1.信息收集

扫描靶机端口，发现开启了22和80，进行详细扫描。

```
└─$ nmap --min-rate 10000 -p- 192.168.0.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-13 11:54 CST
Nmap scan report for 192.168.0.103 (192.168.0.103)
Host is up (0.00041s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:A1:D8:D1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds
```

```
└─$ nmap -sT -sC -sV -O 192.168.0.103 -p22,80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-13 11:55 CST
Nmap scan report for 192.168.0.103 (192.168.0.103)
Host is up (0.0013s latency).

PORT   STATE SERVICE VERSION
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-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:A1:D8:D1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

2.获取shell

访问80页面，发现上传端口，直接上传php的反弹shell文件。拿到shell。


```
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.0.110] from (UNKNOWN) [192.168.0.103] 33960
Linux Baby 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64 GNU/Linux
 23:59:35 up 5 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

3.提权

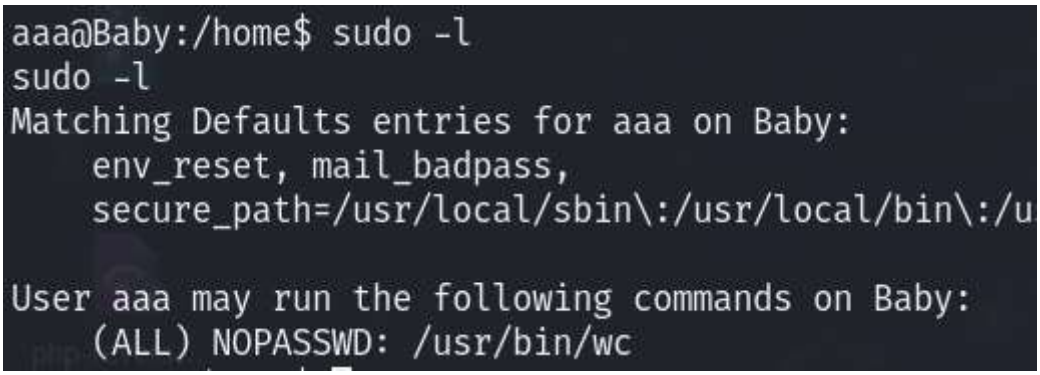
在使用python命令提升交互后，习惯性的进入/home下的用户目录里读取文件，但提示权限不足，这里需要切换至对应用户。

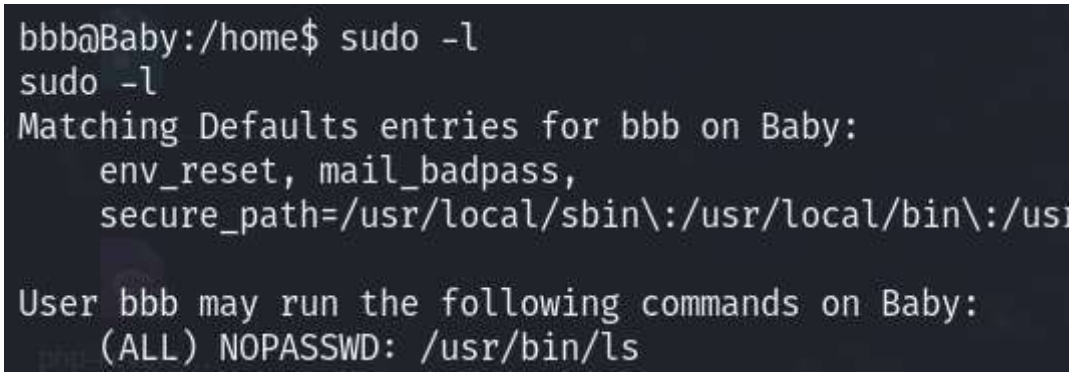
```
www-data@Baby:/home$ cd aaa
cd aaa
bash: cd: aaa: Permission denied
```

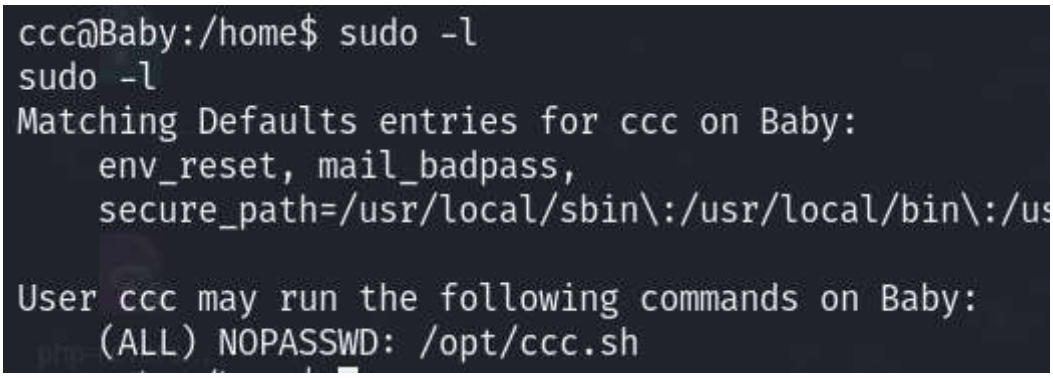
一般靶机的情况下，用户密码都会被隐藏在/var下的相关文件的角落里，但我们找了一圈，并没什么发现，然后读取/etc/passwd，发现可疑线索。

密码疑似为root，使用root为密码切换至aaa用户，成功，考虑到用户间可能会密码相同，用root密码尝试切换bbb，ccc，同样成功。在bbb下发现user.txt ，但读取后显示权限不足，要用root权限才能读取。

不同用户下，sudo无密码执行的命令是不同的，







这里如果要读root下的root.txt 以及user.txt ， 可以直接使用wc命令，来读取。

但无法获取root权限的shell。

切换至ccc用户，执行/opt/ccc.sh。

显示了错误，提示无法复制ccc下的公钥文件，这里推测其可能将公钥复制为root用户的公钥，进入ccc用户下，创建文件夹.ssh，并在kali开启http服务，使用wget将其下载至.ssh文件夹下，这里无法直接执行wget，要结合busybox命令使用，然后再次执行ccc.sh，没有错误回显，执行成功。在kali端通过ssh私钥登录靶机的root用户，拿到root的shell。