут быть использованы злоумышленниками для нахождения слабых мест в системе безопасности.