29、填空题：在 Windows 中对用户账户安全管理使用了（ ）

答：安全账号管理器 SAM

【注：注意了解 Windows 安全管理，目前没有出过题。】

30、简答题：缓冲区溢出的原理

答：很多程序的函数不能进行有效位检查，攻击者利用这一问题通过往程序缓冲区写入超过其长度的内容，从而破坏程序堆栈，是程序转而执行其他指令。

【注：简答题回答言之有理即可，注意尽量使用专业术语来回答，在答题中体现你具备相应素养。】

31、DES 中密码组件 S 盒在 DES 中的作用。根据 S 盒计算 $S_3(101101)$ 的值。S 盒表如下：

14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7

0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8

4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0

15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13

答：S 盒的作用是将 6 位输入变成 4 位输出，由 101101 的第一位与最后一位合并的二进制数作为行号，即（11）=3，以中间四位为列号（0110）=6，查表 S 盒第三行第 6 位为 2，即输出为 0010

【注：DES 算法要清楚其中 P 盒与 S 盒的区别，迭代次数，密钥长度，子密钥产生原理等问题。这个问题考察某一个盒都会给出其中的转换表。】

31、简述 CBC 模式的加密解密示意图，假设加密时明文一个比特错误，对密文造成什么影响。对接收方解密有什么影响？

答：图见信息安全导论 P28。一个比特明文出错，该组密文发生变化，会影响下一次 DES 加密，导致后面都被影响。对于接收方，该组密文解密不成功，但其他数据块无影响。

【注：四种分组密钥的工作模式要了解清楚，目前没有考察过这部分的内容。一般可能出选择题，填空题，个人认为不太可能出大题。需要知道这四种的加解密模式，误差传递，特点。从误差传递的角度出题，可以间接考察对四种工作模式的加解密过程的理解。两种可能出错的地方，一个是比特明文出错，一个是传输过程中出错。两种出错对不同工作模式造成的影响也是不同的。】

32、简答题：ACL 有什么优缺点？

答：优点：表述直观，配置灵活，授权主体可以赋予或收回权限；缺点：任意传递权限，防护低，组织机构，安全需求变化大时较繁琐，单纯使用 ACL，不易实现最小特权原则

【注：明白三种访问控制各自特点，优缺点。特别是分清 RBAC 中的角色，用户组，权限的概念。】

33、简答题：什么是双重签名，其实现原理是什么？

答：SET 协议中交易核心内容 OI 和 PI，双重签名将两部分内容绑定到一起，确保电子交易的有效性和公正性。双重签名生成 OI 和 PI 摘要，合并之后用私钥签名形成双重签名。

【注：注意专业课考试是大约 9 张正反两面空白卷子。一般来说是完全够写的。而且答题形式不限，只需要清楚地让老师明白你的想法即可。所以，一些原理题目可以使用画图+文字描述的形式答题，这样更清晰，让改卷老师一目了然。】

34、设计题，设计防火墙规则，满足一下条件：

①、Telnet 服务：假设一个网络 116.111.4.0 认为 202。208.5.6 上的服务是不安全的，阻止内网对这个站点的访问。

②、邮件服务：允许 SMTP 出站入站服务。邮件服务器 IP 为 116.111.4.1 。

③、WWW 服务:允许内网访问 Internet 上任何网络或者节点,只允许一个公司的网络 98.120.7.0 访问内部 WWW 服务器（116.111.4.5)。

答:

规则	方向	源地址	目的地址	协议	源端口	目的端口	ACK	动作
1	出	116.114.4.0	202.208.5.6	TCP	>1023	23	任意	拒绝
2	入	202.208.5.6	116.111.4.0	TCP	23	>1023	是	拒绝
3	出	116.111.4.1	任意	TCP	>1023	25	任意	允许
4	入	任意	116.111.4.1	TCP	25	>1023	是	允许
5	入	任意	116.111.4.1	TCP	>1023	25	任意	允许
6	出	116.111.4.1	任意	TCP	25	>1023	任意	允许
7	出	116.111.4.0	任意	TCP	>1023	80	任意	允许
8	入	任意	116.111.4.0	TCP	80	>1023	是	允许
9	入	98.120.7.0	116.111.4.5	TCP	>1023	80	任意	允许

10	出	116.111.4.5	98.120.7.0	TCP	80	>1023	是	允许
11	双向	任意	任意	任意	任意	任意	任意	拒绝

【注：从没考察过这个部分知识点，一般来说是不会考的，但也要注意反套路。】

35、**填空题：**DES **的安全性依赖于（ ）盒，**S **盒完成（ ）功能，**P **盒完成（ ）功能**

答：S、代替、置换

【注：所有其他的运算都是线性的，易于分析，而 S 盒是非线性的，更安全】