

注册信息安全专业人员 (渗透测试方向) 白皮书

发布日期：2018 年 9 月



CNITSEC

中国信息安全测评中心

网神信息技术（北京）股份有限公司

©版权 2018-攻防领域考试中心

CISP-PTE/CISP-PTS 白皮书

咨询及索取

关于中国信息安全测评中心 CISP-PTE/CISP-PTS 考试相关的更多信息，请与注册信息安全专业人员攻防领域考试中心联系。

注册信息安全专业人员攻防领域考试中心联系方式

【邮 箱】CISP@360.net

【网 址】<http://www.360.net/service/examcisp>

【地 址】北京市朝阳区来广营创远路 36 号院朝来高科技产业园 7 号楼

【邮 编】100015

网神信息技术（北京）股份有限公司是以“保护大数据时代的安全”为企业使命，以“数据驱动安全”为技术思想，专注于为政府和企业提供新一代网络安全产品和信息安全服务的提供商。公司与中国信息安全测评中心联合成立注册信息安全专业人员攻防领域考试中心，负责注册信息安全专业人员渗透测试工程师（CISP-PTE）、注册信息安全专业人员渗透测试专家（CISP-PTS）考试开发维护、业务推广、市场宣传及持证人员的服务。CISP-PTE/CISP-PTS 专注于培养、考核高级实用型网络安全渗透测试安全人才，是业界首个理论与实践相结合的网络安全专项技能水平注册考试。

目 录

引言.....	1
一、CISP-PTE/CISP-PTS 考试要求.....	2
二、CISP-PTE/CISP-PTS 考试方向.....	2
三、CISP-PTE/CISP-PTS 注册流程.....	4
四、CISP-PTE/CISP-PTS 职业准则.....	4
五、CISP-PTE/CISP-PTS 考生申请资料要求.....	5
六、CISP-PTE/CISP-PTS 收费标准.....	6
七、注册信息安全专业人员攻防领域考试中心联系方式.....	7

引言

21 世纪是信息科学与技术飞速发展的时代，信息成为一种重要的战略资源。信息的获取、存储、处理及其安全保障能力成为一个国家综合国力的重要组成部分。目前，信息产业已成为世界第一大产业，信息科学与技术正处于空前繁荣的阶段。信息安全是信息的影子，哪里有信息，哪里就有信息安全问题。在信息科学与技术发展欣欣向荣的同时，危害信息安全的事件也不断发生。

面对严峻的网络空间安全形势，国内外多位信息安全领域资深专家、学者指出：不断增长的产业链式网络攻击虽然日趋严重，但是更让人担忧的是，网络安全人才的短缺致使各个层级的网络安全团队难以“扩军”，信息安全领域人才的储备量远远跟不上网络安全风险的增长量。

网络安全人才决定网络安全技术的交替、更迭，而人才的短缺直接影响政府事业机关网络防御能力，也导致中、小型企业很难组建自己的安全团队。网络安全防范能力堪忧，严重影响我国网络安全建设。

《网络安全法》第三条提出“国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。”因此，培养“高素质的网络安全和信息化人才队伍”的工作刻不容缓！

中国信息安全测评中心主导的注册信息安全专业人员攻防领域考试中心，通过举办“CISP-PTE / CISP-PTS”技能水平认证考试，锻炼考生实际解决网络安全问题的能力，发现人才，有效增强网络安全防御能力，促进国家企事业单位网络防御能力不断提高。同时引导广大网络安全工作者在推动信息安全工作中建功立业，引导广大信息安全工作者在建设信息化强国过程中发挥中坚作用，引导广大信息安全工作者在我国信息化建设与发展的征途中勇当先锋，团结动员广大网络安全从业者为我国网络安全建设又好又快的发展做出积极的贡献，为企业、事业单位培养和选拔网络安全渗透测试相关岗位的优秀人才。

一、CISP-PTE/CISP-PTS 考试要求

成为注册信息安全专业人员渗透测试工程师（CISP-PTE）、注册信息安全专业人员渗透测试专家（CISP-PTS），必须同时满足以下基本要求：

1、申请成为注册信息安全专业人员渗透测试工程师（CISP-PTE），要求具备一定渗透测试能力，或有意向从事渗透测试的人员，包含信息安全相关专业高校生；申请成为注册信息安全专业人员渗透测试专家（CISP-PTS），要求具备熟练的渗透测试能力；

2、申请成为注册信息安全专业人员渗透测试工程师（CISP-PTE）、注册信息安全专业人员渗透测试专家（CISP-PTS）无学历与工作经验的报考要求；

3、通过注册信息安全专业人员攻防领域考试中心组织的 CISP-PTE/CISP-PTS 考试；

4、同意并遵守 CISP-PTE/CISP-PTS 职业准则；

5、满足 CISP-PTE/CISP-PTS 注册要求并成功通过 CISP-PTE/CISP-PTS 审核；

注册信息安全专业人员渗透测试工程师/渗透测试专家资质证书有效期三年，证书失效后，需重新参加 CISP-PTE/CISP-PTS 注册考试；

二、CISP-PTE/CISP-PTS 考试方向

该注册考试是为了锻炼考生实际解决网络安全问题的能力，有效增强我国网络安全防御能力，促进国家企事业单位网络防御能力不断提高，以发现人才，选拔优秀人才而设立的技能水平考试。

考试内容从多个角度出发，通过客观题与实际操作题相结合（CISP-PTE）或全部为实际操作题（CISP-PTS）的形式，来考核考生的能力，通过多个得分点，对考生全面的考核，考生需要了解最新的网络安全技术，跟踪最新的网络安全动态，能够在真实的网络环境中发现问题和解决问题。同时，也可以为网络安全专业的学生提高自身价值和自身影响力，提供更好的学习素材，为更多热爱网络安全技术、有志于从事网络安全事业的人员提供了一个更加具有优势的平台。

考生应掌握 Web 安全基础知识，了解 HTTP 协议基础，以及一些常见的 Web

安全漏洞，包括注入漏洞、XSS 漏洞、CSRF 漏洞、SSRF 漏洞、文件处理漏洞、访问控制漏洞、会话管理漏洞。考生应该能够理解和发现这些漏洞，并且学会修复这些漏洞的方法，掌握更多的 Web 安全技术。

考生应了解中间件的安全知识，包括 Apache、IIS、Tomcat，以及 JAVA 开发的中间件 Weblogic、Websphere、Jboss 等（其中，Weblogic、Websphere、Jboss 相关知识仅要求参加 CISP-PTS 考试的学员掌握）。了解中间件的特性以及安全加固的方法，避免在安全设置上产生安全问题影响整个安全体系，了解最新的安全漏洞，能够对最新的漏洞做出响应，提高整体安全水平。

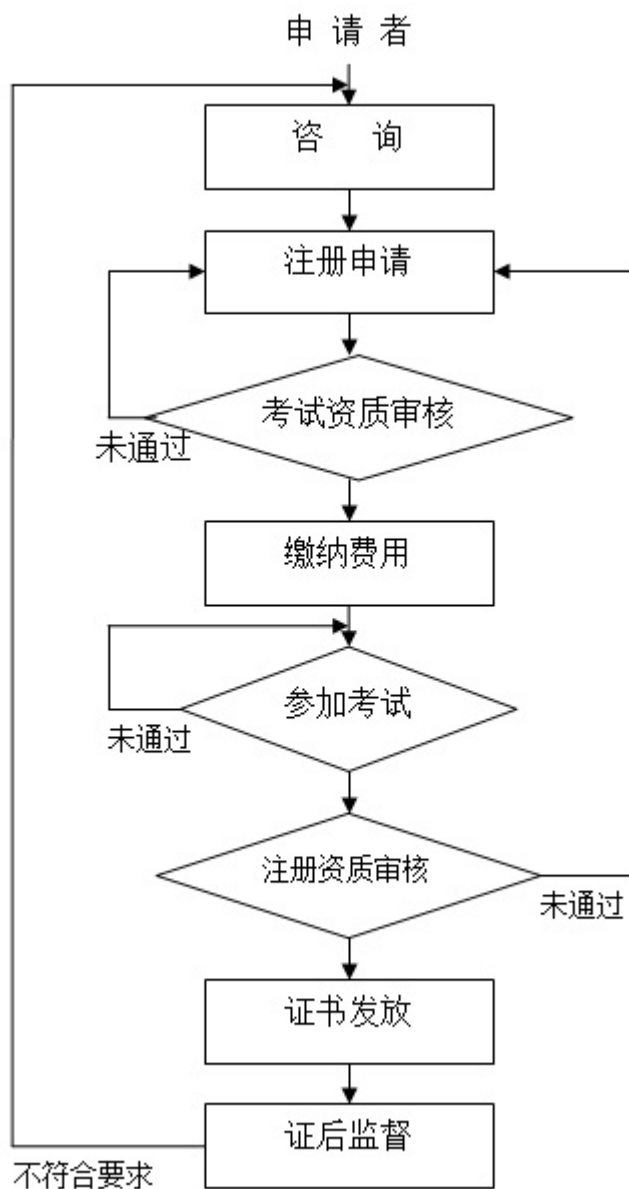
考生应了解操作系统的安全基础知识，包括 Windows、Linux 操作系统账户的分配与安全设置，文件系统权限的管理，日志审计的基本方法，以及第三方应用安全。由此可以加强考生对操作系统安全的理解，了解常见的攻击手段，以及操作系统安全加固的基础知识，通过日志审计进行安全事件分析，掌握最新的系统内核漏信息，能够及时修复漏洞，提高操作系统的安全性能。

考生应了解数据库的安全基础知识，这里以 MSsql、Mysql、Oracle、Redis 数据库为主（其中，Oracle、Redis 相关知识仅要求参加 CISP-PTS 考试的学员掌握），了解数据库的使用方法和语法结构，掌握数据库的安全设置以及权限，角色的分配。了解常用的利用数据库来进行文件操作和权限提升的方法以及应对措施，控制数据库运行权限，保证数据库中的数据完整和安全运营。

通过以上内容的学习，要求考生可以发现和修复网络中的漏洞，掌握更多的安全技能，提高个人的技术能力。具备渗透测试工程师的素养。

具体考试内容、范围及考试形式请下载《CISP-PTE/CISP-PTS 知识体系大纲》进行阅读了解。

三、CISP-PTE/CISP-PTS 注册流程



四、CISP-PTE/CISP-PTS 职业准则

作为国家注册信息安全专业人员应该遵循其应有的道德准则，中国信息安全测评中心为CISP认证人员设定了职业道德准则。

- (1) 维护国家、社会和公众的信息安全

自觉维护国家信息安全，拒绝并抵制泄露国家秘密和破坏国家信息基础设施的行为

自觉维护网络社会安全，拒绝并抵制通过计算机网络系统谋取非法利益和破坏社会和谐的行为；

自觉维护公众信息安全，拒绝并抵制通过计算机网络系统侵犯公众合法权益和泄露个人隐私的行为。

（2）诚实守信，遵纪守法

不通过计算机网络系统进行造谣、欺诈、诽谤、弄虚作假等违反诚信原则的行为；

不利用个人的信息安全技术能力实施或组织各种违法犯罪行为；

不在公众网络传播反动、暴力、黄色、低俗信息及非法软件。

（3）努力工作，尽职尽责

热爱信息安全工作岗位，充分认识信息安全专业工作的责任和使命

为发现和消除本单位或雇主的信息系统安全风险做出应有的努力和贡献

帮助和指导信息安全同行提升信息安全保障知识和能力，为有需要的人谨慎负责地提出应对信息安全问题的建议和帮助

（4）发展自身，维护荣誉

通过持续学习保持并提升自身的信息安全知识；

利用日常工作、学术交流等各种方式保持和提升信息安全实践能力；

以CISP身份为荣，积极参与各种证后活动，避免任何损害CISP声誉形象的行为。

五、CISP-PTE/CISP-PTS 考生申请资料要求

1. 学员需要填写如下申请资料：

《注册信息安全专业人员攻防领域考试及注册申请表》

填写申请表格时应注意：申请表格可采用电子模版录入填写，也可手写，填写过程中应确保内容的真实准确，手写申请表格应用正楷字体，字迹要求清晰可辨。

注：填写注册申请表第二部分时，需要由申请人所在单位（部门）领导签字并加盖本单位公章。

2. 申请（CISP-PTE/CISP-PTS）注册资质除了填写申请书外，还需要准备以下资料：

- 个人近期免冠 2 寸彩色白底证件照片 3 张（非白底照片为不合格照片，将不予采用）

- 身份证复印件 1 份

- 学历学位复印件 1 份

3. 资料的提交时间

学员应在报名时将所有资料全部提交。

六、CISP-PTE/CISP-PTS 收费标准

1、CISP-PTE 收费标准

单位：（元）

收费单位 收费种类	授权培训机构 （元）/人	考试中心	合计
培训费	14800	/	14800
考试费	/	3000	3000
注册费	/	600	600
年金（三年）	/	1400	1400
合计	14800	5000	19800
补考费	/	2500	2500

考试中心收费部分由网神信息技术（北京）股份有限公司先行代收，然后与中国信息安全测评中心统一结算，并开据发票。

2、CISP-PTS 收费标准

单位：（元）

收费单位 收费种类	授权培训机构 （元）/人	考试中心	合计
培训费	19800	/	19800
考试费	/	5500	5500

注册费	/	800	800
年金（三年）	/	1700	1700
合计	19800	8000	27800
补考费	/	4000	4000

考试中心收费部分由网神信息技术（北京）股份有限公司先行代收，然后与中国信息安全测评中心统一结算，并开据发票。

3、收款单位账号

开户行：招商银行股份有限公司北京上地支行

开户名：网神信息技术（北京）股份有限公司

账 号：110902261210802

七、注册信息安全专业人员攻防领域考试中心联系方式

咨询及索取

关于中国信息安全测评中心 CISP-PTE/CISP-PTS 考试相关的更多信息，请与注册信息安全专业人员攻防领域考试中心联系。

【邮 箱】CISP@360.net

【网 址】<http://www.360.net/service/examcisp>

【地 址】北京市朝阳区来广营创远路 36 号院朝来高科技产业园 7 号楼

【邮 编】100015