【精选】哈工大 信息安全概论 万字复习笔记

原创 MarcyTheLibrarian 于 2022-10-05 23:48:23 发布 阅读量1.6k 收藏 23 点赞数 9

分类专栏： 知识点 文章标签： 网络安全

说在前面的话

学弟学妹们，不要担心。虽然这门课学起来令人懵逼（主要是因为它安排在了计算机网络 之前，所以大部分同学都缺少这部分知识储备），但是经的复习，大家都能在较短时间内顺利（甚至是优雅）的通过考试。

下面，将按考点来依次带领大家复习。

请注意：
1.高亮的为重点复习考点哦！
2.最后的那些看起来很水的考点也很有可能考到

2022年春季考试的分值分布

> 单选：10分（每题2分，共5题）
> 填空：10分（每题2分，共5题）
> 简答题：30分（6题，每题5分）
> 计算题：15分（1题）
> 设计题：15分（1题）
> 简述题：10分（1题）
> 辨析题：10分（1题）

考点一 信息安全架构

1 面向目标的知识体系结构

信息安全CIA三元组(信息安全的三个最基本的目标)：
C - 机密性：信息在存储、传输、使用过程中，不会泄露给非授权用户或实体
I - 完整性：信息在存储、传输、使用过程中，不会被非授权用户篡改或防止授权用户对信息进行不恰当的篡改
A - 可用性：凡是为了确保授权用户或实体对信息资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息资源地相关理论技术均属于可用性

如果组织最关心地是对私密信息地保护，就会特别强调机密性原则，如果组织最关心的是随时随地向客户提供正确的信息，那就会突出完整性和可用

DAD三元组(信息安全面临的最普遍的三类风险)：
D - 泄漏、A - 篡改、D - 破坏

2 面向应用的层次型技术架构

信息系统的基本要素：人员、信息、系统；
人员 - 管理安全
信息 - 内容安全、数据安全
系统 - 运行安全、物理安全
三者的五个层次安全有一定顺序关系，每个层次均为其上层提供基础安全保证

安全层次
- 物理安全：指对网络及信息系统物理装备的保护。
- 运行安全：指对网络及信息系统的运行过程和运行状态的保护。
- 数据安全：指对数据收集、存储、检索、传输等过程提供的保护，不被非法冒充、窃取、篡改、抵赖。
- 内容安全：指依据信息内涵判断是否符合特定安全策略，采取相应的安全措施。
- 管理安全：指通过针对人的信息行为的规范和约束，提供对信息的机密性、完整性、可用性以及可控性的保护。

3 面向过程的信息安全保障体系

信息安全保障体系包括四部分内容(PDRR)
P - 保护：指预先采取安全措施，阻止攻击可以发生的条件形成，让攻击者无法顺利地入侵
保护是被动防御，不可能完全阻止各种对信息

R - 恢复：指当危害事件发生后把系统恢复到原来状态或比原来状态更安全的状态，将危害的损失降到最小。

保护是最基本的被动防御措施，也是第一道防线；
检测的重要目的之一是针对突破“保护防线”后的入侵行为进行探测预警；
而反应是在检测报警后针对入侵采取的控制措施；
恢复是针对攻击入侵带来的破坏进行弥补，是最后的减灾方法，如果前面的保障过程有效地控制了攻击行为，恢复过程则无须进行。

4 OSI开放系统互联安全体系结构

安全服务：
1.鉴别服务 - 用于确保某个实体身份的+可靠性
2.访问控制 - 防止对任何资源的非授权访问
3.数据机密性 - 确保只有经过授权的实体才能理解受保护的信息
4.数据完整性 - 防止对数据的未授权修改和破坏
5.抗抵赖性 - 也称不可否认性，用于防止对数据源以及数据提交的否认

安全机制：
1.加密 - 用于保护数据的机密性
2.数字签名 - 保证数据完整性及不可否认性的一种重要手段
3.访问控制 - 与实体认证密切相关
4.数据完整性 - 用于保护数据免受未经授权的修改
5.鉴别交换 - 用于实现通信双方的实体身份鉴别(身份认证)
6.业务流填充 - 针对的是对网络流量进行分析的攻击
7.路由控制 - 可以指定数据报文通过网络的路径
8.公证机制 - 由通信各方都信任的第三方提供

考点二 密码体制的五要素

通常一个完整密码体制要包括如下五个要素：
M - 是可能明文的有限集，称为明文空间
C - 是可能密文的有限集，称为密文空间
K - 是一切可能密钥构成的有限集，称为密钥空间
E - 为加密算法，对于密钥空间的任一密钥加密算法都能够有效地计算
D - 为解密算法，对于密钥空间地任一密钥解密算法都能够有效地计算

一个密码体系如果是实际可用的，必须满足如下特性：

1.加密算法$(E_k:M\to C)$和解密算法$(D_k:C\to M)$满足$D_k(E_k(x))=x$，这里$x\in M$；
2.破译者取得密文后，不能在有效的时间内破解出密钥k或明文x

考点三 仿射密码

仿射密码是替换密码的一个特例，可以看做是移位密码和乘数密码的结合。

其加密变换如下：
$$E_k(m)=(k_1m+k_2)mod\ q$$
仿射密码的密钥为(k_1,k_2)，其中，$k_1,k_2\in(0,q)$,且k_1和q是互素的。
其密码体系描述如下：
$$M=C=Z/(26);$$
$$q=26;$$
$$K=\{k_1,k_2\in Z|0<k_1,k_2<26,gcd(k_1,26)=1\};$$
$$E_k(m)=(k_1m+k_2)mod\ q;$$
$$D_k(c)=k_1^{-1}(c-k_2)mod\ q;$$
其中，
k_1^{-1}为k_1 k在模q下的乘法逆元(不是倒数)
$gcd(k,q)=1$表示k与q的最大公因子为1，即两者互素。
乘法逆元定义：
k^{-1}为k在模q下的乘法逆元，其定义为$k^{-1}*k\ mod\ q=1$

考点四 数据加密标准DES的算法结构和特点

1 S-DES(简化DES)算法结构：

S-DES加密算法输入为一个8位的二进制p明文组和一个10位的二进制密钥，输出为8位二进制密文组；解密与加密基本一致。

置换函数$P8$、$P10$和循环移位函数$Shift$,
初始置换IP、复合函数f_k、转换函数SW以及末尾置换IP^{-1}
加密过程表达式：
$$密文 = IP^{-1}(f_{k_2}(SW(f_{k_1}(IP(明文)))))$$
式中
$$k_1 = P8(Shift(P10(key)))$$
$$k_2 = P8(Shift(Shift(P10(key))))$$
解密过程表达式：
$$明文 = IP^{-1}(f_{k_1}(SW(f_{k_2}(IP(密文)))))$$

2 DES的特点

DES是一种对二进制数据进行分组加密的算法，以64位为分组对数据加密，DES的密钥也是长度为64位的二进制数。
加密算法和解密算法非常相似，唯一的区别在于子密钥的使用顺序正好相反。
DES的整个密码体制是公开的，系统的安全性完全依赖于密钥的保密性。

考点五 公钥密码的思想

公开密钥的核心思想：**单向陷门函数**
如果函数f(x)被称为单向陷门函数，必须满足以下三个条件

1.给定x，计算y=f(x)是容易的
2.给定y，计算x使y=f(x)是困难的(所谓计算$x = f^{-1}(y)$困难是指计算上相当复杂，已无实际意义)
3.存在 δ ，已知 δ 时对给定的任何y，若相应的x存在，则计算x使y=f(x)是容易的
注:
(1)仅满足1、2条的称为单向函数；第3条称为陷门性， δ 称为陷门信息
(2)
当用陷门函数f作为加密函数时，可将f公开，这相当于公开加密密钥P_k。
f函数的设计者将 δ 保密，用做解密密钥，此时 δ 称为秘密钥匙S_k
由于加密函数是公开的，任何人都可以将信息x加密成y=f(x)，然后发送给函数的设计者。
由于设计者拥有S_k，他自然可以利用S_k求解$x = f^{-1}(y)$。
(3)单向陷门函数的第2条性质表明:窃听者由截获的密文y=f(x)推测x是不可行的。

考点六 离散对数问题

1 素数的原根

若a是素数p的原根，则
1.$a \bmod p, a^2 \bmod p, \ldots\ldots, a^{p-1} \bmod p$ $a^p \bmod p$是不同的
2.包含从1到$p-1$间所有正数的某种排列，
对$\forall b \in Z$，有唯一的i，满足$b \equiv a^i \bmod p, (1 \le i \le p-1)$。
注：$b \equiv a^i \bmod p$　　b等价于$b \bmod p = a^i \bmod p$，称为b与a模p同余。

2 离散对数

若a是系数p的一个原根，则$\forall b \in Z(b \bmod p \neq 0)$，必有在唯一的$i(1 \le i \le p-1)$，$s.t.\ b \equiv a^i \bmod p.$
i 称为b的以a为基数且模p的幂指数，即离散对数

3 求解离散对数

对$y \equiv g^x \bmod p$(g为系数p的原根，x与y均为正整数)，则
1.从g，x，p计算y是容易的
2.从g，y，p计算x是困难的
注：离散对数的求解为数学界公认的困难问题

考点七 Diffie-Hellman密钥交换协议

以按如下步骤来做

1.Alice选取大的随机数x < p，并计算$Y = g^x (mod\ P)$。
2.Bob选取大的随机数$x^{'} < p$，并计算$Y^{'} = g^{x^{'}} (mod\ P)$。
3.Alice将Y传送给Bob，Bob将$Y^{'}$传送给Alice。
4.Alice计算$K^{'} = (Y^{'})^x (mod\ P)$，Bob计算$K = (Y)^{x^{'}} (mod\ P)$
显而易见，$K = K^{'} = g^{xx^{'}} (mod\ P)$，即Alice和Bob已获得了相同的秘密值K。双发以K作为加解密钥，以传统对称密钥算法进行保密通信。

考点八 RSA公钥算法

RSA算法的数学基础是初等数论中的欧拉定理以及大整数因子分解问题。
RSA密码体制是一种分组密码，明文和密文均是0到n之间的整数，n的大小通常为1024位二进制数或309位十进制数，因此，$明文空间P=密文空间C 0 < x < n， Z 为 整 数 集 合 } $

RSA密码的密钥生成具体步骤如下：
1.选择两个互异的素数p和q，计算n=pq，$\phi(n) = (p-1)(q-1)$
2.选择整数e，使$gcd(\phi(n)，\ e) = 1$，$且 1 < e < \phi(n)$
3.计算d，使$d \equiv e^{-1}\ mod\ \phi(n)$，即d为模$\phi(n)$下e的乘法逆元
则公开密钥$P_k = \{e，\ n\}$，私用密钥$S_k = \{d，\ n，\ p，\ q\}$
当明文为m，密文为c，加密时使用公开密钥P_k，加密算法$c = m^e\ mod\ n$
解密时使用私用密钥S_k，$m = c^d\ mod\ n$。故e也被称为加密指数，d被称为解密指数。

考点九 散列函数的特点和作用

散列函数 的目的：将任意长的消息映射成一个固定长度的散列值(Hash值)，也称为消息摘要。消息摘要可以作为认证符，完成消息认证。

1.弱无碰撞性：指在 消息特定的明文空间x 中，给定消息$x \in X$，在计算机上几乎找不到不同于x的$x^{{}, x{ '}\in X， 使得h(x)=h(x^{' })$
2.强无碰撞性：指在计算机上几乎找不到不同于x的$x^{'}$，使得$h(x) = h(x^{'})$，$x^{'}$可以不属于X。
注：强无碰撞自然包含弱无碰撞
3.单向性：指通过h的逆函数h^{-1}来求得散列值h(x)的消息原文x在计算上不可行。

考点十 EMI、EMC、防电磁泄漏主要方法

电磁干扰(EMI)：指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。
防止EMI要从两方面考虑，一方面要减少电子设备的电磁发射，另一方面要提高电子设备的 电磁兼容 性(EMC)。

电磁兼容性(EMC)：指电子设备在自己正常工作时产生的电磁环境，与其他电子设备之间相互不影响的电磁特性。

防电磁信息泄漏的基本思想主要包括三个层面：1.抑制电磁发射 2.屏蔽隔离 3.相关干扰

常用的防电磁泄漏的方法有三种：
1.屏蔽法 - 主要用来屏蔽辐射及干扰信号
2.频域法 - 主要解决正常的电磁发射受干扰问题
3.时域法 - 与频域法相似，时域法也是用来回避干扰信号

考点十一 容错与容灾的概念及主要技术方法

容错基本思想：即使出现了错误，系统也可以执行一组规定的程序；或者说，程序不会因为系统中的故障而中断或被修改，并且故障也不会引起运行错。简单地说，容错就是让系统具有抵抗错误带来的能力。

容错系统可分为五种类型：
1.高可用度系统 2.长寿命系统 3.延迟维修系统 4.高性能系统 5.关键任务系统

常用数据容错技术主要有以下四种：
1.空闲设备 - 当正常运行的部件出现故障时，原来空闲的一台立即替补
2.镜像 - 把一份工作交给两个相同的部件同时进行
3.复现 - 也称延迟镜像，原系统故障时，辅助系统只能在接近故障点的地方开始工作。同一时间只需要管理一套设备
4.负载均衡 - 将一个任务分解成多个子任务，分配给不同的服务器执行。

容灾含义：对偶然事故的预防和恢复

解决方案：
一是对服务的维护和恢复
二是保护或恢复丢失的、被破坏的或被删除的

2.充分利用现有资源
3.既重视灾后恢复也重视灾前措施

考点十二 windows的网络认证

用户登入时的身份认证过程也是采用对称密钥加密来完成的
用户与主域控制器共享口令，在域控制器的安全用户管理(SAM)数据库中保存注册用户的用户名、口令的散列以及其他信息。

用户登录具体过程：
1.用户先激活winlogon窗口，并输入用户名和口令，然后向域控制器发送登录请求，**同时计算出口令的散列**[1]，口令及其散列不包含在登录请求信息中
2.**域控制器**收到登录请求后产生一个8字节的质询(挑战)并发送给客户端，同时**取出给用户的口令散列**[2]**，用此口令散列对质询进行散列计算(也称加密)**
散列。
3.**客户端**收到8字节的质询后，首先**使用前边计算得到的口令散列对质询进行散列计算，得到质询散列**[1]，随后将计算出的质询散列作为应答发送给域控
4.域控制器**比对其算出的质询散列**[2]**和用户应答回送的质询散列**[1]，如果相同则登录认证通过，否则登录认证失败，同时向用户发送登录认证结果。

考点十三 利用公开密钥和对称密钥设计认证协议获得会话密钥

描述符号：

$$A \to B表示A向B发送信息$$
$$E_k(x)表示使用共享密钥k对信息进行加密$$
$$x||y表示信息串x和y相连接$$

1 基于对称密钥的认证协议

只有少量用户的封闭网络系统，使用挑战-应答方式认证
对于规模较大的网络系统，依靠可靠的第三方完成认证

基于挑战应答方式的认证协议：

$$1.A \to B : ID_a||ID_b$$
$$2.B \to A : Nb$$
$$3.A \to B : E_k(Nb)$$

2 基于公开密钥的认证协议

A要认证B，有以下两种方式：
（1）方式1

1. A向B发送明文挑战(挑战因子/随机数)
2. B用私钥加密(签名)，返回给A
3. A用B的公钥解密，比对，完成认证

（2）方式2

1. A用B的公钥加密挑战因子(或随机数)发送给B
2. B用私钥解密，返回明文给A
3. A比对，完成认证

考点十四 Kerberos工作原理

Kerberos协议的认证过程分为三个阶段，六个步骤
第一阶段 身份验证服务交换：完成身份认证，获得访问TGS的票据
步骤(1)为请求TGS票据
步骤(2)为返回TGS票据

$$(1)C \to AS : ID_C||ID_{tgs}||TS_1$$
$$(2)AS \to C : E_{KC}[K_{C,tgs}||ID_{tgs}||TS_2||Lifetime_2||Ticket_{tgs}]$$

ID_{tgs}：用请求访问的TGS的标识
TS_1：让AS验证$Client\ C$的时钟是与AS的时钟是否同步的

E_{KC}：基于用户口令的加密，使得AS和$ClientC$可以验证口令，并保护消息
$K_{C,tgs}$：由AS产生，用于在TGS和$ClientC$之间信息的安全交接
ID_{tgs}：确认这个$ticket$是为特定TGS制作的
TS_2：告诉用户该$ticket$签发的时间
$Lifetime_2$：告诉用户该$ticket$的有效期
$Ticket_{tgs}$：用户用来访问TGS的$ticket$，可重用，避免多次认证输入口令，其中，
$Ticket_{tgs} = E_{Ktgs}[K_{C,tgs}||ID_c||AD_C||ID_{tgs}||TS_2||Lifetime_2]$

第二阶段 票据授予服务交换：获得访问应用服务器的票据。
步骤(3)为请求应用服务器票据
步骤(4)为返回应用服务器票据

$(3)C \rightarrow TGS: ID_V||Ticket_{tgs}||Authenticator_C$
$(4)TGS \rightarrow C: E_{K_{C,tgs}}[K_{C,V}||ID_V||TS_4||Ticket_V]$
注：步骤(3)为请求应用服务器票据
ID_V：告诉TGS用户要访问应用服务器V
$Ticket_{tgs}$：向TGS证实该用户已被AS认证
$Authenticator_C$：由用户生成，用于验证时效性
$Authenticator_C = E_{K_{C,tgs}}[ID_C||AD_C||TS_3]$
$E_{K_C,tgs}[]$：使用$ClientC$和TGS共享的密钥加密，用以保护本消息
$K_{C,V}$：由TGS生成，用于$ClientC$和$ServerV$之间信息的安全交换;
ID_V：确认该$ticket$是签发给$setcer\ V$的
TS_4：告诉用户该$ticket$签发的时间
$Ticket_V$：用户用以访问应用服务器V的$ticket$，其中，
$Ticket_V = E_{KV}[K_{C,V}||ID_C||AD_C||ID_V||TS_4||Lifetime_4]$
$E_{K_V}[]$：$Ticket$用只有TGS和$ServerV$共享的密钥加密，以预防篡改

第三阶段 客户与服务器身份验证交换：获得服务步骤
步骤(5)为向应用服务器发起服务请求。
步骤(6)为服务器对客户机可选的身份认证

$(5)C \rightarrow V: Ticket_V||Authenticator$
$(6)V \rightarrow C: E_{K_{C,V}}[TS_5 + 1](for\ mutual\ authentication)$

$Ticket_V$：向服务器证实该用户已被AS认证
$Authenticator_C$：由$ClientC$生成用于验证时效性
$Authenticator_C = E_{K_{C,V}}[ID_C||AD_C||TS_5]$
$E_{K_{C,V}}[]$：使用$ClinetC$和$ServerV$的共享密钥加密，来验证身份并保护本信息

$TS_5 + 1$：向$ClientC$证明这不是重放攻击的应答

考点十五 PKI的体系结构及工作原理

公钥基础设施(PKI)采用数字证书技术来管理公钥，通过第三方的可信任机构——CA认证中心把用户的公钥和用户的其他标识信息捆绑到一起，在互
用户的身份。
在PKI的组成结构中，处在中心位置的是构建PKI的核心技术，即公钥算法和数字证书技术，在此技术基础上实现的PKI平台包括四个基本功能模块和
口模块。

1.认证机构CA：CA是PKI的核心执行机构，也称为认证中心。其主要功能包括数字证书的申请注册、证书签发和管理。

2.证书库：证书库是CA颁发证书和撤销证书的集中存放地，它像网上的“白页”一样，是网上的公共信息库，可供公众进行开放式查询。

4.证书撤销处理：被撤销的CA证书将进入证书库的"黑名单"，用于公众来核实证书的有效性。

5.PKI应用接口：PKI应用接口使使用者与PKI交互的唯一途径，PKI应用接口也可以看成是PKI的客户端软件。

考点十六 访问控制的概念

访问控制：是针对越权使用资源的防御措施，从而使系统资源在合法范围内使用。

访问控制的基本组成元素：
1.主体 - 值提出访问请求的实体，主体是动作的发起者，但不一定是动作的执行者，可以是用户或其他代理用户行为的实体(如进程、作业和程序等)
2.客体 - 是指可以接受主体访问的被动实体。凡是可以被操作的信息、资源、对象都可以认为是客体。
3.访问控制策略 - 指主体对客体的操作行为和约束条件的关联集合

考点十七 DAC、MAC、RBAC的工作原理及特点

自主访问控制DAC
自主访问控制(DAC):允许合法用户以用户或用户组的身份来访问系统控制策略许可的客体，同时阻止非授权用户访问客体，某些用户还可以自主地把的客体的访问权限授予其他用户。
实现上：首先要对用户的身份进行鉴别，然后就可以按照访问控制列表所赋予用户的权限允许或限制用户访问客体资源。主体控制权限的修改通常由特权用户组实现。

强制访问控制MAC
强制访问控制(MAC)：系统事先给访问主体和受控客体分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控客体的安全级别属性再决定访问主体能否访问该受控客体。
主体对客体的访问可以分为以下四种形式：
1.向下读 2.向上读 3.向下写 4.向上写
向下读向上写，防止机密信息向下级泄露，保护机密性
向上读向下写，保护数据的完整性

基于角色的访问控制RBAC
组：具有相同性质(访问权限)的用户集合
角色：一个与特定行为关联的行为与责任的集合
RBAC思想：将访问权限分配给角色，用户饰演角色获得访问许可权。一个用户可当多个角色

考点十八 Windows安全体系结构、活动目录与组策略

整个安全架构的核心是安全策略，完善的安全策略决定了系统的安全性。Windows系统的安全策略明确了系统各个安全组件如何协调工作。

Windows系统安全开始于用户认证，它是其他安全机制能够有效实施的基础，处于安全框架的最外层。

加密和访问控制处于用户认证之后，是保证系统安全的主要手段，加密保证了系统与用户之间的通信及数据存储的机密性；访问控制则维护了用户访则。

审计和管理处于系统的内核层，负责系统的安全配置和事故处理，审计可以发现系统是否曾经遭受过攻击或者正在遭受攻击，并进行追查；管理则是控制系统提供功能接口。

活动目录(AD)存储了有关网络对象的信息，并且让管理员和用户能够轻松地查找和使用这些信息。

组策略(GP)是AD安全性地重要体现，可理解为依据特定地用户或计算机地安全需求定制地安全配置规则

考点十九 传统病毒、蠕虫、木马的结构原理

传统病毒一般由三个主要模块组成，包括启动模块、传染模块和破坏模块。当系统执行了感染病毒地文件时，病毒的启动模块开始驻留在系统内存中和破坏模块的发作均为条件触发，当满足了传染条件，病毒开始传染别的文件；满足了破坏条件，病毒就开始破坏系统。

蠕虫病毒一般不需要寄生在宿主文件中，这一点与传统病毒存在差别，蠕虫病毒具有传染性，它是通过在互联网环境下复制自身进行传播。蠕虫病毒是互联网内的所有计算机，传播途径主要包括局域网内的共享文件夹、电子邮件、网络中的恶意网页和大量存在着漏洞的服务器等。
可以说蠕虫病毒是以计算机为载体，以网络为攻击对象。

木马是有隐藏性的、传播性的、可被用来进行恶意行为的程序。木马一般不会直接对计算机产生危害，主要以控制计算机为目的。
木马的传播方式主要通过电子邮件附件、被挂载木马的网页以及捆绑了木马程序的应用软件。
木马被下载后完成修改注册表、驻留内存、安装后门程序、设置开机加载等，甚至能够使杀毒程序、个人防火墙等防范软件失效。

考点二十 拒绝服务攻击、缓冲区溢出、

通常拒绝服务攻击可分为两种类型：
第一类是利用网络协议的缺陷，通过发送一些非法数据包致使主机系统瘫痪，如Ping of Death；
第二类攻击是通过构造大量网络流量致使主机通信或网络堵塞，使系统不能相应正常的服务，如Smurf。

缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖了合法数据。利用缓冲区溢出攻击，可以导致程序运行统宕机、重新启动等后果，更为严重的是可以利用它执行非授权指令，甚至可以取得系统特权并控制主机，进行各种非法操作。

考点 防火墙主要技术概述

依据防火墙的技术特征，常见的防火墙可以分为包过滤防火墙、代理防火墙和个人防火墙。

包过滤防火墙是面向网络底层数据流进行审计和控管，因此其安全策略主要根据数据包头的源地址、目的地址、端口号和协议类型等标志来指定，可作在网络层和传输层。

代理防火墙是基于代理(Proxy)技术，使防火墙参与到每一个内、外网络之间的连接过程，防火墙需要理解用户使用的协议，对内部节点向外部节点的原审查后，转发给外部服务器；外部节点发送来数据也需要进行还原审查，然后封装转发给内部节点。
代理防火墙主要工作在应用层，有时也称为应用级网关。

个人防火墙使目前普通用户最常用的一种。个人防火墙是一种能保护个人计算机系统安全的软件，它可以直接在用户的计算机上运行，有效地帮助普统进行监控及管理，使个人计算机免受各种攻击

考点 基于网络和基于主机的入侵检测系统的优缺点

入侵检测系统术语

警报
IDS向系统操作人员发出入侵正在发生或正在尝试进行的消息。
异常
用一段时间建立一个主机或者网络活动的轮廓。当一个用户行为或者网络行为与此轮廓距离超过某一个值的时候，需要发出警报，此行为称之为异常
网络入侵特征数据库
将网络入侵行为抽象成特定的字符集和，通过与网络上或主机上的行为向匹配，发现可能的网络入侵。是基于误用检测系统的重要组成部分。
蜜罐（Honeypot）
模拟存在漏洞的系统，为攻击者提供攻击目标。其在网络中没有任何用途，因此任何连接都是可能的攻击。
诱惑攻击者在上面浪费时间，延缓对真正目标的攻击自动响应
一些IDS能够对攻击做出防御性反应
- 重新配置路由器或者防火墙，拒绝来自相同地址的流量
- 发送reset包切断连接攻击者可以通过信任地址实施攻击，引起设备重新配置，达到拒绝服务攻击的目的

考点snorts的工作原理

Snort系统简介
Snort采用基于规则的网络信息搜索机制，对数据包进行内容的模式匹配，从中发现入侵和探测行为。

编写Snort的规则
snort的每条规则都可以分成逻辑上的两个部分：规则头和规则选项
规则头包括：规则行为(rule‘s action)、协议(protocol)、源/目的IP地址、子网掩码以及源/目的端口。
规则选项包含报警信息和异常包的信息(特征码，signature)，使用这些特征码来决定是否采取规则规定的行动。

考点IPSEC协议的体系结构

IPSec基本要件
ESP和AH的有效工作依赖于四个要件。
加密算法、认证算法、解释域DOI（Domain of Interpretation）以及密钥管理。

包括**两个基本协议**，分别封装安全有效负荷协议（ESP）和认证头协议（AH）。这两个协议的有效工作依赖于四个要件，分别为加密算法，认证算法及密钥管理。

IPSec的工作模式
IPSec 标准定义了 IPSec 操作的两种不同模式：传输模式（Transport Mode）和隧道模式（Tunnel Mode）
安全协议AH和ESP，都可以以这两种模式工作。

考点传输方式和隧道方式的区别

部，IPSec头部被放置在新产生的IP头部和以前的IP数据包之间，从而组成一个新的IP头部。

考点SSL握手协议

报文格式：类型（1），长度（3），内容（>=1）

通过在客户端和服务器之间传递消息报文，完成协商谈判。

四个阶段：建立起安全能力；服务器认证与密钥交换；客户端认证与密钥交换；结束；

考点双签名技术原理

将OI与PI这两个部分的摘要绑定在一起，确保交易的有效性与安全性。同时分离OI与PI，确保商家不知道顾客的支付卡信息，银行不知道顾客的订购

双重签名的使用过程

顾客针对PI和OI生成DS，将DS、OI和PIMD发送给商家，商家计算得到POMD=H（PIMD IIH（OI）），然后计算POMD’ =DKUc [DS]，其中KU
公开密钥。如果POMD= POMD’ ，则商家可以认为该DS正确，批准实施进一步交易
顾客需要生成一个对称密钥KS，使用银行的公钥加密KS，并使用KS加密DS、PI和OIMD，通过商家将EKUb
[KS]IIEKs[DS || PI IIOIMD]转发给银行其中KUb为银行的公开密钥银行计算POMD=H（H（PI）II OIMD）和POMD’ =DKUc [DS]，如果POMD
POMD’ ，则银行可以认为该DS正确，批准实施交易。

考点DRM结构原理

分为服务器和客户端两个部分。服务器主要功能是管理版权文件的分发与授权。客户端的主要功能是依据受版权保护文件提供的信息申请授权许可证
权许可信息解密受保护文件，提供给客户使用。

考点数字水印的工作原理

考点cc与bs7799的区别

cc是目前最全面的评价准则，充分突出了“保护轮廓”的概念，侧重点放在系统和产品的技术指标评价上。

Bs7799采用层次化形式定义了11个安全管理要素，还给出了39个主要执行目标和133个具体控制措施，明确了组织机构信息安全管理建设的内容。

考点 风险评估的主要方法

基线评估

详细评估

组合评估

考点 网络安全法（非教材）

2016年11月7日通过

2017年6月1日起施行

考点 等级保护2.0（非教材）

2019年5月13日，网络安全等级保护制度2.0标准正式发布，同时这些标准将于12月1日正式实施，我国迈入2.0时代。

考点 工程伦理道德

要有工程伦理道德。

linux天门 高频命令大全_linux高频命令汇总_大全中会飞的鱼的博客-CSDN...
-G或--no-group 不显示群组名称。 -h或--human-readable 用"K","M","G"来显示文件和目录的大小。 -H或--si 此参数的效果和指定"-h"参数类似,但

密码学基础课后题 qq_44669801的博
密码学基础课后题

单链表（数组模拟：静态链表） weixin_52621900的
单链表 实现一个单链表，链表初始为空，支持三种操作： 向链表头插入一个数； 删除第 kk 个插入的数后面的数； 在第 kk 个插入的数后插入一个数。 现在要对该链表进

【精选】Intel Memory-Management Registers_lldt指令
一、Memory-Management Registers 1.1 Global Descriptor Table Register (GDTR) 1.2 Local Descriptor Table Register (LDTR) 1.3 IDTR Interrupt Descriptor Tab

深度学习(25)——YOLO系列(4)
batch_size=min(batch_size,len(dataset))nw=min([os.cpu_count()//world_size,batch_sizeifbatch_size>1else0,workers])# number of workerssampler=torch.utils

哈工大信息安全概论复习3 qq_45599206的
信息安全概论考点18-25十八、Windows安全体系结构、活动目录与组策略1、Windows系统安全体系结构二级目录三级目录 十八、Windows安全体系结构、活动目录与

哈工大信息安全概论期末知识点总结 cswenboli的博
1、信息安全体系架构:信息安全通常强调所谓的CIA三元组，实际上是信息安全的三个基本目标，即机密性（C）、完整性（I）和可用性（A）机密性是指信息在存储、传

评价入侵检测系统漏洞攻击检测覆盖面的指标_漏洞数量指标
因此通过统计产品相关的CVE条目数量可以大致了解IDS/IPS的漏洞攻击检测覆盖面。我们最原始的评价指标可以是产品相关的CVE漏洞条目个数。 1.2 CVSS漏洞威胁评分

基于网络的入侵检测数据集研究综述(A Survey of Network-based Intru...
是(IDS)意味着某种入侵检测系统被用来创建数据集的标签。由于IDS可能不完美,数据集的一些标签可能是错误的。间接的意思是数据集没有显式的标签,但是标签可以自己

哈工大网络信息安全课件
哈工大网络信息安全课件，介绍信息安全体系架构，物理安全、运行安全和数据安全等。

信息安全概论复习课件
哈工大信息安全概论复习课件，完全是老师划得重点，需要认真背，不说一定都考，但是考点都在。

宽度优先搜索算法实现8数码_经典搜索算法总结_凌沦的博客
迭代加深搜索IDS 双向搜索BS 有信息搜索算法 贪心搜索 A* 搜索 迭代最佳优先搜索RBFS 启发式设计 搜索算法的背景和定义 首先,搜索算法可以分为树搜索和图搜索。 简

某直播弹幕web端js逆向分析---protobuf实战及工具介绍_princezyj的博...
前面的文章应该可以让大家掌握好protobuf吧,只要抓住关键词就行了。前面文章我也提到了某音直播弹幕也是采用protobuf格式传输的,那我们这篇文章就来看看,实

信息安全概论考试重点
从方勇老师的课件里整理出来的考试重点资料。

信息安全概论 pdf
信息安全概论 缩水版 考试专用 pdf 很不错的资料哦..老师考前给的..

Redis 笔记 最新发布 一条菜鸟鱼的
1 redis 概述 redis是一款高性能的NOSQL系列的非关系型数据库 1.1 NOSQL 是什么 NoSQL(NoSQL = Not Only SQL)，意即“不仅仅是SQL”，是一项全新的数据库理

哈工大信息安全概论复习笔记2 qq_45599206的
信息概论考点9-17九、散列函数的特点和作用十、EMI、EMC、防电磁泄漏主要方法十一、容错与容灾的概念及主要技术方法1、容错2、容灾十二、windows的网络认证

哈工大信息安全概论复习笔记(3) www01000134的博
哈工大信息安全概论复习笔记（3） 考点十五 PKI的体系结构及工作原理 公钥基础设施(PKI)采用数字证书技术来管理公钥，通过第三方的可信任机构——CA认证中心把用

信息安全概论(期末知识点复习) qiqi_liuliu的
自己复习用的噢 可能比较乱

哈工大信息安全概论期末复习 何以牵尘的博
根据韩琦老师的期末复习提纲（2022）写出本篇博客进行相应内容的总结，希望对本届及下一届学子有所帮助，准备不周，如有谬误，还请指正，谢谢！

哈工大网络安全课程
哈工大网络安全课件，授课教师王彦，重点复习ppt，考试题所有的内容都来自于此ppt，考试内容有填空题，名词解释和分析题，考研党必备，只要考试前看这一个ppt

信息安全概论 第三版 牛少彰 习题答案.doc
信息安全概论 牛少彰 第三版课后习题答案

哈工大信息安全概论作业合集.zip
哈工大信息安全概论作业合集.zip

《信息安全概论》习题集
简述主动攻击与被动攻击的特点，并列举主动攻击与

MarcyTheLibrarian VIP
码龄2年 暂无认证

118	7万+	3万+	13万+	
原创	周排名	总排名	访问	等级

1313	30	93	17	426
积分	粉丝	获赞	评论	收藏

私信 关注

搜博主文章

热门文章

Visual Studio如何打开项目 17069
git 报错信息：Failed to connect to github.com port 443: Timed out 10137
实现VirtualBox、VMware和Windows之间的复制黏贴操作 8707
在虚拟机安装JDK 4489
ulimit: open files: cannot modify limit: Operation not permitted 3388

分类专栏

软件使用 7篇
git使用 7篇
pgsql 13篇
文档编辑 8篇
图大数据 2篇
openGauss 2篇

最新评论

一串代码<!--{C}%3C!%2D%2D%20%2 ...

Typora配置PicGo提示Failed to fetch问...
头盔护发大使: 实测解决问题

Visual Studio如何打开项目
动名词: 嘿 哥们 别和优越感沾边，能解读到优越感 只能说你想象力丰富了

Visual Studio如何打开项目
〖雪月清〗: 这为啥不能写成博客，博客本来就是相当于社区，大家分享收获、解决 ...

Typora配置PicGo提示Failed to fetch问...
z5558888666: 实测解决问题

最新文章

Anaconda安装pytorch-cuda

Git教程

PostgreSQL常用配置参数【一表说明】

2023年 29篇 2022年 90篇

目录

说在前面的话

2022年春季考试的分值分布

考点一 信息安全架构

1 面向目标的知识体系结构

2 面向应用的层次型技术架构

3 面向过程的信息安全保障体系

4 OSI开放系统互联安全体系结构

考点二 密码体制的五要素

考点三 仿射密码

考点四 数据加密标准DES的算法结构和...

1 S-DES(简化DES)算法结构:

2 DES的特点

考点五 公钥密码的思想