西 安 电 子 科 技 大 学

考试时间 **120** 分钟

试　　题

题号	一	二								总分
		1	2	3	4	5	6	7	8	9	
分数											

1.考试形式：闭卷☑　开卷□ ；　　2.本试卷共二大题，满分 100 分；

3.考试日期：　2021 年　　月　　日；　　(答题内容请写在装订线外)

一、选择题（每小题 2 分，共 20 分）

1. 下列关于计算机安全属性说法不正确的是_____。

A. 计算机安全中的完整性是指确保信息不被非授权修改的属性

B. 在设计计算机安全系统时，机密性、完整性和可用性要同时满足

C. 计算机系统安全中的真实性可以通过数字签名来实现

D. 在设计计算机安全系统时，保证、真实性和匿名性要同时满足

2. 以下不属于物理安全的是_____。

A. 对机房中放置的计算机硬件进行保护

B. 攻击监视器的闪光、声音、无线电或其他信号来检测通信与计算

C. 利用物理系统接口的弱点来渗透系统

D. 通过侦听网络数据报文来获取用户数据

3. 生物特征识别是指基于唯一的生物或生理特征来识别人的手段，作为生物识别的有效特征需满足哪些需求_____。

A. 普遍性、独特性、永久性、可收集性

B. 普遍性、复杂性、永久性、可采集性

C. 普遍性、独特性、稀有性、可收集性

D. 普遍性、复杂性、完整性、可采集性

4. 生日攻击常见于哪一种加密模式中_____。

A. 流密码　　**B.** 分组密码

C. 替换密码　　**D. Hash** 函数

5. 下述关于内存地址空间的访问权限，说法不正确的是_____。

A. 一个进程的地址空间中的文本区域可以读取和写入

B. 一个进程的地址空间中的数据区域可以读取和写入

C. 一个进程的地址空间中的栈(Stack)区域可以读取和写入

D. 一个进程的地址空间中的堆(Heap)区域可以读取和写入

6. 安全策略是完整定义的规则集，以下哪个部分不是其组成部分_____。

A. 主体　　B. 属性

B. 操作　　D. 权限

7. 以下关于 Cookie 的描述错误的一项是_____。

A．Cookie 用来在客户端保存用户的一部分浏览数据

B．用 SSL/TLS 来传输 Cookie 信息可以防止敏感内容被截获

C．Cookie 的引入是因为 HTTP 协议是无状态保留的协议

D．采用会话型 Cookie 就能确保其安全性

8. 以下不属于 DNS 攻击的是_____。

A．网址嫁接　　B．网络钓鱼

C．URL 混淆　　D．DNS 缓存中毒

9. 以下关于防火墙的说法不正确的是_____。

A．防火墙可以通过硬件或软件实现

B．防火墙可以部署在内部或外部网络中

C．防火墙可以禁止内部用户使用某些协议或访问某些网站

D．防火墙用于保护内部用户免受外部网络上的恶意攻击

10. Linux 系统中，文件的权限表示为“-rw-rw-rw-”，下列说法正确的是_____。

A. 文件所有者拥有读、写和执行权限

B. 文件所在组用户拥有读、写和执行权限

C. 其他组用户拥有读和写权限

D. 其他组用户拥有读和执行权限

二、应用题（共 80 分）

1. 与计算机安全相关的基本概念有 C.I.A. (机密性、完整性、可用性)和 A.A.A. (保证、真实性和匿名性)。请分析下述威胁分别影响 C.I.A.和 A.A.A.中的哪个安全属性。（6 分）

（1）攻击者使用 Wireshark 进行数据包嗅探；

（2）攻击者利用僵尸网络发动分布式拒绝服务攻击；

（3）用户将在线音乐商店的音乐烧制成 CD 并分发给多人。

2. 访问控制模型中一般有主体、客体和主体对客体的操作权限等三个要素。假设系统中有主体:{S_1, S_2, S_3, S_4}，客体:{O_1, O_2, O_3, O_4}和操作权限:{R_1, R_2, R_3, R_4}。请分别通过访问控制矩阵和访问控制列表方式来确定特定的访问权限。（6 分）

3. 已知下述 C++程序:（10 分）

```
#include <cstdio>
#include <iostream>
using namespace std;
int main( )
{
    int cookie=1;
    char buf[8];
    printf("%08x %08x\n", &cookie, &buf);
    printf("%d\n", cookie);
    gets(buf);
    if(cookie == 0x61626364)
        printf("win\n");
    return 0;
}
```

（1）分析上述程序容易受到何种类型的攻击，并描述此攻击的基本原理。

（2）请尝试构建 buf 的输入值使得程序打印出“win”，已知 cookie 和 buf 的地址分别为 0x0019ff2c 和 0x0019ff24，且英文字母 a 的 ASCII 码值为 61。

4. 设通信双方采用 RSA 密码体制进行保密通信，接收方的公钥为(e, n) =(3,55) (即 e = 3, 模数 n = 55, p=5, q=11)，发送方待发送的明文消息为 M = 14。（10 分）

（1）求接收方的私钥 d；

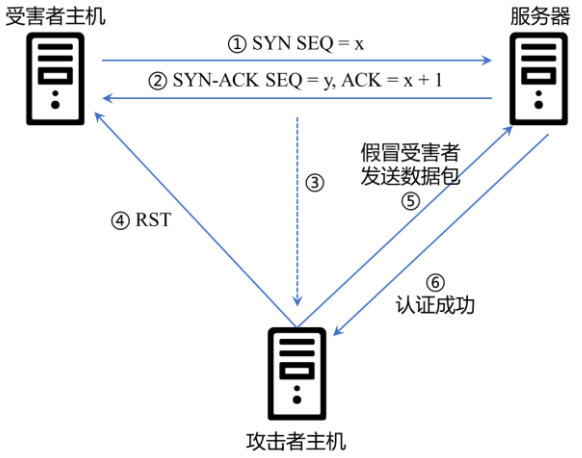
（2）求明文 M 对应的密文 C。

5. “熊猫烧香”是一款拥有自动传播、自动感染硬盘能力和强大破坏能力的病毒，它不但能感染系统中 exe，com，pif，src，html，asp 等文件，它还能终止大量的反病毒软件进程并且会删除扩展名为 gho 的文件。被感染的用户系统中所有.exe 可执行文件全部被改成熊猫举着三根香的模样。2007 年 1 月该病毒初肆虐网络，它主要通过用户运行下载的文件传染。根据该病毒的特点请回答下面的问题：（10 分）

（1）请简述病毒、蠕虫、木马这三种恶意软件的特点；

（2）从“熊猫烧香”的特点来看，该软件属于传统意义上的病毒吗？为什么？

6. 某 TCP 会话劫持攻击的场景如下图所示，请回答以下问题。（10 分）



（1）图中序号③执行的是什么操作？

（2）为什么要进行序号④的操作？

（3）对照序号①和②，请构造一个攻击者在序号⑤的操作中发送的 TCP 握手消息。

7. 某公司管理信息系统的一个 URL 如下所示，该 URL 将通过 GET 方法在后台数据库中查询一个 id 为 1175 的员工的信息。请回答如下问题：（8 分）

```
http://abc-corp.com/staff_search.php?id=1175
```

（1）该 URL 存在什么样的安全隐患？试述原因或举例说明。

（2）如果要避免上述的安全隐患，应该采取何种措施？

8. 指纹识别目前已广泛用于用户身份认证，然而由于手指受伤等原因，指纹识别会导致用户认证失败；此外，攻击者可以用指模等方式伪造合法用户指纹从而获得访问权限。请结合这些指纹识别认证的不足，论述下列问题。（10 分）

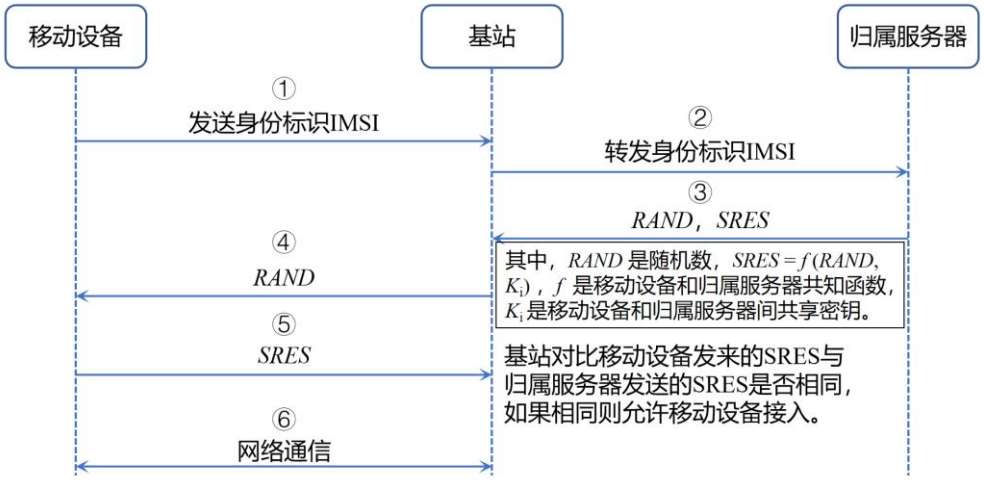
（1）思考如何设计指纹认证方法，以获得比单一指纹更高的安全性。

（2）从指纹认证的缺陷出发，试论述应该如何设计生物特征认证方法从而获得更高的安全强度？

9. “长宁检察在线”2021 年 12 月 15 日发布消息称：近日，张女士收到一条短信，里面写着她的移动积分即将过期，请及时兑换，后面还附有兑换网址。于是张女士随手点开短信中的网址链接，进入标题为“掌上营业厅”的页面，页面要求填写姓名、身份证号、信用卡卡号、交易密码、预留手机号和卡背后三位等信息。张女士按照要求填写了相关信息后，积分却没有兑换成功，页面进入了一直等待的状态，不久后，张女士就收到短信，银行卡上 2000 余元存款被转走，只得向警方报警求助。

在上述案例中，攻击者利用伪基站篡改号码，打着通信运营商或银行的名义，通过“积分兑换现金/大礼包”等虚假短信诱骗用户。（10 分）

（1）请结合以下 2G 鉴权示意图，试分析攻击者为何能够冒充“基站”。



（2）为了让广大没有专业安全知识的群众能够识别和防范伪基站攻击，减少经济损失，请你给出一些实用的建议。