2022 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/

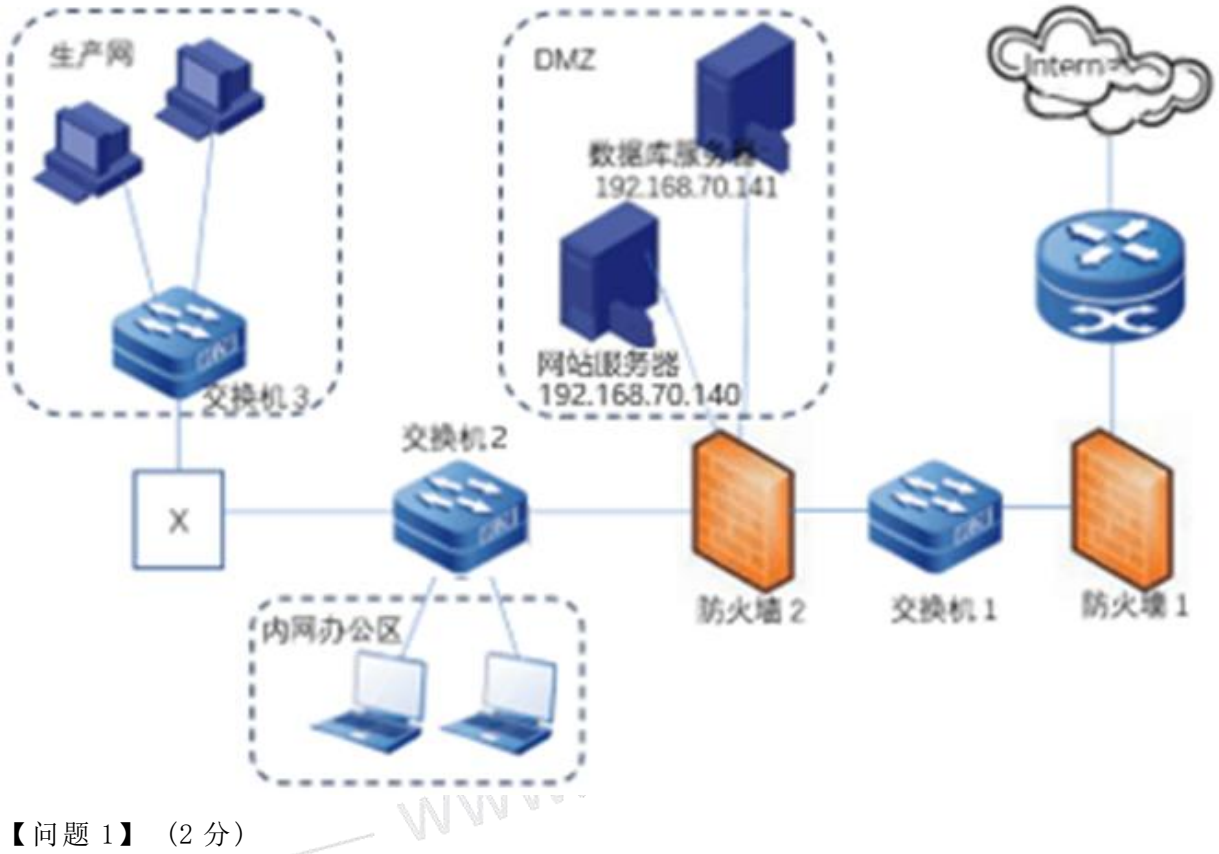
信管网培训中心：www.cnitpm.com/wx/

信管网微信公众号

信管网客服微信号

试题一(20 分)

已知某公司网络环境结构主要由三个部分组成，分别是 DMZ 区、内网办公区和生产区，其拓扑结构如图 1-1 所示。信息安全部的王工正在按照等级保护 2.0 的要求对部分业务系统开展安全配置。图 1-1 当中，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，信息安全部计算机所在网段为 192.168.11.1/24，王所使用的办公电脑 IP 地址为 192.168.11.2.



【问题 1】 (2 分)

为了防止生产网受到外部的网络安全威胁，安全策略要求生产网和其他网之间部署安全隔离装置，隔离强度达到接近物理隔离。请问图中 X 最有可能代表的安全设备是什么?

【问题 2】(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主要有基于双宿主主机防火墙、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 3】(2 分)

通常网络安全需要建立四道防线，第一道是保护，阻止网络入侵，第二道是监测，及时发现入侵和破坏，第三道是响应，攻击发生时确保网络打不垮，第四道是恢复，使网络在遭受攻击时能以

最快速度起死回生。请问拓扑图 1-1 中防火墙 1 属于第几道防线?

【问题 4】(6 分)

图 1-1 中防火墙 1 和防火墙 2 都采用 Ubuntu 系统自带的 iptables 防火墙，其默认的过滤规则如图 1-2 所示

Chain INPUT(policy ACCEPT)

Target prot opt source destination

Chain FORWARD (policy ACCEPT)

Target prot opt source destination

Chain OUTPUT (policy ACCEPT)

Target prot opt source destination

(1)请说明上述防火墙采取的是白名单还是黑名单安全策略

(2)图 1-2 显示的是 iptables 哪个表的信息，请写出表名。

(3)如果要设置 iptables 防火墙默认不允许任何数据包进入，请写出相应命令

【问题 5】(8 分)

DMZ 区的网站服务器是允许互联网进行访问的，为了实现这个目标，王工需要对防火墙进行有效配置。同时王工还需要通过防火墙 2 对网站服务器和数据库服务器进行日常运维

1)防火墙 1 应该允许哪些端口通过?

2)请编写防火墙 1 上实现互联网只能访问网站服务器的 iptables 过滤规则

3)请写出王工电脑的子网掩码

4)为了使王工能通过 SSH 协议远程运维 DMZ 区中的服务器请编写防火墙 2 的 iptables 滤规则。

信管网参考答案：

【问题 1】

网闸

【问题 2】

基于屏蔽子网的防火墙

应用代理位于被屏蔽子网中，对外公开的服务器也放在被屏蔽子网，外部网络只能访问被屏蔽子网，不能直接进入内部网络.

两个包过滤路由器的功能和配置是不同的。包过滤路由器 A 的作用是过滤外部网络对被屏蔽子网的访问。包过滤路由器 B 的作用是过滤被屏蔽子网对内部网络的访问。所有外部网络经由被屏蔽

子网对内部网络的访问，都必须经过应用代理服务器的检查和认证。

【问题 3】

第一道保护

【问题 4】

(1)黑名单安全策略

(2) filter 表

(3) iptables -P INPUT DROP

【问题 5】(8 分)

(1) 80 443

(2) iptables -A INPUT -p tcp - -dport 80,443 -jACCEPT

(3)255.255.255.0

(4) iptables -A INPUT -p tcp -s 192.168.11.2--dport 22 -jACCEPT

查看解析：www.cnitpm.com/st/573432133.html

试题二(20 分)

Linux 系统中所有内容都是以文件的形式保存和管理的，即一切皆文件。普通文本音视频二进制程序是文件，目录是文件，硬件设备(键盘、监视器、硬盘、打印机)是文件，就连网络套接字等也都是文件。在 Linux Ubuntu 系统下执行 Is-l 命令后显示的结果如图 2-1 所示

```
Renshuo@local:~/var/run$ ls -l
d rwx r-x r-x    2 root root     40  7 月 20 日  16:11  openvpn
l rwx rwx rwx    1 root root      8  7 月 20 日  16:11  shm->/dev/shm
s rw- rw- rw-    1 root root      0  7 月 20 日  16:11  snapd.socket
- rw- r-- r--    1 root root      4  7 月 20 日  16:11  crond.pid
- rwx r-x r-x    1 root root 203768  7 月 20 日  16:11  abc
```

【问题 1】(2 分)

请问执行上述命令的用户是普通用户还是超级用户?

【问题 2】(3 分)

(1)请给出图 2-1 中属于普通文件的文件名

2)请给出图 2-1 中的目录文件名

3)请给出图 2-1 中的符号链接文件名

【问题 3】(2 分)

符号链接作为 Linux 系统中的一种文件类型，它指向计算机上的另一个文件或文件夹。符号链接类似于 Windows 中的快捷方式。如果要在当前目录下,创建图 2-1 中所示的符号链接,

请给出相应命令

【问题 4】(3 分)

当源文件(或目录)被移动或者被删除时，指向它的符号链接就会失效

1)请给出命令,实现列出/home 目录下各种类型(如:文件目录及子目录)的所有失效链接

2)在(1)基础上，完善命令以实现删除所有失效链接

【问题 5】(10 分)

Linux 系统的权限模型由文件的所有者、文件的组、其他用户以及读(R)、写(w)、执行(x)组成。

1)请写出第一个文件的数字权限表示

2)请写出最后一个文件的数字权限表示

3)请写出普通用户执行最后一个文件后的有效权限

4)请给出去掉第一个文件的‘X’权限的命令。

5)执行(4)给出的命令后，请说明 root 用户能否进入该文件

信管网参考答案：

【问题 1】(2 分)

普通用户

【问题 2】(3 分)

(1)crond.pid abc

(2)Openvpn

(3)shm

【问题 3】(2 分)

In-s /dev/shm shm

解析:创建软连接: In -s(必须)源文件绝对路径连接文件名

【问题 4】(3 分)

(1)find /home -xtype l

(2) find /home -xtype l -delete

【问题 5】(10 分)

(1)755

(2)755

(3) rx(读、可执行)

(4) chmod a-x openvpn 或, chmod ugo-x openvpn

(5)root 用户不能否进入该文件。因为如果目录没有可执行权限，则无法 cd 到目录中

查看解析：www.cnitpm.com/st/5734415382.html

试题三(18 分)

Windows 系统日志是记录系统中硬件、软件和系统问题的信息，同时还可以监视系统中发生的事件。用户可以通过它来检查错误发生的原因,或者寻找受到攻击时攻击者留下的痕迹有一天，王工在夜间的例行安全巡检过程中，发现有异常日志告警，通过查看 NTA 全流量分析设备，找到了对应的可疑流量，请分析其中可能的安全事件。

日志事件数：3625

级别	日期和时间	来源	事件 ID 任务类别
信息	2022/7/23 22:00:04	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:04	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:04	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:03	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:03	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:03	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:03	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:03	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:03	Microsoft windows security auditing	4625 Logon
信息	2022/7/23 22:00:03	Microsoft windows security auditing	4625 Logon

ID	Source	Destination	Protocol	Info
11898	192.168.69.69	192.168.1.100	TCP	60-49924→3389[ACK] Seq=1 Ack=1 Win=66536 Len=0
11891	192.168.69.69	192.168.1.100	TLSv1	73 Ignored Unknown Record
11892	192.168.1.100	192.168.69.69	TCP	54 3389→49924 [ACK] Seq=1 Ack=20 Win=66536 Len=0
11893	192.168.1.100	192.168.69.69	TLSv1	73 Ignored Unknown Record
11899	192.168.69.69	192.168.1.100	TCP	60-49924→3389[ACK] Seq=20 Ack=20 Win=66536 Len=0
12161	192.168.69.69	192.168.1.100	TLSv1	248 client hello
12162	192.168.1.100	192.168.69.69	TLSv1	878 Server Hello,Certificate,server hello Done
12164	192.168.69.69	192.168.1.100	TLSv1	380 client Key Exchange, Change Cipher spec, Encrypted Handshake Message
12165	192.168.1.100	192.168.69.69	TLSv1	113 Change Cipher spec, Encrypted Handshake Message
12167	192.168.69.69	192.168.1.100	TCP	60-49924→3389[ACK] Seq=548 Ack=903 Win=64768 Len=0
12168	192.168.69.69	192.168.1.100	TLSv1	139 Application Data
12169	192.168.1.100	192.168.69.69	TLSv1	251 Application Data
12170	192.168.69.69	192.168.1.100	TLSv1	875 Application Data
12171	192.168.1.100	192.168.69.69	TLSv1	395 Application Data

【问题 1】(3 分)

访问 windows 系统中的日志记录有多种方法，请问通过命令行窗口快速访问日志的命令名字(事件查看器)是什么?

【问题 2】(2 分)

Windows 系统通过事件 D 来记录不同的系统行为，图 3-1 的事件 ID 为 4625，请结合任务类别，判断导致上述日志的最有可能的情况。备选项:

A、本地成功登录 B、网络失败登录 C、网络成功登录 D、本地失败登录

【问题 3】(2 分)

王工通过对攻击流量的关联分析定位到了图 3-2 所示的网络分组，请指出上述攻击针对的是哪一个端口。

【问题 4】(3 分)

如果要在 Wireshark 当中过滤出上述流量分组请写出在显示过滤框中应输入的过滤表达式

【问题 5】(3 分)

Windows 系统为了实现安全的远程登录使用了 tls 协议，请问图 3-2 中，服务器的数字证书是在哪一个数据包中传递的?通信双方是从哪一个数据包开始传递加密数据的?请给出对应数据包的序号。

【问题 6】(3 分)

网络安全事件可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。请问上述攻击属于哪一种网络安全事件?

【问题 7】(2 分)

此类攻击针对的是三大安全目标即保密性、完整性、可用性中的哪一个?

信管网参考答案:

【问题 1】(3 分)

安全日志 eventvwr.msc

【问题 2】(2 分)

B

【问题 3】(2 分)

3389

【问题 4】(3 分)

ip.addr eq 192.168.69.69

【问题 5】(3 分)

12162，12168

【问题 6】(3 分)

网络攻击事件

【问题 7】(2 分)

保密性

查看解析：www.cnitpm.com/st/5734513539.html

试题四(17 分)

网络安全侧重于防护网络和信息化的基础设施，特别重视重要系统和设施、关键信息基础设施以及新产业、新业务和新模式的有序和安全。数据安全侧重于保障数据在开放、利用、流转等处理环节的安全以及个人信息隐私保护。网络安全与数据安全紧密相连，相辅相成。数据安全要实现数据资源异常访问行为分析，高度依赖网络安全日志的完整性。随着网络安全法和数据安全法的落地，数据安全已经进入法制化时代。

【问题 1】(6 分)

2022 年 7 月 21 日国家互联网信息办公室公布了对滴滴全球股份有限公司依法做出网络安全宙查相关行政处罚的决定，开出了 80.26 亿的罚单，请分析一下，滴滴全球股份有限公司违反了哪些网络安全法律法规?

【问题 2】(2 分)

根据《中华人民共和国数据安全法》，数据分类分级已经成为企业数据安全治理的必选题般企业按数据敏感程度划分,数据可以分为一级公开数据、二级内部数据、三级秘密数据四级机密数据。请问一般员工个人信息属于几级数据?

【问题 3】(2 分)

隐私可以分为身份隐私、属性隐私、社交关系隐私、位置轨迹隐私等几大类，请问员工的薪水属于哪一类隐私?

【问题 4】(2 分)

隐私保护常见的技术措施有抑制、泛化、置换、扰动和裁剪等。若某员工的月薪为 8750 元经过脱敏处理后，显示为 5k-10k，这种处理方式属于哪种技术措施?

【问题 5】(5 分)

密码学技术也可以用于实现隐私保护,利用加密技术阻止非法用户对隐私数据的未授权访问和滥用。若某员工的用户名为“admin”，计划用 RSA 对用户名进行加密，假设选取的两个素数 p=47，q=71，公钥加密指数 e=3。请问:

1)上述 RSA 加密算法的私钥是多少?

2)请给出上述用户名的 16 进制表示的整数值。

3)直接利用(1)中的公钥对(2)中的整数值进行加密是否可行?请简述原因

4)请写出对该用户名进行加密的计算公式

信管网参考答案：

【问题 1】(6 分)

滴滴全球股份有限公司违反《网络安全法》《数据安全法》《个人信息保护法》

【问题 2】(2 分)

二级内部数据

【问题 3】(2 分)

属性隐私

【问题 4】(2 分)

泛化

【问题 5】(5 分)

(1) d=2147

(2)61646D696E

(3)不能，因为明文 m 不能大于 n，如果大于 n，会发生回绕，失去原有属性

(4)C=Mmod n

查看解析：www.cnitpm.com/st/5734613909.html