Отчёт о выполнении. Индивидуальный проект. Этап 3

Сироджиддинов Камолиддин, НКНбд-01-21

Содержание

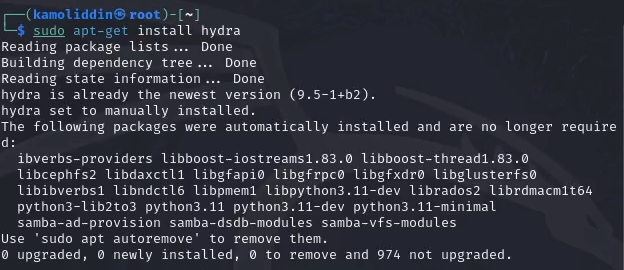
# 1 Цель работы

Исследование и применение инструмента Hydra для подбора имени пользователя и пароля с использованием brute-force атаки на HTTP POST форму, а также анализ результатов выполнения.

## 1.1 Исходные данные:

IP сервера: 178.72.90.181 Сервис: HTTP на стандартном 80 порту Форма авторизации: Метод отправки данных - POST по адресу: http://178.72.90.181/cgi-bin/luci, Параметры формы: username=root&password=test\_password Сообщение при неудачной аутентификации: "Invalid username and/or password! Please try again." Используемая утилита: Hydra ## Подготовка к работе

### 1.1.1 1. Обновление системы

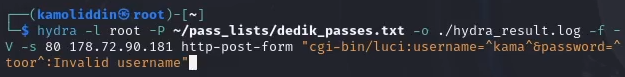
Установка Hydra: Для начала работы с Hydra была произведена установка инструмента на операционной системе с использованием следующих команд: 

### 1.1.2 2. Создание словаря паролей

В процессе атаки использовался заранее подготовленный файл со списком паролей. Для его создания был использован текстовый редактор: 2

Пример содержимого файла: 3

### 1.1.3 3. Описание команды для выполнения brute-force атаки

Была составлена и использована следующая команда Hydra: 

## 1.2 Результаты работы

### 1.2.1 Пример вывода попыток Hydra:

[DATA] attacking service http-post-form on port 80  
[80][http-post-form] host: 178.72.90.181 login: root password: admin  
[STATUS] attack finished for 178.72.90.181 (valid password found)

### 1.2.2 Файл результата (hydra\_result.log):

178.72.90.181:80 http-post-form /cgi-bin/luci root:admin

### 1.2.3 Анализ:

Пароль для пользователя root был успешно подобран. В результате успешной brute-force атаки удалось получить доступ к системе, используя комбинацию root:admin.

# 2 Заключение

В ходе работы было продемонстрировано использование инструмента Hydra для проведения атаки на HTTP POST форму методом brute-force. С помощью указанной команды удалось успешно подобрать пароль для пользователя.

Полученный результат подтверждает эффективность метода brute-force при наличии недостаточно защищённого веб-сервиса с простыми паролями и отсутствием дополнительных защитных механизмов (например, блокировки после нескольких неудачных попыток входа).