**2020年研究生入学考试《信息安全工程》考试大纲**

第一部分 考试说明

一、考试性质

全国硕士研究生入学考试是为高等学校招收硕士研究生而设置的。其中信息安全工程是安全工程专业考生设置的专业课程考试科目（该专业的业务课有多门考试科目），属招生学校自行命题性质。其评分标准是高等学校优秀本科生能达到的及格或及格以上水平，以保证被录取者具有坚实的信息安全基本理论和较强的信息安全工程分析实际问题的能力，有利于招生学校在专业上择优录取。

二、考试的学科范围

应考范围包括计算机网络安全技术基础、信息加密技术、网络安全技术、系统安全等四个部分。

三、评价目标

考试目标在于考查学生信息安全的基本概念、基本理论和方法的掌握以及对实际问题的分析和解决问题的能力。考生应能：

1. 掌握网络入侵与攻击、防火墙与入侵检测的基本原理。
2. 掌握各种古典密码算法和现代密码算法。

2、掌握对称密码体制和非对称密码体制的模型和代表算法以及密码算法的使用。

3、掌握一些主要的TCP/IP协议的缺陷及其安全改进协议或者安全改进方案。

4、掌握基本的系统安全策略；

四、考试形式与考卷结构

答卷形式：闭卷、笔试；试卷中的所有题目全部为必答题。

答题时间：180分钟。

试卷分数：满分为150分。

试卷结构及考查比例：试卷主要分为4部分，即：名词解释 20分，单项选择题30分，问题简答40，综合问题60分。

第二部分 考查要点

1．网络安全概述

(1)了解：网络安全的定义、主要内容、目标。

(2)理解：网络安全体系结构、网络安全策略与技术、网络系统的安全管理。

(3)掌握：网络安全面临的威胁与、风险网络安全评价准则。

2．网络操作系统安全

(1)了解：网络操作系统。

(2)理解：网络操作系统的安全与管理、Windows安全性分析和安全配置。

3．网络实体安全

(1)了解：网络机房设施与环境安全。

(2)理解：网络硬件系统的冗余、服务器与客户机安全。

(3)掌握：路由器安全；交换机安全。

4．网络数据库与数据安全

(1)了解：网络数据库安全概述、大数据及其安全。

(2)理解：网络数据库的安全特性和策略、网络数据库用户管理。

(3)掌握：数据备份、恢复和容灾。

5．数据加密技术与应用

(1)了解：密码学基本概念。

(2)理解：对称加密算法、公钥加密算法、PGP技术、Hash函数、数字签名、PKI、

数字证书等的原理。

(3)掌握：古典加密算法、DES、RSA算法的实现。

6．网络攻防技术

(1)了解：防火墙、入侵检测系统、VPN的基本概念。

(2)理解：VPN的关键技术、木马攻击与防范、网络病毒与防范。

(3)掌握：AH、ESP的实现原理、防火墙体系机构、IDS的常用技术原理、计算机病毒的防治基本方法、常见网络攻击方式。

7．互联网安全

(1)了解：TCP/IP协议及其安全、网站安全、电子邮件安全、黑客攻击和扫描技术的基本概念。

(2)理解：Web服务器的安全配置原则、网络监听和各类型攻击的基本原理。

(3)掌握：端口扫描的程序分析、网络监听的实现原理、Web服务器攻击方式。

8．无线网络安全

(1)了解：无线网络安全威胁。

(2)理解：无线网络的协议与技术。

9．网络安全实践

(1)了解：网络操作系统的安全设置、无线网络安全设置。

(2)理解：数据加密技术的应用、互联网应用案例。

(3)掌握：常用网络工具的使用、网络部件的安全设置。

**第三部分 参考文献**

1、《计算机网络安全技术教程》中国水利水电出版社，刘华春 蒋志平，2010

2、《计算机网络安全（第3版）》刘远生，清华大学出版社，2019

3、《计算机网络信息安全》刘永华， 清华大学出版社，2014

4、《密码学与网络安全（中文导读英文版）》，(美)福罗赞，清华大学出版社，2009