PyTask红队漏洞利用框架功能实现

PyTask官网：seckol.com

需求背景分析

从互联网搜索新闻稿获取到的信息，攻防演练活动有记录是从2016年开始，后面参与的行业越来越多。

此类活动也是检验各方的能力，主要以攻击队和防守方为主。

在越来越多的这类活动需求背景下催生了PyTask红队漏洞利用框架的诞生，给一线安全团队输出技术理念、对抗模式、和工具弹药方法。

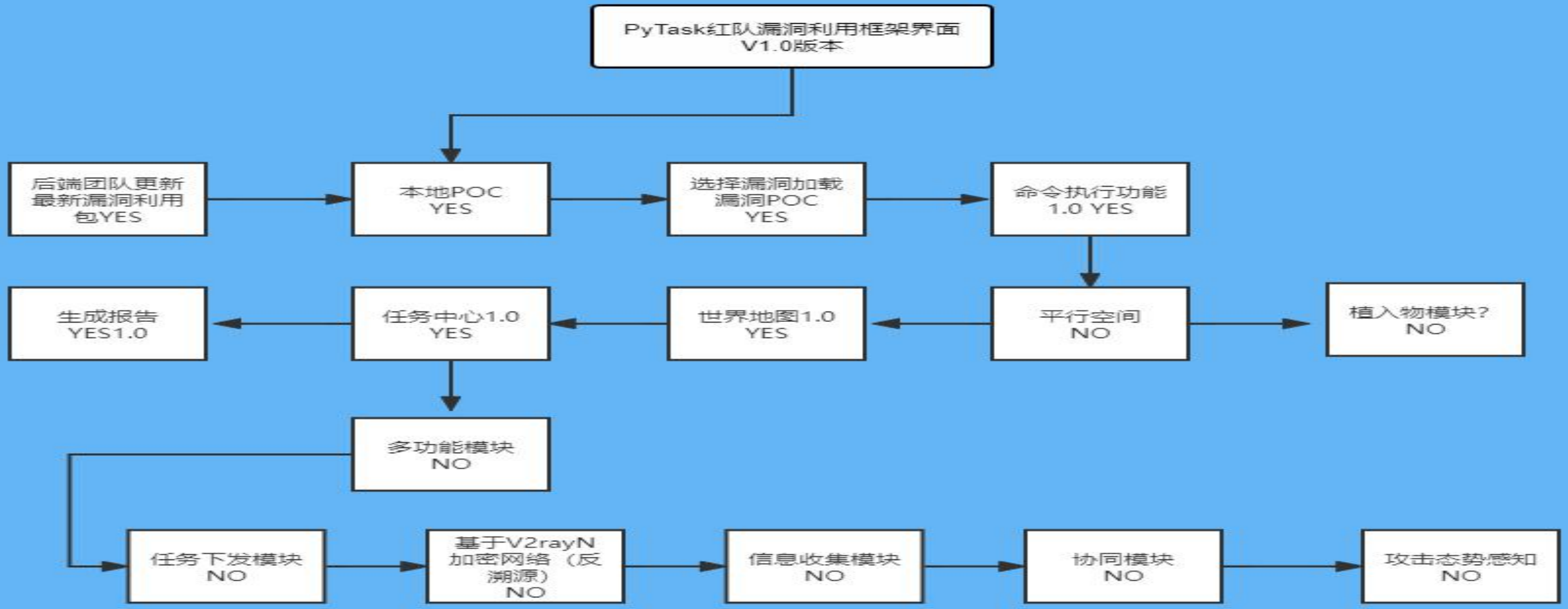
攻防队伍常用的工具，涉及攻防、目标和阵地。

攻：冰蝎、哥斯拉、 FOFA、 ZoomEye、 Goby、 蚁剑、 Metasploit、 Cobalt strike、 Etc.
防：微步情报、微步沙箱、科来流量分析系统、各类开源商用蜜罐、EDR终端安全系统、 Etc.

攻防战赛博空间：IPv4、 IPV6地址

主要针对组织：涉及组织体系架构、业务流程、和生产环境、 Etc.

PyTask红队漏洞利用框架功能架构



收集IDEA>研究实践>代码转换实现涉及阶段

1.概念阶段-耗时?
2.模型阶段-耗时?
3.玩具阶段-耗时?
4.兵器阶段-耗时?

最终解决问题

找POC&EXP费时间搭环境费时间
出报告费时间
部署简单易用
后端团队支持>最新漏洞包>新版本迭代快。

PyTask红队漏洞利用框架V1.0界面

交付模式?

期待，请关注官网https://seckol.com/