36、简述题：简述 ARP 攻击原理

答:、攻击者通过伪造 IP 地址与 MAC 地址的 ARP 相应，产生大量的 ARP 通信使网络阻塞，并持续不断发送伪造的 ARP 响应包，导致代表目标主机的 ARP 缓存中的条目，造成网络中断或中间人攻击。

【注：各种攻击手段，其特点、原理都要十分熟悉，尽量大致能默写出来。】

37、使用 IPtables 实现：（1）禁止别人 ping 自己的主机（2）但可以 ping 外部主机

答:、禁止 ping 请求：iptables -A input -p icmp -s 0/0 --icmp-type 8 -j drop

允许内部请求：iptables -A output -p icmp --icmp-type 8 -j accept

允许回显应答：iptables -A input -p icmp -s 0/0 --icmp-type 0 -j accept

【注:该题已经有点超过考试要求,涉及到 iptables 命令的内容。主要点在于 ping 命令的 icmp-type 上。“8”代表着 icmp 的 echo 请求，“0”代表着 icmp 的 echo 回显应答。这个点在计算机网络中是有要求的。】

38、如果用于 Ua 从 CA1 取得证书，用户 Ub 从 CA2 取得证书，那么 Ua 与 Ub 怎么进行通信？

答：由于证书是不可伪造的，因此 CA 与用户可以将证书放入一个公共目录，当分属不同 CA 的两个用户要安全通信时，需要 CA1 与 CA2 能够安全地交换各自公钥，则 Ua 可以：Ua 可以从公共目录获取由 CA1 签名的 CA2 证书，并验证。

39、假设一个系统采用 PKI 的树状 CA 结构。现在用户 A 想要和用户 B 通信，A 通过信道收到用户 B 的（由 CAx 签名的证书）。如果用户 A 不知道 CAx，用户 A 需要哪些步骤验证他正与用户 B 通信？

答：①、首先用户 A 与 CAx 通信，要求 CAx 提供一个能验证 CAx 公钥的证书。②、假设 CAx 发回一个 CAy 签名的证书，假设用户 A 不知道 CAy，A 将于 CAy 重复上述步骤，直到 A 收到他知道其公钥的 CAr 签名的证书（这里的 CAr 可能是根 CA）。③、然后 A 依次反向验证收到的证书，最后通过验证用户 B 的签名，可以确认他在何用户 B 通信。

【注：PKI 体系的证书链结构对公钥体系与数字证书的现实实践，单纯的数字证书不足以满足现实身份认证需求。所以 PKI 体系中的证书链是比较重要的。需要明白其验证原理，结构特点、CA 证书的生成。特别是其中的签名原理，验证原理。】

40、简述 VPN 如何通过 IPSec 实现端点间的认证和加密服务

答：①、IPSec 过程启动：根据配置的 IPSec 对等实体中的 IPSec 安全策略，指定要被加密的数据流，启动 IKE 交换过程。②、IKE 阶段 1：在该连接阶段，IKE 认证 IPSec，对等实体协商 IKE SA；③、IKE 阶段 2：IKE SA 协商 IPSec SA 的安全关联参数，并在对等实体建立与之匹配的 IPSec SA；④数据传送：IPSec 对等实体根据 SAD 中存储的 IPSec 密钥和参数，相互传送数据。⑤、IPSec 隧道终止：通过删除或者超时结束 IPSec。

【注：此题看似考察的是 VPN，其实原理还是考察 IPSec 的建立过程。要清楚地知道 IPSec 建立过程分为两个阶段，清楚每个阶段又包含哪几种信息交换模式，熟悉几个概念：认证者、验证载荷、SA、SAD、SPD，SA 建立原理。】

41、木马病毒的端口复用和反弹端口原理

答：①、端口复用：将自己的通信端口，直接绑定到正常用户进程端口，将正常数据通过 127.0.0.1 进行转发②、反弹端口：木马启动后主动连接客户端，客户端的端口一般设为 80，用以隐蔽通信，突破防火墙。

42、指定安全策略时有两种思想（1）凡是没有明确表示允许的就要禁止。（2）凡是没有明确表示禁止的就要允许。哪一种对制定网络安全策略是适用的，为什么？

答：理由 1：方法 1 明确规定了用户在网络中访问的权限与能够使用的服务，符合“最小权限”原则，便于网络管理。理由 2：网络服务有很多，当新的服务功能出现时，采用第一种方法将明确是否允许访问新的服务，如果采用第二种则默认用户能够访问这些新的服务。从管理与风险的角度，第二种造成管理混乱，风险增加。

【注：此题可以加深对访问控制策略三原则的理解】

43、（书 P66 习题 4 设计题）在仲裁方式认证下，通信双方 A、B 均在认证仲裁中心 X 注册了公开密钥，由 X 分配 A、B 通信会话密钥 Ks。设计一个使用临时值和时间戳的密钥交换协议，使双方得到 Ks，并确信对方已经取得 Ks（参考 Needham 协议，注明每个参数）

答：$\mathrm{A} \rightarrow \mathrm{X}: ID_A \| ID_B \| N_1$ （ID 为表示，N 为临时值）

$\mathrm{X} \rightarrow A: E_{kpua}[Ks \| ID_B \| N_1 \| E_{kpub}[Ks \| ID_A \| T_1]]$ （E_{kpua} 是通过 A 的公钥加密，$\mathrm{E}_{\mathrm{kpub}}$ 是通过 B 的公钥加密，T1 为时间戳）

$\mathrm{A} \rightarrow \mathrm{B}: \mathrm{E}_{\mathrm{kpub}}[Ks \| ID_A \| T_1]$ （A 转发 X 给 B 的内容）

$B \rightarrow A: E_{Ks}[N_2 \| T_2]$ （Ks 加密挑战值和时间戳）

$A \rightarrow B: E_{Ks}[f(N_2) \| T_2]$ （完成回应 B 的挑战）

【注：此题是书上课后习题，题目是要求通过 KDC 进行密钥分配，书本中内容为 Needham 协议使用对称密钥分配会话密钥，此题改为了让你使用公开密钥分配会话密钥的方式。也反映了考试中，让你使用已知的原理来进行设计的考察思路。既然作为课后题目，同时也是出题人编著的参考书，这种设

计题应该要作为复习的重点，与真题、练习题加以对照，掌握。】

44、简述 DES 子密钥生成原理

答:（图见书 P24 页）①、DES 输入密钥 K（64 位），去除奇偶校验位，得 56 位密钥（PC-1 置换）②、在计算 i 轮迭代所需子密钥时，进行循环左移，每轮左移位数取决于 i 值，这些进循环左移的值作为下一次循环左移的输入。③、将每轮移位的值经 PC-2 置换，所得即子密钥（48 位）

【注：子密钥产生原理，可能作为选择题目，让你选择正确答案。易错点可能在密钥位数，和每轮移位的 i 值，注意结合书中过程图进行理解】