Sneak

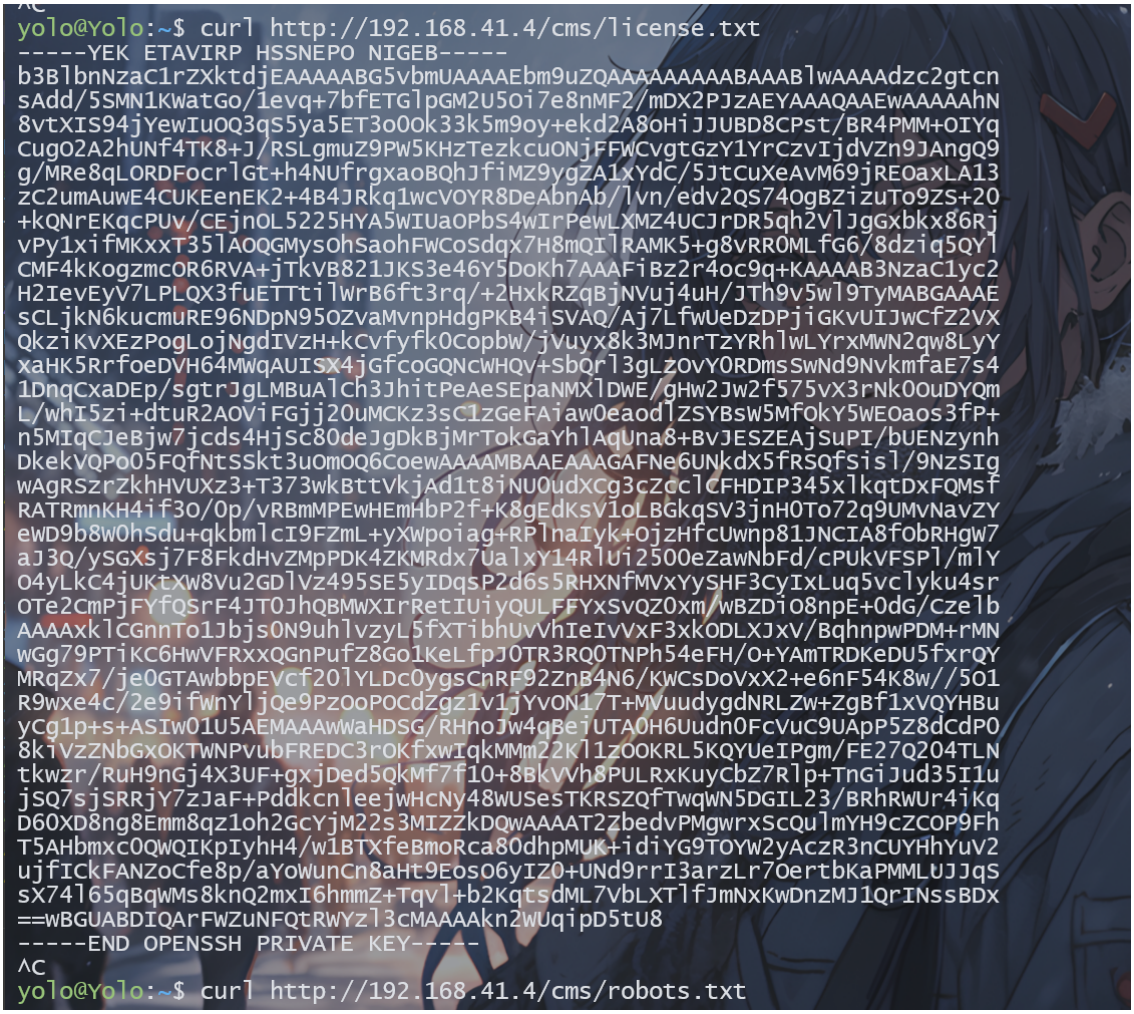
- Write by **Yo1o**

user

扫描目录，发现这里的cms一直302重定向，再深度扫描一下，发现不少好东西

```
┌──(root㉿ kali)-[/home/kali]
└─# gobuster dir -u http://192.168.41.4/cms/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.41.4/cms/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 277]
/.html               (Status: 403) [Size: 277]
/index.php           (Status: 500) [Size: 0]
/rss.php             (Status: 500) [Size: 0]
/content             (Status: 301) [Size: 318] [--> http://192.168.41.4/cms/content/]
/modules             (Status: 301) [Size: 318] [--> http://192.168.41.4/cms/modules/]
/license.txt         (Status: 200) [Size: 2602]
/core                (Status: 301) [Size: 315] [--> http://192.168.41.4/cms/core/]
/install             (Status: 301) [Size: 318] [--> http://192.168.41.4/cms/install/]
/lib                 (Status: 301) [Size: 314] [--> http://192.168.41.4/cms/lib/]
/config.php          (Status: 200) [Size: 0]
/styles              (Status: 301) [Size: 317] [--> http://192.168.41.4/cms/styles/]
/robots.txt          (Status: 200) [Size: 104]
/.html               (Status: 403) [Size: 277]
/.php                (Status: 403) [Size: 277]
```

访问了下license.txt直接把ssh密钥给弄出来了

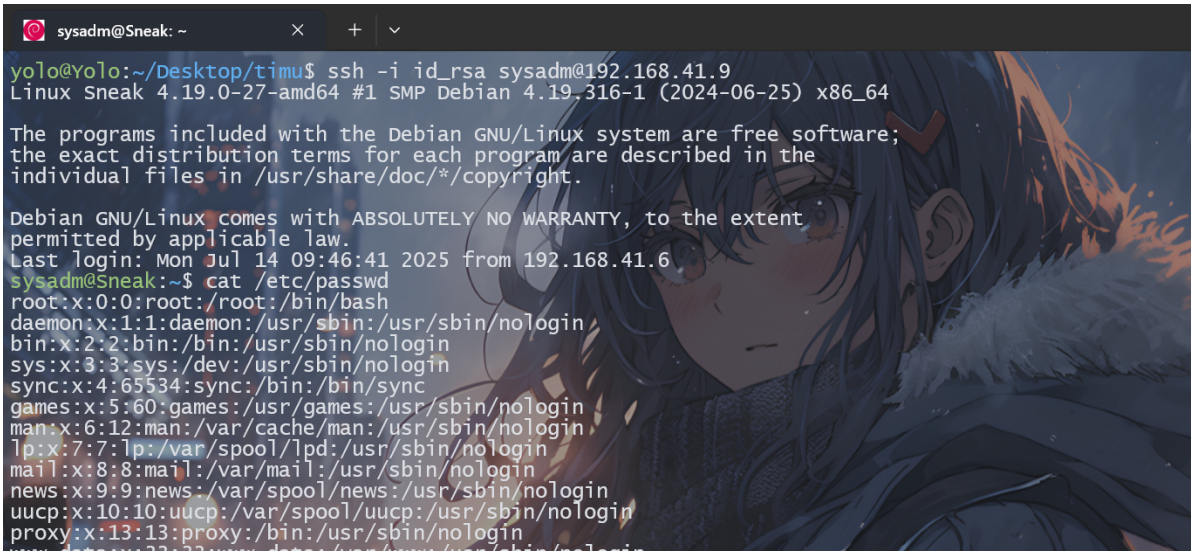


仔细研究下规律（我拿本地的和这个对比了，规律还是很明显的），发现从第一行开始，一行反转，一行不动

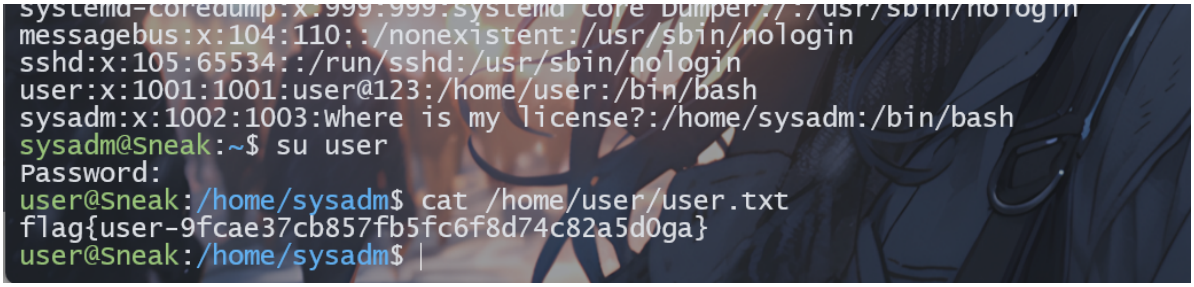
```python
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import sys

def fix_key_with_pattern(input_file, output_file):
    """
    根据“奇数行反转，偶数行不变”的规律来修复密钥文件。
    """
    print(f"[*] 正在读取文件: {input_file}")

    try:
        # 打开输入和输出文件
        with open(input_file, 'r') as f_in, open(output_file, 'w') as f_out:
            # 使用 enumerate 来同时获取行号和行内容 (行号从0开始)
            for line_number, line in enumerate(f_in):
                # 行号0, 2, 4... (即第1, 3, 5行) 需要反转
                if line_number % 2 == 0:
                    # 反转当前行
                    processed_line = line.strip('\n')[::-1] + '\n'
                else:
                    # 偶数行 (第2, 4, 6行) 保持不变
                    processed_line = line

                # 将处理后的行写入新文件
                f_out.write(processed_line)
```

```
        print(f"\n[+] 成功！已根据正确的规律生成最终密钥文件: {output_file}")

    except FileNotFoundError:
        print(f"\n[!] 错误: 输入文件 '{input_file}' 未找到。")
    except Exception as e:
        print(f"\n[!] 发生未知错误: {e}")

if __name__ == '__main__':
    if len(sys.argv) != 3:
        print("用法: python3 fix_key_final.py <原始反转文件名> <新文件名>")
        print("示例: python3 fix_key_final.py id_rsa_sneak_original
id_rsa_final")
        sys.exit(1)

    input_filename = sys.argv[1]
    output_filename = sys.argv[2]

    fix_key_with_pattern(input_filename, output_filename)
```

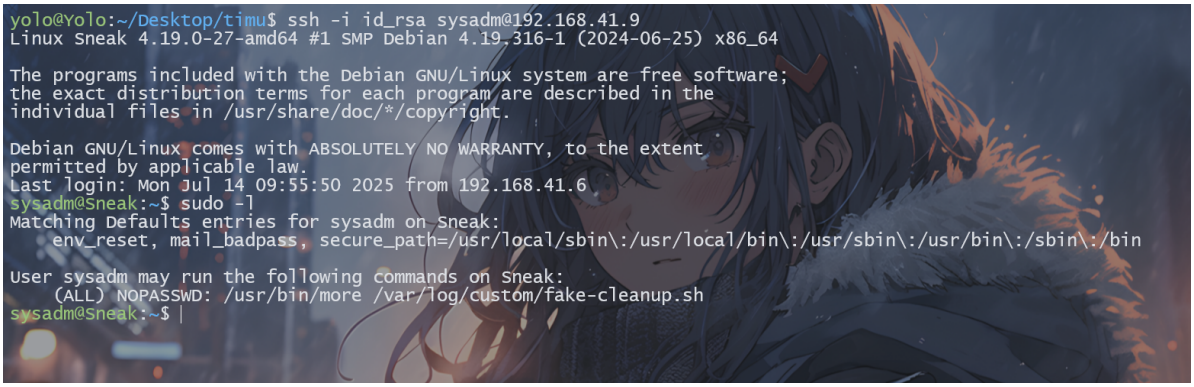
将结果保存好，直接登录



然后能看到user的密码user@123



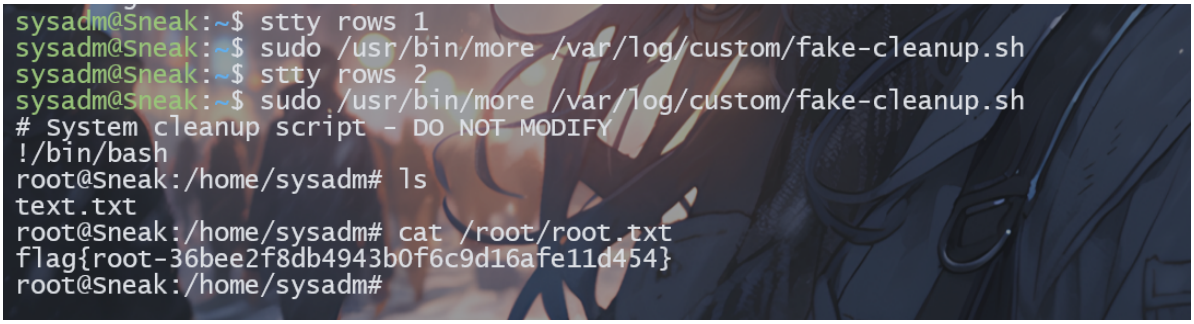
root



回到sysadm，发现了sudo权限，运行后发现那个sh文件仅仅有两行（准确来说是三行吧

也就是说我们运行more的话是不能触发--more--让我们提权的

这个的解决措施之一就是通过设置stty更改高度



最后可以输入reset去恢复设置