56、Windows 通过什么实现访问控制，如何实行访问控制？

答：通过访问令牌和安全描述符实现，账户登录时，LSA 读取用户信息，用这些信息生成访问令牌，相当于票证。该账户启动的进程都会获得令牌的一个副本。当用户试图访问系统资源时，提供令牌副本给 SRM，SRM 会检查访问对象的访问控制列表的访问控制项（ACE）决定是否访问资源。

【注：需要账务 Windows 安全管理的结构特点和访问控制的原理，涉及哪些结构模块。各个模块的功能是什么。】

57、简述 Windows 系统安全认证原理（及优点）

答：①、用户用 winlogon 输入用户名与口令，口令被散列；②、主域控制器取用户口令散列，产生 8 字节质询，发给客户端，同时用用户散列对质询散列。③、客户端用口令散列对质询散列进行响应。④、控制器对比两个质询散列，完成认证。优点：无需网络传输口令及口令散列，保证口令安全。

【注：2019 年 837 试题中，最后一题是设计一个医院的安全认证登录模块。与此处 Windows 系统安全认证本质上是相通。真题的设计题主体可以使用 Windows 安全认证来进行解答，无非是增加一些 SSL 安全协议保证信道安全，使用什么作为登录用户名密码，使用什么加密算法之类的额外知识点。我一再强调大家要培养一个使用书本中的原理完成设计题的解题思路，应试过程中，不太可能有时间想出一个完备、安全的设计。这时候就需要与已知的设计相互参考、比对特点。在已知的设计之上加以修改完成设计题的解答。同理，2018 年 837 试题中的设计题，让你设计某一个系统的访问控制列表，使用相关知识点即可作答。这就要求你对于这些原理的深刻理解，加以应用。】

58、IPv4 存在的缺陷体现在哪些方面？

答：1、IPv4 对 IP 地址不进行认证，缺乏对用户身份的认证，该缺陷容易造成 MAC 欺骗，ARP 欺骗，IP 欺骗，DNS 欺骗等。2、缺乏对承载数据的加密保护，易造成窃听，篡改等数据报操作。3、IP 地址过少不能满足现实需要。4、缺乏防重放攻击措施。

59、由 ESP 协议的报文格式，回答以下问题：1）哪个字段用于防范重放攻击，原理是什么？2）安全参数索引 SPI 的作用？3）哪部分以密文的形式出现？4）简述“认证数据”是如何计算出来的？

答：（1）ESP 使用序列号和抗重放窗口防重放攻击。（具体见抗重放窗口原理）（2）SPI 作用于标识协议所对应的安全关联 SA，协议根据 SPI 在 SPD 与 SAD 中查找相应的安全关联参数与安全策略。（3）ESP 的载荷数据，ESP 尾（载荷长度、下一个头）以密文形式。(4) ESP 将 ESP 头与密文数据一起认证，主要使用基于密钥的 HASH 散列算法(HMAC)进行散列，然后截取前 32 的整数倍字节（通常为 96 位）作为认证数据。

60、AH 与 NAT 会发生冲突吗？为什么？ESP 呢？

答：AH 会发生冲突，无论是传输模式还是隧道模式，AH 都要对整个数据包进行认证，这样经过 NAR 设备后，修改了 IP 地址等信息，IPSec 认为此数据报完整性遭到破坏，从而丢弃。ESP 在传输模式下保护 TCP/UDP，不保护 IP 头，修改 IP 地址不会破坏整个数据包的完整性。但是如果数据报是 UDP 或 TCP，NAT 设备需要修改包的校验值，而校验值被 ESP 保护。所以只有在隧道模式下的 ESP 才能穿过 NAT 设备而不起冲突。

【注：上面三题均出自哈工大信息安全导论期末试题，可见安全协议是重点，主要有 IPSec、SSL 协议，SET 使用的技术，请重点掌握。2019 年考察这部分内容较少。】

61、简述野蛮模式的协商过程，验证载荷是什么？

答：①、发送方发送安全参数，DH 公开值，加密、散列算法、身份认证信息等。②、接收方发回可接受的安全参数、DH 值、身份信息以及验证载荷。③、发送方发送验证载荷给接收方。验证载荷是使用协商得到的安全参数及密钥对接收的信息进行加密散列计算，得到的可验证信息，即为验证载荷。

【注：注意区分 IKE 协商的两种模式，个人认为不太可能考察简答题，可能会出选择填空题，要认清认证者和验证载荷，两种不同协商模式的步骤。】

62、简述维吉尼亚密码、移位密码、乘数密码的原理

答：见书。要分清原理，还要掌握加解密计算。

63、俄语有 32 个字母，设计一个乘数密码来加密，计算潜在的密钥个数。

答：C=m*k mod 32　　gcd(k,32)=1　密钥要求与 32 互素，即 1,3,7,9,11,13,15,17,19,21,23,25,27.

【注：为什么要互素？互素时明文为密文才是一一对应的，不互素时可能出现重复。】

64、（补充）MAC 模型的形式化描述。

答：安全定义类 sc(x) = <L,C>　　x:主、客体　L：安全级别　　C：安全范畴

【注：安全范畴划分实体归属，安全级别是在同一范畴下不同实体级别，两者构成偏序关系 sc(s)>=sc(0)。注意区分二者，只有安全级别能够比较。】

65、DES 中设计的运算有哪些？

答：1、与密钥相关：置换，循环左移；2、基本函数：置换，异或、交换、索引查表。

66、RSA，c=10，e=5，n=35，反求 M

答：n=35=5*7　$\Phi(n)=4*6=24$　$e*d \bmod 24=1 \Rightarrow d=5$　$c^d \bmod 35=M$