## PTES渗透测试执行标准

※前期交互阶段

◎确定范围

〇如何确定范围

〇时间估计

Ｏ预估整体项目的时间周期

Ｏ确定以小时计的额外技术支持

〇问答交谈

Ｏ对业务管理部门的问答交流

Ｏ对系统管理员的问答交流

Ｏ对IT支持的问答交流

Ｏ与普通雇员的问答交流

〇范围勘定

Ｏ确定项目起止时间

Ｏ项目授权信件

Ｏ进入目标规划环节

〇确定IP和域名范围

Ｏ验证范围

〇处理第三方资源

Ｏ云服务

ＯISP

Ｏ网站宿主

ＯMSSP

Ｏ服务器所在国家

〇定义可接受的社会工程学方法

〇拒绝服务测试

〇确定支付细节

〇Delphi Scoping？

◎目标规划

〇确定目标

Ｏ首要目标

Ｏ额外目标

〇业务分析

Ｏ定义目标企业的安全成熟度

〇需求分析

◎测试术语和定义

〇渗透测试术语词汇表

◎建立通讯渠道

〇紧急联络方式

〇应急响应流程

〇进展报告周期

〇确定一个接口联络人

〇PGP或其他加密方式

〇取得与外部第三方的联络方式（宿主...）

◎交互确定规则

〇时间线

〇地点

〇渗透攻击的控制基线

〇敏感信息的披露

〇证据处理

〇例行的进展报告会

Ｏ计划

Ｏ进展

Ｏ问题

〇每天可进行渗透测试的时间

〇避开的范围与规则

〇攻击授权

◎存在的防御能力和技术

〇应急响应和监控

◎保护你自己

〇准备你的测试系统

〇前期交互检查表

〇数据包监听

〇后期交互检查表

※情报收集

◎目标选择

◎开放渠道情报

〇企业

Ｏ物理

**\***位置信息

**\***分布位置

**\***关系网

Ｏ逻辑

**\***业务伙伴

**\***竞争对手

**\***接触关联图

**\***业务服务轮廓图

**\***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

Ｏ组织架构

Ｏ电子

Ｏ财务

〇个人

Ｏ雇员

Ｏ履历背景

Ｏ社交关系网

Ｏ互联网足迹

Ｏ博客

Ｏ最新动态

Ｏ物理位置

Ｏ移动足迹

Ｏ工资银行帐户

◎白盒搜集

〇场内搜集

〇场外搜集

◎人力资源情报

〇关键雇员

〇合作伙伴/供应商

〇社会工程学

◎踩点

〇外部踩点

Ｏ识别客户范围

Ｏ被动信息搜集

Ｏ主动探测

Ｏ建立目标列表

**\***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

〇内部踩点

Ｏ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

**\***旗标攫取

**\***VoIP扫描

**\***ARP探索

**\***DNS探索

Ｏ被动信息搜集

Ｏ建立目标列表

◎识别防御机制

〇网络防御机制

Ｏ简单包过滤

Ｏ流量整形设备

Ｏ信息泄露防护系统

Ｏ加密／隧道机制

〇系统防御机制

Ｏ堆栈保护

Ｏ白名单列表

Ｏ反病毒软件/过滤/行为检测

Ｏ信息泄露防护系统

〇应用层防御机制

Ｏ识别应用层防御

Ｏ编码选项

Ｏ可能潜在的绕过机制

Ｏ白名单区域

〇存储防御机制

Ｏ硬盘保护卡

Ｏ......

※威胁建模

◎业务资产分析

〇私人身份信息，私人健康信息和信用卡信息

〇定义和找出组织的知识产权

〇企业王国的关键资产

Ｏ商业秘密

Ｏ研究和开发

Ｏ市场计划

Ｏ企业银行/信用卡帐户

Ｏ客户资料

Ｏ供应商资料

Ｏ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

〇使用的基础设施

〇人力基础设施

〇使用的第三方平台

◎威胁对手/社区分析

〇内部人员

Ｏ董事会

Ｏ中间管理层

Ｏ系统管理员

Ｏ开发者

Ｏ工程师

Ｏ技术专家

〇竞争对手

〇国家政府

〇有组织的犯罪团队

〇周末工作的网际武士

◎威胁能力分析

〇分析使用的工具

〇可用的相关渗透代码和攻击载荷

〇通讯机制（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

※ 漏洞分析

◎测试

〇主动

Ｏ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

Ｏ手工方法

**\***针对性连接

Ｏ躲避技术

**\***多源探测

**\***IDS逃逸

**\***可变的速度

**\***可变的范围

Ｏ白盒代码审计

**\***白盒漏洞挖掘（0day）

**\***白盒漏洞复现（nday）

**\***白盒既有漏洞补丁绕过（bypass）

〇被动

Ｏ自动化技术

**\***从内部获取的元数据分析

**\***流量监控（如P0f等）

Ｏ手工方法

**\***针对性连接

◎验证

〇扫描器结果关联分析

〇手工验证/协议相关

ＯVPN

**\***指纹识别

ＯCitrix

**\***查点

ＯDNS

ＯWeb

ＯMail

〇攻击路径

Ｏ创建攻击树

〇隔离实验室中试验

〇效果确认

Ｏ手工验证与评审

◎研究

〇对公开资源的研究

Ｏexploit-db

ＯGoogle Hacking

Ｏ渗透代码网站

Ｏ通用/缺省口令

Ｏ厂商的漏洞警告

〇私有环境下的研究

Ｏ建立一个复制环境

Ｏ测试安全配置

Ｏ找出潜在攻击路径

※ 渗透攻击

◎精准打击

◎绕过防御机制

〇反病毒

Ｏ编码

Ｏ加壳

Ｏ白名单绕过

Ｏ进程注入

Ｏ纯内存方式

〇人工检查

〇网络入侵防御系统

〇DEP

〇ASLR

〇VA+NX(Linux)

〇w^x(openBSD)

〇Web应用防火墙

〇栈保护

◎定制渗透攻击路径

〇最佳攻击路径

〇零日攻击

ＯFuzzing

Ｏ逆向分析

Ｏ流量分析

〇公开渗透代码的定制

〇物理访问

Ｏ人为因素

Ｏ主机访问

ＯUSB接口访问

Ｏ防火墙

ＯRFID

Ｏ中间人攻击

Ｏ路由协议

ＯVLAN划分

Ｏ其他硬件 （键盘记录器等）

〇接近的访问（WiFi）

Ｏ攻击AP

Ｏ攻击用户

Ｏ电子频谱分析

〇拒绝服务/勒索

〇Web

ＯSQLi

ＯXSS

ＯCSRF

Ｏ信息泄露

Ｏ其他OWASP Top 10

◎绕过检测机制

〇FW/WAF/IDS/IPS绕过

〇绕过管理员

〇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

〇客户端攻击

ＯPhishing

〇服务端攻击

〇带外攻击

※后渗透攻击

◎基础设施分析

〇当前网络连接分析

〇网络接口查询

〇VPN检测

〇路由检测，包括静态路由

〇网络邻居与系统探查

〇使用的网络协议

〇使用的代理服务器

〇网络拓扑

◎高价值目标识别

◎掠夺敏感信息

〇视频监控器和摄像头

〇从可用通道获取敏感数据

〇查找共享目录

〇音频监控

ＯVoIP

Ｏ麦克风记录

〇高价值文件

〇数据库查点

〇WiFi

〇源代码库

〇识别出客户管理应用

〇备份

Ｏ本地备份文件

Ｏ中央备份服务器

Ｏ远程备份方案

Ｏ录音存储备份

◎业务影响攻击

〇业务盈利途径

〇窃取业务盈利

◎进一步对基础设施的渗透

〇僵尸网络

〇入侵内网

〇检查历史/日志

ＯWindows

ＯLinux

Ｏ浏览器

◎掩踪灭迹

〇记录渗透攻击过程步骤

〇确保清理现场

〇删除测试数据

〇对证据进行打包和加密

〇必要时从备份恢复数据

◎持续性存在

〇自启动恶意代码

〇反向连接

〇Rootkit

Ｏ用户模式

Ｏ内核模式

〇命令控制媒介（http, dns, tcp, icmp）

〇后门

〇植入代码

〇口令保护的VPN

※ 报告

◎执行层面的报告

〇业务影响

〇定制

〇与业务部门的谈话

〇影响底线

〇策略方法路径

〇成熟度模型

〇风险评估术语说明

〇攻击过程与Gant图时间线

〇风险评估

Ｏ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

Ｏ每次事故的损失估计

Ｏ风险推算

**\***威胁

**\***漏洞

**\***组合风险值

◎技术报告

〇识别系统性问题和技术根源分析

〇渗透测试评价指标

Ｏ范围内的系统数量

Ｏ范围内的应用场景数量

Ｏ范围内的业务流程数量

Ｏ被检测到的次数

Ｏ漏洞/漏洞主机数量

Ｏ被攻陷的系统数量

Ｏ成功攻击的应用场景数量

Ｏ攻陷的业务流程次数

Ｏ......

〇技术发现

Ｏ描述

Ｏ截图

Ｏ抓取的请求与响应

Ｏ概念验证性样本代码

〇可重现结果

Ｏ测试用例

Ｏ触发错误

〇应急响应和监控能力

Ｏ情报收集阶段

Ｏ漏洞分析阶段

Ｏ渗透攻击阶段

Ｏ后渗透攻击阶段

Ｏ其他方面（如对第三方的通知等）

〇标准组成部分

Ｏ方法体系

Ｏ目标

Ｏ范围

Ｏ发现摘要

Ｏ风险评定的术语附录

◎提交报告

〇初始报告

〇客户对报告的评审结果

〇对报告的修订

〇最终报告

〇报告初稿与最终报告的版本管理

〇展示报告

Ｏ技术层面

Ｏ管理层面

〇工作例会/培训

Ｏ差距分析（技能/培训）

〇保存证据和其他非产权的数据

〇纠正过程

Ｏ分流

Ｏ安全成熟度模型

Ｏ工作进展计划

Ｏ长期解决方案

Ｏ定义限制条件

〇开发定制工具