Отчёт о выполнении. Индивидуальный проект. Этап 3

Использование Hydra

Щербак Маргарита Романовна, НПИбд-02-21

2024

Содержание

Список иллюстраций

Цель работы

Приобретение практических навыков по использованию инструмента Hydra.

Теоретическое введение

Виртуализация является одним из ключевых инструментов в современной информационной безопасности и IT-инфраструктуре. Использование виртуальных машин (VM) позволяет создавать изолированные среды для работы, тестирования и изучения различных операционных систем и программного обеспечения без риска воздействия на основную систему. Одним из наиболее популярных дистрибутивов, используемых для задач информационной безопасности, является Kali Linux [1].

Kali Linux — это специализированный дистрибутив Linux, разработанный для проведения тестирования на проникновение и анализа информационной безопасности. Он содержит множество инструментов для проведения аудитов безопасности, обнаружения уязвимостей и эксплуатации различных системных слабостей [2].

Некоторые из уязвимостей веб приложений, который содержит DVWA:

- Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей.
- Исполнение (внедрение) команд: Выполнение команд уровня операционной системы.
- Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений.
- Внедрение (инклуд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение.
- SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение.
- Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные фай-

лы на веб сервер.

- Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS.
- Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA:

- Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.
- Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях.
- Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу.
- Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации.

Выполнение проекта

Запуск Hydra

Через терминал запустила Hydra, для графической версии добавила ‘x’ перед командой. Просмотрела и изучила вкладки (рис.1 - рис.2).

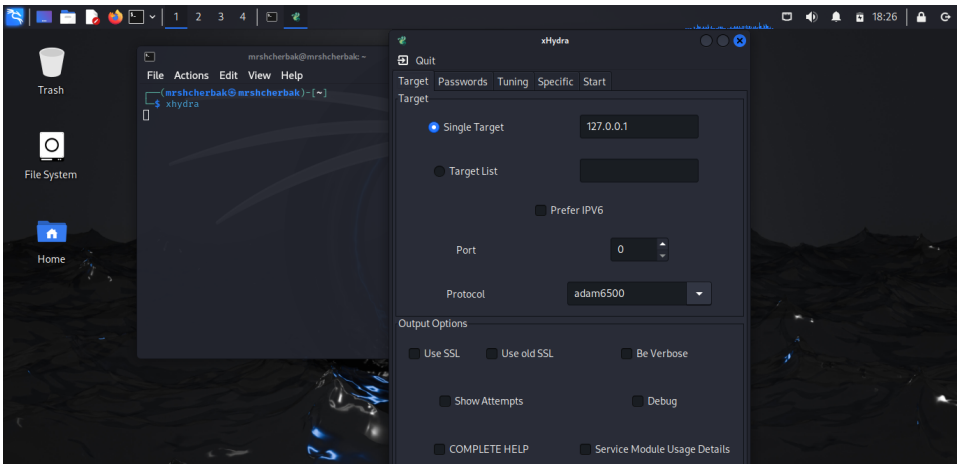

Рис. 1: Запуск Hydra

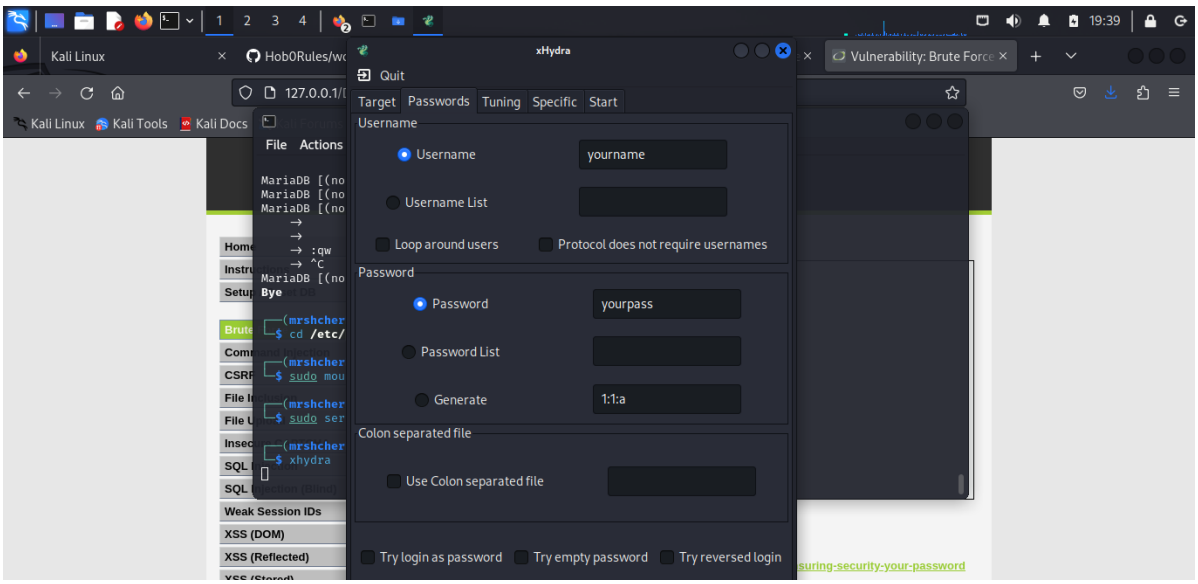

Рис. 2: Просмотр раздела Passwords

Здесь есть несколько вкладок:

- Target - цели атаки;
- Passwords - списки паролей;
- Tuning - дополнительные настройки;
- Specific - настройки модулей;
- Start - запуск и просмотр статуса атаки.

Чтобы пробрутфорсить пароль, нужно иметь список паролей. Список частоиспользуемых паролей можно найти в открытых источниках, я взяла список паролей `rockyou.txt` для kali linux (рис. 3).

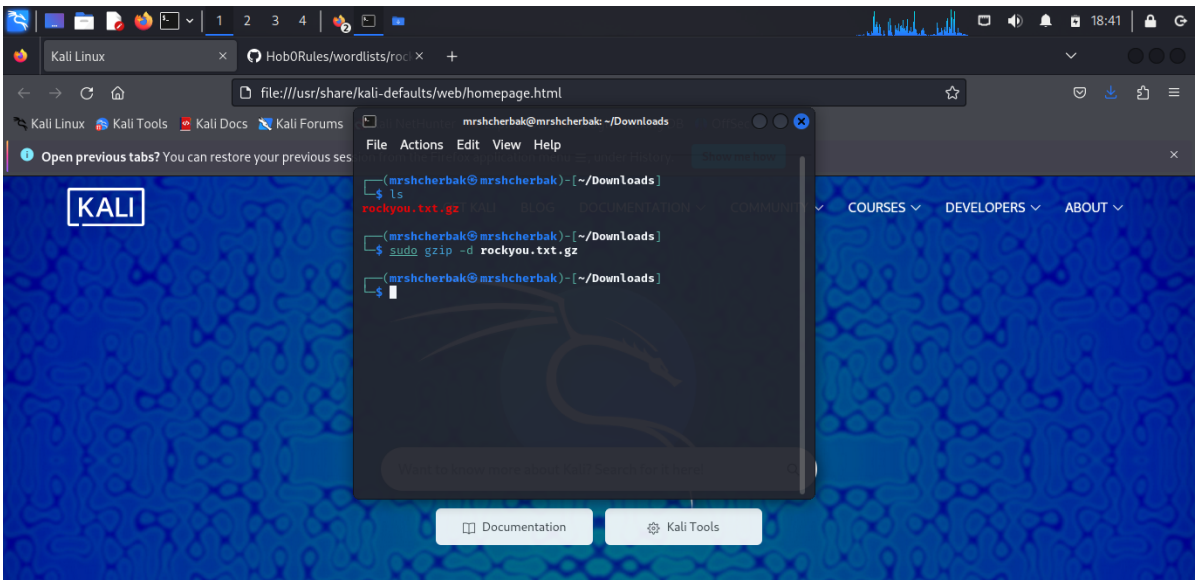

Рис. 3: Распаковка архива со списком паролей

Зашла на сайт DVWA. Для запроса hydra нужны параметры cookie с этого сайта (рис. 4).

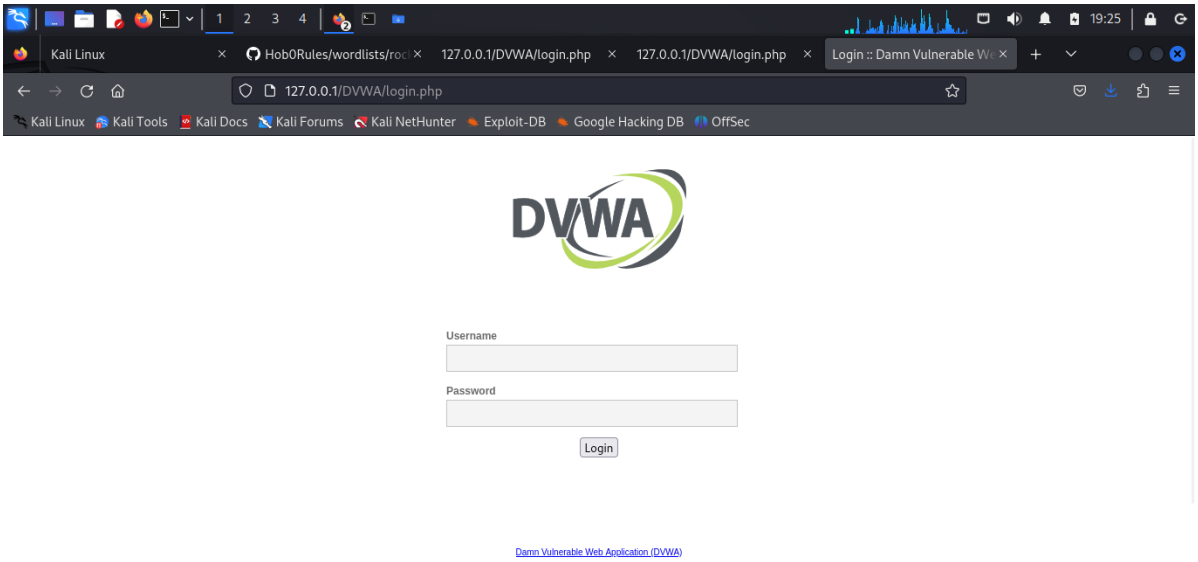

Рис. 4: Сайт с информацией о параметрах Cookie

Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID

(рис. 5).

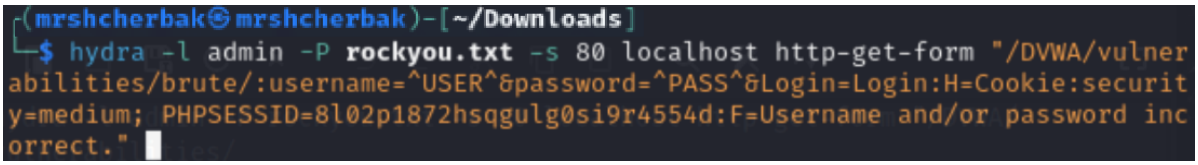

Рис. 5: Запрос Hydra

Получили результат с подходящим паролем (admin, password). Ввела полученные данные на сайт для проверки и получила положительный результат проверки пароля (рис. 6).

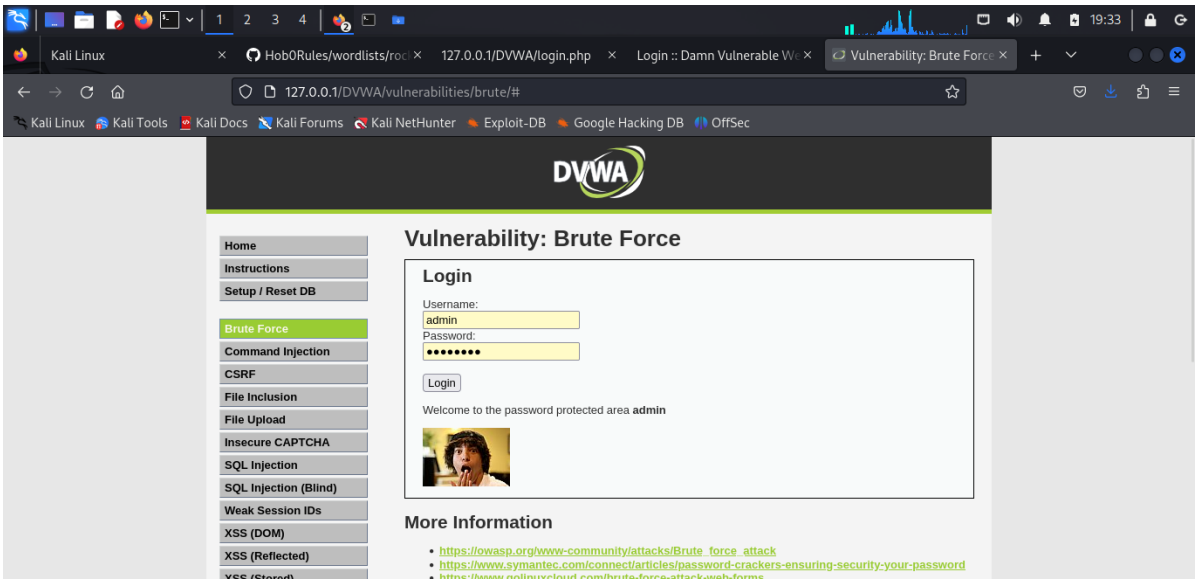

Рис. 6: Проверка и результат

Вывод

Таким образом, в ходе 3 этапа индивидуального проекта я приобрела практические навыки по использованию инструмента Hydra.

Библиография

1. Документация по Virtual Box: https://www.virtualbox.org/wiki/Documentation
2. Документация по этапам индивидульного проекта: Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли П18 Kali Linux. Тестирование на проникновение и безопасность. — СПб.: Питер, 2020. — 448 с.: ил. — (Серия «Для профессионалов»). ISBN 978-5-4461-1252-4