

全国计算机技术与软件专业技术资格（水平）考试

2018 年上半年 信息安全工程师 下午试卷 I

（考试时间 14:00~16:30 共 150 分钟）

请按下述要求正确填写答题纸

1. 本试卷共五道题，全部为必答题，每题 25 分，满分 75 分。
2. 在答题纸的指定位置填写你所在的省、自治区、直辖市、计划单列市的名称。
3. 在答题纸的指定位置填写准考证号、出生年月日和姓名。
4. 答题纸上除填写上述内容外只能写解答。
5. 解答时字迹务必清楚，字迹不清时，将不评分。

本资料由信管网(www.cnitpm.com)整理发布，欢迎到信管网资料库免费下载学习
资料

信管网是专业信息系统项目管理师与信息安全工程师网站。提供了考试资讯、考试报名、成绩查询、资料下载、在线答题、考试培训、证书挂靠、项目管理人才交流、企业内训等服务。

信管网资料库提供了备考信息安全工程师的精品学习资料；信管网案例分析频道拥有丰富的案例范例，信管网考试中心拥有历年所有真题和超过 4000 多道试题免费在线测试；信管网培训中心每年指导考生超 4000 人。

信管网——专业、专注、专心，成就你的项目管理师、工程师梦想！

信管网: www.cnitpm.com

信管网考试中心: www.cnitpm.com/exam/

信管网培训中心: www.cnitpm.com/peixun/

试题一

阅读下列说明,回答问题 1 至问题 4,将解答填入答题纸的对应栏内。

【说明】恶意代码是指为达到恶意目的专门设计的程序或者代码。常见的恶意代码类型有特洛伊木马、蠕虫、病毒、后门、Rootkit、僵尸程序、广告软件。

2017 年 5 月,勒索软件 WanaCry 席卷全球,国内大量高校及企事业单位的计算机被攻击,文件及数据被加密后无法使用,系统或服务无法正常运行,损失巨大。

【问题 1】(2 分)

按照恶意代码的分类,此次爆发的恶意软件属于哪种类型?

【问题 2】(2 分)

此次勒索软件针对的攻击目标是 Windows 还是 Linux 类系统?

【问题 3】(6 分)

恶意代码具有的共同特征是什么?

【问题 4】(5 分)

由于此次勒索软件需要利用系统的 SMB 服务漏洞(端口号 445)进行传播,我们可以配置防火墙过滤规则来阻止勒索软件的攻击,请填写表 1-1 中的空(1)-(5),使该过滤规则完整。

注:假设本机 IP 地址为:1.2.3.4,“*”表示通配符。

表 1-1 防火墙过滤规则表

规则号	源地址	目的地址	源端口	目的端口	协议	ACK	动作
1	(1)	1.2.3.4	(2)	(3)	(4)	(5)	拒绝
...
...	*	*	*	*	*	*	拒绝

信管网参考答案:

【问题一】蠕虫类型

【问题二】Windows 操作系统

【问题三】恶意代码具有如下共同特征:(1) 恶意的目的(2) 本身是计算机程序(3) 通过执行发生作用。

【问题四】(1) * (2) >1024 (3) 445 (4) SMB (5) 0

试题二

阅读下列说明和图,回答问题 1 至问题 3,将解答填入答题纸的对应栏内。

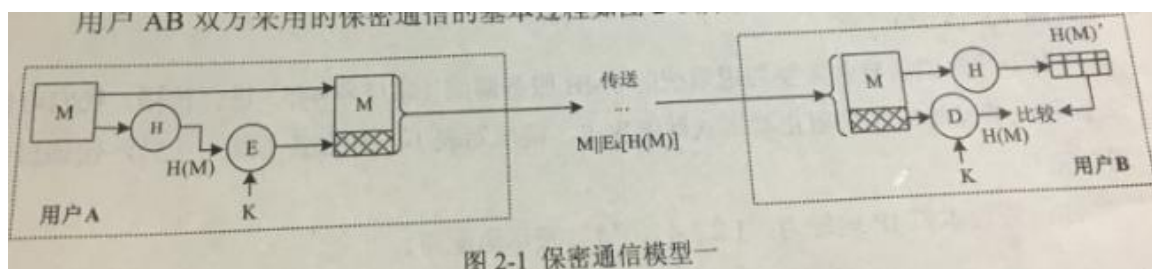
【说明】

密码学的基本目标是在有攻击者存在的环境下,保证通信双方(A 和 B)之间能够使用不安全的通信信道实现安全通信。密码技术能够实现信息的保密性、完整性、可用性和不可否认性等安全目标。一种实用的保密通信模型往往涉及对称加密、公钥密码、Hash 函数、数字签名等多种密码技术。

在以下描述中,M 表示消息,H 表示 Hash 函数,E 表示加密算法,D 表示解密算法,K 表示密钥,SKA 表示 A 的私钥,PKA 表示 A 的公钥,SKB 表示 B 的私钥,PKB 表示 B 的公钥,||表示连接操作。

【问题 1】(6 分)

用户 AB 双方采用的保密通信的基本过程如图 2-1 所示。



请问图 2-1 所设计的保密通信模型能实现信息的哪些安全目标?图 2-1 中的用户 A 侧的 H 和 E 能否互换计算顺序?如果不能互换请说明原因;如果能互换请说明对安全目标的影响。

【问题 2】(4 分)

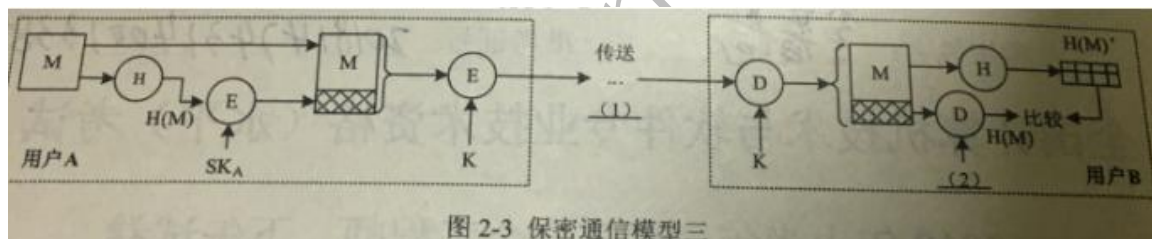
图 2-2 给出了另一种保密通信的基本过程:



请问图 2-2 设计的保密通信模型能实现信息安全的哪些特性?

【问题 3】(5 分)

为了在传输过程中能够保障信息的保密性、完整性和不可否认性,设计了一个安全通信模型结构如图 2-3 所示:



请问图 2-3 中 (1), (2) 分别应该填什么内容?

信管网参考答案:

【问题一】

实现完整性。

可以互换计算顺序,通过互换同样也可达到以上安全目标。

【问题二】

能实现保密性和完整性。

【问题三】

(1) $E_K[M || SK_A(H(M))]$

(2) PK_A

试题三

阅读下列说明,回答问题 1 至问题 3,将解答填入答题纸的对应栏内。

【说明】在 Linux 系统中,用户账号是用户的身份标志,它由用户名和用户口令组成。

【问题 1】(4 分)

Linux 系统将用户名和口令分别保存在哪些文件中?

【问题 2】(7 分)

Linux 系统的用户名文件通常包含如下形式的内容:root:x:0:0:root:root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

hujw:x:500:500:hujianwei:/home/hujw:/bin/bash

文件中的一行记录对应着一个用户,每行记录用冒号(:)分隔为 7 个字段,请问第 1 个冒号(第二列)和第二个冒号(第三列)的含义是什么?上述用户名文件中,第三列的数字分别代表什么含义?

【问题 3】(4 分)

Linux 系统中用户名文件和口令字文件的默认访问权限分别是什么?

信管网参考答案:

【问题 1】

用户名是存放在/etc/passwd 文件中,口令是以加密的形式存放在/etc/shadow 文件中

【问题 2】

第一个冒号的第二列代表口令;第二个冒号的第三列代表用户标识号。

root 用户 id 为 0; bin 用户 id 为 1; hujw 用户 id 为 500。

【问题 3】

用户名文件默认访问权限为 rw-r--r--; 口令字文件的默认访问权限为 r-----。

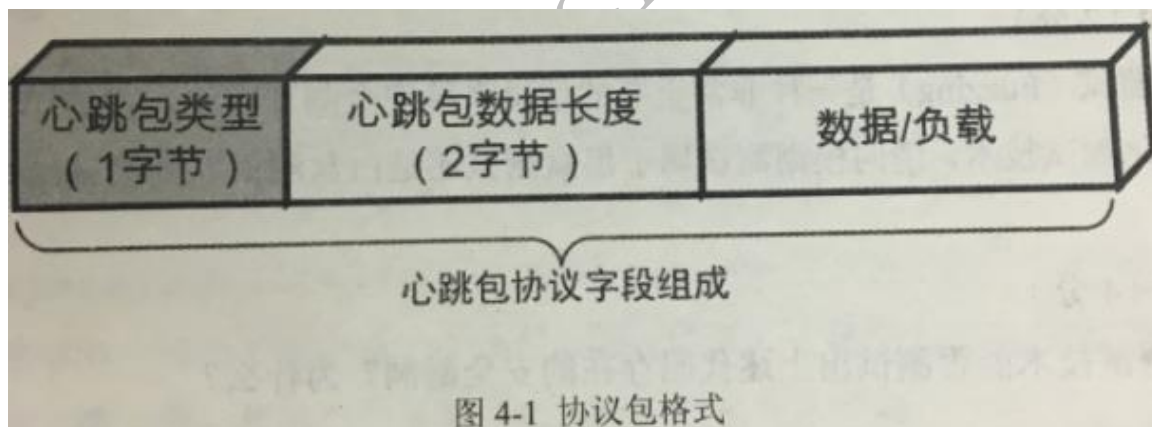
试题四

阅读下列说明和 C 语言代码,回答问题 1 至问题 4,将解答写在答题纸的对应栏内。

【说明】

在客户服务器通信模型中,客户端需要每隔一定时间向服务器发送数据包,以确定服务器是否掉线,服务器也能以此判断客户端是否存活,这种每隔固定时间发一次的数据包也称为心跳包。心跳包的内容没有什么特别的规定,一般都是很小的包。

某系统采用的请求和应答两种类型的心跳包格式如图 4-1 所示。



心跳包类型占 1 个字节,主要是请求和响应两种类型;

心跳包数据长度字段占 2 个字节,表示后续数据或者负载的长度。

接收端收到该心跳包后的处理函数是 process_heartbeat(),其中参数 p 指向心跳包的报文数据,s 是对应客户端的 socket 网络通信套接字。

```
void process_heartbeat(unsigned char *p, SOCKET s)
{
    unsigned short hbtype;
    unsigned int payload;
    hbtype = *p++; // 心跳包类型
    n2s(p, payload); // 心跳包数据长度
    pl = p; // pl 指向心跳包数据
    if (hbtype == HB_REQUEST) {
        unsigned char *buffer, *bp;
        buffer = malloc(1 + 2 + payload);
        bp = buffer; // bp 指向刚分配的内存
        *bp++ = HB_RESPONSE; // 填充 1 byte 的心跳包类型
        s2n(payload, bp); // 填充 2 bytes 的数据长度
        memcpy(bp, pl, payload);
        /* 将构造好的心跳响应包通过 socket s 返回给客户端 */
        r = write_bytes(s, buffer, 3 + payload);
    }
}
```

【问题 1】(4 分)

- (1) 心跳包数据长度字段的最大取值是多少?
- (2) 心跳包中的数据长度字段给出的长度值是否必须和后续的数据字段的实际长度一致?

【问题 2】(5 分)

- (1) 上述接收代码存在什么样的安全漏洞?
- (2) 该漏洞的危害是什么?

【问题 3】(2 分)

模糊测试(Fuzzing)是一种非常重要的信息系统安全测评方法,它是一种基于缺陷注入的自动化测试技术。请问模糊测试属于黑盒测试还是白盒测试?其测试结果是否存在误报?

【问题 4】(4 分)

模糊测试技术能否测试出上述代码存在的安全漏洞?为什么?

信管网参考答案:

【问题 1】

- (1) 心跳包数据长度的最大取值为 65535。
- (2) 必须是一致的。

【问题 2】

“心脏出血”漏洞;会造成有用数据的泄露。

【问题 3】

属于黑盒测试;不存在误报。

【问题 4】

模糊测试技术能够测试出上述存在的安全漏洞;

网络协议的模糊测试是通过特定的 **Socket** 形式将变异或者生成的含有错误信息的数据包发送给目标程序。根据协议的格式、定义,准备大量的测试数据,从客户端发送给服务器端,从而试图找到一些安全漏洞,不需要程序的源代码即可发现问题。

试题五

阅读下列说明和图,回答问题 1 至问题 5,将解答写在答题纸的对应栏内。

【说明】

入侵检测系统(IDS)和入侵防护系统(IPS)是两种重要的网络安全防御手段,IDS 注重的是网络安全状况的监管,IPS 则注重对入侵行为的控制。

【问题 1】(2 分)

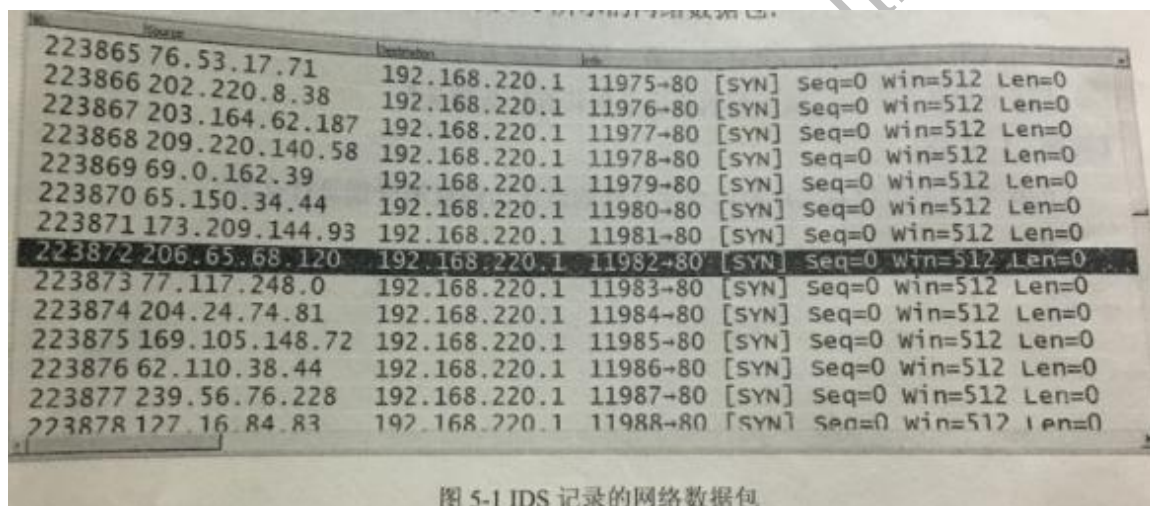
网络安全防护可以分为主动防护和被动防护,请问 IDS 和 IPS 分别属于哪种防护?

【问题 2】(4 分)

入侵检测是动态安全模型(P2DR)的重要组成部分。请列举 P2DR 模型的 4 个主要组成部分。

【问题 3】(2 分)

假如某入侵检测系统记录了如图 5-1 所示的网络数据包:



No.	Source	Destination	Port	Protocol	Seq	Win	Len
223865	76.53.17.71	192.168.220.1	11975-80	[SYN]	Seq=0	win=512	Len=0
223866	202.220.8.38	192.168.220.1	11976-80	[SYN]	Seq=0	win=512	Len=0
223867	203.164.62.187	192.168.220.1	11977-80	[SYN]	Seq=0	win=512	Len=0
223868	209.220.140.58	192.168.220.1	11978-80	[SYN]	Seq=0	win=512	Len=0
223869	69.0.162.39	192.168.220.1	11979-80	[SYN]	Seq=0	win=512	Len=0
223870	65.150.34.44	192.168.220.1	11980-80	[SYN]	Seq=0	win=512	Len=0
223871	173.209.144.93	192.168.220.1	11981-80	[SYN]	Seq=0	win=512	Len=0
223872	206.65.68.120	192.168.220.1	11982-80	[SYN]	Seq=0	win=512	Len=0
223873	77.117.248.0	192.168.220.1	11983-80	[SYN]	Seq=0	win=512	Len=0
223874	204.24.74.81	192.168.220.1	11984-80	[SYN]	Seq=0	win=512	Len=0
223875	169.105.148.72	192.168.220.1	11985-80	[SYN]	Seq=0	win=512	Len=0
223876	62.110.38.44	192.168.220.1	11986-80	[SYN]	Seq=0	win=512	Len=0
223877	239.56.76.228	192.168.220.1	11987-80	[SYN]	Seq=0	win=512	Len=0
223878	127.16.84.83	192.168.220.1	11988-80	[SYN]	Seq=0	win=512	Len=0

图 5-1 IDS 记录的网络数据包

请问图中的数据包属于哪种网络攻击?该攻击的具体名字是什么?

【问题 4】(4 分)

入侵检测系统常用的两种检测技术是异常检测和误用检测,请问针对图中所描述的网络攻击应该采用哪种检测技术?请简要说明原因。

【问题 5】(3 分)

Snort 是一款开源的网络入侵检测系统,它能够执行实时流量分析和 IP 协议网络的数据包记录。

Snort 的配置有 3 种模式,请给出这 3 种模式的名字。

信管网参考答案:

【问题 1】

入侵检测技术 (IDS)属于被动防护;入侵防护系统 (IPS)属于主动防护。

【问题 2】

P2DR 模型包含 4 个主要组成部分包括: Policy (安全策略)、Protection (防护)、Detection (检测)和 Response (响应)。

【问题 3】

属于拒绝服务攻击；具体为 SYN 洪泛攻击。

【问题 4】

应该采用误用检测技术；异常检测方法依赖于正常行为模型的建立，其误检率很高，误用检测依据具体特征库进行判断，其检测准确度很高。

【问题 5】

Snort 的配置的 3 个主要模式：嗅探 (Sniffer)、包记录 (PacketLogger) 和网络入侵检测。

最终答案以信管网题库答案为准：<http://www.cnitpm.com>