渗透测试工程师技术实战课

网络安全之社会工程学应用

社会工程学基础

- 人为因素才是安全的软肋”。而社会工程学正是利用了人的恐惧、好奇等一系列心理，或者利用人们常见弱点，通过多种方式套取个人信息或者实施诈骗。网络钓鱼就是常见的社会工程学攻击之一

  《欺骗的艺术》凯文·米特尼克

- 社会工程学攻击的四个阶段
  - 信息收集(OSTINT、网盘、媒体、垃圾桶、物理)
  - 识别漏洞：与目标建立第一次接触(下套)
  - 规划攻击：与目标建立信任并获取信息
  - 退场：不引起目标怀疑的离开

社会工程学基础

- 粗心
  - 注册近似域名
  - 同形攻击
  - 点击劫持
  - 窃听
- 好奇心
  - 社交网站中的恶意软件活动（“热门视频”诈骗，明星丑闻等）
  - 其他欺骗你的独家内容（与事故或灾难相关的视频或图片等）
  - 社交媒体诈骗：“查一查谁访问了你的个人资料”、“测一测你今年运势如何”等；
  - USB攻击
- 恐惧心理
  - 商业邮件钓鱼/针对 CEO 或 CFO 的欺诈
  - 勒索/敲诈恶意软件
  - 伪装成软件补丁的恶意软件
  - 网络电话诈骗

社会工程学基础

- Setoolkit(Social-Engineering toolkit)
  - 站点克隆：1 2 3 2
  - WEB站点攻击向量：1 2 1 2
  - 中间文件全部存在 ~/.set/目录中

社会工程学基础

- Setoolkit(Social-Engineering toolkit)
  - 站点克隆：1 2 3 2
  - 中间文件全部存在 ~/.set/目录中
- Cobalt Strike
  - 端口转发
  - 监听
  - 生成Windows dll
  - 生成java木马
  - 宏病毒
  - 木马捆绑钓鱼攻击
  - 站点克隆

谢谢观赏