本考试科目考试时间180分钟，满分150分。包括计算机网络及信息安全基础两部分，每部分各75分。  
  
　　**计算机网络部分（75分）  
  
　　一、考试要求**  
  
　　掌握计算机网络的基本概念、基本原理和基本方法；掌握计算机网络的体系结构和典型网络协议，了解典型网络的组成和特点，理解典型网络设备的工作原理；掌握socket编程基本技术；能够运用计算机网络的基本概念、基本原理和基本方法进行网络系统的分析、设计和应用。  
  
　　注：考试内容以参考书目1为主。  
  
　**二、考试内容**  
  
　　1）计算机网络体系结构的概念  
  
　　a:报文交换基本概念  
  
　　b:TCP/IP体系结构  
  
　　c:IP地址，子网  
  
　　2)应用层  
  
　　a:Web与HTTP  
  
　　b:DNS  
  
　　c:SMTP  
  
　　3)传输层  
  
　　a:UDP  
  
　　b:TCP  
  
　　c:拥塞控制  
  
　　4)socket编程  
  
　　a:UDP编程  
  
　　b:TCP编程  
  
　　c:原始套接字编程  
  
　　5)网络层  
  
　　a:链路状态路由协议  
  
　　b:距离向量路由协议  
  
　　c:BGP  
  
　　6)链路层  
  
　　a:ARP  
  
　　b:WIFI  
  
　　c:CDMA  
  
　　**三、试卷结构**  
  
　　1)题型结构  
  
　　a:填空题(0—15分)  
  
　　b:选择题(0—30分)  
  
　　c:简答题(0—30分)  
  
　　d:问答题(0—30分)  
  
　　注：题型分数在以上范围内浮动，总分为75分  
  
　　**四、参考书目**  
  
　　1．JamesF.Kurose,andKeithW.Ross，计算机网络-自顶向下方法（原书第6版），机械工业出版社.2014  
  
　　2.谢希仁.计算机网络（第6版）.电子工业出版社，2013  
  
　　**信息安全部分（75分）  
  
　　一、考试要求**  
  
　　要求考生全面掌握信息安全领域的基本内涵、概念、原理和方法，系统深入地理解密码学基本理论、身份认证、访问控制、计算机病毒与网络入侵、防火墙与入侵检测、安全传输协议、风险评估与控制理论、信息安全标准与法律法规，掌握信息安全服务的逻辑设计与基本技术路线，理解各种信息安全服务之间的相互关系，建立信息安全体系的整体概念。  
  
　　**二、考试内容**  
  
　　1）信息安全的基本概念  
  
　　a:信息安全知识体系结构  
  
　　b:信息的基本安全属性  
  
　　c:信息保障  
  
　　d:安全服务与机制  
  
　　2）密码学基础  
  
　　a:密码分类、作用与基本设计原理  
  
　　b:对称密钥密码与DES  
  
　　c:公开密钥密码、DH密钥交换协议与RSA  
  
　　d：散列函数原理及作用  
  
　　3)身份认证与访问控制  
  
　　a:基于对称密钥的认证设计与kerberos协议  
  
　　b:基于公开密钥的认证设计与PKI理论  
  
　　c:三种典型的访问控制模型及实现机制  
  
　　d:Windows系统网络认证及访问控制  
  
　　4）计算机病毒与网络入侵  
  
　　a:传统计算机病毒、蠕虫病毒、木马病毒的特点、原理与防治  
  
　　b:拒绝服务攻击的特点及典型攻击机理  
  
　　c:欺骗类攻击的特点与典型攻击  
  
　　d：利用型攻击的特点及缓冲区溢出原理  
  
　　5）防火墙、入侵检测与安全传输协议  
  
　　a:防火墙理论与netfilter结构原理  
  
　　b:入侵检测理论与snorts结构原理  
  
　　c:IPSec与SSL协议的组成及工作原理  
  
　　d:SET协议体系与关键技术  
  
　　6）安全风险管理与法律法规  
  
　　a:信息系统风险评估与控制  
  
　　b:CC标准与BS7799  
  
　　c:信息安全道德与法律法规  
  
　　**三、试卷题型结构**  
  
　　a:填空题(0-20分)  
  
　　b:选择题(0-20分)  
  
　　b:简答题(0-30分)  
  
　　c:计算与综合设计题(0-30分)  
  
　　**四、参考书目**  
  
　　1．翟健宏，信息安全导论，科学出版社，2011.07  
  
　　2．刘建伟等，网络安全——技术与实践，清华大学出版社，2011.07