**第二套试卷答案**

1. 填空题
2. 安全服务、安全机制、安全管理
3. 密钥分发困难、密钥管理困难、无法源认证
4. 扫描、嗅探
5. 非军事化区
6. VPN
7. 选择题

A、B、D、C、A、C、D、B、B、C

三.判断题

对错错错错对对对错错

四．简答题

第一题：.

1.网络安全：本质上就是网络上信息的安全，指网络系统的硬件，软件及其系统中的数据安全。

2.四大特征：保密性，完整性，可用性，可控性。

第二题：

1.便于管理。网络中的每一个用户只需要保护自己的私钥，则N个用户仅需产生N对密钥。

2.密钥分配简单。不需要秘密的通道和复杂的协议来传送密钥。公钥可基于公开的渠道分发给其他用户，而私钥则由用户自己保管。

3.可以实现数字签名。

第三题：

设计目标：1. 安全性。 2. 可靠性。 3. 对用户透明性。 4. 可伸缩。

四个基本实体：1. Kerberos客户机。 2. 认证服务器。 3. 票据许可服务器。 4. 应用服务器。

第四题：

1.初始化：注册、密钥对产生、提交申请、审核检查、证书签发、密钥备份

2.颁发：证书检索、证书验证、证书存储、密钥恢复、密钥更新

第五题：

1.攻击者向要测试的端口发送一个SYN探测包

2.若收到目标端口的SYN/ACK数据包表示端口开放；

若收到目标端口的RST/ACK数据包表示端口关闭

3.攻击者向目标端口发送RST数据包，重置TCP链接，防止对方记录

第六题：

1.防火墙不能防范不经防火墙的攻击

2.防火墙不能防范来自内部网络的攻击

3.防火墙不能防范感染了病毒的软件和文件传输

4.防火墙不能防范利用目标网络协议中的缺陷进行攻击

5.防火墙不能防范利用服务器系统漏洞进行攻击

6.防火请不能防范新的网络安全问题

7.防火墙限制了有用的网络服务

以上任写5点即可

五.综合题

第一题:

1.确保所有服务器采用最新的系统,并打上安全补丁

2.删除多余的网络服务,从而减少网络协议的漏洞

3.设置防火墙,过滤掉所有可能伪造的数据包

4.确保从服务器相应的目录或文件数据库中删除未使用的服务

5.禁止内部网络通过Modern连接至PSTN系统

6.禁止使用网络访问程序

7.限制在防火墙外与网络文件共享

8.在防火墙上运行端口映射程序或端口扫描程序

9.检查所有网络设备、主机和服务器系统的日志

10.确保管理人员对所有主机进行检查

第二题：

甲与异地公司搭建Host对Host的VPN。要求通信双方的

所有主机均支持IPsec协议，两个异地VPN的网关必须支

IPsec协议。对视频数据经过IPsec协议处理，这样所有的

通信链路都是安全的。

第三题：我在此简述：甲监听乙的交易数字货币B，提交同类币B，且提高GAS费用给矿工，提前交易，等乙交易完成后，再交易把B换成A