1. trace\_packet抓包及回放

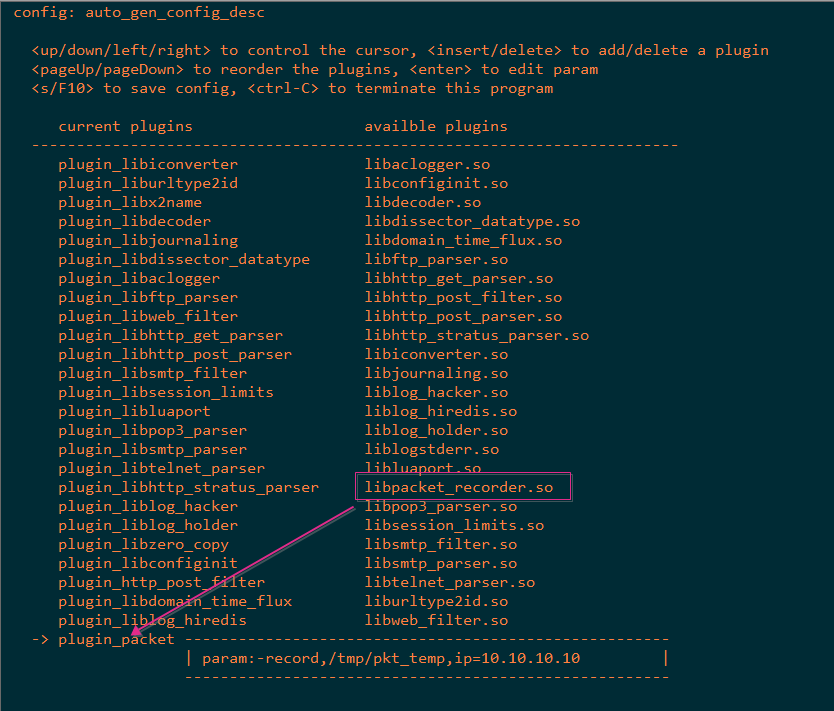
抓trace\_packet包要使用packet\_recorder插件，其原理是向事件框架注册一个监听EVTYPE\_PACKET事件的回调，在回调中将每个trace\_packet写入指定文件。回放过程（步骤x）和零拷贝插件是类似的，一个轮询函数去读指定文件，每读到一个审计包就提交EVTYPE\_PACKET事件。

插件加载脚本/ac/module/actrace/scripts/ntrace-config.js，执行这个脚本，按指示加载指定插件并编辑参数即可。

抓包参数: -record,/tmp/pkt\_temp,ip=10.10.10.10

回放参数: -play,/tmp/pkt\_temp

加载完插件后，重启actrace即开始抓包/回放。每个CPU都会对应去写一个文件，在/tmp目录下会有pkt\_temp.cpu\_id.xxx 这种格式，一般找大小不为0的就是了。抓包完成后要主动卸载packet\_recorder，不然审计进程运行时会不断地写文件。



有时候在lua发现一些异常情况，如某个http请求没有进入脚本逻辑、内容不完整、或进入逻辑的顺序不对。这时要用parse\_pk工具解析内容到指定文件，结合tcpdump抓包分析原因。