渗透测试基础知识

什么是渗透测试

是一种基于道德的尝试，旨在测试和分析保护这些资产和信息的安全防御措施。

伦理

开始前要进行讨论，构成测试协议范围。
黑白灰帽

ROE是在测试初始阶段创建的一份文件。包含三个主要部分最终决定了测试的执行方式。
允许部分、测试范围部分、规则 规则指定了允许使用的技术

测试方法

测试过程中采取的呃呃步骤被称为方法论。实用的方法论是一种巧妙的方法，采取的步骤与当前情况息息相关。
方法的总体主题：信息收集、枚举/扫描、开发、权限提升、后期开发

OWASP

Open Web Application Security Project用于测试Web应用程序和服务的安全性
指出网络应用可能存在的十大安全漏洞、测试方法和补救措施
Adv:易掌握和理解、积极维护且常更新、涵盖参与的所有阶段，专注于网络应用程序和服务
DisAdv:不清楚Web存在哪种类型的漏洞，可能会重叠、不针对任何特定开发周期提出建议、不具备认证 总体内容，全面化内容，类似百度百科

NIST网络安全框架1.1

流行 用于提升机构的网络安全标准并管理网络威胁的风险。为关键基础设施(eg.发电厂)到商业机构的各类机构提供了安全控制指南和成功基准。
Adv.覆盖范围广、制定标准详细、更新频繁、为使用者提供认证、旨在和其他框架一起实施
DisAdv.迭代多，很难决定哪一个适用于组织、审计弱，很难确定违规行为如何发生、未考虑云计算

NCSC CAF

用于评估网络威胁风险以及组织对这些威胁的防御措施
主要关注并评估以下主题：数据安全、系统安全、身份和访问控制、弹性化、监控、响应和恢复计划

Adv:得到政府网安机构支持、提供认证、涵盖了从安全到响应的14项原则
DisAdv:该框架在业内属较新、基于原则和思想，没有具体规则

黑白灰盒测试

黑盒：测试人员不会获得有关应用程序或服务内部运作的任何信息、显著增加了在信息收集和枚举阶段了解目标攻击面所花费的时间。
灰盒：了解有限，类似黑盒 提供有限知识节省时间
白盒：对应用程序和预期行为有充分了解，比黑盒测试耗时，其中的全面知识提供了一种测试方法，可以确保验证整个攻击面