《基于 TCP 流重组的软件行为分析》源代码说明

1 源文件清单

序号	文件相对路径	文件名	用途
1	均位于同一目录下	packet_header.h	头文件
2		pcap-sample.c	识别并重建 FTP 会话
3		se_dbg.h	头文件
4		se_log.h	头文件
5		TCPFlowReconstruction.c	实现 FTP 数据流的重组和 MD5 计算
6		TCPFlowReconstruction.h	头文件
7		tempplugin.py	识别漏洞和恶意代码

2 编译说明

在 linux 系统中，安装好 gcc 和 make 后，直接在文件目录下运行 make all，即可完成编译。

3 使用说明

编译完成会生成一个可执行程序 pcap，以 sample2.pcapng 为参数运行 pcap 即可完成 TCP 流重组。

tempplugin.py：在 IDA pro 中打开 cs-test.2 后，在 file 中点击 Script file，再选中这个 py 文件并打开即可运行。