

# 2021公安部护网行动红队作战手册

## 说明

以下仅针对日常“红队”场景，进行了一次相对全面完整的实战攻击利用技术提炼汇总

针对不同的渗透阶段，所可能会用到的一些技术都做了详尽梳理说明（后面可能还会整理出对应的完整工具链，虽然那不是最主要的）

由于红队不同于一般的渗透测试，强调更多的是如何搞进去拿到相应机器权限 或者 实现某特定目的

而不局限于你一定要在什么时间，用什么技术 或者 必须通过什么途径去搞，相比传统渗透测试，红队则更趋于真实的入侵活动

这种场景其实对防御者的 实战对抗经验 和 技术深度 都是比较大的挑战

所以，以下的所有技术点也几乎都是完全站在这种场景和角度下来考量梳理的

需要特别说明的是，所有攻击手法在现实中都绝不是完全孤立使用的，往往很多手法都是相互灵活组合起来进行循环利用

由于绝大部分内容都是基于本人平时学习实战积累的一些经验，加之每个人的实际渗透思路都不同

所以肯定会有遗漏的地方，也欢迎弟兄们一起来积极指正补充完善

个人觉得，最好的防御永远不是怎么去防某个工具，是个明白人都知道，因为工具这些东西本身就是死的

稍微改下，定制下，现有的规则可能马上就防不住了，且一直会处于疲于应付的被动防御状态

尤其是针对红队这种特殊场景的，你的实际对手很可能都是有一定技术实力的人

所以针对每种核心的攻击技术技术展开做深入分析，直接从源头上进行防御才是最靠谱的

虽然说短期这种成本代价相对较高，但长期来看，是一劳永逸的，沉淀下来的这些东西最终也会慢慢形成自己产品的核心竞争力和特色

说白了，这种对抗，本质上拼的还是双方的技术实力，不仅要能在不知觉的情况下搞进去，而且要能无限制加大对方后期的溯源成本

另外，作为一名合格的攻防人员，工具的熟练掌握仅仅只是极小的一部分，对各种利用原理的深度理解和二次定制能力才是你的核心

## 日常流程简要说明





























































