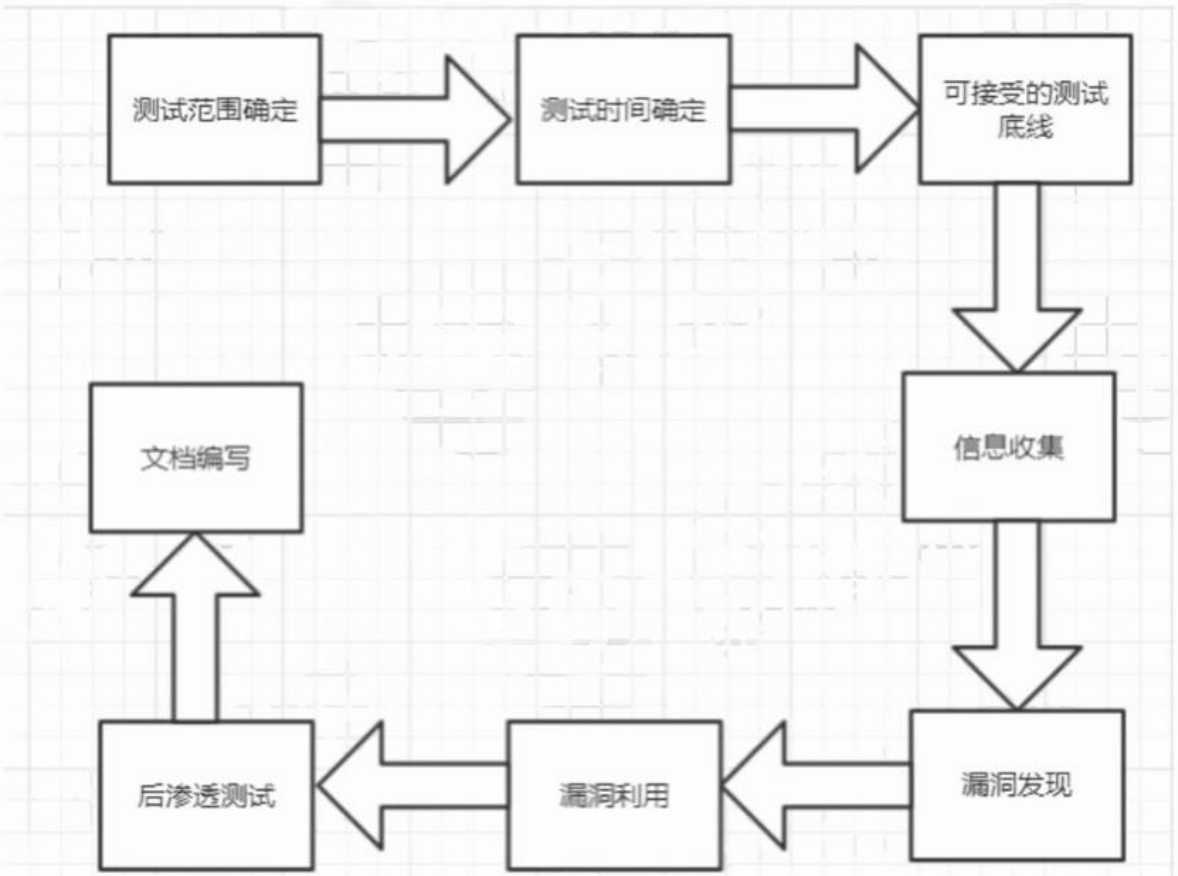
渗透测试工程师技术实战课

渗透测试报告

渗透测试的标准

- 渗透测试是指渗透人员在不同的位置（比如从内网、从外网等位置）利用各种手段对某个特定网络进行测试，以期发现和挖掘系统中存在的漏洞，然后输出渗透测试报告，并提交给网络所有者。网络所有者根据渗透人员提供的渗透测试报告，可以清晰知晓系统中存在的安全隐患和问题。

渗透测试的标准



明确目标

明确目标

- 确定范围：测试目标的范围，ip，域名，内外网
- 确定规则：能渗透到什么程度，时间？能否修改上传？能否提权？哪些社工手段不能使用等
- 确定需求：web应用的漏洞(新上线程序)、业务逻辑漏洞（针对业务的）、人员权限管理漏洞（针对人员、权限）、等等

信息收集

- 主动信息搜集：通过直接访问和扫描信息的方式进行收集信息，缺点是会记录自己的操作信息
- 被动信息搜集：通过第三方服务进行信息搜集，缺点是收集信息有限
- 针对域名
  - 真实ip查询
  - 网站的各种探针类文件，如phpinfo里面的_SERVER["SERVER_ADDR"]也包含的有服务器端的真实ip
  - 通过shodan/zoomeye/fofa搜索网站特殊标题、内容、网站源码
  - whois信息查询
  - 利用搜索引擎发现和侦察信息泄露，如google hacking获得后台，未授权页面，敏感url等
  - 旁站C段查询、子域名信息收集
  - 历史漏洞收集(exploitdb 、hackerone、CNVD 、乌云漏洞库镜像站)/社工
  - 敏感目录/文件/端口信息/网站备案信息
  - F12审查网页元素

漏洞发现

- 漏洞扫描
  - 不同权限的账号测试，了解业务逻辑
- sql注入 (记住千万不要拿任何数据)
- xss漏洞
- 上传漏洞
- 逻辑漏洞
- csrf
- 未授权访问/弱口令
- 各种框架漏洞
- 敏感信息泄露…

漏洞验证/后渗透阶段

- 组合漏洞
- 后渗透阶段
  - 内网渗透
  - 权限维持
  - 权限提升
  - 读取用户hash
  - 浏览器密码

报告编写

- 确漏洞名称以及漏洞原理
- 注明参与人员，测试时间，内网外网
- 按需整理：按照之前第一步跟客户确定好的范围，需求来整理资料，并将资料形成报告
- 补充介绍：要对漏洞成因，验证过程和带来危害进行分析
- 修补建议：当然要对所有产生的问题提出合理高效安全的解决办法
- 风险规避
  - 不要进行诸如ddos攻击，不破坏数据
  - 测试之前对重要数据进行备份
  - 任何测试执行前必须和客户进行沟通，以免引来不必要的麻烦
  - 可以对原始系统生成镜像环境，然后对镜像环境进行测试
  - 明确渗透测试范围

谢谢观赏