PTES渗透测试执行标准（诸葛建伟翻译）

- 1 前期交互阶段
  - 确定范围
    - 如何确定范围
    - 时间估计
      - 预估整体项目的时间周期
      - 确定以小时计的额外技术支持
    - 问答交谈
      - 对业务管理部门的问答交流
      - 对系统管理员的问答交流
      - 对IT支持的问答交流
      - 与普通雇员的问答交流
    - 范围勘定
      - 确定项目起止时间
      - 项目授权信件
      - 进入目标规划环节
    - 确定IP和域名范围
      - 验证范围
  - 目标规划
    - 处理第三方资源
      - 云服务
      - ISP
      - 网站宿主
      - MSSP
      - 服务器所在国家
    - 定义可接受的社会工程学方法
      - 拒绝服务测试
      - 确定交付细节
      - Delphi Scoping?
    - 确定目标
      - 首要目标
      - 额外目标
    - 业务分析
      - 定义目标企业的安全成熟度
    - 需求分析
  - 测试术语和定义
    - 渗透测试术语词汇表
  - 建立通讯渠道
    - 紧急联络方式
    - 应急响应流程
    - 进展报告周期
    - 确定一个接口联络人
    - PGP或其他加密方式
    - 取得与外部第三方的联络方式（宿主…）
  - 交互确定规则
    - 时间线
    - 地点
    - 渗透攻击的控制禁线
    - 敏感信息的放置
    - 证据处理
    - 例行的进展报告会
      - 计划
      - 进展
      - 问题
    - 每天可进行渗透测试的时间
    - 避开的范围与规则
    - 攻击授权
  - 存在的防御能力和技术
    - 应急响应和监控
  - 保护你自己
    - 准备你的测试系统
    - 前期交互检查表
    - 数据包监听
    - 后期交互检查表
- 2 情报搜集
  - 目标选择
  - 开放渠道情报
    - 企业
      - 物理
        - 位置
        - 分布
        - 关系网
      - 逻辑
        - 业务伙伴
        - 竞争对手
        - 接触关联图
        - 物业服务轮廓图
        - 产品线
        - 垂直市场
        - 销售银行帐号
        - 会议安排
        - 关键企业日期
        - 招聘岗位
        - 慈善事业关系
      - 组织架构
      - 电子
      - 财务
    - 个人
      - 雇员
        - 履历背景
        - 社交关系网
        - 互联网足迹
        - 博客
        - 最新动态
        - 物理位置
        - 移动足迹
        - 工资银行帐户
  - 白盒搜集
    - 场内搜集
    - 场外搜集
  - 人力资源情报
    - 关键雇员
    - 合作伙伴/供应商
    - 社会工程学
  - 踩点
    - 外部踩点
      - 建立目标列表
        - 识别客户范围
        - 被动信息搜集
        - 主动探测
        - 确定版本信息
        - 识别补丁级别
        - 搜索脆弱的Web应用
        - 确定封禁阈值
        - 出错信息
        - 找出攻击的脆弱端口
        - 过时系统
        - 虚拟化平台和虚拟机
        - 存储基础设施
      - 主动探测
        - 端口扫描
        - SNMP探查
        - 区域传送
        - SMTP反弹攻击
        - 解析DNS与递归DNS服务器
      - 被动信息搜集
      - 建立目标列表
    - 内部踩点
      - 旗标攫取
      - VoIP扫描
      - ARP探索
      - DNS探索
  - 识别防御机制
    - 网络防御机制
      - 简单包过滤
      - 流量整形设备
      - 信息泄露防护系统
      - 加密／隧道机制
    - 系统防御机制
      - 堆栈保护
      - 白名单列表
      - 反病毒软件/过滤/行为检测
      - 信息泄露防护系统
    - 应用层防御机制
      - 识别应用层防御
      - 编码选项
      - 可能潜在的绕过机制
      - 白名单区域
    - 存储防御机制
      - 硬盘保护卡
      - ……
- 3 威胁建模
  - 业务资产分析
    - 私人身份信息，私人健康信息和信用卡信息
    - 定义和找出组织的知识产权
    - 企业王国的关键资产
      - 商业秘密
      - 研究和开发
      - 市场计划
      - 企业银行/信用卡帐户
      - 客户资料
      - 供应商资料
    - 关键雇员信息
      - 董事会
      - 中间管理层
      - 系统管理员
      - 工程师
      - 技术专家
      - 人力资源
      - 总裁助理
  - 业务流程分析
    - 使用的基础设施
      - 人力基础设施
      - 使用的第三方平台
  - 威胁对手/社区分析
    - 内部人员
      - 董事会
      - 中间管理层
      - 系统管理员
      - 开发者
      - 工程师
      - 技术专家
    - 竞争对手
      - 国家政府
      - 有组织的犯罪团队
      - 周末工作的网际武士
  - 威胁能力分析
    - 分析使用的工具
    - 可用的相关渗透代码和攻击载荷
    - 通讯机制（加密，下载站点，命令控制，安全宿主站点）
    - 找出相关公司被攻击的新闻
- 4 漏洞分析
  - 测试
    - 主动
      - 自动化技术
        - 通用漏洞扫描
          - 基于端口
          - 基于服务
          - 旗标攫取
        - Web应用扫描器
          - 通用的应用层漏洞扫描
          - 目录列举和暴力破解
          - Web服务版本和漏洞辨识
          - 存有漏洞的方法
        - 网络漏洞扫描器
          - VPN
          - IPv6
        - 语音网络扫描
          - 战争拨号
          - VoIP扫描
      - 手工方法
        - 针对性连接
      - 躲避技术
        - 多源探测
        - IDS选逸
        - 可变的速度
        - 可变的范围
    - 被动
      - 自动化技术
        - 从内部获取的元数据分析
        - 流量监控（如POf等）
      - 手工方法
        - 针对性连接
  - 验证
    - 扫描器结果关联分析
    - 手工验证/协议相关
      - VPN
        - 指纹识别
      - Citrix
        - 查点
      - DNS
      - Web
      - Mail
    - 攻击路径
      - 创建攻击树
    - 隔离实验室中试验
    - 效果确认
      - 手工验证与评审
  - 研究
    - 对公开资源的研究
      - exploit-db
      - Google Hacking
      - 渗透代码网站
      - 通用/缺省口令
      - 厂商的漏洞警告
    - 私有环境下的研究
      - 建立一个复制环境
      - 测试安全配置
      - 找出潜在攻击路径
- 5 渗透攻击
  - 精准打击
  - 绕过防御机制
    - 反病毒
      - 编码
      - 加壳
      - 白名单绕过
      - 进程注入
      - 纯内存方式
    - 人工检查
    - 网络入侵防御系统
    - DEP
    - ASLR
    - VA+NX(Linux)
    - w^x(openBSD)
    - Web应用防火墙
    - 栈保护
  - 定制渗透攻击路径
    - 最佳攻击路径
    - 零日攻击
      - Fuzzing
      - 逆向分析
      - 流量分析
    - 公开渗透代码的定制
    - 物理访问
      - 人为因素
      - 主机访问
      - USB接口访问
      - 防火墙
      - RFID
      - 中间人攻击
      - 路由协议
      - VLAN划分
      - 其他硬件（键盘记录器等）
    - 接近的访问（WiFi）
      - 攻击AP
      - 攻击用户
      - 电子频谱分析
    - 拒绝服务/勒索
    - Web
      - SQLi
      - XSS
      - CSRF
      - 信息泄露
      - 其他OWASP Top 10
  - 绕过检测机制
    - FW/WAF/IDS/IPS绕过
    - 绕过管理员
    - 绕过数据泄露防护系统
  - 触发攻击响应控制措施
  - 渗透代码测试
  - 攻击类型
    - 客户端攻击
      - Phishing
    - 服务端攻击
    - 带外攻击
- 6 后渗透攻击
  - 基础设施分析
    - 当前网络连接分析
    - 网络接口查询
    - VPN检测
    - 路由检测，包括静态路由
    - 网络邻居与系统探查
    - 使用的网络协议
    - 使用的代理服务器
    - 网络拓扑
  - 高价值目标识别
  - 掠夺敏感信息
    - 视频监控器和摄像头
    - 从可用通道获取敏感数据
    - 查找共享目录
    - 音频监控
      - VoIP
      - 麦克风记录
    - 离价值文件
    - 数据库查点
    - WiFi
    - 源代码库
    - 识别出客户管理应用
    - 备份
      - 本地备份文件
      - 中央备份服务器
      - 远程备份方案
      - 录音存储备份
  - 业务影响攻击
    - 业务盈利途径
    - 窃取业务盈利
  - 进一步对基础设施的渗透
    - 僵尸网络
    - 入侵内网
    - 检查历史/日志
      - Windows
      - Linux
      - 浏览器
  - 掩踪灭迹
    - 记录渗透攻击过程步骤
    - 确保清理现场
    - 删除测试数据
    - 对证据进行打包和加密
    - 必要时从备份恢复数据
  - 持续性存在
    - 自启动恶意代码
    - 反向连接
    - Rootkit
      - 用户模式
      - 内核模式
    - 命令控制媒介（http, dns, tcp, icmp）
    - 后门
    - 植入代码
    - 口令保护的VPN
- 7 报告
  - 执行层面的报告
    - 业务影响
    - 定制
    - 与业务部门的谈话
    - 影响底线
    - 策略方法路径
    - 成熟度模型
    - 风险评估术语说明
    - 攻击过程与Gant图时间线
    - 风险评估
      - 评估事故频率
        - 可能的事件频率
        - 估计威胁能力(从阶段3威胁建模阶段而来)
        - 评估控制措施强度（从阶段6）
        - 安全漏洞与弱点评估（从阶段5）
        - 所需技能要求
        - 所需访问权限等级
      - 每次事故的损失估计
      - 风险推算
        - 威胁
        - 漏洞
        - 组合风险值
  - 技术报告
    - 识别系统性问题和技术根源分析
    - 渗透测试评价指标
      - 范围内的系统数量
      - 范围内的应用场景数量
      - 范围内的业务流程数量
      - 被检测到的次数
      - 漏洞/漏洞主机数量
      - 被攻陷的系统数量
      - 成功攻击的应用场景数量
      - 攻陷的业务流程次数
      - ……
    - 技术发现
      - 描述
      - 截图
      - 抓取的请求与响应
      - 概念验证性样本代码
    - 可重现结果
      - 测试用例
      - 触发错误
    - 应急响应和监控能力
      - 情报收集阶段
      - 漏洞分析阶段
      - 渗透攻击阶段
      - 后渗透攻击阶段
      - 其他方面（知对第三方的通知等）
    - 标准组成部分
      - 方法体系
      - 目标
      - 范围
      - 发现摘要
      - 风险评定的术语附录
  - 提交报告
    - 初始报告
    - 客户对报告的评审结果
    - 对报告的修订
    - 最终报告
    - 报告初稿与最终报告的版本管理
    - 展示报告
      - 技术层面
      - 管理层面
    - 工作例会/培训
      - 差距分析（技能/培训）
    - 保存证据和其他非产权的数据
    - 纠正过程
      - 分流
      - 安全成熟度模型
      - 工作进展计划
      - 长期解决方案
      - 定义限制条件
    - 开发定制工具