Защита 3 этапа индивидуального проекта

Информационная безопасность

Докладчик

Петрова Мария Евгеньевна

Студентка группы НФИбд-02-21

Студ. билет 1032216450

Российский университет дружбы народов

Цель лабораторной работы

- Использование Hydra.

Задание

- Использование Hydra
- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений.
- Пример работы:
- Исходные данные:
  - IP сервера 178.72.90.181;
  - Сервис http на стандартном 80 порту;
  - Для авторизации используется html форма, которая отправляет по адресу http://178.72.90.181/cgi-bin/luci методом POST запрос вида username=root&password=test_password;
  - В случае не удачной аутентификации пользователь наблюдает сообщение Invalid username and/or password! Please try again.
- Запрос к Hydra будет выглядеть примерно так:
- hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log -f -V -s 80 178.72.90.181 http-post-form "/cgi-bin/luci:username=^USER^&password=^PASS^:Invalid username"
-

- Используется http-post-form потому, что авторизация происходит по http методом post.
- После указания этого модуля идёт строка /cgi-bin/luci:username=^USER^&password=^PASS^:Invalid username, у которой через двоеточие (:) указывается:
    - путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci);
    - строка, которая передаётся методом POST, в которой логин и пароль заменены на ^USER^ и ^PASS^ соответственно (username=^USER^&password=^PASS^);
    - строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username).

- **1.** Нашла и скачала список частоиспользуемых паролей из интернета. rockyou.txt

- **2.** Захожу на сайт DVWA, созданный на прошлом этапе.
- **3.** Для запроса hydra мне понадобятся параметры cookie с этого сайта. я скачала расширение для браузера.
- **4.** Ввела в hydra запрос с нужную информацию
- **5.** В итоге выводится результат с подходящими паролями.
- **6.** Ввела полученные данные на сайт для проверки. Получила положительный результат.

Вывод

- Научилась работать с hydra.