Индивидуальный проект. Этап 3

Использование Hydra

Татьяна Александровна Буллер

Содержание

# 1 Цель работы

Знакомство с инструментом перебора паролей Hydra и простейшим вариантом атаки грубой силы (bruteforce)

# 2 Ход работы

Hydra - инструмент перебора паролей, поддерживающий работу с множеством различных приложений (не только веб-формы, но и другие сервисы, например, ssh и ftp). Используется для перебора по списку пар логин-пароль при аутентификации пользователя в той или иной системе. Такой метод известен как брутфорс - атака грубой силы.

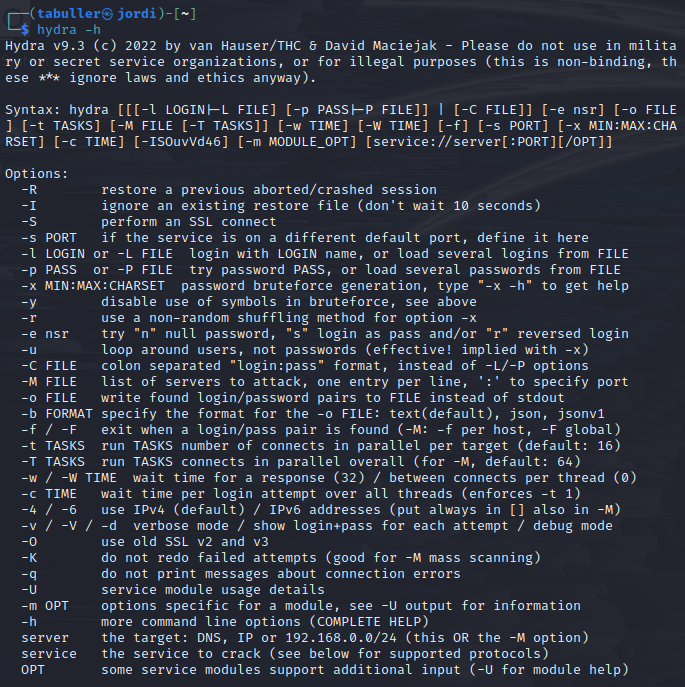


Рис. 1: Справка Hydra

Перейдем на страницу уязвимости Brute Force в DVWA. Страница предлагает форму с двумя полями: username (имя пользователя) и password (пароль). Предположим, что заранее мы не знаем ни одного из компонентов этой пары.

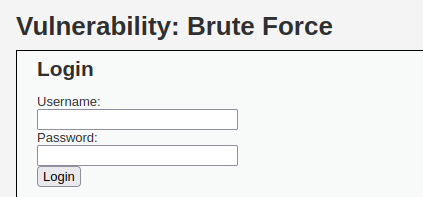


Рис. 2: Страница уязвимости Brute Force

В DVWA мы можем просмотреть исходный код, с помощью которого реализована форма. Это позволяет наглядно видеть, как писать НЕ нужно, и определить вектор или детали осуществления атаки. В случае Brute Force видим, что различаются два варианта развития событий: успешный вход, при котором выводится строка “Welcome…”, и ошибка входа, при которой форма даст ответ “Username and/or password incorrect”. Эти данные пригодятся в дальнейшем для составления команды.

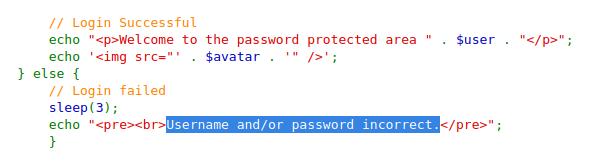


Рис. 3: Исходный код страницы

Попробуем отправить форму со случайными данными и рассмотрим происходящее в разделе Network инструментов разработчика. Видим, что при отправке формы осуществляется GET-запрос, а введенные данные передаются в открытом виде в адресе запроса. Это делает возможным использование Hydra методом http-get-form без модификации отправляемых пакетов: изменять будем только строку запроса.

Рис. 4: GET-запрос

Рис. 4: GET-запрос

Составим команду для Hydra. Первым делом передаем опцию -L <file>, где <file> - имя файла, в котором перечислены варианты логинов. Можно использовать опцию -l: в таком случае пароли будут перебираться для одного пользователя, а логин можно задать строкой. Следующая опция - -P <file>, где <file> - файл с паролями. Аналогично, опция -p будет пробовать только один пароль. Я использую rockyou.txt, по умолчанию включенный в Kali. rockyou.txt был создан в результате утечки базы данных rockyou, социального приложения и рекламной сети. В результате было раскрыто более 32 миллионов паролей пользователей, хранившихся в открытом виде. В качестве аргумента передадим IP-адрес, на котором запущена DVWA. Далее уточним метод (http-get-form) и передадим строку параметров для составления запроса: “/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect.:H=Cookie: security=high; security=low; PHPSESSID=(…)”. Здесь выделяем два параметра: ^USER^ и ^PASS^, куда Hydra будет подставлять варианты из переданных ей списков. “Username and/or password incorrect.” - строка в теле ответа сайта, наличие которой говорит о том, что комбинация логин/пароль не подходит, запросы, которые дали такие ответы, Hydra будет отметать. Дополнительный параметр - кука с айди сессии и уровнем безопасности.

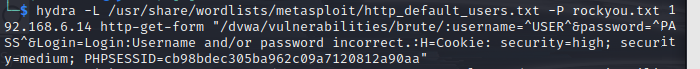


Рис. 5: Команда для Hydra

Спустя некоторое время получаем удачную комбинацию: admin:password. Hydra будет перебирать пароли и дальше (можно задать флаг -F, чтобы после найденной удачной комбинации она закончила перебор), но нам этого результата достаточно. Проверив эту комбинацию на странице, видим, что она действительно работает.

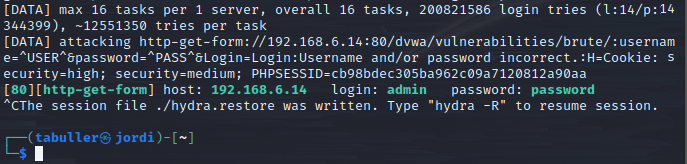


Рис. 6: Успех подбора пароля

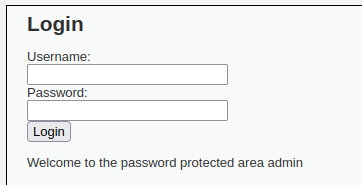


Рис. 7: Успешный “вход”

# 3 Выводы

Было освноено применение инструмента Hydra для перебора паролей и осуществлена простейшая bruteforce-атака на тестовой машине DVWA.