选择题

（1）常见加密算法

对称加密算法：高级加密标准（AES） 数据加密标准（DES）三重数据加密标准（3DES）
非对称加密算法：RSA 算法 椭圆曲线加密（ECC）
数据完整性算法：哈希函数（如 SHA-256）等
密钥派生函数：PBKDF2 和 bcrypt 等

（2）常见网络安全协议（应用层 网络层 邮件）

应用层：HTTPS ；FTPS；SMTPS（使用 SSL/TLS 加密电子邮件传输）；DNS，POP3, IMAP, SSH
网络层：IP(互联网协议), VPN, ARP 防护(地址解析协议),ICMP (互联网控制消息协议)
邮件：SMTP（发送邮件），POP3（接收邮件），IMAP（接收邮件）

OSI 7层网络模型	TCP/IP 4层模型	对应网络协议
应用层	应用层	TFTP、FTP、NFS、WAIS
表示层		Telent、Rlogin、SNMP、Gopher
会话层		SMTP、DNS
传输层	传输层	TCP、UDP
网络层	网际层	IP、ICMP、ARP、RARP、AKP、UUCP
数据链路层	网络接口层	FDDP、Ethernet、Arpanet、PDN、SLIP、PPP
物理层		IEEE 802.1A、IEEE 802.2到IEEE 802.11

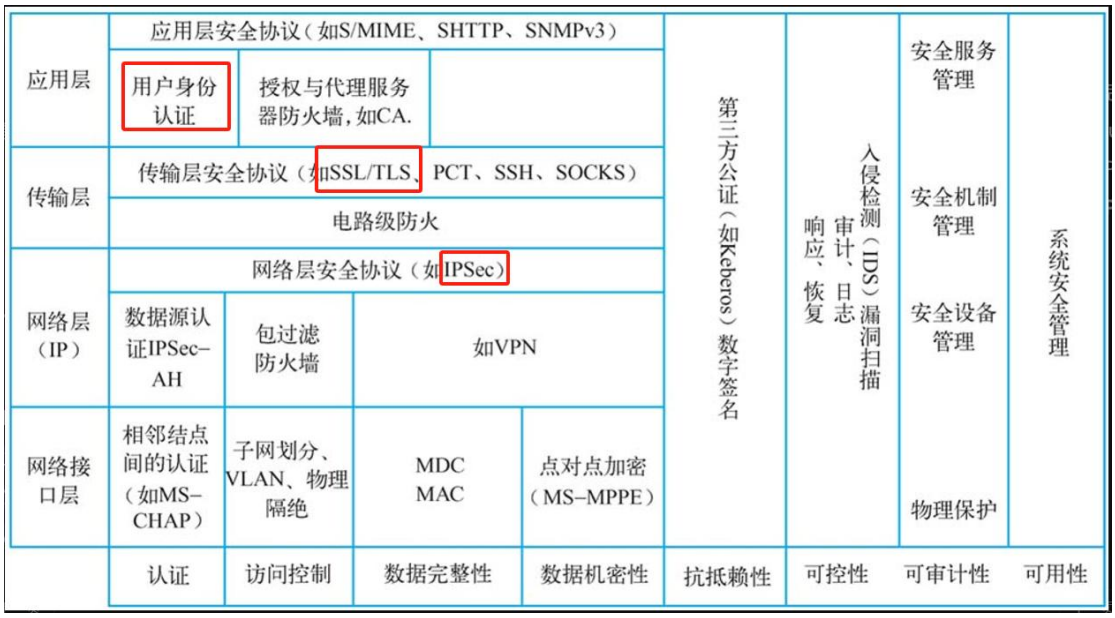
（3）区块链 原理（能干什么） 共识机制 核心思想（能做什么 不能做什么）

区块链技术的基本原理是采用去中心化的方式，通过分布式数据库来记录和存储交易数据。每个块都包含了前一个块的哈希值和自身的交易数据，形成了一个不断增长的链条。每当一个新的块被添加到链条上时，它会自动生成一个新区块，并向前一个块的哈希值添加一个随机数，以确保前一个块的数据不会被篡改。

共识机制，即制定一套规范和标准来约束各个节点的行为。目前最广泛使用的共识机制是工作量证明（Proof of Work）和权益证明（Proof of Stake），它们可以激励节点积极参与验证和记录交易数据，同时惩罚恶意行为。

核心思想：去中心化，它通过分布式数据库来存储和记录交易数据，没有任何一个节点可以控制或篡改整个链条。每个节点都有相同的权力和责任，可以参与验证和记录交易数据。这种去中心化的特点使得区块链技术具有极高的安全性和可靠性。

（4）网络不同层可以提供的安全保障



（5）信息安全的五个基本要素

保密性（Confidentiality）：防止未授权访问通过信息加密和身份认证等手段保护信息不被泄露。
完整性（Integrity）：确保信息在传输、存储和处理过程中不被未授权修改或破坏。
可用性（Availability）：保证授权用户能在需要时访问和使用信息和资源，即系统的正常运行。
可控性（Controllability）：对网络系统和信息传输的控制能力，保障信息的在规定范围内运行。
不可否认性（Non-repudiation）：确保参与者在通信过程中的行为可被验证，以防止否认或抵赖。

（6）网络加密的常用方法

分为数据传输加密和数据存储加密

数据传输加密包含：**链路加密 结点点对点加密 端对端加密**
数据存储加密包含：**利用系统本身的加密功能加密 密码加密法 通过密钥加密**

（7）零日漏洞：

零日漏洞（zero-day）又叫零时差攻击，是指**被发现后立即被恶意利用的安全漏洞**。通俗地讲，即安全补丁与瑕疵曝光的同一日内，相关的恶意程序就出现。这种攻击往往具有很大的突发性与破坏性。

（8）保护数据完整性的技术

（9）保护数据隐私的技术 （数据处理过程中，有无敏感信息等）

1）数据发布匿名保护技术。是对大数据中结构化数据实现隐私保护的核心关键与基本技术手段。能够很好地解决静态和一次发布的数据隐私保护问题。

2）社交网络匿名保护技术。包括两部分：一是匿名用户标识与属性，在数据发布时隐藏用户标志与属性信息；二是匿名用户间的关系，在数据发布时隐藏用户之间的关系。

3）数据水印技术。是指将标识信息以难以察觉的方式嵌入在数据载体内部，且不影响其使用方法，多见于多媒体数据版权保护，也有针对数据库和文本文件的水印方案。

4）风险自适应的访问控制。是针对在大数据场景中，安全管理员可能缺乏足够的专业知识，无法准确地为用户指定其可以访问的数据的情况。

5）数据溯源技术。目标是帮助人们确定数据仓库中各项数据的来源，也可用于文件的溯源与恢复，基本方法是标记法，比如通过对数据进行标记来记录数据在数据仓库中的查询与传播历史。

（10）关键词解释：

缓冲区溢出攻击：缓冲区溢出攻击是指攻击者通过向程序输入超出预期大小的数据，导致程序内存缓冲区溢出，溢出的数据覆盖在合法数据上。这可能允许攻击者执行任意代码、崩溃程序或提权，以取得对系统的更高权限。

拒绝服务攻击（DoS）：拒绝服务攻击是一种通过消耗资源使目标系统或网络瘫痪的攻击。攻击者通常通过发送大量伪造或恶意请求，使服务器无法响应正常用户的请求，从而造成服务中断的情况，目的是拒绝合法用户访问服务。

（3）驻留在多个网络设备上的程序在短时间内产生大量的请求信息冲击某 Web 服务器，导致该服务器不堪重负，无法正常响应其他合法用户的请求，这属于（　　）。

A．上网冲浪　　B．中间人攻击　　C．DDoS 攻击　　D．MAC 攻击

非授权访问：非授权访问是指个人或实体在未经适当许可的情况下，试图访问计算机系统或文件数据等。这类攻击常常利用系统漏洞或窃取凭据进行，可能导致敏感信息泄露、数据篡改或破坏，有时是其他更复杂攻击的前奏。

字典攻击：字典攻击是一种密码破解技术，攻击者使用预先准备好的包含常见密码的字典文件，依次尝试以找到正确的用户密码。这种攻击方法利用了许多人使用简单或预测性密码的习惯，以较高效的方式进行密码破解。

网络监听: 网络监听是一种被动攻击技术，其中攻击者在未经授权的情况下，使用网络嗅探工具捕获和分析网络流量。其目的是获取敏感信息，如登录凭据、电子邮件内容及其他通信数据

端口扫描： 端口扫描攻击是指攻击者通过自动化工具，对目标网络中的主机进行大规模的端口扫描，以识别哪些端口处于开放状态，从而推测出哪些服务正在运行，进而寻找可能的漏洞或弱点，为后续的攻击行动做准备。

木马：木马是一种恶意软件，伪装成合法软件以诱骗用户下载和运行。一旦被执行，木马会在系统中创建后门，允许攻击者远程控制受感染的设备，窃取敏感信息、安装更多恶意软件，或者进行其他恶意活动。

病毒：病毒是一段能够感染其他可执行文件或文档的恶意代码。当宿主文件被执行时，病毒会自我复制并传播到其他文件。病毒通常会对系统造成损害，例如删除文件、破坏数据或者降低系统性能。

蠕虫：蠕虫是一种独立的恶意软件，能够自我复制并通过网络传播，无需附着在其他程序上。蠕虫的传播速度更快，它们通常消耗网络带宽和系统资源，导致性能下降，或造成其它破坏。

（11）SDN 软件定义网络

核心原理： 将网络设备的控制平面和数据平面分离，从而使网络管理更加灵活、集中和可编程。
南向接口：连接 SDN 控制器和**网络设备**，用于向网络设备下发控制和管理指令。
北向接口：连接 SDN 控制器和**应用程序**，使应用能获取网络信息和发送配置请求。

（12）零信任模型

零信任模型是一种网络安全模型，它假定网络内的所有用户、设备和数据都不可信，无论其位置或身份如何。它强制执行对所有访问请求进行持续验证，**即使是在内部网络中也是如此。**
核心思想是 “**从不信任，始终验证**”

（13）蜜罐网络

蜜罐网络技术是一种网络安全策略，它通过设置虚假的计算机系统口、网络服务或数据，**吸引攻击者对这些假目标发起攻击**，从而暴露他们的工具、技术和战术。

（14）密码攻击方式

暴力破解：尝试所有可能的字符组合来猜测密码。
字典攻击：使用预先准备好的常用密码列表来进行尝试。
彩虹表攻击：利用预计算的哈希表来反向查找密码。
社会工程：通过操纵或欺骗用户披露其密码。
网络钓鱼：欺骗用户输入密码到虚假网站或邮件中。
键盘记录器：通过记录用户的键盘输入来获取密码。
中间人攻击：拦截和读取用户与系统之间的通信。

（15）IP 地址欺诈

IP 地址欺诈是一种网络攻击技术，攻击者通过伪造其计算机或网络设备的 IP 地址，试图假装成另一台设备以达到某些目的。

（16）数据备份方式-有

数据备份是将整个数据库复制到另一个磁盘进行保存的过程。当数据库遭到破坏时，可将转存的备份重新恢复并更新事务。数据备份可分为静态备份和动态备份两种。静态备份要求一切事务必须在静态备份前结束，新的事务必须在备份结束后开始，即在备份期间不允许对数据库进行存取或修改等操作。动态备份对数据库中数据的操作无严格限制。

数据备份可以考虑**完全备份（备份）与增量备份（备份）**两种方式。

完全备份是指每次**存储全部数据库**的内容。

增量备份是指每次**只备份上一次备份后更新过**的内容。

判断题

错的比对的多

简答题

1. 黑客攻击方式和流程

（1）隐藏 IP：通过使用代理服务器或者利用入侵傀儡机作为跳板来隐藏自己的真实 IP 地址，避免被追溯。
（2）踩点扫描：利用各种工具扫描目标的网络状态，包括端口扫描、漏洞扫描等，以寻找攻击切入点。
（3）获取控制权：即想方设法获得管理权限，目的是通过网络登录到远程计算机上，对其进行控制，达到攻击目的。
（4）种植后门：利用程序漏洞进入系统后安装后门程序，以便于以后可以不不被察觉地再次进入系统。
（5）隐身退出：黑客入侵完毕后会及时清除登录日志和其他相关地系统日志，达到隐身退出的效果。

2. VPN 定义与作用

VPN（虚拟专用网络）是利用 internet 等公共网络的基础设施，通过**隧道技术**，为用户提供的与专用网络具有相同通信功能的**安全数据通道**。

其主要作用是**隐藏用户的真实 IP 地址，与服务器通信时确保数据传输的安全性，保护用户信息免受黑客攻击。**同时，VPN 可以绕过地理位置限制访问被封锁的网站或服务。
实现技术：
1）隧道技术。它是 VPN 的核心技术，是一种隐式传输数据的方法。
2）加解密技术。常用的信息加密体系主要包括，非对称加密和对称加密两种。
3）密钥管理技术
4）身份认证技术

3. 网络中的不同层的安全

物理层安全关注对物理设备的保护；
数据链路层安全通过协议确保节点之间的数据传输安全；
网络层通过防火墙和 IP 过滤保护数据包；
传输层利用 SSL/TLS 加密数据；
而应用层通过身份认证、访问控制和数据加密保护具体应用。

<table>
<tr><td rowspan="2">应用层</td><td colspan="4">应用层安全协议（如S/MIME、SHTTP、SNMPv3）</td><td rowspan="5">第三方公证（如Keberos）数字签名</td><td rowspan="5">入侵检测（IDS）漏洞扫描
审计、日志
响应、恢复</td><td rowspan="5">安全服务管理
安全机制管理
安全设备管理
物理保护</td><td rowspan="5">系统安全管理</td></tr>
<tr><td>用户身份认证</td><td>授权与代理服务器防火墙，如CA.</td><td colspan="2"></td></tr>
<tr><td rowspan="2">传输层</td><td colspan="4">传输层安全协议（如SSL/TLS、PCT、SSH、SOCKS）</td></tr>
<tr><td colspan="4">电路级防火</td></tr>
<tr><td rowspan="2">网络层（IP）</td><td colspan="4">网络层安全协议（如IPSec）</td></tr>
<tr><td>数据源认证IPSec-AH</td><td>包过滤防火墙</td><td colspan="2">如VPN</td></tr>
<tr><td>网络接口层</td><td>相邻结点间的认证（如MS-CHAP）</td><td>子网划分、VLAN、物理隔绝</td><td>MDC
MAC</td><td>点对点加密（MS-MPPE）</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>认证</td><td>访问控制</td><td>数据完整性</td><td>数据机密性</td><td>抗抵赖性</td><td>可控性</td><td>可审计性</td><td>可用性</td></tr>
</table>

TCP/IP 网络安全技术层次体系

4. 数字签名（方式和方法 验证过程）

数字签名是一种电子认证技术，通过使用公钥加密体系确保信息传递的完整性和真实性。
原理：对消息或文件产生固定长度的短数据。将此短数据负载消息后面，以便确认发送者的身份和该信息的完整性。
生成过程：通过用发送者的私钥加密消息散列的散列值生成签名。
验证：通过接收者使用发送者的公钥解密签名获取散列值，再比对与接收到的消息的散列值是否一致。若一致，说明签名有效且消息未被篡改。
数字签名广泛应用于软件分发、金融交易和电子邮件等场合，以防止数据的伪造和篡改。

5. SQL 注入攻击（原理 预防方法）

SQL 注入攻击是一种攻击者通过在输入字段插入恶意 SQL 代码，从而操控数据库的网络攻击技术。
其**原理**是通过**不完整的输入验证**，使攻击者执行非法的 SQL 命令访问、修改或删除数据库内容或通过验证。
预防方法包括使用**参数化查询和预编译语句**以避免直接嵌入用户输入的 SQL 代码等。

6. 数字孪生（网络安全中的应用 6G 中的应用）

数字孪生是一种将物理对象数字化的表示，通过数据传感、处理和通信技术实时反映物理对象的状态和变化。
其在网络安全中的应用体现在通过**实时监控和仿真模型**，提高对复杂网络环境的可见性和管理能力，帮助快速识别和应对安全事件。
在 6G 中，数字孪生可以**优化网络资源管理和增强网络服务**，如通过仿真环境测试和部署网络安全措施，以及支持个性化的网络体验和服务优化。

7. 量子计算

量子计算基于**量子力学**原理，包括叠加、纠缠和量子隧穿等现象，叠加原理允许量子位同时表示多种状态，大大提高计算效率；纠缠使得量子位间共享信息，实现高效的信息传递。
量子计算机通过量子门操控量子位进行并行计算，使其在某些复杂计算任务中拥有极大的潜力。尤其在密码学、生物医药及其他需要高计算能力领域。

应用题

1. 某种常见攻击的应对（DDoS）网络安全设备的算力 能耗开销等综合考虑

DDoS 攻击，全称为**分布式拒绝服务攻击**，是一种恶意网络攻击，攻击者通过控制大量受感染的计算机或设备（组成一个僵尸网络），同时向目标服务器或网络发送海量请求或数据包，导致其资源耗尽或系统崩溃，从而使合法用户无法访问服务。

应对方法：
1)尽早发现网络系统存在的攻击漏洞，**及时安装系统补丁程序**。对于潜在的 DDoS 应当及时清除，以免留下后患。
2)在网络安全管理方面，要经常检查系统的物理环境，**禁止不必要的网络服务**。利用网络安全设备(如防火墙)等来加固网络的安全性。
3)**对网络安全访问进行控制和限制**，与网络服务提供商协调工作，帮助实现路由的访问控制和对带宽总量的限制。
采用高性能的网络设备。保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用知名度高、口碑好的产品。**尽量避免 NAT 的使用**

2. RSA 算法（PQ 求解 解密 加密）

（1）已知 RSA 算法中，素数 p=5，q=7，模数 n=35，公开密钥 e=5，密文 c=10，求明文。试用手工完成 RSA 公开密钥密码体制算法加密运算。

答案 5

RSA 算法由 Rivest、Shamir 和 Adleman 设计，是最著名的公钥密码算法。其安全性是建立在大数因子分解这一已知的著名数论难题的基础上，即将两个大素数相乘在计算上很容易实现，但将该乘积分解为两个大素数因子的计算量则是相当巨大的，以至于在实际计算中不能实现。RSA 既可用于加密，也可用于数字签名。RSA 算法得到了广泛应用，先进的网上银行大多采用 RSA 算法计算签名。

知识拓展
RSA 算法的安全性

【案例 5-11】 应用 RSA 算法的加/解密过程。

明文为 “HI”，操作过程如下。

1）设计密钥公钥 (e, n) 和私钥 (d, n) 。

令 p=11，q=5，取 e=3。

计算：n=p × q=55，求出 φ(n)=(p−1)(q−1) = 40。

计算：e×d mod φ(n) =1，即在与 55 互素的数中选取与 3 相乘后模是 40、余数是 1 的数，得到 d=27(私钥)。

因此：公钥对为(3,55)，私钥对为(27,55)。

2）加密。（按 1～26 的次序排列字母，则 H 为 8，I 为 9）

用公钥(3,55) 加密：E(H)=8^3 mod 55=17；E(I)=9^3 mod 55= 14（17 为 Q，14 为 N）。

密文为：QN。

3）解密。D(Q)=17^{27} mod 55=8；D(N)=14^{27} mod 55=9。

RSA 算法基于下面两个数论上的事实。

知识拓展
RSA 与图灵奖

1）已有确定一个整数是不是质数的快速概率算法。

2）尚未找到确定一个合数的质因子的快速算法。

RSA 算法的工作原理如下。

假定用户 Alice 要发送消息 m 给用户 Bob，则 RSA 算法的加/解密过程如下。

1）首先，Bob 产生两个大素数 p 和 q（p、q 是保密的）。

2）Bob 计算 n=pq 和 φ(n) =(p−1)(q−1)（φ(n)是保密的）。

3）Bob 选择一个随机数 e(0<e<φ(n))，使得(e，φ(n))=1（即 e 和 φ 互素）。

4）Bob 计算得出 d，使得 d×e mod φ(n)=1（即在与 n 互素的数中选取与 φ(n)互素的

数，可以通过欧几里得算法得出）。私钥是 d，Bob 自留且保密。

5）Bob 将（e，n）作为公钥公开。

6）Alice 通过公开信道查到 n 和 e。对 m 加密，加密 E (m) =m^e mod n。

7）Bob 收到密文 c 后，解密 D (c)=c^d mod n。

RSA 算法的优点是应用更加广泛，缺点是加密速度慢。

如果将 RSA 与 AES 结合使用，则正好可以弥补 RSA 的缺点。即 AES 用于明文加密，RSA 用于 AES 的密钥加密。由于 AES 加密速度快，适合加密较长的消息；而 RSA 可解决 AES 的密钥传输问题。

非对称密码算法与同等安全强度的对称密码算法相比，一般要慢 3 个数量级。因此，非对称密码算法一般用来加密短数据或者用作数字签名，而不是直接用在数据加密上。

RSA算法的基本原理

RSA算法的核心在于利用两个大素数的乘积来生成公钥和私钥。具体步骤如下：

1. 选择两个大素数p和q：这两个素数用于生成公钥和私钥。
2. 计算n=p*q：n是公钥和私钥的共同部分。
3. 计算欧拉函数φ(n)=(p-1)(q-1)：这是小于n且与n互质的正整数的个数。
4. 选择公钥e：e是一个小于φ(n)且与φ(n)互质的整数。
5. 计算私钥d：通过公式ed ≡ 1 mod φ(n)计算d，其中d是e的模φ(n)逆元。

公钥和私钥的生成过程

- 公钥：由e和n组成，用于加密数据。
- 私钥：由d和n组成，用于解密数据。

RSA加密和解密的过程

1. 加密过程：
   - 明文m需要被加密成密文c。
   - 使用公钥(e, n)进行加密，加密公式为 $c = m^e \mod n$。
2. 解密过程：
   - 密文c需要被解密成明文m。
   - 使用私钥(d, n)进行解密，解密公式为 $m = c^d \mod n$。