# 2021 年下半年信息安全工程师
# 《案例分析》真题答案及解析

**本资料由信管网(www.cnitpm.com)整理发布，供信管网学员使用！**

信管网是专业软考中高级与 PMP 考试培训服务网站。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、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软考的精品学习资料；信管网案例分析频道和论文频道拥有丰富的案例范例和论文范例，信管网考试中心拥有软考中高级历年真题和超过 5000 多道试题免费在线测试；信管网每年指导考生超 100000+人。

**信管网——专业、专注、专心，成就你的项目管理师梦想！**

**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/wx/**



**信管网微信公众号**

**信管网客服微信号**

## 1、试题一(共 20 分)

阅读下列说明和图，回答问题 1 至问题 5，将解答填入答题纸的对应栏内。

【说明】在某政府单位信息中心工作的李工要负责网站的设计、开发工作。为了确保部门新业务的顺利上线，李工邀请信息安全部门的王工按照等级保护 2.0 的要求对其开展安全测评。李工提供网站的 网络拓扑图如图 1-1 示。图中，网站服务器的 IP 地址是 192.168.70.140，数据库服务器的 IP 地址是 192.168.70.141。


图 1-1

王工接到网站安全测评任务以后，决定在内网办公区的信息安全部开展各项运维工作，王工使用的办公电脑 IP 地址为 192.168.11.2。

【问题 1】(2 分)

按照等级保护 2.0 的要求，政府网站的定级不应低于几级？该等级的测评每几年开展一次？

【问题 2】(6 分)

按照网络安全测评的实施方式，测评主要包括安全功能检测、安全管理检测、代码安全审查、安全渗透、信息系统攻击测试等。王工调阅了部分网站后台处理代码，发现网站某页面的数据库查询代码存在安全漏洞，代码如下：

```
<?php
if(isset($_GET['Submit'])) {

    //Retrieve data
    $id = $_GET['id'];

    $getid = "SELECT first_name, last_name FROM users WHRER user_id = '$id' ";
    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '<pre>');

    $num =mysql_numrows($result);

    $i = 0;
    while($i < $num){

        $first = mysql_result($result, $i, "first_name");
        $last = mysql_result($result, $i, "last_name");

        echo '<pre>'
        echo 'ID:' . $id . '<br>First name:' .$first . '<br>Surname: ' .$last;
        echo '<pre>'

        $i++;
    }
}
?>
```

(1)请问上述代码存在哪种漏洞？

(2)为了进一步验证自己的判断，王工在该页而的编绀權中输入了漏洞测试语句，发起测试。请

问王工最有可能输入的测试语句对应以下哪个选项？

A. or 1 = 1--order by 1 B. I or '1' =' 1' = I order by I#

C. 1' or 1 = 1 order by I# D. I'and'1'=' 2' order by I#

(3)根据上述代码，网站后台使用的哪种数据库系统？

(4)王工对数据库中保存口令的数据表进行检查的过程中，发现口令为明文保存，遂给出整改建议，建议李工对源码进行修改，以加强口令的安全防护，降低敏感信息泄露风险。下面给出四种在数据库中保存口令信息的方法，李工在安全实践中应采用哪一种方法？

A. Basc64 B. MD5 C.哈希加盐 D.加密存储

【问题 3】(2 分)

按照等级保护 2.0 的要求，系统当中没有必要开放的服务应当尽量关闭。王工在命令行窗口运行了一条命令，查询端口开放请况。请给出王工所运行命令的名字。

【问题 4】(2 分)

防火墙是网络安全区域边界保护的重要技术，防火墙防御体系结构有基于双宿主机防火墙、基于代理型防火墙和基于屏蔽子网的防火墙。图 1-1 拓扑图中的防火墙布局属于哪种体系结构类型？

【问题 5】(8 分)

根据李工提供的网络拓扑图，王工建议部署开源的 Snort 入侵检测系统以提高整体的安全检测和态势感知能力。

(1)针对王工建议，李工查阅了入侵检测系统的基本组成和技术原理等资料。请问以下有关 Snort 入侵检测系统的描述哪两项是正确的？ (2 分)

A.基于异常的检测系统 B.基于误用的检测系统

C.基于网络的入侵检测系统 D.基于主机的入侵检测系统

(2)为了部署 Snort 入侵检测系统，李工应该把入侵检测系统连接到图 1-1 网络拓扑中的哪台交换机？(1 分)

(3)李工还需要把网络流量导入入侵检测系统才能识别流才中的潜在攻击。图 1-1 中使用的均为华为交换机，李工要将交换机网口 GigabitEthernet1/0/2 的流量镜像到部署 Snort 的网口 GigabitEthernet1/0/1 上，他应该选择下列选项中哪一个配置？(2 分)

A. observe-port 1 interface GigabitEthernet1/0/2
interface GigabitEthemet1/0/1
port-mirroring to observe-port 1 inbound/outbound/both

B. observe-port 2 interface GigabitEthernet1/0/2
interface GigabitEthemet1/0/1
port-mirroring to observe-port 1 inbound/outbound/both



C. port-mirroring to observe-port 1 inbound/outbound/both
observe-port 1 interfaceGigabiEthenet1/0/2
interface GigabitEthenet1/0/1

D. observe-port 1 interface GigabitEthernet1/0/1
interface GigabitEthemet1/0/2
port-mirroring to observe-port 1 inbound/outbound/both

(4)Snort 入侵检测系统部署不久，就发现了一起网络攻击。李工打开攻击分组查看，发现很字符看起来不像是正常字母，如图 1-2 所示，请问该用哪种编码方式去解码该网络分组内容？ (I 分)

| | | | |
|---|---|---|---|
| 0050 | 68 75 6d 65 6e 2f 3f 69 64 3d 31 25 45 32 25 38 | humen/?i d=1%E2%8 |
| 0060 | 30 25 39 39 2b 75 6e 69 6f 6e 2b 73 65 6c 65 63 | 0%99+uni on+selec |
| 0070 | 74 2b 31 25 32 43 32 2b 25 32 33 26 53 75 62 6d | t+1%2C2+ %23&Subm |
| 0080 | 69 74 3d 53 75 62 6d 69 74 26 75 73 65 72 5f 74 | it=Submi t&user_t |
| 0090 | 6f 6b 65 6e 3d 31 30 34 38 39 34 34 30 35 63 62 | oken=104 894405cb |
| 00a0 | 62 37 32 39 34 62 34 63 64 33 36 61 62 66 66 65 | b7294b4c d36abffe |
| 00b0 | 62 37 36 30 32 20 48 54 54 50 2f 31 2e 31 0d 0a | b7602 HT TP/1.1·· |
| 00c0 | 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 37 30 | Host: 19 2.168.70 |
| 00d0 | 2e 31 34 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e | .140··Co nnection |
| 00e0 | 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 | : keep-a live··Up |

图 1-2

(5)针对图 1-2 所示的网络分组，李工查看了该攻击对应的 Snort 检测规则，以更好地掌握 Snort 入侵检测系统的工作机制。请完善以下规则，填充空(a)、(b)处的内容。(2 分)

(a) tcp any any -> any any (msg:"XXX";content:" (b)";nocase;sid:1106;)

信管网参考答案：

【问题 1】

二级;两年一次

【问题 2】

(1) SQL 注入漏洞

(2) C

(3) mysql

(4) C

【问题 3】

netstat

【问题 4】

基于屏蔽子网的防火墙

【问题 5】

(1) B、C

(2)交换机 2

(3)D

(4) URL 编码(URL encode)

(5)(a) alert (b) union

查看解析：www.cnitpm.com/st/5229321394.html

**试题二(共 20 分)**

阅读下列说明，回答问题 1 至问题 5，将解答填入答题纸的对应栏内。

【说明】通常由于机房电磁环境复杂，运维人员很少在现场进行运维工作，在出现安全事件需要紧急处理时，需要运维人员随时随地运程开展处置工作。

SSH（安全外壳协议)是一种加密的网络传输协议，提供安全方式访问远程计算机。李工作为公司的安全运维工程师，也经常使用 SSH 远程登录到公司的 Ubuntu 18.04 服务器中进行安全维护。

【问题 1】(2 分)

SSH 协议默认工作的端口号是多少？

【问题 2】(2 分)

网络设备之间的远程运维可以采用两种安全通信方式：一种是 SSH，还有一种是什么？

【间题 3】(4 分)

日志包含设备、系统和应用软件的各种运行信息，是安全运维的重点关注对象。李工在定期巡检服务器的 SSHH 志时，发现了以下可疑记录：

```
Jul 22 17: 17: 52 humen systed-logiad [1182] : Waching sytem buttons on/dev/input/evet0 (Power Button)
Jul 22 17: 17: 52 humen systed-logiad [1182] : Waching sytem buttons on/dev/input/evet1(AT Translated Set 2 keyboard)
Jul 23 09: 33: 41 humen sshd [5423] :pam_unix (sshd:auth) authentication failure, logame= uid=0 euid=0 tty=ssh
ruser=rhost=192.168.107.130 user=humen
Jul 23 09: 33: 43 humen sshd [5423] :Failed password for humen from 192.168.107.130 port 40231 ssh2
Jul 23 09: 33: 43 humen sshd [5423] :Connection closed by authenticating user humen 192.168.107.130 port 40231[preauth]
Jul 23 09: 33: 43 humen sshd [5425] :pam_unix (sshd:auth) :authentication failure; logname= uid=0 euid=0 tty=ssh
ruser=rhost=192.168.107.130 user=humen
Jul 23 09: 33: 45 humen sshd [5425] : Failed password for humen from 192.168.107.130 port 37223 ssh2
Jul 23 09: 33: 45 humen sshd [5425] : Connection closed by authenticating user humen192.168.107.130 port 37223 [preauth]
Jul 23 09: 33: 45 humen sshd [5427] : pam_unix (sshd:auth) :authentication failure;logname= uid=0 euid=0 tty=ssh
ruser=rhost=192.168.107.130 user=humen
Jul 23 09: 33: 47 humen sshd [5427] : Failed password for humen from 192.168.107.130 port 41365 ssh2
```

```
Jul 23 09: 33: 47 humen sshd [5427] :Connection closed by authenticating user humen 192.168.107.130 port 41365 [preauth]
Jul 23 09: 33: 47 humen sshd [5429] : pam_unix (sshd:auth) :authentication failure;logname= uid=0 euid=0 tty=ssh
ruser=rhost=192.168.107.130 user=humen
Jul 23 09: 33: 49 humen sshd [5429] : Failed password for humen from 192.168.107.130 port 45627 ssh2
Jul 23 09: 33: 49 humen sshd [5429] :Connection closed by authenticating user humen 192.168.107.130 port 45627 [preauth]
Jul 23 09: 33: 49 humen sshd [5431] : pam_unix (sshd:auth) :authentication failure;logname= uid=0 euid=0 tty=ssh
ruser=rhost=192.168.107.130 user=humen
Jul 23 09: 33: 51 humen sshd [5431] : Failed password for humen from192.168.107.130 port 42271 ssh2
Jul 23 09: 33: 51 humen sshd [5431] :Connection closed by authenticating user humen 192.168.107.130 port 42271 [preauth]
Jul 23 09: 33: 51 humen sshd [5433] : pam_unix (sshd:auth) :authentication failure;logname= uid=0 euid=0 tty=ssh
ruser=rhost=192.168.107.130 user=humen
Jul 23 09: 33: 53 humen sshd [5433] : Failed password for humen from 192.168.107.130 port 45149 ssh2
Jul 23 09: 33: 53 humen sshd [5433] :Connection closed by authenticating user humen 192.168.107.130 port 45149[preauth]
Jul 23 09: 33:54 humen sshd [5435] :Accepted password for humen from 192.168.107.130 port 45671 ssh2
Jul 23 09: 33: 54 humen sshd [5435] : pam_unix (sshd:auth) : session opened for user humen by (uid=0)
```

(1)请问李工打开的系统日志文律的路径和名称是什么？

(2)李工怀疑有黑客在攻击该系统，请给出判断攻击成功与否的日志以便李工评估攻击的影响。

【问题 4】(10 分)

经过上次 SSH 的攻击事件之后，李工为了加强口令安全，降低远程连接风险，考虑采用免密证书登录。

(1) Linux 系统默认不允许证书方式登录，李工需要实现免密证书登录的功能，应该修改哪个配置件？请给出文件名。

(2)李工在创建证书后需要拷贝公钥信息到服务器中。他在终端输入了以下拷贝命令，请说明命令中“>>”的含义。

```
ssh xiaoming@server cat/home/xiaoming/.ssh/id_rsa.pub> >authorized_keys
```

(3)服务器中的 authorized_keys 文件详细信息如下，请给出文件权限的数字表示。

```
-rw------- 1 root root 0 10月 18 2018 authorized_keys
```

(4)李工完成 SSH 配置修改后需要重启服务，请给出 systemctl 重启 SSH 服务的命令。

(5)在上述服务配置过程中，配置命令中可能包含各种敏感信息，因此在配翼结束后应及时清除历史命令信息，请给出清除系统历史记录应执行的命令。

【问题 5】 (2 分)

SSH 之所以可以实现安全的远程访问，归根结底还是密码技术的有效使用。对于 SSH 协议，不管是李工刚开始使用的基于口令的认证还是后来的基于密钥的免密认证，都是密码算法和密码协议

在为李工的远程访问保驾护航。请问上述安全能力是基于对称密码体制还是非对称密码体制来实现的？

信管网参考答案：

【问题 1】22

【问题 2】VPN

【问题 3】

(1) /var/log/auth.log

(2) cat .lauth.log / grep“Accepted password”。

【问题 4】

(1) /etclssh/sshd_config

(2)追加文件内容

(3) 600

(4) systemctl restart ssh

systemctl restart ssh

dsystemctl restart ssh.service

systemctl restart sshd.service

(5) rm ~/.bash_history

【问题 5】

非对称密码体制

查看解析：www.cnitpm.com/st/5229428662.html

**试题三(共 20 分)**

阅读下列说明和图，回答问题 1 至问题 5，将解答填入答题纸的对应栏内。

【说明】域名系统是网络空间的中枢神经系统，其安全性影响范围大，也是网络攻防的重点。李工在日常的流量监控中，发现如图 3-1 所示的可疑流量，请协助分析其中可能的安全事件。

【问题 1】(4 分)

域名系统采用授权的分布式数据查询系统，完成域名和 IP 地址的解析。李工通过上述流量可以判断域名解析是否正常、有无域名劫持攻击等安全事件发生。

(1)域名系统的服务端程序工作在网络的哪一层？

(2)图 3-1 中的第一个网络分组要解析的域名是什么？

(3)给出上述域名在 DNS 查询包中的表示形式(16 进制)。

(4)由图 3-1 可知李工所在单位的域名服务器的 IP 地址是什么？

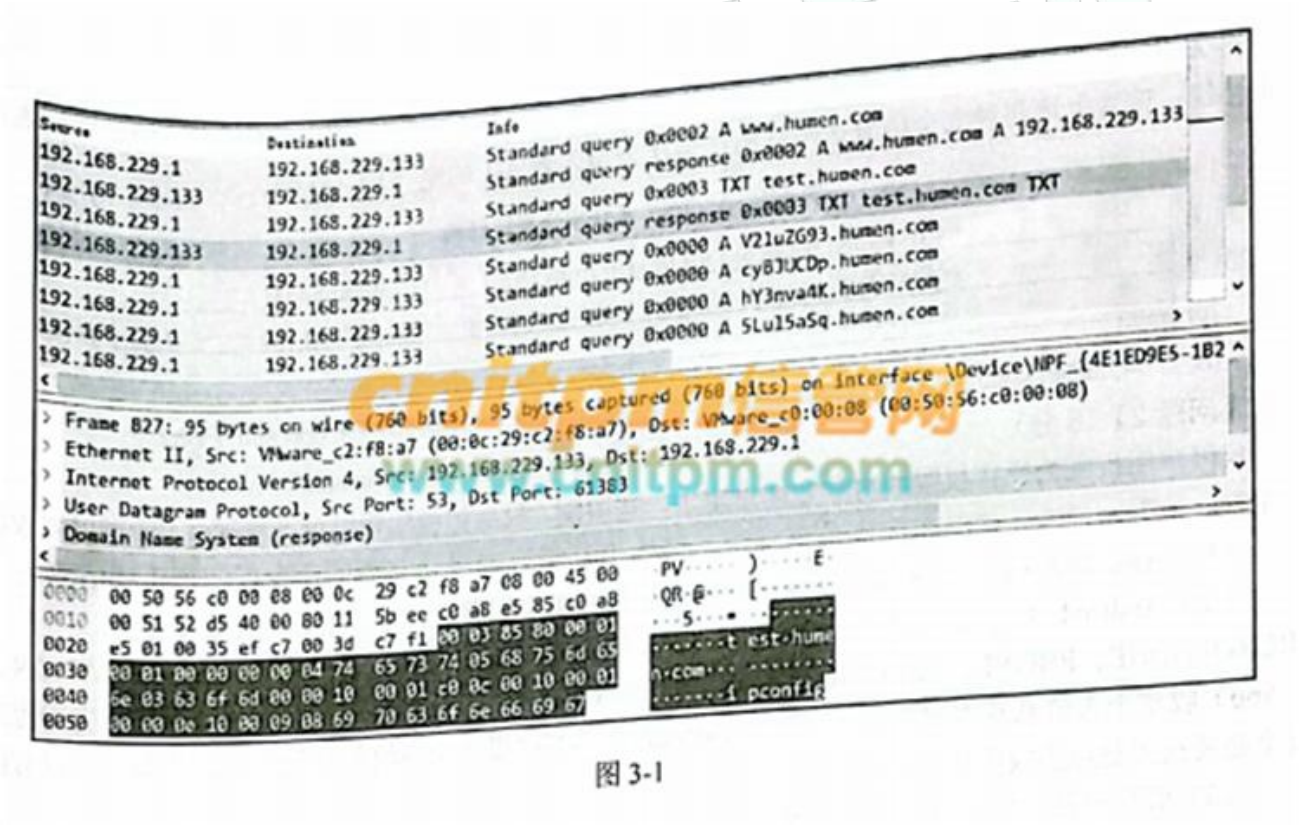


图 3-1

【问题 2】 (2 分)

签于上述 DNS 协议分组包含大量奇怪的子域名，如想知道是哪个应用程序发送的上述网络分组，请问在 Windows 系统下，李工应执行哪条命令以确定上述 DNS 流量来源?

【问题 3】(6 分)

通过上述的初步判断，李工认为 192.168.229.I 的计算机可能已经被黑客所控制(CC 攻击)。黑客

惯用的手法就是建立网络隐蔽通道，也就是指利用网络协议的某些字段秘密传输信息，以掩盖恶意程序的通信内容和通信状态。

(1)请问上述流量最有可能对应的恶意程序类型是什么？

(2)上述流量中隐藏的异常行为是什么？请简要说明。

(3)信息安全目标包括保密性、完整性、不可否认性、可用性和可控性，请问上述流量所对应的网络攻击违反了信息安全的哪个目标？

【问题 4】(6 分)

通过上述的攻击流分析，李工决定用防火墙隔离该计算机，李工所运维的防火墙是 Ubuntu 系统自带的 iptables 防火墙。

(1)请问 iptables 默认实现数据包过滤的表是什么？该表默认包含哪几条链？

(2)李工首先要在 ipables 防火墙中查看现有的过滤规则，请给出该命令。

(3)李工要禁止该计算机继续发送 DNS 数据包，请给出相应过滤规则。

【问题 5】(2 分)

在完成上述处置以后，李工需要分析事件原因，请说明导致 DNS 成为 CC 攻击的首选隐蔽传输通道协议的原因。

信管网参考答案：

【问题 1】

(1)应用层

(2) www.humen.com:

(3)03777770568756d656e03636f6d

(4)192.168.229.133

【问题 2】

由流量的源端口号和 netstat/b 对应的进程关联即可得知

【问题 3】

(1)特洛伊木马

(2) 执行 ipconfig 命令，回传网络信息

(3)完整性

【问题 4】

(1) filter; INPUT, FORWARD 和 OUTPUT

(2) iptables-L

(3) iptables-l INPUT-s 192.168.229.1 -j DROP

【问题 5】

放行

查看解析：www.cnitpm.com/st/522953774.html

**试题四(共 15 分)**

阅读下列说明和图，回答问题 1 至问题 4，讲解答填入答题纸的对应栏内

【说明】近期，按照网络安全审查工作安排，国家网信办会同公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等部门联合进驻某出行科技有限公司，开展网络安全审查，移动 APP 安全检测和个人数据安全再次成为关注焦点。

【问题 1】(4 分)

为保护 Android 系统及应用终端平台安全，Android 系统在内核层、系统运行层、应用框架层以及应用程序层采取了相应的安全措施，以尽可能地保护移动用户数据、应用程序和设备安全。在 Android 系统提供的安全措施中有安全沙箱、应用程序签名机制；权限声明机制、地址空间布局随机化等，请将上述四种安全措施按照其所在层次分填入表 4-1 的空(1)-(4)

表 4-1 Android 系统安全系统结构

| | |
|---|---|
| 应用程序层 | (1) |
| 应用框架层 | (2) |
| 系统运行程序层 | (3) |
| 内核层 | (4) |

【问题 2】(6 分)

权限声明机制为操作权限和对象之间设定了一些限制，只有把权限和对象进行绑定，才可以有权操作对象(1)请问 Android 系统应用程序权限声明信息都在哪个配置文件中？给出该配置文件名。(2)Android 系统定义的权限组包括 CALENDAR、CAMERA、CONTACTS、LOCATION、 MICROPHONE、PHONE、SENSORS，SMS、STORAGE.按照《信息安全技术 移动互联网应用程序(App)收集个人信息基本规范》，运行在 Android9.0 系统中提供网络约车服务的某出行 App 可以有的最小必要权限是以上权限组的哪几个？

(3)假如有移动应用 A 提供了 AService 服务，对应的权限描述如下：

```
1.  <permission
2.          android:name="USER_INFO"
3.          android:label="read user information"
4.          android:description="get user information"
5.          android: ProtectionLevel="signature"
6.  />
7.  <service android:name="com.demo. AService"
8.          android:exported="true"
9.          android:permission="com.demo.permission.USER_INFO"
10. </service>
```



如果其他应用 B 要访问该服务，应该申明使用该服务，将以下申明语句补充完整。

11.< android:name='com.demo. AService">

【问题 3】(3 分)

应用程序框架层集中了很多 Android 开发需要的组件，其中最主要的就是 Activities. BroadcastReceiver. Services 以及 Content Providers 这四大组件，围绕四大组件存在很多的攻击方法，请说明以下三种攻击分别是针对哪个组件。

(1)目录遍历攻击。

(2)界面劫持攻击。

(3)短信拦截攻击。

【问题 4] (2 分)

移动终端设备常见的数据存储方式包括：①SharedPreferences；②文件存储；③SQLite 数据库；④ContentProvider；⑤网络存储。

从以上 5 种方式中选出 Android 系统支持的数据存储方式，给出对应存储方式的编号。

信管网参考答案：

【问题 1]

(1)权限声明机制

(2)应用程序签名机制

(3)安全沙箱

(4)地址空间布局随机化

【问题 2】

(1) AndroidManifest.xml

(2) LOCATION、PHONE

(3) user-permission

【问题 3】

(1)目录遍历攻击: Content Providers

(2)界面劫持攻击: Activities

(3)短信拦截攻击:Broadcast Receiver

【问题 4】

①②③④⑤

查看解析：www.cnitpm.com/st/5229618782.html