1、ping 命令

检测网络的连通性和可到达性。

ping命令功能是通过发送ICMP包来检验与另一台TCP/IP主机的IP级连接情况。网管员常用这个命令检测网络的连通性和可到达性。同时，应答消息的接收情况将和往返过程的次数一起显示出来。

（1）如果只使用不带参数的ping命令，窗口将会显示命令及其各种参数使用的帮助信息。

（2）使用ping命令的语法格式是：ping 对方计算机名或者IP地址

2、网络安全管理技术概念

网络安全管理技术是实现网络安全管理和维护的技术，需要利用多种网络安全技术和设备，对网络系统进行安全、合理、有效和高效的管理和维护。

网络安全管理技术一般需要实施一个基于多层次安全防护的策略和管理协议，将网络访问控制、入侵检测、病毒检测和网络流量管理等安全技术应用于内网，进行统一的管理和控制，各种安全技术彼此补充、相互配合，对网络行为进行检测和控制，形成一个安全策略集中管理、安全检查机制分散布置的分布式安全防护体系结构，实现对内网进行安全保护和管理。

监控和审计是

与网络管理密切相关的技术。监控和审计是通过对网络通信过程中可疑、有害信息或行为进行记录为事后处理提供依据，从而对黑客形成一个强有力的威慑和最终达到提高网络整体安全性的目的。

3、如何实现主机网络安全防护功能?

采用主机网络安全技术.

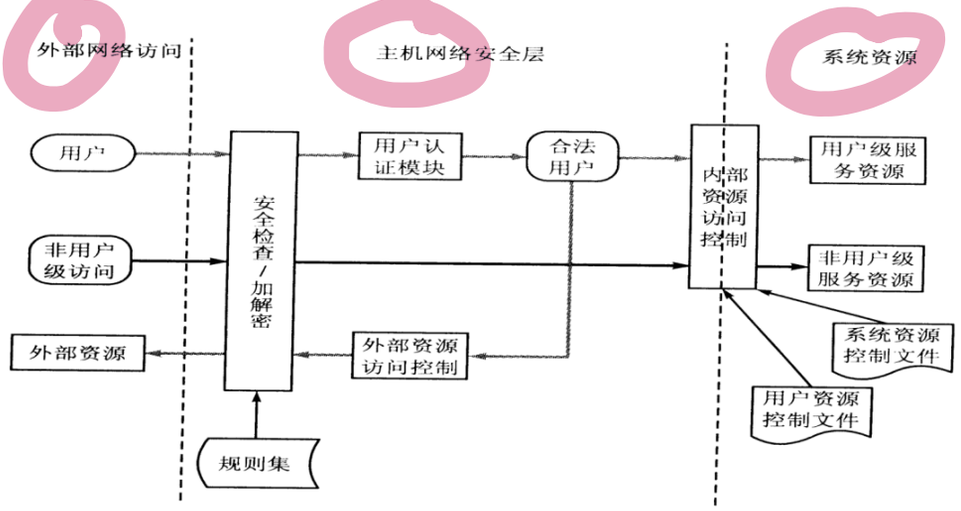
主机网络安全技术是一种主动防御的安全技术，它结合网络访问的网络特性和操作系统特性来设置安全策略，用户可以根据网络访问的访问者及访问发生的时间、地点和行为来决定是否允许访问继续进行，以使同一用户在不同场所拥有不同的权限，从而保证合法用户的权限不被非法侵占。主机网络安全技术考虑的元素有IP地址、端口号、协议、MAC地址等网络特性和用户、资源权限以及访问时间等操作系统特性，并通过对这些特性的综合考虑，来达到用户网络访问的细粒度控制。

与网络安全采用安全防火墙、安全路由器等在被保护主机之外的技术手段不同，主机网络安全所采用的技术手段通常在被保护的主机内实现，并且一般为软件形式。因为只有在被保护主机之上运行的软件，才能同时获得外部访问的网络特性以及所访问资源的操作系统特性。

应用最为广泛的此类产品有Wietse Venema 开发的共享软件TCP Wrapper。TCP Wrapper是一种对进入的网络服务请求进行监视与过滤的工具，可以截获Systat、Finger、FTP、Telnet、Rlogin、RSH、Exec、TFTP、Talk等网络服务请求，并根据系统管理员设置的服务的访问策略来禁止或允许服务请求。

主机网络安全系统是为了解决主机安全性与访问方便性之间的矛盾，将用户访问时表现的网络特性和操作系统特性进行综合考虑，因此，这样的系统必须建立在被保护的主机上，并且贯穿于网络体系结构中的应用层、传输层、网络层之中。在不同的层次中，可以实现不同的安全策略。

更复杂的设计可以在更多的层实现更多的安全功能，下面就前面的设想提出一个可行的主机网络安全系统的结构模型，如图所示。



4、密码破解攻防

1)密码攻防的方法

一般密码攻击有3种方法:

(1) 通过网络监听非法得到用户密码

(2) 密码破解

(3) 放置木马程序

2) 密码攻防对策

通常保持密码安全的要点:

(1) 要将密码写下来，以免遗失；

(2) 不要将密码保存在电脑文件中；

(3) 不要选取显而易见的信息做密码；

(4) 不要让他人知道；

(5) 不要在不同系统中使用同一密码；

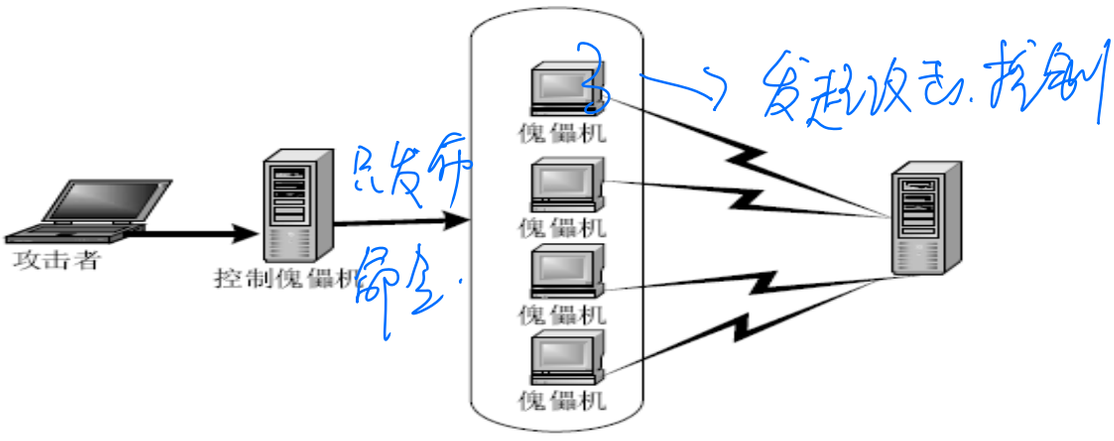
(6) 在输入密码时应确认身边无人或其他人在1米线外看不到输入密码的地方；

(7) 定期改变密码，至少2 —5个月改变一次。

5、以SYN FlooD攻击为例，分析分布式拒绝服务攻击运行的原理是什么?

1) 攻击运行原理

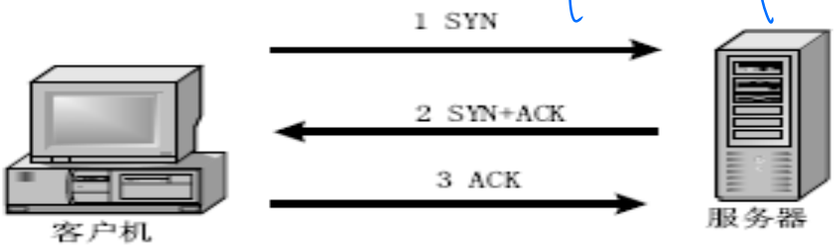
如图所示，一个比较完善的DDoS 攻击体系分成4 大部分，最重要的第2 和第3 部分，它们分别用做控制和实际发起攻击;对第4 部分的受害者来说，DDoS的实际攻击包是从第3部分攻击傀儡机上发出的，第2部分的控制机只发布命令而不参与实际的攻击。



2) DDoS 攻击实例 — —目前最流行的DDoS 攻击手段SYN Flood 攻击

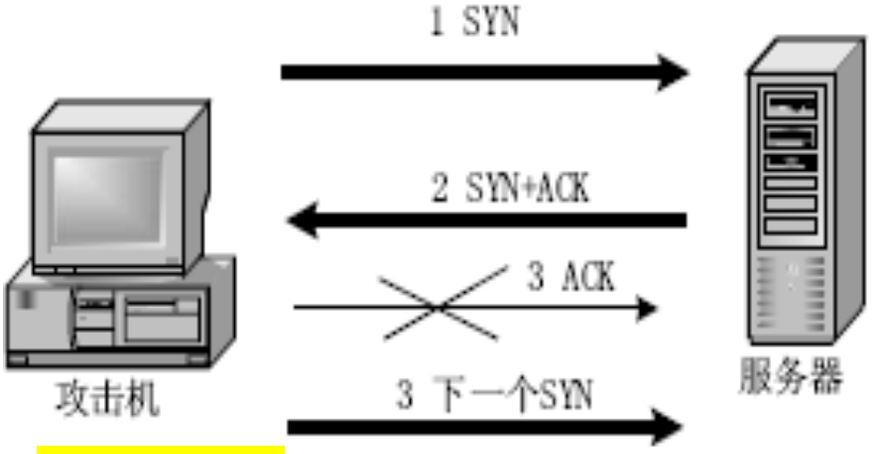
1) Syn Flood 原理与三次握手

Syn Flood 利用了TCP/IP协议的固有漏洞。面向连接的TCP 三次握手是Syn Flood 存在的基础。TCP 连接的三次握手过程，如图所示。



TCP三次握手过程中，在第一步，客户端向服务端提出连接请求。服务端收到该TCP 分段后，在第二步以自己的ISN 回应(SYN 标志置位)，同时确认收到客户端的第一个TCP 分段(ACK 标志置位)。在第三步中，客户端确认收到服务端的ISN(ACK标志置位)。到此为止建立完整的TCP 连接，开始全双工模式的数据传输过程。

2) Syn Flood 攻击者不会完成三次握手。如图所示。



6、数字签名与对签名的验证实现过程

数字签名的全过程分两大部分，即签名与验证。

数字签名过程

分两部分：左侧为签名过程，右侧为验证过程。即发方将原文用哈希算法求得数字摘要，用签名私钥对数字摘要加密求得数字签名，然后将原文与数字签名一起发送给收方；收方验证签名，即用发方公钥解密数字签名，得出数字摘要；收方将原文采用同样哈希算法又得一新的数字摘要，将两个数字摘要进行比较，如果两者匹配，说明经数字签名的电子文件传输成功。如图5-5 所示。

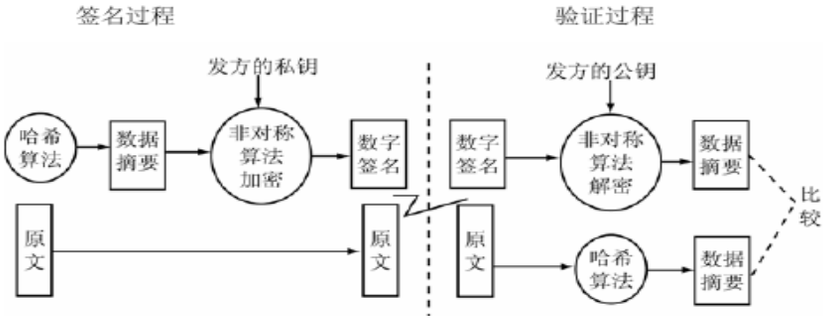


图5-5 数字签名原理

7、试述访问控制的安全策略以及实施原则?

1. 基于身份的规则的安全策略

建立基于身份安全策略和基于规则安全策略的基础是授权行为。

(1)

基于身份的安全策略是过滤对数据或资源的访问，只有能通过认证的那些主体才有可能正常使用客体的资源。基于身份的安全策略包括基于个人的策略和基于组的策略，主要有两种基本的实现方法，分别为能力表和访问控制表。

基于个人的策略。基于个人的策略是指以用户个人为中心建立的一种策略，由一些列表组成。这些列表针对特定的客体，限定了哪些用户可以实现何种安全策略的操作行为。

基于组的策略。基于组的策略是基于个人的策略的扩充，指一些用户被允许使用同样的访问控制规则访问同样的客体。

(2) 基于规则的安全策略

基于规则的安全策略中的授权通常依赖于敏感性。在一个安全系统中，数据或资源应该标注安全标记。代表用户进行活动的进程可以得到与其原发者相应的安全标记。在实现上，由系统通过比较用户的安全级别和客体资源的安全级别来判断是否允许用户进行访问。

8、安全策略实施原则

安全策略实施原则：访问控制安全策略的实施原则围绕主体、客体和安全控制规则集三者之间的关系展开。

(1)

最小特权原则。是指主体执行操作时，按照主体所需权利的最小化原则分配给主体权力。最小特权原则的优点是最大限度地限制了主体实施授权行为，可以避

免来自突发事件、错误和未授权主体的危险。也就是说，为了达到一定目的，主体必须执行一定操作，但他只能做他所被允许做的，其他除外。

(2) 最小泄漏原则。是指主体执行任务时，按照主体所需要知道的信息最小化的原则分配给主体权力。

(3)

多级安全策略。是指主体和客体间的数据流向和权限控制按照安全级别的绝密（TS）、秘密（S）、机密（C）、限制（RS）和无级别（U）5级来划分。多级安全策略的优点是避免敏感信息的扩散。具有安全级别的信息资源，只有安全级别比它高的主体才能够访问。

9、简述安全审计的目的和类型?

目的和意义在于：

(1) 对潜在的攻击者起到重大震慑和警告的作用；

(2) 测试系统的控制是否恰当，以便于进行调整，保证与既定安全策略和操作能够协调一致。

(3) 对于已经发生的系统破坏行为，作出损害评估并提供有效的灾难恢复依据和追究责任的证据；

(4) 对系统控制、安全策略与规程中特定的改变作出评价和反馈，便于修订决策和部署。

(5) 为系统管理员提供有价值的系统使用日志，帮助系统管理员及时发现系统入侵行为或潜在的系统漏洞。

10、试述DES算法的加密过程?

DES是一种专为二进制编码数据设计的、典型的按分组方式工作的单钥密码算法。**基本原理**是将二进制序列的明文分组，然后用密钥对这些明文进行替代和置换，最后形成密文。DES算法是对称的，既可用于加密又可用于解密。密钥输入顺序和加解密步骤完全相同，从而在制作DES芯片时很容易达到标准化和通用化，很适合现代通信。

DES采用64位长的密钥，包括8个校验位，密钥长度为56位，可将原文的多个64位块变换成加密的多个64位代码块。**原理**是将原文经过一系列的排列与置换所产生的结果再与原文异或合并。该加密过程重复16次，每次所用的密钥位排列不同。即使按照目前的标准，采用该方法的加密结果也相当安全。然而，任何安全都是相对的。

11. 密码分析

密码分析就是在不知道密钥的情况下，利用数学方法破译密文或找到秘密密钥。

(1)

已知明文的破译方法：密码分析员可以通过一段明文和密文的对应关系，经过分析发现加密的密钥。所以，过时或常用加密的明文、密文和密钥，仍然具有被利用的危险性。

(2) 选定明文的破译方法：密码分析员可以设法让对手加密一段选定的明文，并获得加密后的结果，经过分析也可以确定加密的密钥。

12、如何进行简单的变位加密？已知明文是“来宾已出现住在人民路”，密钥是：4168257390，则加密后，密文是什么？

简单的变位加密：首先选择一个用数字表示的密钥，写成一行，然后把明文逐行写在数字下。按密钥中数字指示的顺序，逐列将原文抄写下来，即为加密后的密文。

密钥：4 1 6 8 2 5 7 3 9 0

明文：来 宾 已 出 现 住 在 人 民 路

0 1 2 3 4 5 6 7 8 9

密文：路 宾 现 人 来 住 已 在 出 民

13、已知明文是“One World One Dream”，按行排在矩阵中，置换f=[1,2,3,4 / 3,4,2,1]，用矩阵变位加密方法后，密文是什么？

矩阵变位密码是把明文中的字母按给定的顺序排列在一个矩阵中，然后用另一种顺序选出矩阵的字母来产生密文。

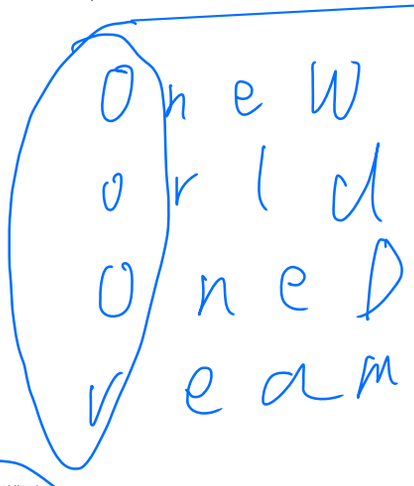
按照置换f中第1行的顺序将明文安排在一矩阵中：

O n e W

o r l d

O n e D

r e a m



按照置换f中第2行的顺序2413将上述矩阵中的各行重新排列：

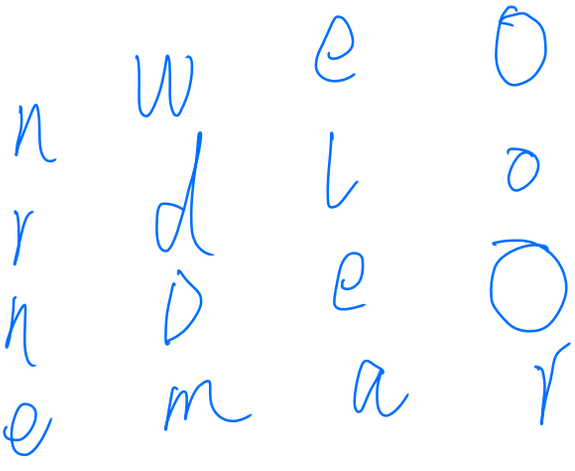
n W O e

r d o l

n D O e

e m r a

则密文是：**nWOerdolnDOeem**ra



书上P127 加密5-10

请补充表4.1中的内容（1）和（2），并根据上述规则表给出该企业对应的安全需求。 【问题2】 （4分）

一般来说，安全规则无法覆盖所有的网络流量。因此防火墙都有一条缺省（默认）规则，该规则能覆盖事先无法预料的网络流量。请问缺省规则的两种选择是什么?

【问题3】 （6分）

请给出防火墙规则中的三种数据包处理方式。

【问题4】 （4分）

防火墙的目的是实施访问控制和加强站点安全策略，其访问控制包含四个方面的内 容：服务控制、方向控制、用户控制和行为控制。请问表4.1中，规则A涉及访问控制的哪几个方面的内容?

信管网2019年信息安全工程师案例分析真题试题四参考答案

【问题1】

（1）53 （2）Drop

企业对应的安全需求有:

（1）允许内部用户访问外部网络的网页服务器;

（2）允许外部用户访问内部网络的网页服务器（202.114.64.125）；

（3）除1和2外，禁止其他任何网络流量通过防火墙。

【问题2】

两种缺省选择是，默认拒绝或者默认允许。

【问题3】

Accept、Reject、Drop

【问题4】

服务控制、方向控制和用户控制。