棱镜计划的爆料人是（）。

A.

爱德华·斯诺登

B.

朱利安·阿桑奇

C.

劳拉·珀特阿斯

D.

乔治·布什

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

2013年6月，斯诺登披露了美国国家安全局关于棱镜计划PRISM的监听项目秘密文档，该项目直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报包括微软、雅虎、谷歌、苹果等在内的9家国际网络巨头都参与其中

教师评语：

暂无

2.

习近平主席在2014年提出：没有（）就没有国家安全。

A.

互联网

B.

信息安全

C.

网络安全

D.

基础网络

满分：20.00 分

得分：20.00 分

你的答案：

C

正确答案：

C

答案解析：

习近平主席在2014年2月的《在中央网络安全和信息化领导小组第一次会议上的讲话》中指出：没有网络安全就没有国家安全，没有信息化就没有现代化。

教师评语：

暂无

二、多选题 (共 40.00 分)

1.

信息系统资源安全的基本属性包括（）。

A.

保密性

B.

完整性

C.

可用性

D.

可控性

E.

不可抵赖性

满分：20.00 分

得分：20.00 分

你的答案：

A B C D E

正确答案：

A B C D E

答案解析：

信息系统资源安全的五个基本属性：保密性；完整性；可用性；可控性；不可抵赖性

教师评语：

暂无

2.

不可抵赖性是指（）。

A.

信息的接收者无法否认已经接收的信息

B.

信息的接收者无法解密信息

C.

信息的发送者无法加密信息

D.

信息的发送者无法否认已发出的信息

满分：20.00 分

得分：20.00 分

你的答案：

A D

正确答案：

A D

答案解析：

不可抵赖性通常又称为不可否认性，是指信息的发送者无法否认已发出的信息，信息的接收者无法否认已经接收的信息

教师评语：

暂无

三、判断题 (共 20.00 分)

1.

网站被篡改是破坏了计算机系统安全的保密性（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

B

正确答案：

B

答案解析：

网站被篡改是破坏了计算机系统安全的完整性；保密性是确保信息不暴露给未授权的实体或进程，主要是采用加密机制，即防泄密

教师评语：

暂无

对称加密方案中需要保持私密的是（）。

A.

加密算法

B.

解密算法

C.

密钥

D.

密文

满分：25.00 分

得分：25.00 分

你的答案：

C

正确答案：

C

答案解析：

密钥即发送方和接收方使用的秘密信息，从而实现加密和解密功能

教师评语：

暂无

2.

根据使用的密钥数，密码可以分为对称密码和（）。

A.

替换密码

B.

分组密码

C.

公钥密码

D.

流密码

满分：25.00 分

得分：25.00 分

你的答案：

C

正确答案：

C

答案解析：

非对称加密又称公钥密码，即发送者和接收者使用不同的密钥进行加密和解密。

教师评语：

暂无

二、多选题 (共 25.00 分)

1.

密码体制根据明文转换成密文的操作类型可将密码分为以下三类（）。

A.

替换密码

B.

换位密码

C.

私钥密码

D.

乘积密码

满分：25.00 分

得分：25.00 分

你的答案：

A B D

正确答案：

A B D

答案解析：

根据明文转换成密文的操作类型可将密码分为以下三类：第一类是替换密码,即每一个元素、比特或者字母都映射到另一个元素；第二类是换位密码，即所有元素都被重新再排列；第三类是乘积密码，即包括了多级替换和换位组合的密码。

教师评语：

暂无

三、判断题 (共 25.00 分)

1.

使用对称加密算法时，发送方需要将密钥安全地发送给接收方（）。

A.

正确

B.

错误

满分：25.00 分

得分：25.00 分

你的答案：

A

正确答案：

A

答案解析：

一般来说，对称加密算法是公开的，只要求密钥保持私密性因此需要存在一个安全的通道去分发密钥。

教师评语：

暂无

在密码分析中，攻击者掌握信息最少的攻击方式是（）。

A.

已知明文攻击

B.

唯密文攻击

C.

选择明文攻击

D.

选择密文攻击

满分：16.00 分

得分：16.00 分

你的答案：

B

正确答案：

B

答案解析：

已知明文攻击是指攻击者掌握了某段明文 x 和对应密文 y；唯密文攻击是指在仅知已加密文字（即密文）的情况下进行攻击；选择明文攻击指攻击者掌握对加密机的访问权限，可构造任意明文所对应的密文；选择密文攻击指攻击者掌握对解密机的访问权限，可构造任意密文所对应的明文。可以看出唯密文攻击中，攻击者只掌握了密文，信息量最少。

教师评语：

暂无

2.

如果使用凯撒密码对“szu”进行加密，其得到的密文为（）。

A.

ucx

B.

vcx

C.

ucw

D.

vcw

满分：16.00 分

得分：16.00 分

你的答案：

B

正确答案：

B

答案解析：

凯撒密码是最早的替换密码，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文，一般移动3位，即s->v，z->c，u->x。

教师评语：

暂无

3.

当密钥空间为10bit时，总共有多少种密钥（）。

A.

256

B.

512

C.

1024

D.

2048

满分：16.00 分

得分：16.00 分

你的答案：

C

正确答案：

C

答案解析：

密钥空间为10bit，即2的10次方=1024。

教师评语：

暂无

4.

如果使用栅栏密码对“helloworld”进行加密，其得到的密文为（）。

A.

hloolewlrd

B.

holollewrd

C.

hololelwrd

D.

hloolelwrd

满分：16.00 分

得分：16.00 分

你的答案：

D

正确答案：

D

答案解析：

栅栏密码也称栅栏易位，即把将要传递的信息中的字母交替排成上下两行，再将下面一行字母排在上面一行的后边，从而形成一段密码。

教师评语：

暂无

5.

对维吉尼亚密文“zdfdnqgqfv”进行解密，密钥为“szu”，原文为（）。

A.

helloworld

B.

happyworld

C.

university

D.

educations

满分：16.00 分

得分：16.00 分

你的答案：

A

正确答案：

A

答案解析：

可使用维吉尼亚密码表格查表解密，或网页在线解密。

教师评语：

暂无

二、多选题 (共 20.00 分)

1.

当密文满足下面哪些条件时则称该加密方案是计算安全的（）。

A.

破译密文的代价小于被加密信息的价值

B.

破译密文的代价超出了被加密信息的价值

C.

破译密文的时间超出信息的有效生命期

D.

破译密文的时间小于信息的有效生命期

满分：20.00 分

得分：20.00 分

你的答案：

B C

正确答案：

B C

答案解析：

当加密方案产生的密文满足下面条件之一时则称该加密方案是计算安全的：第一是破译密文的代价超出了被加密信息的价值；第二次，破译密文的时间超出信息的有效生命期。

教师评语：

暂无

DES算法属于（）。

A.

对称加密

B.

不对称加密

C.

不可逆加密

D.

以上都不是

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

DES算法为密码体制中的对称密码体制，又被称为美国数据加密标准。

教师评语：

暂无

二、判断题 (共 80.00 分)

1.

DES算法不易遭受穷举搜索攻击（）。

A.

正确

B.

错误

满分：40.00 分

得分：40.00 分

你的答案：

B

正确答案：

B

答案解析：

在有限时间内使用超算技术可以穷举搜索56比特密钥的所有组合。

教师评语：

暂无

2.

3DES就是执行三重DES算法（）。

A.

正确

B.

错误

满分：40.00 分

得分：40.00 分

你的答案：

A

正确答案：

A

答案解析：

3DES就是执行三重DES算法，使用三重DES加密一般需要三个不同密钥，但也可以在E-D-E，即加密、解密、加密的序列下使用两个密钥。

教师评语：

暂无

AES算法中，密钥长度不同，推荐加密轮数不同（）。

A.

正确

B.

错误

满分：100.00 分

得分：100.00 分

你的答案：

A

正确答案：

A

答案解析：

AES-128使用10轮加密，AES-192使用12轮加密，AES-256使用14轮加密。

教师评语：

暂无

使用电子密码本与密码分组链接模式时，每个明文分组Pi与前一分组的密文Ci进行（）操作。

A.

与非

B.

或非

C.

异或

D.

同或

满分：100.00 分

得分：100.00 分

你的答案：

C

正确答案：

C

答案解析：

每个明文分组Pi与前一分组的密文Ci进行异或后再进行加密。

教师评语：

暂无

对于相同的密文、密钥和偏移量，使用不同的分组加密模式得到的密文相同（）。

A.

正确

B.

错误

满分：100.00 分

得分：100.00 分

你的答案：

B

正确答案：

B

答案解析：

由不同的分组加密过程可知，密文不同，也可以去在线网站实际测试。

教师评语：

暂无

以下哪种WIFI加密算法最不安全（）。

A.

WEP

B.

WPA

C.

WPA2

D.

EAP

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

WEP协议的在数据传输时，对数据的加密和解密都使用同样的算法和密钥，使用了RC4作为流加密协议，用于生成密钥流的初始向量IV是明文的方式。而该向量只有24位，这就使得在2^24个数据包后至少出现一次重复IV值，并且在实际中IV值重复的概率远远大于1/2^24，因而攻击者可轻易暴力破解获取IV。

教师评语：

暂无

二、多选题 (共 40.00 分)

1.

关于无线WEP流密码算法，以下那一个说法是正确的（）。

A.

WEP未有破解方法

B.

WEP已有破解方法

C.

WEP使用了RC4算法

D.

WEP是一种对称密钥机制

满分：40.00 分

得分：40.00 分

你的答案：

B C D

正确答案：

B C D

答案解析：

WEP协议的在数据传输时，对数据的加密和解密都使用同样的算法和密钥，使用了RC4作为流加密协议，用于生成密钥流的初始向量IV是明文的方式。而该向量只有24位，这就使得在2^24个数据包后至少出现一次重复IV值，并且在实际中IV值重复的概率远远大于1/2^24，因而攻击者可轻易暴力破解获取IV。

教师评语：

暂无

三、判断题 (共 30.00 分)

1.

只要知道伪随机数的种子与生成算法，就可以预测随机数（）。

A.

正确

B.

错误

满分：30.00 分

得分：0 分

你的答案：

B

正确答案：

A

答案解析：

对于没有真随机源的伪随机数发生器，知道种子是可以预测随机数的。

教师评语：

暂无

公钥体制RSA的安全性是基于（）。

A.

背包算法

B.

离散对数

C.

椭圆曲线算法

D.

大整数因子分解

满分：33.34 分

得分：33.34 分

你的答案：

D

正确答案：

D

答案解析：

在生成私钥时需要两个大素数相乘得到N，若无法将大整数N分解，则无法找到N的欧拉函数，则无法找到N的模反元素，则无法解密密文。

教师评语：

暂无

2.

关于RSA算法的说法不正确的是（）。

A.

RSA算法是一种对称加密算法

B.

RSA算法的运算速度比DES慢

C.

RSA算法可用于某种数字签名方案

D.

RSA的安全性主要基于大整数因子分解的难度

满分：33.33 分

得分：33.33 分

你的答案：

A

正确答案：

A

答案解析：

RSA算法是一种非对称加密算法，即加密和解密使用不同的密钥。另外RSA加解密时是需要进行次幂运算，故速度比DES慢。

教师评语：

暂无

3.

公钥密码是指（）。

A.

对称密钥技术，有1个密钥

B.

不对称密钥技术，有2个密钥

C.

对称密钥技术，有2个密钥

D.

不对称密钥技术，有1个密钥

满分：33.33 分

得分：33.33 分

你的答案：

B

正确答案：

B

答案解析：

非对称加密算法，即加密和解密使用不同的2个密钥。

教师评语：

暂无

攻击者如果拦截了公钥,随后将这个公钥记录并替换为自己的公钥再发送给接收方，这种攻击属于（）。

A.

重放攻击

B.

Smurf攻击

C.

字典攻击

D.

中间人攻击

满分：50.00 分

得分：50.00 分

你的答案：

D

正确答案：

D

答案解析：

中间人攻击(MITM)的方法不能破译RSA，但却是一种针对机密性的有效攻击。就是主动攻击者混入发送者和接收者中间，对发送者伪装成接收者，对接收者伪装成发送者的攻击方式。

教师评语：

暂无

二、多选题 (共 50.00 分)

1.

关于Shamiar秘密共享方法，需要收集多少人才可以恢复数据（）。

A.

t-2

B.

t-1

C.

t

D.

t+1

满分：50.00 分

得分：50.00 分

你的答案：

C D

正确答案：

C D

答案解析：

需要收集t个人及以上的数据，带入求解多项式系数，才可以得出秘密K。

教师评语：

暂无

在数字签名中，消息的发送方使用( )进行数字签名。

A.

接收方公钥

B.

接收方私钥

C.

发送方公钥

D.

发送方私钥

满分：20.00 分

得分：20.00 分

你的答案：

D

正确答案：

D

答案解析：

数字签名技术中，发送方使用自己的私钥进行数字签名。

教师评语：

暂无

2.

关于单向散列函数，下面说法错误的是（）。

A.

能处理任意大小的信息，其生成的信息摘要数据块总是具有固定的大小

B.

对相同的源数据执行该函数得到的信息摘要相同

C.

生成的信息摘要是不可预见的，原始数据的一个微小变化都会对新产生的信息摘要产生很大的影响

D.

具有可逆性，可以通过信息摘要重新生成原始数据信息

满分：20.00 分

得分：20.00 分

你的答案：

D

正确答案：

D

答案解析：

数字签名技术中，发送方使用自己的私钥进行数字签名。

教师评语：

暂无

二、多选题 (共 60.00 分)

1.

关于数字签名，下面说法正确的是（）。

A.

数字签名技术能够保证信息传输过程中的安全性

B.

数字签名技术能够保证信息传输过程中的完整性

C.

数字签名技术能够对发送者的身份进行认证

D.

数字签名技术能够防止交易中抵赖的发生

满分：30.00 分

得分：0 分

你的答案：

C D

正确答案：

B C D

答案解析：

数字签名可以提供以下功能：验证作者签名日期和时间，实现不可否认性功能；可以验证消息内容，实现完整性检查功能；可以通过第三方认证解决纠纷，实现公开验证性功能，防止交易中抵赖的发生。但不能保证传输过程中的安全性，仍需要进行加密传输。

教师评语：

暂无

2.

常用的散列算法有（）。

A.

MD4

B.

MD5

C.

SHA1

D.

SHA256

满分：30.00 分

得分：30.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

MD4 MD5 fAA1 SHA256 均是常见的散列算法，又称数据摘要算法，也称哈希算法（HASH）。

教师评语：

暂无

关于消息认证的叙述，下面说法错误的是( )。

A.

消息认证又称为完整性校验，在OSI安全模型中称为封装

B.

消息认证就是接收者能够检验收到的消息是否真实的方法

C.

消息认证使接收者能识别信息源、内容的真伪、时间性和确定的信息

D.

认证在相互通信的双方进行，是一种实时认证

满分：32.50 分

得分：32.50 分

你的答案：

D

正确答案：

D

答案解析：

消息认证不一定是实时的，如存储系统或电子邮件系统

教师评语：

暂无

2.

关于消息认证，下面不属于检验内容的是( )。

A.

消息的内容是否保持其完整性

B.

消息的序号和时间性

C.

证实消息的信源和信宿

D.

消息是否已被窃取

满分：32.50 分

得分：32.50 分

你的答案：

D

正确答案：

D

答案解析：

消息认证不可检验消息是否被窃取，但可以验证是否被篡改。

教师评语：

暂无

二、多选题 (共 35.00 分)

1.

采用散列函数实现的认证码有（）。

A.

HMAC

B.

CMAC

C.

CCM

满分：35.00 分

得分：35.00 分

你的答案：

A B C

正确答案：

A B C

答案解析：

HMAC CMAC CCM均为常见的消息认证码算法。

教师评语：

暂无

关于Kerberos，下面说法错误的是（）。

A.

Kerberos使用公钥加密机制

B.

Kerberos可用于分布式环境中

C.

Kerberos不需要新人所有工作器

D.

Kerberos需要所有人信任一个中央认证服务器

满分：50.00 分

得分：50.00 分

你的答案：

A

正确答案：

A

答案解析：

Kerberos依赖于对称加密机制，不使用公钥加密机制。

教师评语：

暂无

二、判断题 (共 50.00 分)

1.

使用Kerberos时，要求各服务器上的时间一致（）。

A.

正确

B.

错误

满分：50.00 分

得分：50.00 分

你的答案：

A

正确答案：

A

答案解析：

Kerberos需要使用到包含同步时钟，故需要时间一致。

教师评语：

暂无

关于联合身份管理的叙述，下面说法正确的是（）。

A.

联合身份管理可以达到单点登陆随意通行的目的

B.

用户可以在此信任域中对不同身份进行联合或解除联合

C.

安全域之间相互自主或独立没有中央控制

D.

Identity 2.0是对一类用户为中心支持跨域的身份认证机制的泛称

满分：100.00 分

得分：100.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

联合身份管理是一个通用身份管理框架，所有选项均正确。

教师评语：

暂无

下列哪些措施可以提高无线安全防护（）。

A.

开启WPA2加密

B.

关闭SSID广播

C.

定期更改密码

D.

不随意连接陌生wifi

满分：30.00 分

得分：30.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

WPA2可以防止你的无线网络被它人破解；关闭SSID广播后wifi依然可以使用，只需要手动设置需要连接wifi的名称，可以提高破解难度；定期更改密码也可以提高破解难度；随意连接wifi可能会在上网过程中遇到中间人攻击。

教师评语：

暂无

2.

物理层安全面临的威胁有（）。

A.

搭线窃听

B.

电磁辐射信号还原

C.

物理临近

D.

电源安全

满分：30.00 分

得分：30.00 分

你的答案：

A B C

正确答案：

A B C

答案解析：

电源安全属于机器物理上的安全，不是网络上的第一层物理层的安全。

教师评语：

暂无

二、判断题 (共 40.00 分)

1.

智能手机没有任何物理攻击方法（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

B

正确答案：

B

答案解析：

智能手机在传输数据时可能会受到物理层上的攻击

教师评语：

暂无

2.

电磁泄漏是指信息系统的设备在工作时能经过地线、电源线、信号线、寄生电磁信号或谐波等辐射出去，产生电磁泄漏。（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

这些电磁信号如果被接收下来，经过提取处理，就可恢复出原信息，造成信息失密。

教师评语：

暂无

无线网络环境包括三部分，分别是：（）。

A.

无线客户端

B.

无线接入点

C.

无线电波

D.

wifi热点

满分：40.00 分

得分：40.00 分

你的答案：

A B C

正确答案：

A B C

答案解析：

wifi热点是俗称，是无线接入点AP的一种。

教师评语：

暂无

二、判断题 (共 60.00 分)

1.

WEP算法是安全的（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

B

正确答案：

B

答案解析：

WEP协议的在数据传输时，对数据的加密和解密都使用同样的算法和密钥，使用了RC4作为流加密协议，用于生成密钥流的初始向量IV是明文的方式。而该向量只有24位，这就使得在2^24个数据包后至少出现一次重复IV值，并且在实际中IV值重复的概率远远大于1/2^24，因而攻击者可轻易暴力破解获取IV。

教师评语：

暂无

2.

无线流量可以被范围内的无线电监测，不需要物理连接（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

无线流量通常使用电磁波作为载体，电磁波的传播是非定向的。

教师评语：

暂无

以下哪些选项是正确的（）。

A.

IPSec对于用户应用程序时透明的

B.

IPSec在传输层以下

C.

HTTPS使用了IPSec

D.

IPSec可以保证路由架构安全

满分：30.00 分

得分：30.00 分

你的答案：

A B D

正确答案：

A B D

答案解析：

HTTPS是应用层协议，IPSec是网络层的加密，HTTPS使用SSL作为加密方法，而不是IPSec。

教师评语：

暂无

二、判断题 (共 70.00 分)

1.

IP安全包括IPv4安全及IPv6安全（）。

A.

正确

B.

错误

满分：23.34 分

得分：23.34 分

你的答案：

A

正确答案：

A

答案解析：

IPv4是IP协议的第四版，IPv6是IP协议的第六版，它们都是IP协议。

教师评语：

暂无

2.

IPSec提供了访问控制服务（）。

A.

正确

B.

错误

满分：23.33 分

得分：23.33 分

你的答案：

A

正确答案：

A

答案解析：

IPSec提供了访问控制，比如说规定哪些用户可以接入IPSEC

教师评语：

暂无

3.

IPSec有传输模式和隧道模式两种（）。

A.

正确

B.

错误

满分：23.33 分

得分：23.33 分

你的答案：

A

正确答案：

A

答案解析：

IPSec有传输模式和隧道模式两种。

教师评语：

暂无

封装安全载荷(ESP)提供了哪些服务（）。

A.

消息内容的机密性

B.

数据源认证

C.

无连接完整性

D.

有限的流量保密性

满分：40.00 分

得分：40.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

ESP这样的一个协议,它提供了消息内容的机密性,数据源认证,无连接完整性,反重播服务,有限的流量保护。

教师评语：

暂无

二、判断题 (共 60.00 分)

1.

安全关联是发送方和接收方之间通信安全的单向关系（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

安全关联是发送方和接收方之间通信安全的单向关系。

教师评语：

暂无

2.

可以使用重放数据包的方法攻击ESP服务（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

B

正确答案：

B

答案解析：

ESP提供了反重播服务，可以防止数据包被重放。

教师评语：

暂无

SSL包含的协议有哪些（）。

A.

SSL 记录协议

B.

SSL 握手协议

C.

SSL 更换密码协议

D.

SSL 警报协议

满分：40.00 分

得分：40.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

SSL包含SSL记录协议，SSL握手协议，SSL更换密码协议，SSL警报协议

教师评语：

暂无

二、判断题 (共 60.00 分)

1.

现在商业界，政府，工业界广泛采用Web服务（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

商业界，政府，工业界广泛采用Web服务。

教师评语：

暂无

2.

SSL 支持使用Diffie Hellman密钥交换（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

SSL支持使用Diffie Hellman密钥交换功能。

教师评语：

暂无

HTTPS使用的底层协议是（）。

A.

SSH

B.

IPSec

C.

TLS

D.

WEP

满分：30.00 分

得分：30.00 分

你的答案：

C

正确答案：

C

答案解析：

SSL是由网景公司首先提出来的，之后业界将SSL协议进行标准化，标准化之后的协议，称之为TLS协议。

教师评语：

暂无

二、多选题 (共 40.00 分)

1.

SSH包含的子协议有（）。

A.

SSH 传输层协议

B.

SSH 用户认证协议

C.

SSH 密钥交换协议

D.

SSH 连接协议

满分：40.00 分

得分：40.00 分

你的答案：

A B D

正确答案：

A B D

答案解析：

SSH包含的子协议有SSH传输层协议，SSH用户认证协议，SSH连接协议。

教师评语：

暂无

三、判断题 (共 30.00 分)

1.

端口转发支持将任何不安全的TCP连接转换成安全的SSH连接（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

端口转发支持将任何不安全的TCP连接转换成安全的SSH连接。

教师评语：

暂无

Web会话管理典型技术包括（）。

A.

Cookie

B.

Session

C.

Token

D.

HTML

满分：40.00 分

得分：40.00 分

你的答案：

A B C

正确答案：

A B C

答案解析：

Web会话管理典型技术包括Cookie Session Token

教师评语：

暂无

二、判断题 (共 60.00 分)

1.

Web安全的本质是信任问题（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

web安全本质上是一种信任问题，信任就是，我们访问的网站是可信的吗，用户是可信的吗。

教师评语：

暂无

2.

Cookie不能保存于硬盘中，仅可以保存于内存。（）

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

B

正确答案：

B

答案解析：

cookies可以存在本地硬盘和内存之中。

教师评语：

暂无

以下哪些是Web存在的安全风险（）。

A.

Cookie攻击

B.

XSS

C.

CSRF

D.

SQL注入

满分：40.00 分

得分：40.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

XSS：跨站脚本攻击。CSRF：跨站请求伪造

教师评语：

暂无

二、判断题 (共 60.00 分)

1.

Cookie存在着被攻击的危险（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

如果Cookies泄露，其他人可以冒充这个Cookies的原使用者。

教师评语：

暂无

2.

SQL注入可以读取整个数据库的内容。（）

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

SQL注入攻击可以获取数据库的访问权限，通过构造特殊的SQL查询语句，可以读取整个数据库。

教师评语：

暂无

PGP支持的功能有（）。

A.

消息认证

B.

消息加密

C.

消息压缩

D.

邮件服务器认证

满分：40.00 分

得分：40.00 分

你的答案：

A B C

正确答案：

A B C

答案解析：

PGP功能包含了消息认证，消息加密，加密及认证，但无法认证服务器。

教师评语：

暂无

二、判断题 (共 60.00 分)

1.

Email在邮件服务器中存在被特权管理员查看的风险（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

邮件在邮件服务器中有可能被那些特权管理员进行查看。

教师评语：

暂无

2.

PGP发送二进制数据时会将数据转化为ASCII字符（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

处理二进制数据，比如说图像、视频这样的二进制数据，需要将它转化为ASCII编码，使用一个称之为radix-64这样的编码算法。

教师评语：

暂无

S/MIME的功能包括：（）。

A.

仅数据保密

B.

仅数据签名

C.

数据保密后签名

满分：30.00 分

得分：30.00 分

你的答案：

A B C

正确答案：

A B C

答案解析：

S/MIME的功能包括：数据保密和数据签名，两个功能可同时选择。

教师评语：

暂无

二、判断题 (共 70.00 分)

1.

S/MIME协议基于MIME协议做了安全性增强（）。

A.

正确

B.

错误

满分：23.33 分

得分：23.33 分

你的答案：

A

正确答案：

A

答案解析：

S/MIME协议基于MIME协议做了安全性增强。

教师评语：

暂无

2.

DKIM协议描述了如何由邮件服务提供商使用密码学工具对消息进行安全保护，消息接收方对消息进行验证（）

A.

正确

B.

错误

满分：23.34 分

得分：23.34 分

你的答案：

A

正确答案：

A

答案解析：

DKIM协议描述了如何由邮件服务提供商使用密码学工具对消息进行安全保护，消息接收方对消息进行验证。

教师评语：

暂无

3.

S/MIME和PGP都需要邮件客户端的更改才支持（）。

A.

正确

B.

错误

满分：23.33 分

得分：23.33 分

你的答案：

B

正确答案：

B

答案解析：

S/MIME对当前协议进行更改，也就是说需要邮件客户端来支持消息的S/MIME解码。而PGP不需要。

教师评语：

暂无

面哪一个不是漏洞传播机制（）。

A.

利用网页漏洞主动传播

B.

利用电子邮件系统传播

C.

通过局域网传播

D.

通过即时工具传播

满分：25.00 分

得分：25.00 分

你的答案：

A

正确答案：

A

答案解析：

蠕虫的传播机制主要包含利用系统漏洞主动传播，也可以利用电子邮件系统传播，还可以通过局域网传播，通过即时工具来传播，还有把前面几种方法组合来进行传播。

教师评语：

暂无

二、多选题 (共 35.00 分)

1.

病毒的结构包括（）。

A.

初始模块

B.

引导模块

C.

感染模块

D.

触发模块

E.

破坏模块

满分：35.00 分

得分：35.00 分

你的答案：

B C D E

正确答案：

B C D E

答案解析：

病毒的结构主要包含引导模块，感染模块，触发模块和破坏模块。

教师评语：

暂无

三、判断题 (共 40.00 分)

1.

独立恶意软件和寄生恶意软件的区别是代码是否独立（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

非独立的恶意代码，他自身只是一段代码，必须寄生在某个程序或文档中，作为该程序的一部分进行传播和运行。

教师评语：

暂无

2.

静态代码测试适用于测试阶段，而不是早期代码开发阶段（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

B

正确答案：

B

答案解析：

静态代码测试比较适用于早期的代码开发阶段而不是测试阶段。

教师评语：

暂无

哪个不属于win32平台下的网络监听工具（）。

A.

WinPcap

B.

windump

C.

tcpdump

D.

sniffer

满分：20.00 分

得分：20.00 分

你的答案：

C

正确答案：

C

答案解析：

tcpdump运行在UNIX或LINUX平台下。

教师评语：

暂无

2.

哪个不是攻击准备阶段的基本步骤（）。

A.

扫描

B.

找点

C.

踩点

D.

查点

满分：20.00 分

得分：20.00 分

你的答案：

B

正确答案：

B

答案解析：

准备实施攻击时，一般已经确认需要攻击的点，不用再找点。

教师评语：

暂无

二、多选题 (共 40.00 分)

1.

一般网络攻击分为哪几个阶段（）。

A.

攻击准备阶段

B.

攻击实施阶段

C.

攻击善后阶段

D.

攻击总结阶段

满分：20.00 分

得分：20.00 分

你的答案：

A B C

正确答案：

A B C

答案解析：

一般网络攻击都分为三个阶段，首先是攻击准备阶段，然后是攻击实施阶段，最后是攻击善后阶段。

教师评语：

暂无

2.

攻击善后阶段主要包括哪些（）。

A.

日志清理

B.

安装后门

C.

内核套件

D.

消除攻击痕迹

满分：20.00 分

得分：20.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

攻击的善后阶段，主要包括，日志清理，安装后门和内核套件等等，需要清理痕迹。

教师评语：

暂无

三、判断题 (共 20.00 分)

1.

攻击善后阶段不包括内核套件（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

B

正确答案：

B

答案解析：

善后阶段通常需要留后门，会使用到内核套件rootkit。

教师评语：

暂无

中国的等级保护将计算机信息安全等级分为几个等级（）。

A.

三个等级

B.

四个等级

C.

五个等级

D.

六个等级

满分：30.00 分

得分：30.00 分

你的答案：

C

正确答案：

C

答案解析：

中国计算机信息安全等级，划分了五个等级。

教师评语：

暂无

二、多选题 (共 40.00 分)

1.

操作系统通常采用哪些安全技术（）。

A.

主体标识与鉴别

B.

客体资源

C.

访问控制

D.

安全审计

满分：40.00 分

得分：40.00 分

你的答案：

A C D

正确答案：

A C D

答案解析：

目前各种操作系统都采用了许多安全技术，第一就是主体标识与鉴别，第二就是访问控制，第三是安全审计。

教师评语：

暂无

三、判断题 (共 30.00 分)

1.

存在绝对安全的信息系统（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

B

正确答案：

B

答案解析：

没有绝对安全的信息系统。

教师评语：

暂无

下列哪项不存在于注册表的数据结构（）。

A.

根键

B.

支键

C.

子键

D.

键值项

满分：30.00 分

得分：30.00 分

你的答案：

B

正确答案：

B

答案解析：

注册表的数据结构跟文件目录比较相似，主要包含根键，子键和键值项三部分。

教师评语：

暂无

二、多选题 (共 70.00 分)

1.

Windows具有哪些审计日志（）。

A.

应用程序日志

B.

系统日志

C.

安全日志

D.

目录服务日志

E.

文件复制日志

F.

DNS服务日志

满分：35.00 分

得分：35.00 分

你的答案：

A B C D E F

正确答案：

A B C D E F

答案解析：

Windows具有六种审计日志，包含应用程序日志，系统日志，安全日志，目录服务日志，文件复制日志，DNS服务日志等等

教师评语：

暂无

2.

Linux中的三类主要的日志子系统是（）。

A.

连接时间日志

B.

进程统计日志

C.

错误日志

满分：35.00 分

得分：35.00 分

你的答案：

A B C

正确答案：

A B C

答案解析：

在Linux系统中有三类主要的日志子系统，连接时间日志，进程统计日志，错误日志。

教师评语：

暂无

按照部署位置不同分类的防火墙是哪个（）。

A.

代理防火墙

B.

混合防火墙

C.

状态检测防火墙

D.

软件防火墙

满分：20.00 分

得分：20.00 分

你的答案：

B

正确答案：

B

答案解析：

按照部署位置不同防火墙可以分为：边界防火墙，个人防火墙，混合防火墙。

教师评语：

暂无

2.

电路级代理工作在OSI模型的哪层（）。

A.

传输层

B.

网络层

C.

应用层

D.

会话层

满分：20.00 分

得分：20.00 分

你的答案：

D

正确答案：

D

答案解析：

电路级代理，也被称作电路层网关，它工作在OSI模型的会话层，维护一张合法的会话连接表，然后进行会话层过滤。

教师评语：

暂无

二、多选题 (共 60.00 分)

1.

防火墙的工作模式有（）。

A.

路由模式

B.

透明模式

C.

简单模式

D.

混合模式

满分：30.00 分

得分：30.00 分

你的答案：

A B D

正确答案：

A B D

答案解析：

防火墙的工作模式包括三种，第一种称为路由模式，也就是防火墙以第三层对外连接，接口具有IP地址。第二种工作模式称为透明模式就是防火墙以第二层对外连接，接口无IP地址。第三种称为混合模式，假设防火墙既存在工作在路由模式的接口，也存在工作在透明模式接口，我们就说它工作在混合模式。

教师评语：

暂无

2.

防火墙的性能指标（）。

A.

吞吐量

B.

延时

C.

丢包率

D.

背靠背

满分：30.00 分

得分：30.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

防火墙的性能指标有九种：吞吐量，延时，丢包率，背靠背，最大并发连接数，最大并发连接建立速率，最大策略数，平均无故障间隔时间，支持的最大用户数。

教师评语：

暂无

入侵检测技术是实现P2DR模型中的（）部分的主要技术手段。

A.

安全策略

B.

防护

C.

检测

D.

响应

满分：20.00 分

得分：20.00 分

你的答案：

C

正确答案：

C

答案解析：

入侵检测技术就是实现P2DR模型中的detection检测部分。

教师评语：

暂无

二、多选题 (共 40.00 分)

1.

入侵检测原理（）。

A.

数据采集

B.

数据存储

C.

入侵分析

D.

响应处理

满分：40.00 分

得分：40.00 分

你的答案：

A C D

正确答案：

A C D

答案解析：

入侵检测的工作原理主要包含下面几方面，首先是数据收集，或者说数据采集，然后进行入侵分析，然后会进行响应处理。

教师评语：

暂无

三、判断题 (共 40.00 分)

1.

IDS是一种积极主动的安全防护技术（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

入侵检测系统俗称IDS，是一种对网络传输进行实时监控，在发现可疑传出时发出警报，或者采取主动反应措施的网络安全设备，它与其他的网络安全设备不同之处在于，它是一种积极主动的安全防护技术。

教师评语：

暂无

2.

统计分析是比较测量属性的平均值和偏差（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

统计分析是首先给系统对象，比如说用户的文件、目录和设备，创建一个统计描述或者称为正常的轮廓，统计正常使用时一些测量属性如访问次数、操作失败次数和延时等等。测量属性的平均值和偏差，被用来与网络系统的行为进行比较，任何观察值在正常值范围之外时，就会认为有入侵发生。

教师评语：

暂无

不属于Snort的工作模式（）。

A.

嗅探器

B.

数据包记录器

C.

数据包转发器

D.

网络入侵检测系统

满分：20.00 分

得分：0 分

你的答案：

B

正确答案：

C

答案解析：

snort有三种工作方式，嗅探器，数据包记录和网络入侵检测系统。

教师评语：

暂无

二、多选题 (共 60.00 分)

1.

入侵检测的分类方法（）。

A.

数据来源

B.

分析方法

C.

时效性

D.

分布性

满分：30.00 分

得分：30.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

可以分为主机入侵检测系统，俗称HIDS，和网络入侵检测系统，称为NIDS。然后根据采用的分析方法不同，可以分为异常检测模型或者是误用检测模型。根据时效性来分可以分为离线入侵检测系统，和在线入侵检测系统。根据分布性可以分为集中式入侵检测系统和分布式入侵检测系统。

教师评语：

暂无

2.

基于统计的异常检测模型有（）。

A.

操作模型

B.

方差模型

C.

多元模型

D.

马尔柯夫过程模型

满分：30.00 分

得分：30.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

常见的就是基于统计的异常入侵检测，可以通过操作模型，方差模型，多元模型，马尔柯夫过程模型来实现。

教师评语：

暂无

三、判断题 (共 20.00 分)

1.

网络入侵检测系统与操作系统无关（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

网络型入侵检测系统与操作系统无关，不会增加网络中主机的负担。

教师评语：

暂无

入侵检测技术是实现P2DR模型中的（）部分的主要技术手段。

A.

安全策略

B.

防护

C.

检测

D.

响应

满分：20.00 分

得分：20.00 分

你的答案：

C

正确答案：

C

答案解析：

入侵检测技术就是实现P2DR模型中的detection检测部分。

教师评语：

暂无

二、多选题 (共 40.00 分)

1.

入侵检测原理（）。

A.

数据采集

B.

数据存储

C.

入侵分析

D.

响应处理

满分：40.00 分

得分：40.00 分

你的答案：

A C D

正确答案：

A C D

答案解析：

入侵检测的工作原理主要包含下面几方面，首先是数据收集，或者说数据采集，然后进行入侵分析，然后会进行响应处理。

教师评语：

暂无

三、判断题 (共 40.00 分)

1.

IDS是一种积极主动的安全防护技术（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

入侵检测系统俗称IDS，是一种对网络传输进行实时监控，在发现可疑传出时发出警报，或者采取主动反应措施的网络安全设备，它与其他的网络安全设备不同之处在于，它是一种积极主动的安全防护技术。

教师评语：

暂无

2.

统计分析是比较测量属性的平均值和偏差（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

统计分析是首先给系统对象，比如说用户的文件、目录和设备，创建一个统计描述或者称为正常的轮廓，统计正常使用时一些测量属性如访问次数、操作失败次数和延时等等。测量属性的平均值和偏差，被用来与网络系统的行为进行比较，任何观察值在正常值范围之外时，就会认为有入侵发生。

教师评语：

暂无

不属于Snort的工作模式（）。

A.

嗅探器

B.

数据包记录器

C.

数据包转发器

D.

网络入侵检测系统

满分：20.00 分

得分：20.00 分

你的答案：

C

正确答案：

C

答案解析：

snort有三种工作方式，嗅探器，数据包记录和网络入侵检测系统。

教师评语：

暂无

二、多选题 (共 60.00 分)

1.

入侵检测的分类方法（）。

A.

数据来源

B.

分析方法

C.

时效性

D.

分布性

满分：30.00 分

得分：30.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

可以分为主机入侵检测系统，俗称HIDS，和网络入侵检测系统，称为NIDS。然后根据采用的分析方法不同，可以分为异常检测模型或者是误用检测模型。根据时效性来分可以分为离线入侵检测系统，和在线入侵检测系统。根据分布性可以分为集中式入侵检测系统和分布式入侵检测系统。

教师评语：

暂无

2.

基于统计的异常检测模型有（）。

A.

操作模型

B.

方差模型

C.

多元模型

D.

马尔柯夫过程模型

满分：30.00 分

得分：30.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

常见的就是基于统计的异常入侵检测，可以通过操作模型，方差模型，多元模型，马尔柯夫过程模型来实现。

教师评语：

暂无

三、判断题 (共 20.00 分)

1.

网络入侵检测系统与操作系统无关（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

网络型入侵检测系统与操作系统无关，不会增加网络中主机的负担。

教师评语：

暂无

下列哪项不在物联网的三层结构（）。

A.

感知层

B.

数据链路层

C.

网络层

D.

应用层

满分：30.00 分

得分：30.00 分

你的答案：

B

正确答案：

B

答案解析：

第一层是感知层处于最底层，第二层是网络层，第三层就是应用层。

教师评语：

暂无

二、多选题 (共 70.00 分)

1.

物联网有什么特征（）。

A.

全面的感知

B.

快速联网

C.

可靠的传输

D.

智能处理

满分：35.00 分

得分：35.00 分

你的答案：

A C D

正确答案：

A C D

答案解析：

物联网它有什么特征，第一个特征就是全面的感知，第二部分可靠的传输，第三个就是要智能处理。

教师评语：

暂无

2.

本章节提及了哪些物联网相关的安全问题或安全技术（）。

A.

数据隐私保护

B.

密钥管理问题

C.

安全路由的协议

D.

容侵容错

满分：35.00 分

得分：35.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

以上所有选项均在本章节中有所提及。

教师评语：

暂无

本章节提及了哪些车联网相关的安全问题或安全技术特点（）。

A.

车与车之间车际网

B.

高速移动带来的网络拓扑变化

C.

汽车行业的标准不统一

D.

ECU单元被控制

满分：40.00 分

得分：40.00 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

以上所有选项均在本章节中有所提及。

教师评语：

暂无

二、判断题 (共 60.00 分)

1.

车联网也是一类物联网，它是物联网在城市交通网络里边的一个具体应用（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

车联网也是一类物联网，它是物联网在城市交通网络里边的一个具体应用。

教师评语：

暂无

2.

车联网的架构和物联网一样分为三部分：感知层、网络层、应用层（）。

A.

正确

B.

错误

满分：30.00 分

得分：30.00 分

你的答案：

A

正确答案：

A

答案解析：

车联网的架构和物联网一样分为三部分：感知层、网络层、应用层。

教师评语：

暂无

当前网络的局限有（）。

A.

复杂性

B.

不一致的策略

C.

无法扩展

D.

对供应商的依赖

满分：26.66 分

得分：26.66 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

当前网络的局限主要体现在以下几方面，首先是复杂性，第二不一致的策略，第三无法扩展性，第四是对供应商的依赖。

教师评语：

暂无

2.

属于SDN的体系结构的有（）。

A.

应用层

B.

控制层

C.

数据层

D.

基础设施层

满分：26.67 分

得分：26.67 分

你的答案：

A B D

正确答案：

A B D

答案解析：

软件定义网络从体系上可以分为三个层次，最上面是应用层，中间是控制层，在最下面是基础设施层。

教师评语：

暂无

3.

SDN的特点有（）。

A.

控制转发分离

B.

控制平面集中化

C.

转发平面通用化

D.

控制器软件可编程

满分：26.67 分

得分：26.67 分

你的答案：

A B C D

正确答案：

A B C D

答案解析：

SDN的体系结构特点，控制转发分离，可以支持第三方控制面设备通过，OpenFlow等南向的开放式的协议，远程控制，使用硬件的交换和路由功能，控制平面集中化。

教师评语：

暂无

二、判断题 (共 20.00 分)

1.

SDN构建的是开放可编程的网络环境（）。

A.

正确

B.

错误

满分：20.00 分

得分：20.00 分

你的答案：

A

正确答案：

A

答案解析：

软件定义网络可以被视为是一种全新的网络技术，通过分离网络设备的控制面与数据面，将网络的能力抽象为应用程序接口提供给应用层，从而构建了开放可编程的网络环境。

教师评语：

暂无

比特币数量将限制在（）万。

A.

1900

B.

2000

C.

2100

D.

2200

满分：20.00 分

得分：20.00 分

你的答案：

C

正确答案：

C

答案解析：

比特币货币系统总数量永久被限制在2100万个。

教师评语：

暂无

二、多选题 (共 80.00 分)

1.

智能合约的工作原理（）。

A.

构建合约

B.

计算

C.

存储

D.

执行

满分：26.67 分

得分：26.67 分

你的答案：

A C D

正确答案：

A C D

答案解析：

智能合约的工作原理就是，构建合约，存储，执行。

教师评语：

暂无

2.

区块链隐私是指（）。

A.

身份隐私

B.

信息隐私

C.

交易隐私

D.

数据隐私

满分：26.67 分

得分：26.67 分

你的答案：

A C

正确答案：

A C

答案解析：

区块链的隐私，主要包含身份隐私和交易隐私。

教师评语：

暂无

3.

数字货币的两大问题（）。

A.

双重支付问题

B.

拜占庭将军问题

C.

连接问题

D.

分布问题

满分：26.66 分

得分：26.66 分

你的答案：

A B

正确答案：

A B

答案解析：

数字货币存在着两大问题：第一就是双重支付问题，是指同一笔钱被使用超过一次；另一个问题称为拜占庭将军问题，他是在缺少可信中心节点的情况下，分布式节点怎么达成共识建立互信的问题。

教师评语：

暂无