渗透测试流程

前期交互阶段

项目开展前的准备工作

与客户交流，确定渗透测试的目的、范围和时间

确定渗透测试的方式，如黑盒测试、白盒测试或灰盒测试

签订保密协议，确保客户的信息和测试结果不会泄露

与团队成员进行沟通，确保每个人都清楚自己的职责和任务

与客户保持沟通，及时反馈测试进展和结果

确定测试报告的格式和内容

与客户讨论测试结果，确定下一步的工作计划

项目管理

使用项目管理工具，如Trello、Asana或Jira，来跟踪和管理测试任务

设置任务的优先级和截止日期，确保测试工作按时完成

定期向客户汇报测试进展和结果，确保客户了解测试工作的情况

与团队成员协作，确保每个人都清楚自己的任务和责任

及时解决测试过程中遇到的问题和困难，确保测试工作顺利进行

信息收集阶段

信息收集是渗透测试的第一步，主要目的是通过各种手段获取目标系统的相关信息，为后续的攻击和渗透测试提供基础。

主动信息收集

主动信息收集是指通过直接与目标系统进行交互来获取信息的方法。这种方法通常会被目标系统记录下来，因此需要谨慎使用。

端口扫描

使用工具如Nmap、Masscan等对目标系统的端口进行扫描，以确定哪些端口是开放的。

服务识别

在确定开放端口后，需要进一步识别这些端口上运行的服务，以及这些服务的版本信息。

操作系统识别

通过分析目标系统的响应特征，可以推断出其操作系统的类型和版本。

漏洞扫描

使用漏洞扫描工具，如Nessus、OpenVAS等，对目标系统进行全面的漏洞扫描，以发现潜在的安全漏洞。

Web应用扫描

对于Web应用程序，可以使用专门的工具，如Burp Suite、OWASP ZAP等，进行深入的漏洞扫描和分析。

社会工程学

利用人性的弱点，通过欺骗、诱导等手段获取目标系统的信息。

钓鱼攻击

制作伪造的登录页面或邮件，诱导目标用户输入敏感信息。

社交媒体挖掘

从社交媒体平台上获取目标用户的个人信息和动态，以便进行针对性的攻击。

物理访问

尝试通过物理手段访问目标系统，如破坏门锁、使用钥匙卡等。

被动信息收集

被动信息收集是指在不与目标系统直接交互的情况下，通过公开渠道获取目标系统的相关信息。这种方法通常不会被目标系统记录下来，因此相对安全。

公开信息查询

通过搜索引擎、社交媒体、公开数据库等渠道，查询目标系统的公开信息，如域名注册信息、IP地址、网站结构等。

DNS信息收集

通过查询DNS记录，获取目标系统的域名解析信息，如子域名、邮件服务器等。

网络流量分析

通过监听网络流量，分析目标系统的通信协议、数据传输等，以获取敏感信息。

社交媒体挖掘

从社交媒体平台上获取目标用户的个人信息和动态，以便进行针对性的攻击。

搜索引擎利用

利用搜索引擎的高级搜索功能，如Google Dorking，查找目标系统的敏感信息。

漏洞利用阶段

漏洞利用阶段是渗透测试的核心阶段，主要目的是通过已知的漏洞或攻击手段，获取目标系统的访问权限。

漏洞利用

漏洞利用是指通过已知的漏洞或攻击手段，获取目标系统的访问权限。

漏洞选择

根据目标系统的操作系统、应用程序等信息，选择合适的漏洞进行利用。

漏洞利用工具

使用专业的漏洞利用工具，如Metasploit、Exploit-DB等，可以大大提高漏洞利用的效率和成功率。

手动漏洞利用

对于一些特殊的漏洞，可能需要手动编写利用代码进行攻击。

权限提升

获取初始访问权限后，通常需要进一步提升权限，以获取更高的系统控制权。

本地权限提升

利用本地系统的漏洞或配置错误，提升权限。

域权限提升

在域环境中，利用域控制器的漏洞或配置错误，提升权限。

后渗透阶段

后渗透阶段是指在成功获取目标系统访问权限后，进一步深入挖掘系统内部的敏感信息，并尽可能地扩大攻击范围。

信息收集

信息收集是后渗透阶段的重要任务之一，主要目的是获取更多的目标系统内部信息，为后续的攻击和渗透测试提供更多的线索。

系统信息收集

收集目标系统的操作系统版本、补丁安装情况、已安装的软件列表等信息。

网络信息收集

收集目标系统的网络配置信息，如IP地址、子网掩码、网关、DNS服务器等。

用户信息收集

收集目标系统的用户账户信息，如用户名、密码哈希值、用户组等。

敏感数据查找

在目标系统中查找敏感数据，如数据库文件、配置文件、日志文件等。

权限维持

权限维持是指在成功获取目标系统访问权限后，采取一些措施来保持这种访问权限，以便后续的攻击和渗透测试。

后门程序

在目标系统中植入后门程序，以便在需要时重新获取访问权限。

计划任务

利用操作系统的计划任务功能，定期执行某些脚本或程序，以维持访问权限。

服务劫持

通过修改或替换目标系统的服务程序，以维持访问权限。

痕迹清除

在完成渗透测试后，清除在目标系统上留下的痕迹，以避免被发现。

日志清除

清除目标系统的日志文件，以隐藏攻击行为。

文件删除

删除在目标系统上创建的临时文件和工具，以减少被发现的风险。

时间戳修改

修改文件的时间戳，以隐藏攻击行为。

报告撰写

在完成渗透测试后，需要撰写一份详细的报告，总结测试过程、发现的漏洞、攻击路径等信息，并提出修复建议。

报告结构

报告通常包括以下几个部分：执行摘要、测试范围、测试方法、发现的漏洞、攻击路径、修复建议等。

报告内容

报告内容应该详细描述每个发现的漏洞，包括漏洞的原理、影响范围、利用方法等。

报告格式

报告可以采用多种格式，如PDF、Word、HTML等，根据客户的需求选择合适的格式。

报告交付

在完成报告撰写后，需要将报告交付给客户，并进行必要的解释和说明。