* **假如你是单位WEB服务器管理员，试述你会采取哪些主要措施来保障WEB服务器安全。**

（1） 访问控制（IP地址限制、Windows帐户、请求资源的Web权限、资源的NTFS权限）；

（2） 用虚拟目录隐藏真实的网站结构；

（3） 设置基于SSL的加密和证书服务，以保证传输安全；

（4） 完善定期审核机制；

（5） 安装防火墙及杀毒软件；

（6） 及时安装操作系统补丁，减少操作系统漏洞等等。

* **试编写一个简单的口令管理策略。**

（1）所有活动账号都必须有口令保护。

（2）生成账号时，系统管理员应分配给合法用户一个唯一的口令，用户在第一次登录时应该更改口令。

（3）口令必须至少要含有8个字符。

（4）口令必须同时含有字母和非字母字符。

（5）必须定期用监控工具检查口令的强度和长度是否合格。

（6）口令不能和用户名或者登录名相同。

（7）口令必须至少60天更改一次。

* **假如你是一个网络管理员，请说明你会采取哪些措施来构建网络安全体系，这些措施各有什么作用。**

（1） 保证物理安全，将重要设备放入专门房间，保持良好环境，有专入制度。

（2） 在网关出口使用防火墙，如果对网络安全要求较高，可以使用状态检测型防火墙，如果对速度要求高可以使用硬件防火墙。

（3） 在防火墙后面使用入侵检测系统IDS，与防火墙配合使用，以加强内网安全。

（4） 做好操作系统、数据库系统、应用软件及时升级维护打补丁，消除漏洞；

（5） 做好数据备份，保障数据安全；

（6） 使用正版杀毒软件并及时升级；

（7） 对外通信采用IPSec或SSL等安全协议和技术，保障通信安全；

（8） 为系统和用户设置安全口令及权限，做好访问控制，保障系统使用安全；

（9） 建立完善的安全管理制度、审计制度、建立应急响应机构和机制；

（10） 做好内部安全监管、安全培训等。

* **试论述目前造成计算机网络不安全的原因是什么?可采取哪些相应的安全措施？**

不安全原因1.网络自身的特性2.网络技术的开放3．网络协议的漏洞4. 通信系统和信息系统的自身缺陷5.系统"后门”6.黑客及病毒等恶意程序的攻击。

措施:制定安全策略：如采用什么样的安全保障体系、确定网络资源职责划分、制定使用规则、制定日常维护规程、确定在遇到安全问题时采取的措施；采取加密、数字签名、访问控制、数据完整性、鉴别、业务填充、路由控制、可信第三方证书等机制。具体技术措施如：1）设置IP限制，屏蔽有威胁的IP地址2）设置身份验证，确保只有合法用户才能访问授权范围内的资源3）设置资源的WEB权限4）设置文件或目录的NTFS权限5）用虚拟目录隐藏真实的网站结构6）设置基于SSL的加密和证书服务，保证传输安全7）完善定期审核机制8）安装防火墙软件9）安装杀毒软件10）及时安装操作系统补丁，减少操作系统漏洞.

* **分析讨论信息系统所面临的安全威胁（至少5种）。**

（1） 软硬件故障：由于设备硬件故障、通信链接中断、信息系统或软件Bug导致对业务、高效稳定运行的影响。

（2） 物理环境威胁：断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害。

（3） 无作为或操作失误：由于应该执行而没有执行相应的操作，或无意的执行了错误的操作，对系统造成影响。

（4） 管理不到位：安全管理无法落实，不到位，造成安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行。

（5） 恶意代码和病毒：具有自我复制、自我传播能力，对信息系统构成破坏的程序代码。

（6） 越权或滥用：通过采用一些，超越自己的权限访问了本来无权访问的资源；或者滥用自己的职权，做出破坏信息系统的行为。

（7） 黑客攻击技术：利用黑客工具和技术，例如，侦察、密码猜测攻击、缓冲区溢出攻击、安装后门、嗅探、伪造和欺骗、拒绝服务攻击等手段对信息系统进行攻击和入侵。

（8） 物理攻击：物理接触、物理破坏、盗窃

* **请利用加密技术设计一套机制，用于实现商品的真伪查询。**

系统产生一随机数并存储此数，然后对其加密，再将密文贴在商品上。当客户购买到此件商品并拨打电话查询时，系统将客户输入的编码(即密文)解密，并将所得的明文与存储在系统中的明文比较，若匹配则提示客户商品是真货，并从系统中删了此明文；若不匹配则提示客户商品是假货。

* **请利用认证技术设计一套机制，用于防止电脑彩票伪造问题。**

首先，系统给彩票编好码，习惯称之为条形码；然后，将条形码通过Hash运算，得到相应的消息摘要；接着，对消息摘要进行加密，得到相应密文；最后，系统将条形码与密文绑定在一起并存储，若需要查询时只要查看条形码与密文是否相关联即可。这样，即可实现电脑彩票防伪，因为伪造者是无法伪造密文的。

* **请说明数字签名的主要流程。**

(1) 采用Hash算法对原始报文进行运算，得到一个固定长度的消息摘要(Message Digest)，消息摘要具有单向性、散列性和无碰撞性。

(2) 发送方用目己的私有密钥对摘要进行加密来形成数字签名。

(3) 这个数字签名将作为报文的附件和报文一起发送给接收方。

(4) 接收方首先对接收到的原始报文用同样的算法计算出新的报文摘要，再用发送方的公开密钥对报文附件的数字签名进行解密，比较两个报文摘要，如果值相同，接收方就能确认该数字签名是发送方的，否则就认为收到的报文是伪造的或者中途被篡改。

* **用户A需要通过计算机网络安全地将一份的机密文件传送给用户B，B希望A今后对该份机密文件无法抵赖，请问如何实现。**

答：假定通信双方分别为Alice和Bob，（1）双方选用一个公开密钥密码系统；（2）双方把自己的公开密钥通过PKI证书传送给对方；（3）加密方Alice将用自己的私钥加密文件，再用Bob的公钥加密文件，然后发送给Bob；（4）解密方Bob收到后用自己的私钥解密，再用Alice的公钥解密，就可以得到原机密文件。

* **简述公钥密码体制的基本思想。**

答：①公钥密码体制的基本思想是把密钥分成两个部分：公开密钥和私有密钥（简称公钥和私钥），公钥可以向外公布，私钥则是保密的；密钥中的任何一个可以用来加密，另一个可以用来解密；公钥和私钥必须配对使用，否则不能打开加密文件；已知密码算法和密钥中的一个，求解另一个在计算上是不可行的。②相对于传统密码体制来说，公钥密码体制中的公钥可被记录在一个公共数据库里或以某种可信的方式公开发放，而私有密钥由持有者妥善地秘密保存。这样，任何人都可以通过某种公开的途径获得一个用户的公开密要，然后进行保密通信，而解密者只能是知道私钥的密钥持有者，该体制简化了密钥的分配与分发；同时因为公钥密码体制密钥的非对称性以及私钥只能由持有者一个人私人持有的特性，使得公钥密码体制不仅能像传统密码体制那样用于消息加密，实现秘密通信，还可以广泛应用于数字签名、认证等领域。

* **高级持续性威胁APT攻击案例分析：**

①对谷歌等公司的激光攻击事件。

②对伊朗核设施的攻击事件。

③对韩国农协银行的攻击事件。

* **包过滤技术的局限**

1. 定义包过滤路由器，可能是一项复杂的工作。因为网络管理员需要详细地了解Internet（因特网）的各种服务、包头格式以及希望在每个域查找的特定的值。
2. 路由器信息包的吞吐量，随包过滤路由器数量的增加而减少。
3. 不能彻底防止地址欺骗。大多数包过滤路由器都是基于“源IP地址、目的IP地址”进行过滤的，而IP地址的伪造，是很容易、很普遍的。
4. 一些应用协议不适合于数据包过滤。即使是完美的数据包过滤，也会发现一些协议并不适合于经由数据包过滤安全保护。如RPC（远程过程调用）、X- Window和FTP（文件传输协议）。
5. 正常的过滤路由器无法执行某些安全策略。例如，数据包说它们来自什么主机，而不是什么用户，因此，我们不能强行限制特殊的用户。
6. 一些包过滤路由器不提供任何日志能力，直到闯入发生后，危险的封包才可能检测出来。

* **军事作战中，A需要通过计算机网络给B发送大量资料，A应该如何和B进行安全的信息传送，请说明具体步骤**

在军事作战中确保大量资料的安全传送至关重要。以下是确保安全传送的具体步骤：

数据加密：使用强加密算法（例如AES）对资料进行加密。这确保即使数据被截获，也无法被未经授权的人读取。

建立安全通道：利用安全协议（如SSL或TLS）建立安全的通信通道。这种通道保护数据在传输过程中免受窃听或篡改。

强制访问控制：实施强制访问控制模型，为数据设定明确的访问权限，确保只有授权的用户才能够访问和接收数据。

数字签名：对数据进行数字签名以验证数据的完整性和来源。这确保接收方能够确认数据未被篡改，并验证发送方的身份。

物理安全措施：除了网络安全措施外，确保在物理上保护计算机设备和网络设施，防止未经授权的人员接触到这些设备。

分段传输与重组：将大量资料分割成小块，并通过安全通道单独传输，最后在接收端重组。这有助于降低传输过程中的风险。

实时监控和审计：在传输过程中实时监控数据流，记录访问记录和操作路径，及时发现异常行为或攻击。

安全性审查和更新：定期对安全措施进行审查和更新，确保与最新威胁和需求保持同步，及时调整和改进安全措施。

* **一家公司，只使用了防火墙安全技术，请说服主管外加一个入侵检测技术。**

当谈到网络安全时，防火墙是保护系统免受未经授权访问的重要工具，但它并不能完全保证网络免受所有威胁。加入入侵检测技术可以提供额外的安全层面，让我为您列举几点：

实时威胁检测：入侵检测系统能够监控网络流量和系统活动，及时发现异常行为或潜在攻击，迅速做出反应。这种实时检测可以大大降低潜在攻击造成的损害。

综合防御：单独依赖防火墙可能无法完全拦截所有攻击。入侵检测技术可以通过分析多种数据源，识别新型威胁和攻击模式，提供更全面的安全保护。

合规性要求：许多行业和法规要求公司采取特定的安全措施来保护数据和网络。入侵检测技术常常是符合这些合规性要求的重要手段之一。

攻击后分析：如果出现了安全漏洞或者遭受攻击，入侵检测系统可以帮助公司进行事后分析，找出攻击源头和漏洞，从而改善安全策略，避免未来类似事件的发生。

增强安全意识：引入入侵检测技术可以提高公司对安全威胁的认识和了解，促进员工更积极地参与安全培训和实践，从而加强整体安全文化。

将入侵检测技术与防火墙结合使用可以建立更强大的安全防线，提高对抗各种安全威胁的能力，确保公司网络和数据的安全。

* **举3个例，说明在日常社交网络平台中容易出现的信息安全问题，并给予改进建议。**

**个人隐私泄露：**

问题： 用户可能过度分享个人信息，如生日、地址、电话号码等，导致隐私泄露。

建议： 用户应该谨慎分享个人信息，并定期审查和更新隐私设置，限制谁可以看到自己的信息。

**恶意链接和欺诈活动：**

问题： 用户可能受到欺诈性链接或信息欺诈的威胁，如虚假广告、诱导点击等。

建议： 警惕点击不明链接，安装反欺诈软件，对于可疑信息保持警惕，并报告可疑行为给平台。

**账号被盗：**

问题： 弱密码或不安全的登录方式可能导致账号被盗。

建议： 使用强密码并定期更换，启用两步验证，避免使用相同的密码在多个平台上，定期审查登录活动。

**虚假信息和网络欺凌：**

问题： 虚假信息、恶意评论、网络欺凌等可能伤害用户感情和声誉。

建议： 确保对社交平台上的信息进行验证和审查，避免敏感话题，及时举报和屏蔽恶意行为。

**数据隐私问题：**

问题： 平台可能收集和分享用户的个人数据，存在隐私泄露风险。

建议： 定期审查隐私政策，了解平台对数据的使用和分享方式，控制个人数据的共享范围。

* **企业内部员工在公司网络上访问敏感数据时，可能存在哪些安全风险？列举并提出相应的安全措施和建议**

未授权访问： 员工可能在未经授权的情况下访问敏感数据，例如使用其他员工的凭证或绕过权限。

安全措施： 实施强制访问控制（MAC）和基于角色的访问控制（RBAC），限制员工仅能访问其职责所需的数据；启用身份验证和严格的账户管理。

数据泄露： 员工可能意外或故意泄露敏感信息，例如将数据发送到错误的收件人或通过不安全的通信渠道传输数据。

安全措施： 加强员工的安全意识培训，教育他们识别敏感信息并正确处理；实施数据分类和加密，限制敏感信息的传输方式。

内部威胁： 内部员工可能有恶意行为，例如窃取数据、篡改信息或故意破坏系统。

安全措施： 实施行为监控和异常检测系统，定期审计员工访问记录；建立内部报告机制，让员工能够匿名举报可疑行为。

弱密码和凭证共享： 使用弱密码或共享凭证可能导致未经授权的访问。

安全措施： 强制员工使用复杂密码，并定期更改；启用多因素身份验证（MFA）以增强账户安全性。

社会工程攻击： 员工可能成为社会工程攻击的目标，被诱骗提供凭证或敏感信息。

安全措施： 提高员工的安全意识，教育他们如何识别和应对社会工程攻击；建立流程，确保敏感信息只在特定安全环境中共享。

* **一个政府部门需要将机密文件传输给另一个部门，如何确保文件在传输过程中的安全性？详细描述具体步骤和技术手段。**

加密文件：使用强加密算法（如AES）对机密文件进行加密。确保只有授权人员能够解密文件。

建立安全通道：使用安全协议（如SSL/TLS）建立加密的安全通道，保护数据在传输过程中的隐私和完整性。

使用安全传输协议：选择安全的文件传输协议，如SFTP（Secure File Transfer Protocol）或FTPS（FTP over SSL/TLS），以确保数据在传输时受到保护。

数字签名验证：对机密文件进行数字签名，并确保接收方可以验证文件的完整性和来源。

访问控制和权限设置：设定适当的访问控制和权限，确保只有授权人员能够访问和下载这些文件。

分割和加密传输：将大文件分割成小块，然后分别加密和传输，减少单个文件传输的风险，同时增加数据安全性。

双因素身份验证：在文件传输的过程中，要求双方进行身份验证，使用多因素身份验证（如用户名密码配合短信验证码或硬件令牌）确保身份的真实性。

实时监控和审计：在传输过程中实时监控数据流，记录传输活动和访问日志，及时发现异常行为。

端到端的安全性：确保整个传输链路的每个环节都是安全可信的，从发送方到接收方，每个环节都需要严格控制和保护。

定期审查和更新：定期审查安全策略和技术措施，确保与最新的安全标准和威胁情报保持一致，并不断优化安全性。

* **一家银行的ATM系统可能面临哪些安全挑战？提出解决方案以保护ATM系统免受潜在威胁。**

卡片复制和欺诈： 黑客可能尝试复制银行卡信息，制作伪造卡片，并通过ATM系统进行欺诈性取款。

解决方案： 使用EMV芯片技术替代磁条卡，采用动态加密和验证，增强卡片的安全性；实施欺诈检测系统，监控异常取款行为。

恶意软件攻击： 针对ATM系统的恶意软件可能导致信息窃取、卡号盗取或恶意控制ATM机。

解决方案： 定期更新ATM系统软件和操作系统，安装最新的安全补丁；使用防病毒软件和行为检测系统进行实时监控和防御。

物理攻击和钓鱼： 黑客可能尝试物理攻击ATM机，例如使用假面板或钓鱼设备窃取卡片信息或窃取现金。

解决方案： 安装物理安全设备，如监控摄像头和钞箱破坏检测器；对ATM机进行定期巡检和维护，防止物理攻击。

网络攻击和数据泄露： 针对ATM系统的网络攻击可能导致数据泄露和服务中断。

解决方案： 建立强固的防火墙和入侵检测系统，实施网络分段和加密通信，保护ATM系统免受网络攻击。

未经授权的访问和内部威胁： 内部员工或授权者可能滥用权限，窃取客户信息或篡改ATM系统。

解决方案： 实施严格的访问控制和权限管理，定期审计员工访问记录，确保仅授权人员能够访问敏感数据。

* **一家跨国公司在不同地区有分支机构，如何确保公司内部通信的安全性和保密性？列出解决方案。**

加密通信：使用端到端加密的通信工具，如加密邮件服务、安全即时通讯应用程序或VPN（虚拟专用网络），确保通信内容在传输过程中得到加密。

严格的访问控制：建立基于角色的访问控制，限制员工只能访问其需要的信息和资源，确保敏感信息仅对有权访问者可见。

使用安全的通信协议：鼓励或强制使用安全的通信协议，如TLS/SSL，确保数据在传输时得到保护。

安全培训和意识提升：为员工提供安全意识培训，教育他们识别和应对网络钓鱼、恶意软件等安全威胁，确保他们在通信中遵循最佳安全实践。

加强设备和网络安全：在各分支机构部署防火墙、入侵检测系统和反病毒软件，确保网络和设备安全；同时定期进行安全审计和漏洞扫描。

加密存储和备份：对敏感数据进行加密存储，并定期备份数据，以防止数据丢失或泄露。

多重身份验证：强制启用多因素身份验证（MFA）来保护账户安全，确保只有授权人员可以访问敏感信息。

严格审查和监控：对公司内部通信进行严格的监控和审计，记录访问和通信日志，及时发现异常行为和潜在的安全风险。

合规性和法律规定：遵守各地区的合规性要求和隐私法律规定，确保公司内部通信符合当地法律法规。

安全文化建设：建立和促进安全文化，使员工意识到安全是每个人的责任，并鼓励报告安全漏洞和问题。

* **一所学校的学生使用公共Wi-Fi上网，可能遇到的安全风险是什么？给予学生使用公共Wi-Fi时的安全建议。**

**安全风险：**

窃听和数据泄露： 公共Wi-Fi网络可能存在安全漏洞，黑客可以窃听数据流量，导致个人信息泄露。

恶意热点： 黑客可能设立假的Wi-Fi热点，冒充公共网络，吸引用户连接并窃取信息。

恶意软件攻击： 学生可能受到恶意软件的攻击，如间谍软件或恶意代码，导致设备感染病毒或个人信息泄露。

**安全建议：**

使用加密网络： 尽量连接加密的Wi-Fi网络，如WPA2/WPA3加密，以确保数据在传输时被加密。

使用VPN： 使用虚拟专用网络（VPN），它可以加密网络流量，增强数据安全性，并避免窃听。

更新设备和应用： 确保设备和应用程序都是最新版本，以修复已知漏洞，并避免被利用。

禁用自动连接： 禁用设备上的自动连接功能，避免随意连接未知的Wi-Fi网络。

启用防火墙： 启用设备上的防火墙功能，增加对不明来源的连接的阻挡。

谨慎访问敏感网站和输入个人信息： 避免在公共Wi-Fi上访问银行账户、输入密码或其他敏感个人信息。

使用HTTPS网站： 尽可能访问使用HTTPS加密的网站，这些网站提供更高级别的安全性。

退出网络后及时断开连接： 在使用完毕后及时断开连接，避免长时间保持连接公共Wi-Fi。

开启设备锁定功能： 开启设备锁定功能（PIN码、指纹或面部识别），以保护设备在连接过程中的安全。

* 一**个小型初创企业没有专门的安全团队，如何建立基本的安全基础设施？列出切实可行的安全措施和建议。**

安全培训和意识提升：为员工提供基本的安全意识培训，教育他们识别和应对常见的网络威胁和风险。

设备安全和更新：定期更新所有设备的操作系统和应用程序，确保设备安全漏洞得到修复。

强化账户安全：强制使用强密码，并定期更改密码；启用双因素身份验证（MFA）以增强账户安全性。

备份和恢复：定期备份重要数据，并测试恢复流程，以防止数据丢失或损坏时的灾难。

网络安全基础设施：部署基本的网络安全措施，如防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）和安全网关，保护网络不受攻击。

安全更新和漏洞管理：定期检查和安装安全补丁，保持系统和应用程序处于最新状态，并实施漏洞管理策略。

访问控制和权限管理：确保对公司资源的访问控制，限制员工访问敏感信息的权限。

制定安全政策：制定适合公司规模的安全政策，包括使用政策、数据备份政策、密码政策等，确保员工遵守最佳安全实践。

监控和日志记录：部署基本的监控系统，记录网络活动和安全事件，及时发现异常行为。

外部支持和咨询：考虑与安全服务提供商或专业咨询公司合作，获得安全建议和支持，填补安全团队的缺失。