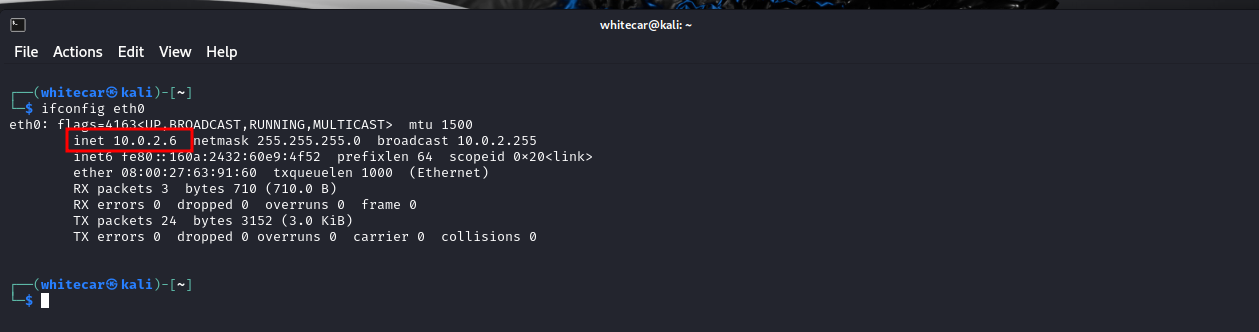
**Empire: Breakout**

Перед началом тестирования я бы хотел уточнить пару моментов. Первое, все результаты сканирований, скриншоты и заметки будут доступны на [моем гитфабе](https://github.com/WhiteCarVM/HackingSkills). Второе, ключевые моменты тестирования, я буду обозначать с помощью **жирного цвета**. Я бы советовал обратить на них внимание. А теперь к делу!!!

**Мне дан IP адрес цели: 10.0.2.9**

Для начала мне необходимо узнать IP адрес моей виртуальной машины Kali Linux. Для этого я использую команду «*ifconfig»****.*** Вместо с командой указываю интерфейс, с помощью которого виртуальная машина общается с внешним миром. В данном случае это «e*th0».* Итак, конечная команда: «**ifconfig eth0».** Можно просто указать «*ifconfig*» и в списке интерфейсов найти *eth0:*



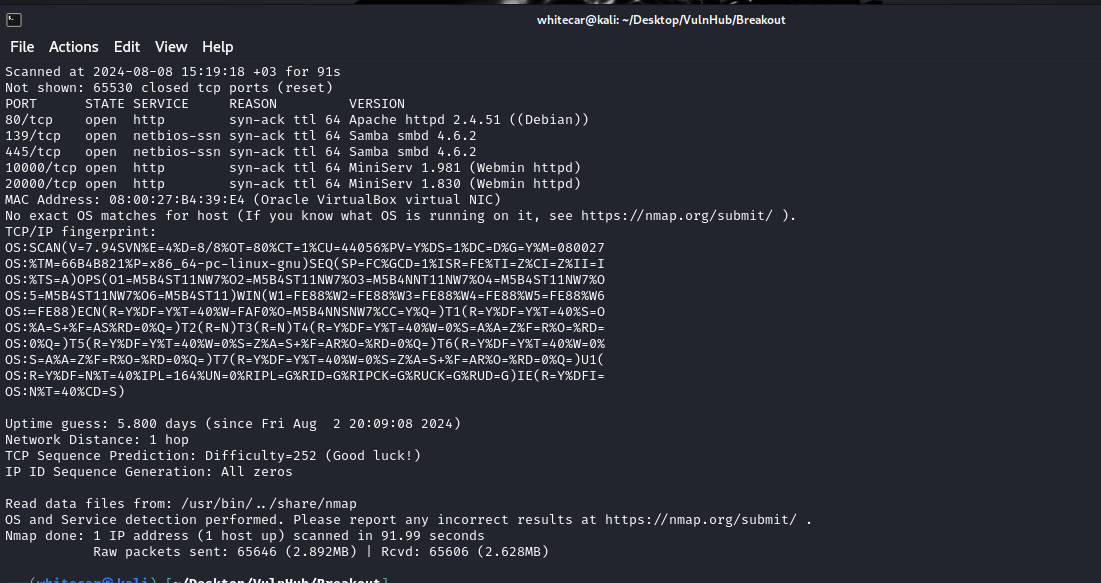
**Рисунок 1: IP адрес атакующего**

Как видно из скриншота, **IP адрес моей виртуальной машины: 10.0.2.6**

Далее мы переходим к этапу сбора информации и начнем с поиска открытых портов. Для этого я использую инструмент nmap и в окно терминала ввожу команду «**nmap -sS -sV -vvv -p- -T4 -oA ./Scans/NmapFirstScan -O 10.0.2.9**».

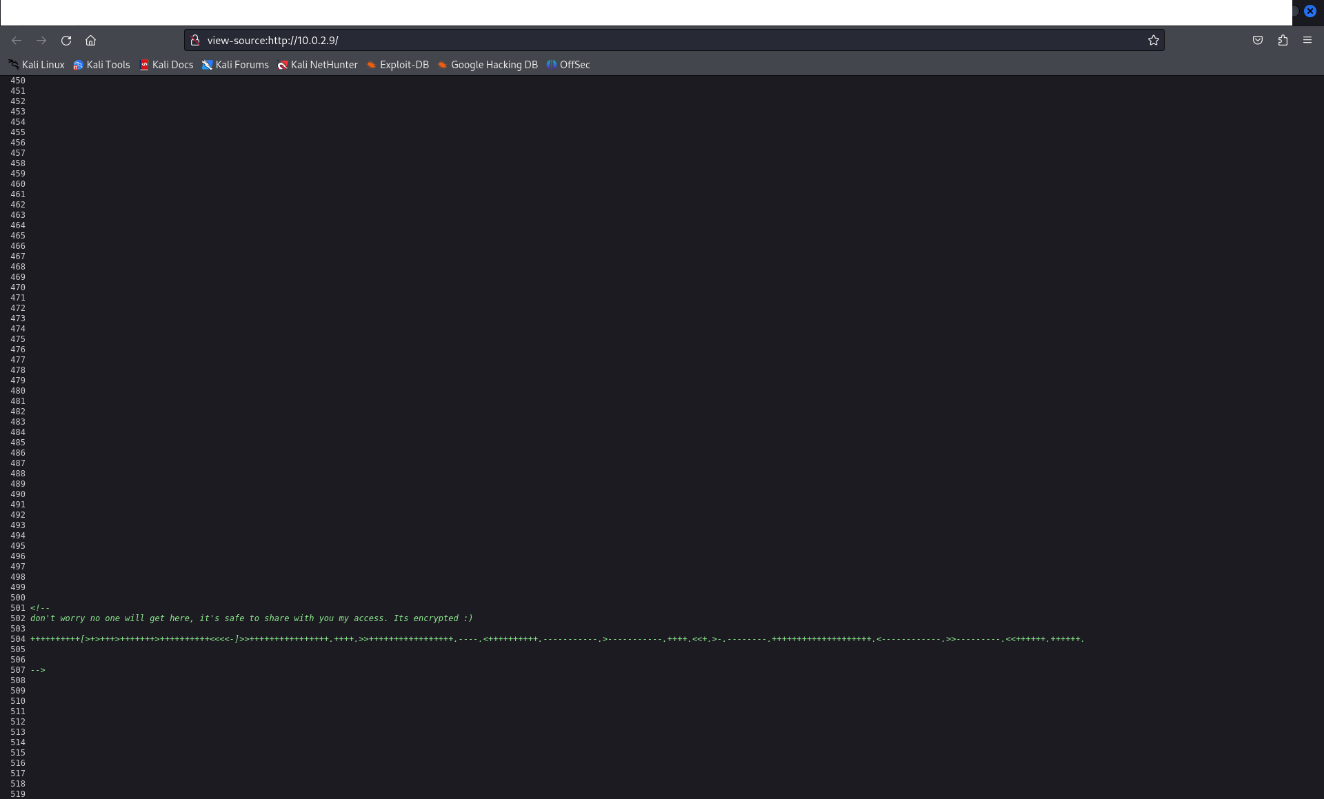
С результатами сканирования можно ознакомиться либо в выходном файле (смотри github), либо на скриншоте снизу, либо ниже. Результаты сканирования:

1. Предполагаемая ОС: Linux 4.X|5.X (Debian) ;
2. MAC адрес: 08:00:27:F9:52:FC (Oracle VirtualBox virtual NIC) ;
3. Открытые порты:
   1. 80/tcp http Apache httpd 2.4.51 ((Debian));
   2. 139/tcp netbios-ssn Samba smbd 4.6.2;
   3. 445/tcp netbios-ssn Samba smbd 4.6.2;
   4. 10000/tcp http MiniServ 1.981 (Webmin httpd);
   5. 20000/tcp http MiniServ 1.830 (Webmin httpd):



**Рисунок 2: результаты сканирования nmap**

На 80-ом порту расположен веб-сайт. Для перечисления я использовал инструмент gobuster. С его помощью мне удалось найти лишь одну директорию: «/manual». Скорее всего, это просто веб-сервер. Файл «robots.txt» отсутствует. В исходном коде страницы мне удалось найти подсказку (смотри ниже).



**Рисунок 3: Подсказка в исходном коде страницы**

Сам комментарий выглядит следующим образом:

**<!--**

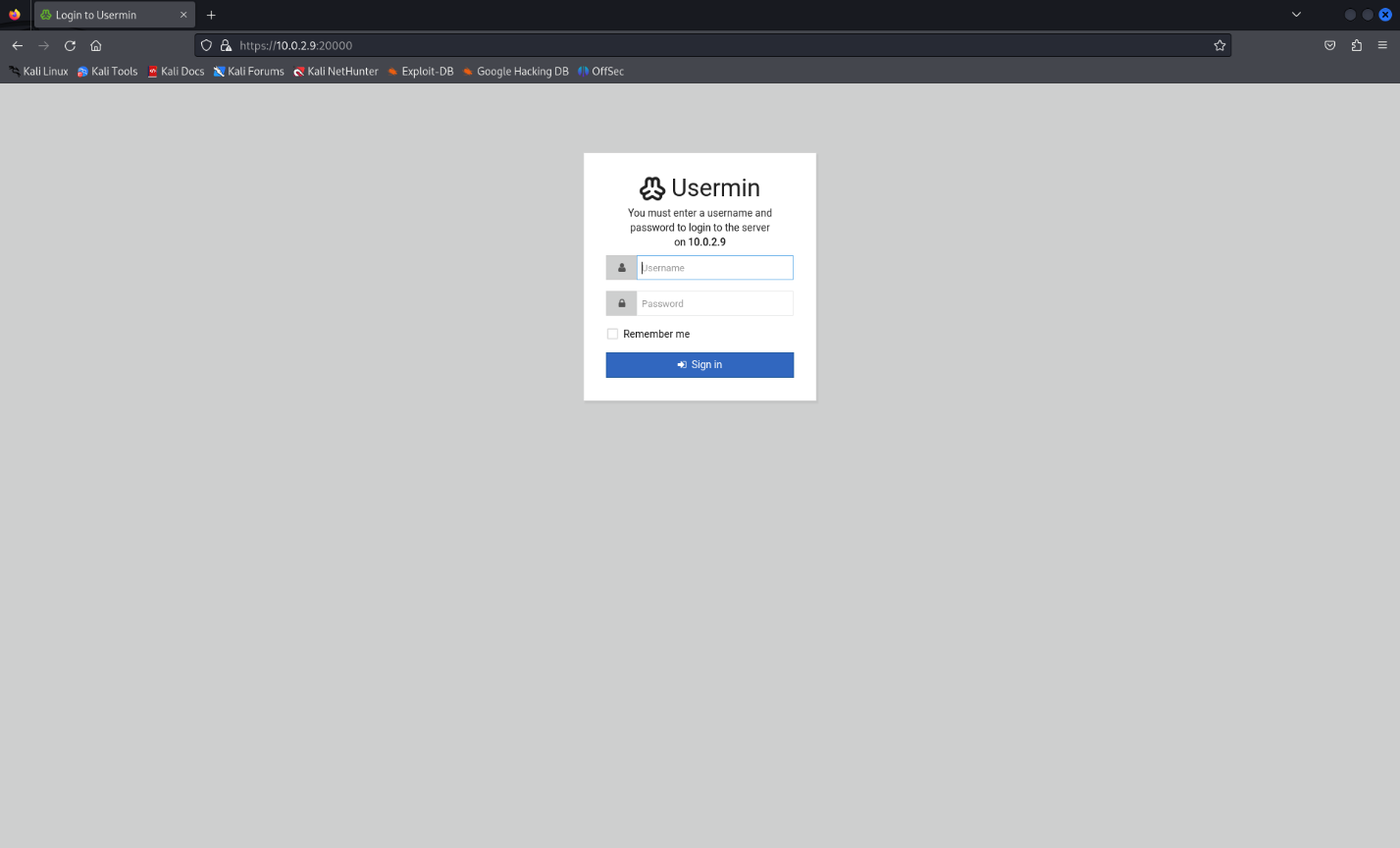
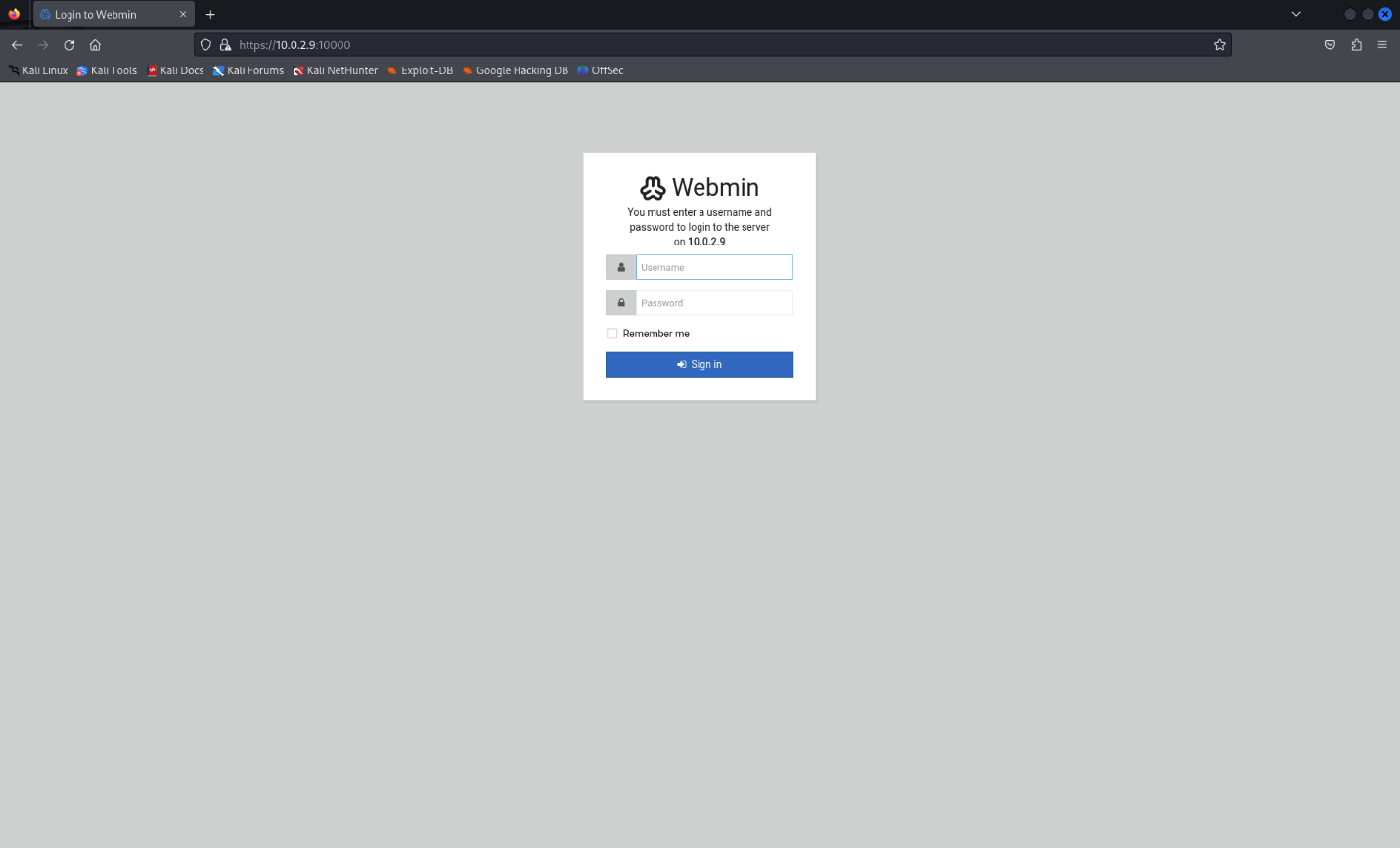
**don't worry no one will get here, it's safe to share with you my access. Its encrypted :)**

**++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>++++++++++++++++.++++.>>+++++++++++++++++.----.<++++++++++.-----------.>-----------.++++.<<+.>-.--------.++++++++++++++++++++.<------------.>>---------.<<++++++.++++++.**

**p-->**

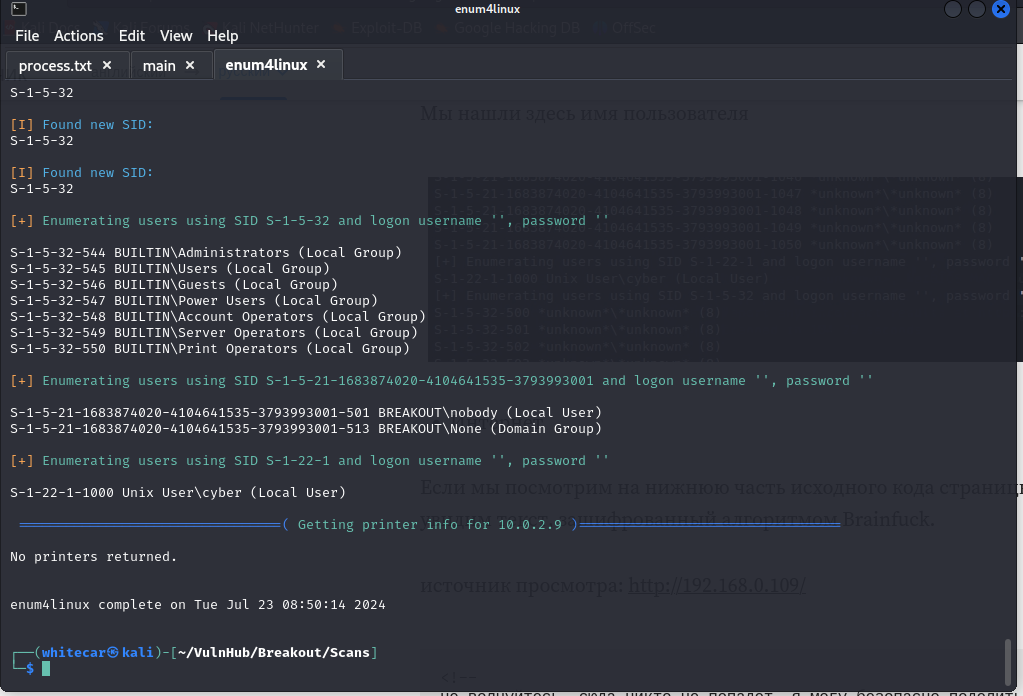
Мне удалось декодировать это. Я получил следующее «**.2uqPEfj3D<P'a-3**». Скорее всего, это какой-то пароль.

На 10000-ом и 20000-ом портах расположены формы для входа на сервер. Это две разные формы. Они понадобятся далее.



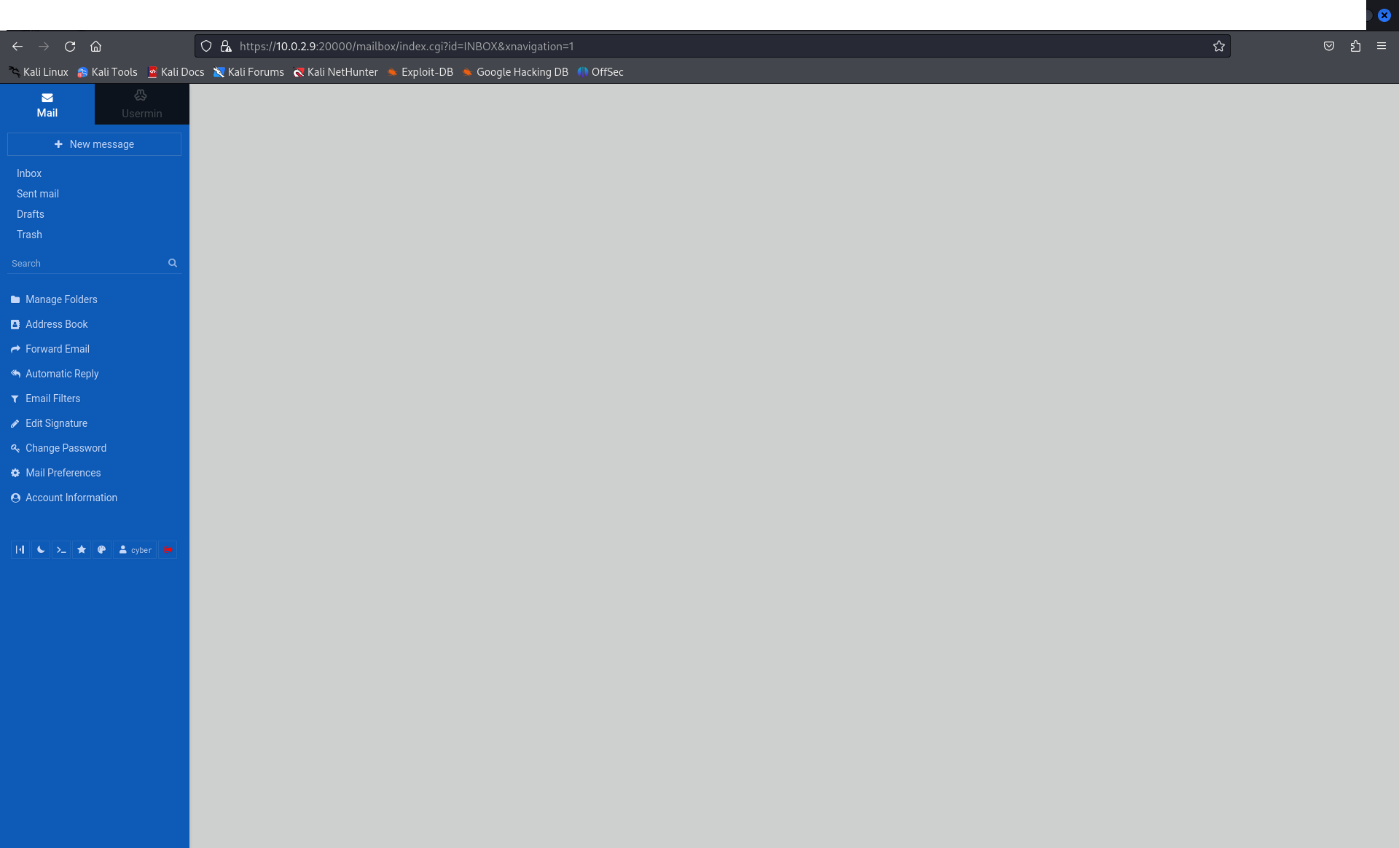
**Рисунки 4-5: Страницы, расположенные на 10000-ом и 20000-ом портах**

На 445-ом порту расположен сервис Samba. Собирать данные из этого сервера удобно при помощи инструмента enum4linux. Из результатов работы enum4linux мне удалось извлечь имя пользователя – **cyber**:



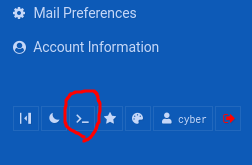
**Рисунок 6: Результаты работы enum4linux**

Итак, нам удалось собрать комбинацию: «**cyber – .2uqPEfj3D<P'a-3**». С её помощью я могу войти на сайт, расположенный на 20000-ом порту:



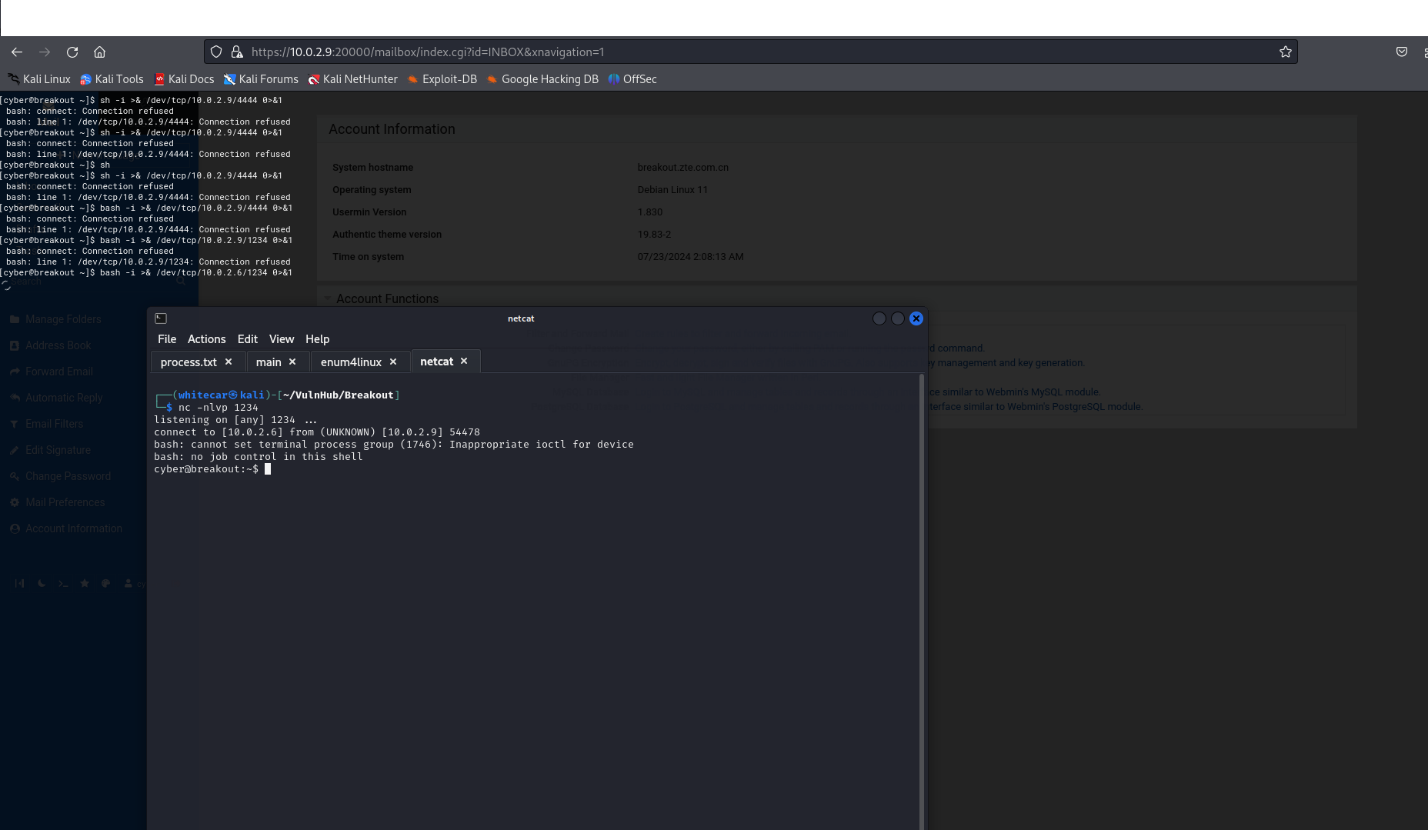
**Рисунок 7: Вход на сайт**

Приступаю к анализу страницы – и сразу вижу **одну интересную кнопку**. Внешне эта кнопка напоминает терминал:



**Рисунок 8: Терминал**

И это действительно терминал!!! Воспользовавшись сайтом «**https://www.revshells.com/**», я составил нагрузку, чтобы получить реверс шелл. У меня все получилось:



**Рисунок 9: Реверс шелл**

Я являюсь пользователем cyber, значит могу читать все его файлы. В домашней директории пользователя находился первый флаг **user.txt**. Я прочитал его: **3mp!r3{You\_Manage\_To\_Break\_To\_My\_Secure\_Access}**

Далее мне необходимо повысить свои привилегии: из пользователя cyber превратиться в пользователя root. Для этого я провожу анализ системы:

1. История пустая;
2. команда sudo не найдена;
3. Я могу читать файл /etc/passwd , но не могу ничего туда записывать;
4. SUID биты бесполезны;
5. Версия ядра: 5.10.0-9-amd64 . Ядро уязвимо к DirtyPipe, но я не смог проэксплуатировать;
6. Я перебросил скрипт «linuxenum.sh», результаты работы которого записаны в файл «**linuxenum\_results.txt**».

С помощью скрипта я нашел файл «**.old\_pass.bak**», но не смог его распаковать. К счастью в пользовательской директории находился Tar. У него есть возможность чтения файлов. Мой дальнейший **алгоритм действий**:

1. ./tar -cf pass.tar /var/backups/.old\_pass.bak
2. tar -xf pass.tar
3. cat /var/backups/.old\_pass.bak

Я открыл файл и нашел **пароль root**. Став root я прочитал файл «**root.txt**», который находился в директории /root: **3mp!r3{You\_Manage\_To\_BreakOut\_From\_My\_System\_Congratulation}**

После всех этих действий, как примерные пентестеры, мы очищаем после себя систему: удаляем наши файлы, в данном случае, и выходим из системы.

Breakout является машиной легкого уровня. Она очень полезна для новичка, так как в ней отточить навыки использования стандартных инструментов и в ней нет каких-то сложных механизмов. Тестирование окончено, спасибо за внимание.