- dnat：改写数据包目的 IP 地址为某特定 IP 或 IP 范围，可以指定 port 对应的范围，进行完此处理动作后将直接跳往下一个规则链（filter:input 或 filter:forward）。

IPtables 的命令参数非常多，在考试中，主要用到的是 IP 地址伪装和数据包过滤的相关参数。

【例 9-4-15】数据包过滤命令示例。

用 IPtables 建立包过滤防火墙，以实现对内部的 WWW 和 FTP 服务器进行保护。基本规则如下：

```
[root@hunau sbin]# iptables -f   #先清除 mput 链的所有规则
[root@hunau sbin]# iptables -p forward drop   #设置防火墙 forward 链的策略为 drop，也就是防火墙的默认规则是：先禁止转发任何数据包，然后再依据规则允许通过的包
[root@hunau sbin]# iptables -a forward -p tcp -d 172 28 27.100 --dport www -i eth0 -j accept   #开放服务端口为 TCP 协议 80 端口的 WWW 服务
[root@hunau sbin]# iptables -a forward -p tcp -d 172.28 27 100 --dport ftp -i eth0 -j accept   #开放 FTP 服务，其余的服务依此类推即可。这里要特别注意的是，设置服务器的包过滤规则时要保证服务器与客户机之间的通信是双向的，因此不仅要设置数据包流出的规则，还要设置数据包返回的规则。下面是内部数据包流出的规则
[root@hunau sbin]# iptables -a forward -s 172 28 27 0/24 -i eth1 -j accept   #接收来自整个内部网络的数据包并使之通过
```


5 模拟测试，反复操练

经历过前 4 天的学习后，进入最后一天的学习了。今天最主要的任务就是做模拟题、熟悉考题风格、检验自己的学习成果。考生一定摩拳擦掌好久了吧？下面就一起来进入吧。

第 1～2 学时　模拟测试（上午一）

1．国家密码管理局于 2006 年公布了“无线局域网产品须使用的系列密码算法”，其中规定签名算法应使用的算法是__(1)__。

A．DH　　B．ECDSA　　C．ECDH　　D．CPK

2．以下网络攻击中，__(2)__属于被动攻击

A．拒绝服务攻击　　B．重放　　C．假冒　　D．窃听

3．下列算法中，不属于非对称加密算法的是__(3)__。

A．ECC　　B．DSA　　C．RSA　　D．RC5

4．利用 3DES 进行加密，以下说法正确的是__(4)__。

A．3DES 的密钥长度是 56 位

B．3DES 全部使用三个不同的密钥进行三次加密

C．3DES 的安全性高于 DES

D．3DES 的加密速度比 DES 加密速度快

5．面向身份信息的认证应用中，最简单的认证方法是__(5)__。

A．基于数据库的认证　　B．基于摘要算法认证

C．基于 PKI 认证　　D．基于账户名/口令认证

6．在报文摘要算法 MD5 中，首先要进行明文分组与填充，其中分组时明文报文摘要按照__(6)__位分组。

A．128　　B．256　　C．512　　D．1024

7．报文摘要算法 SHA-1 输出的位数是__（7）__。

A．100 位　　B．128 位　　C．160 位　　D．180 位

8．利用报文摘要算法生成报文摘要的目的是__（8）__。

A．验证通信对方的身份，防止假冒

B．对传输数据进行加密，防止数据被窃听

C．防止发送方否认发送过的数据

D．防止发送的报文被篡改

9．公钥体系中，用户甲发送给用户乙的数据要用__（9）__进行加密。

A．甲的公钥　　B．甲的私钥　　C．乙的公钥　　D．乙的私钥

10．在电子政务信息系统设计中应高度重视系统的__（10）__设计，防止对信息的篡改、越权获取和蓄意破坏。

A．容错　　B．结构化　　C．可用性　　D．安全性

11．以下关于入侵检测设备的叙述中，__（11）__是不正确的。

A．不产生网络流量　　B．部署在靠近攻击源的地方，则很有效

C．使用在尽可能接近受保护资源的地方　　D．必须跨接在链路上

12．代理服务器防火墙主要使用代理技术来阻断内部网络和外部网络之间的通信，达到隐蔽内部网络的目的。以下关于代理服务器防火墙的叙述中，__（12）__是不正确的。

A．仅“可以信赖的”代理服务才允许通过

B．由于已经设立代理，因此任何外部服务都可以访问

C．允许内部主机使用代理服务器访问 Internet

D．不允许外部主机连接到内部安全网络

13．完整性是信息未经授权不能进行改变的特性，它要求保持信息的原样。下列方法中，不能用来保证应用系统完整性的措施是__（13）__。

A．安全协议　　B．纠错编码　　C．数字签名　　D．信息加密

14．在信息系统安全管理中，业务流控制、路由选择控制和审计跟踪等技术主要用于提高信息系统的__（14）__。

A．保密性　　B．可用性　　C．完整性　　D．不可抵赖性

15．以下选项中，不属于生物特征识别方法的是__（15）__。

A．语音识别　　B．指纹识别

C．气味识别　　D．身份证号识别

16．计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效应的确定和提取。以下关于计算机取证的描述中，错误的是__（16）__。

A．计算机取证的通常步骤有：准备工作、保护目标计算机系统（保护现场）、确定电子证据、收集电子证据、保全电子证据

B．计算机取证的工具有 X-Ways Forensics、X-Ways Trace、FBI 等

C．计算机取证时，可先将目标主机设置为蜜罐，等待犯罪嫌疑人破坏证据时，一举抓获

D．电子证据综合了文本、图形、图像、动画、音频及视频等多种类型的信息

17．注入语句：http：//xxx.xxx.xxx/abc.asp?p=YY and db_name()>0 不仅可以判断服务器的后台数据库是否为 SQL Server，还可以得到__（17）__。

A．当前连接数据库的用户数量　　B．当前连接数据库的用户名

C．当前正在使用的用户口令　　D．当前正在使用的数据库名

18．数字水印利用人类的听觉、视觉系统的特点，在图像、音频、视频中加入特定的信息，使人很难察觉，而通过特殊方法和步骤又能提取所加入的特定信息。数字图像的内嵌水印有很多鲜明的特点，其中，加入水印后图像不能有视觉质量的下降，与原始图像对比，很难发现二者的差别属于__（18）__。

A．透明性　　B．机密性　　C．鲁棒性　　D．安全性

19．数字水印常用算法中，__（19）__算法将信息嵌入到随机选择的图像点中最不重要的像素位上。

A．Patchwork　　B．LSB　　C．DCT　　D．NEC

20．数字水印空间域算法中，__（20）__算法利用像素的统计特征将信息嵌入像素的亮度值中。该算法先对图像分块，再对每个图像块进行嵌入操作，可以加入更多信息。

A．Patchwork　　B．LSB　　C．DCT　　D．NEC

21．下列网络攻击行为中，属于 DoS 攻击的是__（21）__。

A．特洛伊木马攻击　　B．SYN Flooding 攻击

C．端口欺骗攻击　　D．IP 欺骗攻击

22．下面属于蠕虫病毒的是__（22）__。

A．Worm.Sasser 病毒　　B．Trojan.QQPSW 病毒

C．Backdoor.IRCBot 病毒　　D．Macro.Melissa 病毒

23．杀毒软件报告发现病毒 Macro. Melissa，由该病毒名称可以推断出病毒类型是__（23）__，这类病毒的主要感染目标是__（24）__。

（23）A．文件型　　B．引导型　　C．目录型　　D．宏病毒

（24）A．.exe 或.com 可执行文件　　B．Word 或 Excel 文件

C．DLL 系统文件　　D．磁盘引导区

24．依据《中华人民共和国网络安全法》，某大学购买了上网行为管理设备，安装时设定设备日志应该保存__（25）__。

A．1 个月　　B．3 个月　　C．6 个月　　D．12 个月

25．依据《信息安全等级保护管理办法》要求，某政府信息化办公室按照密级为机密的标准，对单位涉密信息系统实施分级保护，其保护水平总体上不低于国家信息安全等级保护__（26）__的水平。

A．第二级　　B．第三级　　C．第四级　　D．第五级

26．《中华人民共和国刑法》（2015 修正）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__（27）__有期徒刑或者拘役。

A．一年以上　　B．三年以下　　C．五年以上　　D．三年以上七年以下

27．依据《信息安全等级保护管理办法》，信息系统的安全保护等级分为__（28）__级。

A．2　　B．3　　C．4　　D．5

28．《信息安全等级保护管理办法》中，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。该系统的安全保护等级为__（29）__级。

A．2　　B．3　　C．5　　D．6

29．依据《信息安全等级保护管理办法》，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。这种措施属于__（30）__级。

A．2　　B．3　　C．5　　D．6

30．__（31）__是应用系统工程的观点、方法，分析网络系统安全防护、监测和应急恢复。这一原则要求在进行安全规划设计时充分考虑各种安全措施的一致性，不要顾此失彼。

A．木桶原则　　B．整体原则

C．等级性原则　　D．动态化原则

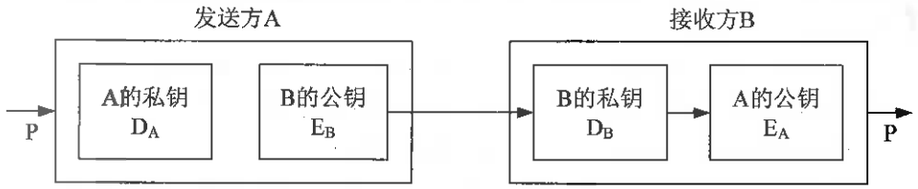
31．一个数据包过滤系统被设计成只允许用户许可服务的数据包进入，而过滤掉不必要的服务。这属于__（32）__基本原则。

A．最小特权　　B．最大共享　　C．开放系统　　D．封闭系统

32．安全电子邮件使用__（33）__协议。

A．PGP　　B．HTTPS　　C．MIME　　D．DES

33．下图为一种数字签名方案，网上传送的报文是__（34）__，防止 A 抵赖的证据是__（35）__。



（34）A．P　　B．$D_A(P)$　　C．$E_B(D_A(P))$　　D．D_A

（35）A．P　　B．$D_A(P)$　　C．$E_B(D_A(P))$　　D．D_A

34．在 X.509 标准中，不包含在数字证书中的数据域是__（36）__。

A．序列号　　B．签名算法

C．认证机构的签名　　D．私钥

35．某 Web 网站向 CA 申请了数字证书。用户登录该网站时，通过验证__（37）__，可确认该数字证书的有效性，从而__（38）__。

（37）A．CA 的签名　　B．网站的签名

C．会话密钥　　D．DES 密码

（38）A．向网站确认自己的身份　　B．获取访问网站的权限

C．和网站进行双向认证　　D．验证该网站的真伪

36．计算机感染特洛伊木马后的典型现象是__（39）__。

A．程序异常退出　　B．有未知程序试图建立网络连接

C．邮箱被垃圾邮件填满　　D．Windows 系统黑屏

37．下列行为不属于网络攻击的是__（40）__。

A．连续不停 Ping 某台主机　　B．发送带病毒和木马的电子邮件

C．向多个邮箱群发一封电子邮件　　D．暴力破解服务器密码

38．窃取是对__（41）__的攻击，DDos 攻击破坏了__（42）__。

（41）A．可用性　　B．保密性　　C．完整性　　D．真实性

（42）A．可用性　　B．保密性　　C．完整性　　D．真实性

39．下面__（43）__地址可以应用于公共互联网中。

A．10.172.12.56　　B．172.32.12.23

C．192.168.22.78　　D．172.16.33.124

40．ICMP 协议属于因特网中的__（44）__协议，ICMP 协议数据单元封装在__（45）__中。

（44）A．数据链路层　　B．网络层

C．传输层　　D．会话层

（45）A．以太帧　　B．TCP 段

C．UDP 数据报　　D．IP 数据报

41．ARP 协议的作用是__（46）__，它的协议数据单元封装在__（47）__中传送。ARP 请求是采用__（48）__方式发送的。

（46）A．由 MAC 地址求 IP 地址　　B．由 IP 地址求 MAC 地址

C．由 IP 地址查域名　　D．由域名查 IP 地址

（47）A．IP 分组　　B．以太帧　　C．TCP 段　　D．UDP 报文

（48）A．单播　　B．组播　　C．广播　　D．点播

42．下面信息中__（49）__包含在 TCP 头中而不包含在 UDP 头中。

A．目标端口号　　B．顺序号　　C．发送端口号　　D．校验号

43．在进行域名解析过程中，由__（50）__获取的解析结果耗时最短。

A．主域名服务器　　B．辅域名服务器

C．本地缓存　　D．转发域名服务器

44．在 Kerberos 认证系统中，用户首先向__（51）__申请初始票据，然后从__（52）__获得

会话密钥。

（51）A．域名服务器 DNS　　B．认证服务器 AS
　　C．票据授予服务器 TGS　　D．认证中心 CA

（52）A．域名服务器 DNS　　B．认证服务器 AS
　　C．票据授予服务器 TGS　　D．认证中心 CA

45．如果一个登录处理子系统允许处理一个特定的用户识别码，以绕过通常的口令检查，则这种威胁属于__（53）__。

A．假冒　　B．授权侵犯　　C．旁路控制　　D．陷门

46．HTTPS 是一种安全的 HTTP 协议，它使用__（54）__来保证信息安全，使用__（55）__来发送和接收报文。

（54）A．IPSec　B．SSL　　C．SET　　D．SSH

（55）A．TCP 的 443 端口　　B．UDP 的 443 端口
　　C．TCP 的 80 端口　　D．UDP 的 80 端口

47．以下用于在网络应用层和传输层之间提供加密方案的协议是__（56）__。

（56）A．PGP　　B．SSL　　C．IPSec　　D．DES

48．主动防御是新型的杀病毒技术，其原理是__（57）__。

A．根据特定的指令串识别病毒程序并阻止其运行
B．根据特定的标志识别病毒程序并阻止其运行
C．根据特定的行为识别病毒程序并阻止其运行
D．根据特定的程序结构识别病毒程序并阻止其运行

49．很多系统在登录时都要求用户输入以图片形式显示的一个字符串，其作用是__（58）__。

A．阻止没有键盘的用户登录　　B．欺骗非法用户
C．防止用户利用程序自动登录　　D．限制登录次数

50．IPSec 的加密和认证过程中所使用的密钥由__（59）__机制来生成和分发。

A．ESP　　B．IKE　　C．TGS　　D．AH

51．针对用户的需求，设计师提出了用物理隔离来实现网络安全的方案。经过比较，决定采用隔离网闸实现物理隔离。物理隔离的思想是__（60）__，隔离网闸的主要实现技术不包括__（61）__。

（60）A．内外网隔开，不能交换信息
　　B．内外网隔开，但分时与另一设备建立连接，间接实现信息交换
　　C．内外网隔开，但分时对一存储设备写和读，间接实现信息交换
　　D．内外网隔开，但只有在经过网管人员或网管系统认可时才能连接

（61）A．实时开关技术　　B．单向连接技术
　　C．网络开关技术　　D．隔离卡技术

52．用于保护通信过程的初级密钥在分配时，通常的形式是__（62）__，利用其加密或解密时，应实施的操作是__（63）__。

（62）A．一次一密的明文　　B．一次一密的密文
　　C．可多次使用的密文　　D．不限次数的密文

（63）A．利用二级密钥解密出原始密钥
　　B．利用主密钥解密出原始密钥
　　C．利用二级密钥和主密钥解密出原始密钥
　　D．利用自身私钥解密出原始密钥

53．椭圆曲线密码 ECC 是一种公开密钥加密算法体制，其密码由六元组 T=<p,a,b,G,n,h>表示。用户的私钥 d 的取值为__（64）__，公钥 Q 的取值为__（65）__。

利用 ECC 实现数字签名与利用 RSA 实现数字签名的主要区别是__（66）__。

（64）A．0～n-1 间的随机数　　B．0～n-1 间的一个素数
　　C．0～p-1 间的随机数　　D．0～p-1 间的一个素数

（65）A．Q=dG　B．Q=ph　　C．Q=ab G　　D．Q=hnG

（66）A．ECC 签名后的内容中没有原文，而 RSA 签名后的内容中包含原文
　　B．ECC 签名后的内容中包含原文，而 RSA 签名后的内容中没有原文
　　C．ECC 签名需要使用自己的公钥，而 RSA 签名需要使用对方的公钥
　　D．ECC 验证签名需要使用自己的私钥，而 RSA 验证签名需要使用对方的公钥

54．S 盒是 DES 中唯一的非线性部分，DES 的安全强度主要取决于 S 盒的安全强度。DES 中有__（67）__个 S 盒，其中__（68）__。

（67）A．2　　B．4　　C．6　　D．8

（68）A．每个 S 盒有 6 个输入，4 个输出
　　B．每个 S 盒有 4 个输入，6 个输出
　　C．每个 S 盒有 48 个输入，32 个输出
　　D．每个 S 盒有 32 个输入，48 个输出

55．RC4 是 Ron Rivest 为 RSA 设计的一种序列密码，它在美国一般密钥长度是 128 位，因为受到美国出口法的限制，向外出口时限制到__（69）__位。

A．64　　B．56　　C．32　　D．40

56．打电话请求密码属于__（70）__攻击方式。

A．木马　　B．社会工程
C．电话窃听攻击　　D．电话系统漏洞

57．Certificates are __（71）__ documents attesting to the __（72）__ of a public key to an individual or other entity. They allow verification of the claim that a given public key does in fact belong to a given individual. Certificates help prevent someone from using a phony key to __（73）__ someone else. In their simplest form, certificates contain a public key and a name. As commonly used, a certificate also contains an __（74）__ date, the name of the CA that issued the certificate, a serial number, and perhaps other information. Most importantly, it contains the digital __（75）__ of the certificate issuer.

The most widely accepted format for certificates is X.509 , thus, certificates can be read or written by any application complying with X.509.

（71）A. text　B. data　C. digital　D. structured

（72）A. connecting　B. binding　C. composing　D. conducting

（73）A. impersonate　B. personate　C. damage　D. control

（74）A. communication　B. computation　C. expectation　D. expiration

（75）A. signature　B. mark　C. stamp　D. hypertext

第 3～4 学时　模拟测试（下午一）

试题一（共 20 分）

【说明】

密码编码学是研究把信息（明文）变换成没有密钥就不能解读或很难解读的密文的方法，密码分析学的任务是破译密码或伪造认证密码。

【问题 1】（10 分）

通常一个密码系统简称密码体制，请简述密码体制的构成。

【问题 2】（3 分）

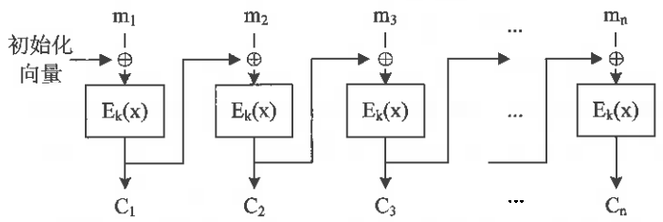
根据所基于的数学基础的不同，非对称密码体制通常分为__（1）__、__（2）__、__（3）__。

【问题 3】（2 分）

根据密文数据段是否与明文数据段在整个明文中的位置有关，可以将密码体制分为__（4）__体制和__（5）__体制。

【问题 4】（5 分）

在下图给出的加密过程中，m_i（i=1,2,…,n）表示明文分组，c_i（i=1,2,…,n）表示密文分组，K 表示密钥，E 表示分组加密过程。该分组加密过程属于哪种工作模式？这种分组密码的工作模式有什么缺点？



试题二（共 15 分）

【说明】

RSA 是典型的非对称加密算法，该算法基于大素数分解。核心是模幂运算。利用 RSA 密码可以同时实现数字签名和数据加密。

【问题 1】（3 分）

简述 RSA 的密钥生成过程。

【问题 2】（4 分）

简述 RSA 的加密和解密过程。

【问题 3】（4 分）

简述 RSA 的数字签名过程。

【问题 4】（4 分）

在 RSA 中，已获取用户密文 C=10，该用户的公钥 e=5，n=35，求明文 M。

试题三（共 10 分）

【说明】

阅读下面程序，回答问题 1 至问题 3。

```
void function(char *str)
{
    char buffer[16],
    strcpy(buffer,str);
}
void main()
{
  int t;
  char buffer[128];
  for(i=0;i<127;i++)
    buffer[i] ='A';
    buffer[127]=0;
  function(buffer);
  print("This is a test\n");
}
```

【问题 1】（3 分）

上述代码能否输出“This is a test”？上述代码存在什么类型的隐患？

【问题 2】（4 分）

造成上述隐患的原因是？

【问题 3】（3 分）

给出消除该安全隐患的思路。

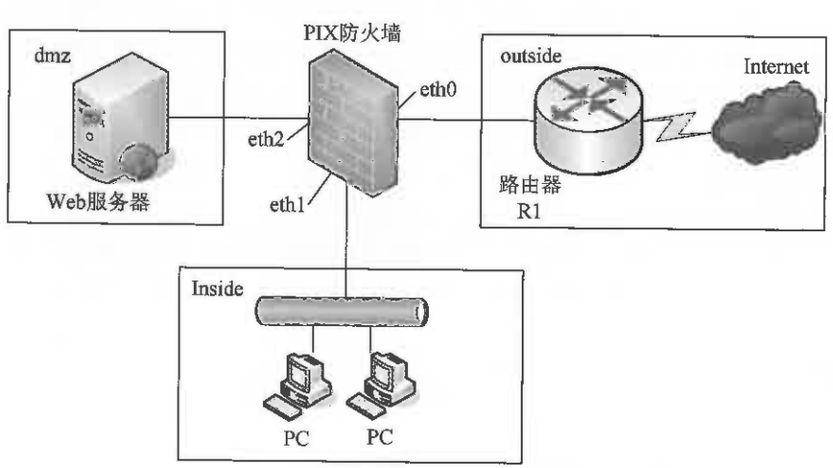
试题四（共15分）

【说明】

某公司通过 PIX 防火墙接入 Internet，网络拓扑如下图所示。

在防火墙上利用 show 命令查询当前配置信息如下：

```
PIX#show config
...
nameif eth0 outside security 0
nameif eth1 inside security 100
nameif eth2 dmz security 40
...
fixup protocol ftp 21
fixup protocol http 80___(1)___
...
ip address outside 61.144.51.42 255.255.255.248
ip address inside 192.168.0.1 255.255.255.0
ip address dmz 10.10.0.1 255.255.255.0
...
global (outside) 1 61.144.51.46
nat (inside) 1 0.0.0.0 0.0.0.0
...
route outside 0.0.0.0 0.0.0.0 61.144.51.451   ___(2)___
...
```



【问题 1】（4 分）

解释（1）、（2）处画线语句的含义。

【问题 2】（6 分）

根据配置信息填写以下表格。

习题用表

域名称	接口名称	IP 地址	IP 地址掩码
inside	eth1	___(3)___	255.255.255.0
outside	eth0	61.144.51.42	___(4)___
dmz	___(5)___	___(6)___	255.255.255.0

【问题 3】（2 分）

根据所显示的配置信息，由 inside 域发往 Internet 的 IP 分组在到达路由器 R1 时的源 IP 地址是___(7)___。

【问题 4】（3 分）

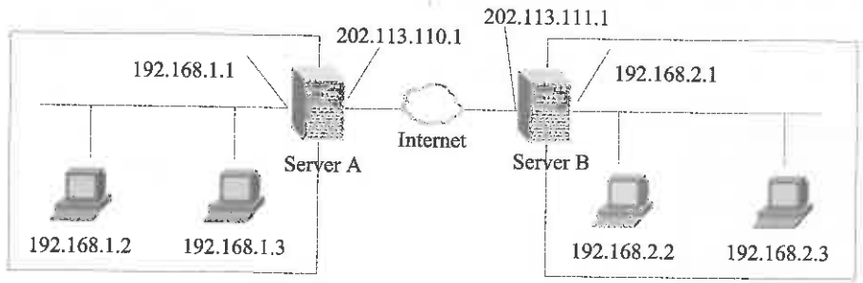
如果需要 dmz 域的服务器（IP 地址为 10.10.0.100）对 Internet 用户提供 Web 服务（对外公开 IP 地址为 61.144.51.43），请补充完成下列配置命令。

```
PIX（config）#static（dmz,outside）___(8)___ ___(9)___
PIX（config）#conduit permit tcp host ___(10)___ eq www any
```

试题五（共15分）

【说明】

某企业在公司总部和分部之间采用两台 Windows Server 2003 服务器部署企业 IPSec VPN，将总部和分部的两个子网通过 Internet 互连，如下图所示。



【问题 1】（3 分）

隧道技术是 VPN 的基本技术，隧道是由隧道协议形成的，常见隧道协议有 IPSec、PPTP 和 L2TP，其中___(1)___和___(2)___属于第二层隧道协议，___(3)___属于第三层隧道协议。

【问题 2】（3 分）

IPSec 安全体系结构包括 AH、ESP 和 ISA KMP/Oakley 等协议。其中，___(4)___为 IP 包提供信息源验证和报文完整性验证，但不支持加密服务；___(5)___提供加密服务；___(6)___提供密钥管理服务。

【问题 3】(6 分)

设置 Server A 和 Server B 之间通信的“筛选器 属性”界面如图 1 所示，在 Server A 的 IPSec 安全策略配置过程中，当源地址和目标地址均设置为“一个特定的 IP 子网”时，源子网 IP 地址应设为__(7)__，目标子网 IP 地址应设为__(8)__。如图 2 所示的隧道设置中的隧道终点 IP 地址应设为__(9)__。

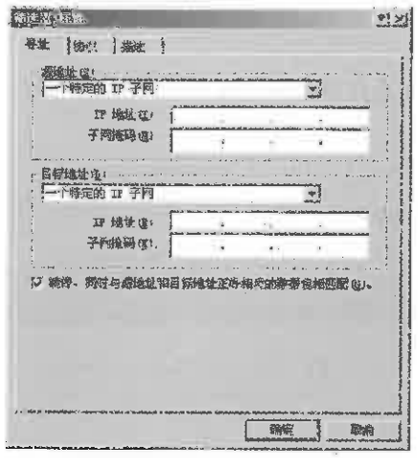


图 1 “筛选器 属性”对话框

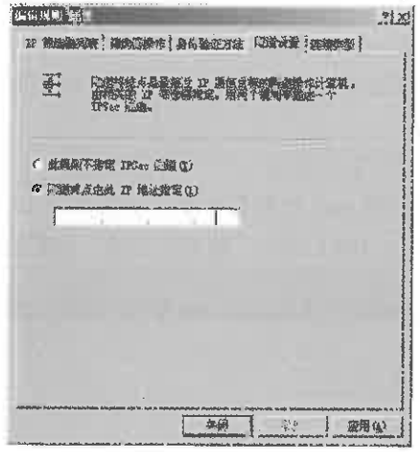


图 2 “编辑规划 属性”对话框

【问题 4】(3 分)

在 Server A 的 IPSec 安全策略配置过程中，Server A 和 Server B 之间通信的 IPSec 筛选器“许可”属性设置为“协商安全”，并且安全措施为“加密并保持完整性”，如图 3 所示。根据上述安全策略填写图 4 中的空格，表示完整的 IPSec 数据包格式。

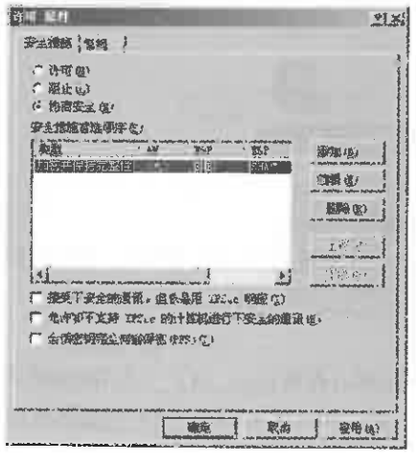


图 3 “许可 属性”对话框

新 IP 头	(10)	(11)	TCP 头	数据	(12)

图 10-4 数据包格式

(10)～(12)备选答案：

A. AH 头　　B. ESP 头　　C. 旧 IP 头　　D. 新 TCP 头

E. AH 尾　　F. ESP 尾　　G. 旧 IP 尾　　H. 新 TCP 尾

第 5～6 学时 模拟测试点评（上午一）

试题 1 解析

国家密码管理局于 2006 年 1 月 6 日发布公告，公布了“无线局域网产品须使用的系列密码算法”，包括：

- 对称密码算法：SMS4；
- 签名算法：ECDSA；
- 密钥协商算法：ECDH；
- 杂凑算法：SHA-256；
- 随机数生成算法：自行选择。

其中，ECDSA 和 ECDH 密码算法须采用国家密码管理局指定的椭圆曲线和参数。

试题答案：B

试题 2 解析

攻击可分为两类：

■主动攻击涉及修改数据流或创建数据流，它包括假冒、重放、修改消息与拒绝服务。

■被动攻击只是窥探、窃取、分析重要信息，但不影响网络、服务器的正常工作。

试题答案：D

试题 3 解析

加密密钥和解密密钥相同的算法，称为对称加密算法。常见的对称加密算法有 DES、3DES、RC5、IDEA

加密密钥和解密密钥不相同的算法，称为非对称加密算法，这种方式又称为公钥密码加密算法。在非对称加密算法中，私钥用于解密和签名，公钥用于加密和认证。典型的公钥密码体制有 RSA、DSA、ECC。

试题答案：D

试题 4 解析

3DES 是 DES 的扩展，是执行了三次的 DES。3DES 安全强度较高，可以抵抗穷举攻击，但是用软件实现起来速度比较慢。

3DES 有两种加密方式：

■第一、三次加密使用同一密钥，这种方式密钥长度 128 位（112 位有效）。

■三次加密使用不同密钥，这种方式密钥长度 192 位（168 位有效）。

目前中国人民银行的智能卡技术规范支持 3DES。

试题答案：C

试题 5 解析

用户名/口令认证技术是最简单、最普遍的身份识别技术，如各类系统的登录等。

试题答案：D

试题 6 解析

消息摘要算法 5（MD5），把信息分为 512 比特的分组，并且创建一个 128 比特的摘要。

试题答案：C

试题 7 解析

安全 Hash 算法（SHA-1），把信息分为 512 比特的分组，并且创建一个 160 比特的摘要。

试题答案：C

试题 8 解析

Hash 函数用于构建数据的“指纹”，而“指纹”用于标识数据，可以防止发送的报文被篡改。

试题答案：D

试题 9 解析

在非对称加密算法中，私钥用于解密和签名，公钥用于加密和认证。因此用乙的公钥加密信息发给乙是合适的。

试题答案：C

试题 10 解析

安全性设计可以防攻击、破坏、篡改等。

试题答案：D

试题 11 解析

入侵检测设备由于可以使用旁路方式部署，不必是跨接方式部署，因此可以不产生流量。

IDS 部署在尽可能接近受保护资源的地方可以起到更好的保护作用，部署在尽可能靠近攻击源的地方则最有效，但因为攻击源的不确定性，所以很难做到。

试题答案：D

试题 12 解析

代理服务型防火墙:防火墙代替用户访问所需信息，再将信息转发给用户。优点是安全，缺点是速度较慢。

这种方式下，也不是所有外部服务都能访问，只有“可以信赖的”代理服务才允许通过。

试题答案：B

试题 13 解析

完整性是信息未经授权不能进行改变的特性。保证完整性手段有安全协议、纠错编码、数字签

名、公证。信息加密属于保证信息不被泄漏给未授权的人。

试题答案：D

试题 14 解析

提高可用性常用方法有：身份识别、访问控制、业务流控制、跟踪审计。

试题答案：B

试题 15 解析

经验表明身体特征（指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和 DNA 等）和行为特征（签名、语音、行走步态等）可以对人进行唯一标识，可以用于身份识别。目前指纹识别技术发展最为深入。

试题答案：D

试题 16 解析

计算机取证时首先必须隔离目标计算机系统，不给犯罪嫌疑人破坏证据的机会。实际取证工作需要遵循一个重要的原则：尽量避免在被调查的计算机上进行工作。

试题答案：C

试题 17 解析

SQL Server 有 user、db_name()等系统变量，利用这些系统值不仅可以判断 SQL-SERVER，而且还可以得到大量有用信息。如：

- 语句 http://xxx.xxx.xxx/abc.asp?p=YY and user>0，不仅可以判断是否是 SQL-SERVER，而且还可以得到当前连接数据库的用户名。
- 语句 http://xxx.xxx.xxx/abc.asp?p=YY and db_name()>0，不仅可以判断是否是 SQL Server，而还可以得到当前正在使用的数据库名。

试题答案：D

试题 18 解析

数字图像的内嵌水印有很多鲜明的特点，具体如下：

透明性：水印后图像不能有视觉质量的下降，与原始图像对比，很难发现二者的差别。

鲁棒性：图像中的水印经过变换操作（如加入噪声、滤波、有损压缩、重采样、D/A 或 A/D 转换等）后，不会丢失水印信息，仍然可以清晰地提取。

安全性：数字水印应能抵抗各种攻击，必须能够唯一地标识原始图像的相关信息，任何第三方都不能伪造他人的水印图像。

试题答案：A

试题 19 解析

LSB 算法将信息嵌入到随机选择的图像点中最不重要的像素位上，这可保证嵌入的水印是不可见的。

试题答案：B

试题 20 解析

Patchwork 算法利用像素的统计特征将信息嵌入像素的亮度值中。该算法先对图像分块，再对

每个图像块进行嵌入操作，可以加入更多信息。

试题答案：A

试题 21 解析

拒绝服务攻击（Denial of Service，DoS），即攻击者想办法让目标机器停止提供服务或资源访问。TCP SYN Flooding 建立大量处于半连接状态的 TCP 连接就是一种使用 SYN 分组的 DoS 攻击。

试题答案：B

试题 22 解析

蠕虫病毒的前缀是 Worm。

试题答案：A

试题 23 解析

Macro.Melissa 是一种宏病毒，主要感染 Office 文件。

试题答案：（23）D　（24）B

试题 24 解析

《中华人民共和国网络安全法》规定如下：

第二十一条　采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。

试题答案：C

试题 25 解析

《信息安全等级保护管理办法》规定如下：

第二十七条　涉密信息系统建设使用单位应当依据涉密信息系统分级保护管理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。

试题答案：C

试题 26 解析

《中华人民共和国刑法》（2015 修正）对计算机犯罪的规定如下：

第二百八十五条　【非法侵入计算机信息系统罪】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，处三年以下有期徒刑或者拘役。

试题答案：B

试题 27 解析

依据《信息安全等级保护管理办法》第七条，信息系统的安全保护等级分为五级。

试题答案：D

试题 28 解析

依据《信息安全等级保护管理办法》：

第七条　信息系统的安全保护等级分为五级，其中：

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对

社会秩序和公共利益造成损害，但不损害国家安全。

试题答案：A

试题 29 解析

依据《信息安全等级保护管理办法》

第八条　信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级，信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级，信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

试题答案：B

试题 30 解析

整体性原则是应用系统工程的观点、方法，分析网络系统安全防护、监测和应急恢复。这一原则要求在进行安全规划设计时充分考虑各种安全配套措施的整体一致性，不要顾此失彼。

试题答案：B

试题 31 解析

最小特权管理一方面给予主体“必不可少”的权力，确保主体能在所赋予的特权之下完成任务或操作；另一方面，给予主体“必不可少”的特权，限制了主体的操作。这样可以确保可能的事故、错误、遭遇篡改等原因造成的损失最小。

试题答案：A

试题 32 解析

标准的电子邮件协议使用 SMTP、POP3 或者 IMAP。这些协议都是不能加密的。而安全的电子邮件协议使用 PGP 加密。

试题答案：A

试题 33 解析

数字签名的作用是确保 A 发送给 B 的信息就是 A 本人发送的，并且没有改动。

（1）A 使用“摘要”算法（SHA-1、MD5 等）对发送信息进行摘要。

（2）使用 A 的私钥对消息摘要进行加密运算。加密摘要和原文一并发给 B。

验证签名的基本过程则如下：

（1）B 接收到加密摘要和原文后，使用和 A 同样的“摘要”算法对原文再次摘要，生成新摘要。

（2）使用 A 公钥对加密摘要解密，还原成原摘要。

（3）两个摘要对比，一致则说明由 A 发出并且没有经过任何篡改。

由此可见，数字签名功能有信息身份认证、信息完整性检查、信息发送不可否认性，但不提供原文信息加密，不能保证对方能收到消息，也不对接收方身份进行验证。

所以 E_B（$D_A(P)$）是网上传送的报文，即 A 私钥加密的原文，被 B 公钥加密后传输到网上。

$D_A(P)$是被 A 私钥加密的信息，不可能被第三方篡改，所以可以看作 A 身份证明。

试题答案：（34）C　（35）B

试题 34 解析

在 X.509 标准中，包含在数字证书中的数据域有证书、版本号、序列号（唯一标识每一个 CA 下发的证书）、算法标识、颁发者、有效期、有效起始日期、有效终止日期、使用者、使用者公钥信息、公钥算法、公钥、颁发者唯一标识、使用者唯一标识、扩展、证书签名算法、证书签名（发证机构即 CA 对用户证书的签名）。

试题答案：D

试题 35 解析

用户登录该网站时，通过验证 CA 的签名，可确认该数字证书的有效性，从而验证该网站的真伪。

试题答案：（37）A　（38）D

试题 36 解析

任何木马程序成功入侵到主机后都要和攻击者进行通信。计算机感染特洛伊木马后的典型现象就是有未知程序试图建立网络连接。

试题答案：B

试题 37 解析

单位因为工作的要求往往需要群发邮件，因此向多个邮箱群发同一封电子邮件，一般不认为是网络攻击。

试题答案：C

试题 38 解析

窃取是攻击者绕过系统的保密措施得到可用的信息。DDos 就是用分布式的方法，用多台机器进行拒绝服务攻击，从而使服务器变得不可用。

试题答案：（41）B　（42）A

试题 39 解析

在 A 类地址中，10.0.0.0 到 10.255.255.255 是私有地址。

在 B 类地址中，172.16.0.0 到 172.31.255.255 是私有地址。

在 C 类地址中，192.168.0.0 到 192.168.255.255 是私有地址。

试题答案：B

试题 40 解析

Internet 控制报文协议（ICMP）是 TCP/IP 协议簇的一个子协议，是网络层协议，用于 IP 主机和路由器之间传递控制消息。ICMP 报文是封装在 IP 数据报内传输的。

试题答案：（44）B　（45）D

试题 41 解析

地址解析协议（ARP）是将 32 位的 IP 地址解析成 48 位的以太网地址；而反向地址解析（RARP）则是将 48 位的以太网地址解析成 32 位的 IP 地址。ARP 报文封装在以太网帧中进行发送。

请求主机以广播方式发出 ARP 请求分组。ARP 请求分组主要由主机本身的 IP 地址、MAC 地址以及需要解析的 IP 地址三个部分组成。

试题答案：（46）B　（47）B　（48）C

试题 42 解析

TCP 报头包括源端口号、目标端口号、顺序号和校验号等字段；而 UDP 报头不包括顺序号字段。

试题答案：B

试题 43 解析

本地缓存改善了网络中 DNS 服务器的性能，减少反复查询相同域名的时间，提高解析速度，节约出口带宽。这种方式由于没有域名数据库，因此获取解析结果的耗时最短。

试题答案：C

试题 44 解析

在 Kerberos 认证系统中，用户首先向认证服务器 AS 申请初始票据，然后从票据授予服务器 TGS 获得会话密钥。

试题答案：（51）B　（52）C

试题 45 解析

陷门：是在某个系统或某个文件中设置的“机关”，使得当提供特定的输入数据时，允许违反安全策略。

授权侵犯：又称内部威胁，授权用户将其权限用于其他未授权的目的。

旁路控制：攻击者通过各种手段发现本应保密却又暴露出来的一些系统“特征”，利用这些“特征”，攻击者绕过防线守卫者渗入系统内部。

试题答案：D

试题 46 解析

SSL 是解决传输层安全问题的一个主要协议，其设计的初衷是基于 TCP 协议之上提供可靠的端到端安全服务。应用 SSL 协议最广泛的是 HTTPS，它为客户浏览器和 Web 服务器之间交换信息提供安全通信支持。它使用 TCP 的 443 端口发送和接收报文。

试题答案：（54）B　（55）A

试题 47 解析

SSL 是在网络应用层和传输层之间提供加密方案的协议。

试题答案：B

试题 48 解析

主动防御技术是根据特定行为判断程序是否为病毒。

试题答案：C

试题 49 解析

很多系统在登录时都要求用户输入以图片形式显示的一个字符串，可防止非法用户利用程序自动生成密码登录，即用暴力方式破解密码。

试题答案：C

试题 50 解析

IPSec 的加密和认证过程中所使用的密钥由 Internet 密钥交换协议（IKE）机制来生成和分发。

试题答案：B

试题 51 解析

网闸借鉴了船闸的概念，设计上采用“代理+摆渡”方式。摆渡的思想是内外网进行隔离，分时对网闸中的存储进行读写，间接实现信息交换；内外网之间不能建立网络连接，不能通过网络协议互相访问。网闸的代理功能是数据的“拆卸”，把数据还原成原始的部分，拆除各种通信协议添加的“包头包尾”，在内外网之间传递净数据。

网闸的主要实现技术包括实时开关技术、单向连接技术和网络开关技术。

- 实时开关：原理是使用硬件连接两个网络，两个网络之间通过硬件开关来保证不同时**连通**。通过开关的快速切换，并剥去 TCP 报头，通过不可路由的数据转存池来实现数据**转发**。
- 单向连接：数据只能从一个网络单向向另外一个网络摆渡数据，两个网络是完全断开的。单向连接实际上通过硬件实现一条“只读”的单向传输通道来保证安全隔离。
- 网络开关：是将一台机器虚拟成两套设备，通过开关来确保两套设备不连通，同一时刻最多只有一个虚拟机是激活的。

试题答案：（60）C （61）D

试题 52 解析

初级密钥通常采用一次一密的使用形式，在将密钥的明文传输给对方时，需要使用更高级的密钥进行加密。对方接收到加密的初级密钥后，需要将其解密才能使用。

试题答案：（62）A （63）A

试题 53 解析

ECC 规定用户的私钥 d 为一个随机数，取值范围为 0～n-1。公钥 Q 通过 dG 进行计算。

利用 ECC 实现数字签名与利用 RSA 实现数字签名的主要区别是，ECC 签名后的内容中包含原文，而 RSA 签名后的内容中没有原文。

试题答案：（64）A （65）A （66）B

试题 54 解析

S 盒变换是一种压缩替换，通过 S 盒将 48 位输入变为 32 位输出。共有 8 个 S 盒，并行作用。每个 S 盒有 6 个输入，4 个输出，是非线性压缩变换。

试题答案：（67）D （68）A

试题 55 解析

RC4 是 Ron Rivest 为 RSA 设计的序列密码，RC4 算法简单、速度快、容易用软硬件实现，因此应用广泛。出于种种原因，美国政府限制出口超过 40 位密钥的 RC4 算法。

试题答案：D

试题 56 解析

为某些非容易的获取信息，利用社会科学（此指其中的社会常识），尤其心理学、语言学、欺诈学并将其进行综合，有效地利用（如人性的弱点），并最终获得信息为最终目的学科称为“社会工程学”。

信息完全定义的社会工程是使用非计算机手段（如欺骗、欺诈、威胁、恐吓甚至实施物理上的盗窃）得到敏感信息的方法集合。

试题答案：B

试题 57 解析

数字认证是一种证明个人或其他机构**拥有**某一公开密钥的**数字**文件。数字认证用于确定某一给定的公钥是否确实属于某个人或某个机构。数字认证有助于防止有人**假冒**别人的秘钥。形式最简单的数字认证包含一个公钥和一个用户名。通常，数字认证还包括**有效期**，发证机关名称，序列号，也许还包含其他信息。最重要的是，它包含了发证机关的数字**签名**。最普遍公认的数字认证标准是 X.509 国际标准，任何遵循 X.509 的应用程序都能读写遵循 X.509 标准的数字认证。

试题答案：（71）C （72）B （73）A （74）D （75）A

第 7～8 学时 模拟测试点评（下午一）

试题一分析

密码分组链接模式（CBC）可以分为密文链接方式和明密文链接方式。

（1）CBC 的密文链接方式。

密文链接方式中，输入是当前明文组与前一密文组的异或。

CBC 的密文链接方式下：加密会引发错误传播无界，解密引发错误传播有界。CBC 不利于并行计算。

（2）CBC 的明密文链接方式。

明密文链接方式中，输入是前一组密文和前一组明文异或之后，再与当前明文组异或。CBC

的明密文链接方式下：加密和解密均会引发错误传播无界。

试题一答案

【问题1】（10分）

密码体制由以下五个部分组成：

（1）明文空间M：全体明文的集合。

（2）密文空间C：全体密文的集合。

（3）加密算法E：一组明文M到密文C的加密变换。

（4）解密算法D：一组密文C到明文M的加密变换。

（5）密钥空间K：包含加密密钥K_e和解密密钥K_d的全体密钥集合。

【问题2】（3分）

（1）基于因子分解。

（2）基于离散对数。

（3）基于椭圆曲线离散对数。

注：（1）～（3）次序可以变化。

【问题3】（2分）

（4）分组密码。

（5）序列密码。

注：（4）～（5）次序可以变化。

【问题4】（5分）

该加密过程属于CBC的密文链接方式。

CBC的密文链接方式下：加密会引发错误传播无界，解密引发错误传播有界。CBC不利于并行计算。

试题二分析

已知n=35，得到p和q分别为5和7；

计算φ(n) =(p–1)×(q–1)=24

已知公钥e=5，又由于私钥d满足ed=1mod (p–1)×(q–1)，因此d=5

明文$M=C^d \bmod n=10^5 \bmod 35=5$

试题二答案

【问题1】（3分）

选出两个大质数p和q，使得p≠q

计算p×q=n

计算φ(n) =(p–1)×(q–1)

选择e，使得1<e<(p–1)×(q–1)，并且e和(p–1)×(q–1)互为质数

计算解密密钥，使得ed=1 mod (p–1)×(q–1)

公钥=e，n

私钥=d，n

公开n参数，n又称为模

消除原始质数p和q

【问题2】（4分）

设定C为密文，M为明文：

加密：

$C=M^e \bmod n$

解密：

$M=C^d \bmod n$

【问题3】（4分）

设M为明文，M的签名过程为：

签名：$M^d \bmod n$

验证签名：$(M^d)^e \bmod n$

【问题4】（4分）

M=5

试题三分析

C语言程序在内存中分为三个部分：程序段、数据段和堆栈。程序段里存放程序的机器码和只读数据；数据段存放程序中的静态数据；动态数据则通过堆栈来存放。在内存中，它们的位置如下图所示。

内存高位

堆　栈
数 据 段
程 序 段

内存低位

Function()函数将长度为128字节的字符串拷贝到只有16字节的缓冲区中去；而调用strcpy()函数进行字符串拷贝时，没有进行缓冲区越界检查。

下图中可以看到执行function()函数前后的堆栈情况。

程序执行 function()函数完毕时，由于缓冲区溢出，子程序的返回地址被覆盖，变成了0x41414141（AAAA的ASCII码表示，A的ASCII码为0x41）。因此无法执行print("This is a test\n")语句。此时，返回地址已经不正常，也无法预计会执行什么指令。

压入堆栈中 的参数	内存高位	… A …
返回地址		AAAA
少量缓存		… 在此向上共 256 个 A
缓存 16 字节空间	内存低位	16 个 A

执行 strcpy()前　　执行 strcpy()后

试题三答案

【问题 1】（3 分）

不能。（1 分）

代码存在缓冲区溢出错误。（2 分）

【问题 2】（4 分）

（1）function()函数将长度为 128 字节的字符串拷贝到只有 16 字节的缓冲区中去。（2 分）

（2）strcpy()函数进行字符串拷贝时，没有进行缓冲区越界检查。（2 分）

【问题 3】（3 分）

防范缓冲溢出的策略有：

- 系统管理防范策略：关闭不必要的特权程序、及时打好系统补丁。（1 分）
- 软件开发的防范策略：正确编写代码、缓冲区不可执行、改写 C 语言函数库、程序指针完整性检查、堆栈向高地址方向增长等。（2 分）

试题四分析

Fixup 命令可以启用或者禁止特定的服务、协议。

题干出现的 PIX 配置语句含义解释如下：

```
PIX#show config
…
nameif eth0 outside security 0          //eth0 接口命名为 outside，安全级别设置为 0
nameif eth1 inside security 100         //eth1 接口命名为 inside，安全级别设置为 100
nameif eth2 dmz security 40             //eth2 接口命名为 dmz，安全级别设置为 40
…
fixup protocol ftp 21                   //启动 FTP 协议，允许 21 端口的数据通过
fixup protocol http 80                  //启动 HTTP 协议，允许 80 端口的数据通过
…
```



```
ip address outside 61.144.51.42   255.255.255.248     //配置 outside 接口 IP 地址与掩码
ip address inside 192.168.0.1     255.255.255.0       //配置 inside 接口 IP 地址与掩码
ip address dmz 10.10.0.1    255.255.255.0             //配置 dmz 接口 IP 地址与掩码
…
global（outside）1 61.144.51.46
//经 outside 接口去外网的数据，地址转换为 61.144.51.46，全局地址池标志为 1，所以由 inside 域发往 Internet 的 IP 分组，在到达路由器 R1 时的源 IP 地址是 61.144.51.46
nat（inside）1 0.0.0.0   0.0.0.0
//所有地址按地址池 1 定义进行地址转换
…
route outside 0.0.0.0 0.0.0.0 61.144.51.45 1          //设定默认路由，所有数据通过 61.144.51.45 转发
```

使用 static 命令配置静态地址映射，使得内外部地址一一对应。

```
Firewall（config）#static（internal_interface_name，external_interface_name）outside_ip_address inside_ip_address
其中 internal_ interface _name 表示内部网络接口，安全级别较高，如 inside；
external_ interface _name 表示外部网络接口，安全级别较低，如 outside；
outside_ip_address 表示共有 IP 地址；inside_ip_address 表示被转换的 IP 地址。
```

如果需要 dmz 域的服务器（IP 地址为 10.10.0.100）对 Internet 用户提供 Web 服务（对外公开 IP 地址为 61.144.51.43），就需要完成两步工作：

①将 10.10.0.100 和 61.144.51.43 建立映射关系。

```
PIX（config）#static（dmz,outside）61.144.51.43 10.10.0.100 可以完成这种映射。
```

②防火墙上放开外网地址 61.144.51.43 的 80 端口。

```
PIX（config）#conduit permit tcp host 61.144.51.43 eq www any 可以完成端口放开的任务。
```

试题四答案

【问题 1】（4 分）

（1）启用 FTP 服务　　（2 分）

（2）设置 eth0 口的默认路由，指向 61.144.51.45，且跳步数为 1（2 分）

【问题 2】（6 分）

（3）192.168.0.1　　（1.5 分）

（4）255.255.255.248　　（1.5 分）

（5）eth2　　（1.5 分）

（6）10.10.0.1　　（1.5 分）

【问题 3】（2 分）

（7）61.144.51.46

【问题 4】（3 分）

（8）61.144.51.43　　（1 分）

（9）10.10.0.100　　（1 分）

（10）61.144.51.43　　（1 分）

试题五分析

【问题1】(3分，各1分)

表　常见的隧道协议

协议层次	实例
数据链路层	L2TP、PPTP、L2F
网络层	IPSec
传输层与应用层之间	SSL

【问题2】(3分，各1分)

IPSec安全体系结构包括AH、ESP和ISA KMP/Oakley等协议。其中，AH为IP包提供信息源验证和报文完整性验证，但不支持加密服务；ESP提供加密服务；ISA KMP/Oakley提供密钥管理服务。

【问题3】(6分，各2分)

“筛选器 属性”界面配置源子网IP地址（内网地址）和目的子网IP地址（内网地址）。

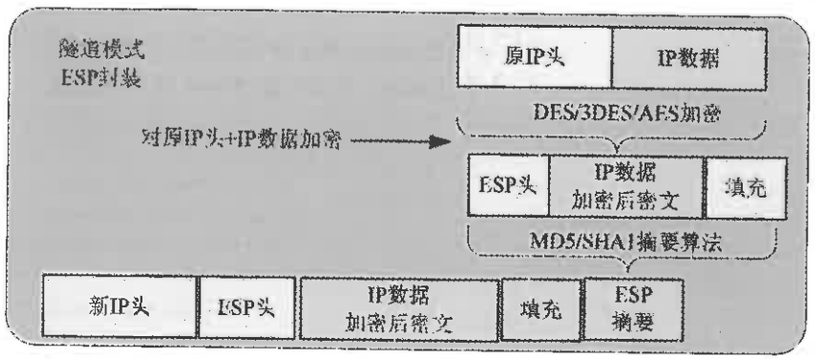
针对Server A，源子网IP地址（内网地址）为192.168.1.2/32，所以“筛选器 属性”界面源子网IP地址应设为**192.168.1.0**；目的子网IP地址（内网地址）为192.168.1.2/32，所以“筛选器 属性”界面目标子网IP地址应设为**192.168.2.0**。

“编辑规则 属性”界面的隧道地址应该配置隧道对端（公网地址）。

针对Server A隧道对端（公网地址）为202.113.111.1，所以隧道设置中的隧道终点IP地址应设为**202.113.111.1**。

【问题4】(3分，各1分)

本题要求“加密并保持完整性”，由于AH协议不支持加密，因此采用ESP封装。前面题目给出了总公司与子公司通信建立了隧道，因此采用隧道模式。具体如下图所示。



这里IP数据加密后，密文可以看作旧IP头，ESP摘要可以看作ESP尾。

试题五答案

【问题1】(3分，各1分)

(1) PPTP

(2) L2TP（1、2顺序可调换）

(3) IPSec

【问题2】(3分，各1分)

(4) AH

(5) ESP

(6) ISA KMP/Oakley

【问题3】(6分，各2分)

(7) 192.168.1.0

(8) 192.168.2.0

(9) 202.113.111.1

【问题4】(3分，各1分)

(10) B或ESP头

(11) C或旧IP头

(12) F或ESP尾