**本课程基本概念**

根据信息安全体系要求，本课程在展开检测和防护内容时，重点关注以下基本概念：

信息安全、漏洞、PDRR、缓冲区溢出攻击、注入攻击、社会工程学、ARP欺骗

灾难备份、ISC2安全体系、访问控制、ACL、数字签名、信息摘要、DMZ

VPN隧道、隧道模式、传输模式、计算机犯罪、信息系统等级保护

**名词解释**

**堡垒（Bastion）主机**是保障生产系统安全的常用方法，是位于外围网络中的服务器，向内部和外部用户提供服务。主要包括：Web服务器，VPN服务器

**信息安全：**信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

**漏洞：**指硬件、软件或策略上存在的安全缺陷，从而使得攻击者能够在未授权的情况下访问、控制系统。

**PDRR**: PDRR(Protection,Detection,Reaction,Recovery，既防护、检测、响应、恢复)模型。

**缓冲区溢出攻击：**向缓冲区写入超过缓冲区长度的内容，造成缓冲区溢出，破坏程序的堆栈，使程序转而执行其他的可能带有攻击的指令，达到攻击的目的。

**注入攻击：**将不受信任的数据作为命令或查询的一部分发送到解析器时引发的攻击。攻击者把操作命令插入到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命令。

**跨站脚本攻击**：攻击者利用网站程序对用户输入过滤不足的漏洞，输入可以显示在页面上对其他用户造成影响的HTML代码，从而盗取用户资料、利用用户身份进行某种动作或者向访问者散播恶意代码的一种攻击方式。

**ARP欺骗：**针对以太网地址解析协议（ARP）的一种攻击技术，通过欺骗局域网内访问者PC的网关MAC地址，使访问者PC错以为攻击者更改后的MAC地址是网关的MAC，导致网络不通。

**DMZ：**安装防火墙后，网络服务器也成为内部网络的一部分，不能被网外用户直接访问。而网络服务器一般是必须向外提供服务的。

为了解决外部网络不能访问网络服务器的问题，将内网机器与网络服务器分离开，成为两个组成部分：真正的内网和DMZ区。

DMZ：是一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，外网用户可方便访问DMZ的资源。

**社会工程学：**是一种通过受害者心理弱点、本能反应、好奇心、信任、贪婪等心理缺陷进行诸如欺骗、伤害等危害手段，获得自身利益的手法。

信息系统安全“**木桶原则**”：对于一个信息系统来说，它的安全性不在于它是否采用了最新的加密算法或最先进的设备，而是由系统本身最薄弱之处，即漏洞所决定的。

**灾难备份**：利用技术、管理手段以及相关资源，确保已有的关键数据和关键业务在灾难发生后在确定的时间内可以恢复和继续运营的过程

**ISC2安全体系**: 国际信息系统安全认证组织: 1．物理屏障层：场地设备安全，含警卫，监控等；2．技术屏障层：计算机技术，网络技术，通信技术3．管理屏障层：人事，操作，设备4．法律屏障层：民法，刑法5．心理屏障层：全民国防意识

**访问控制**：在保障授权用户能获取所需资源的同时拒绝非授权用户的安全机制。

**ACL**：访问控制列表(ACL)是一种基于包过滤的访问控制技术，它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。访问控制列表被广泛地应用于路由器和三层交换机。

**数字签名**：信息发送者使用公开密钥算法技术，产生别人无法伪造的一段数字串。发送者用自己的私有密钥加密数据传给接收者，接收者用发送者的公钥解开数据后，就可以确定消息来自于谁，同时也是对发送者发送信息的真实性的一个证明。发送者对所发信息不能抵赖。

**信息摘要：**消息摘要算法的主要特征是加密过程不需要密钥，并且经过加密的数据无法被解密，目前可以被解密逆向的只有CRC32算法，只有输入相同的明文数据经过相同的消息摘要算法才能得到相同的密文。

**VPN隧道：**隧道协议利用附加的报头封装帧，附加的报头提供了路由信息，封装后的包所途经的公网的逻辑通道称为隧道。

**SSL VPN：**SSL VPN即指采用[SSL协议](https://baike.baidu.com/item/SSL%E5%8D%8F%E8%AE%AE/4602579" \t "https://baike.baidu.com/item/SSL%20VPN/_blank)来实现远程接入的一种新型VPN技术。它包括：服务器认证，客户认证、SSL链路上的[数据完整性](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%AE%8C%E6%95%B4%E6%80%A7/110071" \t "https://baike.baidu.com/item/SSL%20VPN/_blank)和SSL链路上的数据保密性。

**隧道模式**：对整个IP数据包进行加密或认证。在VPN技术中，通信时对整个IP包进行加密，使用一个新的IPSec包打包，不支持多协议，用于实现路由器、网关之间的安全通信。

**传输模式：**只对IP数据包的有效负载进行加密或认证。在VPN技术中，通信时对IP包的地址部分不作处理，仅对数据负载进行加密，用于实现端对端安全通信，即主机之间实现完整的端对端通信保护，

**计算机犯罪**：行为人通过计算机操作所实施的危害计算机信息系统（包括内存数据及程序）以及其他严重危害社会的并应当处以刑罚的行为。

**信息系统等级保护**：是对信息和信息载体按照重要性等级分级别进行保护的一种工作，有定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段。

### RSA算法要求

**要求：**掌握给定素数及公钥后，会计算私钥、对给定信息加密、对密文进行解密。

例：给定素数p=7,q=13。n=91,Fn=72

选定公钥e=5，计算得出私钥d。

de mod 72=1     5d-72k=1         找到合适的d=29

                      5d mod 72=1

给定信息m=6  
加密：6^5 mod 91=41

给定密文c=41  
解密：41^d mod 91= 41 ^29 mod 91 = 6     **de mod n=  ((d mod n) \* (e mod n) ) mod n**

(((41\*41) mod 91)^14 \* 41 ) mod 91

((43\*43 mod 91 ) ^ 7 \* 41 ) mod 91

((29\*29) mod 91 ) ^3 \*29 \*41) mod 91

22\*22\*22\*29\*41 mod 91 =6

### 实验部分内容要求

**3、针对应用了解端口的三大分类，135、445、1433、3306、3389、4899、5901、43958等端口分属哪类？对应什么应用？并掌握ARP欺骗的原理与防范方法。**

网络端口的分类：

按端口号可分为3大类：

（1）公认端口（Well-KnownPorts）：范围从0到1023

它们紧密绑定（binding）于一些服务。通常这些端口的通讯明确表明了某种服务的协议。例如：21端口分配给FTP服务，25端口分配给SMTP（简单邮件传输协议）服务，80端口分配给HTTP服务，135端口分配给RPC（远程过程调用）服务等等。

我们在IE的地址栏里输入一个网址的时候（ 比如www.cce.com.cn）是不必指定端口号的，因为在默认情况下WWW服务的端口 号是“80”。

网络服务是可以使用其他端口号的，如果不是默认的端口号则应该在 地址栏上指定端口号，方法是在地址后面加上冒号“:”（半角），再加上端口 号。比如使用“8080”作为WWW服务的端口，则需要在地址栏里输入“www.cce.com.cn:8080”。

但是有些系统协议使用固定的端口号，它是不能被改变的，比如139 端口专门用于NetBIOS与TCP/IP之间的通信，不能手动改变。

（2）动态端口（Dynamic Ports）：范围从1024到65535

之所以称为动态端口，是因为它 一般不固定分配某种服务，而是动态分配。动态分配是指当一个系统进程或应用 程序进程需要网络通信时，它向主机申请一个端口，主机从可用的端口号中分配 一个供它使用。当这个进程关闭时，同时也就释放了所占用的端口号。

    (2.1)注册端口（RegisteredPorts）：从1024到49151。它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用         于许多其它目的。例如：许多系统处理动态端口从1024左右开始。

(2.2)动态和/或私有端口（Dynamicand/orPrivatePorts）：从49152到65535。理论上，不应为服务分配这些端口。实际上，机器通常从1024    起分配动态端口。但也有例外：SUN的RPC端口从32768开始。

TCP 135= 微软DCE RPC end-point mapper服务 DCOM服务，冲击波病毒利用，不能关闭

TCP 445=Microsoft-DS，为共享开放，震荡波病毒利用，一般应关闭

TCP 1433=Microsoft的SQL服务开放端口

3306 MySQL开放此端口

TCP 3389= 超级终端（ 远程桌面）

TCP 4899=Remote Administrator服务器

5901 虚拟网络计算机显示1

43958 Serv-U的本地管理端口，只允许127.0.0.1连接

arp欺骗攻击的核心思想就是向目标主机发送伪造的arp应答，用伪造的ip-mac地址之间的映射更新目标主机的arp缓存。

课程主要内容

**掌握基本概念--理清安全体系--加密认证是基础--网络安全有保证--内容安全是目标--安全管理是规范，标准法律是准绳。**

21、针对信息安全事件，会分析风险因素并从技术、管理、法规等方面给出解决办法。

**1、信息安全的概念，信息安全理念的三个阶段（信息保护-5特性，信息保障-PDRR，综合应用-PDRR+管理）**

概念：信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

三个阶段：

（1）信息保护阶段：信息安全的基本目标应该是保护信息的机密性、完整性、可用性、可控性和不可抵赖性。

（2）信息综合保障阶段--PDRR模型

保护（Protect）、检测（Detect）、响应（React）、恢复（Restore）

（3）信息安全整体解决方案：在PDRR技术保障模型的前提下，综合信息安全管理措施，实施立体化的信息安全防护。即整体解决方案＝PDRR模型 + 安全管理。

**2、ISC2的五重保护体系，信息安全体系-三个方面，信息安全技术体系**

国际信息系统安全认证组织（International Information Systems Security Certification Consortium，简称ISC2）将信息安全划分为5重屏障共10大领域。

（1）．物理屏障层（2）．技术屏障层（3）．管理屏障层（4）．法律屏障层（5）．心理屏障层

信息安全体系-三个方面：信息安全技术体系、信息安全组织机构体系、信息安全管理体系

信息安全技术体系：划分为物理层安全、系统层安全、网络层安全、应用层安全和管理层安全等五个层次。

1）物理安全技术（物理层安全）。该层次的安全包括通信线路的安全、物理设备的安全、机房的安全等。

2）系统安全技术（操作系统的安全性）。该层次的安全问题来自网络内使用的操作系统的安全，主要表现在三个方面：一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

3）网络安全技术（网络层安全）。主要体现在网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段、网络设施防病毒等。

4）应用安全技术（应用层安全）。主要由应用软件和数据的安全性产生，包括Web服务、电子邮件系统、DNS等。此外，还包括病毒对系统的威胁。

5）管理安全性（管理层安全）。安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。

**3、信息系统安全，等级保护，认证**

五个安全等级：

第一级—用户自主保护级 第二级—系统审计保护级

第三级—安全标记保护级 第四级—结构化保护级

第五级—访问验证保护级

从第一级到第五级安全等级逐级增高，高级别安全要求是低级别要求的超集。

分级保护的认证：

（1）信息安全产品认证 （2）信息系统安全认证

（3）信息安全服务资质认证 （4）注册信息安全专业人员资质认证（简称CISP）

**4、物理安全的概念，涉及的三个方面的内容**

物理安全的概念：指为了保证信息系统安全可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境人员，系统等采取适当的安全措施。

三个方面：

信息系统的物理安全涉及到整个系统的配套部件、设备和设施的安全性能、所处的环境安全以及整个系统可靠运行等三方面，是信息系统安全运行的基本保障。

**5、灾难备份的概念，安全备份三要素，备份的方式、存储技术**

灾难备份：是指利用技术、管理手段以及相关资源，确保已有的关键数据和关键业务在灾难发生后在确定的时间内可以恢复和继续运营的过程。

灾难备份三要素：一是系统中的部件、数据都具有冗余性，即一个系统发生故障，另一个系统能够保持数据传送的顺畅；二是具有长距离性，因为灾害总是在一定范围内发生，因而保持足够长的距离才能保证数据不会被同一个灾害全部破坏；三是灾难备份系统追求全方位的数据复制，上述三要素也称为“3R要素”（Redundance、Remote、Replication）。 数据备份方式：

（1）全备份：是指对整个系统进行包括系统和数据的完全备份。

（2）增量备份：是指每次备份的数据只是相当于上一次备份后增加的和修改过的数据。

（3）差分备份：就是每次备份的数据是相对于上一次全备份之后新增加的和修改过的数据。 常用的存储优化技术有：

直接连接存储DAS（Direct Attached Storage, DAS）：数据被存储在各服务器的磁盘族或磁盘阵列等存储设备中。

网络连接存储NAS（Network Attached Storage, NAS）：数据的存储（DAS）和处理（服务器）功能分离。

存储区域存储SAN（Storage Area Network, SAN）：SAN是用于连接服务器和存储装置（大容量磁盘阵列和备份磁带库）的专用网络。

虚拟存储(Storage Virtualization)：就是把多个存储介质模块（如硬盘、RAID等）通过一定的手段集中管理起来，所有的存储模块在一个存储池中得到统一管理。调配灵活、使用合理，是目前的发展方向之一。

**6、操作系统安全的概念，5大技术要求**

概念：操作系统的安全主要通过身份鉴别、自主访问控制、标记和强制访问控制、数据流控制、审计、数据完整性、数据保密性等几方面来实现系统的安全需要。操作系统的安全，应该从安全功能和安全保证两方面综合考虑。

操作系统安全的技术要求：

1. 身份鉴别

<1>用户标识

<2>用户鉴别

<3>用户主体行为绑定

1. 访问控制

<1>自主访问控制

<2>强制访问控制

<3>基于角色的访问控制

1. 安全审计
2. 用户数据的完整性和保密性
3. 可信路径

**7、访问控制：概念，类型，控制过程**

概念：访问控制是在保障授权用户能获取所需资源的同时拒绝非授权用户的安全机制，是信息安全理论基础的重要组成部分。

类型：自主访问控制、强制访问控制和基于角色的访问控制

控制过程：当一个账号被创建时，Windows系统为它分配一个SID，并与其他账号信息一起存入SAM数据库。

用户登录管理。登录主机（通常为工作站）的系统首先把用户输入的用户名、口令和用户希望登录的服务器／域信息送给安全账号管理器，安全账号管理器将这些信息与SAM数据库中的信息进行比较，如果匹配，服务器发给工作站允许访问的信息，并返回用户的安全标识和用户所在组的安全标识，工作站系统为用户生成一个进程。服务器还要记录用户账号的特权、主目录位置、工作站参数等信息。

本地安全授权机构为用户创建访问令牌，包括用户名、所在组、安全标识等信息。此后用户每新建一个进程，都将访问令牌复制作为该进程的访问令牌。

用户访问进程管理。安全引用监视器将用户/进程的访问令牌中的SID与对象安全描述符中的自主访问控制表进行比较，从而决定用户是否有权访问对象。

**8、安全审计的概念、作用**

概念：安全审计是指在一个信息系统中以维护系统安全为目的的审计，即为了保障系统、网络和数据不受来自外部和内部用户的入侵和破坏，而运用各种技术手段实时收集和监控系统中每一个组成部分的状态、安全事件，以便集中报警、分析、处理的一种技术手段。

作用：提供对受保护客体访问的审计跟踪功能，保护审计记录不被未授权访问、修改和破坏。提供可选择的审计事件，生成的审计日志可管理。

**9、风险评估的概念**

风险评估：就是对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用而带来风险的可能性的评估。

**10、加密技术的一般概念，密码体制及类型，公钥体制的特点**

概念：加密技术的基本思想就是伪装信息，使非法接入者无法理解信息的真正含义。

2）密码体制：

<1>对称密钥密码体制。

若发送和接受数据的双方所用的加密密钥和解密密钥相同，或实质上相同，我们称其为对称密钥，又叫专用密钥加密。

<2>非对称密钥密码体制（也成公钥体制）

非对称加密算法需要两个密码：公开密钥（Public Key）和私有密钥（Private Key）。公开密钥和私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私钥才能解密；如果用私有密钥对数据进行加密，只有用对应的公钥才能解密。

公钥体制的特点：优点是仅需要保密解密密钥，密钥管理比较简单，适合开放性要求，缺点是密码算法一般比较复杂，加、解密速度较慢。

**11、信息加密传输、发送者身份认证的实现方式。数字签名、身份认证、消息认证、信息隐藏的概念。**

通信加密方式：

链路加密：对网络中两个相邻节点之间传输的数据进行加密保护。

节点加密：在信息传输路过的节点处进行解密和加密（操作方式上与链路加密类似，但节点中也是密文，用另一种密钥实现）

端到端加密：数据在从源点到终点的传输过程中始终以密文形式存在。

身份认证常用的方式：通行字方式和持证方式。

数字签名技术：数字签名就是信息发送者使用公开密钥算法技术，产生别人无法伪造的一段数字串。

身份认证技术：被认证方在没有泄露自己身份信息的前提下，能够以电子的方式来证明自己的身份，其本质就是被认证方拥有一些秘密信息，除被认证方自己外，任何第三方（某些需认证权威的方案中认证权威除外）无法伪造，被认证方能够使认证方相信他确实拥有那些秘密，则他的身份就得到了认证。

消息认证技术：指通过对消息或消息相关信息进行加密或签名变换进行的认证，目的是为防止传输和存储的消息被有意或无意地篡改。（包括消息内容认证、消息的源和宿认证、消息的序号和操作时间认证）

信息隐藏技术：信息隐藏是把机密信息隐藏在大量信息中不让对手发觉的一种方法。信息隐藏的方法主要有隐写术、数字水印技术、可视密码、潜信道、隐匿协议等。

数字水印技术：数字水印就是将特定的标记隐藏在数字产品中，用以证明原创者对产品的所有权，并作为起诉侵权者的证据。

**12、掌握RSA算法密钥生成、加密/解密的过程。在此基础上掌握给定公钥会解密等运算。**

密钥生成：

首先要使用概率算法来验证随机产生的大的整数是否质数，这样的算法比较快而且可以消除掉大多数非质数。假如有一个数通过了这个测试的话，那么要使用一个精确的测试来保证它的确是一个质数。

除此之外这样找到的p和q还要满足一定的要求，首先它们不能太靠近，此外p-1或q-1的因子不能太小，否则的话N也可以被很快地分解。

此外寻找质数的算法不能给攻击者任何信息，这些质数是怎样找到的，尤其产生随机数的软件必须非常好。要求是随机和不可预测。这两个要求并不相同。一个随机过程可能可以产生一个不相关的数的系列，但假如有人能够预测出（或部分地预测出）这个系列的话，那么它就已经不可靠了。比如有一些非常好的随机数算法，但它们都已经被发表，因此它们不能被使用，因为假如一个攻击者可以猜出p和q一半的位的话，那么他们就已经可以轻而易举地推算出另一半。

此外密钥d必须足够大，1990年有人证明假如p大于q而小于2q（这是一个很经常的情况）而，那么从N和e可以很有效地推算出d。此外e = 2永远不应该被使用。

密钥分配：

和其它加密过程一样，对RSA来说分配公钥的过程是非常重要的。分配公钥的过程必须能够抵挡一个从中取代的攻击。假设Eve交给Bob一个公钥，并使Bob相信这是Alice的公钥，并且她可以截下Alice和Bob之间的信息传递，那么她可以将她自己的公钥传给Bob，Bob以为这是Alice的公钥。Eve可以将所有Bob传递给Alice的消息截下来，将这个消息用她自己的密钥解密，读这个消息，然后将这个消息再用Alice的公钥加密后传给Alice。理论上Alice和Bob都不会发现Eve在偷听他们的消息。今天人们一般用数字认证来防止这样的攻击。

RSA算法是一种非对称密码算法，所谓非对称，就是指该算法需要一对密钥，使用其中一个加密，则需要用另一个才能解密。

RSA的算法涉及三个参数，n、e1、e2。

其中，**n是两个大质数p、q的积，n的二进制表示时所占用的位数，就是所谓的密钥长度。**

e1和e2是一对相关的值，e1可以任意取，但要求e1与(p-1）\*(q-1）互质；再选择e2，要求（e2\*e1）mod((p-1）\*(q-1））=1。

（n，e1）,(n，e2）就是密钥对。其中**(n，e1）为**公钥，**(n，e2）为私钥。[**

RSA加解密的算法完全相同，设A为明文，B为密文，则：A=B^e2 mod n；B=A^e1 mod n；（公钥加密体制中，一般用公钥加密，私钥解密）

e1和e2可以互换使用，即：

A=B^e1 mod n；B=A^e2 mod n;

**13、PKI的概念和组成**

公钥基础设施PKI：PKI是一个用公钥密码算法原理和技术来提供安全服务的通用性基础平台，用户可以利用PKI平台提供的安全服务进行安全通信。

PKI的组成：由五个部分组成：认证中心CA，注册机构RA、证书库CR、证书申请者、证书信任方。前三个部分是PKI的核心，证书申请者和证书信任方则是利用PKI进行网上交易的参与者。

**14、防火墙的概念、作用、特点、技术分类**

网络防火墙：是隔离在本地网络与外界网络之间执行访问控制策略的一道防御系统，包括硬

件和软件，目的是保护网络不被他人侵扰。

防火墙的作用：

1)防火墙是网络安全的屏障 2)防火墙可以强化网络安全策略

3)对网络存取和访问进行监控审计 4)防止内部信息的外泄

5)部署NAT功能 6)对网络攻击进行监测和报警

基本特征：

1）内部网络和外部网络之间的所有网络数据流都必须经过防火墙

2）只有符合安全策略的数据流才能通过防火墙

3）防火墙自身应具有非常强的抗攻击免疫力

技术分类：（六种）

1）包过滤型防火墙 2）应用网关型防火墙

3）混合或复杂网关型防火墙 4）代理服务型防火墙

5）状态检测型防火墙 6）深度检测型防火墙

**15、入侵检测的概念、系统组成，四类主要技术**

入侵检测（Intrusion Detection）：就是通过从计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象，并对此做出适当反应的过程。

入侵检测系统的组成：

事件产生器（Event generators）：从整个计算环境中获得事件，并向系统的其他部分提供此事件。

事件分析器（Event analyzers）：分析得到的数据据并产生分析结果。

响应单元（Response units）：对分析结果作出作出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。

事件数据库（Event databases）：保存各种中间和最终数据的数据库。

一般将四个组件分为两大部分：引擎和控制中心。

引擎用于读取原始数据和产生事件

控制中心用于显示和分析事件以及策略定制等工作

入侵检测技术：静态配置分析、异常检测技术、误用检测技术、基于系统关键程序的安全规格描述方法。

**16、VPN的概念、常用隧道协议，IPSec两种封装模式的特点、三个主要协议的作用，VPN的应用模式**

虚拟专用网（Virtual Private Network，VPN）指的是依靠ISP（Internet服务提供商）和其他NSP（网络服务提供商），在公用网络中建立虚拟的专用数据通信网络的技术。

常用隧道协议：

PPTP协议允许对IP、IPX或NetBEUI数据流进行加密，然后封装在IP包头中通过企业IP网络或公共因特网络发送。

L2TP协议允许对IP，IPX或NetBEUI数据流进行加密，然后通过支持点对点数据报传递的任意网络发送，如IP，X.25，帧中继或ATM。

IPSec隧道模式允许对IP负载数据进行加密，然后封装在IP包头中通过企业IP网络或公共IP因特网络如Internet发送。

IPSec两种封装模式的特点：

传输模式：只对IP数据包的有效负载进行加密或认证。此时，继续使用以前的IP头部，只对IP头部的部分域进行修改，而IPSec协议头部插入到IP头部和传输层头部之间。

隧道模式：对整个IP数据包进行加密或认证。此时，需要新产生一个IP头部，IPSec头部

被放在新产生的IP头部和以前的IP数据包之间，从而组成一个新的IP头部。

IPSec的三个主要协议：

1）ESP（Encapsulating Security Payload）：ESP协议主要用来处理对IP数据包的加密。ESP是与具体的加密算法相独立的，几乎支持各种对称密钥加密算法，默认为3DES和DES。

2）AH(Authentication Header)：AH只涉及到认证，不涉及到加密。

3）IKE(Internet Key Exchange)：IKE协议主要是对密钥交换进行管理，它主要包括三个功能：①对使用的协议、加密算法和密钥进行协商；②方便的密钥交换机制(这可能需要周期性的进行)；③跟踪对以上这些约定的实施。

VPN的应用模式：

1、远程访问 2、远程网络互连 3、网络内部安全

**17、信息安全职业道德主要关注的问题**

职业：职业的通俗表述就是人们所从事的工作。一定的职业是从业者获取生活来源、扩大社 会关系和实现自身价值的重要途径。

道德：是依靠社会舆论、传统习惯、教育和人的信念的力量去调整人与人、个人与社会之间 关系的一种特殊的行为规范。

职业道德：就是同人们的职业活动紧密联系的符合职业特点所要求的道德准则、道德情操与 道德品质的总和。道德要求和行为准则

信息安全的职业道德：主要是指计算机、网络技术使用的道德规范。

**18、什么是计算机犯罪？有哪三种主要形式？**

计算机犯罪：是指行为人通过计算机操作所实施的危害计算机信息系统（包括内存数据及程序）以及其他严重危害社会的并应当处以刑罚的行为。

主要形式：

第285条：非法侵入国家计算机信息系统罪，列举式并规定了相应的刑罚。

第286条：破坏计算机信息系统罪，列举式并规定了相应的刑罚。

第287条：利用计算机犯罪，作为犯罪工具的原则性规定，刑罚由相关条款规定。

**19、信息系统安全保护法律规范由哪三类内容构成？**

法律体系：一个国家全部现行法律规范分类组合为不同的法律部门而形成的有机联系的统一 整体。《宪法》和《刑法》等。

政策体系：政府制定相应的法律、法规，强制性加大对信息系统安全保护的力度。

强制性技术标准：国家发布了多个技术标准，并且要求强制性地执行。

**20、信息系统安全等级保护分级的衡量标准是什么？相关的主要标准与政策有哪些？分别有什么作用？**

衡量标准：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度（客体：国家安全、社会秩序 公共利益、公民 法人和其他组织的合法权益）

相关政策：

中华人民共和国计算机信息系统安全保护条例

（1994年2月18日中华人民共和国国务院令147号）

信息安全等级保护管理办法

2007年6月22日，由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室等国家四部委制定完成并审批通过

计算机信息系统安全保护等级划分准则 案例

（GB 17859-1999）于1999年9月13日发布

GB 22239-2008-T 信息安全技术 信息系统安全等级保护基本要求

GB 22240-2008-T 信息安全技术 信息系统安全等级保护定级指南 实施指南

《商用密码管理条例》、《中华人民共和国电子签名法》、《计算机软件保护条例》等。

信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，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，信息系统受到破坏后，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，信息系统受到破坏后，会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，信息系统受到破坏后，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，信息系统受到破坏后，会对国家安全造成特别严重损害。