网络空间安全导论作业

目录

0925

问题一：请列举几个平时在使用计算机和网络访问时遇到的信息安全问题？以及当时的解决方案？

- 恶意软件攻击，包括病毒、木马等，它们可能会窃取个人信息或破坏数据。解决方案包括安装和及时更新防病毒软件，不打开不明电子邮件附件，定期备份数据。
- 网络钓鱼：攻击者通过伪装成可信任的实体，试图获取用户的个人信息，又如下图的 jAccount 钓鱼。解决方案包括提高警惕，不点击不明链接，不轻易透露个人信息，使用双因素认证来增加安全性。
- 拒绝服务攻击（DDoS）：攻击者通过发送大量请求使网络服务瘫痪。防御措施包括使用防火墙来识别和过滤恶意流量，以及实施流量监控和过滤机制。
- 未授权访问：未经许可的用户访问网络或系统。可以通过设置防火墙，实施访问控制列表，以及使用虚拟专用网络（VPN）来保护网络。

问题二：当前我国面临的网络空间安全的现状是怎样的?

- APT 攻击活动频繁：针对中国的 APT 攻击活动持续存在，主要针对政府、国防军工、科研等行业领域，以窃取信息和情报为主。
- DDoS 攻击、漏洞安全、恶意代码等问题依然突出：全年全网网络层的 DDoS 攻击次数达 2.51 亿次，新收录漏洞数同比基本持平，恶意程序拦截量总体趋于平缓但拦截量仍较大。
- 政策和法规不断完善：中国已经建立了以《网络安全法》为核心的网络安全法律体系，并且正在不断细化和完善相关立法，以适应网络技术的快速发展和新出现的安全挑战。
- 人工智能技术在网络安全中的应用：AI 技术正在被广泛应用于网络安全领域，包括威胁检测、自动化安全防护等，但同时也带来了新的挑战和风险。
- 网络安全企业的出海战略：面对国内市场的激烈竞争，越来越多的中国网络安全企业开始拓展海外市场，寻求新的增长点。
- 实战化演练需求提升：实战攻防演习成为政企用户网络安全保护的常态化工作，有效推动了政企用户增加对网络安全实战化、体系化及安全运行能力的建设投入。

问题三：为什么要研究网络空间安全?

- 研究网络空间安全事关国家安全，网络空间已成为国家战略的一部分，网络安全直接关系到国家的政治、经济、军事和社会安全。随着数字经济的发展，网络空间安全对于保护关键基础设施、商业机密和金融系统至关重要。此外，研究网络空间安全有利于维护社会稳定，网络空间的不安全因素可能会导致社会不稳定，如网络谣言、网络欺诈等。通过研究网络空间安全，可以提高对网络攻击的防御能力，减少安全事件的发生。
- 研究网络空间安全有利于个人隐私保护和应对新型威胁，网络安全技术的不断进步推动了加密技术、安全协议等相关技术和产品的发展的同时，新的网络威胁也在不断出现，如人工智能被用于网络攻击，需要不断研究和应对。
- 网络空间安全的研究有助于完善相关法律法规，为网络行为提供法律依据。
- 网络空间安全是全球性问题，需要国际间的合作与交流，共同应对跨国网络犯罪。
- 网络空间安全领域的研究有助于培养专业人才，满足社会对网络安全专家的需求。

1009

问题一：什么是网络空间？为什么网络空间存在严峻的信息安全问题?

- 网络空间是信息时代人们赖以生存的信息环境，是所有信息系统的集合。

- 网络空间存在严峻的信息安全问题，主要是因为网络技术的广泛应用和数据价值的上升导致了安全威胁的增加。随着互联网的普及，网络黑客、电信网络诈骗等犯罪问题频发，技术进步使得网络诈骗手法不断翻新。同时，网络空间与物理空间、社会空间的逐步融合，使得攻击武器和攻击方式复杂多样，攻击组织经常会利用跨网跨域的手段实施渗透 。此外，关键信息基础设施的攻击活动一旦成功，将极大影响相关行业的正常运行，甚至威胁国家安全。

问题二：网络空间安全学科的主要研究方向及内容是什么?

- 密码学：对称密码；公钥密码；哈希函数；密码协议；新型密码如生物密码、量子密码、混沌密码等；密码管理；密码应用。
- 网络安全：网络安全威胁；通信安全；协议安全；网络防护；人侵检测与态势感知；应急响应与灾难恢复；可信网络；网络安全管理。
- 系统安全：系统的安全威胁；系统的设备安全；系统的硬件子系统安全；系统的软件子系统安全；访问控制；可信计算；系统安全等级保护；系统安全测评认证；应用信息系统安全。
- 内容安全：内容安全的威胁；内容的获取；内容的分析与识别；内容安全管理；信息隐藏；隐私保护；内容安全的法律保障。
- 信息对抗：通信对抗；雷达对抗；光电对抗；计算机网络对抗。

问题三：信息安全的三大定律是什么?

- 信息安全的普遍性定律：哪里有信息，哪里就有信息安全问题。
- 信息安全的中性定律：安全与方便是一对矛盾。
- 信息安全的就低性定律(木桶原理)：信息系统的安全性取决于最薄弱部分的安全性。

问题四：简述信息安全分级保护和信息安全等级保护

- 信息安全分级保护是指对信息系统按照其重要程度和涉密程度进行分级别保护的一种制度。其等级分五级：
  - 第一级：自主保护级。等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益；
  - 第二级：指导保护级。等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全；
  - 第三级：监督保护级。等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害；
  - 第四级：强制保护级。等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害；
  - 第五级：专控保护级。等级保护对象受到破坏后，会对国家安全造成特别严重损害。
- 信息系统安全等级保护的内容可分为系统定级、系统备案、建设整改、等级测评、监督检查五个方面。信息系统的运营和使用单位需要根据自身系统的实际情况，按照国家标准和技术要求，确定系

统的安全保护等级，并采取相应的管理和技术措施来保障系统安全。同时，还需要定期对安全状况进行检查和评估，确保安全措施的有效性。

- 2019 年 5 月 10 日，《信息安全技术网络安全等级保护基本要求》修订，其中标准名称、等级保护对象、安全要求、安全分类发生变化，新增安全管理中心和可信验证。

问题五：信息安全法律法规有几大类别？请举例说明？

- 国家法律法规：中华人民共和国宪法、中华人民共和国刑法、中华人民共和国国家安全法、中华人民共和国预防未成年人犯罪法、全国人大常委会关于维护互联网安全的决定、中华人民共和国电子签名法、中华人民共和国治安管理处罚法、中华人民共和国侵权责任法、中华人民共和国保守国家秘密法、全国人大常委会关于加强网络信息保护的决定、中华人民共和国网络安全法、中华人民共和国密码法。
- 行政法规：中华人民共和国计算机信息系统安全保护条例、中华人民共和国计算机信息网络国际联网管理暂行规定、商用密码管理条例、中华人民共和国电信条例、互联网信息服务管理办法、计算机软件保护条例、互联网上网服务营业场所管理条例、信息网络传播保护条例。
- 部门规范：计算机信息网络国际联网安全保护管理办法、计算机信息系统保密管理暂行规定、信息安全产品测评认证管理办法、计算机病毒防治管理办法、公用电信网间互联管理规定、电子认证服务管理办法、商用密码产品生产管理规定、互联网电子邮件服务管理办法、互联网安全保护技术措施规定、信息安全等级保护管理办法、通信网络安全防护管理办法。

1023

问题一：《中华人民共和国网络安全法》哪一年开始实施？它的实施具有什么意义？

- 《中华人民共和国网络安全法》自 2017 年开始实施，其出台具有里程碑式的意义。它是全面落实党的十八大和十八届三中、四中、五中、六中全会相关决策部署的重大举措，是我国第一部网络安全的专门性综合性立法，提出了应对网络安全挑战这一全球性问题的中国方案。立法进程的快速推进，显示了党和国家对网络安全问题的高度重视，是我国网络安全法治建设的一个重大战略契机。网络安全有法可依，信息安全行业将由合规性驱动过渡到合规性和强制性驱动并重。

问题二：根据《中华人民共和国保守国家秘密法》，什么是国家秘密？

- 国家秘密的本质特征是国家秘密必须同国家的安全和利益密切相关。
- 国家秘密的程序特征是国家秘密必须依照国家的法律、法规所规定的程序确定。

- 国家秘密的时空特征是国家秘密必须而且能够在一定时间内限定一定范围的人员知悉。

问题三：根据《中华人民共和国保守国家秘密法》，请简述有哪些违反规定的行为？

- 非法获取、持有国家秘密载体的；
- 买卖、转送或者私自销毁国家秘密载体的；
- 通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的；
- 邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的；
- 非法复制、记录、存储国家秘密的；
- 在私人交往和通信中涉及国家秘密的；
- 在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密的；
- 将涉密计算机、涉密存储设备接入互联网及其他公共信息网络的；
- 在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换的；
- 使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息的；
- 擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；
- 将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途的。

问题四：根据《中华人民共和国密码法》，我国的密码分为哪几类？分别应用于什么场景？

- 我国的密码分为核心密码、普通密码、商用密码三类。
- 核心密码专门用于保护国家最高等级的绝密信息，常见于政府、军队、外交等对国家机密安全要求极高的重要领域的通信及数据加密。
- 普通密码用于保护国家机密信息，涉及国家安全和社会稳定的部门、单位使用，比如党政军机关的内部信息系统等。
- 商用密码用于保护不属于国家秘密的信息，广泛应用于企业和公众的网络通信、电子商务、物联网、云服务、金融交易、企业内部通信、个人隐私数据加密等领域。

问题五：根据《中华人民共和国数据安全法》，国家建立数据分类分级保护制度，分类分级的主要依据是什么？

- 分类分级主要依据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。

1030

问题一：古典密码分哪些种类？哪些古典密码采用了移位代换？哪些古典密码采用了置换变换？

- 古典密码主要分为替换密码和置换密码两大类；
- 移位代换的代表有恺撒密码、维吉尼亚密码、普莱费尔密码；
- 置换变换的代表有栅栏换位、矩形换位。

问题二：为什么说一次一密在理论上安全的？一次一密在实际应用中存在什么问题？

- 密钥本身随机，而且密钥只使用一次。即使获得了上次通信的密文和密钥，攻击者仍然无法确定下次通信的真正密钥；
- 需要建立庞大的随机字母集，工作量巨大，而且存在密钥分发的问题。

问题三：简述一个保密通信系统的数学模型由哪几部分组成？

- 信源、加密器、信道、解密器、信宿。

问题四：随着新技术的发展，密码学面临哪些新的安全挑战？

- 由于大数据的数据量特别巨大，数据存在多样性，使密码算法需要处理的数据规模不断增大，使用密码技术的成本不断提高，这就要求密码算法具有高效性和很强的适应性（柔性）；
- 物联网面临着数据安全、网络安全、系统安全、隐私保护的问题，物联网对密码提出了新的挑战；
- 量子计算机加快了密钥的搜索速度，对密码学提出了挑战；
- 区块链技术对密码学的新挑战。

问题五：信息隐藏和信息保密有何本质区别？

- 信息加密所隐藏的是消息的内容，攻击者虽然知道其存在，但难以提取其中的信息；
- 而信息隐藏则是将需要保密的信息“乔装打扮”后藏匿在信息空间中的一个大且复杂的子集中，目的是使攻击者难以搜寻其所在，它所隐藏的是信息的存在形式。

问题六：Shannon 所提出的设计强密码的思想主要包含哪两个重要的变换？这些变换的作用是什么？

- Shannon 所提出的设计强密码的思想主要包含扩散和混淆。

- 扩散：将明文的统计特征尽可能地扩散到密文中，使得明文和密文之间的统计关系变得极其复杂。具体来说，实现扩散的方式是让明文中的每一位数字能够影响密文中多位的值，或者说使密文中的每一位都依赖于明文中的多位数字。
- 混淆：混淆是指使密码系统的加密过程变得复杂，以至于攻击者难以通过分析密文和密钥之间的关系来推断出密钥，即使知道加密算法也无法轻易地从密文推断出明文，主要通过替换等方式来实现。混淆的目的是增加攻击者破解密码的难度，使得即使攻击者拥有无限的计算资源，也无法有效地破解密码。

1106

问题一：密码体制从原理上可分为哪两大类？这两类密码体制在密钥的使用上有何不同?

- 密码体制从原理上可分为单钥加密体制和双钥加密体制两类。
- 单钥加密体制：文件加密和解密使用相同的密钥或相近；
- 双钥加密体制：需要公开密钥和私有密钥一对密钥。如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。

问题二：密码攻击有哪些类型？有哪些方法?

- 类型：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、选择文本攻击。
- 方法：穷举攻击法、数学攻击法、物理攻击法。

问题三：按照密码算法的类型，列举出一些目前国内外知名的密码算法。

- 序列密码（流密码）：RC4（在 SSL/TLS、IEEE 802.11 WEP 协议，以及 Microsoft Windows、Lotus Notes、Apple AOCE、Oracle Secure SQL 等系统中）；
- 分组密码：DES（三重 DES）、IDEA、RC5、RC6、CAST - 128；
- 公钥密码：RSA、Rabin、ElGamal、ECC；
- 国产密码：SSF33、SM 系列、ZUC 密码。

问题四：公钥密码系统的三种应用是什么？公钥密码系统对应的数学难题有哪些?

- 应用：加密/解密、数字签名、密钥交换；

- 对应的数学难题：大整数因子分解问题、离散对数问题 (DLP 问题)、椭圆曲线上的离散对数问题（ECDLP）。

问题五：什么是身份基密码、属性基密码和同态密码？

- 身份基公钥密码是一种公钥密码体制，有效简化了公钥基础设施中证书权威对用户证书管理带来的复杂密钥管理问题。
- 属性基公钥密码是在身份基公钥密码体制的一种扩展，将代表用户身份的字符串由一系列描述用户特征的属性所代替，在云计算、物联网等多用户环境下可以灵活地实现用户的细粒度访问控制。
- 同态密码是指支持在密文上进行特定类型运算的加密方案。同态加密允许直接对加密数据进行操作，而无需先对其进行解密，操作结果解密后与对明文进行相应操作的结果相同。这种特性在云计算、大数据处理等场景中非常有价值，例如可以在不泄露用户隐私数据的情况下，让云服务提供商对加密数据进行计算。

1113

问题一：什么是 OSI 安全体系结构？列出并简要定义安全服务和安全机制的分类，并简述安全服务与安全机制之间的关系。

- OSI 参考模型是由国际化标准组织制定的开放式通信系统互联参考模型(Open System Interconnection Reference Model， OSI/RM)，网络通信分为七层。在此基础上扩充确立的 OSI 安全体系结构包括五类安全服务和八类安全机制。
- 安全服务是增强数据处理系统和信息传递安全性的措施或服务，ISO 7498-2 中将其分为认证服务、访问控制服务、数据机密性服务、数据完整性服务和非否认服务。
- 安全机制是安全服务的实现手段，一个安全服务可由多个安全机制实现，一个安全机制也可用于实现多个安全服务。

问题二：基本的安全威胁有哪些？

- 窃听。
- 信息泄露（密码破解、数据破译等）。
- 病毒感染、木马、蠕虫等恶意代码的攻击。
- 非法使用（如缓冲区溢出攻击）。
- 完整性侵犯(通过篡改、删除和插入等破坏信息)。
- 拒绝服务（DDOS 攻击）。
- 假冒 (攻击者利用冒充手段窃取信息、入侵系统、破坏网络正常通讯或欺骗合法主机和合法用户)。

- 流量分析 (通过对网上的信息流的观察和分析推断出网上传输的有用信息，例如有无传输、传输的数量、方向和频率等)。
- 其他威胁(人员疏忽/误操作、电磁泄漏、消息重发、业务否认、截获/修改等)。

问题三：列出并简要定义被动攻击和主动攻击的分类，并简述被动攻击和主动攻击之间有何区别?

- 被动攻击：对所传输的信息进行窃听和监测。
- 主动攻击：恶意篡改数据流或伪造数据流等攻击行为。
- 区别：被动攻击难以检测但采取某些安全防护措施就可有效阻止；主动攻击易于检测但难以阻止。

问题四：网络攻击的常见形式有哪些?

- 口令窃取、欺骗攻击、陷阱和后门攻击、认证失效、协议缺陷、信息泄露、指数攻击、拒绝访问攻击。

问题五：什么是缓冲区溢出攻击？针对缓冲区溢出攻击，有什么好的防护办法?

- 缓冲区溢出攻击是通过造成缓冲区溢出并用指定地址覆盖返回地址而进入指定程序的方式来获得系统权限进而进行的攻击。
- 防护办法：在硬件和操作系统级别，采用栈随机化、栈破坏检测、数据执行保护、地址空间布局随机化、结构化异常处理程序等措施；在编程实践和代码安全方面，采用输入验证和边界检查、使用安全的编程语言、改进 C 语言函数库；在系统和网络安全措施方面，及时打补丁、使用网络安全设备，提高系统的安全性。

问题六：简述分布式拒绝服务攻击?

- 分布式拒绝服务攻击（Distributed Denial of Service， DDoS）是一种基于 DoS 攻击、但形式特殊的拒绝服务攻击，采用分布、协作的大规模攻击方式。攻击者利用大量的网络流量或请求来淹没目标服务器、服务或网络资源，使其无法正常响应合法用户的请求，攻击来自多个源头（通常是被攻击者控制的大量计算机，即“僵尸网络”或“肉鸡”），通过消耗服务器或网络资源实现“拒绝服务”目的。

问题七：什么是 P2DR 模型?

- P2DR 模型是可量化的、可由数学证明的、基于时间的安全模型，包含安全策略(Policy)、防护(Protection)、检测(Detection)和响应(Response)。安全策略是核心，防护预防安全事件，检测是静态防护转化为动态防护的关键及强制落实安全策略的工具，响应是解决安全潜在威胁的有效方

法。其基本思想是用时间尺度衡量体系能力和安全性，安全目标是增大保护时间，减少检测和响应时间。

1127

问题一：防火墙的类型有哪些？各类防火墙的特点？

- 类型：包过滤防火墙、电路级网关防火墙、应用级网关防火墙。
- 特点：包过滤防火墙利用对数据包的分析能力，在网络层根据包头信息有选择地实施允许通过或阻断，可分为动态、静态和状态检测包过滤防火墙；电路级网关工作在会话层，通常作为应用代理服务器的一部分，不允许端到端 TCP 直接连接，充当中介接收和转发请求；应用级网关防火墙对整个数据包进行检查，在应用层过滤，针对每个服务运行一个代理、逐个检查和过滤数据包，采用“强应用代理”，能自动创建必要的包过滤规则，是较安全的防火墙结构之一。

问题二：防火墙有哪些控制功能？防火墙的局限性有哪些？什么是 DMZ？

- 控制功能：有服务控制、方向控制、用户控制、行为控制四种，通过设置访问控制规则，对进出网络边界的数据流进行过滤。
- 局限性：不能防范内部人员的攻击、不能防范绕过它的连接、不能防备全新的威胁、不能防范恶意程序和病毒（数据驱动式攻击）。
- DMZ：为配置管理方便，内网中向外提供服务的服务器放在的单独网段。

问题三：什么是防火墙，为什么需要有防火墙？

- 防火墙是在两个网络之间执行访问控制策略的一个或一组安全系统，由软件和硬件组成，是实现网络安全策略的有效工具之一，位于安全与不安全网络之间，属于边界防护设备，可过滤进出网络边界的数据流，保护本地系统或网络不受基于网络的安全威胁。

问题四：什么是入侵监测系统？入侵检测方法有哪些？

- 入侵检测系统（IDS）是对网络传输进行即时监视，发现可疑传输时发出警报或采取主动反应措施的网络安全设备，通过收集和分析网络或系统关键点信息，发现违反安全策略行为和袭击迹象，但基本不具有访问控制能力，单独使用不能保护网络。
- 入侵检测方法有异常检测、误用检测和特征检测。

问题五：IPsec 提供哪些服务？IPsecVPN 有哪两种工作模式，这两种工作模式有何区别？

- IPsec 提供的服务有：机密性（加密）、数据完整性（接收方可以检验数据是否更改或篡改过）、身份验证（检验数据来源的身份）、反重播保护（检测并拒绝重播数据包）。
- IPsecVPN 两种工作模式分别是传输模式和隧道模式。传输模式保护 IP 载荷，应用于两台主机之间，保护传输层协议头，实现端到端通信安全性，要求主机支持 IPsec；隧道模式保护整个 IP 包，把源数据包封装在新包内，在隧道端点间通过公共互联网络路由。

问题六：我国的网络安全划分为哪几个安全等级？每个安全等级划分的依据是什么？

- 我国网络安全分为五个安全保护等级：
  - 第一级：用户自主保护级，受破坏会损害相关公民、法人和其他组织合法权益，但不危害国家安全、社会秩序和公共利益的一般网络。
  - 第二级：系统审计保护级，受破坏会严重损害相关公民、法人和其他组织合法权益，或危害社会秩序和公共利益，但不危害国家安全的一般网络。
  - 第三级：安全标记保护级，受破坏会特别严重损害相关公民、法人和其他组织合法权益，或严重危害社会秩序和公共利益，或危害国家安全的重要网络。
  - 第四级：结构化保护级，受破坏会特别严重危害社会秩序和公共利益，或严重危害国家安全的特别重要网络。
  - 第五级：访问验证保护级，受破坏会特别严重危害国家安全的极其重要网络。

问题七：针对工业互联网的攻击发起点有哪些？有哪些具体威胁？

- 攻击发起点：物理层、网络层和控制层。
- 具体威胁：在物理层，智能电子设备易受硬件入侵、旁路攻击和逆向工程攻击等；在网络层，通信协议可能受中间人和拒绝服务攻击等；在控制层，用户可能受钓鱼网站攻击等社交攻击，还有工控设备高危漏洞、外围设备后门、高级持续性威胁(APT)、工业网络病毒、无线技术应用的风险等。

问题八：物联网感知识别层面临哪些安全挑战？

- 物理攻击：攻击者破坏传感器等设备，或盗窃、破解终端设备获取敏感信息，非法更换传感器导致数据异常。
- 伪造或假冒攻击：利用安全漏洞获取节点身份和密码信息，假冒身份通信，进行非法或恶意行为。
- 信号泄露与干扰：拦截、篡改、伪造、重放传感网络数据和信令，导致信息错误或泄露，资源耗尽攻击耗尽终端电量。
- 隐私泄露：RFID 标签、二维码等使物联网用户易被扫描、定位和追踪。

问题九：我国网络安全事件分为哪几类以及分为哪几个级别？

- 分类：国家标准 GB/Z20986 - 2007《信息安全技术信息安全事件分类分级指南》将网络安全事件分为 7 个基本分类，包括有害程序事件、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、灾难性事件、其他网络安全事件。
- 级别：《国家网络安全事件应急预案》将网络安全事件分为 4 个级别，特别重大事件(Ⅰ级)、重大事件(Ⅱ级)、较大事件(Ⅲ级)、一般事件(Ⅳ级)，划分依据是事件对信息系统的破坏程度和社会影响大小。

问题十：计算机病毒的主要特点有哪些？计算机病毒主流检测技术有哪些？

- 主要特点：
  - 传染性：通过各种渠道扩散到更多计算机系统。
  - 隐蔽性：隐藏进程、文件等延长生命周期。
  - 寄生性：附着在正常程序中，先于正常程序执行。
  - 潜伏性：感染后长期隐藏，满足条件才发作。
  - 破坏性：对系统及应用程序产生不同程度影响。
- 主流检测技术：基于特征码的传统检测技术、基于行为的传统检测技术、基于云技术的云查杀技术、基于大数据与人工智能的查杀技术。

问题十一：按照漏洞扫描的技术执行形式的维度划分，漏洞扫描技术分为哪些？什么是原理检测和版本检测？

- 漏洞扫描技术分为：黑盒扫描(DAST)、交互式扫描(IAST)、白盒扫描(SAST)。
- 原理检测(POC 检测)：对目标机相关端口发送特殊数据包判断漏洞是否存在，由漏洞验证代码或数据判断。
- 版本检测：依照漏洞库标准，根据漏洞与系统版本关联关系检测。

1211

问题一：操作系统通常由进程管理、内存管理、外设管理、文件管理、处理器管理等子系统组成，是不是把这些子系统的安全机制实现好了，操作系统的安全目标就实现了？为什么？

- 不是。因为就算各个子系统都能够确保不泄露信息，某些子系统的相互作用也可能泄露信息。

问题二：涌现性和综合特性都是整体特性，请分析说明两者的区别?

- 综合特性：可以分解为系统组成部分的特性。
- 涌现性：不可还原（即不可分解）为系统组成部分的特性。

问题三：请对安全管理和风险的概念进行分析，以此为基础，说明在安全管理工程中为什么要遵循风险管理原则?

- 安全管理是在安全策略的指导下进行的一系列管理活动，包括标识组织资产并制定、说明和实施保护策略和流程，资产包括系统、信息、机器、建筑物、人员等。
- 风险是指某物遭受伤害或损失的可能性。
- 遵循风险管理原则可标识威胁、评估现有威胁控制措施的有效性、确定风险后果、排定风险优先级、划分风险类型并选择合适策略或响应，有助于聚焦日常管理，贯穿安全理念，明确和落实安全责任，提升系统安全性。

问题四：请说明针对数据库应用的 SQL 注入攻击的原理?

- SQL 注入攻击是攻击者把 SQL 命令插入到 Web 表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的 SQL 命令。

问题五：什么是跨站脚本攻击（XSS）？请分析说明跨站脚本攻击（XSS）威胁会给 Web 应用系统带来什么样的安全风险?

- 跨站脚本攻击（XSS）指在脚本中加入一些破坏计算机系统的指令，当用户浏览网页调用这些脚本时，系统会受到攻击。
- 安全风险包括攻击者劫持用户会话、插入恶意内容、重定向用户、使用恶意软件劫持用户浏览器、繁殖 XSS 蠕虫，甚至破坏网站、修改路由器配置信息等。

问题六：请简要说明访问网站时涉及的 cookie 是什么，它是如何泄露个人敏感信息的?

- Cookie 是浏览器与服务器交互时，由 Web 服务器建立、发送，由浏览器保存的赋值信息，是简单文本文件，约 255 个字符，占 4KB 空间，用于记录用户在网站的操作信息，后续交互时返还给服务器辅助判断用户状态。
- 其安全性问题在于包含用户 IP 地址、密码等重要信息，且服务器检索在用户硬盘进行，攻击者可修改 cookie 欺骗服务器认证，从而泄露信息。

1218

问题一：信息内容安全的主要技术有哪些?

- 内容获取：包括动态网络社区信息的深入提取、跨网络媒体内容的高性能提取、混合网络身份获取。
- 内容分析：涵盖多源网络媒体信息的数据清洗、海量非结构化信息的数据仓储域数据挖掘、多媒体群体理解技术。
- 内容网络：涉及内容网络命名攻击、内容网络缓存污染、内容网络路由攻击。

问题二：信息内容安全威胁主要有哪些?

- 信息内容面临泄露（非授权访问）、欺骗、破坏和篡夺等威胁，同时恶意用户产生传播的恶意内容也是潜在安全威胁。

问题三：典型的信息内容的获取技术有哪些？并简要说明其原理。

- 基于 Cookie 机制实现身份认证：利用 Cookie 记录用户信息辅助身份确认。
- 基于浏览器模拟的获取技术：通过模拟浏览器行为获取信息。
- 网络爬虫：按照一定规则自动抓取网页内容。
- 信息内容特征抽取与选择：从大量信息中提取关键特征进行筛选。
- 原理：从初始 URL 集合出发，进行信息获取、解析和判重等操作。

问题四：信息过滤技术有哪些分类与应用?

- 分类：
  - 根据过滤方法分类：基于内容的过滤、基于用户兴趣的过滤、协作过滤。
  - 根据操作的主动性过滤：主动过滤、被动过滤。
  - 根据过滤位置分类：信息的源头过滤、服务器和客服端过滤。
  - 根据过滤的目的分类：用户过滤、安全过滤。
- 应用：包括 Internet 搜索结果过滤、用户电子邮件过滤、浏览器过滤、专为未成年人过滤、为客户过滤等。

问题五：什么是内容中心网络？内容中心网络的架构有哪些基本组成?

- 内容中心网络(Content Centric Network,CCN)是 2009 年提出的新型下一代网络体系结构，基于内容命名，核心思想是用内容名字替代 IP 地址进行路由。
- 基本组成：

- 内容信息对象：如网页、文档等各类可访问对象。
- 命名：具有全局性和唯一性，类似 IP 地址，有分层和扁平命名方案。
- 路由：发送和接收方向 Internet 发送消息摘要和订阅兴趣。
- 缓存：每个 CCN 节点维护缓存表，缓存接收的内容消息对象。
- 应用程序编程接口：用于内容信息对象的发布和获取操作。

问题六：针对内容中心网络架构的常见攻击有哪些？简要说明每种攻击方式?

- 命名相关攻击：
  - 监视列表攻击：通过监视列表获取信息进行攻击。
  - 嗅探攻击：窃取命名相关信息。
- 路由相关攻击：
  - DDOS 攻击：用大量流量淹没路由资源。
  - 欺骗攻击：欺骗路由节点。
- 缓存相关攻击：驱逐流行内容攻击，破坏缓存机制。
- 其他攻击：
  - 假冒攻击：假冒合法节点。
  - 重放攻击：重放合法数据包进行攻击。

1225

问题一：身份认证的主要方法有哪些？并对每个方法原理进行简单描述。

- 用户名/口令认证(所知)：简单易用，无需硬件设备，但口令易泄露、易受攻击且复杂口令难记。
- 动态口令/一次性口令 OTP(所有)：基于变化的运算因子产生一次性口令，符合标准双运算因子。
- 挑战应答认证(所有)：通过一轮应答利用一次性随机数防重放攻击，基于单向密码函数或数字签名算法。
- 基于生物特征的认证(个人特征)：利用生物特征如指纹等认证，可信度高但辨别失败率高且不能挂失。
- 图灵测试：通过特定问题区分人与程序，防范暴力破解。
- 多因子认证：结合多种认证方式。

问题二：身份认证的主流标准有哪些？FIDO 认证协议的主要目的是什么？

- RADIUS：用于接入认证和计费服务，在企业信息系统接入中有应用。
- 在线快速身份认证 FIDO：使用生物特征识别技术代替口令，基于生物特征解锁加密密钥与服务器认证，实现无口令登录，包括通用身份认证框架 UAF 和通用第二因子认证协议 U2F。
- 联盟身份管理 FIM：使用户可用同一身份访问联盟企业资源，支持跨域链接，如 Oauth 系统定义相关角色，大公司多有应用。
- FIDO 认证协议的主要目的是制定无口令身份认证协议。

问题三：挑战应答认证协议为什么可以对抗重放攻击？

- 挑战应答认证协议通过一轮应答实现验证者对证明者的认证，在此过程中利用一次性随机数。当攻击者试图重放之前的认证信息时，由于一次性随机数的特性，重放的信息中的随机数与当前认证流程中的随机数必然不同，验证者能够轻易识别出这是重放攻击而拒绝认证，从而有效对抗重放攻击。

问题四：什么是联盟身份管理？

- 联盟身份管理（Federated Identity Management，FIM）是一种允许用户使用同一个身份在组成联盟的所有企业中访问相应资源的机制。它支持用户身份跨安全域链接，用户在一个域中完成认证后，无需再次独立登录，即可访问联盟内其他域的资源。例如，在一些大型企业集团或合作组织中，通过联盟身份管理，员工可以使用其在所属企业的身份凭证，便捷地访问集团内其他关联企业的特定系统和资源，大大提高了用户访问的便利性和效率，同时也有助于企业间的协同合作与信息共享。

问题五：访问控制模型有哪些？

- 自主访问控制模型（DAC）：资源拥有者能够按照自身意愿决定是否授予其他用户对其资源的访问权限。这种模型的优点是策略制定较为灵活，资源拥有者可以根据具体情况进行个性化的权限分配；然而，其缺点也较为明显，安全性相对较差，因为资源的访问权限完全取决于拥有者的主观判断，可能存在误操作或恶意授权的风险，容易导致信息泄露或非法访问。
- 强制访问控制模型（MAC）：该模型会为用户和数据分别划分安全等级，并且规定信息只能从低安全等级向高安全等级流动。其优势在于能够严格控制信息流向，保障信息的保密性和完整性；但不足之处在于权限管理的效率较低，缺乏灵活性，因为安全等级的划分相对固定，难以适应复杂多变的实际应用场景和用户需求。
- 基于角色的访问控制模型（RBAC）：通过引入角色的概念来描述访问控制策略。系统中的用户和权限都与特定角色相对应，用户通过被赋予相应角色来获得访问权限。其核心思想是将访问权限与角色紧密联系，实现了用户与权限的分离，简化了授权管理过程。例如，在一个企业的信息管理系

统中，可以设置“经理”“员工”“财务人员”等不同角色，每个角色具有特定的访问权限，当用户的职位或职责发生变化时，只需调整其对应的角色，而无需对每个具体权限进行单独修改。

问题六：虚拟化主要有哪些方式？其面临的安全威胁是什么？

- 虚拟化的方式主要包括裸金属架构、寄居架构和容器。
  - 裸金属架构：直接在硬件上安装虚拟化软件，然后在其上运行多个虚拟机。这种架构能够提供较好的性能和隔离性，但对硬件资源的要求相对较高。
  - 寄居架构：在现有的操作系统上安装虚拟化软件来创建虚拟机。其优点是安装和使用相对简便，但由于依赖于底层操作系统，可能会受到底层系统的稳定性和安全性影响。
  - 容器：利用操作系统的内核功能实现轻量级的虚拟化，多个容器可以共享同一个操作系统内核。容器具有启动速度快、资源占用少等优势，但也存在一定的安全风险，如容器之间的隔离性相对较弱。
- 面临的安全威胁：
  - 虚拟机逃逸：恶意代码可能突破虚拟机的隔离机制，访问宿主机或其他虚拟机的资源，从而导致严重的安全问题。
  - 边信道攻击：攻击者通过利用共享资源（如缓存、内存等）的隐通道来窃取信息，这种攻击方式较为隐蔽，难以检测和防范。
  - 网络隔离：在虚拟化环境中，确保不同虚拟机或容器之间的网络隔离是一个关键问题，如果网络隔离措施不完善，可能会导致信息泄露或非法访问。
  - 镜像和快照的安全：虚拟机镜像和快照可能包含敏感信息，如果没有进行适当的加密和保护，一旦被攻击者获取，可能会造成信息泄露。

问题七：简述区块链的数据结构，说明其为什么具有不可篡改的特性。

- 区块链是一种以哈希链为基础的数据结构。它通过哈希函数将每个区块中的交易信息进行哈希计算，并将前一个区块的哈希值包含在当前区块的头部，以此形成一个链式结构。每个区块中的交易信息都有对应的哈希值，并且由这些哈希值作为叶子节点生成二叉 Merkle 树，Merkle 树的根节点哈希值保存在本区块的块头部分。
- 其不可篡改的特性主要基于以下原因：若要篡改区块链中的某一条记录，首先需要修改该记录所在区块的哈希值，但由于区块头部包含了前一个区块的哈希值，所以仅仅修改一个区块的哈希值是不够的，还需要依次修改后续所有区块的哈希值，或者重新生成一条比原链更长的区块链。在实际应用中，随着区块链的不断增长和节点的广泛分布，要实现这样的篡改几乎是不可能的。一般情况下，当一个区块后面有 6 个新的区块生成时，该区块就被认为具有较高的不可篡改可信度，可以正式加入到区块链的稳定结构中。

问题八：简述人工智能对网络安全的影响。

- 人工智能对网络安全产生了多方面的影响，是一把“双刃剑”。
- 积极影响：
  - 威胁检测与防御：人工智能能够快速分析海量的网络数据，及时发现潜在的安全威胁和新出现的攻击模式。例如，通过机器学习算法对网络流量进行实时监测，可以准确识别出异常行为，如端口扫描、恶意软件传播等，并迅速采取相应的防御措施，大大提高了网络安全的响应速度和准确性。
  - 自动化防御修复：借助人工智能技术，安全系统可以实现自动化的防御和修复过程。当检测到安全漏洞或攻击时，系统能够自动执行预先设定的修复策略，如自动更新补丁、隔离受感染的设备等，减少了人工干预的时间和成本，提高了系统的安全性和稳定性。
  - 智能分析与决策：人工智能可以对复杂的安全数据进行深度分析，为安全管理人员提供有价值的决策支持。例如，通过对历史安全事件的分析和学习，预测未来可能发生的安全风险，并制定相应的预防策略，帮助企业提前做好安全防范工作。
- 消极影响：
  - 安全漏洞与攻击面扩大：人工智能技术本身也存在安全漏洞，随着其在网络安全领域的广泛应用，这些漏洞可能被攻击者利用，从而引发新的安全问题。例如，人工智能模型可能受到对抗样本攻击，导致错误的决策或预测，为攻击者提供可乘之机。
  - 人工智能辅助的网络犯罪：犯罪分子也开始利用人工智能技术来实施更加复杂和隐蔽的网络犯罪。例如，利用人工智能生成的恶意软件可以自动躲避传统的安全检测机制，增加了安全防范的难度。
  - 隐私保护挑战：人工智能在分析和处理大量数据的过程中，可能会涉及到用户的隐私信息。如果这些数据没有得到妥善的保护，可能会导致用户隐私泄露，引发严重的社会问题。
  - 伦理道德问题：人工智能在网络安全中的应用也引发了一系列伦理道德问题，如自动化决策的公正性、责任界定等。例如，当人工智能系统自动对网络攻击进行反击时，可能会误伤到无辜的用户，如何确保这种反击行为的合理性和合法性是一个亟待解决的问题。

问题九：什么是证书链？根 CA 证书由谁签发?

- 证书链是一系列用于验证实体（如网站、用户等）身份的数字证书。在这个链条中，每个证书都由上一级权威机构进行数字签名，以证明其有效性。用户的身份与所持有的公钥通过证书进行绑定，由可信任的权威机构 CA 对这种绑定关系进行数字签名认证。
- 在树型信任体系中，根 CA 证书是由根 CA 自身签发的。根 CA 作为整个信任体系的核心和基础，是整个证书链的起点和锚点。它的公钥被广泛信任，用于验证下级 CA 证书或用户证书的真实性。上级 CA 则负责为下级 CA 或者用户颁发证书，通过这种层级结构，构建起一个完整的信任体系，确保网络通信中各方身份的真实性和可靠性。例如，在常见的 SSL/TLS 证书体系中，浏览器通常会内置一些根 CA 的公钥，用于验证网站证书的有效性，从而保证用户与网站之间的安全通信。