1 取款机首要的安全考虑是 :

电子设备的物理安全 网络可用性 网络延迟

2 问企业要通过其网络边界保护IM通讯，问对于企业来说最大的顾虑/问题是什么：A IM客户端使用随机端口 B 运行某些IM客户端无需管理员权限 C选项是允许im在不同的供应商之间通讯 D某些IM不需要安装即可运行

3连续安全监控计划如何降低风险Information Security Continuous Monitoring（ISCM/SCM）选项基本都不记得了，你们网上找一下，好像是美国政府的某个东西

4 使用正式安全测试报告的结构和格式的主要好处是什么

a 对高层如何如何 b对高管如何如何 c 对技术团队如何如何 d 对技术团队如何如何 抱歉实在不记得了，完全懵逼

5 建立医疗保健设施主要的安全考虑是什么

a 安全，容量， 合规

b 通风好，能源足够

c 大平层，便于移动办公

d 加固存储区域，适当通风，安全的收货区域

6 序列号预测可能是哪种攻击

a 拒绝服务

b 中间人

c 忘了

d 身份盗用

7 CTPED的前提是什么

a 良好环境可以改善建筑周边犯罪率

b 改进的物理安全可以改变访问此设施人员的行为，从而降低犯罪率

8 -1某组织指派安全专家应对淹没攻击：

1 以下哪种伙伴关系有助于快速缓解淹没攻击：

a 和线路提供商

b 和银行

3 和供应商

4 和用户

8-2 关于淹没攻击，潜在的威胁是什么？

就记得一个，我选的，攻击的组织者可能勒索钱财

8-3 安全专家需要关注的重点是什么？

就记得一个，我选的，防止僵尸网络的持续破坏

这个就是考APT了吧！

9还有关于USB传输的问题，习题上那个翻译非常有问题

原题是：

某企业管理层关注数据安全的问题，并有4个需求：

9-1 要求传输到USB设备上的数据的安全

英语的关键字是 transported data secure

所以我选了 使用加密的虚拟磁盘

那是有保密性要求

9-2 还有个需求是如何保护数据完整性

我选了定期进行VALIDATION

其他选项大概是 定期把磁带送到供应商处 ， 设定备份周期

10还有问 安全工程中 哪个是对于系统安全要求的反馈源

我选了系统架构， 还有的选项是CONOPS（好像是 运维概念）

11软件工程中， Software Assurance主要致力于干啥

选项是 提供一致的安全需求列表

指派安全人员进行安全需求评估

亲自评估什么需要保护，什么人需要保护，需要保护多久

还有两个选项不记得了

12 安全模型和网络，云考了很多

比如某个模式下数据丢失是谁的责任，数据泄漏引起的财务损失是谁的责任

法律基本没考

13 妈蛋Ipsec考了大概10题，各种问法 AH ESP 隧道模式 传输模式

14链路加密和端到端加密考了，原题

15问一个有多个角色的联网信息系统，要实现可靠的访问控制，第一步要做什么 A 用户配置文件 B ACL C 用于访问矩阵 D 基于角色的访问控制矩阵

16一直纠结的那个陷门，不是要搞什么合成交易，

而是要在生产系统里插入虚构但是可以识别的交易

所以我选了 只能在开发环境使用

因为在生产环境使用陷门和插入虚假交易都是不允许的，尤其是后者

17对硬件加密模块最有效的攻击是：

功耗 中间人 还有两个忘了

18取款机首要的安全考虑是

电子设备的物理安全 网络可用性 网络延迟

## 做题方法：

**一，可能正确的答案：**

选择适当的控制措施

根据实际情况选择措施

基线

门槛

工作方法

**二，可能不正确的答案：**

所有

没有

必须

Only 只有

**三，答案的三种类别：**

1、预防性的

2、探测性的

3、事后的

**尽量选预防的，尽量不要选事后性的**

## 题目

在与其他组织建立一个联合单点登陆（SSO）解决方案，下列哪项是组织主要关注的？

A.        发送声明给身份供应商

B.        定义身份的映射方案

C.        从合作伙伴的域申请身份声明

D.        让资源供应商查询身份供应商

根据下列情况什么时候变更防火墙配置的哈希值？

A.        在防火墙配置变更之前做哈希

B.        防火墙配置做增量备份

C.        配置变更后更新

通信网络中端到端加密的缺点是如下？

A.        防火墙和流量监控系统无法识别数据类型

B.        导致需要提升大量带宽

C.        加密原因导致性能下降可能造成通信中断

在哪个阶段需要展示DRP计划？？

A.沟通 B.计划 C.提交 D.恢复

web系统的cookie，攻击者可以绕过什么验证？

A.  有身份检查 B.  密码检查 C.  授权检查啥的 D.  认证

一家公司把他们的设备都搬到一个大的共享的机房里他们最重要做的是什么？

A.        设置互联网防火墙 B.        加强服务器控制台的验证

C.        给线缆打标签 D.        机柜加锁

有个外包公司的顾问，去你公司干活，违反了你们公司使用电脑的规章制度，问通过什么来惩罚他？

A. 用自己公司的政策规定 B. 外包公司的政策规定 C. 合同规定 D. 法律规定

SDLC在什么阶段，最可能发生审计行动？

A 初始 B 开发 C 运行维护 D实施

SDLC在什么阶段，可以更改安全保证内容以保证开发过程中减少变更

A 合同订立 B 开发 C 运行维护

SDLC 在什么环境就应该开始考虑安全需求

需求分析确认 实现 运行维护 处理

真实性包括？

1完整性和验证（优先） 2完整性和不可否认

防止内部威胁最好的方法

A 双因素 B 按业务部门分割数据库

测试BCP应急响应计划的对象

A 应急疏散 B 系统备份 C 渗透测试 D 设置故障热线

DR 进行功能响应的测试：

A应急疏散 B渗透测试 C.数据备份

DR 培训的目的：

a 正确应对安全事件 b 针对具体事件做出正确的反应

应急计划最重要的资产是？

A 全员员工 B 防火设施 C 酱油 D 酱油

开始审计之前，审计团队的头必须干什么？

A 拿正式书面授权 B 跟高层管理者碰头，商量预期结果

在一个有多用户访问的应用，一下哪类是访问控制的第一步？

A 创建访问控制矩阵ACM B ACL

安全评估和授权过程中，硬件清单和软件清单主要的目的是？

用于安全鉴证 检查系统边界 创建授权列表

Web应用在使用什么协议对数据防泄漏是最大的挑战？

HTTP XML WEBSOCKET

使⽤ html5，和下⾯那项，会带来⽹络数据泄露的挑战？

A. Cross Origin Resource Sharing (CORS)

B. WebSockets

C. Document Object Model (DOM) trees

D. Web Interface Definition Language (IDL) ）

在移动代码开发过程中，什么阶段决定了在哪类设备上开发?

A 初始 B 开发 C 规划 D 酱油

渗透测试发现漏洞，问最快速的解决方法？

A 代码修复 B 应用防火墙加规则

已知某程序有输入验证漏洞，以下最快速的做法

A 停止服务 B 代码修复 C 实施 IDS D 应用防火墙添加规则

安全评估过程中，组织本身在评估过程中的作用？

A 如果抛弃组织结构，安全策略将不适用 B 衡量与标准的差距

对于备份介质，下列对称加密方法最合适的是

A DES B AES

独立测试的优势？

A 增加隐藏功能被发现的概率/提⾼发现隐藏⻛险点的可能性

B 减少隐藏功能被发现的概率

如果电脑被盗了，下列哪个方法能够最有效的保证数据不泄密？

A 设置BIOS密码 B 文件加密 C 全磁盘加密

以下哪项是预防性访问控制？

A 酱油

B 在入口处设置陷阱（如果是陷门，双门防护就是这个）

C 访问控制软件

D ⼊侵检测系统

一个攻击者通过企业VPN开始攻击网络服务器，以下哪种访问控制措施可以防护这类攻击？

A 防火墙上通过限制有效范围外的IP访问

D 网络服务器上通过使用用户名密码

关于安全基线的最佳描述：

A组织的高级别安全定义

B用来信息安全管理的软件

C用来支撑组织信息安全政策的实践证明

D在组织实施一致的安全配置

软件开发管理流程(SDLC)维持最新的硬件和软件清单是：（争议）

A系统管理的重要XXXX

B变更管理的重要XXXX

C风险管理的重要XXXX

D质量管理的重要XXXX

数据标记（marking）和数据标签（labeling）的区别是

A数据标记是人类可读的，数据标签是内部数据结构使用的

B数据标签是人类可读的，介质标签是内部数据结构使用的

C数据标记是公开的法律/法规定义的，数据标签是内部信息安全政策定义的

D数据标签是公开的法律/法规定义的，数据标记是内部信息安全政策定义的

关于组织最大的数据保留风险是：

A保留超过数据有效期但是有数据取证需要的数据

B保留超过数据有效期但是没有数据取证需要的数据

C删除超过数据有效期但是有数据取证需要的数据

D删除超过数据有效期但是没有数据取证需要的数据

场景是管理层对介质管理提出要求

1）USB传输的数据必须要有安全管控

2）备份数据要保证完整性

问题1：对于第一个要求应该怎么做：

A只允许传输只读文件 B使用虚拟硬盘

C定期格式化硬盘 D禁用USB

问题2：对于第二个要求应该怎么做：

A定期将备份磁带运到异地场所

B定期对备份数据进行校验

下列哪个访问策略是系统用于用户对访问对象的固有安全（fixed secure）属性

A MAC B DAC C ACL D授权用户访问

Which security access policy contains fixed security attributes that are used by the

system to determine a user's access to a file or object?

哪个安全访问策略包含固定的安全属性，系统⽤来确定⽤户对⽂件或对象的访问？

A.强制访问控制 B. ⾃主访问控制 C.访问控制列表 D.授权⽤户控制

（固定了客体，应该选 ACL，如果固定了主体，就是能⼒表，不固定主体和客体，

才是 ACM）

使用一次性密码本的双因素认证防止了下面的什么攻击

A重放 B暴力破解

以下哪个定义了恶意的AP

A没有通过防火墙管理的AP

B没有使用WEP和3DES加密的AP

C接入交换机但是没有网络管理员管理的AP

D被某种特洛伊木马或者恶意软件感染的AP

场景是企业有一些服务器放在互联网，然后某天有一台互联网服务器遭到破坏，管理层收到报告，并由管理层转给了安全经理

问题1：安全经理收到报告之后首先要做的是：

C用备份数据对互联网服务器进行恢复

D对报告进行调查

问题2：破坏是由于缺少一个安全修复程序引起，在打上补丁之后，什么时候对系统进行上线：

A对该漏洞进行全面评估和测试后

B对互联网服务器进行漏洞渗透测试和评估之后

C立即上线保证业务的连续性

D检验互联网服务器的完整性并获得相应的授权之后

网络管理外包最有效保障安全的措施： (争议)

A 增强安全访问控制

B 签订保密协议

C 把所有跟敏感信息相关的内容记录下来

D链接安全策略

端口扫描时会出现什么意想不到的事情？

a.开启以前未开启的端口

b.拒绝服务

c.开通管理员权限

漏洞扫描可能会造成以下：

A、打开端口

B、拒绝服务DOS

如何进行客户端的安全控制 选择有（我选客户端漏洞扫描）

关闭不必要和web 服务、

对客户端扫描漏洞进安全评估

wifi 802.11g那个版本有什么特点？

A向后兼容801.11b

B提供更快速率

C支持令牌

个人对网络的访问是基于？

A风险矩阵 B数据分类 C数据价值 D业务需求

一个组织想采用 WEB 程序来让员工访问客户信息数据，决定其安全级别的是：

a.数据价值 b 加密要求 c 服务器要求 d 访问控制方式

某些高级语言不易产生缓冲区攻击，但什么情况还是会造成缓冲区攻击？

A第三方库(优先) B plugin C supporting application

哪一项攻击会影响VOIP通道的完整性？

A、影响机密性的选项 B、中间人（影响完整性及机密性） C、资源耗尽

审计师要求软件留后门 （trapdoor）以方便合成交易，在使用trapdoor的时候要注意什么？

b 需要有良好的访问控制，在生产环境使用（争议）

c 在开发环境使用

d 要确保做好单向散列，在系统生命周期结束之后要剔除

收集个人隐私在系统中保存的时候怎么做比较增加安全性：

列加密 collunn加密 Tokenization

组织的服务器遇到flood攻击，以下方法可以有效解决的是

a 购买不同运营商的带宽

b 将你的服务下线

c 找安全供应商购买最新的安全软件

d 应⽤防⽕墙设置

组织的服务器遇到flood攻击，以下⽅法是快速有效解决⽅法

a 购买不同运营商的带宽

b 将你的服务下线

c 找安全供应商购买最新的安全软件

d 应⽤防⽕墙设置

组织服务器遇到flood攻击，服务器在遇到大量请求的时候会做的是 （flood是泛洪）

a 目前服务器的端口上尝试不断进行回应

b 保留资源来等待后续请求

组织服务器遇到源地址不可达的syn攻击，服务器在遇到大量请求的时候会做的是 （半开）

a 目前服务器的端口上尝试不断进行回应

b 保留资源来等待后续请求

对于组织来说如果对于在采用了对应某个安全合规要求的所有措施后，可能出现的结果是

a 安全隐患的解决 b 成本大幅增加

c 风险相关 d 投资回报(ROI)的增加

采用所有可能的安全措施后可能：

a与业务保持一致 b总体风险降低 c ROI 增加

对于数据库的信息保护，哪个更彻底？AC其实都可以用来保护隐私（争议）

A数据库透明加密 B列加密

C标记化 D数据元素级别替换

以下哪个能最好说明了最小特权？

A. 员工跟管理员审查自己的所有的权限 B. 员工给部门负责人审查自己所有的权限

C. 管理员审查员工的所有权限 D. 管理员列出所有员工的权限给部门负责人审查

密码加密存储依赖：

加密密码 单项哈希

异地备份的优点

1. 可用性 B易操作 C易恢复

对于安全培训和教育实施最好的是

A 强制员工定期进行培训学习（效果最好）

B 给员工群发邮件，题型每日安全热点

C 组织员工参加安全意识培训

使用第三方身份管理的好处

A．Web登录 B．自动化账号管理 C. 目录同步

内存中组织低级别进程向高级别进程访问，增加的单独的安全机制是：

A 异步执行 B 内存分段 C多态处理器

组织要跟合作伙伴共享一些信息，信息系统打通，有验证、授权、审计的需求、基于什么技术实现？

A SAML B XACML

购买PEN-TEST需要考略什么：

A 网络渗透和应用程序渗透不一样    B 任何时候不要把计划给系统管理员

数据包头使用隐写术，可以会被利用来干嘛

A、改变路由方向 B、隐蔽通道 C、增加包头字段 D、隐藏包头

⽹络层协议的保留字段被使⽤（类似含义），会带来什么问题？

A、改变路由方向 B、隐蔽通道 C、增加包头字段 D、隐藏包头

在进行渗透测试时，测试人员对一下哪一项信息最感兴趣？

A 工作申请宣传册 B 安装后门的位置

C 主要的网络接入点 D 能够攻击弱点的漏洞

XSS影响的是？

A服务器 B用户 C网络 D打酱油

用一种编程语言降低缓存区溢出，但是

A需要图片支持 B需要代码支持 3需要机器支持 4 需要打酱油支持

系统保护隐私的第一步是干嘛？

A尽量减少收集 B加密 C数据隐藏 D数据存储

在安全威胁较低的情况下，使⽤包过滤防⽕墙？

A 更⽅便、更灵活、可以解决 IP 欺骗攻击

B 更⽅便、更灵活、透明

“鉴证”（Accreditation就是认可）是什么意思？

管理层在知情的状况下决定是否接收⻛险

用于局域网间的端口认证，单点…..

A 80211 B 802.1x C802.1q D 802.3z

某场景， 移动代码安全需要关注的⽅⾯？

Web 浏览器、电⼦邮件、即时消息、媒体播放器

道德基于？

A⺠法 B刑法 C个⼈诚信 D合规性

SPA是什么？（简单电⼒分析， 简单功耗分析）

A静电放电， B功耗， C发电， D磁场

SPA是在密码或别的安全相关操作时直接观察功耗，可以得知设备运⾏时的信息如密钥资料。

路由器对应 OSI 模型中 7 层⾥⾯的那两层之间？

数据链路层与传输层

TCP/IP 的应⽤层对于 OSI 模型中除了应⽤层外还有哪⼏层？

表示层和会话层

CC（通⽤准则）⾥⾯哪⼀个定义了可重⽤的安全需求？

PP、 TOE、 ST

⽹络传输中最能保证传输信息的完整性和机密性？

TLS、 SSL、 IPSEC

安全度量是什么？

量化安全⼯作的有效性 加速安全评估

企业的 dns 服务器有两个事件发⽣

a、 dns 服务器收到⼤量针对 www.123456.com 的解析请求

b、 dns 服务器对这些请求返回错误的反馈

问题 1：如果此时企业的⽤户访问 www.123456.com，会发⽣什么？

A、浏览器没反应

B、显示 dns 出错

C、被正确解析

D、被解析成错误的⽹站

问题 2： dns 服务器受到了什么攻击？

A、 ddos B、 缓存中毒

使⽤ SAML ⾄少需要？

⽤户⾄少在⼀个商户上注册（关注此选项，依靠 IDP）已经有了一个provision id

场景题：组织采用了云安全供应商的云主机服务，云服务商供了第三方的身份认证服务

题目一，企业对于使⽤云服务造成了数据残留的⻛险，由谁负最终的责任？

A数据所有者 、 B数据处理者、 C保管员

题目二，因身份认证问题导致金钱损失谁负责：

A组织 B云服务商 C身份认证服务提供商

IPSEC 哪个协议提供机密性和完整性？

A,AH B,ESP

一个员工上传病毒到内网， 司法鉴定人员应该怎么做最佳：

A、断掉员工电脑网络连接 B、内部公告病毒影响 D、扣留该员工电脑

下列哪⼀项最有助于降低某设备获取其他设备的数据包的可能性？

A过滤器 B交换机（PS：一个口一个广播域） C路由器 D防⽕墙

安全委员会的职责：

确保安全符合法律法规 对安全措施起督导作⽤

IDC 机房空调等环境形成的“正⽓压”指什么？（空气只往外流）

选项： A、 IDC 内的⽓流想通过窗⼦跑出来； C、外边的⽓流想通过窗⼦跑进去

⼀个系统不允许⾮法⽤户，必须关注什么

选项： A,FAR B,FRR 《选 FAR，第⼆类错误，错误的接受》

那种路由协议能抵御 DDOS 攻击

链路状态 BGP(可以流量清洗) 静态 弹性

哪种路由最安全？

静态路由 距离⽮量 链路状态 BGP

猜测序列号是什么攻击

窃听 中间⼈

DRP（还是 BCP）培训的最后⼀步是什么？

员⼯反馈意⻅ 员⼯测试

组织的安全策略应该怎样？

被管理层认可 员⼯接收

嵌⼊式系统容易发⽣什么？

信息泄露

系统攻击是由于没打安全补丁，问怎么打补丁

测试后再打

打完补丁的服务器应当：

直接上线 测试完整性并取得授权后再上线 执行漏洞测试后上线

（黑客）为什么使用硬件 keylogger 而不是软件 keylogger（键盘记录器）？

物理安全、 适合多个用户、 可以通过网络传送数据、 保存数据

公司把设备和科研移到海外，安全官应担⼼什么？

A.设备被盗 B.物理安全得不到保障 C.知识产权 D.缺少安全措施

哪个更容易监测出来漏洞？

硬件 内核 软件

哪种设施更容易监测出来漏洞：

硬件、软件、内核

SCADA那种⼯控系统打补丁最⼤⻛险是？

A没有补丁缺乏⼚家⽀持 B⽼旧设备

秘密级别较低的⽂件授予可写权限，适合什么安全模型？

BIBA BLP CW 无干扰

秘密级别较⾼的⽂件授予只读权限，秘密级别较低的⽂件授予可写权限，适合什么安全

模型？

A.BLP B.Biba C.clark-wilson

vpn 对数据通信进⾏了加密，但如果不采⽤其他措施，可以能会导致什么?

ddos 服务盗窃 公钥被盗 加密秘钥被修改

⽹卡设置了混合模式，但只收到⾃⼰的⽹络信息，原因是什么?

防⽕墙禁⽌嗅探 ⽹络使⽤交换机模式

NIC混合模式可能导致的安全风险： （解释：抓包需要先讲网卡设置为混合模式，可以收到更多到本机的包）

A.嗅探 B.欺骗 C.中间人 D. DOS

定期检查网卡NIC，是为了

A、防嗅探 B、中间人

使⽤ saml 最起码的要求是什么?

⽤户⾄少在⼀个商户上注册

哪⼀个是对所有的过程和⽂件的变更进⾏控制

配置管理 CMMI 流程化

记录所有硬件和软件的资产主要⽤于

配置管理 变更管理 ⻛险评估

认可是在 SDLC 的哪个阶段结束后完成

运⾏和维护 验证 实施

软件补丁是要什么部⻔去发布

安全 运维

给软件打补丁是由谁来执行：

安全人员 运维人员 管理层 审计人员

哪个组件提供了 SCAP ⾃动评估的漏洞信息？

CVE

⾼层让公司在安全⽅⾯保持合规为了什么？

展示 DC－DD（适度关注/勤勉） 保护公司的架构

wifi 安全选择算法 ECC 而不是 RSA：

a ECC密钥长度更长 b ECC速度快、资源占用少

c 提供更强的加密 d RAS有安全漏洞

PPP ⽀持多点、多协议认证

哪个提供多协议认证加密支持： PPP

身份建⽴需要什么？

PROVISION（条款）

有 web 业务，需要认证授权和审计，需要那个服务/协议？

Ldap saml

在⼀个有⼈有计算机的地⽅的防⽕设施选哪个？

A 湿管 B预制 C FM200

嵌⼊式系统容易受到什么攻击？

硬件加密容易最容易被什么攻击？

引⼊⼀个错误后，对硬件电流、辐射进⾏分析属于什么⽅法？

都是功耗攻击（旁路的）

联合身份认证的标准是什么，

a、802.11i b、kerberos c、ldep、 d、saml

以下哪个协议在互联⽹上提供最好的机密性和安全性

A tls B sha C ssl D cbc-mac

计算机⽤户对什么内容负最主要责任

a 数据分类 b ⽤户账号的操作 c 账号管理

PKI在什么情况下对CA的认证产⽣交叉数字证书?

B 当CA之间需要互相认证 D 当数字证书在CA之间进⾏传输

通过环境设计预防犯罪的定义是什么 这题很贱 有两个选项

a 通过环境的健康化（单词health）来降低犯罪的可能性

b 通过优化设施（facility）的优化改进，来减少犯罪

进⾏安全评估的时候⾸先要进⾏以下哪个步骤

a bia b 确定安全评估需求 c 买最先进的安全技术

审计⼈员进⾏安全审计的时候第⼀步要做啥（争议）

a 和管理层沟通说明审计要达到的效果

b 确定访谈⼈员

c 获取关于安全规范的最佳实践

业务⼈员（staff members） 《应该翻译成员⼯》 对数据中⼼有问题的设备进⾏下线的

时候，以下哪个是合规

a 只有管理层有权限

b 需要适当的授权⼈员的审批

c 只有特定设备可以下线

d 需要业务经理（staff member Manager）的审批《应该翻译成员⼯经理》

对于跨国商业合作中的数据加密存储和传输应⽤，最有可能遇到的问题是

a、国与国之间的加密标准规范不统⼀（⼤概这个意思）

b、部分国家的法规监管要求加密数据必须和密钥⼀起传送

c、部分国家的技术实⼒⽆法⽀持加密传输（⼤概这个意思）

d、很多国家地区的法规不允许过于强的加密，甚⾄可能不允许加密

从组织的⾓度来看，要求安全⼯作⼈员在⼯作中尊重isc的安全道德是为了什么

组织的声誉 安全⼯作⼈员的形象

以下组织遇到的哪类安全问题直接会可能造成⾦钱上的损失

1. 声誉 b、信息 c、信⽤ d、设备

进⾏安全意识培训程序的最后⼀部是

a 评估培训有效性 b 收集员⼯的反馈 c 收集培训未涉及的内容以便将来的程序改进

哪个攻击使⽤了icmp

a 泪滴攻击 b smurf攻击 c 中间人 D ddos

Srnurf（蓝精灵）：属于泛洪DOS，它使用Internet 控制消息协议(ICMP) 回送数据包，反弹攻击，消耗带宽（ICMP）

某个程序的语⾔已经对缓冲区溢出攻击进⾏了有效预防，然⽽以下哪类问题还会可能造

成缓冲区溢出攻击？

b 在编程中调⽤了别的库 d 使⽤这⼀程序语⾳实现的应⽤程序

基于单向散列的密码认证系统依赖于？

单向函数的可靠性

IPSEC在隧道模式下报头和报⽂的加密是？

a 都加密 b 都不加密 c 报头加密报⽂不加密 d 报头不加密报⽂加密

IPSEC传输模式下的封装安全载荷(ESP)的作⽤是？

A.加密和可选择验证整个IP包

B. 加密和可选择验证IP头部，⽽不是IP载荷

C. 加密和可选择验证IP载荷，⽽不是IP头部

D. 验证IP载荷及选择的部分IP头部

1、使⽤ TPM ⽐ USB 的好处

防篡改 速度快 使⽤更⻓密钥

在带宽受限的情况下，使⽤那种⽅法传递断⾔

SAML oauth的 access token（更高效）

如何获取⽤于法庭的证据?

e-discovery 强行逼供 硬盘虚拟化 交换协议

渗透测试进⼊系统后，为了xx需要xx？

1.横向提升特权， 2 纵向提升特权， 3 特权账号， 4 系统管理员账号

以下哪项必须成为⽀持电⼦发现存储在云环境中的数据的合同的⼀部分？

A. 与组织⽬录服务集成以进⾏身份验证

B. 数据的标记

C. 混合部署模式的住宿

D. 数据位置的识别

欧盟 - 美国安全港隐私政策必须符合以下哪些要素？

A. 对数据主体收集的信息将保留多⻓时间以及将如何最终处理的解释。

B. 如果数据主体需要更正，可以在收集信息的组织联系哪些⼈员。

C. 对信息收集机构遵守的监管框架和合规标准的解释。

D. 对采集机构采集的数据主题信息的所有技术的解释。

DRP最少多久审批一次：

高层变动 每季度 每年或根据业务需求更少频次 按业务需求

个人或组帐户权限评审频率：

a.升职 b离职 c 持续 D每年一次或更低频率

让SLA发挥效用的……：

管理层approve 管理层review 双方公开 双方认可

ipsec保障机密和完整性的安全机制是：

AH ESP IKE

被DDOS攻击后，采取安全策略的第一个步骤是

执行可行性分析

了解现有网络运营和技术

采购抗DDOS设备

对安全渗透公司提供的方案进行评估

安全度量（metric）是为了：

量化安全措施的有效性 加速安全评估

和第三方签署合同，合同中机构有什么样的权力：

a.保留审计控制的权利 b.保留续保时更改合同的权利

c.泄密时终止合同的权利 d.做对方公司安全评估的权利

已知某程序有输入验证漏洞，以下最合适的做法（）

A 停止服务 B 代码修复 C IDS D应用防火墙添加规则

缓冲区溢出会导致：

A 改变系统恢复的程序 B 执行任意代码

以下哪项是机密性必须包含的

A 数据保留 B 文档处置 数据处置 文件保留

合规的目的：

提高（improve）态势/减少监管 提高态势/减少攻击影响

减少态势/减少监管 减少策略/减少攻击影响

哪两个职责需要分离：

a 系统开发和系统维护 b 生产控制和数据控制

收集个人隐私在系统中保存的时候怎么做比较增加安全性：

列加密 行加密 Tokenization

存储和处理PII时以下哪个选项是最重要的考虑因素？

A加密和散列所有PII，以避免泄露和篡改

B将PII储存不超过一年

C避免在云服务提供商中储存PII

D遵守收集限制法律法规

公司生产环境准备接入了一个第三方软件，该公司怎么做为最佳：

A. 执行软件漏洞扫描 B. 和第三方公司签署修复合同 C. 进行软件备份托管

用户验收测试时发现了 bug，软件开发人员要做什么？

a. 执行一个全面的同行评审 b.发邮件通知开发团队的头儿

c.修补漏洞 d.用变更管理工具做记录

当在单元测试中发现了一个安全漏洞时，软件开发人员必须要做下面哪项？

A. 执行一个全面的同行评审 B. 修补该漏洞，并通知开发团队

C. 将漏洞细节电子邮件发送给开发团队负责人 D. 使用变更管理工具记录该问题

云服务中搜集个人隐私采用什么方法比较好：

a 数据加密 b 标记化（Tokenization）

怎么可以防止两个人在工作中串谋

A. 最小特权 B. 岗位轮换 C. 职责分离 D. 强制休假

恶意程序在一定限制时间范围内访问了其他正常程序的进程，什么攻击？

A.后门 B.特洛伊木马 C.缓冲区溢出 D.竞争状态

在一个 OFF-site（异地站点） 站点备份数据的优点：

A.数据可用性 B.易操作 C.易恢复

什么会引起 Dr评审：

a 高导管理人员变更 b 安全委员会人员增加 c 组织合并

某员工截获了安全官发给 CEO 的邮件，他篡改后再发给 CEO，这是个什么攻击：

a伪装 b中间人 c 欺骗 d dos

应对暴力破解密码，可以：

a用户密码意识培训并强制实施复杂口令机制 b用户意识培训

C实施强制复杂口令 D登录次数超限后强制锁定帐户

移动终端面临的最大安全漏洞：

a 操作系统 b互联网应用程序

计算机管理中，有一个管理组需要共享使用一组高级别的凭据，哪个是最佳实践：

a 对使用凭据的程序进行 check out 《check in, check out,就知道是谁在用了》

b 记录使用日志

S／MIME 靠什么交换密钥？

A 共享 B 证书《数字证书》 C IKE《⽤于 IPSec》

为什么用多重散列？

一个散列被碰撞后，还有其他散列可以防止失效

企业中，常见的物理防护设备是哪个？

摄像头、 门锁、 酱油

项目（系统）已经启动了， DR 的顺序是什么？（具体情况具体分析）

风险分析 战略开发 计划实施 测试和维护

风险评估-业务影响分析-制定策略-开发计划-培训测试-维护

什么是信息安全政策？

A特定的情况给予的特定步骤，B所有行业接受的特定规则，C代表管理层所发表的声明原则

网线捆绑在一起，会导致哪个选项

A.bleeding B.cross talk（串扰） C.中间人攻击 D.DDoS

幼儿园实施什么物理访问措施最好：

A.防尾随 B.双因素认证 C.报警器连到安全控制系统 D.行为分析检测

被动式红外传感器用于非气候控制环境：

A.相对于背景温度降低检测到的物体温度。

B.相对于背景温度增加检测到的物体温度。

C.自动补偿背景温度的变化。

D.独立于背景温度检测特定温度的物体。

对已收集的详细日志进行分析，可能存在什么问题？

A收集的日志使用的时候发现不可用 B大部分的应用和系统不支持日志

C日志中缺少用户和应用程序的详细访问信息 D不能及时审核

邮件服务还有文件传输服务是哪层的？

应用层 网络层 传输层 数据链路层

隐写术用信息隐藏到图片中使用了什么技术：

1散列(hash)二进制 2安全哈希(hash) 3 LSB最低有效位

最大中断时间的定义:

A 允许业务中断的最大时间，如果该时间无法恢复那么该业务就无法进行恢复

对于跨国犯罪的取证，面临的最大困难是？

A 对于取证没有一个国际通用标准 B 别的国家的时间戳不能作为证据

跨国计算机犯罪最大的问题是？

A、没有一个标准统一的法律 B、无法确认时间戳之类的意思 C、无法识别IP

渗透测试发生在操作和维护阶段

如果未采取其他的措施，那么加密后的通信还会遇到什么攻击？（VPN对数据通信进行了加密，但如果不采用其他措施，可能会受到什么攻击？）

A、公钥被盗 B、盗窃服务（Theft Service） C、密钥篡改 D、DDOS

制定物理安全的防护模板（protection profile）（即指PP）之前需要做的是：

A、识别技术要求 B、信息资产识别 C、选择位置 D、地址勘测

下面哪个最好的描述了紧急情况？

A、非法或不道德的用来捕获嫌疑犯的行为或方法

B、诱捕（Enticement）是用来捕获嫌疑人行动的

C、黑客没有真正伤害任何人

D、因为担心嫌疑人试图破坏证据，那么执法人员会迅速扣押证据

哪个身份管理流程是由主体的身份建立的？

A、注册 Enrollment

B、开通 Provisioning

C、授权 Authorization

D、信任 Trust

恢复测试至少多长时间进行评审？

A、每季度 B、持续 C、在高级管理层指导下开展 D、仅在变更时

火灾中，使用哪种门禁最好？

A、电子 B、密码 C、钥匙锁 D、推杆式

IP源地址和目的地址在哪一层被处理？ 网络层

## 连线拖图题

ip掩码  --- 隐藏IP地址

ip伪造 ----  伪造源或者目的IP地址

Ip重定向 ---- 路由重定向访问IP地址

x头（x标记）----  邮件服务器中转时候加上的内容

邮件头 -----  邮件发送客户端加上的内容

信封头 ---- 邮件接收服务器加上的内容

云目录     既能本地也能云端使用帐号登录

目录同步  类似于ldap找AD同步信息

云帐号     云的单点登录，关键词SSO

CC评估保证级别，7级

EAL1 功能测试

EAL2 结构测试

EAL3 系统测试和检查

EAL4 系统设计测试和回顾

EAL5 半正式设计和测试

EAL6 半正式验证，设计和测试

EAL7 正式验证，设计和测试

拖图：网络拓扑

Untrust 外网，访问用户

DMZ 缓冲区，应用服务器

Trust 内网

访问控制方法：

对象是设备 系统 信息 数据 人 建筑

右边的方法是： 加密，物理控制，意识培训，等等方法

设备 防火墙

系统 认证、认可

信息 加密

数据 加密或者XX

人 意识培训

建筑 物理控制

安全控制策略对应关系

信息 ------- 加密

设施 ------- 窗户/栅栏

设备 ------- 防火墙

系统 ------- 认证（认证，认可）

人员角色：

审计委员会 由董事会任命，以帮助其审查和评估公司内部运作、内部审计系统报表的透明度和准确性，使公司的投资者、客户和债权人继续保持对组织机构的信心

外部审计师 往往代表法律机构，确保组织符合法律要求

内部审计师 内部人员，负责测试和认证安全策略是否被正确实现，以及相关的安全解决方案是否合适。

执行管理层 C开头的管理者，CEO/CFO/CPO/CIO等

合规官 关注于法律法规的人 理解为要我做

安全官 关注于安全的人 理解为我要做

安全委员会 决策并批准安全相关事务、策略、标准、指南和程序。

数据分类排序：

第一步：记录信息资产（第一步：定义数据分配级别）

第二步：分配分类级别（第二步：记录信息资产）

第三步：应用适当安全标记

第四步：定期进行分类评审

第五步：信息分类解除

带外令牌 类似于短信验证码，（带外，独立于通道外的另一条通道）

秘密令牌 银行的口令卡，密保卡

一次性密码设备 同步或异步令牌

加密设备 U盾

查询令牌 查询信息的令牌

预登记令牌 先登录的令牌

什么类型的访问控制策略？

技术 -------- 生物识别

逻辑 -------- 受限用户界面

管理 -------- 数据标签分类

物理 -------- RFID卡

测试的种类

回归测试——修改了旧代码后，重新进行测试以确认修改没有引入新的错误或导致其他代码产生错误。

结构测试——又称白盒测试，测试者全面了解程序内部逻辑结构、对所有逻辑路径进行测试。

非功能测试——所有其他方面的测试，包括性能、负载、可靠性等（关键词包括，可靠性、兼容性）

功能测试——又称黑盒测试，涉及了软件在功能上正反两面的测试（关键词包括，标准化、安全性）

火的分类：

A 类 普通易燃物

B 类 液态易燃物

C 类 电子物品

D类 金属物品

软件安全工程中制定的黑盒测试计划，用于衡量系统对不正确、非法输入或非预期的操作错误等情况的反应

等价类分析 ------- 选择不属于已知分类的一个输入

边界值分析 ------- 选择超过有效值域边界外的输入

决策表分析 ------- 选择输入值无效的组合

基于状态分析 ------- 选择对于每种已知的条件，选择非预期的输入

介质销毁从最佳到最差

物理销毁》消磁》复写》格式化

销毁》净化》清除》消除》删除

工控拖图

内网： 历史数据、工作站

DMZ : 应用服务器、控制区域

工控区： 人机界面

误拒绝率(FRR) 1类错误

误接受率(FAR) 2类错误

唯⼀性 ------ identity 标识

有效性(validation)《可以翻译成验证》 ------ Authentication 认证

控制 ------- authorization 授权

了解、执行、计划软件开发的初始 BSIMM

认证 ISIS（信息安全管理体系）系统 ISO27001

评价目标软件的安全保护等级 ISO15408

BSIMM，将每一类安全措施分成三级，在每⼀级中又包含当前级别应当实现的安全目标，并指出了与之相对应的具体安全活动。根据这种分级策略以及相应的可鉴别的分步实现目标，形成了整个 BSIMM 的成熟度模型。

ISO27001，信息安全管理体系要求。

ISO15408， Common Criteria V2.1，CC通用准则， CC是信息技术安全性评估标准，用来评估信息系统、信息产品的安全性。 CC 标准的评估分为两个方面：安全功能需求和安全保证需求。

SOC3， Service Organization Controls， SOC3 是一个一般用途的报告，只包括一个审计师的意见，即是否达到了服务性机构控制体系鉴证的标准。 SOC3 不包括配套的细节。 SOC报告用于解决用户广泛的需求——安全、隐私和可用性等。

BCP\DRP的步骤

一，风险评估

二，业务影响分析

三，制定策略

四，开发计划

五，培训测试

六，维护