计算机三级——信息安全技术

题型：单选题 50 个，前 40 个每题一分，后 10 个每题两分；填空题 20 分，一空一分；综合题 20 分

第一套

一、选择题

1.信息技术的产生于发展，大致经历的三个阶段是：电讯技术的发明、计算机技术的发展、互联网的使用

2.同时具有强制访问控制核自主访问控制属性的访问控制模型是：Chinese Wall

3.信息安全的五个基本属性：机密性、可用性、可控性、不可否认性（不可抵赖性）、完整性

4.信息安全地位和作用（错误的）是：信息安全无法影响人们的工作和生活

5.哈希函数，正确的：MD5 算法首先将任意长度的消息填充为 512 的倍数，然后进行处理

6.对称密码（错误的）是：密钥管理和分发简单

7.消息认证不能预防的攻击：发送方否认

8.关于 Diameter 和 RADIUS 区别，（错误的）是：RADIUS 支持认证和授权分离，重授权可以随时根据需求进行；Diameter 中认证与授权必须成对出现

9.关于非集中式访问控制的说法，（错误的）是：在许多应用中，Kerberos 协议需要结合额外的单点登录技术以减少用户在不同服务器中的认证过程

10.（不）属于 IKE 协议的是：Kerberos

11.KPI 系统（不）包括：CDS

12.下列协议中，状态检测防火墙技术能够对其动态连接状态进行有效检测和防护的是：TCP

13.（不）属于分组密码工作模式：CCB

14.关于访问控制主体和客体，（错误）的是：一个对象或数据如果是主体，则其不可能是客体

15.关于进程管理，（错误）的是：进程与 CPU 的通信是通过系统调用来完成的

16.关于守护进程，（错误）的是：守护进程不能完成系统任务

17.Unix 系统中，改变文件分组的命令：chgrp

18.（不）属于 Windows 环境子系统的：Win8

19.有关视图，（错误）的是：视图和表都是关系，都储存数据

20.有关事务处理（错误）的是：不能回退 SELECT 语句，因此事务处理中不能使用该语句

21.P2DR 模型组成部分的核心：策略

22.ESP 协议不能对其进行封装的是：链路层协议

23.Kerberos 协议是分布式网络环境的一种：认证协议

24.用户认证的请求通过加密信道进行传输的是：HTTPS

25.AH 协议具有的功能：数据完整性鉴别

26.（不属于）IPv4 中 TCP/IP 协议栈安全缺陷的：没有提供复杂网络环境下的端到端可靠传输机制

27.可为电子邮件提供数字签名和数据加密功能的是：S/MIME

28.在计算机网络系统中，NIDS 的探测器要连接的设备是：交换器

29.下列网络地址，（不属于）私有 IP 地址的是：59.64.0.0

私有 IP 地址范围：A：10.0.0.0~10.255.255.255 即：10.0.0.0/8

B：172.16.0.0~172.31.255.255 即：172.16.0.0/12

C：192.168.0.0~192.168.255.255 即：192.168.0.0/16

30.软件漏洞网络攻击框架性工具：Metasploit
31.OWASP 的十大安全威胁排名中，位列第一的是：注入攻击
32.提出软件安全开发生命周期 SDL 模型的公司是：微软
33.（不属于）代码混淆技术的是：语法转换
34.（不属于）漏洞定义三要素的是：漏洞在计算机系统中不可避免
35.关于堆和栈在内存中增长方向：堆由低地址向高地址增长，栈由高地址向低地址增长
36.（不属于）缓冲区溢出的是：整数溢出
37.在信息安全事故响应中，必须采取的措施中（不包括）：保护物理资产
38.关于系统整个开发过程描述，（错误）的是：系统的生命周期是无限长的
39.在信息安全管理中的控制策略实现后，接下来要采取的措施（不包括）：逐步消减安全控制方面的开支
40.关于信息安全管理体系认证的描述，（错误的）是：每个组织都必须进行认证
41.依据涉密信息系统分级保护管理规范和技术标准，涉密信息系统建设使用单位将保密级别分为三级：秘密、机密和绝密
42.基本安全要求中基本技术要求从五个方面提出，（不包含）在五个方面的是：路由安全
43.（不属于）应急计划三元素的是：基本风险评估
44.（不属于）审核准备工作内容的是：加强安全意识教育
45.关于可靠电子签名：电子签名制作数据用于电子签名时，属于电子签名人专有
46.企业销售商用密码产品时，应向国家密码管理机构申请，其必需具备的条件：有独立的法人资格
47.电子认证服务提供者由于违法行为被吊销电子认证许可证书后，其直接负责的主管人员和其他直接责任人员多长时间内不得从事电子认证服务：10 年
48.（没必要）进行电子签名的文件：涉及停止供水、供热、供气、供电等公用事业服务的信息文件
49.关于可靠电子签名描述：签署时电子签名制作数据仅由电子签名人控制
50.（不应）被列为国家秘密的是：企业的商用信息

二、填空题

51.计算机系统安全评估的第一个正式标准是：可信计算机评估标准/TCSEC 标准，它具有划时代的意义，为计算机安全评估奠定了基础
52.信息安全的发展大致经历了三个主要阶段：通信保密阶段、计算机安全阶段和信息安全保障阶段
53.由于网络信息量十分巨大，仅依靠人工的方法难以应对网络海量信息的收集和处理，需要加强相关信息技术的研究，即网络舆情分析技术
54.消息摘要算法 MD5 可以对任意长度的明文，产生 128 位的消息摘要
55.验证所收到的消息确实来自真正的发送方且未被篡改的过程是消息认证
56.基于矩阵的行的访问控制信息表示的是访问能力表，即每个主体都附加一个该主体可访问的客体的明细表
57.强制访问控制系统通过比较主体和客体的安全标签来决定一个主体是否能够访问某个客体
58.在标准的模型中，将 CPU 模式从用户模型转到内核模式的唯一方法是触发一个特殊的硬件自陷，如中断、异常等
59.在 Unix/Linux 中，每一个系统与用户进行交流的界面，称为终端
60.在 Unix/Linux 中，root 账号是一个超级用户账户，可以对系统进行任何操作
61.TCG 使用了可信平台模块，而中国的可信平台以可信密码模块为核心

62.根据 ESP 封装内容的不同，可将 ESP 分为传输模式和隧道模式
63.PKI 是创建、管理、存储、分布和作废数字证书的一系列硬件、软件、人员、策略和过程的集合
64.木马程序由两部分程序组成，黑客通过客户端程序控制远端用户的计算机
65.通过分析代码中输入数据对程序执行路径的影响，以发现不可信的输入数据导致的程序执行异常，是污点传播分析技术
66.恶意影响计算机操作系统、应用程序和数据的完整性、可用性、可控性和保密性的计算机程序是恶意程序
67.根据加壳原理的不同，软件加壳技术包括压缩保护壳和加密保护壳
68.处于未公开状态的漏洞是 0day 漏洞
69.国家信息安全漏洞共享平台是 CNCERT 联合国内重要信息系统单位建立的信息安全漏洞信息共享知识库，它的英文缩写是 CNVD
70.电子签名需要第三方认证，是由依法设立的电子认证服务提供方提供认证服务的

三、综合题

71~75（6′）

为了构建一个简单、安全的“客户机/服务器”模式的应用系统，要求①能安全存储用户的口令（无须解密）；②用户口令在网络传输中需要被保护；③用户与服务器需要进行密钥协商，以便在非保护信道中实现安全通信；④在通信过程中能对消息进行认证，以确保消息未被篡改。

假设要构建的应用系统允许使用 MD5、AES、Diffie-Hellman 算法，给定消息 m，定义 MD5（m）和 AES（m）分别表示 m 的相应处理。请回答：

（1）为了安全存储用户的口令，服务器需要将每个用户的口令采用 MD5（1′）算法运算后存储

（2）在建立安全通信前，用户需要首先提交用户名和口令到服务器进行认证，为了防止口令在网络传输中被窃听，客户机程序将采用 MD5（1′）算法对口令运算后再发送

（3）为了在服务器和认证通过的用户之间建立安全通信，即在非保护的信道上创建一个会话密钥，最有效的密钥交换协议是 Diffie-Hellman（1′）算法

（4）AES 算法的分组长度是 128（1′）位

（5）为了同时确保数据的保密性和完整性，用户采用 AES 对消息 m 加密，并利用 MD5 产生消息密文的认证码，发送给服务器；假设服务器收到的消息密文为 c，认证码为 z，服务器只需要验证 z 是否等于 MD5（c）（2′）即可验证消息是否在传输过程中被篡改

76~79（4′，每空一分）

为了增强数据库的安全性，请按要求完成下列题目

（1）请按操作要求补全 SQL 语句：

为角色 R1 分配 Student 表的 INSERT、UPDATE 权限：

```
GRANT INSERT,UPDATE
ON TABLE Student
TO R1;
```

减少角色 R1 的 SELECT 权限;

```
REVOKE SELECT
ON TABLE Student
FROM R1
```

（2）事务处理是一种机制，用来管理必须成批执行的 SQL 操作，以保证数据库不包含不完整的操作结果。请回答下列问题：

A.每个事务均以 BEGIN TRANSACTION 语句显式开始，以 ROLLBACK 或 COMMIT 语句显式结束

B.在 INSERT、UPDATE、DROP 和 DELETE 语句中，不能回退的语句是 DROP 语句

80~89（10′，每空一分）

下图是TCP半连接扫描的原理图。其中，图1为目标主机端口处于监听状态时，TCP半连接扫描的原理图；图2为目标主机端口未打开时，TCP半连接扫描的原理图。请根据TCP半连接扫描的原理，补全扫描过程中各数据包的标志位和状态值信息。

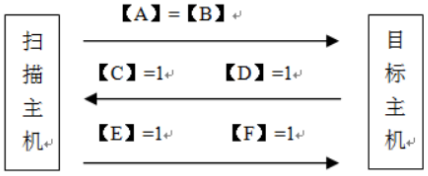


图 1　目标主机端口处于监听状态的 TCP 半连接扫描原理图

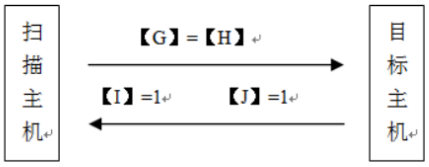


图 2 目标主机端口未打开时的 TCP 半连接扫描原理图

请在下表中输入 A-J 代表的内容：

A:syn

B:1

C:syn

D:ack

E:rst

F:ack

G:syn

H:1

I:rst

J:ack

第二套

一、选择题

1.《可信计算机评估准则》（TCSEC，也称为橘皮书）将计算机系统的安全划分为：四个等级七个级别
2.IATF 将信息系统的信息保障技术层面划分为四个技术框架焦点域。（不包含）在其中的是：技术
3.计算机系统安全评估的第一个正式标准是：TCSEC
4.IATF 将信息系统的信息保障技术层面划分为四个技术框架焦点域。（不包含）在其中的是：资产
5.（不属于）哈希函数应用的是：数据加密
6.不能用于产生认证码的是：数字签名
7.在强制访问控制模型中，属于混合策略模型的是：Chinese Wall 模型
8.关于自主访问控制的说法，（错误的）是：基于矩阵的列的访问控制信息表示的是访问能力表，即每个客体附加一个它可以访问的主体的明细表
9.关于 RADIUS 协议，（错误的）是：RADIUS 协议提供了完备的丢包处理及数据重传机制
10.关于 Kerberos 协议，（错误的）是：身份认证采用的是非对称加密机制
11.关于分组密码工作模式，（错误的）是：CBC 模式的初始向量需要保密，它必须以密文形式与消息一起传送
12.关于非对称密码，（错误的）是：公开密钥密码安全性高，与对称密码相比，更加适合于数据加密
13.关于 MD5 和 SHA 说法，（错误的）是：SHA 算法要比 MD5 算法更快
14.下列协议不能被攻击者用来进行 DoS 攻击的是：IPSec
15.关于文件系统管理，（错误的）是：文件系统在安装操作系统之后才会创建
16.Linux 系统启动后运行的第一个进程是：init
17.（不属于）Unix/Linux 文件类型的是：可执行文件（exe）
18.关于 root 账户说法，（错误的）是：Unix/Linux 超级用户账户只有一个
19.在 Windows 系统中，查看当前已经启动的服务列表的命令：net start
20.关于 SQL 命令：删除表的命令是 DROP
21.关于木马反弹端口技术，（错误的）是：反弹端口技术中，由跳板计算机将变动后的 IP 地址主动通知木马服务端程序
22.下列攻击手段中，（不属于）诱骗式攻击的是：ARP 欺骗
23.（不属于）分布式访问控制方法的是：RADIUS
24.关于 IPSec 的描述：IPSec 支持 IPV4 和 IPV6 协议
25.关于 SSL 协议的描述：为应用层提供了加密、身份认证和完整性验证的保护
26.（不属于）PKI 信任模型的是：链状信任模型
27.误用检测技术（不包括）：统计分析
28.（不属于）木马自身属性特点的是：感染性
29.攻击者向目标主机发起 ACK-Flood 时，目标主机收到攻击数据包后回应的是：ACK 和 RST 标志位设为 1 的数据包
30.（不属于）软件动态安全检测技术的是：词法分析
31.下列软件，采用软件动静结合安全检测技术的是：BitBlaze
32.（不属于）恶意程序传播方法的是：加壳欺骗
33.关于软件测试的描述，（错误的）是：模型检验是一种软件动态安全检测技术

34.微软公司安全公告中定义为：“重要”的漏洞，对应的漏洞危险等级是：第二级
35.属于 UAF（use-after-free）漏洞的是：内存地址对象破坏性调用的漏洞
36.Windows 操作系统提供的软件漏洞利用防范技术（不包括）：NOP
37.在信息资产管理中，标准信息系统的因特网组件（不包括）：电源
38.在信息资产管理中，标准信息系统的组成部分（不包括）：解决方案
39.关于信息资产评估，（错误的）是：应该给每项资产分配相同权重
40.关于体系审核，（错误的）是：对不符合的纠正措施无须跟踪审查
41.应急计划过程开发的第一阶段是：业务影响分析
42.（不属于）访问控制实现方法的是：虚拟性访问控制
43.信息安全的目标是：将残留风险保护在机构可以随时控制的范围内
44.信息系统的安全保护等级分为：五级
45.机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级，同时确定：保密期限和知悉范围
46.电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后：五年
47.国家秘密的保密期限不能确定时，应当根据事项的性质和特点，确定：解密条件
48.电子认证服务提供者拟暂停或终止电子认证服务时，应当提前就业务承接及其他相关事项通知有关各方，该时间提前：90 日
49.被称为“中国首部真正意义上的信息化法律”的是：电子签名法
50.违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处以：5 年以下有期徒刑或者拘役

二、填空题

51.1949 年，香农发表的《保密系统的通信理论》，是现代通信安全的代表作，是信息安全发展的重要里程碑
52.IATF 提出的信息保障的核心思想是纵深防御战略
53.分类数据的管理包括这些数据的存储、分布移植和销毁
54.传统对称密码加密时所使用的两个技巧是：代换和置换
55.当用户身份被确认合法后，赋予该用户进行文件和数据等操作权限的过程称为授权
56.自主访问控制模型的实现机制是通过访问控制矩阵实施的，而具体的实现办法，则是通过访问能力表或访问控制表来限定哪些主体针对哪些客体可以执行什么操作
57.恶意行为审计与监控，主要监测网络中针对服务器的恶意行为，包括恶意的攻击行为和入侵行为
58.每个事务均以 BEGIN TRANSACTION 语句显式开始，以 COMMIT 或 ROLLBACK 语句显式结束
59.控制其它程序运行，管理系统资源并为用户提供操作界面的系统软件的集合是操作系统
60.进程与 CPU 通信是通过中断信号来完成的
61.在 Unix/Linux 系统中，服务是通过 inetd 进程或启动脚本来启动
62.主要适用于有严格的级别划分的大型组织机构和行业领域的信任模型是层次信任模型
63.NIDS 包括探测器和控制台两部分
64.指令寄存器 eip 始终存放着返回地址
65.根据软件漏洞具体条件，构造相应输入参数和 Shellcode 代码，最终实现获得程序控制权的过程，是漏洞利用
66.攻击者窃取 Web 用户 SessionID 后，使用该 SessionID 登录进入 Web 目标账户的攻击方法，被称为会话劫持

67.通过分析代码中输入数据对程序执行路径的影响，以发现不可信的输入数据导致的程序执行异常，这种技术被称为污点传播分析技术

68.栈指针寄存器 esp 始终存放栈顶指针

69.信息安全管理的主要内容，包括信息安全管理体系、信息安全风险评估和信息安全管理措施三个部分

70.电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务 60 日前向国务院信息产业主管部门报告

三、综合题

71~76（6′，每空一分）

为了构建一个简单、安全的“客户机/服务器”模式的应用系统，要求：①能安全存储用户的口令（无须解密），且对网络传输中的口令进行保护；②使用第三方权威证书管理机构 CA 来对每个用户的公钥进行分配。假设要构建的应用系统只允许使用 MD5、AES、RSA 算法。请回答下述问题：

（1）为了安全存储用户的口令，服务器需要将每个用户的口令采用 MD5 算法运算后存储。为了能通过用户名和口令实现身份认证，用户将采用相同的算法对口令运算后发送给服务器

（2）SHA 算法的消息摘要长度为 160 位

（3）用户可将自己的公钥通过公钥证书发送给另一用户，接收方可用证书管理机构对证书加以验证

（4）要实现消息认证，产生认证码的函数类型有三类：消息加密、消息认证码和哈希函数

（5）为了确保 RSA 密码的安全，必须认真选择公钥参数（n，e）：模数 n 至少 1024 位；为了使加密速度快，根据“反复平方乘”算法，e 的二进制表示中应当含有尽量少的 1

77~80（4′，每空一分）

为了增强数据库的安全性，按要求完成题目

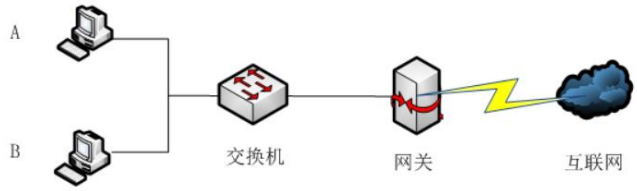
（1）数据库渗透测试的对象主要是数据库的身份验证系统和服务监听系统

（2）通常情况下，SOL 注入攻击所针对的数据信道包括存储过程和 Web 应用程序输入参数

（3）事务处理是一种机制，用来管理必须成批执行的 SQL 操作，以保证数据库不包含不完整的操作结果。在 INSERT、UPDATE、CREATE 和 DELETE 语句中，不能回退的语句是 CREATE 语句

81~90（10′，每空一分）

在下图中，内网有两台计算机A和B，通过交换机连接到网关设备最后连入互联网，其中计算机A的IP地址为192.168.1.10，MAC地址为MACA；计算机B的IP地址为192.168.1.20，MAC地址为MACB；网关设备的IP地址为59.60.1.1，MAC地址为MACG。



其中，计算机 B 感染了 ARP 病毒，此 ARP 病毒向其它内网计算机发起伪装网关 ARP 欺骗攻击，它发送的 ARP 欺骗数据包中，IP 地址为 59.60.1.1，MAC 地址为 MACB

为了防止 ARP 欺骗，需要在内网计算机和网关设备上进行 IP 地址与 MAC 地址的双向静态绑定。

首先，在内网的计算机 A 设置防止伪装网关欺骗攻击的静态绑定：

arp -d//清空 ARP 缓存表

arp -s 59.60.1.1 MACG//将 IP 地址与 MAC 地址静态绑定

arp -d//清空 ARP 缓存表
arp -s 192.168.1.10 MACA//将 IP 地址与 MAC 地址静态绑定

第三套

一、选择题

1.信息安全属性中，含义是“保证数据的一致性，防止数据被非法用户篡改”的是：完整性
2.关于信息安全的地位和作用的阐述中，（错误的）是：信息安全无法影响人们的工作和生活
3.TCSEC 将计算机系统安全划分为：四个等级七个级别
4.信息安全属性中，含义是“保证信息不被窃听，或窃听者不能了解信息的真实含义”的是：机密性
5.（不能）用于身份认证的是：AC 证书
6.关于自主访问控制，（错误的）是：访问矩阵中的每列表示一个主体，每一行则表示一个受保护的客体
7.（不属于）强制访问控制模型的是：RBAC
8.关于非集中式访问控制，（错误的）是：在许多应用中，Kerberos 协议需要结合单点登录技术以减少用户在不同服务器中的认证过程
9.关于访问控制技术，（错误的）是：RADIUS 将加密客户端和服务器之间的所有数据，而 TACACS+仅需要加密传送的密码
10.（不能）用于数字签名的算法：Diffie-Hellman
11.如果密钥丢失或其它原因在密钥未过期之前，需要将它从正常运行使用的集合中除去，称为密钥的：撤销
12.关于消息认证的说法，（错误的）是：消息认证码既可提供认证又可提供保密性
13.防范计算机系统和资源被未授权访问，采取的第一道防线是：访问控制
14.（不能）保证数据完整性的是：视图
15.关于进程管理，（错误的）是：线程是用于组织资源的最小单位，线程将相关的资源组织在一起，这些资源包括内存地址空间、程序、数据等
16.Unix 系统最重要的网络服务进程是：inetd
17.（不属于）Windows 系统进程管理工具的是：本地安全策略
18.关于 GRANT 语句，（错误的）是：发出该 GRANT 语句的只能是 DBA 或者数据库对象创建者，不能是其它任何用户
19.（不属于）数据库软件执行的完整性服务：关系完整性
20.（不属于）网站挂马的主要技术手段是：下载挂马
21.数据包内容选项中，ESP 协议在传输模式下（不进行）加密的是：源 IP 和目标 IP
22.IPSec 协议属于：第三层隧道协议
23.证书的验证需要对证书的三个信息进行确认，（不包括）：验证保密性，即证书是否由 CA 进行了数字签名
24.关于防火墙，（错误的）是：不能防范针对面向连续协议的攻击
25.主要在操作系统的内核层实现的木马隐藏技术是：Rootkit 技术
26.“震荡波”病毒进行扩散和传播所利用的漏洞是：操作系统服务程序漏洞
27.（不能）有效防范网络嗅探的是：TELNET
28.TCP 三次握手过程中，第一次握手数据包控制位中的标志位状态为：SYN=1,ACK=1
29.（不属于）软件安全保护技术的是：软件逆向分析技术
30.（不能）有效检测采用加壳技术的恶意程序的是：特征码查杀技术
31.下列漏洞库中，由国内机构维护的漏洞库是：CNNVD
32.关于堆描述：堆是一个先进先出的数据结构，在内存中的增长方向是从低地址向高地址增长

33.当用户双击自己 Web 邮箱中邮件的主题时，触发了邮件正文页面中的 XSS 漏洞，这种 XSS 漏洞属于：存储型 XSS
34.（不属于）恶意程序传播方法的是：修改浏览器配置
35.综合漏洞扫描（不包含）的功能：SQL 注入扫描
36.信息安全管理体系（ISMS）体现的思想是：预防控制为主
37.关于信息安全管理，（错误的）是：零风险是信息安全管理工作的目标
38.为了保证整个组织机构的信息安全，下列措施（错误的）是：应当增加系统的输入输出操作，减少信息的共享
39.在制定一套好的安全管理策略时，制定者首先必须：与决策层进行有效沟通
40.在风险管理中，应采取适当的步骤，以确保机构信息系统具备三个安全特性。（不包括）在其中的是：坚固性
41.重要安全管理过程（不包括）：安全资质评审
42.关于系统维护注意事项，（错误的）是：维护人员接收到一个更改要求，必须纳入这个更改
43.BS 7799 是依据英国的工业、政府和商业共同需求而制定的一个标准，它分为两部分：第一部分为“信息安全管理事务准则”，第二部分为：信息安全管理系统的规范
44.《计算机信息系统安全保护等级划分准则》将信息系统安全分为五个等级。（不包括）：协议保护级
45.《刑法》中有关信息安全犯罪的规定包括：3 条
46.《计算机信息系统安全保护等级划分准则》的安全考核对象，（不包含）：数据信道传输速率
47.电子认证服务提供者被依法吊销电子认证许可证书的，其业务承接事项的处理按照下列哪个机构的规定执行：国务院信息产业主管部门
48.六个国家在 1996 年联合提出了信息技术安全评价的通用标准（CC），其中（不包括）：中国
49.在安全管理的方针手册中，（不属于）主要内容的是：信息管理的流程
50.（不属于）风险控制的基本策略的是：消除漏洞产生的影响（消除）

二、填空题

51.信息安全的五个属性是机密性、完整性、可用性、可控性、不可否认性
52.上世纪 90 年代中期，六国七方（加拿大、法国、德国、荷兰、英国、美国国家标准与技术研究院（NIST）及美国国家安全局（NSA））提出的信息技术安全性评估通用准则，英文简写为 CC，是评估信息技术产品和系统安全性的基础准则
53.恶意行为的监测方式主要分为两类：主机监测和网络监测
54.密码设计应遵循一个公开设计的原则，即密钥体制的安全应依赖于对密钥的保密，而不应依赖于对算法的保密
55.AES 的分组长度固定为 128 位，密钥长度则可以是 128、192 或 256 位
56.基于 USB Key 的身份认证系统主要有两种认证模式：挑战/应答模式和基于 PKI 体系的认证模式
57.任何访问控制策略最终可以被模型化为访问矩阵形式，行对应于用户，列对应于目标，矩阵中每一元素表示相应的用户对目标的访问许可
58.信任根和信任链是可信计算平台的最主要的关键技术之一
59.在 CREATE TABLE 语句中使用 DEFAULT 子句，是定义默认值首选的方法
60.当用户代码需要请求操作系统提供的服务时，通常采用系统调用的方法来完成这一过程
61.当操作系统为 0 环和 1 环执行指令时，它在管理员模式或内核模式下运行

62.SSL 协议包括两层协议：记录协议和握手协议
63.CA 通过发布证书黑名单，公开发布已经废除的证书
64.攻击者通过精心构造超出数据范围的索引值，就能够对任意内存地址进行读写操作，这种漏洞被称为数组越界漏洞
65.在不实际执行程序的前提下，将程序的输入表示成符号，根据程序的执行流程和输入参数的赋值变化，把程序的输出表示成包含这些符号的逻辑或算数表达式，这种技术称为符号执行技术
66.被调用的子函数下一步写入数据的长度，大于栈帧的基址到 ESP 之间预留的保存局部变量的空间时，就会发生栈的溢出
67.漏洞利用的核心，是利用程序漏洞去执行 shellcode 以便劫持进程的控制权
68.软件安全检测技术中，定理证明属于软件静态安全检测技术
69.风险评估分为自评估和检查评估
70.国家秘密的保密期限，绝密级不超过 30 年，除另有规定

三、综合题

71~76（6′，每题一分）

为了构建一个简单、安全的“客户机/服务器”模式的应用系统，要求:①能安全存储用户的口令（无须解密）;②用户口令在网络传输中需要被保护;③用户与服务器需要进行密钥协商，以便在非保护信道中实现安全通信;④在通信过程中能对消息进行认证，以确保消息未被篡改。

假设要构建的应用系统允许使用 MD5、AES、Diffie-Hellman 算法，给定消息 m，定义 MD5(m)和 AES(m)分别表示对 m 的相应处理。为了准确地描述算法，另外定义如下:给定数 x、y 和 z，x*y 表示乘法运算，x/y 表示除法运算，x^y 表示指数运算，而 x^(y/z)表示指数为 y/z。请回答下述问题:

（1）为了安全存储用户的口令，服务器需要将每个用户的口令采用 MD5 算法运算后存储
（2）在建立安全通信前，用户需要首先提交用户名和口令到服务器进行认证，为了防止口令在网络传输中被窃听，客户机程序将采用 MD5 算法对口令运算后再发送
（3）为了在服务器和认证通过的用户之间建立安全通信，即在非保护的信道上创建一个会话密钥，最有效的密钥交换协议是 Diffie-Hellman 算法
（4）假定有两个全局公开的参数，分别为一个素数 p 和一个整数 g，g 是 p 的一个原根，为了协商共享的会话密钥：

首先，服务器随机选取 a，计算出 A=g^a mod p，并将 A 发送给用户；
然后，用户随机选取 b，计算出 B=g^b mod p，并将 B 发送给服务器
最后，服务器和用户就可以计算得到共享的会话密钥 key=g^(a*b) mod p

77~80（4′，每空一分）

为了增强 Windows 系统的安全，填空：
（1）权限适用于对特定对象如目录和文件的操作，每一个权限级别都确定了一个执行特定的任务组合的能力，包括 Read、Execute、Write、Delete 和 SetPermission 等。如果对目录有 Execute 权限，表示可以穿越目录，进入其子目录
（2）要使网络用户可以访问在 NT Server 服务器上的文件和目录，必须首先对这些文件和目录建立共享
（3）为了防止网络黑客在网络上猜出用户的密码，可以在连续多次无效登录之后对用户账号实行锁定策略
（4）在 Windows 系统中，任何涉及安全对象的活动都应该受到审核。审核报告将被写入安全日志中，可以使用事件查看器来查看

81~90（10′，每空一分）

下图为一个单位的网络拓扑图。根据防火墙不同网络接口连接的网络区域，将防火墙控制的区域分为内网、外网和DMZ三个网络区域。为了实现不同区域间计算机的安全访问，根据此单位的访问需求和防火墙的默认安全策略，为防火墙配置了下面三条访问控制规则。请根据访问控制规则表的要求，填写防火墙的访问控制规则（表1）。其中，“访问控制”中Y代表允许访问，N代表禁止访问。

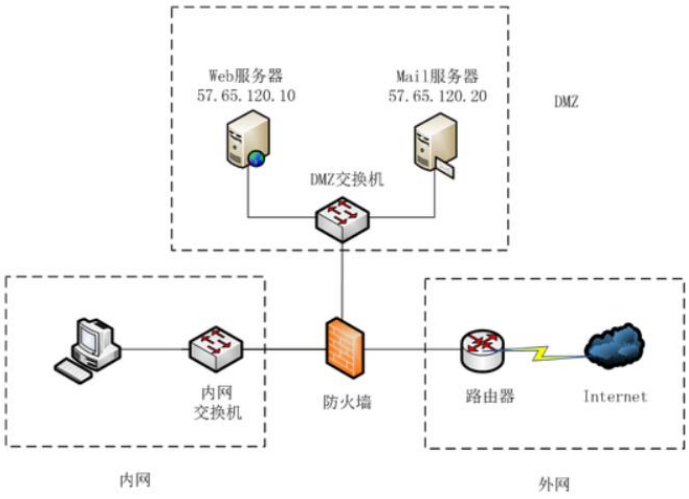


图 网络拓扑图

表 1 防火墙访问控制规则表

访问规则	源区域	目的区域	目的 IP	协议名称	访问控制
内网可访问 Web 服务器	内网	DMZ	57.65.120.10	HTTP	Y
外网可访问 Mail 服务器	外网	DMZ	57.65.120.20	SMTP 或 POP3	Y
任意地址访问任意地址	任意	任意	任意	任意	N

第四套

一、选择题

1.发表于 1949 年的《保密系统的通信理论》把密码学置于坚实的数学基础之上，标志着密码学形成一门学科。该论文的作者是：Shannon

2.依照时间顺序，信息技术的产生于发展大致经历了三个阶段，（不属于）这三个阶段的是：数据库技术的应用

3.属于信息安全问题产生内在根源的是：互联网的开放性

4.香农在 1949 年发表的论文《保密系统的通信理论》，用信息论的观点对保密问题进行了全面的论述，它是信息安全发展的重要里程碑

5.关于强制访问控制，（错误的）是：Biba 模型作为 BLP 模型的补充而提出，利用“不上读/不下写”的原则来保证数据的完整性

6.进行简单的用户名/密码认证，且用户只需要一个接受或拒绝即可进行访问（如在互联网服务提供商 ISP 中）的是：RADIUS

7.关于密码技术，（错误的）是：密码体制的安全既依赖于对密钥的保密，又依赖于对算法的保密

8.两个不同的消息具有相同的消息摘要的现象，称为：碰撞

9.除去奇偶校验位，DES 算法密钥的有效位数是：56

10.关于身份认证，（错误的）是：生物特征识别技术是目前身份认证技术中最常见、最安全的技术

11.关于消息认证，（错误的）是：传统密码只能提供保密性，不能用于消息认证

12.（不属于）集中式访问控制协议的是：Kerberos 协议

13.关于访问控制模型，（错误的）是：BLP 安全模型利用“不下读/不上写”的原则来保证数据的保密性

14.模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入地探测，发现系统最脆弱环节的技术是：渗透测试

15.关于线程，（错误的）是：线程是为了节省资源而可以在同一个进程中共享资源的一个执行单位

16.关于保护环，（错误的）是：3 环中的主体不能直接访问 1 环中的客体，1 环中的主体同样不能直接访问 3 环中的客体

17.在 Unix 系统中，改变文件拥有权的命令是：chmod

18.在 Unix 系统中，查看最后一次登录文件的命令是：lastlog

19.如果所有外键参考现有的主键，则说明一个数据库具有：参照完整性

20.深入数据库之内，对数据库内部的安全相关对象进行完整的扫描与检测，即：内部安全检测

21.端口扫描时，采用慢速扫描技术的原因：慢速扫描可以隐藏端口扫描行为

22.关于网络漏洞扫描工具的描述，（错误的）是：网络漏洞搜啊秒工具可以扫描微软 Word 软件的漏洞

23.下列攻击技术中，利用服务器端漏洞进行攻击的是：SQL 注入攻击

24.（不属于）木马功能的是：主动感染

25.关于防火墙 DMZ 区域的描述，（错误的）是：外网的计算机不能访问 DMZ 区域的计算机

26.（不包含）在数字证书中的信息：用户的私钥

27.端口扫描时，隐蔽性最高的扫描方法是：TCP FIN 扫描

28.（不属于）软件安全开发技术的是：安全发布
29.基于硬件介质的软件安全保护技术（不包括）：数字证书
30.关于栈，正确的：栈是一个后进先出的数据结构，在内存中的增长方向是从高地址向低地址增长
31.（不属于）防火墙体系结构的是：屏蔽中间网络体系结构
32.综合漏洞扫描（不包含）：恶意程序扫描
33.（不属于）整数溢出原因的是：条件未判断
34.攻击者利用栈溢出发起攻击时，向存在漏洞的软件程序输入的数据，一般（不包括）：Heap
35.（不属于）信息安全风险评估基本方法的是：长远风险评估
36.关于信息安全管理基本技术要求所涉及的五个层面描述，正确的是：物理安全、网络安全、主机安全、应用安全和数据安全
37.事故响应（IR）是为计划、检测、和改正事故对信息资产的影响而采取的一系列行动，（不属于）事故响应阶段的是：观察
38.关于信息安全威胁类型与实例的对应关系中，（错误的）是：蓄意信息敲诈行为；非法使用硬件设备或信息
39.涉密信息系统分级保护管理规范和技术标准所划分的三个密级中，（不包含）：保密
40.（不属于）访问控制类型的是：检验性的访问控制
41.在访问控制管理时，由访问控制依赖的四个原则转换成的三个职责，（不包含）：责任衡量
42.按照实现方法，访问控制可分为如下三类：行政性访问控制、逻辑/技术性访问控制、物理性访问控制
43.信息系统的安全保护等级由两个定级要素决定，它们是：等级保护对象受到破坏时所侵害的客体；对客体造成侵害的程度
44.基于对电子签名认证证书或者电子签名的信赖，从事有关活动的人或机构被称为：电子签名依赖方
45.国家秘密的保密期限，应当根据事项的性质和特点进行制定，对不能确定期限的，应当确定：解密条件
46.系统安全维护的正确步骤是：报告错误、处理错误、处理错误报告
47.（不属于）销售商用密码产品必需的申请条件是：要求注册资金超过 200 万人民币
48.关于可靠电子签名特点，（错误的）是：电子签名的验证属于电子签名人专有
49.针对 Web 系统的源代码进行全面的代码安全性分析，以全面检测分析 Web 应用程序的安全性问题是指：白盒测试方法
50.审查数据电文作为证据的真实性时，需要考虑的因素：用以鉴别发件人方法的可靠性

二、填空题

51.信息技术可能带来的一些负面影响包括？信息泛滥、信息污染和信息犯罪
52.IATF 提出了三个主要核心要素：人员、技术和操作
53.根据具体需求和资源限制，可以将网络信息内容审计系统分为流水线模型和分段模型两种过程模型
54.RSA 密码建立在大整数因式分解的困难性之上，而 ElGamal 密码建立在离散对数的困难性之上
55.对称密钥体制，根据对明文的加密方式的不同而分为两类：分组密码和序列密码
56.产生认证码的函数类型，通常有三类：消息加密、消息认证码和哈希函数
57.基于矩阵的列的访问控制信息表示的是访问控制表，即每个客体附加一个它可以访问的主体的明细表
58.为不同的数据库用户定义不同的视图，可以限制各个用户的访问范围

59.对于数据库的安全防护分为三个阶段：事前检查、事中监控和事后审计
60.数据库软件执行三种类型的完整性服务：语义完整性、参照完整性和实体完整性
61.数据库都是通过开放一定的端口，来完成与客户端的通信和数据传输
62.入侵检测系统可以实现事中防护，是指入侵攻击发生时，入侵检测系统可以通过与防火墙联动从而实现动态防护
63.不同于包过滤防火墙技术，代理服务器在应用层对数据进行基于安全规则的过滤
64.模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，发现系统最脆弱的环节的技术是渗透测试
65.隶属于中国信息安全测评中心的中国国家信息安全漏洞库，其英文缩写为 CNNVD
66.由大量 NOP 空指令 0x90 填充组成的指令序列是滑板指令
67.软件安全开发技术，主要包括建立安全威胁模型、安全设计、安全编码和安全测试等几个方面
68.微软 SDL 模型的中文全称为软件安全开发生命周期模型
69.信息安全风险评估的复杂程度，取决于受保护的资产对安全的敏感程度和所面临风险的复杂程度
70.《信息系统安全保护等级划分标准》中提出了定级的四个要素：信息系统所属类型、业务数据类型、信息系统服务范围和业务自动化处理程度

三、综合题

71~76（6′，每空一分）

为了构建一个简单、安全的“客户机/服务器”模式的应用系统，防止非法的客户机接入，要求每个用户进行身份认证。假设服务器的公钥为 PK，私钥为 SK；用户 Alice 的公钥为 PKA，私钥为 SKA。Alice 和服务器互相知道彼此的公钥。请回答：

（1）为了完成服务器对 Alice 的认证：首先，服务器产生一个随机数 r，为了保护该随机数，服务器将使用 Alice 的公钥对其加密后发送给 Alice；然后，Alice 用自己的私钥进行解密得到随机数 r；第三，Alice 用自己的私钥对该随机数进行签名，并将签名结果发送给服务器；最后，服务器用 Alice 的公钥对签名结果进行校验，如果校验通过，则对 Alice 的身份认证通过

（2）为了确保 RSA 密码的安全，必须认真选择参数：模数 n 至少 1024 位；为了使加密速度快，根据“反复平方乘”算法，e 的二进制表示中应当含有尽量少的 1

77~80（4′，每空一分）

为了增强 UNIX/Linux 系统的安全，完成下列题目

（1）UNIX 文件系统安全就是基于 i 结点中三段关键信息：UID、GID 和模式

（2）查看 UNIX 文件权限的命令：$ls-l

（3）为一个文件的拥有者授予可读和可写权限，给分组和其它用户只有可读权限，则权限位为“rw-r—r--”。将该权限位用八进制数表示为 644

（4）如果要给文件 foo 的分组以读权限，则使用如下命令：$chomd g+r foo

81~90（10′，每空一分）

如下图所示，A计算机和B计算机之间部署了防火墙进行安全防护，A计算机的IP地址为192.168.20.100，B计算机是Web服务器，其IP地址为58.64.152.20，仅对外开放了443端口的访问服务。
防火墙的安全配置要求为：
（1）仅允许B计算机接收A计算机发来的对443端口的访问请求，禁止接收A计算机的其它访问请求；
（2）禁止B计算机对A计算机的访问请求。

请按照上述安全配置要求，完成下面的防火墙包过滤规则表。

要求：（1）“操作”的规则设置可选项为：通过、阻断；（2）“标志位”的规则设置格式为“标志位=数值”，比如RST=0，如果有多个标志位请以逗号隔开；如果不设置标志位，请填写“无”。

图 网络拓扑图

包过滤规则表

序号	方向	源 IP	目标 IP	协议	源端口	目标端口	标志位	操作
1	A 到 B	192.168.20.100	58.64.152.20	TCP	大于 1023	443	无	通过
2	B 到 A	58.64.152.20	192.168.20.100	TCP	443	大于 1023	ACK=1	通过
3	任意网址	任意	任意	任意	任意	任意	任意	到任意网址

第五套

一、选择题

1.美国制定数据加密标准 DES（Data Encryption Standard）的年份是：1977
2.信息安全的发展大致经历了三个阶段。（不属于）三个阶段的是：互联网使用阶段
3.与等级保护工作（不相关）的是：《电子签名法》
4.信息保障的指导性文件《信息保障技术框架》（Information Assurance Technical Framework，IATF）是由：美国国家安全局（NSA）制定的
5.（不包含）在数字证书中的是：用户的私钥
6.关于密码技术的描述，（错误的）是：数字签名系统一定具有数据加密功能
7.用于验证消息完整性的是：消息摘要
8.属于单密钥密码算法的是：DES 算法
9.关于 USB Key 身份认证，（错误的）是：USB Key 的身份认证模式只有挑战/应答模式
10.关于集中式访问控制，（错误的）是：如果进行简单的用户名/密码认证，且用户只需要一个接受或拒绝即可获得访问，TACACS+是最适合的协议
11.（不属于）分布式访问控制方法的是：基于 PKI 体系的认证模式
12.关于数字签名，正确的：数字签名能够解决篡改、伪造等安全性问题
13.Diffie-Hellman 算法是一种：密钥交换协议
14.关于 SQL 注入，（错误的是）：防火墙能对 SQL 注入漏洞进行有效防范
15.关于 CPU 模式和保护的说法，（错误的）是：环号越高，赋予运行在该环内的进程的权限就越大
16.关于守护进程的说法，（错误的）是：当控制终端被关闭时，包括守护进程在内的所有进程都会自动关闭
17.如果要给文件 foo 的分组以读权限，所使用的命令是：chmod g+r foo
18.关于信任属性，（错误的）是：信任具有对称性，即若 A 信任 B，则 B 信任 A
19.关于结构化查询语言基本命令，（错误的）是：删除基本表的基本命令是 DELETE
20.（不属于）数据库事务处理特性的是：完整性
21.利用 ICMP 协议进行扫描时，可以扫描的目标主机信息是：IP 地址
22.只能用于端口扫描的软件：Nmap
23.下列拒绝服务攻击中，（不通过）传输层实施的是：Script Flood
24.有关远程控制技术的描述，（错误的）是：防火墙可以拦截木马服务端对木马客户端的连接
25.（不属于）木马隐藏技术的是：端口反弹
26.PKI 系统中，OCSP 服务器的功能是：OCSP 服务器为用户提供证书在线状态的查询
27.（不能）对 ARP 欺骗攻击起到防范和检测作用的是：PKI
28.DoS 攻击的实现方式，（不包括）：通过耗尽目标主机的存储空间，实施 DoS 攻击
29.说法（错误的）是：RARP 协议的作用就是通过自身的 IP 获得对应的 MAC 地址
30.（不属于）漏洞定义三要素的是：漏洞是由于计算机系统设计、开发和运行中的疏漏而导致的
31.（不能防止）Web 系统出现安全配置错误的是：及时配置好 Web 防火墙
32.关于栈的描述，正确的：栈空间的增长方向是由高地址向低地址增长，数据写入栈帧的填充方向是从低地址向高地址增长
33.（不属于）缓冲区溢出漏洞的是：整数溢出
34.栈帧地址的分配动态变化时，下列技术中，可以使新的返回地址定位到 shellcode 起始地

址的是：jmp esp
35.严格按照各阶段进行开发，只有在前一个阶段的评审通过后才能够进行下一个阶段，这种软件开发生命周期模型是：瀑布模型
36.下列软件安全保护技术中，使用压缩算法的是：软件加壳技术
37.风险管理的第一个任务是：风险识别
38.关于信息安全管理基本管理要求所涉及的五个层面的描述中，正确的：安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理
39.信息安全风险评估的三种方法是：基本风险评估、详细风险评估、两者相结合
40.风险分析主要分为：定量风险分析和定性风险分析
41.在基本安全管理措施中，访问控制依赖的原则（不包括）：共享
42.制定业务持续性计划时，策略选择的决定性因素是：成本
43.灾难恢复中，可用于恢复持续性之外的其他意图的选项，（不包括）：即时监控
44.关于国家秘密的处理方法的说法，正确的：在专用 VPN 中传递国家秘密
45.属于《计算机信息系统安全保护等级划分标准》安全考核指标的是：审计
46.电子签名认证证书应当载明：电子认证服务者名称、证书持有人名称、证书序列号、证书有效期
47.机构想要提供电子认证服务，应具备的必须条件包括：具有符合国家安全标准的技术和设备
48.GB/T？AAAA-AAAA 是指：信息安全技术、信息系统安全等级保护定级指南
49.根据《信息安全等级保护管理办法》，如果对社会秩序、公共利益造成了严重损害，或对国家安全造成损害，该破坏应归属为安全保护等级的：三级
50.责制定有关密钥管理、数字签名、安全评估内容的组织是：ISO/IEC JTC1

二、填空题

51.IATF 提出了三个核心要素，分别是：人员、技术和操作
52.信息安全问题产生根源可分为内因和外因，其中信息安全内因主要来源于信息系统的复杂性
53.一个审计系统通常由三部分组成：日志记录器、分析器、通告器，分别用于收集数据、分析数据及通报结果
54.用户接口是为方便用户使用计算机资源所建立的用户和计算机之间的联系，主要有两类接口：作业级接口和程序级接口
55.TCG 可信计算系统结构可划分为三个层次，分别为可信平台模块、可信软件栈和可信平台应用软件
56.产生认证符的函数类型，通常由如下三类：消息加密、消息认证码和哈希函数
57.自主访问控制模型的实现机制通过访问控制矩阵实施，具体的实现办法是通过访问能力表或访问控制表来限定哪些主体针对哪些客体可以执行什么操作
58.现代 CPU 通常运行在两种模式下，即用户模式和内核模式
59.在 Unix/Linux 中，主要的审计工具是 syslogd 守护进程
60.用于设置数据库审计功能的 SQL 命令是 AUDIT
61.每个数据库事务均以 BEGIN TRANSACTION 语句显式开始，以 COMMIT 或 ROLLBACK 语句显式结束
62.ARP 协议的主要作用是完成 IP 地址到 MAC 地址之间的转换
63.IPSec 协议框架中包括两种网络安全协议，其中支持加密功能的安全协议是 ESP 协议
64.通过分析软件代码中变量的取值变化和语句的执行情况，来分析数据处理逻辑和程序的控制流关系，从而分析软件代码的潜在安全缺陷的技术是数据流分析技术

65.软件漏洞危险等级中最高的等级是紧急

66.攻击者通过精心构造超出数组范围的索引值，就能够对任意内存地址进行读写操作，这种漏洞称为数组越界漏洞

67.结合了程序理解和模糊测试的软件动态安全检测技术，称为智能模糊测试技术

68.对恶意程序进行查杀的最基本杀毒技术是特征码查杀技术

69.CC 评估等级每一级均需评估七个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估

70.关于国家秘密，机关、单位应当根据工作需要，确定具体的保密期限、解密时间，或者解密条件

三、综合题

71~76（6′，每空一分）

为了构建一个基于公有云的数据共享系统，要求：①数据加密之后上传到云服务器；②需要校验存储在云服务器数据的完整性；③数据加密密钥需要安全地发送给允许访问数据的用户

根据题意完成下列各题：假设要构建的应用系统允许使用的密码学算法包括 MD5、SHA1、AES、RSA、ECC 算法

（1）在数据上传之前，需要采用高效、安全的加密算法对数据进行加密，可采用的加密算法为 AES

（2）为了校验数据的完整性，需要计算所上传数据的消息摘要，为了获得更高的安全性，应该采用的密码学算法为 SHA1

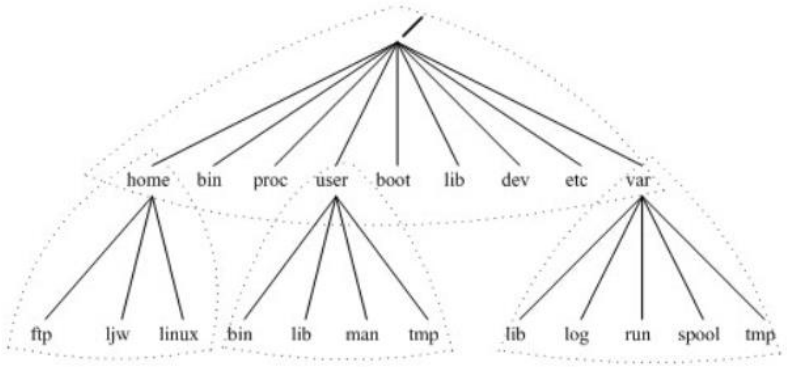
（3）假设用户 B 的公钥为 PUB，私钥为 PRI，为了将数据加密秘钥发送给用户 B，数据上传者将使用 B 的公钥 PUB 对该密钥进行加密；用户 B 则使用自己的私钥 PRI 进行解密

（4）消息摘要算法 MD5 对任意长度的明文产生 128 位的消息摘要

（5）为了确保 RSA 密码的安全，模数 n 至少 1024 位

77~80（4′，每空一分）

文件系统安全是UNIX/Linux系统安全的核心，请按要求完成相关的下列题目



（1）如图所示，树中的每项都由若干属性来描述，这些属性大多数保存在磁盘中一个称为“i 节点（inode）”的数据结构中。UNIX 文件系统安全就是基于 i 节点中三段关键信息：UID、GID 和模式。其中，UID 是指 A、模式是指 E（选择）

A、文件拥有者　　B、文件创建者　　C、文件所在分组　　D、文件所在盘符

E、文件的权限设置　　F、文件的操作类型

（2）使用 ls 命令查看 UNIX 文件权限显示的结果为“-rw-rw-rw-”，其中第一个“-”表示 B（选择）

A、任何人无法写入该文件　　B、该文件是一个正规文件

C、该文件不属于任何分组　　D、该文件是一个二进制文件

（3）在图中，表示特殊设备文件的目录文件是 dev

81~90（10′，每空一分）

如图1所示，A计算机和B计算机之间部署了防火墙进行NAT地址翻译，A计算机的IP地址为172.16.20.10，防火墙的IP地址为54.60.122.20，B计算机的IP地址为210.64.102.30。对于A计算机访问B计算机的网络请求，防火墙进行NAT地址翻译，请根据NAT地址翻译的原理，将图1中（1）、（2）、（3）、（4）四个数据包的源IP、源端口、目标IP、目标端口信息填入“NAT地址翻译表”中的相应位置。（每空1分，共10分）

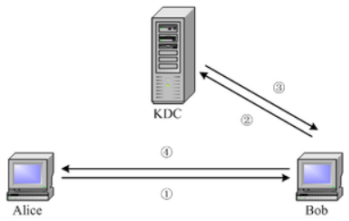


图1

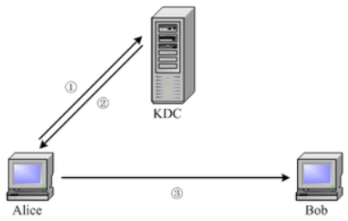


图2

表 NAT 地址翻译表

数据包序号	源 IP	源端口	目标 IP	目标端口
（1）	172.16.20.10	2025	210.64.102.30	8080
（2）	54.60.122.20	3680	210.64.102.30	8080
（3）	210.64.102.30	8080	54.60.122.20	3680
（4）	54.60.122.20	3680	172.16.20.10	2025

第六套

一、选择题

1.美国联邦政府颁布数字签名标准（Digital？Signature？Standard，DSS）的年份是：1994
2.信息安全技术包括：以上都对
3.美国联邦政府颁布高级加密标准（Advanced？Encryption？Standard，AES）的年份是：2001
4.信息安全技术的核心是：密码技术
5.有关单点登录，（错误的）是：单点登录可以细致地分配用户权限，实现细粒度的访问控制
6.产生认证码的方法（不包括）：消息摘要
7.Biba 模型属于：强制访问控制
8.关于 Kerberos 协议，（错误的）是：身份认证采用的是非对称加密机制
9.MAC 是指：强制访问控制
10.最早的代换密码是：Caesar 密码
11.DAC 是指：自主访问控制
12.（不属于）对称密码算法的是：ECC
13.（不能）通过消息认证技术解决的攻击：泄密
14.关于数据库安全特性检查，正确的：渗透测试的对象主要是数据库的身份验证系统和服务监听系统
15.（不属于）引导程序的是：MS-DOS
16.关于守护进程，正确的：守护进程通常周期性地执行某种任务或等待处理某些发生的事件
17.在 Windows 操作系统启动过程中，初始化工作后，从硬盘上读取 boot.ini 文件并进行系统选择的程序是：Ntldr
18.中国可信平台与 TCG 可信平台最根本的差异是：所使用的可信平台模块不同，TCG 可信平台使用了 TPM，而中国可信平台使用了可信密码模块 TCM
19.在 SQL 语句中，修改表中数据的基本命令是：UPDATE
20.下列操作中，（不能）在视图上完成的是：在视图上定义新的表
21.下列（错误的）是：RARP 协议的作用就是通过自身的 IP 获得对应的 MAC 地址
22.（不属于）主流捆绑技术的是：网站挂马捆绑
23.跨站点请求伪造攻击属于伪造客户端请求的一种攻击方式，简写为：CSRF
24.针对 80 端口传输的数据，专用的 Web 防火墙比普通的网络防火墙增加了：对应用层的过滤
25.Windows7 操作系统中，配置 IPSec 时支持的身份验证方法（不包括）：会话密钥
26.验证数字证书的真实性，是通过：验证证书中证书认证机构的数字签名来实现
27.SSL 协议中记录协议的作用：完成传输格式的定义
28.验证所收到的消息确实来自真正的发送方并且未被篡改的过程：消息认证
29.对传送的会话或文件密钥进行加密时，采用的密钥是：秘钥加密秘钥
30.下列漏洞中，描述为“由于程序处理文件等实体时在时序和同步方面存在问题，存在一个机会窗口使攻击者能够实施外来的影响”的是：竞争条件漏洞
31.国家信息安全漏洞共享平台的英文缩写是：CNVD
32.栈指针寄存器 esp 中保存的是：栈顶指针
33.在进行栈溢出漏洞利用时，不属于漏洞利用数据项的是：exploit

34.下列微软的安全技术，对程序分配的内存地址进行随机化分布的是：ASLR
35.（不属于）软件源代码静态安全检测技术的是：模糊测试
36.下列恶意程序传播手段中，利用网络服务程序的漏洞进行传播的是：局域网传播
37.为使审核效果最大化，并使体系审核过程的影响最小，必须的是：组织机构要对审核过程本身进行安全控制
38.风险评估主要依赖的因素，（不包括）：灾难恢复策略
39.信息安全管理的基本技术要求设计的五个方面是：物理安全、网络安全、主机安全、应用安全和数据安全
40.信息安全管理的主要内容包括：信息安全管理体系、信息安全风险管理和信息安全管理措施三个部分
41.风险评估分为：自评估和检查评估
42.“信息安全管理措施”详细介绍了：基本的管理措施和重要的管理过程
43.信息安全风险评估的复杂程度，取决于：受保护的资产对安全的敏感程度和所面临风险的复杂程度
44.《信息系统安全等级保护基本要求》所涉及到的基本技术要求，（不包含）：存储安全
45.国家秘密的保密期限，除另有规定，绝密级不超过：30 年
46.《信息系统安全保护等级划分准则》提出的定级四要素（不包括）：用户类型
47.CC 评估等级每一级均需评估七个功能类，即配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估
48.关于国家秘密，机关、单位应当根据工作需要，确定具体的：保密期限、解密时间，或者解密条件
49.ISO 13335 标准首次给出了关于 IT 安全的六个方面含义，包括：保密性、完整性、可用性、审计性、认证性和可靠性
50.《保守国家秘密》法第十九条规定，当国家秘密的保守期限已满时，下列做法（不正确）的是：无条件解密

二、填空题

51.保证信息机密性的核心技术是密码学
52.IATF 提出的信息保障的核心思想是：纵深防御战略
53.蜜网是在蜜罐技术基础上逐渐发展起来的一个新概念，又可称为诱捕网络
54.网络信息内容监控的主要方法为：网络舆情分析
55.扩散和混淆是对称密码设计的主要思想
56.序列密码，也被称为流密码，是将明文和密钥都划分为位或字符的序列，并且对明文序列中的每一位或字符都用密钥序列中的对应分量来加密
57.自主访问控制模型的实现机制通过访问控制矩阵实施，具体的实现办法是通过访问能力表或访问控制表来限定哪些主体针对哪些客体可以执行什么操作
58.操作系统使用保护环机制来确保进程不会在彼此之间或对系统的重要组件造成负面影响
59.在 Unix/Linux 系统中，服务是通过 inetd 进程或启动脚本来启动的
60.服务发现，也称为端口扫描，主要是对数据库的开放端口进行扫描，检查其中的安全缺陷，比如开放了多余的服务端口等
61.用于取消数据库审计功能的 SQL 命令是 NOAUDIT
62.证书链的起始端被称为信任锚
63.根据数据采集方式的不同，IDS 可以分为 NIDS 和 HIDS
64.会话劫持是一种通过窃取用户的 SessionID 后，利用它登录目标账户的攻击方法
65.美国国家漏洞数据库的英文简写为：NVD

66.按照漏洞生命周期的不同阶段进行的漏洞分类中，处于未公开状态的漏洞称为 0day 漏洞

67.软件加壳技术的原理是对可执行文件进行压缩或加密，从而改变可执行文件中代码的表现形式

68.软件漏洞危险等级中最低的等级是：低危

69.信息安全管理体系的主要内容，包括信息安全管理框架及其实施、信息安全管理体系审核与评审和信息安全管理体系的认证

70.《计算机信息系统安全保护等级划分准则》将信息系统安全分为自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级五个等级

三、综合题

71~75（6′，最后一空 2′，其余一空一分）

计划构建一个基于密码机制的网络数据安全传输系统，假设数据收发两端的用户分别为 Alice 和 Bob。回答问题：

（1）为了协商并保护数据传输密钥，一种简单有效的做法是采用公钥密钥体制：首先，Alice 在发送数据前，随机生成一个对称密钥，然后使用 Bob 的公钥对该密钥进行加密，并发送给 Bob；然后，Bob 收到密文后，便用自己的私钥进行解密即可得到 Alice 生成的对称密钥

（2）为了同时确保数据的完整性，可以利用 MD5 产生消息密文的认证码，该认证码的长度为 128 位

（3）假设 Alice 的 RSA 公钥为（e=3，n=15）。Bob 发送消息 m=4 给 Alice，则 Bob 对消息加密后得到的密文是 4。已知素数 p=3，q=5，则 Alice 的私钥 d=3

76~79（4′，每空一分）

为了增强数据库的安全性，按要求补全 SQL 语句：

（1）创建一个角色 R1：CREATE ROLE R1;

（2）为角色 R1 分配 Student 表的 INSERT、UPDATE、SELECT 权限：GRANT INSERT,UPDATE,SELECT?ON?TABLE?Student？TO?R1;

（3）减少角色 R1 的 SELECT 权限：REVOKE SELECT?ON?TABLE?Student?FROM?R1;

（4）将角色 R1 授予王平，使其具有角色 R1 所包含的全部权限：GRANT R1?TO?王平

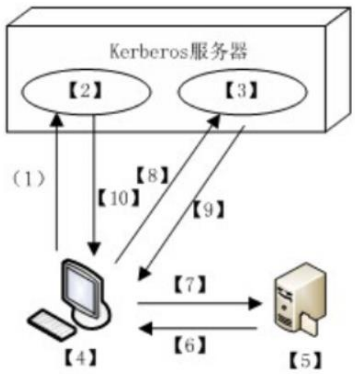
80~89（10′，每空一分）

按要求完成题目：

Kerberos V5 协议是属于应用层的安全协议。Kerberos V5 协议的参与者共三方：Client（用户计算机）、Server（用户计算机希望访问的应用服务器）和 Kerberos 服务器（为 Client 访问 Server 提供身份鉴别和权限许可的服务器）。其中，Kerberos 服务器包括：AS 服务器和 TGS 服务器。AS 服务器用于鉴别 Client 用户身份的真实性，TGS 服务器用于鉴别 Client 是否具有访问 Server 的权限。

（1）根据上述各参与方的名称，补充完整图中 Kerberos V5 协议的【2】~【5】

（2）Kerberos V5 协议通过 6 步实现对用户的认证，其中第 1 步已在图中标位（1），请将后续第 2 步到第 6 步的序号 2~6，填写到对应的【6】~【10】中正确的位置



【2】AS
【3】TGS
【4】Client
【5】Server
【6】6
【7】5
【8】3
【9】4
【10】2

第七套

一、选择题

1.Chinese Wall 安全策略的基础是：客户访问的信息不会与目前他们可支配的信息产生冲突
2.信息安全的五个基本属性包括：机密性、完整性、可用性、可控性和不可否认性
3.当代信息安全学起源于 20 世纪 40 年代的通信保密，主要关注信息在通信过程中的安全性，即“机密性”
4.中央于 2003 年 9 月颁布的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发 27 号文件），标志着我国信息安全保障体系建设工作的开始
5.属于保密性模型的是：Bell-Lapudula 模型
6.没有采用 Feistel 网络的密码算法是：AES
7.有关公钥存储，（错误的）是：需要对公钥进行机密性保护
8.完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，发现系统脆弱环节的过程是：渗透测试
9.美国联邦政府颁布数字签名标准（Digital Signature Standard,DSS）的年份：1994
10.（不属于）非对称密钥体制优点的是：加解密速度快，不需占用较多的资源
11.关于加密算法应用范围，正确的：DSS 用于数字签名，RSA 用于加密和签名
12.Alice 通过密钥 K2 加密消息 M 产生密文 E（K2,M），然后通过密钥 K1 生成 MAC 为 C（K1,E（K2,M））, 之后 Alice 将密文和 MAC 发送给 Bob；Bob 用密钥 K1 和密文生成一个 MAC 并和 Alice 的 MAC 比较，假如相同再用 K2 解密密文。该过程所提供的安全服务是：保密性和消息完整性
13.下列情景属于身份认证过程的是：用户依照系统提示输入用户名和口令
14.（不可以）通过事务处理回退的语句：DROP
15.用来做攻击诱捕的有真实操作系统的虚拟机系统，可以收集到丰富的主机响应信息的是：高交互蜜罐
16.完成用户代码请求操作系统服务的过程，所采用的方法是：系统调用
17.Windows 操作系统核心组件中，硬件抽象层组件是：HAL.dll
18.有关数据库安全，（错误的）是：防火墙能对 SQL 注入漏洞进行有效防范
19.“使用管理权限，恶意的开发人员可以禁用审计机制、开设伪造的账户以及转账等”，这类数据库安全威胁是：特权提升
20.（不能）将 CPU 模式从用户模式转到内核模式的方法是：系统调用
21.因为 IKE 建立在 ISAKMP 框架上，IKE 协商安全参数要经过：两个阶段
22.利用 Wireshark 对 IPSec 协议协商的前 10 个数据包进行网络嗅探，捕获的数据包是：ISAKMP 协议数据包
23.Ping 命令利用的是：ICMP 协议
24.（不支持）对 IP 地址进行扫描的是：Wireshark
25.（不能）防范网络嗅探工具对数据包进行嗅探的协议是：TELNET
26.静态包过滤防火墙技术对数据包进行过滤的协议层为：网络层和传输层
27.SSL 加密的协议层是：应用层
28.被称为半连接扫描的端口扫描技术是：TCP SYN 扫描
29.（不能）进行漏洞扫描的软件：Nmap
30.内存空间中用于存放动态数据的区域被称为：堆
31.通过教育培训，培养开发团队员工的安全意识，这是软件安全开发生命周期模型的：第 0 阶段

32.基于软件技术的安全保护方法（不包括）：加密狗
33.描述正确的是：栈是一个后进先出的数据结构，往低地址增长
34.关于堆和栈的描述，正确的：堆在内存中的增长方向是从低地址向高地址增长
35.指令寄存器 eip 中存放的指针始终指向：返回地址
36.恶意程序传播方法（不包括）：加壳
37.信息安全风险管理主要包括：风险的识别、风险的评估和风险控制策略
38.信息安全管理体系认证基于的原则是：自愿
39.为客体分配访问权限是实施组织机构安全性策略的重要部分，分配权限时依据的重要原则是：最少特权
40.在对一个计算机硬件资产的跟踪识别管理中，（不能）有效地识别该资产的属性是：软件版本号
41.在建立信息安全管理框架时，确定管制目标和选择管制措施所遵循的基本原则是：费用不高于风险所造成的损失
42.安全组织机构中的“三结合”指的是：领导、保卫和计算机技术人员相结合
43.信息安全管理体系是一个系统化、程序化和文件化的管理体系，它所属的范畴是：风险管理
44.信息技术安全评价通用标准（CC），是由六个国家联合提出，并逐渐形成国际标准：ISO 15408
45.ISO 13335 标准给出的 IT 安全六个方面的定义，包含：机密性、完整性、可靠性
46.中国信息安全测评中心的英文缩写是：CNITSEC
47.ISO 13335 标准首次给出了关于 IT 安全的 6 个方面含义：完整性、可用性、审计性、认证性、可靠性和机密性
48.电子签名认证证书应当载明的内容是：电子认证服务提供者名称、证书持有人名称、证书序列号、证书有效期、证书持有人电子签名验证数据
49.应当根据情况变化及时变更国家秘密的密级、知悉范围和保密期限
50.《信息安全等级保护管理办法》的五个安全保护等级中，描述为“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”的是：四级

二、填空题

51.信息系统安全保障涵盖三个方面：生命周期、保障要素和安全特征
52.P2DR 安全模型的核心是策略
53.恶意行为的监控方式主要分为两类：主机监测和网络监测
54.网络信息内容监控的主要方法为网络舆情分析
55.密码系统通常由五部分组成：消息空间、密文空间、密钥空间、加密算法和解密算法
56.密钥分配可以分为三类：人工密钥分发、基于中心的密钥分发和基于认证的密钥分发
57.常用的认证协议包括基于口令的认证协议、基于对称密码的认证协议和基于公钥密码的认证协议
58.每个数据库事务均以 BEGIN TRANSACTION 语句显示开始，以 COMMIT 或 ROLLBACK 语句显示结束
59.Select、Update 和 Insert 语句中，不能回退事务的是 SELECT
60.现在的许多操作系统并不经常使用第二保护环，有的甚至根本不用
61.Windows 有三种类型的事件日志：系统日志、应用程序日志和安全日志
62.IDS 的异常检测技术主要通过统计分析方法和神经网络方法实现
63.为了捕获网络接口收到的所有数据帧，网络嗅探工具会将网络接口设置为混杂模式
64.恶意程序会修改被感染计算机的 Hosts 文件，利用虚假 IP 地址的映像劫持技术来屏蔽被

感染计算机与安全站点之间的连接

65.根据软件漏洞具体条件，构造相应输入参数和 shellcode 代码，最终实现获得程序控制权的过程，被称为漏洞利用

66.通常情况下，软件动态安全检测技术检测漏洞的准确率高于软件静态安全检测技术

67.针对运行中的软件程序，通过构造非正常的输入来检测软件运行时是否出现故障或崩溃，这种软件检测技术被称为软件动态安全检测技术

68.专门寄生在具有宏功能的文档或模板中的计算机病毒被称为宏病毒

69.信息安全工作人员在上岗前、在岗期间和离职时都要严格按照人员安全控制策略执行安全措施

70.关于国家秘密，机关、单位应当根据工作需要，确定具体的保密期限、解密时间，或者解密条件

三、综合题

71~76（6′，每空一分）

在一个基于公钥密码机制的安全应用系统中，假设用户 Alice 和 Bob 分别拥有自己的公钥和私钥。请回答：

（1）在选择公钥密码 RSA、ECC 和 ElGamal 时，为了在相同安全性的基础上采用较短的密钥，应该选择其中的 ECC，且应确保选取的参数规模大于 160 位

（2）为了获得两方安全通信时所需的密钥，应用系统采用了基于中心的密钥分发，利用可信第三方 KDC 来实施。图 1 所示的密钥分发模型是推模型，图 2 所示的密钥分发模型是拉模型

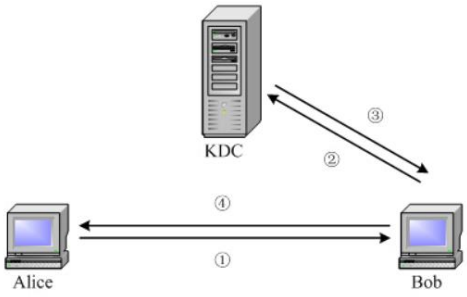


图1

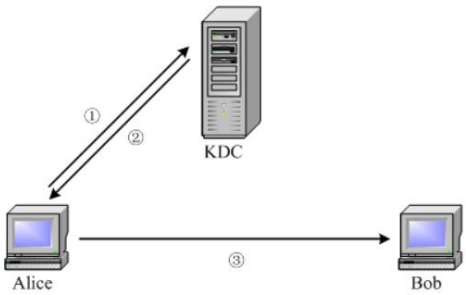


图2

（3）为了预防 Alice 抵赖，Bob 要求 Alice 对其发送的消息进行签名。Alice 将使用自己的私钥对消息签名；而 Bob 可以使用 Alice 的公钥对签名进行验证

77~80（4′，每空一分）

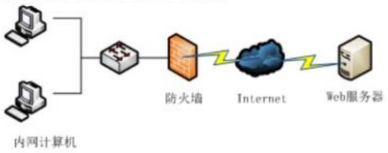
回答有关数据库自主存取控制问题：

（1）自主存取控制可以定义各个用户对不同数据现象的存取权限，向用户授予权限的 SQL 命令是 GRANT，如果指定了 WITH GRANT OPTION 子句，则获得某种权限的用户还可以把这种权限再授予其他的用户；向用户收回所授予权限的 SQL 命令是 REVOKE

（2）对数据库模式的授权则由 DBA 在创建用户时实现，如果在 CREATE USER 命令中没有指定创建的新用户的权限，默认该用户拥有 CONNECT 权限

81~90（10′，每空一分）

某公司网络拓扑图如下图所示。



现需要通过设置防火墙的包过滤规则，达到如下要求：

1）内网计算机的网段是10.102.50.*；

2）外网计算机不允许访问内网；

3）限制内网计算机只能访问IP为65.20.30.105的外网Web服务器，且仅允许访问该服务器上采用SSL协议（利用443端口提供服务）对外服务的网站。

请补充完整下面的包过滤规则表，其中“操作”可填选项包括“允许”和“拦截”两项。（每空1分，共10分）

规则	方向	源 IP	目标 IP	传输层协议	源端口	目标端口	标志位	操作
1	内网到外网	【1】	【2】	【3】	>1023	【4】	无	允许
2	外网到内网	【5】	【6】	【7】	【8】	>1023	ACK=1	【9】
3	任意网址到任意网址	任意	任意	任意	任意	任意	任意	【10】

【1】10.102.50.*

【2】65.20.30.105

【3】TCP

【4】443

【5】65.20.30.105

【6】10.102.50.*

【7】TCP

【8】443

【9】允许

【10】拦截

第八套

一、选择题

1.当代信息安全学起源于二十世纪四十年代的通讯保密，其中确保通信过程安全的核心技术是：密码学

2.美国第一个用于军事目的的计算机网络 ARPAnet 出现在：20 世纪 60 年代末

3.我国专家在 1999 年提出的更为完善的“保护-预警-监测-应急-恢复-反击”模型（即 PWDRRC 模型），使信息安全保障技术体系建立在更为坚实的基础之上

4.中央于 2003 年 9 月颁布的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发 27 号文），标志着我国信息安全保障体系建设工作的开始

5.假设 Alice 的 RSA 公钥为（e=3，n=55）。Bob 发送消息 m=14 给 Alice，则 Bob 对消息加密后得到的密文是：49

6.有关访问控制中客体和主体概念的说法，（错误的）是：主体只能是访问信息的程序、进程

7.属于序列密码算法的是：RC4

8.访问控制模型中，支持安全标签的是：强制访问控制

9.限定一个用户对一个客体目标访问的安全属性集合是：访问控制标签列表

10.Kerberos 协议设计的核心是：在用户的验证过程中引入一个可信的第三方，即 Kerberos 验证服务器

11.（不属于）网络中不良信息监控方法的是：帧过滤技术

12.有关对称密码，（错误的）是：IDEA 属于序列密码

13.AES 的整体结构采用的是：SP 网络

14.Linux 进程间通信时使用的特殊文件是：Sockets

15.使用 ls 命令查看 UNIX 文件权限显示的结果为“drw-r---w-”，说明拥有者对该文件：可读可写

16.可以替换 inetd 功能的是：xinetd

17.使用 ls 命令查看 UNIX 文件权限显示的结果为“drw-rw-rw-”，其中第一个“d”表示：该文件是一个目录

18.关于用户数字证书对应用户私钥的描述，（错误的）是：用户的私钥保存在数字证书中下发给用户

19.关于进程管理，（错误的）是：进程管理是通过系统调用来完成的

20.操作系统内核处于保护环结构中的：0 环

21.（不能）防范网络嗅探工具对数据包嗅探的技术是：VLAN

22.关于弱口令扫描技术，正确的：弱口令扫描主要包括：基于字典攻击的扫描技术和基于穷举攻击的扫描技术

23.将电子邮件发送到邮件服务器的简单邮件传输协议是：SMTP

24.UDP Flood 攻击是：耗尽目标主机网络带宽的攻击

25.（不属于）木马隐藏技术的是：反弹端口

26.防火墙能够防范的攻击的是：对内网的漏洞扫描攻击

27.Internet 上提供的一种查找相关域名、IP 地址、E-mail 信箱、联系电话等信息的服务是：whois

28.TCP 的端口号范围是：0~65535

29.Nmap 支持的扫描功能是：端口扫描

30.针对恶意程序检测查杀的主要技术，（不包括）：网络数据包查杀

31.服务器端的安全防护策略（不包括）：Web 服务器上应选择安全的、可信的浏览器
32.由国内机构维护的漏洞数据库是：CNVD
33.限制内存堆栈区的代码为不可执行状态的技术：DEP
34.限制内存堆栈区的代码为不可执行状态的技术：DEP
35.在微软的 SDL 模型中，第 0 阶段是：准备阶段
36.为了劫持进程的控制权，漏洞利用的核心是利用程序漏洞去执行：shellcode
37.在定义 ISMS 的范围时，为了使 ISMS 定义得更加完整，组织机构无需重点考虑的实际情况是：发展规划
38.审核准备是体系审核工作的一个重要阶段，准备阶段工作做得越细致，现场审核就越深入。准备工作（不包括）：确定不符合项并编写不符合报告
39.组织机构进行信息安全管理体系认证的目的，（不包括）：完全避免风险，避免损失
40.属于信息系统的安全考核指标的是：身份认证
41.信息安全管理体系属于：风险管理的范畴
42.建立信息安全管理框架时要确定管理目标和选择管理措施，其基本原则是：费用应不高于风险所造成的损失
43.信息安全管理体系审核，是指组织机构为验证所有安全程序的正确实施和检查信息系统符合安全实施标准的情况所进行的系统的、独立的检查和评价。它是信息安全管理体系的：一种自我保证手段
44.“泄露会使国家安全和利益遭受严重的损害”的保密级别是：机密级国家秘密
45.《信息系统安全等级保护划分准则》定级的四个要素，（不包括）：信息载体类型
46.有关商用密码管理政策的说法，正确的：商用密码的科研任务由国家密码管理机构制定的单位承担
47.信息技术安全评价的通用标准（CC）发布于：1998 年
48.美国国防部于 1985 年公布的被认为是计算机系统安全评估的第一个正式标准是：可信计算机系统安全评估标准（TCSEC）
49.CC 标准是信息技术安全评价的国际标准，我国与之对应的标准为：GB/T 18336
50.关于可靠的电子签名，（错误的）是：作为电子签名的加密密钥不可以更换

二、填空题

51.信息安全管理工作的核心是风险处置，信息安全管理工作的基础是风险评估
52.在信息安全发展的通信保密阶段，人们主要关注信息在通信过程中的安全性问题，即“机密性”
53.将未使用地址空间伪装成活动网络空间，通过与入侵者的主动交互获取入侵详细信息，以达到对攻击活动进行监视、检测和分析的目的的网络监测技术是蜜罐技术
54.密码系统通常由五部分组成：消息空间、密文空间、密钥空间、加密算法和解密算法
55.密钥分配可以分成三类：人工密钥分发、基于中心的密钥分发和基于认证的密钥分发
56.用的认证协议包括基于口令的认证协议、基于对称密码的认证协议和基于公钥密码的认证协议
57.基于角色的访问控制（RBAC，Role-based Access）模型的要素包括用户、角色和许可等基本定义
58.定义一个用户的数据库存取权限，就是要定义这个用户可以在哪些数据库对象上进行哪些类型的操作
59.操作系统为 0 环和 1 环执行指令时，它在管理员模式或内核模式下运行
60.在 UNIX 系统中，只要将用户的 UID 和 GID 设置为 0 就可以将其变成超级用户
61.Windows 有三种类型的事件日志：系统日志、应用程序日志和安全日志

62.可以通过网络等途径，自动将自身的全部或部分代码复制传播给网络中其它计算机的完全独立可运行程序是蠕虫

63.SSL 协议中，客户通过对服务器端发来的证书进行验证，以完成对服务器端的身份认证

64.窃取用户 SessionID 后，使用该 SessionID 登录进入目标账户的攻击方法被称为会话劫持

65.限制内存堆栈区的代码为不可执行的状态，从而防范溢出后代码的执行，这种技术被称为数据执行保护

66.自主访问控制模型的实现机制是控制矩阵通过实施的，而具体的实现办法，则是通过访问能力表或访问控制表来限定哪些主体针对哪些客体可以执行什么操作

67.恶意行为审计与监控，主要监测网络中针对服务器的恶意行为，包括恶意的攻击行为和入侵行为

68.恶意行为的监测方式主要分为两类：主机监测和网络监测

69.信息安全管理体系（ISMS）是一个系统化、程序化和文件化的管理体系，属于风险管理的范畴，体系的建立基于系统、全面和科学的安全风险评估

70.电子签名认证证书应当载明下列内容：电子认证服务者名称、证书持有人名称、证书序列号和证书有效期

三、综合题

71~75（6′，最后一空两分，其余一空一分）

在网络通信环境中，可能有下述攻击:

①泄密：将消息透露给没有合法密钥的任何人或程序。

②传输分析：分析通信双方的通信模式。在面向连接的应用中，确定连接的频率和持续时间；在面向连接或无连接的环境中，确定双方的消息数量和长度。

③伪装：欺诈源向网络中插入一条消息。如攻击者产生一条消息并声称这条消息是来自某合法实体，或者非消息接收方发送的关于收到或未收到消息的欺诈应答。

④内容修改：对消息内容的修改，包括插入、删除、转换和修改。

⑤顺序修改：对通信双方消息顺序的修改，包括插入、删除和重新排序。

⑥计时修改：对消息的延时和重放。

⑦发送方否认：发送方否认发送过某消息。

⑧接收方否认：接收方否认接收到某消息。

请回答下列题目：

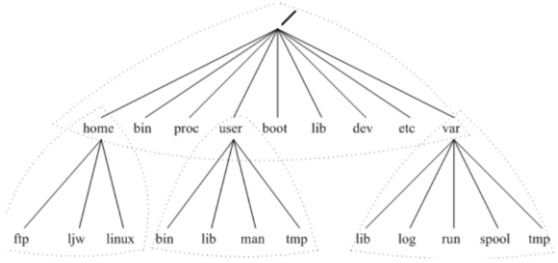
（1）防范前两种攻击的方法是消息加密；防范第 3 种到第 6 种攻击的方法一般称为消息认证；防范第 7 种攻击的方法属于数字签名

（2）在利用 SHA 算法产生消息密文的认证码时，认证码的长度为 160 位

（3）在加密消息时，假设某用户的 RSA 公钥为（e=3，n=15）。Bob 发送消息 m=5 给 Alice，则 Bob 对消息加密后得到的密文是 5

76~79（4′，每空一分）

文件系统安全是 UNIX/Linux 系统安全的核心，按要求完成题目：



（1）当攻击者篡改文件时，他们经常因修改 i 节点设置而留下一个足印，该足印有时能用

来作为搜索攻击者的证据

（2）在上图中，表示用户命令的可执行文件（二进制）的目录文件是：bin

（3）每个文件和目录有三组权限与之相关：一组为文件的拥有者，一组为文件所属分组的成员，一组为其它的所有用户（通常用“theworld”或“others”指代）。ls-l 命令可以查看 UNIX 文件权限，如果

$ls-l

-rw-rw-rw- 3 jrandom albion 15 Apr 14 1998 mbox

则表示：mbox 是一个文件，分组成员有可读、可写权限

80~89（10′，每空一分）

在下图中，内网有两台计算机 A 和 B，通过交换机连接到网关，最后连入互联网，其中计算机 A 的 IP 地址为 172.16.3.20，MAC 地址为 MACA；计算机 B 的 IP 地址为 172.16.3.30，MAC 地址为 MACB；网关设备的 IP 地址为 69.70.2.1，MAC 地址为 MACW。请完成下列题目：

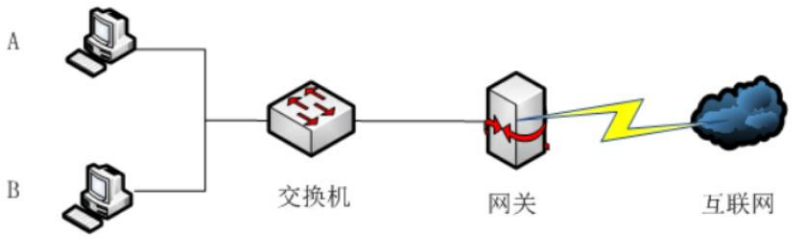


图　网络拓扑图

（1）计算机 B 感染了 ARP 病毒，此 ARP 病毒向其它内网计算机发起伪装网关 ARP 欺骗攻击，它发送的 ARP 欺骗数据包中，IP 地址为 69.70.2.1，MAC 地址为 MACB

（2）为了防止 ARP 欺骗，需要在内网计算机和网关设备上进行 IP 地址与 MAC 地址的双向静态绑定。

首先，在内网中的计算机 A 设置防止伪装网关欺骗攻击的静态绑定：

arp -d //清空 ARP 缓存表

arp -s 69.70.2.1 MACW //将 IP 地址与 MAC 地址静态绑定

然后，在网关设备中对计算机 A 设置 IP 地址与 MAC 地址的绑定：

arp -d //清空 ARP 缓存表

arp -s 172.16.3.20 MACA //将 IP 地址与 MAC 地址静态绑定

第九套

一、选择题

1.关于信息技术积极影响的说法，正确的：全对
2.人为的网络攻击是信息安全问题产生的：外因
3.P2DR 安全模型的 4 个主要部分，（不包括）：计划
4.1972 年完成的著名的 Anderson 报告，是计算机安全发展的重要里程碑
5.系统产生一个随机数 r，并对其加密提供给用户；用户解密后计算 r+1 的加密密文，并与用户返回的值进行比较，若两者相等，则系统认为用户的身份为真。该身份认证过程是：一次性口令认证
6.有关智能卡存储用户私钥的说法，（错误的）是：易于全面推广
7.（不属于）数据库渗透测试的是：发现数据库服务端口
8.（不属于）数据库安全检测的是：入侵检测
9.哈希函数属于：单向函数
10.两个通信终端用户在一次交换数据时所采用的密钥是：会话密钥
11.两个通信终端用户在以此交换数据时所采用的密钥是：会话密钥
12.AAA 管理（不包括）：访问控制
13.（不属于）分布式访问控制方法的是：Diameter
14.在 Linux/UNIX 系统中，用户命令的可执行文件通常存放在：/bin
15.将查询结果中的重复元组去掉的 SQL 子句是：DISTINCT
16.关于视图的描述，（错误的）是：视图机制的安全保护功能比较精细，通常能达到应用系统的要求
17.能创建基本表和视图，但是不能创建模式和新用户的权限是：RESOURCE 权限
18.（不可以）将 CPU 模式从用户模式转到内核模式的是：系统调用
19. 在 Linux/UNIX 系统中，编号为 1 的进程是：init
20.关于保护环机制的说法，（错误的）是：环号越低，赋予运行在该环内的进程的权限就越小
21.为了防止网络攻击者对目标主机和网络的扫描，可部署：防火墙
22.采用 rootkit 技术的木马属于：第五代木马
23.SYN-Flood 属于：TCP 协议层攻击
24.跨站点请求伪造攻击伪造的是：客户端请求
25.“192.169.1.1”属于：C 类 IP 地址
26.有关 TCP 标志位的说法，（错误的）是：PSH 标志位表示出现差错，必须释放 TCP 连接重新建立新连接
27.有关 IPS 功能的描述中，正确的：IPS 具有在应用层进行拦截和检测的功能
28.SSL 协议中握手协议的作用是：完成传输格式的定义
29.依据映射方式的不同，NAT 分为三种类型，（不包括）：动态 NAT
30.关于软件安全检测技术的描述中，（错误的）是：软件动态安全检测技术的直接分析对象是软件源代码和可执行代码
31.（不属于）软件安全保护技术的是：模型检验技术
32.（不属于）恶意程序检测查杀技术的是：移动介质查杀
33.数组越界漏洞触发式的特征，（不包括）：对整型变量进行运算时没有考虑到其边界范围
34.将内存中敏感区域设置为不可执行（non-executable）状态，从而在溢出后即使跳转到恶意代码的地址，恶意代码也将无法运行，这种技术是：DEP

35.常用的软件测试方法（不包括）：蓝盒测试
36.软件的动态安全检测技术（不包括）：词法分析
37.要制定一套好的安全管理策略，必须与决策层进行有效沟通，并得到组织机构高层领导的支持与承诺。其作用（不包括）：制定的安全管理策略能够充分体现组织机构业务特征
38.首次给出关于 IT 安全的机密性、完整性、可用性、审计性、认证性和可靠性 6 个方面含义的标准是：ISO 13335
39.组织机构实施信息安全管理体系认证所根据的国际信息安全管理标准为：BS7799 标准
40.风险管理的第一阶段是：风险识别
41.电子认证服务提供者签发的电子签名认证证书应当载明的内容，（不包括）：证书涉及的私钥
42.违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机系统，处有期徒刑 3 年以下
43.国家秘密的密级分为：秘密、机密、绝密三级
44.根据《信息安全等级保护管理办法》，信息系统分为：五个安全保护等级
45.机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级，同时确定：保密期限和知悉范围
46.绝密级国家秘密是最重要的国家秘密，对其描述最准确的是：泄露会使国家安全和利益遭受特别严重的损害
47.关于 GB/T 18336《信息技术安全性评估准则》的优点，（错误的）是：评估结果最终是一个客观参考性的结果，是一个通过或者未通过的声明，但对企业的实际指导意义很强
48.基于对电子签名认证证书或者电子签名的信赖，从事有关活动的人或机构被称为：电子签名依赖方
49.有关数据库安全，（错误的）是：用户可能将合法的数据库权限用于未经授权的目的，这种威胁是过度的特权滥用
50.对数据库的开放端口进行扫描，检查其中的安全缺陷，比如开放了多余的服务端口等，这种数据库安全检测是：服务发现

二、填空题

51.信息安全保障工作的内容包括：确定安全需求、设计和实施安全方案、进行信息安全评测和实施信息安全监控与维护
52.在计算机系统中，认证、访问控制和审计共同建立了保护系统安全的基础，其中的最后一项是对认证和访问控制的有效补充
53.蜜罐技术是一种网络监测技术，它将未使用地址空间伪装成活动网络空间，通过与入侵者的主动交互获取入侵详细信息，以达到对攻击活动进行监视、检测和分析的目的
54.信任根和信任链是可信计算平台最主要的关键技术之一
55.密码设计应遵循一个公开设计的原则，即密钥体制的安全应依赖于对密钥的保密，而不应依赖于对算法的保密
56.主要适用于有严格的层次级别划分的大型组织机构和行业领域的信任模型是信任模型
57.安全散列算法 SHA 所产生的摘要比消息摘要算法 MD5 长 32 位
58.在数据库中，用户权限是由两个要素组成的：数据库对象和操作类型
59.在 CREATE TABLE 语句中使用子句，DEFAULT 是定义默认值首选的方法
60.当用户身份被确认合法后，赋予该用户进行文件和数据等操作权限的过程称为授权
61.当用户代码需要请求操作系统提供的服务时，通常采用系统调用的方法来完成这一过程
62.两台配置了 IPSec 协议的 Windows 计算机进行 IPSec 初始连接时，通过 Wireshark 嗅探的前面 10 个数据包是 ISAKMP 协议的数据包

63.支持多种不同类型的 CA 系统相互传递信任关系的是桥 CA 信任模型
64.根据软件漏洞具体条件，构造相应输入参数和 Shellcode 代码，最终实现获得程序控制权的过程，是漏洞利用
65.攻击者窃取 Web 用户 SessionID 后，使用该 SessionID 登录进入 Web 目标账户的攻击方法，被称为会话劫持
66.通过分析代码中输入数据对程序执行路径的影响，以发现不可信的输入数据导致的程序执行异常，这种技术被称为污点传播分析技术
67.栈指针寄存器 esp 始终存放栈顶指针
68.攻击者通过精心构造超出数组范围的索引值，就能够对任意内存地址进行读写操作，这种漏洞被称为数组越界漏洞
69.信息安全风险评估的复杂程度，取决于受保护的资产对安全的敏感程度和所面临风险的复杂程度
70.《计算机信息系统安全保护等级划分准则》将信息系统安全分为自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级五个等级

三、综合题

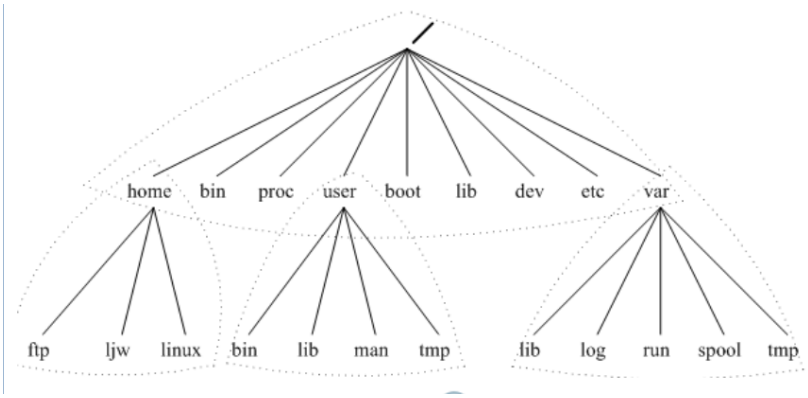
71~75（6′，倒数第二空两分，其余一空一分）

按要求完成有关数字签名题目：
（1）一个数字签名体制都要包括两个过程：签名和验证签名
（2）假设用户 A 和用户 B 利用公开密钥密码进行数字签名
①签名的时候，用户 A 将使用自己的私有密钥对明文数据 M 进行签名
②用户 B 收到签名后，将使用用户 A 的公开密钥对签名进行认证
（3）假设 Alice 的 RSA 公钥为（e=3，n=33），已知素数 p=3，q=11，则 Alice 的私钥 d=7。Alice 要发送消息 m=3 给 Bob，并对该消息进行签名后得到的签名是 9

(3) 根据RSA算法，由p、q算出：φ(n) = (p-1)*(q-1) = 2*10=20，再由e*d mod φ(n) = 1
可知：3*d mod 20 = 1可求得私钥d=7
若Alice发送消息m=3给Bob，并对消息m进行签名，所以需要使用Alice的私钥d签名，签名算法是m^d mod n = 3^7 mod 33 = 9，所以Alice发送的签名是 9

76~79（4′，每空一分）

文件系统安全是 UNIX/Linux 系统安全的核心，完成下列题目：



（1）当攻击者篡改文件时，他们经常因修改 i 节点设置而留下一个足印，该足印有时能用来作为搜索攻击者的证据
（2）在上图中，表示用户命令的可执行文件（二进制）的目录文件是/bin
（3）每个文件和目录有三组权限与之相关：一组为文件的拥有者，一组为文件所属分组的成员，一组为其它所有用户（通常用“theworld”或“others”指代）。ls-l 命令可以查看

UNIX 文件权限，如果

$ls-l

-rw-rw-rw- 3 jrandom albion 15 Apr 14 1998 mbox

则表示：mbox 是一个文件，分组成员有可读、可写权限

80~89（10′，每空一分）

完成下列题目：

（1）IPSec 协议是一组开放协议的总称，和 SSL 协议不同，IPSec 协议对网络层协议数据封装后进行传输，而 SSL 协议对应用层协议数据进行加密后传输

（2）IPSec 协议包括网络安全协议和密钥上协商协议两部分。其中，网络安全协议又包括两种协议。根据对数据包中封装内容的不同，这两种协议又分为两种封装模式。下面的图 1 至图 4 为两种协议不同模式下的封装格式示意图，补充图中的内容

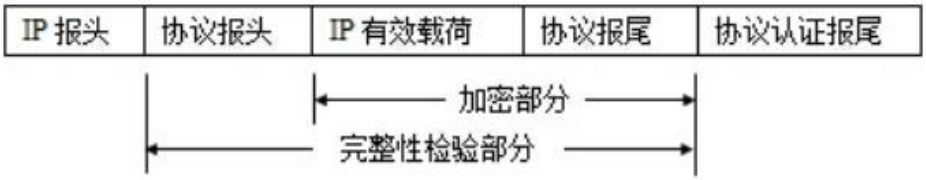


图 1 安全载荷封装（或 ESP）协议传输模式的封装格式

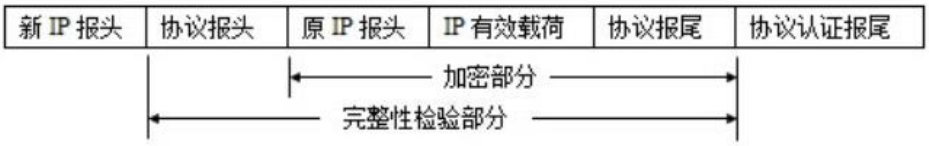


图 2 安全载荷封装（或 ESP）协议隧道模式的封装格式

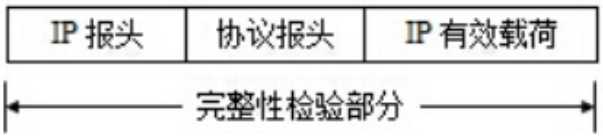


图 3 认证协议头（或 AH）协议传输模式的封装格式

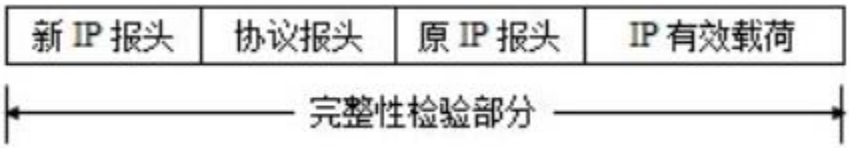


图 4 认证协议头（或 AH）协议隧道模式的封装格式

第十套

一、选择题

1.信息系统所面临的安全风险包括：全是
2.信息安全问题产生的根源中，内因是：信息系统的复杂性
3.信息系统的飞速发展，对人类社会产生了重要影响，其主流是积极的，但也客观存在一些负面影响。（不属于）信息技术消极影响的是：信息爆炸
4.宣告科学的密码学时代到来的文献是：《保密系统的通信理论》
5.（不属于）身份认证手段的是：消息认证
6.数字签名的签名过程使用的是签名者的：私钥
7.已知最早的代换密码是：Caesar 密码
8.有关密码分组链模式，（错误的）是：在一些非加密场景下是不能应用的，比如报文鉴别与认证
9.属于哈希函数特点的是：抗碰撞性
10.美国联邦政府在上世纪 90 年代制定的数字签名标准是：DSS
11.能够抵抗内容修改、顺序修改等攻击的技术是：消息认证
12.有关 RADIUS 协议，（错误的）是：是一种非集中式访问控制技术
13.属于网络中不良信息监控方法的是：网址过滤技术
14.（无法）将 CPU 模式从用户模式转到内核模式的是：系统调用
15.有关 UNIX/Linux 系统安全，（错误的）是：UNIX/Linux 超级用户账户只有一个
16.在 Windows 系统中，可以通过修改日志文件访问权限防止日志信息被清空，但采用的文件系统格式必须是：NTFS
17.在 Windows 系统中，表示可以穿越目录并进入其子目录的权限是：Execute
18.TCB 是指：可信计算基
19.在数据库内部，有的内置函数和过程存在严重的安全漏洞，比如缓冲区溢出漏洞。这些安全漏洞的一个重要特征是：每个安全漏洞只存在于相应的某个具体版本
20.两台配置了 IPSec 协议的 Windows 计算机进行 IPSec 初始连接时，通过 Wireshark 嗅探的 IPSec 前面 10 个数据包的协议类型是：ISAKMP
21.支持多种不同类型的 CA 系统相互传递信任关系的信任模型是：桥 CA 信任模型
22.下列协议层发生的攻击行为，IPS 可以检测拦截而硬件包过滤防火墙不能检测拦截的是：应用层
23.根据 IDS 检测入侵行为的方式和原理的不同，IDS 的检测技术可以分为基于异常检测和基于误用检测
24.在 TCP 三次握手中，第三次握手的数据包的 SYN 和 ACK 标志位分别为：0,1
25.有关 UDP 和 TCP 协议的描述，（错误的）是：UDP 是面向连接的传输层协议
26.有关 SMTP 协议的描述，（错误的）是：SMTP 在传输层基于 UDP 协议进行传输
27.为判断目标主机是否连通，ping 命令利用的是：ICMP 协议
28.网站挂马能成功实施的前提条件，（不包括）：用户计算机中没有安装杀毒软件或主动防御软件
29.（不属于）软件漏洞特点的是：软件漏洞存在的非长期性
30.在缓冲区和函数返回地址增加一个 32 位的随机数 security_cookie，在函数返回时，调用检查函数检查 security_cookie 的值是否有变化，这种保护技术是：GS
31.软件开发生命周期模型（不包括）：线性模型
32.在软件开发的设计阶段，应用的安全设计原则（不包括）：权限关联原则

33.微软的软件安全开发生命周期模型中最早的阶段是：第 0 阶段：准备阶段
34.静态安全分析技术检测源代码安全缺陷和漏洞的主要优势是：不需要构建代码运行环境，分析效率高，资源消耗低
35.通过分析代码中输入数据对程序执行路径的影响，以发现不可信的输入数据导致的程序执行异常，被称为：污点传播分析技术
36.信息安全管理体系（ISMS）是一个系统化、程序化和文件化的管理体系，属于风险管理的范畴，体系的建立基于系统、全面和科学的安全风险评估
37.为了风险管理的需要，一本方针手册还是必要的。手册一般包括的内容有：全部
38.在信息安全管理措施中，事故响应的四个阶段分别为计划、检测、反应和恢复
39.信息安全管理体系审核包括两方面审核，即技术和管理
40.信息安全管理体系（ISMS）建立的基础是：安全风险评估
41.信息安全政策是一个组织机构的信息安全的：最高方针
42.进行信息安全风险评估时，所采取的评估措施与组织机构对信息资产风险的保护需求相一致。具体的风险评估方法有：三种
43.CC 标准将评估过程划分为两部分，即功能和保证
44.《信息系统安全保护等级划分准则》中提出了定级的四个要素：信息系统所属类型、业务数据类型、业务自动化处理程度和信息系统服务范围
45.涉及国家安全和利益的事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为：国家秘密
46.根据国家商用密码管理政策，商用密码产品须由国家密码管理机构许可的单位销售。未经许可，任何单位或者个人不得销售商用密码产品
47.我国于 1984 年成立了全国信息技术安全标准化技术委员会，其缩写为：CITS
48.国际信息安全标准化组织（不包括）：WTO
49.与我国标准 GB/T 18336 对应的国际标准为：ISO 15408
50.《刑法》有关信息安全犯罪的规定第 285 条：违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的处 3 年以下有期徒刑或拘役

二、填空题

51.DES 密码的结构基于 Feistel 网络
52.无论是对称密码还是非对称密码，其安全性实际取决于对密钥的安全保护
53.AAA 是指认证、授权和审计
54.通过对日志进行分析，发现所需事件信息和规律是安全审计的根本目的
55.在 20 世纪 90 年代初提出了两种有效的对称密码的选择明文分析方法：差分分析和线性分析
56.当操作系统为 0 环和 1 环时，它在管理员模式或内核模式下运行
57.UNIX 文件系统安全基于 i 节点中的三段关键信息，即文件拥有者、文件所在分组和模式
58.TCG 定义可信计算平台的信任根包括三个根：可信测量根、可信存储根和可信报告根
59.在数据库中，为不同的用户定义不同的视图，可以限制其访问范围
60.根据 IDS 检测入侵行为的方式和原理的不同，可以分为基于误用检测的 IDS 和基于异常检测的 IDS
61.Webshell 与被控制的服务器通过 80 端口传递交互的数据
62.可以通过网络等途径，自动将自身的全部或部分代码复制传播给网络中其它计算机的完全独立可运行程序是蠕虫
63.在不实际执行程序的前提下，将程序的输入表示成符号，根据程序的执行流程和输入参

数的赋值变化，将程序的输出表示成包含这些符号的逻辑或算术表达式，这种技术被称为符号执行技术

64.信息安全风险评估的复杂程度，取决于受保护资产的对安全的敏感程度和所面临风险的复杂程度

65.Web 安全检测技术包括黑盒检测和白盒检测两种主要检测技术

66.软件保护技术中，通过对可执行文件的压缩或者加密，进而改变可执行文件中的代码表现形式以增加动态逆向分析的难度，被称为软件加壳技术

67.CC 评估等级每一级均需评估七个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估

68.中国信息安全测评中心的英文简称是 CNITSEC

69.《计算机信息系统安全保护等级划分准则》主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计

70.CC 评估等级每一级均需评估 7 个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估

三、综合题

71~76（6′，每空一分）

在一个基于公钥密码机制的安全应用系统中，假设用户 Alice 和 Bob 分别拥有自己的公钥和私钥，回答问题：

（1）在产生 Alice 和 Bob 的密钥时，如果采用 RSA 算法，选取的模数 n 至少要有 1024 位，如果采用椭圆曲线密码，选取的参数 p 的规模应不少于 160 位

（2）基于公钥证书的密钥分发方法是目前广泛流行的密钥分发机制，用户可将自己的公钥通过证书发给另一用户，接收方可用证书管理机构的公钥对证书加以验证

（3）实际应用中为了缩短签名的长度、提高签名的速度，而且为了更安全，常对信息的摘要进行签名

（4）基于公钥密码也可以实现身份认证，假定 Alice 和 Bob 已经知道对方的公钥，Alice 为了认证 Bob 的身份：

首先，Alice 发送给 Bob 一个随机数 a，即 Alice→Bob：a；

然后，Bob 产生一个随机数 b，并将 b 及通过其私钥所产生的签名信息发送给 Alice，假设用 SignB 表示用 Bob 的私钥产生数字签名的算法，即 Bob→Alice：n||SignB（a||b）；

最后，为了认证 Bob 的身份，Alice 得到随机数 b 和签名信息之后，只需要使用 Bob 的公钥对签名信息进行解密，验证解密的结果是否等于 a||b 即可

77~80（4′，每空一分）

补全有关 Windows 的安全实践：

（1）Winlogon 调用 GINA DLL，并监视安全认证序列，所调用的 DLL 将提供一个交互式的界面为用户登录提供认证请求

（2）为了防止网络黑客在网络上猜出用户的密码，可以在连续多次无效登录之后对用户账号实行锁定策略

（3）在 Windows 系统中，任何涉及安全对象的活动都应该受到审核，审核报告将被写入安全日志中，可以使用“事件查看器”来查看

（4）为了增强对日志的保护，可以编辑注册表来改变日志的存储目录。点击“开始”→“运行”，在对话框中输入命令“Regedit”，回车后将弹出注册表编辑器

81~90（10′，每空一分）

下图为通过防火墙NAT功能进行地址翻译的示意图。其中，内网计算机的IP为172.16.36.18，它通过防火墙的NAT进行IP地址翻译后，连接外网IP为105.49.90.20的Web服务器；防火墙的公网IP地址为59.86.106.55。

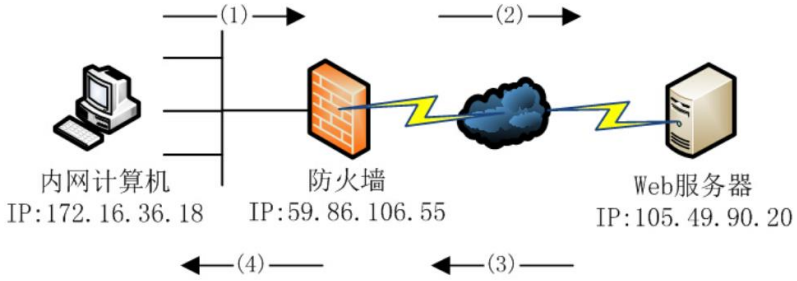


图 NAT地址翻译网络环境

请根据NAT地址翻译的流程，补充下表中的空白。

表 NAT地址翻译的流程

序号	源 IP	源端口	目标 IP	目标端口
（1）	172.16.36.18	1620	105.49.90.20	80
（2）	59.86.106.55	5875	105.49.90.20	80
（3）	105.49.90.20	80	59.86.106.55	5875
（4）	59.86.106.55	5875	172.16.36.18	1620

第十一套

一、选择题

1.关于信息与知识、信号、数据、情报关系的说法，（错误的）是：信息是信号的载体，信号是信息所承载的内容

2.信息安全发展大致经过了 3 个阶段，（不包括）：互联网安全阶段

3.中央于 2003 年 9 月颁布的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发 27 号文件），标志着我国信息安全保障体系建设工作的开始

4.信息保障技术框架（IATF）的核心要素（不包括）：纵深防御战略

5.在对称密码设计中，用以达到扩散和混淆目的的方法是：乘积迭代

6.有关密码分组链模式（即 CBC），（错误的）是：在一些非加密场景下是不能应用的，比如报文鉴别与认证

7.对传送的会话或文件密钥进行加密时采用的密钥：密钥加密密钥

8.（不属于）哈希函数特点的是：可逆性

9.MD5 算法的消息摘要长度为：128

10.哈希函数不能应用于：消息加密

11.属于保密性强制访问控制模型的是：Bell-LaPudula 模型

12.RADIUS 是指：拨号用户远程认证服务

13.网络内容监控的主要方法是：网络舆情分析

14.在保护环结构中，操作系统内核处于：0 环

15.有关 UNIX/Linux 系统安全，（错误的）是：通常情况下，建议使用超级用户登录，以拥有更多权限

16.在 Windows NT 里，口令字密文保存在：SAM 文件

17.在 Windows 系统中，表示可以穿越目录并进入其子目录的权限是：Execute（X）

18.TPCM 是指：可信平台控制模块

19.有关数据库安全，（错误的）是：使用管理权限，恶意的开发人员可以禁用审计机制、开设伪造的账户以及转账等，这种威胁是过度的特权滥用

20.在数据库内部，有的内置函数和过程存在严重的安全漏洞，比如缓冲区溢出漏洞。这些安全漏洞一个重要的特征是：每个安全漏洞只存在于相应的某个具体版本

21.（不能）扫描网络端口的工具是：tracert

22.为了捕获网络接口收到的所有数据帧，网络嗅探工具会将网络接口设置为：混杂模式

23.主要的捆绑技术（不包括）：网站钓鱼捆绑

24.属于内核隐藏技术的是：RootKit 技术

25.木马的特点中（不包括）：感染性

26.根据数据采集方式的不同，IDS 可以分为：NIDS 和 HIDS

27.IDS 探测器连接到：交换机的网络端口

28.攻击者利用栈溢出发起攻击时，向存在漏洞的软件程序输入的数据不包括：原返回地址

29.关于 SEHOP，（错误的）是：SEHOP 是 Windows 异常处理机制中所采用的重要数据结构链表

30.安全测试往往需要从攻击者的角度开展测试，（不属于）安全测试的是：全面测试软件的功能实现

31.在软件设计初期，就需要按照安全设计的原则对软件进行全面考虑，（不属于）安全设计原则的是：避免代码重用

32.可对 Windows 系统文件进行签名验证的微软工具是：sigverif

33.（不属于）逆向分析辅助工具的是：Wireshark
34.恶意程序对计算机感染后的破坏功能，（不包括）：诱骗下载
35.在信息安全事故响应中，（非必须）采取的措施是：首先保护物理资产的安全，然后尽可能保护人员的生命安全
36.对系统开发过程的描述中，（错误的）是：系统的生命周期是无限长的
37.（不属于）应急计划三元素的是：基本风险评估
38.在信息资产管理中，（不属于）标准信息系统因特网组件的是：不间断电源
39.在信息资产管理中，标准信息系统的组成部分（不包括）：解决方案
40.在信息安全管理中的控制策略实现后，接下来要采取的措施（不包括）：逐步消减安全控制方面的开支
41.关于信息安全管理体系认证，（错误的）是：每个组织都必须进行认证
42.信息安全管理体系的审核准备工作（不包括）：加强安全意识教育
43.信息安全管理体系体现的主要思想是：预防控制为主
44.风险管理包括两个主要任务：风险识别和风险控制
45.依据涉密信息系统分级保护管理规范和技术标准，涉密信息系统建设使用单位将保密级别分为三级，即秘密 机密 绝密
46.关于可靠的电子签名，正确的：电子签名制作数据用于电子签名时，属于电子签名人专有
47.企业销售商用密码产品时，应向国家密码管理机构申请，必需具备的条件是：有独立的法人资格
48.由于社会群体中个人文化水准、道德观念、价值取向等千差万别，必然导致一些不良网络行为。下列网络行为涉嫌违法的是：人肉搜索
49.电子认证服务提供者由于违法行为被吊销电子认证许可证书后，其直接负责的主管人员和其他直接责任人员不得从事电子认证服务的时间期限为：10 年
50.GB/T 22239 标准（《信息系统安全等级保护基本要求》）提出和规定了对不同安全保护等级信息系统的最低保护要求，称为：基本安全要求

二、填空题

51.信息安全的五种基本属性是机密性、完整性、可控性、可用性和不可否认性
52.IATF（Information Assurance Technical Framework）是美国国家安全局制定的描述信息保障的指导性文件，其中提出了三个主要核心要素，即人员、技术和操作
53.DES 算法的密钥长度是 64 位，但其中有 8 位被用做奇偶校验
54.消息加密本身提供了一种认证手段。在这种方法中，整个消息的密文作为认证码
55.基于矩阵的列的访问控制信息表示的是访问控制表，即每个客体附加一个它可以访问的主体的明细表
56.基于角色的访问控制模型的要素包括用户、角色和许可的基本定义
57.加密算法一般要能抵抗选择明文攻击才认为是安全的
58.操作系统的功能模块，一般以进程的方式在后台运行，以启动服务的方式对用户提供访问接口
59.在 UNIX/Linux 中，服务就是运行在网络服务器上监听用户请求的过程，服务是通过端口号来区分的
60.在 Windows NT 里，口令字密文保存在 SAM 文件里
61.在 Windows 系统中，查看进程命令并能查看进程同服务的关系的 DOS 命令，是 tasklist
62.完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标数据库系统的安全做深入的探测，发现系统最脆弱的环节，此类数据库安全检测技术叫做渗透测试

63.ping 命令利用 ICMP 协议的数据包检测远端主机和本机之间的网络链路是否连通
64.软件保护技术中，在保持原有代码功能的基础上，通过代码变换等手段降低代码的人工可读性，隐藏代码原始逻辑的技术，称为代码混淆技术
65.软件保护技术中，通过将可执行文件进行解压缩或者解密，从而使可执行文件还原为可执行的正常状态，被称为软件脱壳技术
66.通过伪装欺骗手段诱使用户安装运行，对远端目标主机实现远程控制，但不具有复制、传播能力的恶意代码是木马
67.出现漏洞的可能性是指成功攻击机构内某个漏洞的概率
68.通过将恶意程序加载到虚拟环境中运行，从而让恶意程序自动脱壳还原为原有状态，再进行检测查杀的技术，被称为虚拟机查杀技术
69.信息安全风险管理主要包括风险的识别、风险的评估和风险控制策略
70.ISO 13335 标准首次给出了关于 IT 安全的保密性、完整性、可用性、审计性、认证性、可靠性六个方面含义

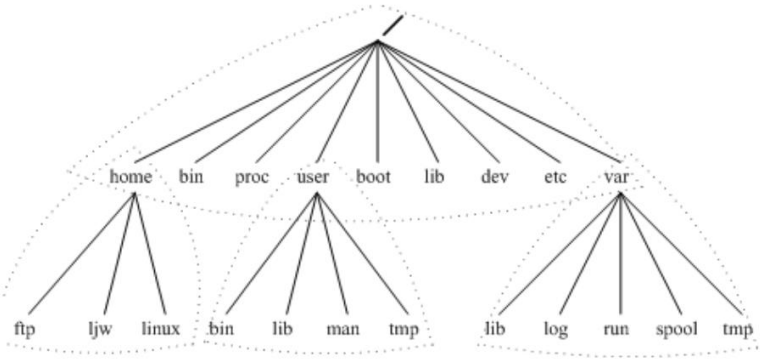
三、综合题

71~76（6′，每空一分）

按要求完成有关数字签名的题目：
（1）一个数字签名体制都要包括两个过程：签名和验证签名
（2）为了实现数字签名，应成立相应的管理机构，并制定规章制度，统一负责签名及验证等技术问题、用户的登记注册、纠纷的仲裁等一些列问题。
①用户 A 和用户 B 利用公开密钥密码进行数字签名时，首先要将各自的公开密钥公开登记并存入管理中心共享的公开密钥数据库，以此作为对方及仲裁者验证签名的数据之一
②签名的时候，用户 A 将使用自己的私有密钥对明文数据进行签名
③用户 B 收到签名后，将使用用户 A 的公开密钥对签名进行验证
（3）实际应用中为了缩短签名的长度、提高签名的速度，而且为了更安全，常对信息的摘要进行签名

77~80（4′，每空一分）

文件系统安全是 UNIX/Liunx 系统安全的核心，完成题目：



（1）当攻击者篡改文件时，他们经常因修改 i 节点设置而留下一个足印，该足印有时能用来作为搜索攻击者的证据
（2）在上图中，表示特殊设备文件的目录文件是 dev
（3）每个文件和目录有三组权限与之相关：一组为文件的拥有者，另一组为文件所属分组的成员，第三组为其他所有用户（通常用“the world”或“others”指代）。ls-l 命令可以查看 UNIX 文件权限，如果：
ls-l
drwxr-x---　1jrandom hackers　96 Mar　2 09:47 backups

则表示：backups 是一个目录，分组成员有可读、不可写和可执行权限

81~90（10′，每空一分）

下图是TCP半连接扫描的原理图。图1为目标主机端口处于监听状态时，TCP半连接扫描的原理图；图2为目标主机端口未打开时，TCP半连接扫描的原理图。请根据TCP半连接扫描的原理，补全扫描过程中各数据包的标志位和状态值信息

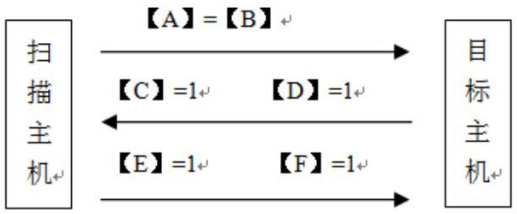


图 1　目标主机端口处于监听状态的 TCP 半连接扫描原理图

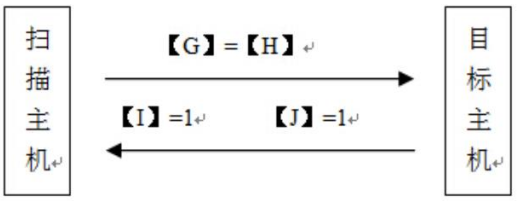


图2 目标主机端口未打开TCP半连接扫描原理图

请在下表中输入【A】-【J】代表的内容

【A】SYN
【B】1
【C】SYN
【D】ACK
【E】RST
【F】ACK
【G】SYN
【H】1
【I】RST
【J】ACK

第十二套

一、选择题

1.信息系统的复杂性是信息安全问题产生的：内因
2.《信息保障技术框架（IATF）》的核心要素，（不包括）：设备
3.1977 年，美国制定的数据加密标准（DES），为加密算法的标准化奠定了基础
4.信息安全的 5 个基本属性，是指：完整性、机密性、可用性、可控性、不可否认性
5.最难防范的密码学攻击方式是：选择密文攻击
6.有关密码分组链模式，（错误的）是：在一些非加密场景下是不能应用的，比如报文鉴别与认证
7.由用户选出或由系统分配给用户的可在较长时间内用户所专用的秘密密钥时：用户密钥
8.属于哈希函数特点的是：单向性
9.MD5 算法的消息摘要长度为：128
10.能够抵抗伪装、内容修改等攻击的技术是：消息认证
11.（不属于）强制访问控制模型的是：访问矩阵模型
12.属于非集中访问控制方法的是：访问矩阵模型
13.网络内容监控的主要方法是：网络舆情分析
14.（无法）将 CPU 模式从用户模式转到内核模式的是：系统调用
15.有关 UNIX/Linux 系统安全，（错误的）是：fmask 命令设置了用户创建文件的默认权限
16.在 Windows 系统中，可以通过修改日志文件访问权限以防止日志信息被清空，但采用的文件系统格式必须是：NTFS
17.在 Windows 系统中，可以查看目录中的子目录和文件名，也可以进入其子目录的目录权限是：List
18.TPM 是指：可信平台模块
19.有关数据库安全，（错误的）是：一个大学管理员在工作中只需要能够更改学生的联系信息，不过他可能会利用过高的数据库更新权限来更改分数，这种威胁是合法的特权滥用
20.属于数据库动态安全防护的是：数据库入侵检测防护
21.TCP 全连接扫描是：TCP 三次握手扫描
22.网络 23 端口对应的协议为：TELNET
23.不能防范网络嗅探的协议是：AH
24.硬件防火墙的平台架构（不包括）：IAAS 架构
25.文件完整性检验技术主要用于：HIDS
26.对于已知攻击类型的检测非常有效，而对攻击的变种和新的攻击几乎无能为力的 IDS 检测技术为：误用检测
27.IPSec 协议提供的安全功能（不包括）：故障诊断
28.SET 协议安全性高于 SSL 协议是由于：SET 协议将整个信息流动过程都进行了安全保护
29.能提供电子邮件数字签名和数据加密功能的协议是：S/MIME
30.漏洞定义的三个要素（不包括）：漏洞是系统中难以克服的缺陷或不足
31.微软的软件安全开发生命周期模型中的最后一个阶段是：安全响应执行
32.在软件设计初期，就需要按照安全设计的原则对软件进行全面考虑，（不属于）安全设计原则的是：最多公用原则
33.将可执行文件进行解压缩或者解密，从而使可执行文件还原为可执行的正常状态的技术是：软件脱壳
34.（不属于）代码混淆技术的是：软件水印

35.Web 安全防护技术（不包括）：虚拟机查杀技术
36.一个用户通过更改 URL 等操作可以成功访问到未被授权的内容，是：不安全的直接对象引用
37.应急计划过程开发的第一阶段是：业务影响分析
38.（不属于）访问控制实现方法的是：虚拟性访问控制
39.信息安全中的风险控制目标是：将残留风险保护在机构可以随时控制的范围内
40.ISMS 所体现的思想是：预防控制为主
41.关于信息安全管理，（错误的）是：安全认证是信息管理工作的目的
42.在信息安全管理中，（不属于）访问控制的是：预留性访问控制
43.关于风险管理，（错误的）是：风险识别是为了说明风险评估的结果
44.电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后：5 年
45.国家秘密的保密期限不能确定时，应当根据事项的性质和特点，确定其：解密条件
46.电子认证服务提供者拟暂停或者终止电子认证服务时，应当提前多长时间就业务承接及其他相关事项通知有关各方：90 日
47.被称为“中国首部真正意义上的信息化法律”的是：电子签名法
48.违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处以几年以下有期徒刑或者拘役：5 年
49.CC 将评估过程划分为功能和保证两个部分，评估等级分为：7 个等级
50.《信息系统安全等级保护基本要求》中的基本管理要求所涉及的层面，（不包括）：业务范围管理
二、填空题
51.20 世纪 60 年代末，美国出现了第一个计算机网络 ARPAnet
52.《信息保障技术框架》（IATF）提出的信息保障的核心思想是纵深防御战略
53.传统对称密码加密时所使用的两个技巧是：代换和置换
54.无论是对称密码还是非对称密码，其安全性实际取决于对密钥的安全保护
55.消息加密本身提供了一种认证手段，其中整个消息的密文作为认证码
56.审计就是对日志记录的分析，并以清晰的、能理解的方式表述系统信息
57.由于网络信息量十分巨大，仅依靠人工的方法难以应对网络海量信息的收集和处理，需要加强相关信息技术的研究，即网络舆情分析技术
58.在 UNIX/Linux 中，主要的审计功能是由 syslogd 守护进程完成的
59.如果所有外键参考现有的主键，则说明一个数据库具有参照完整性
60.拥有 CONNECT 权限的用户不能创建新用户，不能创建模式，也不能创建基本表，只能登陆数据库
61.为不同的数据库用户定义不同的视图，可以限制各个用户的访问范围
62.处于所有根 CA 的中心，与所有 CA 系统之间建立对等的信任关系，并实现信任传递的 CA 被称为桥 CA
63.防火墙所具备的网络地址翻译技术的英文缩写为 NAT
64.缓冲区溢出漏洞是由于向程序的缓冲区中输入的数据超过其规定长度，破坏程序正常的堆栈，使程序执行其他指令
65.栈指针寄存器 esp 用于存放栈顶指针
66.糊测试属于软件动态安全测试技术
67.数据流分析技术是通过分析软件代码中变量的取值变化和语句的执行情况，来分析数据处理逻辑和程序的控制流关系，从而分析软件代码的潜在安全缺陷

68.软件产品的攻击面包括一个软件可能遭受外来攻击的所有攻击点，包括代码、网络接口、服务和协议

69.技术和管理层面的良好配合，是组织机构实现网络与信息安全系统的有效途径

70.国家秘密的保密期限，除另有规定外，机密级不超过 20 年

三、综合题

71~76（6′，每空一分）

假设用户 Alice 和 Bob 分别拥有自己的公钥和私钥，按要求完成有关数字签名的题目：

（1）为了预防 Alice 抵赖，Bob 要求 Alice 对其发送的消息进行签名。Alice 将使用自己的私钥对消息签名；如果要求对消息保密传输，Alice 将使用 Bob 的公钥对消息加密

（2）在产生 Alice 和 Bob 的密钥时，如果采用 RSA 算法，选取的模数至少要有 1024 位，如果采用椭圆曲线密码，选取的参数 p 的规模应大于 160 位

（3）基于签名机制也可以实现身份认证，Alice 为了认证 Bob 的身份：

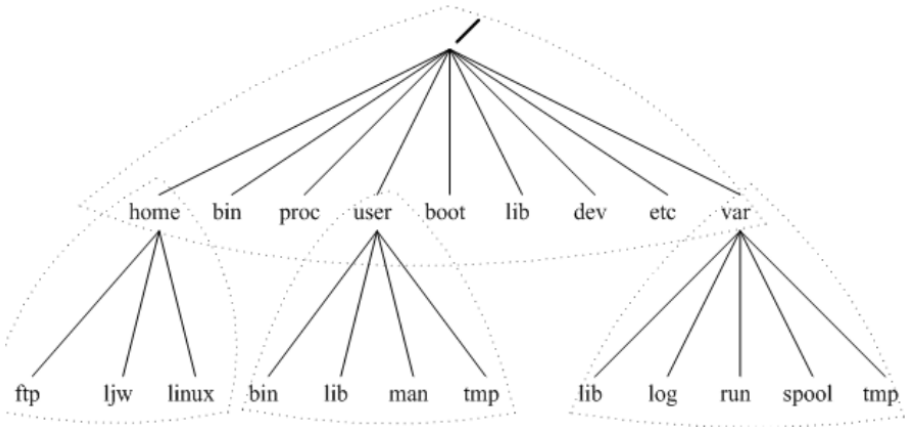
首先，Alice 发送个 Bob 一个随机数 a，即 Alice→Bob：a；

然后，Bob 产生一个随机数 b，并将 b 以及使用私钥对随机数签名的信息发送给 Alice，用 SignB 表示用 Bob 的私钥产生数字签名，即 Bob→Alice：b||SignB（a||b）

最后，为了认证 Bob 的身份，Alice 得到随机数 b 和签名信息之后，只需要使用 Bob 的公钥对签名信息进行解密，验证解密的结果是否等于 a||b 即可

77~80（4′，每空一分）

文件系统安全是 UNIX/Liunx 系统安全的核心，按要求填空：



（1）当攻击者篡改文件时，他们经常因修改 i 节点设置而留下一个足印，该足印有时能用来作为搜索攻击者的证据

（2）在图中，表示特殊设备文件的目录文件是 dev

（3）每个文件和目录有三组权限与之相关：一组为文件的拥有者，一组为文件所属分组的成员，一组为其它所有用户（常用“the world”或“others”指代）。ls-l 命令可以查看 UNIX 文件权限，如果：

$ls-l

-rw------- 1 jrandom hackers 2967 Aug 30 1994 private

则表示：private 是一个文件，拥有者有可读、可写和不可执行权限

81~88（10′，前两空每空两分，后面每空一分）

IPSec 协议是现在 VPN 中使用最广泛的一种协议，它是一组开放协议的总称，包括网络安全协议和密钥协商协议两部分

1.网络安全协议包括 AH 和 ESP 协议两种，在 Windows7 操作系统中，IPSec 协议在配置时可选择的算法包括：A.DES　B.MD5　C.3DES　D.SHA-1

选择：

（1）在配置 AH 协议时，可配置的全部算法为：BD

（2）在配置 ESP 协议时，可配置的全部算法为：ABCD

2.密钥协商协议中的 IKE 协议属于混合型协议，由三个协议组成，请回答：

（1）IKE 创建在 G 协议定义的框架上，沿用了 I 协议的密钥交换模式和 F 协议的共享密钥和密钥组成技术

（2）IKE 使用两阶段协商安全参数。第一阶段交换 H，主要通过两种模式实现。第二阶段利用第一阶段建立的安全关联来创建其它协议的安全关联，用于 IPSec 协议时，创建 E

（3）如果通过 Wireshark 捕获 IPSec 的前面 10 个数据包，这 10 个数据包显示的协议名是 G 协议

E.IPSec SA　　F.SKEME　　G.ISAKMP　　H.IKE SA　　I.Oakley

第十三套

一、选择题

1.信息技术的产生与发展经历了三个阶段，（不包括）：大规模集成电路的应用
2.20 世纪 60 年代末，美国出现了第一个计算机网络 ARPAnet，其目的是用于：军事
3.关于信息与消息的说法，（错误的）是：消息是信息的精确概念
4.信息安全的基本属性，（不包括）：公开性
5.属于序列密码算法的是：RC4
6.使用 Caesar 密码，k 取值为 3，则对明文“meet me after the toga party”加密得到的密文是：phhw ph diwhu wkh wrjd sduwb
对字母表中的每个字母，用其之后的第k个字母来替换。
7.ElGamal 密码所依赖的数学难题是：离散对数
8.属于哈希函数特点的是：单向性
9.SHA 所产生的消息摘要的长度，比 MD5 的长：32 位
10.第一个实用的在非保护信道中创建共享密钥的方法是：Diffie-Hellman 算法
11.验证所收到的消息确实来自真正的发送方，并且未被篡改的过程是：消息认证
12.（不属于）强制访问控制模型的是：访问矩阵模型
13.在活动网络中被动监听网络流量，利用检测算法识别网络入侵行为的恶意行为监控方式是：网络监测
14.有关守护进程，（错误的）是：守护进程不能完成系统任务
15.有关 UNIX/Linux 系统安全，（错误的）是：users 命令用来管理和维护系统的用户信息
16.表示硬件抽象层的 Windows 操作系统核心组件是：Hal.dll
17.可以显示本地计算机硬件、系统组件和软件环境的完整视图的，由 Windows 提供的查看系统信息的工具是：Msinfo32
18.TCB 是指：可信计算基
19.有关数据库安全，（错误的）是：SQL 注入攻击利用的是 SQL 语法，可以不受限制地访问整个数据库，但无法达到控制服务器的目的
20.对数据库的开放端口进行扫描，检查其中的安全缺陷的安全检测技术是：服务发现
21.属于网络层协议的是：RIP
22.IP 地址的前两个比特位为 10，网络号长度有 14 位，这类 IP 地址属于：B 类
23.TCP 头部格式中，表示出现差错，必须释放 TCP 连接重新建立新连接的标志位是：RST
24.TCP 半连接扫描是：TCP SYN 扫描
25.有关盲攻击，（错误的）是：使用网络嗅探工具可捕获目标主机的 TCP 数据包
26.（不属于）诱骗式攻击的是：拒绝服务攻击
27.采用 rootkit 技术的木马属于：第五代
28.webshell 在被控服务器上传递远程控制数据的网络端口是：80
29.ESP 协议为基于 IPSec 的数据通信提供的安全保护机制，（不包括）：加密存储
30.国家信息安全漏洞共享平台的英文缩写为：CNVD
31.整数溢出的三种溢出原理，（不包括）：代码溢出
32.exploit 的含义是：漏洞利用
33.有关 Heap Spray 技术，（错误的）是：Heap Spray 攻击会导致被攻击进程的内存占用非常小
34.软件开发生命周期模型，（不包括）：白盒模型
35.在软件开发设计阶段应考虑的安全原则，（不包括）：充分考虑安全的条件

36.安全测试往往需要从攻击者的角度开展测试，安全测试技术（不包括）：分析源代码中函数的逻辑关系
37.定义 ISMS 的范围，就是在组织机构内选定架构 ISMS 的范围
38.有关 ISMS 文件控制的描述，（错误的）是：文件发布前无须履行审批手续
39.信息安全风险评估所采取的方法，（不包括）：概要风险评估
40.有关信息安全管理体系（ISMS）构架的具体措施，（不包括）：安全宣传手册发放
41.信息安全管理体系评审程序，（不包括）：复核评审报告
42.制定业务可持续性计划时，有多种策略可选。一般情况下不选择：主站点
43.访问控制依赖的原则，包括身份标识、责任衡量、授权和验证
44.信息安全技术评估准则将评估过程分为两个部分：功能和保证
45.信息安全等级保护的基本管理要求从安全管理制度、人员安全管理、系统建设管理和系统运维管理几个方面提出
46.电子签名认证证书应当载明的内容，（不包括）：证书持有人的公民身份证件信息
47.等级保护的重要标准，（不包括）：信息系统安全等级保护战略方针
48.有关电子签名的内容，正确的：签署后对数据电文内容和形式的任何改动都能够被发现
49.有关商用密码产品的描述，正确的：商用密码产品可由国家密码管理机构许可的单位销售
50.商用密码技术属于国家秘密。国家对商用密码产生的科研、生产、销售和使用实行专控管理

二、填空题

51.信息安全技术的核心是：密码
52.信息安全的内因是信息系统的复杂性
53.传统对称密码加密时所使用的两个技巧是：代换和置换
54.DES 算法的分组大小为 64 位
55.随着 PKI 技术日趋成熟，许多应用中开始使用数字证书进行身份认证与数字加密
56.基于角色的访问控制模型的要素包括用户、角色许可等基本定义
57.集中式的 AAA 管理协议包括拨号用户远程认证服务 RADIUS、终端访问控制器访问控制系统 TACACS 和 Diameter 等
58.用户应用程序代码在用户模式下运行，操作系统代码在内核模式下运行
59.为了防止网络黑客在网络上猜出用户的密码，可以在连续多次无效登陆之后对用户账号实行锁定策略
60.拥有 CONNECT 权限的用户不能创建新用户，不能创建模式，也不能创建基本表，只能登录数据库
61.在数据库中，GRANT 和 REVOKE 语句分别用于向用户授权和收回对数据的操作权限
62.跨站脚本攻击的英文缩写为：XSS
63.ESP 协议处理并传输数据的性能小于 AH 协议
64.限制内存堆栈区的代码为不可执行的状态，从而防范溢出后的代码的执行，这种技术是数据执行保护技术，它的英文缩写为：DEP
65.漏洞利用的核心是利用程序漏洞去执行 shellcode 以便劫持进程的控制权
66.微软的软件安全开发生命周期模型中，最初的准备阶段属于第 0 阶段
67.通过分析代码中输入数据对程序执行路径的影响，以发现不可信的输入数据导致的程序执行异常，被称为污点传播分析技术
68.结合了程序理解和模糊测试的技术，称为智能模糊测试技术
69.风险管理的第一阶段为风险识别

70.《电子签名法》被称为“中国首部真正意义上的信息化法律”，极大地推进了我国电子商务发展，是扫除我国电子商务发展障碍的重要步骤

三、综合题

71~75（6′，最后一空 2 分，其余一空一分）

假设用户 Alice 和 Bob 分别拥有自己的公钥和私钥，完成题目：

（1）为了预防 Alice 抵赖，Bob 要求 Alice 对其发送的消息进行签名。Alice 将使用自己的私钥对消息签名；如果要求对消息保密传输，Alice 将使用 Bob 的公钥对消息加密

（2）基于签名机制也可以实现身份认证，Alice 为了认证 Bob 的身份：

首先，Alcie 发送给 Bob 一个随机数 x，即 Alice→Bob：x；

然后，Bob 产生一个随机数 b，并将 b 以及使用私钥对随机数签名的信息发送给 Alice，用 SignB 表示用 Bob 的私钥产生数字签名，即：Bob→Alice：b||SignB（x||b）

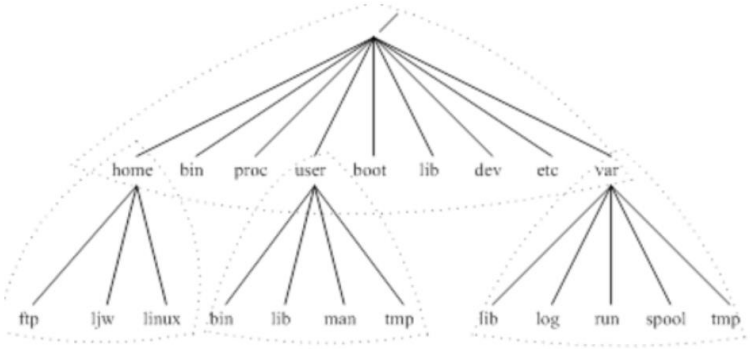
最后，为了认证 Bob 的身份，Alice 得到随机数 b 和签名信息之后，只需要使用 Bob 的公钥对签名信息进行解密，验证解密的结果是否等于 x||b 即可

（3）假设 Alice 的 RSA 公钥为（e=3，n=15），已知素数 p=3，q=5。Alice 要发送消息 m=3 给 Bob，并对该消息进行签名后得到的签名是 12

(3) RSA算法中，首先根据两个素数p和q，计算出n，题意p和q是3和5，所以n=p*q=15 Φ(n)=(p-1)*(q-1)=2*4=8, 根据e*d=1modΦ(n)，即3*d=1mod8，可求得Alice的私钥为d=3，使用私钥对消息m进行签名，33mod15 = 12，即使用Alice的私钥对消息m签名的结果为12。

76~79（4′，每空一分）

文件系统安全是 UNIX/Linux 系统安全的核心，填空：



（1）在图中，表示用户命令的可执行文件的目录文件是 bin

（2）每个文件和目录有三组权限与之相关：一组为文件的拥有者，一组为文件所属分组的成员，一组为其它所有用户。ls-l 命令可以查看 UNIX 文件权限，如果：

$ls-l

-rwx------ 1jrandom hackers 2967 Aug 30 1994 private

则表示：private 是一个文件，其它用户有不可读、不可写和不可执行权限

（3）对于一个文件，用户可以使用 chmod 命令来改变文件的权限设置

80~89（10′，每空一分）

填空：

（1）公共密钥基础设施（英文缩写 PKI）是一个用公钥密码学技术来实施和提供安全服务的安全基础设施，它是创建、管理、存储、分布和作废数字证书的一系列软件、硬件、人员、策略和过程的集合

（2）证书签发机构是公共密钥基础设施的核心机构，提供数字证书生成、证书发放、证书的管理等服务。证书注册机构是接受客户证书申请并进行审核注册的机构

（3）数字证书的存储格式标准有多种，X.509 是最基本的证书存储格式。采用此格式的证

书结构如下所示：
证书的版本号
证书序列号
签名算法
证书签发机构名
证书有效期
证书持有者用户名
证书用户公钥信息
签发者唯一标识符
证书持有者唯一标识符
签名值
其中，签名值是证书签发机构对证书上述内容的数字签名值
（4）数字证书在使用过程中，为了验证此数字证书的真实性，其它用户、应用程序或实体需下载安装 CA 根证书，使用此证书中的公钥对证书中的数字签名进行验证

第十四套

一、选择题

1.关于信息的四种定义，我国学者钟义信先生提出的是：信息是事物运动的状态和状态变化的方式
2.关于信息安全技术的分类中，密码技术属于：核心基础安全技术
3.香农在 1949 年发表的论文《保密系统的通信理论》，用信息论的观点对保密问题进行了全面论述，它是信息安全发展的重要里程碑
4.美国第一个用于军事目的的计算机网络 ARPAnet 出现在：20 世纪 60 年代末
5.（不属于）对称密码的是：MD5
6.CBC 是指：密码分组链模式
7.（不属于）有效的 RSA 密钥长度的是：128 位
8.属于对称密钥体制优点的是：加密/解密速度快，不需占用较多的资源
9.（不属于）身份认证手段的是：基于消息认证码的认证
10.关于访问控制中主体和客体概念的说法，正确的：主体是一个主动的实体，它提供对客体中的对象或数据的访问要求
11.应用在多边安全系统中的安全模型是：Chinese Wall 模型
12.实施强制访问控制的依据是：安全标签
13.Kerberos 协议设计的核心是：在用户的验证过程中引入一个可信的第三方，即 Kerberos 验证服务器
14.能对操作系统的服务进行请求的是：系统调用
15.在 UNIX/Linux 系统中，配置文件通常存放在：/etc
16.能打开 Windows 操作系统注册表命令是：Regedit
17.可以用来查看进程，并能查看进程发起程序的 DOS 命令是：netstat
18.在保护环结构中，处于 0 环的是：操作系统内核
19.数据库内部大量内置函数和过程的安全漏洞的重要特征是：每个安全漏洞只存在于相应的某个具体版本
20.关于 SQL 注入的说法，（错误的）是：入侵者通过 SQL 注入可以获得敏感信息，但是无法控制服务器
21.被称为秘密扫描的端口扫描技术是：TCP FIN 扫描
22.（不能）进行端口扫描的软件是：Wireshark
23.为了捕获网络接口收到的所有数据帧，网络嗅探工具会将网络接口设置为：混杂模式
24.（不属于）诱骗攻击的是：注入攻击
25.关于拒绝服务攻击，（不属于）在传输层发起的是：Script Flood
26.（不属于）木马特点的是：感染性
27.关于 IPS 系统描述，（错误的）是：控制台以串联方式部署在网络中以实现网络数据的拦截
28.由两个包过滤路由器和一个堡垒主机构成的防火墙体系结构是：屏蔽子网体系结构
29.收到攻击行为和非正常操作的行为特征，以建立特征库进行检测的 IDS 系统，属于：误用检测型 IDS
30.属于 UAF（Use-After-Free）漏洞的是：内存地址对象破坏性调用漏洞
31.（不属于）漏洞定义三要素的是：漏洞的存在会对软件造成较大危害
32.微软公司安全公告中，危险等级最高的漏洞等级是：严重
33.将系统关键地址随机化，从而使攻击者无法获得需要跳转的精确地址的技术是：ASLR

34.微软的 SDL 模型中，最后的（第 12）阶段是：安全响应运行
35.（不属于）软件静态安全检测技术的是：模糊测试
36.（不属于）Web 服务器端安全防护技术的是：定期更新 Web 服务器上浏览器的安全插件
37.技术层面和管理层面的良好配合，是组织机构实现网络与信息安全系统的有效途径。其中，管理层面实现的途径是：架构信息安全管理体系
38.在制定信息安全政策时，（错误的）是：要制定一个包含组织机构内所有层面的安全方针的政策
39.风险管理的第一阶段是：风险识别
40.关于风险控制策略的解释中，（错误的）是：缓解：消除漏洞产生的影响
41.关于残留风险的描述，（错误的）是：信息安全的目标是把残留风险降低为零
42.建立完善的信息安全管理体系（ISMS）要求体现：预防控制为主的思想
43.信息资产最重要的三个属性是：机密性、完整性和有效性
44.《信息安全等级保护管理办法》的五个安全保护等级中，描述为“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”的是：三级
45.描述正确的是：信息系统安全保护等级级别取决于信息系统被破坏后产生的损害
46.属于信息系统的安全考核指标的是：数据完整性
47.“泄露会使国家安全和利益遭受特别严重的损害”的保密级别是：绝密级国家秘密
48.ISO 13335 标准给出的 IT 安全六个方面的定义中，包含：审计性、认证性、可靠性
49.国家秘密的保密期限，除另有规定外，一般秘密级不超过 10 年
50.电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后 5 年

二、填空题

51.1937 年，香农在美国麻省理工学院发表了《继电器和开关电路的符号分析》硕士论文，奠定了计算机二进制的基础
52.信息安全保障工作的内容包括：确定安安需求、设计和实施安全方案、进行信息安全评测和实施信息安全监控与维护
53.审计就是对日志记录的分析，并以清晰的、能理解的方式表述系统信息
54.SHA-1 的输出是 160 位
55.消息加密本身提供了一种认证手段。在这种方法中，整个消息的密文作为认证码
56.基于矩阵的行的访问控制信息表示的是访问能力表，即每个主体都附加一个该主体可访问的客体的明细表
57.基于角色的访问控制模型的要素包括用户、角色和许可的基本定义
58.进程管理是通过中断完成的
59.UNIX 文件系统安全基于 i 节点中的三段关键信息：文件拥有者、文件所在分组和模式
60.Windows 系统提供的查看系统信息的工具是 msinfo32，它可以显示本地计算机硬件、系统组件和软件环境的完整视图
61.TCG 定义可信计算平台的信任根包括三个根：可信测量根、可信存储根和可信报告根
62.存储型 XSS 又被称为持久型跨站脚本攻击
63.数字证书真实性的验证是通过验证证书中 CA 的数字签名来实现的
64.处于未公开状态的漏洞被称为 0day 漏洞
65.当一个函数被调用时，这个被调用函数的相关信息会保存在内存的栈区，这块内存中连续的栈区域又称为栈帧
66.通过向目标软件输入大量的畸形数据并监测目标系统的异常来发现潜在的软件漏洞，这

种测试技术被称为模糊测试
67.Web 安全检测技术包括黑盒检测和白盒检测两种主要检测技术
68.基于硬件介质的软件安全保护技术包括加密狗、加密光盘和专用接口卡等
69.信息安全管理方面的内容主要包括信息安全管理体系、信息安全风险管理和信息安全管理措施三个部分
70.机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级，同时确定保密期限和知悉范围

三、综合题

71~76（6′，每空一分）

计划构建一个基于密码机制的网络数据的安全传输系统，假设数据收发两端的用户分别为 Alice 和 Bob

为了准确地描述算法，定义如下：给定数 x、y 和 z，x*y 表示乘法运算，x/y 表示除法运算，x^y 表示指数运算，而 x^{y/z}表示指数为 y/z；约定在英文半角状态下完成表达式输入

（1）为了确保数据传输的速度，应该采用对称密码对数据进行加解密

（2）该系统可以采用密钥协商交换协议来协商一个数据传输密钥，第一个实用的在非保护信道中创建共享密钥的方法是 Diffie-Hellman 算法。在该算法中，有两个全局公开的参数，分别为一个素数 p 和一个整数 g，g 是 p 的一个原根。为了协商数据传输密钥：首先，Alice 随机选取 a，计算出 A=g^a mod p，Bob 随机选取 b，计算出 B=g^b mod p；然后，Alice 和 Bob 交换 A 和 B。此时，Alice 和 Bob 就分别计算出共享的密钥为：K=g^{a*b} mod p

（3）为了协商并保护数据传输密钥，另外一种简单有效的做法是采用公钥密钥体制：首先，Alice 在发送数据前，随机生成一个对称密钥，然后使用 Bob 的公钥对该密钥进行加密，并发送给 Bob；然后，Bob 收到密文后，使用自己的私钥进行解密即可得到 Alice 生成的对称密钥

77~80（4′，每空一分）

关于数据库的安全性控制，常用的方法包括用户标识和鉴定、存取控制、审计、数据加密等，填空：

（1）数据库系统提供了两种存取控制机制：自主存取控制和强制存取控制

（2）自主存取控制中，GRANT 语句用于向用户授予权限，REVOKE 语句用于向用户收回授予的权限

（3）审计功能把用户对数据库的所有操作自动记录下来放入审计日志中。对修改 Table1 表结构或修改 Table1 表数据的操作进行审计的 SQL 命令是：AUDIT ALTER,UPDATE ON Table1

81~90（1′，每空一分）

某单位将部署网络安全产品对单位的网络进行防护，要求针对Web服务器部署的安全设备应具备应用层的防护能力，且采购的IDS和IPS为同一厂商的设备，控制台可以同时管理IDS和IPS。请完成下列相关的题目。

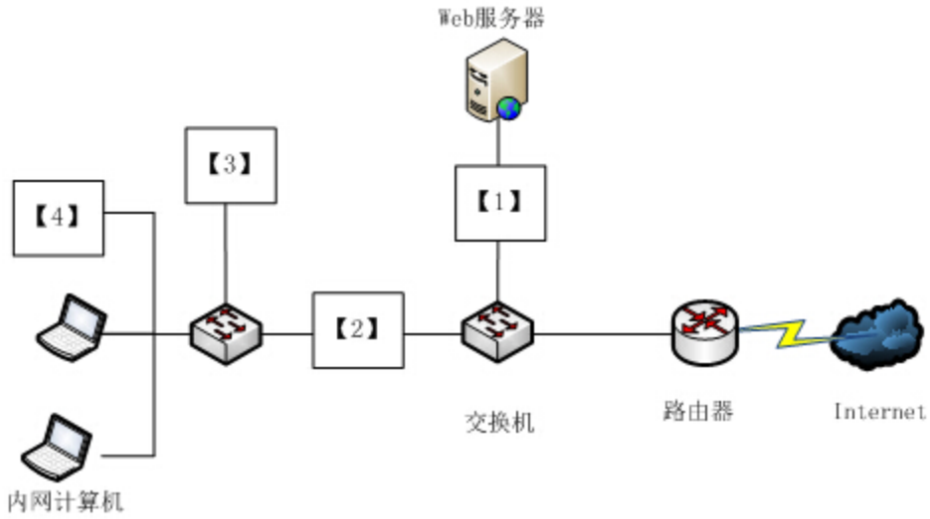


图 网络拓扑图

（1）填空【1】~【4】

IPS 网络设备　　防火墙　　IDS 探测器　　控制台

（2）对于 IPS 的配置，控制台与 IPS 网络设备的连接方式应该配置为主动控制台方式，由控制台去连接 IPS 网络设备获取信息

（3）为了提高内网的安全性，需要为防火墙进行默认访问控制规则的配置。填空：

表 防火墙访问控制规则表

序号	源区域	目的区域	访问权限
1	内网	外网	允许
2	外网	内网	禁止
3	任意	任意	禁止

第十五套

一、选择题

1.信息安全发展所经历的阶段，（不包括）：网络安全阶段
2.香农的论文《保密系统的通信理论》用信息论的观点对保密问题进行了论述，是信息安全发展的里程碑，这篇论文发表在：1949 年
3.信息系统安全保障的几个方面，（不包括）：安全技术
4.P2DR 安全模型的核心是：策略
5.（不属于）对称密码算法的是：ECC
6.使用 Caesar 密码，k 取值为 4，对明文“password is root”加密得到的密文是：tewwasvh mw vssx
7.RSA 所依赖的数学难题是：大整数因式分解
8.有关哈希函数的描述，（错误的）是：SHA 算法要比 MD5 算法更快
9.由 SHA 算法生成的消息摘要的长度为：160
10.能够抵抗发送方否认的技术是：数字签名
11.基于 PKI 体系的认证模式所采用的身份认证手段是：USB Key 认证
12.有关非集中式访问控制，（错误的）是：Kerberos 协议需要结合单点登录技术以减少用户在不同服务器中的认证过程
13.在用户主机上安装反病毒软件和基于主机的入侵检测软件，对入侵主机的已知恶意代码进行检测和告警的恶意行为的监控方式是：主机监测
14.操作系统的引导程序，（不包括）：Reboot
15.有关 UNIX/Linux 系统安全，（错误的）是：last 命令用于显示上一个执行过的命令
16.在 Windows 系统中，可用于管理启动和停止服务的系统进程是：services.exe
17.在 Windows 系统中，安全账号管理器的英文缩写是：SAM
18.TCM 是指：可信密码模块
19.有关数据库安全，（错误的）是：备份数据库是否加密，对数据库安全影响不大
20.在数据库内部，存在大量的内置函数和过程，这些函数和过程有的存在严重的安全漏洞。这些安全漏洞一个重要的特征是：每个安全漏洞只存在于相应的某个具体版本
21.属于网络层协议的是：OSPF
22.范围为 128.0.0.0~191.255.255.255 的 IP 地址，属于 B 类
23.ping 命令可以检测目标计算机和本机之间的网络链路是否连通，利用的协议是：ICMP
24.（不能）防范网络嗅探工具对数据包进行嗅探的是：FTP
25.将攻击数据包的源地址和目的地址都设置成目标主机的 IP 地址，这种攻击是：Land 攻击
26.Script Flood 攻击属于：应用层协议攻击
27.注入攻击的防范措施，（不包括）：按照最大权限原则设置数据库的连接权限
28.对非法 webshell 控制网站服务器的防范措施，（不包括）：全面检测系统的注册表、网络连接、运行的过程
29.有关 SSL 协议，（错误的）是：SSL 协议在 HTTP 协议之上
30.栈指针寄存器 esp 中存放的指针指向：栈顶地址
31.下列描述正确的：程序员负责堆中变量的分配与释放，而栈中变量空间的分配与释放由程序负责
32.软件开发设计阶段应考虑的安全原则，（不包括）：封闭设计原则
33.安全编程时需要考虑的原则，（不包括）：数据的开放性

34.静态安全检测技术，（不包括）：模糊测试
35.代码混淆技术，（不包括）：功能转换
36.根据软件加壳的目的和作用，软件加壳技术分为：压缩保护壳和加密保护壳
37.系统维护的注意事项，（不包括）：删除错误报告及日志文件
38.用户账户管理，（不包括）：共享用户账户
39.试图防止漏洞被利用的风险控制策略，是：避免
40.访问控制所保护的客体属性，（不包括）：纠正性
41.访问控制管理的重要组成部分，（不包括）：日志备份
42.危机管理的关键部分，（不包括）：灾难恢复
43.安全组织的职能包括：全对
44.信息安全等级保护的基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出
45.（没有）涉嫌违法的是：在和朋友的私人交往和通信中涉及彼此隐私的
46.计算机使用应遵守的道德规范，（不包括）：不经常使用非正版软件
47.从事电子认证服务，应当向国务院信息产业主管部门提出申请，并提交符合法律的相关材料。主管部门应当自接到申请起 45 日内作出许可或者不予许可的决定
48.有关电子认证服务，（错误的）是：电子认证服务提供者可以暂停或者终止电子认证服务，但须在暂停或者终止服务后及时向国务院信息产业主管部门报告
49.CC（《信息技术安全性评估准则》）将评估过程划分为两个部分，评估等级分为七个等级
50.有关信息安全风险评估工作，都应遵循国家颁布的文件要求，该类文件包括：全部

二、填空题

51.信息保障技术框架（IATF）的核心要素为人员、技术和操作
52.信息安全的基本属性主要包括 5 个方面：完整性、机密性、可用性、可控制性和不可否认性
53.DES 密码结构基于一个被称为 Feistel 网络的结构
54.CBC 是指密码分组链模式
55.基于动态口令认证的方式主要有动态短信密码和动态口令牌两种方式，口令一次一密，大大提高了安全性
56.自主访问控制模型的实现机制是通过访问控制矩阵实施，而具体的实现办法则是通过访问能力表或访问控制表来限定哪些主体针对哪些客体可以执行什么操作
57.由于网络信息量十分巨大，仅依靠人工的方法难以应对网络海量信息的收集和处理，需要加强相关信息技术的研究，即网络舆情分析技术，以达到围绕中介性社会事件的发生、发展和变化，分析民众对社会管理者产生和持有的社会政治态度等目的
58.用户应用程序代码在用户模式下运行，操作系统代码在内核模式下运行
59.修改了日志文件的存放目录后，日志还是可以被清空的，而通过修改日志文件访问权限可以防止这种事情发生，前提是 Windows 系统要采用 NTFS 文件系统格式
60.数据库系统提供了两种存取控制机制：自主存取控制和强制存取控制
61.在数据库中，GRANT 和 REVOKE 语句分别用于向用户授权和收回对数据的操作权限
62.分布式拒绝服务攻击的英文缩写为：DDOS
63.CA 对用户进行身份验证后，签发的用于标志用户身份信息的一系列数据，用来在网络通讯中识别通讯各方的真实身份，并具有对用户身份标识的唯一性，这是证书
64.当对整数进行加乘等运算时，计算结果如果大于该类型整数的取值范围时发生的溢出被称为整数溢出

65.通过网络等途径，自动将自身的全部代码或部分代码通过网络复制、传播给其它网络中计算机的完全独立可运行程序，被称为蠕虫

66.处于未公开状态的漏洞被称为 0day 漏洞

67.MITRE 公司建立的通用漏洞列表相当于软件漏洞的一个行业标准，通用漏洞列表的英文缩写为 CVE

68.在不实际执行程序的前提下，将程序的输入表示成符号，把程序的输出表示成包含这些符号的逻辑或算术表达式的技术，被称为符号执行技术

69.信息安全管理体系审核是为了获得审核证据，对体系进行客观的评价

70.可信计算机系统安全评估准则的英文缩写是 TCSEC

三、综合题

71~75（6′，最后一空两分，其余一空一分）

（1）为了实现数字签名，应成立相应的管理机构，并制定规章制度，统一负责签名及验证等技术问题、用户的登记注册、纠纷的仲裁等一系列问题。

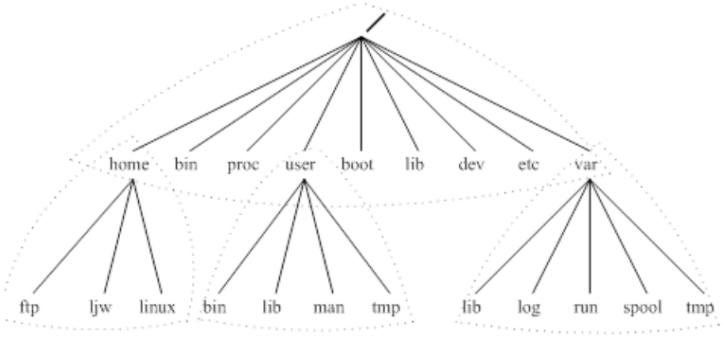
①用户 Alice 和用户 Bob 利用公开密钥密码进行数字签名时，首先要将各自的公开密钥公开登记并存入管理中心的共享的公开密钥数据库，以此作为对方及仲裁者验证签名的数据之一。

②为了预防 Alice 抵赖，Bob 要求 Alice 对其发送的消息进行签名。Alice 将使用自己的私有密钥对消息签名；如果要求对消息保密传输，Alice 将使用 Bob 的公开密钥对消息加密。

（2）假设 Alice 的 RSA 公钥为(e=3, n=15)，已知素数 p=3，q=5。Bob 对于收到的来自 Alice 的签名消息 13，验证签名后得到的原始明文消息是 7

76~79（1′，每空一分）

文件系统安全是 UNIX/Linux 系统安全的核心，请按要求完成下列题目。



（1）在图中，表示用户起始目录的目录文件是 home

（2）每个文件和目录有三组权限与之相关：一组为文件的拥有者，一组为文件所属分组的成员，一组为其它所有用户（通常用“the world”或“others”指代）。ls -l 命令可以查看 UNIX 文件权限，如果：

$ ls -l

-rwx------1jrandom hackers 2967 Aug 30 1994 private

则表示: private 是一个文件，拥有者有可读、可写和可执行权限

（3）对于用户创建文件的默认权限，可以使用 umask 命令来设置

80~89（10′，每空一分）

根据下列对木马技术演变的描述，完成填空。

（1）第 1 代木马的连接是从木马的客户端主动连接木马的服务端。

（2）第 3 代木马的连接是从木马的服务端主动连接木马的客户端。

（3）第 3 代木马由于采用了反弹端口技术，能穿透硬件防火墙，但不能穿透软件防火墙。
（4）第 5 代木马和第 4 代木马都采用了隐藏技术，其中前者比后者在隐藏技术方面有了进一步的提升，它通过使用 rootkit 技术实现木马运行时进程、文件、服务、端口等的隐藏。

第十六套

一、选择题

1.（不属于）信息系统的安全风险隐患来源的是：用户频繁进行网络浏览
2.与等级保护工作（不相关）的是：《电子签名法》
3.信息保障的指导性文件《信息保障技术框架》，是由：美国国家安全局（NSA）制定的
4.数据加密标准 DES 制定的年份是：1977
5.（不属于）非对称密钥体制优点的是：加解密速度快，不需占用较多的资源
6.关于加密算法应用范围的描述，正确的：DSS 用于数字签名，RSA 用于加密和签名
7. Alice 通过密钥 K2 加密消息 M 产生密文 E(K2,M)，然后通过密钥 K1 生成 MAC 为 C(K1，E(K2,MI))，之后 Alice 将密文和 MAC 发送给 Bob; Bob 用密钥 K1 和密文生成一个 MAC 并和 Alice 的 MAC 比较，假如相同再用 K2 解密密文。该过程所提供的安全服务是：保密性和消息完整性
8.Diffie-Hellman 算法是一种：密钥交换协议
9.下列情景属于身份认证过程的是：用户依照系统提示输入用户名和口令
10.Chinese Wall 安全策略的基础是：客户访问的信息不会与目前他们可支配的信息产生冲突
11.下列访问控制模型中，支持安全标签的是：强制访问控制
12.限定一个用户对一个客体目标访问的安全属性集合是：访问控制标签列表
13.Kerberos 协议设计的核心是：在用户的验证过程中引入一个可信的第三方，即 Kerberos 验证服务器
14.关于进程管理的描述，（错误的）是：进程管理是通过系统调用来完成的
15.操作系统内核处于保护环结构中的：0 环
16.在 Linux/UNIX 系统中，用户命令的可执行文件通常存放在：/bin
17.将查询结果中的重复元组去掉的 SQL 子句是：DISTINCT
18.关于视图的描述，（错误的）是：视图机制的安全保护功能比较精细，通常能达到应用系统的要求
19.（不属于）数据库渗透测试的是：发现数据库服务端口
20.（不属于）数据库安全检测的是：入侵检测
21.被称为半连接扫描的端口扫描技术是：TCP SYN 扫描
22.（不能）进行漏洞扫描的是：Nmap
23.（不能）防范网络嗅探工具对数据包嗅探的技术是：VLAN
24.（不属于）操作系统平台中软件漏洞的是：XSS 漏洞
25.UDP Flood 攻击是：耗尽目标主机网络带宽的攻击
26.（不属于）木马隐藏技术的是：反弹端口
27.防护墙能够防范的攻击的是：对内网的漏洞扫描攻击
28.在 TCP 三次握手中，第一次握手的数据包的 SYN 和 ACK 标志位分别为：1,0
29.（没采用）公钥密码体制和数字证书的协议是：Kerberos
30.由国内机构维护的漏洞数据库是：CNVD
31.限制内存堆栈区的代码为不可执行状态的技术是：DEP
32.软件开发生命周期模型（不包括）：循环模型
33.在微软的 SDL 模型中，第 0 阶段是：准备阶段
34.关于软件安全检测技术的描述，（错误的）是：软件动态安全检测技术的直接分析对象是软件源代码和可执行代码

35.（不属于）软件安全保护技术的是：模型检验技术
36.（不属于）恶意程序检测查杀技术的是：移动介质查杀
37.在对一个计算机硬件资产的跟踪识别管理中，（不能）有效地识别该资产的属性是：软件版本号
38.风险控制的首选策略是：避免
39.在一个管理制度完善、工作机制有效的安全组织机构中，（不允许）出现的现象是：信息安全组织应当由隶属于单位的计算机运行或计算机应用部门来负责
40.在 ISMA 架构的具体实施中，关于安全事件记录的描述（错误的）是：安全事件的记录保存不受任何约束
41.关于信息安全管理的英文缩写，（错误的）是：灾难恢复计划—RIP
42.信息安全管理体系审核包括：内部审核和外部审核
43.物理与环境安全中，目前经常采用的视频监视系统是：闭路电视监视系统
44.ISO 13335 标准给出的 IT 安全六个方面的定义，包含：机密性、完整性、可靠性
45.中国信息安全测评中心的英文缩写是：CNITSEC
46.属于信息系统的安全考核指标的是：身份认证
47.《信息安全等级保护管理办法》的五个安全保护等级中，描述为“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”的是：四级
48.“泄露会使国家安全和利益遭受严重的损害”的保密级别是：机密级国家秘密
49.信息安全管理基本技术要求从五个层面提出:物理安全、网络安全、应用安全、主机安全和：数据安全
50.国家秘密的保密期限，除另有规定外，机密级不超过 20 年

二、填空题

51.在信息安全发展的通信保密阶段，人们主要关注信息在通信过程中的安全性问题，即“机密性”
52.信息安全保障工作的内容包括：确定安全需求、设计和实施安全方案、进行信息安全评测和实施信息安全监控与维护
53.在计算机系统中，认证、访问控制和审计共同建立了保护系统安全的基础，其中的最后一项是对认证和访问控制的有效补充。
54.安全散列算法 SHA 所产生的摘要比消息摘要算法 MD5 长 32 位
55.消息加密本身提供了一种认证手段。在这种方法中，整个消息的密文作为认证码
56. 基于矩阵的列的访问控制信息表示的是访问控制表，即每个客体附加一个它可以访问的主体的明细表
57.基于角色的访问控制模型的要素包括用户、角色和许可的基本定义。
58.进程与 CPU 通信是通过中断来完成的
59. UNIX 文件系统安全基于 i 节点中的三段关键信息，即文件拥有者、文件所在分组和模式
60. TCG 定义可信计算平台的信任根包括三个根:可信测量根、可信存储根和可信报告根
61.在数据库中，为不同的用户定义不同的视图，可以限制其访问范围
62. PKI 是创建、管理、存储、分发和作废数字证书的一系列软件、硬件、人员、策略和过程的集合
63.根据 TCP/IP 开放模型的层次划分，SSL 协议为应用层的访问连接提供认证、加密和防篡改功能
64.在缓冲区溢出攻击中，被植入的一段用以获得执行权限的代码被称为 shellcode 代码
65.攻击者通过精心构造超出数组范围的索引值，就能够对任意内存地址进行读写操作，这

种漏洞是数组越界漏洞
66.结合了程序理解和模糊测试的测试技术，被称为智能模糊测试技术
67.通过网络等途径，自动将自身的全部或部分代码复制传播给网络中其它计算机的完全独立的可运行程序，被称为蠕虫
68.Web 安全检测技术包括黑盒检测和白盒检测两种主要检测技术
69.出现漏洞的可能性是指成功攻击机构内某个漏洞的概率
70.有关国家秘密的相关事项中，应当根据事项的具体性质和特点，按照维护国家安全和利益的需要，限定在必要的期限内，不能确定期限的，应当确定解密条件

三、综合题

71~76（6′，每空一分）

为了构建一个简单、安全的“客户机/服务器”模式的应用系统，防止非法的客户机接入，要求每个用户进行身份认证。假设服务器的公钥为 PK，私钥为 SK；用户 Alice 的公钥为 PKA，私钥为 SKA。Alice 和服务器互相知道彼此的公钥。请回答下述问题

（1）为了完成服务器对 Alice 的认证：首先，服务器产生一个随机数 r，为了保护该随机数，服务器将使用 Alice 的公钥对其加密后发送给 Alice；然后，Alice 用自己的私钥进行解密得到随机数 r；第三，Alice 用自己的私钥对该随机数进行签名，并将签名结果发送给服务器；最后，服务器用 Alice 的公钥对签名结果进行校验，如果校验通过，则对 Alice 的身份认证通过

（2）为了确保 RSA 密码的安全，必须认真选择参数：模数 n 至少 1024 位；为了使加密速度快，根据“反复平方乘”算法，e 的二进制表示中应当含有尽量少的 1

77~80（4′，每空一分）

为了增强 Windows 系统的安全，填空：

（1）权限适用于对特定对象如目录和文件的操作，每一个权限级别都确定了一个执行特定的任务组合的能力，包括 Read、Execute、Write、Delete 和 SetPermission 等。如果对目录有 Execute 权限，表示可以穿越目录，进入其子目录

（2）要使网络用户可以访问在 NT Server 服务器上的文件和目录，必须首先对这些文件和目录建立共享

（3）为了防止网络黑客在网络上猜出用户的密码，可以在连续多次无效登录之后对用户账号实行锁定策略

（4）在 Windows 系统中，任何涉及安全对象的活动都应该受到审核。审核报告将被写入安全日志中，可以使用事件查看器来查看

81~90（10′，每空一分）

为了实现对目标主机的远程控制，木马程序都采用 C/S 的结构，它由两部分程序组成，即客户端和服务端木马程序。请完成下列相关题目

（1）第一代和第二代木马采用的网络连接方法，是由木马的客户端程序连接木马服务端程序

（2）随着防火墙技术的大量应用，第三代及之后的木马为了突破防火墙的拦截，采用了反弹端口技术，由木马的服务端程序主动连接木马的客户端程序。

（3）通过反弹端口技术，木马服务端可连接采用动态公网 IP 地址的木马客户端，木马客户端的动态 IP 地址和端口通过代理服务器来传递。参见下图，假设网络中三台计算机分别是木马客户端、代理服务器和木马服务端，请补充下面采用反弹端口技术的木马连接过程：

图　反弹端口的连接方式

首先，木马客户端将更新后的 IP 地址和端口号保存到代理服务器；其次，木马服务端连接代理服务器获取更新后的 IP 和端口信息；最后，木马服务端按照新的 IP 地址和端口连接木马客户端

第十七套

一、选择题

1.信息安全的发展大致经历了三个阶段。（不属于）这三个阶段的是：互联网使用阶段

2.P2DR 模型是美国 ISS 公司提出的动态网络安全体系的代表模型，可用数学公式表达式表达为 Pt>Dt+Rt，其中 Pt 表示：系统防护时间

3.美国联邦政府颁布数字签名标准的年份是：1994

4.信息安全技术包括：全对

5.密码分析者（攻击者）已知加密算法和要解密的密文时，所能发起的攻击类型：唯密文攻击

6.DES 的密码结构基于：Feistel 网络

7.（不能）用于产生认证码的是：帧校验序列

8.有关 Diffie-Hellman 算法，（错误的）是：支持对所生成的密钥的认证

9.强制访问控制模型中，属于保密性模型的是：Bell-Lapudula

10.属于 RADIUS 协议优点的是：简单明确，可扩充

11.属于单点登录缺点的：需细致地分配用户权限，否则易于造成用户权限过大

12.假设 Alice 的 RSA 公钥为(e=3,n=55)。Bob 发送消息 m=14 给 Alice，则 Bob 对消息加密后得到的密文是：49

【解析】RSA算法中，加密运算为：C = Me mod n，所以Bob对消息加密的过程如下：C = 143 mod 55 = 49，密文为49。本题答案为A。

13.有关访问控制中主体和客体概念的说法中，（错误的）是：主体只能是访问信息的程序、进程

14.（不可以）将 CPU 模式从用户模式转到内核模式的是：系统调用

15.在 Linux/UNIX 系统中，编号为 1 的进程是：init

16.Windows 中必须存在的环境子系统是：win32

17.TCM 是指：可信密码模块

18.关系数据库系统中的所有数据以表格的方式来描述，每一个数据表又可以称为：关系

19.（不属于）数据库安全模型的是：基于过程的模型

20.“一个大学管理员在工作中只需要能够更改学生的联系信息，不过他可能会利用过高的数据库更新权限来更改分数”，这类数据库安全威胁是：过度的特权滥用

21.能提供源主机应用程序和目标主机应用程序之间数据端到端传输服务的 TCP/IP 层次是：传输层

22.通过 MAC 地址获取对应 IP 地址的协议是：RARP

23.TCP 头部字段中有 6 个标志位，表示出现差错释放 TCP 连接后重新建立新连接的标志位是：RST

24.关于弱口令扫描技术，正确的：弱口令扫描主要包括：基于字典攻击的扫描技术和基于穷举攻击的扫描技术

25.（不能）防范网络嗅探的：SMTP

26.（不属于）诱骗式攻击手段的是：漏洞利用

27.针对 XSS 的防范措施（不包括）：按照最小权限原则设置数据库的连接权限

28.Internet 上提供的一种查找相关域名、IP 地址、E-mail 信箱、联系电话等信息的服务是：whois

29.TCP 的端口号范围是：0-65535
30.数组越界漏洞触发时的特征，（不包括）：对整型变量进行运算时没有考虑到其边界范围
31.指令寄存器 eip 存放一个指针，该指针始终指向：返回地址
32.针对 Heap Spray，Windows 系统最好的防范方法是：开启 DEP
33.（不属于）软件安全开发技术的是：安全防护
34.微软的 SDL 模型中，通过教育培训培养开发团队员工的安全意识，属于：第 0 阶段：准备阶段
35.属于可执行代码静态安全检测技术的是：基于程序结构和程序语义的安全检测技术
36.（不属于）逆向分析辅助工具的是：MetaSploit
37.信息安全管理体系是一个系统化、程序化和文件化的管理体系，它所属的范畴是：风险管理
38.在定义 ISMS 的范围时，为了使 ISMS 定义得更加完整，组织机构无需重点考虑的实际情况是：发展规划
39.信息安全风险评估的复杂程度取决于受保护的资产对安全的敏感程度和所面临风险的复杂程度。可供选择的风险评估方法，（不包括）：特殊风险评估
40.有关信息安全管理体系，（错误的）是：信息安全管理工作的基础是风险处置
41.在具体实施 ISMS 构架时，组织机构应建立一个文件控制程序。下列对该程序控制范围的描述中，（错误的）是：体系文件不属于信息资产，不必进行密级标记
42.在建立信息安全管理框架时，确定管制目标和选择管制措施所遵循的基本原则是：费用不高于风险所造成的损失
43.信息安全管理体系认证基于：自愿原则
44.机关、单位应当根据工作需要，确定国家秘密的具体的解密时间(或者解密条件)和：保密期限
45.符合计算机使用道德规范的是：不破坏别人的计算机系统资源
46.属于《计算机信息系统安全保护等级划分准则》中安全考核指标的是：身份认证
47.信息安全管理基本管理要求涉及五个方面内容，即：物理安全、网络安全、主机安全、应用安全和数据安全
48.机构想要提供电子认证服务，属于应具备的必须条件的是：具有符合国家安全标准的技术和设备
49.ISO13335 标准首次给出了关于 IT 安全的 6 个方面含义：机密性、可用性、审计性、认证性、可靠性和完整性
50.《计算机信息系统安全保护等级划分准则》将信息系统安全分为 5 个等级：系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级和自主保护级

二、填空题

51.信息安全的五种基本属性是机密性、完整性、可控性、可用性和不可否认性
52.P2DR 模型包括策略、防护、检测、响应 4 个部分
53.加密算法一般要能抵抗选择明文攻击才认为是安全的
54.哈希函数可以将任意长度的输入经过变换后得到固定长度的输出
55.实际应用中为了缩短签名的长度、提高签名的速度，而且为了更安全，常对信息的摘要进行签名
56.访问控制是在身份认证的基础上，依据授权对提出的资源访问请求加以控制
57.审计就是对日志记录的分析，并以清晰的、能理解的方式表述系统信息
58.环决定对敏感系统资源的访问级别，环号越低，赋予运行在该环内的进程的权限就越大
59.在 UNIX/Linux 中，服务就是运行在网络服务器上监听用户请求的进程，服务是通过端

口号来区分的
60.在 Windows 系统中，查看进程命令并能查看进程同服务的关系的 DOS 命令，是 tasklist
61.美国国防部在 1983 年制定了世界上第一个《可信计算机系统评估准则》，准则中第一次提出可信计算机和可信计算基的概念，并把可信计算基作为系统安全的基础
62.黑客通过诱使用户访问来实施网络欺诈的伪造网站，通常称为钓鱼网站
63.根据 IDS 检测入侵行为的方式和原理的不同，IDS 分为两种入侵检测技术。其中，基于统计分析的 IDS 检测技术属于异常检测技术
64.软件保护技术中，通过对可执行文件的压缩或者加密，进而改变可执行文件中的代码表现形式以增加动态逆向分析的难度，被称为软件加壳技术
65.通过网络等途径，自动将自身的全部代码或部分代码通过网络复制、传播给其它网络中计算机的完全独立可运行程序，被称为蠕虫
66.通过将恶意程序加载到虚拟环境中运行，从而让恶意程序自动脱壳还原为原有状态，再进行检测查杀的技术，被称为虚拟机查杀技术
67.如果攻击者窃取了用户的 Session，并一直保持其有效，而服务器对于活动的 Session 一直不销毁，攻击者就能通过此 Session—直使用用户的账户，这是会话保持攻击
68.缓冲区溢出攻击中，植入的一段用以获得执行权限的代码，被称为 shellcode
69.ISMS 强调遵守国家有关信息安全的法律法规及其他合同方要求，强调全过程和动态控制，体现预防为主的思想
70.CC 标准是指《信息技术安全性评估准则》，其对应的国标编号为 GB/T 18336

三、综合题

71~76（6′，每空一分）

为了构建一个基于公有云的数据共享系统，要求：
①数据加密之后上传到云服务器
②需要校验存储在云服务器数据的完整性
③数据加密密钥需要安全地发送给允许访问数据的用户
请根据题意完成下列各题：
假设要构建的应用系统允许使用的密码学算法包括 MD5、SHA1、AES、RSA、ECC 算法
（1）在数据上传之前，需要采用高效、安全的加密算法对数据进行加密，可采用的加密算法为 AES
（2）为了校验数据的完整性，需要计算所上传数据的消息摘要，为了获得更高的安全性，应该采用的密码学算法为 SHA1
（3）假设用户 B 的公钥为 PUB，私钥为 PRI，为了将数据加密密钥发送给用户 B，数据上传者将使用 B 的公钥 PUB 对该密钥进行加密；用户 B 则使用自己的私钥 PRI 进行解密
（4）消息摘要算法 MD5 对任意长度的明文产生 128 位的消息摘要
（5）为了确保 RSA 密码的安全，模数 n 至少 1024 位

77~80（4′，每空一分）

为了增强 UNIX/Linux 系统的安全，请按要求完成下列相关的题目
（1）UNIX 文件系统安全就是基于 i 节点中三段关键信息：UID、GID 和模式
（2）查看 UNIX 文件权限的命令:$ ls-l。
（3）为一个文件的拥有者授予可读和可写权限，给分组和其它用户只有可读权限，则权限位为“rw-r--r--”。将该权限位用八进制数表示为 644
（4）如果要给文件 foo 的分组以读权限，则使用如下命令:$ chmod g+r foo

81~90（10′，每空一分）

（1）IPSec 协议是一组开放协议的总称，和 SSL 协议不同，IPSec 协议对网络层协议数据

封装后进行传输，而 SSL 协议对应用层协议数据进行加密后传输

（2）IPSec 协议包括网络安全协议和密钥协商协议两部分。其中，网络安全协议又包括两种协议。根据对数据包中封装内容的不同，这两种协议又分为两种封装模式。下面的图 1 至图 4 为两种协议不同模式下的封装格式示意图，请补充图中的内容

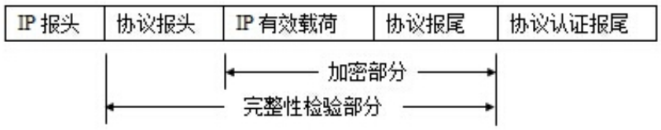


图1 _____ 协议 _____ 模式的封装格式

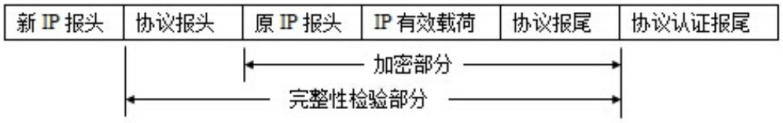


图2 _____ 协议 _____ 模式的封装格式

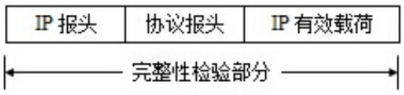


图3 _____ 协议 _____ 模式的封装格式

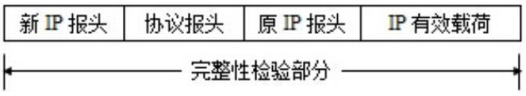


图4 _____ 协议 _____ 模式的封装格式

补充图中的内容：

图 1　ESP 协议传输模式的封装格式

图 2　ESP 协议隧道模式的封装格式

图 3　AH 协议传输模式的封装格式

图 4　AH 协议隧道模式的封装格式

第十八套

一、选择题

1.信息技术的产生与发展大致经历的三个阶段是：电讯技术的发明、计算机技术的发展、互联网的使用

2.信息技术的消极影响，（不包括）：信息隐藏

3.信息安全发展经历的阶段，（不包括）：网络安全阶段

4.信息安全是网络时代国家生存和民族振兴的根本保障

5.美国联邦政府 2001 年颁布的高级加密标准是：AES

6.密码学的英文是：Cryptography

7.假设用户 Alice 的 RSA 公钥为(e=3, n=15)，当 Bob 发送消息给 Alice 时，如果明文 m=4，则对应的密文是：4

【解析】RSA算法中，加密算法为：
C=me mod n，所以Bob对信息加密的过程如下：c=43mod 15=4,密文为4。
答案为A选项。

8.计算机可以在多项式时间复杂度内解决的问题称为：P 问题

9.有关 RADIUS 协议，（错误的）是：RADIUS 协议提供了完备的丢包处理及数据重传机制

10. Bell-LaPadula 模型是一种：强制访问控制模型

11.有关 Kerberos 协议，（错误的）是：身份认证采用的是非对称加密机制

12.用做攻击诱捕的有真实操作系统的虚拟机系统，可以收集到丰富的主机响应信息的是：高交互蜜罐

13.属于分组密码算法的是：SM4

14.需要系统完成特定功能时，通过调用系统中特定的子程序完成的过程，称为：系统调用

15.Linux 系统启动后执行第一个进程是：init

16.有关文件系统管理，（错误的）是：文件系统在安装操作系统之后才会创建

17.在 Windows 系统中，查看当前已经启动的服务列表的命令是：net start

18.有关 SQL 命令，正确的：删除表的命令是 DROP TABLE

19.数据库中，（不能）保证数据完整性的功能是：视图

20.有关数据库安全，（错误的）是：防火墙能对 SQL 注入漏洞进行有效防范

21.OSI/RM 参考模型定义了 7 个层次，从下到上依次是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层

22.TCP 数据包头部的 RST 标志位表示：出现差错，必须释放 TCP 连接，重新建立连接

23.在 Internet 上，Whois 服务能查找的信息中，（不包括）：登录用户

24.网络端口所对应的网络服务中，（错误的）是：110 端口为 SMTP 服务

25.能隐藏端口扫描行为的是：乱序扫描和慢速扫描

26.能防御对 Web 服务器攻击的设备，（不包括）：入侵检测系统

27.防火墙包过滤技术（不能）过滤的是：HTTP 数据包内容

28.入侵防御系统的功能，（不包括）：检测系统漏洞

29.PKI 的核心是：数字证书

30.基址指针寄存器 EBP 存放的指针始终指向：基地址

31.（不属于）软件安全开发技术范畴的是：风险评估

32.代码混淆技术的实现手段，（不包括）：语义转换

33.根据水印的加载位置，软件水印可以分为：代码水印和数据水印

34.恶意程序的传播方法，（不包括）：网络钓鱼
35.Web 安全防护技术，（不包括）：UPS 安全防护
36.软件漏洞产生的原因，（不包括）：软件编译过程中没有采用/GS 安全选项
37.ISMS 体现的思想是：预防控制为主
38.信息安全管理体系审核，包括两个方面的审核，即管理和技术
39.信息安全管理体系认证基于的原则：自愿
40.组织机构进行信息安全管理体系认证的目的，一般包括：全选
41.风险管理的第一阶段是：风险识别
42.信息安全管理措施中，访问控制的实现分类，（不包括）：完整性访问控制
43.为了保证整个信息系统的安全，必须保证系统开发过程的安全，系统的整个开发过程可以划分为五个阶段，即：规划、分析、设计、实现和运行
44.我国发布的第一个有关信息安全方面的标准是在：1985 年
45.1996 年提出，并逐渐形成国际标准 ISO 15408 的标准是：信息技术安全评价通用标准(CC)
46.CC 将评估过程分为两个部分，即：功能和保证
47.根据《信息安全等级保护管理办法》，信息系统受到破坏后，对国家安全造成特别严重损害的，属于：第五级
48.国家秘密的密级分为三级，即绝密、机密和秘密
49.关于电子签名，（错误的）是：只要签署后对电子签名的任何改动都能够被发现，则认为该电子签名就是可靠的
50.电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期那限至少为电子签名认证证书失效后：五年

二、填空题

51.香农在 1949 年发表的论文《保密系统的通信理论》，用信息论的观点对保密问题进行了全面的论述，它是信息安全发展的重要里程碑
52.IATF(Information Assurance TechnicalFramework)是美国国家安全局制定的描述信息保障的指导性文件，其中提出了三个主要核心要素，即人员、技术和操作
53.AES 密码的分组长度是 128 位
54.理想的哈希函数 H 对于不同的输入，获得的哈希值不同。如果存在 x、x’两个不同的消息，存在 H(x)= H(x’)，则称 x 和 x’是哈希函数 H 的一个碰撞
55.消息的接收方可以通过签名来防止所有后续的抵赖行为，因为接收方可以通过出示其给别人看来证明信息的来源
56.AAA 是指认证、授权和审计
57.恶意行为审计与监控主要监测网络中针对服务器的恶意行为，包括恶意的攻击行为和入侵行为
58.操作系统的功能模块，一般以进程的方式在后台运行，以启动服务的方式对用户提供访问接口
59.进程管理是通过中断实现的
60.在 UNIX/Linux 系统中，服务是通过 inetd 进程或启动脚本来启动
61.信任根和信任链是可信计算平台的主要关键技术
62.在 TCP 三次握手中，第二次握手由目标主机发给源主机响应的数据包中序号 SEQ 为 Y,第三次握手由源主机发给目标主机的数据包确认号为 Y+1
63.持久型的跨站脚本攻击也被称为存储型 XSS
64. 限制内存堆栈区的代码为不可执行的状态，从而防范溢出后代码执行的技术是数据执

行保护技术

65.在不实际执行程序的前提下，将程序的输入表示成符号，根据程序的执行流程和输入参数的赋值变化，把程序的输出表示成包含这些符号的逻辑或算术表达式，这种技术被称为符号执行

66.通过向目标软件输入大量的畸形数据并监测目标系统的异常来发现潜在的软件漏洞，这种技术被称为模糊测试技术

67.可以通过网络等途径，自动将自身的全部代码或部分代码，通过网络复制、传播给其它网络中计算机的完全独立可运行程序是蠕虫

68.处于未公开状态的漏洞被称为 0day 漏洞

69.只参照标准所提到的风险项对组织机构的资产进行风险评估的方法叫做基本风险评估

70.《电子签名法》被称为中国首部真正意义上的信息化法律

三、综合题

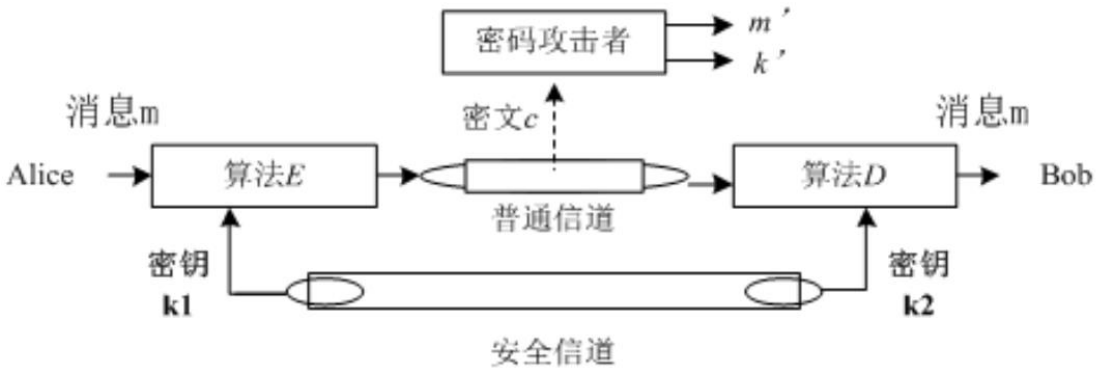
71~75（6′，倒数第二空两分，其余一空一分）

一个密码系统如下图所示。请用如下的 A-F 中的一个选项（例如:A)回答各个题目：

A—对称　B—非对称　C—内容修改　D—顺序修改　E—计时修改　F—发送方否认

G—接收方否认　H—伪装　I—唯密文攻击　J—已知明文攻击　K—选择明文攻击

L—选择密文攻击　M—公钥　N—私钥　O—消息摘要　P—密文



（1）如果密钥 k1 与密钥 k2 相等，则该密码是一种 A 密码

（2）密码攻击者可以对消息内容进行插入、删除、转换等操作，这种攻击叫做 C

（3）如果密码攻击者能任意选择明文并获得该明文对应的密文，基于这些信息去猜测密钥的攻击是 K

（4）如果密钥 k1 和密钥 k2 相等，为了确保消息在传输过程中没有被篡改，Alice 可以计算消息 m 的 O，并附加在 m 后面，然后加密即可

（5）密码攻击者可以将截获的密文消息进行延时和重放，这种攻击叫做 E

76~79（4′，每空一分）

请补全下列有关 Windows 的安全实践：

（1）在 Windows 系统里，用户口令的密文一般保存在 SAM 文件里

（2）在 Windows 系统中，任何涉及安全对象的活动都应该受到审核，审核报告将被写入安全日志中，可以使用“事件查看器”来查看

（3）有两类用户权限，其中登录权限是指账户在通过身份验证之前所具备的权限，而操作权限是指账户在通过身份验证之后所具备的权限

（4）为了增强对日志的保护，可以编辑注册表来改变日志的存储目录。点击“开始”→“运行”，在对话框中输入命令“Regedit”，回车后将弹出注册表编辑器

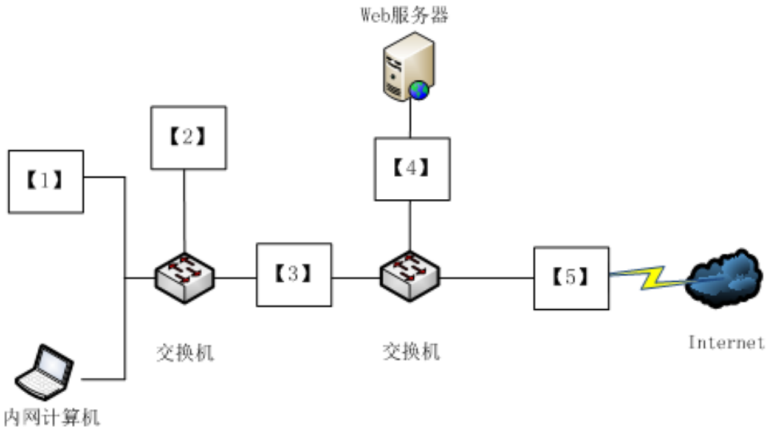
80~89（10′，每空一分）

某单位需要部署安全防护产品，要求防护 Web 服务器的安全设备应具备网络层、传输层的安全防护能力。

请在图 1 中【1】【2】【3】【4】【5】位置处合理部署下面 5 种设备：路由器、防火墙、IDS 探测器、IPS 网络设备、IPS 控制台。每个设备只能部署在一个位置。

为了提高内网的安全性，下面为防火墙进行默认访问控制规则的配置，请补充完整表 1 中的控制规则。其中，访问权限包含允许和禁止两个选项。

序号	源区域	目的区域	访问权限
1	内网	外网	【6】
2	内网	DMZ	【7】
3	外网	内网	【8】
4	外网	DMZ	【9】
5	DMZ	内网	【10】



【1】IPS 控制台
【2】IDS 探测器
【3】IPS 网络设备
【4】防火墙
【5】路由器
【6】允许
【7】允许
【8】禁止
【9】允许
【10】禁止