第九章 单元测试题及参考答案

一、选择题

1.数据(　)服务可以保证信息流、单个信息或信息中指定的字段，保证接收方所接收的信息与发送方所发送的信息是一致的。（B）

A.认证　　B.完整性　　C.加密　　D.访问控制

2.在可信计算机系统评估准则中，计算机系统安全等级要求最高的是（ ）级。（D）

A.D　　B.C1　　C.B1　　D.A1

3.当网络安全遭到破坏时，通常要采取相应的行动方案。如果发现非法入侵者可能对网络资源造成严重的破坏时，网络管理员应采取。（C）

A.跟踪方式　　B.修改密码　　C.保护方式　　D.修改访问权限

4.入侵检测系统 IDS 是对的恶意使用行为进行识别的系统。（A）

Ⅰ.计算机Ⅱ.网络资源 III.用户口令Ⅳ.用户密码

A.Ⅰ、Ⅱ　　B.Ⅰ、III　　C.Ⅰ、III 与Ⅳ

D.III 与Ⅳ

5.入侵检测系统 IDS 需要分析的数据称为事件，它可以是网络中的数据包，也可以是从系统日志得到的信息，也可能是经过协议解析的。（C）

A.用户信息　　B.应用层协议　　C.数据包

D.资源使用记录

6.网络病毒感染的途径可以有很多种，但是最容易被人们忽视，并且发生得最多的是(　)。（D）

A.操作系统　　B.软件商演示软件

C.系统维护盘　　D.网络传播

二、计算与问答题

1.VPN的隧道协议主要有哪些？

答：

VPN 隧道协议在 TCP/IP 协议栈中的层次目前主要有两类隧道协议：

（1）第二层隧道协议：把各种网络层协议(如 IP、IPX 和 AppleTalk 等)封装到数据链路层的点到点协议(PPP)帧里，再把整个 PPP 帧装入隧道协议里。主要使用的第二层隧道协议有：点对点隧道协议 PPTP、第二层转发协议 L2F、第二层隧道协议 L2TP。

（2）第三层隧道协议：主要有 IP 层安全协议(IPSec，IP Security)、移动 IP 协议和虚拟隧道协议(VTP，Virtual Tunnel Protocol)。

2.什么是消息摘要算法？什么是消息认证码？消息摘要和消息认证码的主要区别是什么？

答：报文鉴别分为报文的完整性鉴别和报文的来源鉴别，其中报文的完整性鉴别一般通过消息摘要 MD（Message Digest）算法来验证，消息摘要算法也被称为消息摘要函数、哈希函数、散列函数或杂凑函数。

报文的来源鉴别可以使用消息认证码 MAC(Message Authentication Code)，MAC 是消息和密钥的函数，可以看作是带密钥的消息摘要函数。

3.网络安全协议主要有哪些？

答：

为了解决 TCP/IP 协议簇的安全性问题，弥补 TCP/IP 协议簇在设计之初对安全功能的考虑不足，IETF 等相关组织不断地改进现有协议并设计了新的安全通信协议，形成了由各层安全通信协议构成的 TCP/IP 协议簇的安全架构，具体如下表所示。

应用层	S-HTTP，SSH，SSL-Telnet，SSL-SMTP，SSL-POP3，PET，PEM，S/MIME，PGP
传输层	SSL，TLS,SOCKS v5
网络层	IPSec
网络接口层	PPTP，L2TP，L2F

4.数据包过滤型防火墙和应用代理防火墙的各自的优缺点是什么？

答：

包过滤防火墙具有如下的特点：

（1）实现容易；

（2）数据吞吐率较高；

（3）易配置；

（4）对应用完全透明；

（5）对会话内容无法监控，安全性能较低。

应用代理防火墙具有如下的特点：

（1）可以对应用层数据进行处理；

（2）对数据包的检测能力比较强；

（3）双向通信必须经过应用代理，禁止 IP 转发；

（4）难于配置；

（5）处理速度慢。