网安概论3

519021910025 钟睿哲

1. 黑客攻击的一般过程是什么?
    1. 预攻击（踩点和扫描）
        1. 目的:
           收集信息，进行进一步攻击决策
        2. 内容:
           获得域名及IP分布
           获得拓扑及OS等
           获得端口和服务
           获得应用系统情况
           跟踪新漏洞发布
    2. 攻击（入侵、获取权限、提升权限）
        1. 目的：进行攻击，获得系统的一定权限
        2. 内容:
           获得远程权限
           进入远程系统
           提升本地权限
           进一步扩展权限
           进行实质性操作
    3. 后攻击（清除日志、安插后门）
        1. 目的:
           消除痕迹，长期维持一定的权限
        2. 内容:
           植入后门木马
           删除日志
           修补明显的漏洞
           进一步渗透扩展
2. 网络信息安全产生的原因有哪些?
    1. 物理安全因素（物理设备和通信线路）
    2. 方案设计因素
    3. 系统安全因素
    4. TCP/IP协议的安全因素
    5. 人的因素

    1. 人员无意的始误和错误行为
    2. 人员的恶意攻击
    3. 管理上面的因素
3. 什么是社会工程学攻击?
    1. 社会工程学攻击，是一种通过受害者心里弱点、本能反应、好奇心、信任、贪婪等心里陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法。
    2. 黑客社会工程学是非传统的信息安全，它不是利用软件或系统的漏洞实现入侵的，黑客通过社会工程学攻击的方式只需要拨打一个电话，使用专用的术语，报出内部人员使用的账号信息，获取更多的信息，从而轻松绕过所有技术上的防护，实现恶意攻击的目的。
4. 常见的攻击方法有哪些？什么是缓冲区溢出攻击?
    1. 网络监听
    2. 密码破解
    3. 会话劫持攻击
    4. 缓冲区溢出攻击
    5. 拒绝服务攻击
    6. 网络蠕虫
    7. 木马攻击
    8. SQL注入攻击
    9. 缓冲区攻击：
        1. 缓冲区溢出攻击又称堆栈溢出：简单地说就是程序对接受的输入数据没有进行有效检测导致的错误，后果可能造成程序崩溃或者是执行攻击者的命令。缓冲区溢出漏洞在系统软件和应用软件中是大量存在的。
        2. 利用缓冲区溢出攻击可以导致：系统宕机、系统重启动、程序运行失败、获得非授权指令得到系统特权等。
        3. 在某些情况下，如果用户输入的数据长度超过应用程序给定的缓冲区，就会覆盖其他数据区。这就称“缓冲区溢出”。