

# CISP-PTE考试题型及必备题库学习资料

## 一、CISP-PTE 认证简介

**CISP-PTE** (Certified Information Security Professional – Penetration Test Engineer)，即**注册信息安全专业人员-渗透测试工程师**，是中国信息安全测评中心（CNITSEC）推出的国家级信息安全专业人员认证。该认证专注于培养和考核学员的**实际网络安全渗透测试能力**，是衡量渗透测试工程师专业水平的重要标准。

## 二、考试题型与结构

CISP-PTE考试总分为 **100分**，**70分及以上**为通过。考试形式结合了理论知识和实战操作，旨在全面检验考生的理论基础和动手能力。

题型	数量	分值	占比	考察内容
客观单项选择题	20题	20分	20%	基础理论、法律法规、渗透测试流程等理论知识。
实操题	5题	50分	50%	针对特定漏洞（如SQL注入、文件上传等）的独立渗透操作，每题需获取一个Key。
综合渗透题	1题	30分	30%	模拟真实环境，要求考生从信息收集到权限获取的完整渗透过程，需获取多个Key。

**考试特点：**

- 重实战：** 实操题和综合渗透题占总分的80%，对考生的实际操作能力要求极高。
- 靶场环境：** 考试在特定的靶场环境中进行，考生需通过渗透手段获取Flag（Key）来得分。

### 三、核心知识体系（必备学习资料）

CISP-PTE的知识体系大纲围绕渗透测试的四大核心领域展开，是备考的“必备学习资料”框架。

知识类别	核心内容概述	学习重点
Web安全基础	HTTP协议、Web常见漏洞（SQL注入、XSS、CSRF、文件上传、文件包含、SSRF、反序列化等）。	掌握各类Web漏洞的原理、利用方法和修复建议。
中间件安全	Apache、IIS、Tomcat、Weblogic、JBoss、Websphere等主流中间件的配置缺陷和漏洞利用。	熟悉中间件的默认配置、常见漏洞（如弱口令、未授权访问）及提权思路。
操作系统安全	Windows和Linux操作系统的基础安全机制、信息收集、权限提升、后门技术。	熟练掌握Windows和Linux下的提权技巧和常用命令。
数据库安全	Mssql、Mysql、Oracle、Redis等数据库的注入、提权、安全配置。	掌握数据库注入的各种技巧，以及通过数据库获取系统权限的方法。

### 四、必备题库与学习资料（干货细化）

CISP-PTE的备考资料应聚焦于实战技术和核心知识点的深入理解。以下是针对各知识点的具体“干货”内容：

1. Web安全实操重点与绕过技巧

漏洞类型	核心干货内容	绕过技巧 (Bypass)
SQL注入	盲注技术 (布尔盲注、时间盲注)、联合查询、报错注入、利用SQLi读写文件 (如 <code>into outfile</code> )。	空格绕过: 使用 <code>/**/</code> 、 <code>()</code> 、 <code>%0a</code> 等代替空格。引号绕过: 使用Hex编码或 <code>CHAR()</code> 函数。函数绕过: 使用等价函数或大小写混淆。
文件上传	MIME类型绕过、黑名单绕过 (大小写、特殊字符、点号空格)、解析漏洞利用 (如Apache、IIS、Nginx)、条件竞争。	双写后缀: <code>php.php</code> 、 <code>php5.php</code> 。0x00截断: 利用系统对文件名处理的差异。图片马: 结合文件包含漏洞执行代码。
文件包含	本地文件包含 (LFI) 读取敏感文件、远程文件包含 (RFI) 执行远程代码、Session文件包含、日志文件包含。	路径截断: 利用 <code>../</code> 或 <code>./</code> 进行路径遍历。过滤器利用: 使用 <code>php://filter</code> 读取源码。
命令执行	无回显命令执行 (利用DNS外带、延时)、管道符/连接符 ( <code>`</code>	<code>,</code> 、 <code>&amp;</code> 、 <code>&amp;&amp;</code> 、

2. 操作系统安全 (提权) 实操重点

操作系统	核心干货内容	提权工具与方法
Linux提权	内核漏洞提权 (如Dirty Cow、CVE-2021-4034等)、SUID/SGID文件利用、定时任务 (Cron) 滥用、不安全配置 (如 <code>/etc/passwd</code> 权限)。	信息收集: <code>uname -a</code> 、 <code>cat /etc/issue</code> 。自动化脚本: <code>LinEnum.sh</code> 、 <code>LinPEAS</code> 。内核利用: 使用 <code>searchsploit</code> 查找对应漏洞的C语言代码, 并在目标机上编译执行。
Windows提权	内核漏洞提权、服务配置错误 (不安全的 <code>服务路径</code> 、权限)、令牌窃取 (Token Impersonation)、未引用的服务路径 (Unquoted Service Path)。	自动化脚本: <code>PowerSploit</code> 、 <code>WinPEAS</code> 。手动检查: 检查服务权限、注册表配置、系统补丁情况。

3. 数据库与中间件安全

- 数据库安全: 重点掌握数据库的默认端口、弱口令爆破、利用数据库特性进行提权 (如MySQL的UDF提权、MSSQL的 `xp_cmdshell`)。

- **中间件安全：**熟悉主流中间件（如Tomcat、Weblogic）的**默认管理后台路径、弱口令、反序列化漏洞**（如Weblogic T3协议）。

## 4. Webshell隐藏与免杀技术

在实操中，成功上传Webshell后，如何维持权限和躲避检测是关键。

- **语法逻辑免杀：**使用生僻函数、异或、取反等方式混淆代码，避免被静态特征码检测。
- **动态隐藏：**将Webshell代码插入到目标网站的**函数库文件或配置文件**等不显眼的位置，或利用**图片马**结合文件包含漏洞执行。
- **流量隐藏：**使用自定义的加密通信协议或利用HTTP协议的特定字段进行数据传输，躲避流量监控。

## 五、备考建议

---

- **以实操为核心：**将80%的精力投入到实操练习中，确保能够独立完成信息收集、漏洞利用、权限提升和后门清除的完整渗透流程。
- **熟悉靶场环境：**尽量在与考试环境相似的靶场中练习，熟悉工具的使用和操作系统的特性。
- **理论不放松：**理论选择题虽然只占20%，但却是实操的基础。务必通过培训讲义和题库，巩固基础理论知识。
- **总结归纳：**对每一次实操练习进行详细记录和总结，形成自己的“渗透测试手册”，这比单纯的“题库”更有价值。