渗透测试流程介绍

渗透测试

渗透测试一定要按照必要的流程才能更大地提高渗透测试的成功性，所以我们应该要好好地清楚渗透测试必要的流程。我们可以把渗透测试的流程分为6个阶段这6个阶段都是必不可少的。

前期交互

这个阶段是指与客户交流渗透测试的要求和确定和渗透团队确定攻击的范围。该阶段是收集客户的要求,并制定渗透测试的计划和对团队每个人的分配工作。

收集渗透目标的情报

收集渗透目标的情报是最重要的阶段。如果收集到有用的情报资料的话，可以大大提高对渗透测试的成功性。收集渗透目标的情报一般是对目标系统的分析，扫描探测,服务查点，扫描对方漏洞，查找对方系统IP等等。有时候渗透测试者也会使用上社会工程学。渗透测试者会尽力收集目标系统的配置与安全防御以及防火墙等等。

与团队交流阶段

收集好目标系统的情报后,不要急于渗透目标系统，要与渗透团队进行头脑风暴。往往一个人的力量是不够的，团队集合起交流的力量是非常强大的。因为团队里面每一个人所拥有的特点和特长都会不一样。大家交流的话，可以取长补短。所以与团队交流这个阶段可以确定更快,更容易地制定入侵目标系统的方案。

漏洞分析阶段

漏洞分析阶段要综合以上所有的阶段收集回来的情报。特别是漏洞扫描结果,服务器的配置，防火墙的使用情况情报最为重要。渗透测试者可以根据以上的情报进行开发渗透代码。渗透测试者会找出目标系统的安全漏洞和挖掘系统拥有的未知漏洞进行渗透。漏洞分析阶段是进行攻击的重要阶段。

入侵者可能利用的漏洞

软件编写存在bug；系统配置不当；口令失窃；嗅探未加密通讯数据；设计存在缺陷；系统攻击

渗透攻击阶段

来到渗透攻击的阶段渗透测试者就要利用找到的目标系统漏洞进行渗透入侵,从而得到管理权限。渗透攻击的代码可以利用公开的渠道获取渗透代码，也可以由渗透测试者马上开发针对目标系统的渗透代码。如果是黑盒测试的话，渗透攻击的难度就会加多许多。黑盒测试要考虑到目标系统的检测机制,和要防止被目标系统的应急响应团队的追踪。

报告阶段

渗透测试的过程和挖掘出的安全漏洞最终都会报告给客户。渗透测试员一般都会提交渗透时发现目标系统的不足，安全漏洞，配置的问题，防火墙的问题等等。以及渗透测试员会帮助他们进行对安全漏洞的修复,和其他问题的建议与帮助等等。