Ch1：introduction

脆弱点―威胁―控制的范式

Vulnerability

Threat：

C-I-A Triad：Confidentiality（机密性），Integrity（完整性），Availability（可用性）

Advanced Persistent Threat (APT)（有针对性地有组织的攻击）

Attack：

* *Interception 窃听*, or unauthorized viewing
* *Modification篡改*, or unauthorized change
* *Fabrication伪造*, or unauthorized creation
* *Interruption中断*, or preventing authorized access

Countermeasure or control：

纵深防御 - Defense in Depth 或 Layered Security。

中文解释：纵深防御是一种安全策略，通过在网络的不同层次（如物理层、网络层、应用层等）部署多种安全措施，形成多层防护，使得即使某一层被突破，其他层次仍然能够提供保护，从而增强整个系统的安全性。

Method—Opportunity—Motive（方法―时机―动机模型）

在网络安全中，"Method" 可能指的是黑客使用的攻击手段，如钓鱼、恶意软件或DDoS攻击；"Opportunity" 可能是指系统配置错误或未打补丁的漏洞；而 "Motive" 可能是指为了经济利益、竞争情报或政治目的。通过分析这些因素，组织可以更好地评估风险并采取相应的安全措施。

Ch2：

两类基本的网络安全控制策略：

**身份鉴别Authentication：**

Something the user knows密码

安全密码规则：

* 避免密码共用
* 8位或8位以上
* 包含字母、数字和特殊字符的组合
* 不用生日和姓名

Something the user is生物特征（Biometrics）

Something user has令牌（token）

**访问控制：**

Reference Monitor (参考监控器)

中文解释：参考监控器是一个抽象概念，用于实现和强制执行访问控制策略。它负责检查所有访问尝试，确保它们符合安全策略。参考监控器必须是不可篡改的、始终可用的，并且其决策必须是可验证的。

Access Control Directory (访问控制目录)

中文解释：访问控制目录是一个结构化的数据存储，用于保存关于系统资源和用户访问权限的信息。它通常包含资源的标识和相应的访问控制信息。

Access Control Matrix (访问控制矩阵)

中文解释：访问控制矩阵是一种表示访问控制策略的表格结构，行表示用户或主体，列表示资源或对象，矩阵中的单元格则表示特定用户对特定资源的访问权限。

Access Control List (ACL) (访问控制列表)

中文解释：访问控制列表是一种用于定义对某一资源访问权限的列表，其中列出了允许访问该资源的用户及其具体权限。每个资源都有一个ACL来管理其访问控制。

Procedure-Oriented Access Control (面向程序的访问控制)

中文解释：面向程序的访问控制是一种通过特定程序或应用来控制访问权限的机制。该方法根据程序的需求和功能来限制用户或其他程序对资源的访问。

Role-Based Access Control (RBAC) (基于角色的访问控制)

中文解释：基于角色的访问控制是一种访问控制方法，通过分配用户到特定角色，然后根据角色来授予访问权限。这种方法简化了权限管理，因为权限是与角色关联的，而不是与个体用户直接关联。

Plaintext（明文）

Ciphertext（密文）

**对称加密 (Symmetric Encryption)**

定义：使用相同的密钥进行加密和解密

每对通信双方都需要共享一个秘密密钥，随着通信方数量的增加，密钥管理变得复杂。

**非对称加密 (Asymmetric Encryption)**

定义：使用一对密钥进行加密和解密，一个是公开密钥（public key），另一个是私有密钥（private key）。发送方使用接收方的公钥加密数据；接收方使用自己的私钥解密数据

特点：

安全性高：公开密钥用于加密，私有密钥用于解密。即使公开密钥泄露，私有密钥仍然保持安全。

速度慢：由于算法复杂，非对称加密的加密和解密速度较慢，不适合大规模数据加密。

密钥管理简化：每个用户只需要维护一对密钥，公开密钥可以自由分发，私有密钥必须保密。

Stream Ciphers（流密码）：在流密码中，数据流的每个字节都是单独加密的

Block Ciphers（分组密码）：与流密码不同，分组密码将一组明文符号加密为单个块

DES（The Data Encryption Standard）：Symmetric block cipher

AES（Advanced Encryption System）：Symmetric block cipher

Ch3：

**缓冲区溢出**

危害：overwriting

覆盖程序的另一部分数据 程序中的指令 属于其他程序的数据或代码 属于操作系统的数据或代码。覆盖程序的指令会为攻击者提供该程序的执行权限 覆盖操作系统指令为攻击者提供操作系统的执行权限

措施：

不要超出开辟空间界限

写入前检查长度

确认数组下标在限制范围内

仔细检查边界条件代码是否存在偏差 1 错误

将输入限制为可接受的字符数

限制程序的权限以减少潜在危害

许多语言都有溢出保护

代码分析器可以识别许多溢出漏洞

堆栈中的金丝雀值以示信号修改（堆栈中的金丝雀值（Canary Values）是一种用于检测和防止基于堆栈的缓冲区溢出攻击的安全机制）

**竞态条件：race condition（OS）**

**恶意代码（malware）**

特点：

**危害：**

对用户和系统的危害：

向用户联系人发送电子邮件

删除或加密文件 勒索病毒

修改系统信息，如 Windows 注册表

窃取敏感信息，例如密码

附加到关键系统文件

将恶意软件副本隐藏在多个互补位置

对世界的危害：

众所周知，一些恶意软件会感染数百万个系统，并以几何速度增长

受感染的系统通常成为新感染的集结地

**预防：**

使用从可靠来源获得的软件

杀毒软件

在隔离环境中测试软件

仅当知道附件是安全的时才打开它们

将每个网站都视为潜在有害网站

创建和维护备份

恶意代码的主要类型：病毒、木马和蠕虫。

1. **病毒（Virus）**：
   * 病毒是一种恶意软件，它能够自我复制并将自身的副本插入到其他程序中。病毒通常需要宿主程序来执行，并且可以通过多种方式传播，例如通过电子邮件附件、下载的文件或可移动介质。
   * 病毒可以导致数据损坏、系统性能下降，甚至完全系统崩溃。
2. **蠕虫（Worm）**：
   * 蠕虫是一种独立运行的恶意软件，它不需要宿主程序。蠕虫能够自我复制，并利用网络（如电子邮件、即时通讯、网络漏洞等）传播到其他计算机或设备。
   * 蠕虫可以迅速传播，消耗大量网络带宽，可能导致网络拥堵甚至服务中断。
3. **特洛伊木马（Trojan Horse）**：
   * 特洛伊木马是一种伪装成合法软件的恶意程序，它声称具有某种有用的功能，但实际上隐藏着恶意功能。用户可能会被欺骗下载或安装特洛伊木马，而不知道其真实目的。
   * 特洛伊木马可以执行各种恶意行为，如窃取敏感信息、安装后门、删除文件、控制受感染的计算机等。

**Ch4：操作系统**

Layer design 和 modular design

层次化设计方法在解决和处理复杂问题时的优势和方法

1. 模块化 (Modularity)

易于维护：系统被划分为多个独立的模块，每个模块负责特定的功能。这样，修改一个模块不会影响其他模块，降低了维护难度。

可重用性：不同层次的模块可以在其他项目中重复使用，提高了代码的重用性。

2. 易于理解 (Ease of Understanding)

简化复杂性：通过分层设计，将复杂系统划分为更易于理解的子系统，使开发人员更容易理解和管理整个系统。

明确的职责划分：每一层都有明确的职责和功能，开发人员可以专注于某一层的设计和实现。

3. 灵活性 (Flexibility)

易于扩展：新的功能可以通过在适当的层次上添加新的模块来实现，而不需要对整个系统进行大规模改动。

易于替换：某一层的实现可以被替换或改进，而不影响其他层次。这使得系统可以灵活适应新的需求或技术。

4. 可测试性 (Testability)

独立测试：每一层可以独立进行测试，确保其功能正确性。这样可以更早发现和解决问题，提高系统的可靠性。

分层调试：如果系统出现问题，可以从上到下或从下到上逐层进行调试，快速定位问题所在。

5. 安全性 (Security)

安全隔离：分层设计可以在不同层次之间实现安全隔离，限制不同层次之间的直接访问，从而提高系统的安全性。

访问控制：每一层可以实现不同的访问控制策略，确保只有授权的模块或用户可以访问敏感数据或功能。

6. 协作性 (Collaboration)

并行开发：不同层次的模块可以由不同的团队或开发人员并行开发，提高开发效率。

责任明确：每个团队或开发人员可以专注于特定层次的实现，责任明确，有助于团队协作。

操作系统的层次化设计方法

将操作系统的所有功能模块根据调用次序排成若干层，每层之间只存在单向调用关系，高层 的模块依赖于底层的模块，且不同层次具有不同的权限和可信度

设计安全操作系统的原则

简约设计、分层设计（分层信任）、内核化设计、引用监视器、可信系统（按照一定的安全策略信任系统）

**rootkit** 是一种恶意软件包，它获得并利用 root 状态或有效地成为操作系统的一部分

Rootkit 通常会竭尽全力避免被发现，或者如果被发现并部分删除，则重新建立自己

这可能包括拦截或修改基本的操作系统功能

可信操作系统：Trusted Computing Base (TCB) 监控并保护四种基本交互的机密性和完整性：进程激活、执行域切换、内存保护和 I/O 操作。

1. **身份鉴别（Authentication）**：
   * **原理**：确认用户或系统的身份。
   * **手段**：
     + **密码**：传统的用户名和密码组合。
     + **生物识别**：指纹、面部、虹膜等生物特征。
     + **令牌**：使用一次性密码（OTP）或硬件令牌。
     + **多因素认证**：结合两种或以上的身份验证方法。
2. **访问控制（Access Control）**：
   * **原理**：限制用户或系统对资源的访问权限。
   * **手段**：
     + **自主访问控制（DAC）**：由资源所有者决定谁可以访问资源。
     + **角色基于访问控制（RBAC）**：根据用户的角色分配访问权限。
     + **强制访问控制（MAC）**：系统强制实施访问控制策略。
     + **属性基于访问控制（ABAC）**：根据属性（如用户属性、资源属性）控制访问。
3. **日志审计（Auditing）**：
   * **原理**：记录和审查系统活动，用于监控和事后分析。
   * **手段**：
     + **日志记录**：记录用户活动、系统事件等。
     + **日志管理**：集中管理日志，保证日志的完整性和可用性。
     + **日志分析**：使用自动化工具分析日志，检测异常行为。
4. **数据存储保密性（Data Storage Confidentiality）**：
   * **原理**：保护存储的数据不被未授权访问。
   * **手段**：
     + **数据加密**：使用加密算法保护数据。
     + **访问控制列表（ACL）**：限制对数据的访问。
     + **数据库安全**：使用数据库特定的安全措施，如SQL注入防护。
5. **数据传输保密性（Data Transmission Confidentiality）**：
   * **原理**：保护数据在传输过程中不被截获或篡改。
   * **手段**：
     + **SSL/TLS**：使用安全协议加密数据传输。
     + **VPN**：虚拟私人网络提供安全的网络连接。
6. **数据存储完整性（Data Storage Integrity）**：
   * **原理**：确保存储的数据未被未授权修改或损坏。
   * **手段**：
     + **哈希函数**：使用哈希值检测数据是否被篡改。
     + **写入权限控制**：限制谁可以修改数据。
7. **数据传输完整性（Data Transmission Integrity）**：
   * **原理**：确保数据在传输过程中保持完整，未被篡改。
   * **手段**：
     + **消息认证码（MAC）**：确保数据的完整性和认证。
     + **数字签名**：使用公钥加密技术验证数据的完整性和来源

**Ch5：**

两个重要思想：

（1）对于网络结构设计的层次化分析设计方法。

（2）网络安全纵深防御的思想方法。

5种安全技术：

（1）无线网络安全协议和标准（WEP\WPA）

（2）拒绝服务攻击（Dos和DDos）

（3）VPN技术

（4）防火墙的主要原理和利用访问控制规则及进行网络流量控制的方法。

（5）入侵监测方法和技术（IDS\IPS）

【分析】网络拓扑图识读和分析方法。

通信设备

1. cable电缆：双绞线，同轴电缆
2. 光纤optical fiber（主干线路上常使用）
3. 微波Microwave
4. 卫星通信satellite communication
5. Wifi,传输距离短，易遮挡

通信媒体脆弱性：

wiretaps窃听, sniffers嗅探器 rogue receivers流氓接收器, interception拦截, and impersonation冒充

网络通信的威胁：

Interception 窃听, or unauthorized viewing

Modification篡改, or unauthorized change

Fabrication伪造, or unauthorized creation

Interruption中断, or preventing authorized access

Security Perimeters安全边界

What Makes a Network Vulnerable to Interception?是什么让一个网络很容易被截获？

1）匿名性Anonymity

2）Many points of attack攻击点多 ：庞大的网络意味着许多潜在的切入点

3）Sharing共享性

4）System complexity系统的复杂性

5）Unknown perimeter未知边界:网络的可扩展性也意味着网络的边界是不确定的。一台主机可能同时是两个不同网络的节点，因此，在一个网络中的资源也可以被其他网络的用户访问

6）Unknown path未知路径:从一个主机到另一个主机可能有许多路径，包括不可信的路径

网络数据损坏（data corruption）既可能是由传输媒介的轻微错误导致的，也可能是由恶意的目的引发的，对于这两个原因都应该注意防范。

Modification and Fabrication篡改或伪造的方式：

Data corruption 数据损坏

可能是有意的或无意的，恶意的或非恶意的，定向的或随机的

Sequencing顺序

更改排列数据的顺序，例如按顺序到达的数据包

Substitution 替代

将数据流的一部分替换为另一部分数据流

Insertion 插入

将数据值插入到流中的一种替换形式，比如插入恶意代码。

Replay 重复

重复攻击是指攻击者拦截并存储合法数据，然后在不适当的时间或环境下重新发送这些数据，以欺骗系统或用户

服务中断的原因：

Routing（路由）：如果配置不当，可能会导致路由信息错误，从而影响整个网络的数据传输，这种现象称为路由中毒。

Excessive Demand（过剩需求）：网络的带宽和处理能力是有限的。过剩需求指的是对网络资源的需求超出了其承载能力。攻击者可以通过生成大量流量来模拟这种过剩需求，从而对网络的关键部分造成压力，导致服务不可用或性能下降。

Component Failure（元件失效）：网络中的硬件或软件组件可能会因为各种原因失效，包括硬件故障、软件错误或外部因素。元件失效通常是不可预测的，如果没有适当的冗余和故障转移机制，可能会导致服务中断

无线网络中的脆弱点Vulnerabilities in Wireless Networks（Wifi的优点：一台AP可以接入多台设备）

1. 机密性Confidentiality：如果数据在开放的环境中进行传输，则其他人就有可能会得到这些数据
2. Integrity完整性
3. Availability可用性

4. Unauthorized WiFi access未授权的无线访问：未授权的设备可以尝试和访问接入点建立连接

5.WiFi protocol weaknesses无线协议的弱点：最常用的无线网络数据加密方式：WEP（最早的一代加密方式），WPA

How WEP（Wired equivalent privacy） Works：

客户端和接入点(AP)有一个预共享密钥

AP向客户端发送一个随机数，然后客户端使用密钥对其进行加密并返回给AP

AP使用密钥解密该数字，并检查它是否与之前发送给客户端的数字相同

客户端通过身份验证后，AP和客户端使用密钥加密的消息进行通信

WEP Weaknesses弱点：

1. **Weak encryption key（脆弱的加密密钥）**：
   * WEP 使用的加密密钥通常较短，这使得它容易被破解。
2. **Static key（静态密钥）**：
   * 如果密钥长时间不更换，攻击者可以通过捕获和分析大量数据包来尝试推断密钥。
3. **Weak encryption process（弱加密过程）**：
   * WEP 的加密过程存在缺陷，使得攻击者可以通过暴力破解或其他攻击方法较快地破解密钥。
4. **Weak encryption algorithm（弱加密算法）**：
   * WEP 使用的 RC4 流密码算法在设计上存在缺陷，容易受到各种攻击。
5. **IV collisions（初始化向量冲突）**：
   * WEP 使用的初始化向量（IV）较短，这增加了 IV 冲突的可能性，一旦发生冲突，攻击者可以利用这一弱点来破解加密。
6. **Faulty integrity check（错误的完整性检查）**：
   * WEP 的完整性检查机制存在缺陷，攻击者可以修改数据包并计算出新的校验值，使得接收方无法检测到数据已被篡改。
7. **No authentication（无鉴别）**：
   * WEP 缺乏有效的鉴别机制，任何设备只要知道网络的 SSID 和 MAC 地址，就可以连接到网络，这增加了未授权访问的风险。

Wi-Fi Protected Access (WPA) 是一种无线网络安全标准，旨在解决 WEP 存在的安全问题。以下是对 WPA 优势的解释：

1. **Non-static encryption key（非静态密钥）**：
   * WPA 引入了一种称为 TKIP（Temporal Key Integrity Protocol）的加密算法，它为每个传输的数据包生成一个临时密钥，从而提高了安全性。
2. **Authentication（鉴别）**：
   * WPA 支持多种身份验证方法，包括预共享密钥（PSK，也称为密码）、802.1X 认证、令牌或数字证书，这增加了网络的安全性。
3. **Strong encryption（强加密）**：
   * 虽然 WPA 初始版本使用 TKIP 作为加密算法，但随后的 WPA2 采用了更为安全的 AES（高级加密标准）算法，提供了更强的加密保护。
4. **Integrity protection（完整性保护）**：
   * WPA 引入了 Michael 完整性检查算法，它与数据一起加密，提供了比 WEP 更好的数据完整性保护。
5. **Session initiation（会话初始化）**：
   * WPA 和 WPA2 的会话初始化过程更加健壮，包括四步握手过程，这有助于确保网络连接的安全性。

拒绝服务攻击（DoS，Denial of Service）是一种旨在使计算机系统或网络无法向其用户正常提供服务的攻击方式。以下是对您提到的几种攻击类型的解释：

1. **Volumetric attacks（容量耗尽攻击）**：
   * 这种攻击通过向目标系统发送大量流量，超过其处理能力，从而使得系统无法处理合法的请求。这种攻击通常使用僵尸网络（botnets）来发起。
2. **Application-based attacks（基于应用的攻击）**：
   * 这种攻击针对特定应用程序或服务的弱点，例如通过发送恶意构造的请求来利用软件漏洞，导致应用程序崩溃或无法响应。
3. **Disabled communications（通信中断）**：
   * 这种攻击的目的是中断或破坏网络通信，使得用户无法访问服务。这可能通过多种方式实现，如截断网络连接、干扰信号或破坏通信基础设施。
4. **Hardware or software failure（硬件或软件故障）**：
   * 虽然硬件或软件故障本身不一定是攻击的结果，但它们可能被用作攻击手段，例如通过利用软件中的漏洞来导致系统崩溃，或通过物理手段破坏硬件。

具体的DoS Attack:

1. **Ping Flood**：
   * 通过发送大量的ICMP Echo请求（即“ping”命令）到目标服务器，试图耗尽其网络带宽或处理能力。
2. **Smurf Attack**：
   * 利用ICMP广播消息，攻击者发送伪造源IP地址的ICMP请求到一个网络的广播地址，导致该网络的所有主机都向被伪造的源IP地址发送回复，从而产生大量流量。
3. **Echo-Chargen**：
   * 这是一种结合了Echo和Chargen服务的攻击。攻击者向目标发送Echo请求，目标响应后，攻击者又向目标发送Chargen请求，目标再响应，如此循环，创建了一个反馈循环，导致大量流量。
4. **Teardrop Attack**：
   * 通过发送重叠的IP片段来攻击目标系统，这些片段在重组时会导致缓冲区溢出或系统崩溃。
5. **DNS Spoofing**：
   * 也称为DNS缓存污染，攻击者通过伪造DNS响应来将域名解析指向错误的IP地址，从而截获或篡改流量。
6. **Rerouting Routing**：
   * 攻击者通过操纵路由信息，如使用伪造的ICMP重定向消息，来改变数据流向，可能导致流量被重定向到攻击者控制的服务器。
7. **Session Hijacking**：
   * 这不是一种DoS攻击，而是一种会话劫持攻击。攻击者通过盗取或预测会话标识符（如cookies或会话令牌），接管一个已经建立的网络会话。

分布式拒绝服务（DDoS）攻击是一种通过多个来源同时向目标系统**发送大量流量，**以耗尽其资源并使其无法正常服务的攻击类型。以下是您提到的几个概念的解释：

1. **Botnets（僵尸网络）**：
   * 僵尸网络是由被恶意软件感染并**受攻击者远程控制**的计算机组成的网络。攻击者可以利用僵尸网络中的计算机同时向目标发起DDoS攻击，使得攻击流量来自多个分散的源，难以防御。

**后面都是防御措施**：

网络加密：

1. **Link Encryption（链路加密）**：
   * 链路加密是指在网络链路层对数据进行加密，确保在传输过程中的数据安全。然而，链路加密通常只保护网络中的一个特定部分，并不涵盖整个通信路径。
2. **End-to-End Encryption（端到端加密）**：
   * 端到端加密是指在数据的发送端进行加密，在接收端进行解密，整个过程中数据在传输和存储时都是加密状态。这种加密方式可以保护数据不被中间节点读取或篡改，常用于保护通信的隐私和完整性

远程登陆服务器不加密的用Telnet，加密的用SSH（UNIX）和远程桌面（windows）

SSL（secure socket layer） and TLS（Transport Layer Security）：都是用来保护web浏览器和服务器之间的通信的协议，都在传输层工作。

在1999年SSL的升级中，它被重命名为传输层安全(TLS)。

洋葱路由（Onion Routing）是一种网络通信协议，用于**匿名化数据传输的路径**，使得通信的发起者和接收者的身份以及通信内容都得到保护。这种技术允许用户在互联网上进行匿名通信，而不必担心其通信被追踪或监视。

VPN（重点）**Virtual Private Networks**：

通过一个公用网络建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。

 VPN的优点 ：

网络隐私保护：VPN能够加密用户的网络流量，有效保护个人隐私信息。

突破地域限制：VPN可以帮助用户访问地理位置受限的网站和服务。

信息安全性：VPN可以有效防止黑客窃取个人信息。

防火墙firewall：防火墙是在受保护(或“内部”)网络与不可信(或“外部”)网络之间对所有通信信息按照设定的规则来进行过滤的设备。

特点：

* Always invoked (cannot be circumvented) 始终调用（无法规避）
* Tamperproof防篡改
* Small and simple enough for rigorous analysis体积小，足够简单，可以进行严格的分析

Types of Firewalls：

1. **Packet filtering gateways or screening routers（数据包过滤网关或筛选路由器）**：
   * 这种防火墙工作在网络层，根据IP地址和其他数据包头部信息（如端口号）来决定是否允许数据包通过。它们通常基于访问控制列表（ACL）来过滤流量。
2. **Stateful inspection firewalls（状态检查防火墙）**：
   * 状态检查防火墙不仅检查每个数据包，还跟踪连接的状态，确保数据包是合法会话的一部分。这种防火墙可以提供更高级的过滤规则和更好的安全性。
3. **Application-level gateways, also known as proxies（应用级网关，也称为代理）**：
   * 应用级网关或代理防火墙工作在应用层，能够检查数据包的内容，并根据应用协议的特定规则来控制流量。它们可以提供更深入的检查和更细粒度的控制。
4. **Circuit-level gateways（电路级网关）**：
   * 电路级网关在会话层工作，监控TCP握手过程，仅允许建立成功的连接通过。它们不检查数据包内容，但可以防止未授权的连接尝试。
5. **Guards（守卫）**：
   * 守卫是一种防火墙，通常用于控制对特定网络资源的访问。它们可能结合了多种防火墙技术，以提供更全面的安全控制。
6. **Personal or host-based firewalls（个人或基于主机的防火墙）**：
   * 个人或基于主机的防火墙安装在单个设备上，如个人电脑或移动设备，用于保护该设备免受未授权的访问和网络攻击。

DMZ，是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。该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，如企业Web服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络。因为这种网络部署，比起一般的防火墙方案，对来自外网的攻击者来说又多了一道关卡

纵深防御：有多层防御

NAT（Network Address Translation）：解决IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机

数据丢失防护（DLP，Data Loss Prevention）是一套用于检测、监控和防止敏感数据泄露的技术。DLP 解决方案可以部署在各种环境中，以确保组织的信息安全。

1. **Indicators DLP looks for（DLP寻找的指标）**：
   * **Keywords（关键词）**：
   * **Traffic patterns（流量模式）**
   * **Encoding/encryption（编码/加密）**
2. **Preventing accidental incidents（防止意外事件）**：
   * DLP在防止意外数据泄露方面非常有效，例如通过限制对敏感数据的访问或阻止将敏感数据发送到未授权的目的地。
3. **Circumvention by malicious users（恶意用户规避）**：
   * 尽管DLP可以有效地防止意外事件，但恶意用户可能会找到绕过DLP的方法，例如通过使用隐蔽的传输渠道或复杂的编码技术。

入侵检测系统（Intrusion Detection System, IDS）和入侵防御系统（Intrusion Prevention System, IPS）是网络安全领域中两种重要的技术，它们用于检测和防御网络攻击。以下是对这两种系统的详细解释：

**入侵检测系统（IDS）**

1. **功能**：
   * 实时监控网络流量和系统活动，以发现潜在的恶意行为。
   * 通过分析数据包和系统日志，使用签名匹配、异常检测等方法来识别攻击。
2. **警报**：
   * 当检测到可疑活动时，IDS会发出警报，通知系统管理员或安全团队。
3. **被动性**：
   * IDS通常是被动的，它不直接阻止攻击，而是通过警报来提醒相关人员采取措施。
4. **部署方式**：
   * 可以是网络基的（NIDS），监控整个网络流量。
   * 也可以是主机基的（HIDS），监控单个系统或应用程序的活动。

**入侵防御系统（IPS）**

1. **功能**：
   * IPS在IDS的基础上增加了主动防御的能力，能够自动阻止或缓解检测到的攻击。
2. **主动性**：
   * IPS可以实时阻止攻击，而不仅仅是发出警报。
3. **部署方式**：
   * **直连部署**：IPS设备串联在网络中，流量必须经过IPS设备，这样它可以实时检测并阻止攻击。
   * **旁路部署**：IPS设备通过端口镜像或TAP（测试访问点）接收网络流量的副本，进行监控和分析，但不直接参与流量传输。

**区别和联系**

* **相同点**：IDS和IPS都用于检测网络中的恶意活动，它们可以共享检测技术和规则库。
* **不同点**：
  + IDS主要负责检测和警报，而IPS则增加了防御措施。
  + IPS可以对流量进行更深入的检查，可能需要更多的计算资源。

**应用场景**

* **IDS**：适用于需要监控网络活动但不直接干预的场景，如安全监控中心或大型企业的安全运营团队。
* **IPS**：适用于需要实时防御攻击的场景，如关键基础设施、金融服务网络等

SIEM（Security Information and Event Management ）：接入各个用户访问的日志（什么时候登录，做了什么，提交了什么数据，下载了什么东西，访问量哪个交换机等等），对这些数据进行存储收集并分析，从而发现潜在的安全风险和攻击行为。

规范定义：安全信息和事件管理（SIEM）技术通过对来自各种事件和上下文数据源的安全事件的实时收集和历史分析来支持威胁检测和安全事件响应。它还通过分析来自这些来源的历史数据来支持合规报告和事件调查。SIEM技术的核心功能是广泛的事件收集，以及跨不同来源关联和分析事件的能力。

ch6：

【认识、描述】隐私的基本概念和隐私保护的重要性。

隐私保护的主要保护对象：

个人信息、金融信息、生物特征、位置信息等

Identity

Finances

Health

Biometrics

Privileged communications

Location data

当前大数据、数据挖掘、爬动、COOKIE分析等隐私发现技术的主要技术思路和安全防范策略。

Ch7：

数据安全与数据库：

安全要求：

大型：Oracle ， DB2, Informix中型：Microsoft SQL Server小型：MySql, SQL Lite,

The most common database query language is SQL

数据库的安全需求：

1.数据库的物理完整性（**Physical integrity**）:数据库中的数据不受停电之类问题的影响，并且人们可以重建被灾难破坏的数据库。  
2.数据库的逻辑完整性**Logical integrity**:保护数据库的结构。例如，有了数据库的逻辑完整性，修改一个域的值不会影响其他的域。

3.元素完整性**Element integrity**:每个元素中包含的数据都是正确的。

4.可审计性Auditability:数据库日志可跟踪谁访问(或修改)了数据库的元素，或者访问(或修改)了什么元素

5.用户鉴别**User authentication**:对每一名用户都必须加以鉴别，包括审计跟踪和允许访问特定的数据。

6.访问控制**Access control**:用户只能访问被授权的数据，不同的用户有不同的访问模式(如读或写)。

7.可用性**Availability**:用户可以访问数据库中的授权数据和一般数据。  
作为一种大型的系统软件，数据库系统中也存在着各种各样的安全漏洞，其中危害性较大的有缓冲区溢出、堆溢出和SQL注入等

针对数据库的攻击：

1. 弱口令攻击：密码强度低或没有，导致未授权用户访问。
2. 利用漏洞对数据库发起的攻击
3. SQL Serever的单字节溢出攻击
4. SQL注入攻击
5. **Inherently sensitive（固有敏感）**：
   * 某些信息由于其性质而被认为是敏感的，例如，密码和武器存放地点因其对安全的影响而被认为是固有敏感的。
6. **From a sensitive source（来自敏感来源）**：
   * 信息的敏感性可能来自于其来源。例如，来自保密线人的信息可能具有高度的敏感性，因为泄露这些信息可能会危及线人的安全或调查的完整性。
7. **Declared sensitive（声明敏感）**：
   * 有些数据被明确声明为敏感信息，如机密文件或匿名捐赠者的名字。这种声明通常伴随着特定的保护措施和访问控制。
8. **Part of a sensitive attribute or record（敏感属性或记录的一部分）**：
   * 在数据库或记录中，某些属性可能被认为是敏感的，例如员工数据库中的薪资信息。这些信息需要特别的保护，以防止未经授权的访问或泄露。
9. **Sensitive in relation to previously disclosed information（与先前披露的信息相关的敏感性）**：
   * 某些信息可能在与其他已公开信息结合时变得敏感。例如，一个加密文件本身可能不敏感，但如果与打开它的密码一起考虑，则变成了敏感信息。
10. **An encrypted file combined with the password to open it（加密文件及其打开密码）**：
    * 加密文件和相应的密码组合在一起时，构成了敏感数据。如果两者同时泄露，可能会导致敏感信息的暴露

Ch8：

对称密钥密码体制；公开密钥加密、数字签名；端点鉴别协议；防火墙及入侵检测。

**数字签名Digital Signatures**：使用私钥对数据进行签名，接收方使用发送方的公钥验证签名。数字签名保证数据的完整性和不可否认性。