

文盛教育 2023 年计算机科学与技术专业冲刺预测

信息安全 模拟试卷（四）

一、选择题（每题 2 分，共 20 分）

- 姓 名

班 级

学 号
1. 以下网络安全所实施的技术中，属于被动攻击技术的是（ ）

A. 网络扫描 B.信息篡改 C.网络入侵 D.加密技术
2. 以下拒绝服务攻击中，利用了 TCP 连接中的三次握手协议的是（ ）

A.PING OF DEATH B.Tear drop C. Udp Flood D.SYN FLOOD
3. 以下攻击方式中，不考虑所需要的时长，一定可以实现口令破解的是（ ）

A.字典攻击 B.暴力破解 C.组合攻击 D.网络监听
4. 以下病毒的特征中，哪一项是计算机病毒基本特征（ ）

A.传染性 B.寄生性 C.触发性 D.潜伏性
5. 攻击者已知加密算法，已知待破解的密文，已知一条或者多条明文-密文对。这属于（ ）

A. 已知明文攻击 B. 唯密文攻击 C. 选择明文攻击 D. 选择密文攻击
6. 在 DES 加密过程中，每一轮加密使用的子密钥长度为（ ）

A.64 位 B.54 位 C.48 位 D.32 位
7. 以下不属于防火墙 CPU 结构的是（ ）

A. X86 架构 B. ASIC 架构 C. NP 架构 D.INTEL 架构
8. windows 操作系统注册表中，包含文件和文件扩展名的是（ ）

A. HKEY_CLASSER_ROOT B. HKEY_USER C. HKEY_LOCAL_MACHINE D. HKEY_CURRENT_CONFIG
9. 以下不属于 web 服务器漏洞的是（ ）

A. SQL 注入 B. 条件竞争 C. 拒绝服务 D.口令破解
10. 关于 DES 算法，以下说法不正确的是（ ）

A.综合应用了置换、代替密码技术

B.属于分组密码并采用对称结构

C.加密解密共用一个算法

D.算法的安全性基于数论中大整数分解的困难性

二、判断题（每题 2 分，共 20 分）

1. playfair 密码中，整理后的明文和原始明文一定是一致的()
2. 在利用 RSA 算法做数字签名时，加密使用的是公钥（ ）
3. 公钥算法比对称密钥算法更安全（ ）
4. 防火墙不能解决来自内部网络的攻击和安全问题()
5. 虚拟内存设置越大，计算机运行速度越快()
6. 几乎所有关系数据库都有 SQL 注入的风险（ ）
7. 蠕虫病毒特点是通过互联网络进行传播（ ）
8. 木马程序一般由两部分组成，分别是服务器端和客户端，其中服客户端程序指的是运行在被控制的电脑的木马程序，该程序为.exe 后缀（ ）
9. 在分布式拒绝服务攻击中，对目标主机发动直接进攻的是“傀儡机”()
10. 黑客攻击中，对操作系统扫描的目的是找到系统安全漏洞()

三、简单题（每题 10 分，共 20 分）

1. 什么是防火墙，从实现形式上看分为哪些种类？从技术的角度，其功能有哪些？
2. DES 加密的基本步骤是什么？

四、计算题（第 1、2 题各 5 分，第 3、4、5 题每题 10 分，共 40 分）

1. 假定凯撒密码的密钥 $k=12$ ，密文: C=HCKAPQEADCXY,求明文

2. 使用矩阵排列的方法加密明文，密钥：54213，明文：I have to study hard after the examination.

3. 已知 playfair 密码的密钥：jump and laugh,明文：there are so many stars in the sky.求密文.

4. 假定 DES 算法中 s 盒（S 盒表见教材）的输入为（AEF2101034BA）HS 盒数据参考教材（P143 页的八个盒数据），P 盒置换表如下，求最终输出结果

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

P 盒置换后得数据填写下表

5. 假定 RSA 算法中，取 $p=11$ ， $q=17$ ，加密密钥为 $e=7$ 求加密和解密解密密钥。如果用该密钥来做数据加密，明文 $M=2$,求密文。