《网络安全技术》习题与答案

目　录

浙江工商大学信电学院

《网络安全技术》课程组

二〇一〇年十一月

第一章　概述和密码学基础

1. 简述信息安全技术的三个发展阶段。

答：信息安全技术的发展可大致分为三个阶段：

1、单机系统信息保密阶段（1988 年以前）：这一阶段网络尚未形成或者大规模普及，用户环境相对纯净，对于可能产生的安全风险没有足够意识，安全目标主要集中在对单机系统内的信息机密性保护上；

2、网络信息安全阶段（1988 年-1996 年）：1988 年 Morris 蠕虫事件的爆发凸显了保障网络信息安全的必要性和紧迫性。除了继续沿用和研究各种信息加密技术之外，还开发了许多针对网络环境的被动防御技术，其主要安全目标是保障网络系统的安全可靠运行；

3、信息安全保障阶段：（1996 年-至今）：来源于 1996 年美国国防部 DoD 指令 5-3600.1（DoDD 5-3600.1），通过确保信息及信息系统的可用性、完整性、机密性、和不可否认性来保护信息系统的作战行动。不仅包含安全防御的概念，更扩充了主动和积极的防御概念，其主要安全目标主体由网络安全转移到信息及系统安全。

2. 简述导致计算机网络脆弱性的原因。

答：计算机网络脆弱性主要由以下原因引起：1、体系结构的脆弱性：上层服务对下层服务存在依赖性，当下层服务出错时上层服务会受影响；2、网络通信的脆弱性：通信协议或通信系统的安全缺陷会危及网络系统的整体安全；3、操作系统的脆弱性：利用操作系统的漏洞和缺陷发起网络攻击是最常见的攻击形式；4、应用系统的脆弱性：设计不当或存在缺陷的应用系统也可能成为网络脆弱性的原因之一；5、网络管理的脆弱性：人性和人为等因素可能在管理方面引入额外的安全风险；6、其它因素：例如自然灾害、追求灰色利益、人类好奇心理、政治或军事冲突等非技术因素。

3. 分析主动攻击和被动攻击的异同点。

答：被动攻击是指不影响正常通信内容、传输路径和通信模式的隐蔽攻击方式，常用于进行目标探测或信息搜集；主动攻击则通过篡改通信内容、传输路径或通信模式以期达到攻击目的，更具直接性和破坏性。首先，二者都属于安全攻击行为，都具有不同程度的危害性；其次，被动攻击具有隐蔽性，难以检测但易于预防；而主动攻击恰好相反，其攻击行为比较容易发现，易于检测但难以预防；最后，二者并不孤立，通常需要结合起来使用。

4. 何谓业务填充技术？主要用途如何？

答：所谓的业务填充即使在业务闲时发送无用的随机数据，增加攻击者通过通信流量获得信息的困难，是一种制造假的通信、产

生欺骗性数据单元或在数据单元中产生数据的安全机制。该机制可用于提供对各种等级的保护，用来防止对业务进行分析，同时也增加了密码通讯的破译难度。发送的随机数据应具有良好的模拟性能，能够以假乱真。该机制只有在业务填充受到保密性服务时才有效。可利用该机制不断地在网络中发送伪随机序列，使非法者无法区分有用信息和无用信息。

5. 分别简述 P^2DR、PDRR、WPDRRC 模型。

答：P^2DR 模型是美国国际互联网安全系统公司 ISS 最先提出的，包含四个安全元素：策略、防护、检测、响应。在统一的安全策略指导下，防护、检测、响应形成一个完备的、闭环的动态自适应安全体系。P^2DR 模型建立在基于时间的安全理论基础上，要求防护时间大于检测时间加上响应时间，即：$P_t > D_t + R_t$。该模型基本体现了完整的信息安全体系思想。

PDRR 模型在 P^2DR 模型的基础上把恢复环节提到了和防护、检测、响应等环节同等的高度，保护、检测、恢复、响应共同构成了完整的安全体系。PDRR 也是基于时间的动态模型，其中，恢复环节对于信息系统和业务活动的生存起着至关重要的作用，组织只有建立并采用完善的恢复计划和机制，其信息系统才能在重大灾难事件中尽快恢复并延续业务。

WPDRRC 模型全面涵盖了各个安全因素，突出了人、策略、管理的重要性，反映了各个安全组件之间的内在联系。该模型主要由六个元素构成：预警、保护、检测、响应、恢复、反击。

6. 试分析古典密码和现代密码的异同？

答：在 1949 年之前，是密码发展的第一阶段—古典密码体制。古典密码体制是通过某种方式的文字置换和移位进行，这种置换或移位一般是通过某种手工或机械变换方式进行转换，同时简单地使用了数学运算。古典密码的安全性主要依赖对算法本身的保密，密钥的地位和作用并不十分突出。虽然在古代加密方法中已体现了密码学的若干要素，但它只是一门艺术，而不是一门科学。

在 1949 年之后，是现代密码学的发展阶段。1949 年 Shannon 发表了题为《保密通信的信息理论》的著名论文，把密码学置于坚实的数学基础之上，标志着密码学作为一门学科的形成，这是密码学的第一次飞跃。1976 年，W. Diffie 和 M. Hellman 在《密码编码学新方向》一文中提出了公开密钥的思想，这是密码学的第二次飞跃。现代密码有着坚实的理论基础，同时严格遵循 Kerchoffs 准则：其安全性完全取决于对密钥而非算法的保密。相对于古典密码，现代密码是真正意义上的科学，其安全性、功能性和适用性都获得了长足发展。

7. 何谓 Kerchoffs 准则？有何实际意义？

答：1883 年 Kerchoffs 第一次提出密文编码原则：即加密的安全性应当基于对密钥的保密而不是对加密算法的保密。这一原则对

于密码学发展具有重要指导意义，获得普遍承认，并成为区分古典密码和现代密码的分界线。

违背 Kerchoffs 可能导致以下问题：1、兼容性问题：不同加密算法或同一加密算法的不同版本之间难以相互兼容；2、必须信任某个可信方：确信其不会泄漏或滥用应当被保密的密码算法；3、如果密码算法被泄漏，则所有采用此算法加密的信息机密性都将丧失，而且很难追查泄漏源；4、没有经过公开检验的加密算法通常含有较多的安全缺陷，其实际安全性有待商榷；5、难以形成公开的加密标准，不利于密码学的长远发展。

8. 何谓混合密钥体制？简述混合密钥体制下的消息传递过程。

答：对称密码体制算法简单，加解密速度快，但密钥管理较为困难；非对称密码体制算法比较复杂，加解密速度慢，但密钥管理相对容易，因此混合密钥体制同时运用对称和非对称密码体制，在实现快速加解密的同时方便密钥管理。其消息传递过程如下：第一步，数据发送者 A 用对称密钥把需要发送的数据加密；第二步，A 用接收者 B 的公开密钥将对称密钥加密，形成数字信封，然后将加密数据和数字信封一起传给 B；第三步，B 收到加密数据和数字信封后，用自己的私钥将数字信封解密，获取 A 加密数据时的对称密钥；第四步，B 使用该对称密钥解密收到的加密数据。

9. 何谓弱密钥？DES 算法中随机选中弱密钥的概率是多少？

答：DES 算法在每次迭代时都有一个子密钥供加密用。如果给定初始密钥 k，使得各轮子密钥都相同，即有 $K_1=K_2=\ldots=K_{16}$，则称给定密钥 k 为弱密钥。对于弱密钥 k，有 $DES_K(DES_K(x))=x$，$DES^{-1}_K(DES^{-1}_K(x))=x$ 成立；而对一般密钥 k 只满足 $DES_K(DES^{-1}_K(x))=DES^{-1}_K(DES_K(x))=x$。显然，弱密钥使得 DES 选择明文攻击下的搜索量减半。根据算法结构，DES 共有 4 个弱密钥，并且密钥有效长度为 56 比特，因此随机选中弱密钥的概率为 $4/2^{56}\approx 5.55\times 10^{-17}$。

10. RSA 公钥算法的理论基础为何？试简述其优缺点。

答：RSA 算法的理论基础为大整数分解的困难性。若已知两个大素数 p、q，求 $n=p\times q$ 只需要一次乘法，但若由 n 分解出 p、q 则是一个非常困难的问题。虽然整数分解问题已进行了几世纪研究，但至今尚未发现快速算法。RSA 算法既可用于数据加密，也可用于数字签字，同时也具有一般非对称密码算法的特点：运算量大、加解密速度慢。另外，由于指数运算保持了输入的乘法结构，攻击者可能借此发起选择明文攻击，达到消息破译、骗取签字等目的。最后，因为在共用模数的前提下，如果两个密钥互素，则可用任一密钥恢复明文，因此多用户尽量不要共用同一模数 n，避免遭受共模攻击。

11. 试从密码分析者的角度出发简述密码分析的四种类型。

答：根据密码分析者所能获得的信息的类型，可将密码分析分成下列几类：唯密文攻击：攻击者只有密文串，想求出明文或密钥；

已知明文攻击：攻击者知道明文串及对应的密文串，想求出密钥或解密变换；选择明文攻击：攻击者不仅知道明文串及其对应密文串，而且可选择用于加密的明文，想求出密钥及解密变换；选择密文攻击：攻击者不仅知道明文串及对应密文串，且密文串由攻击者选择，想求出密钥及解密变换。这几类攻击的强度依次增大，唯密文攻击最弱。

12. 何谓杂凑函数的弱抗碰撞性和强抗碰撞性？

答：抗碰撞性是衡量杂凑函数安全性的重要指标。所谓弱抗碰撞性是指：对于任意的明文 M，找到另外一个明文 N，使得 M≠N 但 hash(M)=hash(N)在计算上是不可行的。所谓强抗碰撞性是指：找到任意一对明文 M、N，使得 M≠N 但 hash(M)=hash(N)在计算上是不可行的。就安全程度而言，强抗碰撞性要高于弱抗碰撞性：如果没有强碰撞，肯定没有弱碰撞；反之不成立。

13. 何谓生日攻击？其结论对保障杂凑函数的安全性有何意义？

答：生日攻击是指找到一个与某人生日相同的概率超过 0.5 时，所需总人数为 183 人；但要找到至少两人生日相同的概率超过 0.5 时，所需总人数仅仅为 23 人。该事实揭示了对于特定输出长度的杂凑算法，强碰撞攻击的成功概率要远远高于弱碰撞攻击。为防御生日攻击，应选用较大输出长度的杂凑算法。

14. 生日攻击实例中攻击者意图生成何种碰撞？成功概率如何？

答：攻击者意图在两组合同中各选一份使得其杂凑值相同，既非弱碰撞攻击也非强碰撞攻击，而是介于两者之间的一种形式。为计算成功概率，先考虑 M 组中的一份合同均不与 M⁻组中任一份合同杂凑值相同的概率：$\rho_1=(1-1/2^{64})^{2^{32}}$；其次，当 M 组中的任一份合同都满足这一条件时，攻击者才会失败，对应概率为：$\rho_2=\rho_1^{2^{32}}=((1-1/2^{64})^{2^{32}})^{2^{32}}=(1-1/2^{64})^{2^{64}}$；最后，攻击者成功的概率则为：$\rho=1-\rho_2=1-(1-1/2^{64})^{2^{64}}$。其中^表示乘方运算。

15. 同上，若 A 先随机提交 M⁺供 B 签名，再次回答问题 Q_{14}。

答：若 A 先提交 M⁺供 B 签名，则只能试图在 M⁻组中选取一份与 M⁺杂凑值相同的合同，因此攻击退化为弱碰撞攻击。其成功概率为：$\rho=1-\rho_1=1-(1-1/2^{64})^{2^{32}}$。其中^表示乘方运算。

16. 比较 Q_{14} 和 Q_{15} 的结果，从中可以得出何种结论？

答：通过对比 Q_{14} 和 Q_{15} 的结果，可以得知强碰撞攻击的成功概率大于弱碰撞攻击，因此杂凑函数的安全程度主要应以强抗碰撞性而不是弱抗碰撞性来衡量。另外，攻击成功概率随杂凑函数输出长度的增长而迅速衰减，因此为确保安全性，应选用较大输出长度的杂凑函数。

17. 消息认证（MAC）有何局限？应如何解决？

答：消息认证可以保护信息交换双方不受第三方的攻击，但不能处理通信双方的相互攻击。信宿方可以伪造消息并称消息发自信

源方：信宿方产生一条消息，并用和信源方共享的密钥产生认证码，并将认证码附于消息之后。信源方也可以否认曾发送过某消息，因为信宿方可以伪造消息，所以无法证明信源方确实发送过该消息。在收发双方不能完全信任的情况下，引入数字签名来解决上述问题，数字签名的作用相当于手写签名。

18. 试简述数字签名算法应具备的基本特征。

答：数字签名必须具有下述特征：收方能够确认或证实发方的签名，但不能伪造，简记为 R1-条件；发方发出签名的消息给收方后，就不能再否认他所签发的消息，简记为 S-条件；收方对已收到的签名消息不能否认，即有收报认证，简记作 R2-条件；第三者可以确认收发双方之间的消息传送，但不能伪造这一过程，简记作 T-条件。

19. 简述 RSA 算法的摘要消息签名和验证流程。

答：签字过程如下：1、签字方 A 生成明文消息 M 的摘要 D；2、A 使用自己的签字私钥 d_A 对明文摘要 D 进行签字得到结果 S；3、A 公布明文消息 M 和签字结果 S。对应验证流程如下：1、验证方 B 对明文消息 M 进行杂凑运算得到摘要 D′；2、B 使用 A 的验证公钥 e_A 处理签字结果 S 得到摘要 D；3、B 比对两个摘要值 D 和 D′：若二者相等则签字有效，否则签字无效。

20. 何谓盲签名和群签名？后者特征如何？

答：一般数字签名中，总是要先知道文件内容而后才签署，这正是通常所需要的。但有时需要某人对一个文件签名，但又不让他知道文件内容，称此为盲签名。Chaum 在 1983 年首次提出盲签名概念，普遍适应于电子选举、数字货币协议中。

群体密码学由 Desmedt 于 1987 年提出，群签名是群体密码学中的课题，1991 由 Chaum 和 van Heyst 提出。其特点有：只有群体成员才能代表群体签名；接收到签名的人可以用公钥验证群签名，但不可能知道由群体中那个成员所签；发生争议时可由群体中的成员或可信赖机构识别群签名的签名者。

21. 何谓实体认证和消息认证？

答：认证分为实体认证和消息认证：实体认证是对通信主体的认证，目的是识别通信方的真实身份，防止假冒，常用数字签名的方法；消息认证是对通信数据的认证，目的是验证消息在传送或存储过程中是否被篡改，一般用消息摘要的方法。

22. 试列举常用的实体认证技术。

答：常用的实体认证技术包括：1、主体特征认证：目前已有的方法包括：视网膜扫描、声音验证、指纹和手型识别器。这些识别系统能够检测指纹、签名、声音、零售图案这样的物理特征；2、口令机制：口令是相互约定的代码，假设只有用户和系统知道。口令可有用户选择或系统分配，验证时用户先输入某标志信

息(如用户名),系统可以为用户生成一个一次性口令的清单;3、一次性口令:一次性口令系统允许用户每次登录时使用不同的口令。系统在用户登录时给用户提供一个随机数,用户将这个随机数送入口令发生器,口令发生器以用户的密钥对随机数加密,然后用户再将口令发生器输出的加密口令送入系统。系统再进行同样方法计算出一个结果,比较两个结果决定是否该身份有效;4、智能卡:访问不但需要口令,也需要物理智能卡。在允许进入系统之前需要检查其智能卡。智能卡内有微处理器和存储器,可已加密的形式保存卡的 ID 及其他身份认证数据;5、身份认证协议:通过网络协议对通信主体进行身份认证。不同的身份认证协议对于窃听、窜扰、重放和冒充等攻击手段具有不同的防御能力。

23. 试简述双向公钥实体认证流程。

答:双向公钥实体认证流程如下:1、A 首先生成质询信息 R_A,R_A是一个随机数;接着 A 用 B 的公钥 K_B加密会话信息 $\{A, R_A\}$,然后发给 B;2、B 用自己的私钥解出 $\{A, R_A\}$,再生成质询信息 R_B和会话密钥 K_S,接着 B 用 A 的公钥 K_A加密会话信息$\{R_A, R_B, K_S\}$,然后发给 A;3、A 用自己的私钥解出 $\{R_A, R_B, K_S\}$,核对 R_A无误后,用 K_S加密 R_B,然后发给 B。B 收到后用 K_S解出 R_B,核对无误后完成双向认证。

第二章　操作系统安全

1. 简述Intel x86系列处理器和Windows 2000分别支持的运行模式。

   答：Intel x86处理器支持4种运行模式，或称计算环(ring)：Ring 0：最高优先级；Ring 1；Ring 2；Ring 3：最低优先级。Windows 2000仅使用两种运行模式：Ring 0，内核模式：所有内核模式进程共享一个地址空间；Ring 3，用户模式：每个用户模式进程拥有自己私有的虚拟内存空间。

2. 如何度量操作系统的安全程度？简述TCSEC评估标准。

   答：操作系统安全程度被分为八个等级（D1、C1、C2、B1、B2、B3、A1和A2）。其中D1系统的安全度为最低，常见的无密码保护的个人计算机系统即属此类；通常具有密码保护的多用户工作站系统属于C1级，如Windows 2000。

   操作系统安全程度的度量标准目前常用美国国防部系统所制定的TCSEC（“Trusted Computer System Evaluation Criteria”（1985）），其评估标准主要是基于：1、系统安全政策（Policy）的制定；2、系统使用状态的可审性（Accountability）；3、安全政策的准确解释和实施的可靠性（Assurance）。

3. 简述Windows 2000系统的六大主要安全元素。

   答:Windows 2000系统的六大主要安全元素依次为:审计(Audit)；管理(Administration)；加密(Encryption)；权限控制(Access Control)；用户认证（User Authentication）；安全策略（Corporate Security Policy）。其中Windows NT/2K系统内置支持用户认证、访问控制、管理和审核。

4. 简述Windows 2000安全子系统的工作过程。

   答：用户通过本地、网络(除账号标识外还可采用令牌、指纹、视网膜、IC卡等方式)登陆Windows 2000操作系统，身份鉴别子系统（LSA）向本地用户和工作组的数据库SAM发送Kerberos或者NTLM协议进行认证,认证通过则登录成功并获得访问令牌,发送令牌等信息给安全引用监视器(SRM)来检查访问令牌和被访问对象的ACL，由授权管理子系统(LSA)设置对象的ACL,并由审计子系统（LSA）对验证、授权过程作日志审核,最后根据用户的权限和对象的ACL进行访问控制。

5. 简述Windows 2000安全子系统的五个安全组件及对应功能。

   答：Windows 2000安全子系统包括五个安全组件：安全标识符、访问令牌、安全描述符、访问控制列表和访问控制项。

   安全标识符（Security Identifiers）:

   a）就是我们经常说的SID，每次当我们创建一个用户或一个组的时候，系统会分配给改用户或组一个唯一的SID，当你重新安装Windows NT后，也会得到一个唯一的SID。

b) SID 永远都是唯一的，由计算机名、当前时间、当前用户态线程的 CPU 耗费时间的总和三个参数决定以保证它的唯一性。

访问令牌（Access tokens）:

a) 用户通过验证后，登陆进程会给用户一个访问令牌，该令牌相当于用户访问系统资源的票证。当用户试图访问系统资源时，将访问令牌提供给 Windows NT，然后 Windows NT 检查用户试图访问对象上的访问控制列表。

b) 如果用户被允许访问该对象，Windows NT 将会分配给用户适当的访问权限。访问令牌是用户在通过验证的时候由登陆进程所提供的，所以改变用户的权限需要注销后重新登陆，重新获取访问令牌。

安全描述符（Security descriptors）:

a) Windows NT 中的任何对象的属性都有安全描述符这部分。它保存对象的安全配置。

访问控制列表（Access control lists）:

a) 访问控制列表有两种：任意访问控制列表（Discretionary ACL）、系统访问控制列表（System ACL）。

b) 任意访问控制列表包含了用户和组的列表，以及相应的权限，允许或拒绝。每一个用户或组在任意访问控制列表中都有特殊的权限。而系统访问控制列表是为审核服务的，包含了对象被访问的时间。

访问控制项（Access Control Entries）:

a) 包含了用户或组的 SID 以及对象的权限。访问控制项有两种：允许访问和拒绝访问。拒绝访问的级别高于允许访问。

b) 当使用管理工具列出对象的访问权限时，列表的排序是以文字为顺序的，它并不象防火墙的规则那样由上往下的。不过好在并不会出现冲突，拒绝访问总是优先于允许访问的。

6. 假设 beta75 为某 Windows 2000 系统账户，隶属于组 A 和组 B:

A、若先删除该用户然后重建同名用户，能否恢复原访问权限?

B、若某资源允许组 A 访问但禁止组 B 访问，beta75 能否访问?

C、若另一系统中有同名用户，是否具备对原系统的访问权限?

D、在另一系统中是否可以强制获得资源访问权限？如何操作?

E、如何保证用户安全标识符的唯一性?

答：A、不能。因为资源的访问权限是基于用户 SID 的，而 SID 具备唯一性，不可能通过重建同名账户生成相同的 SID;

B、不能。因为在判别资源访问权限时，拒绝权限优先级高于许可

权限;

C、不能。同 A,另一系统的同名账户与本系统账户具有不同的 SID;

D、可以。需要管理员权限和物理访问，挂载原分区并设置访问权限或取得所有权;

E、SID 由系统根据计算机名、当前时间、用户态线程的 CPU 耗时总和自动生成，并且被加密存储在安全账户管理器（SAM）中防止被篡改。

7. 简述 Windows 2000 系统的本地登录过程。

答: 当从 Windows 2000 Professional or Server 登录时，Windows 2000 用两种过程验证本地登录: Windows 2000 首先尝试使用 Kerberos 作为基本验证方式; 如果找不到 Key Distribution Center 服务, Windows 会使用 Windows NT LanManager(NTLM)安全机制来验证在本地 SAM 中的用户。本地登录验证过程如下: 1、输入用户名及密码然后按回车键,Graphical Identification and Authentication(GINA)会收集这些信息; 2、GINA 传送这些安全信息给 Local Security Authority(LSA)来进行验证; 3、LSA 传送这些信息给 Security Support Provider Interface(SSPI), SSPI 是一个与 Kerberos 和 NTLM 通讯的接口服务; 4、SSPI 传送用户名及密码给 Kerberos SSP, Kerberos SSP 检查目的机器是本机还是域名: 如果是本机, Kerberos 返回错误消息给 SSPI; 如果找不到 KDC, 机器生成一个用户不可见的内部错误; 5、这个内部错误促发 SSPI 通知 GINA。GINA 再次传送这些安全信息给 LSA。LSA 再次传送这些安全信息给 SSPI; 6、这次 SSPI 传送用户名及密码给 NTLM driver MSV1-0 SSP。NTLM driver 用 Netlogon 服务和本地 SAM 来验证用户。如果 NTLM 和 Kerberos 都无法验证账号, 用户会收到错误消息提示输入正确的用户名和密码。

8. 简述 Windows 2000 系统中用户访问某资源时的授权过程。

答: 用户登入系统后首先从 LSA 获得访问令牌，其中含有用户名、SID 以及该用户对应权限。当用户申请访问某资源时，安全引用监视器（SRM）对比该用户权限和资源的访问控制列表: 若具有许可权限则允许其访问，否则拒绝; 必要时对验证、授权过程作日志审核。

9. 何谓 Windows 加密文件系统（EFS）？简述其特点。

答: “加密文件系统” (EFS)提供一种核心文件加密技术，该技术用于在 NTFS 文件系统卷上存储已加密文件。一旦加密了文件或文件夹，你就可以像使用其他文件和文件夹一样使用它们。对加密该文件的用户，加密是透明的，这表明不必在使用前解密已加密的文件，你可以像平时那样打开和更改文件。但试图访问已加密文件或文件夹的入侵者将被禁止这些操作: 如果入侵者试图打开、复制、移动或重新命名已加密文件或文件夹，将收到拒绝访问的消息。EFS（加密文件系统）是依赖用 NTFS 文件系统来工作的。

也就是说要想使用 EFS 功能我们的分区必须是 NTFS 类型。其实，EFS 也是 NTFS 文件系统安全性的一个实例体现。EFS 对于加密数据的用户来说是透明的，EFS 同时使用了私钥和公钥的加密方案。

10. 如何检查 Windows 2000 系统中是否有非法启动程序？

答: 检查两个文件夹和八个注册键。看看里面有哪些是你不想要的，删除即可。

1）文件夹一、当前用户专有的启动文件夹这是许多应用软件自动启动的常用位置，Windows 自动启动放入该文件夹的所有快捷方式。用户启动文件夹一般在:\Documents and Settings\<用户名字>\“开始”菜单\程序\启动，其中“<用户名字>”是当前登录的用户账户名称。

2）文件夹二、对所有用户有效的启动文件夹这是寻找自动启动程序的第二个重要位置，不管用户用什么身份登录系统，放入该文件夹的快捷方式总是自动启动—这是它与用户专有的启动文件夹的区别所在。该文件夹一般在:\Documents and Settings\All Users\“开始”菜单\程序\启动。

3）注册表三、Load 注册键介绍该注册键的资料不多，实际上它也能够自动启动程序。位置:HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\load。

4)Userinit 注册键位置: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit。这里也能够使系统启动时自动初始化程序。通常该注册键下面有一个 userinit.exe。这个键允许指定用逗号分隔的多个程序，例如“userinit.exe,OSA.exe”(不含引号)。

5)Explorer\Run 注册键和 load、Userinit 不同，Explorer\Run 键在 HKEY_CURRENT_USER 和 HKEY_LOCAL_MACHINE 下都有，位置是:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run，和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run。

6)RunServicesOnce 注册键: RunServicesOnce 注册键用来启动服务程序，启动时间在用户登录之前，而且先于其它通过注册键启动的程序。RunServicesOnce 注册键的位置是:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce，和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce。

7)RunServices 注册键: RunServices 注册键指定的程序紧接 RunServicesOnce 指定的程序之后运行，但两者都在用户登录之前。RunServices 的位置是:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices，和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

\RunServices。

8)RunOnce\Setup 注册键 RunOnce\Setup 指定了用户登录之后运行的程序，它的位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup，和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\Setup。

9)RunOnce 注册键安装程序通常用 RunOnce 键自动运行程序，它的位置在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 和 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce。HKEY_LOCAL_MACHINE 下面的 RunOnce 键会在用户登录之后立即运行程序，运行时机在其他 Run 键指定的程序之前。HKEY_CURRENT_USER 下面的 RunOnce 键在操作系统处理其他 Run 键以及“启动”文件夹的内容之后运行。如果是 XP，你还需要检查 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx。

10)Run 注册键 Run 是自动运行程序最常用的注册键，位置在：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run，和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows\CurrentVersion\Run。HKEY_CURRENT_USER 下面的 Run 键紧接 HKEY_LOCAL_MACHINE 下面的 Run 键运行，但两者都在处理“启动”文件夹之前。汇总如下：\Documents and Settings\<用户名字>\“开始”菜单\程序\启动\Documents and Settings\All Users\“开始”菜单\程序\启动 HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\loadHKEY_CURRENT。

11. 简述保障 Windows 2000 系统账户安全的基本措施。

答：可以停掉 Guest 账号、创建 2 个管理员用账号、把系统 Administrator 账号改名、设置屏幕保护密码等确保安全，也可以利用 win2000 的安全配置工具来配置策略、关闭不必要的服务、关闭不必要的端口、禁止建立空连接和安装微软最新的补丁程序等措施来加强 Windows 2000 账户安全。

12. 为什么要尽量避免使用管理员账户进行日常工作？

答：采用管理员账户进行日常工作往往会留下痕迹，如果黑客希望远程登录系统的话，就必须拥有具有远程登录权限的账户，而管理员账户自然是具备了远程登录的权限。另外由于 Administrator 是系统中默认建立的管理员账户，而且一般无法删除，所以黑客都会选择 Administrator 作为用户名猜测登录密码。虽然使用“组策略”可以修改 Administrator 的用户名，可是一旦黑客给 Administrator 起了个“小名”(影子账户)，再怎么改用户名也没用了。用管理员账户进行日常工作会带来大量的安全隐患，并给黑客留下可乘之机。

13. 简述 Unix 文件系统权限，比较其与 Windows 文件权限的异同。

答：Unix 下文件有 3 种权限：读、写和执行；文件有三种权限所属：拥有者、组群及其它用户；因此共有 9 种权限组合模式。与 Windows 文件权限的异同：1、文件执行权限上的差异分析：Unix 在对文件专门进行了执行权限的控制，在 Windows 下其权限只有读、写的控制；2、相同的组不同的用户具有不同的权限：在 Unix 系统中，即使相同组的用户，默认情况下其对于文件的权限也是不同的，而 Windows 操作系统下同一个组的用户往往具有相同的权限；3、谁可以更改文件的权限：在 Unix 操作系统上，文件的所有权人与 root 账户才能够修改文件的权限，在 Windows 操作系统中，往往只要对这个文件具有写权限的人就可以这个文件的权限 4、文件权限控制的漏洞：解决方法文件权限与目录权限配合使用才有效。

14. 在 Unix 系统中 uid 是否具备唯一性？对系统安全有何影响？

答：在 Unix 内部只用一个数字标示每一个用户：用户的标识符(UID)，通常系统管理员给计算机上的每个一用户分配一个不同的 UID，系统只根据 UID 确定其操作权限。用户标识(UID)取值 0-65535，其中习惯于将 0-99 分配给系统管理帐号。Unix 系统凭借文件/etc/passwd 实现用户名与 UID 之间的映射关系。UID 是操作系统用于标识用户的实际信息；用户名被提供仅仅是方便用户的考虑。两个具有相同 UID 的用户将被视为同一个用户，即使用他们具有不同的用户名和口令，它们可以自由地读取和删除对方的文件，以及取消对方的进程。

15. 什么是 SUID 和 SGID 程序？为什么要有 SUID 和 SGID 程序？

答：Unix 中的 SUID(Set User ID)/SGID(Set Group ID)设置了用户 id 和分组 id 属性，允许用户以特殊权利来运行程序，这种程序执行时具有宿主的权限。SUID 程序是为了使普通用户完成一些普通用户权限不能完成的任务而设置的。比如每个用户都允许修改自己的密码，但是修改密码时又需要 root 权限，所以修改密码的程序需要以管理员权限来运行。

16. 什么是 su 和 sudo 程序？如何限制二者的使用范围？

答：su 是切换用户命令，而 sudo 允许分配给普通用户一些合理的“权利”，让他们执行一些只有超级用户或其他特许用户才能完成的任务，是需要授权许可的，所以也被称为授权许可的 su。sudo 通过配置文件/etc/sudoers 进行授权。su 是切换到超级用户的命令，sudo 只是交给普通用户一点点超级用户的权力。

17. 什么是硬链接和符号链接？二者有何区别？

答：硬链接是一个目录项，比如文件名或索引节点号，可以将文件名与文件的位置关联起来；符号链接指存储了一个字符串的文件，这个字符串可以在路径名解析的过程中，用于修改路径名。两者区别：1、硬链接是通过 i 节点来关联文件，不同的文件系

统都有自己独立的 i 节点，所以硬链接不能跨越文件系统，不能指向目录；2、符号链接是通过文件名来关联文件，即使原文件删除，符号链接可依然存在，但指向为空。符号链接可以跨越文件系统，也可以指向目录；3、硬链接用 ln 创建，符号链接用 ln -s 创建；4、符号链接类似 Windows 里的快捷方式，硬链接类似于共享；5、lstat()可以获取链接文件本身的信息，stat()函数获取指向文件的信息。

18. 什么是粘着位（sticky bit）？为什么要使用粘着位？

答：粘着位，又称保存文本位，其实质是一个权限控制属性。通常情况下，粘着位既可以用在普通文件上，也可以用在目录文件上。当用在普通文件上时，粘着位可以把某个程序文件的 SUID 置位。并且它的文本映像将永久保存在交换区里。当程序获得了 CPU 使用权时，就可以快速的装载到内存中，故粘着位可以提高系统程序的运行效率。另外利用粘着位能够防止其他用户对文件进行恶意删除。

19. 什么是安全 Shell（SSH）？为什么要使用 SSH?

答：SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定，是建立在应用层和传输层基础上的安全协议。SSH 是专为远程登录会话和其他网络服务提供安全性的可靠协议。通过使用 SSH 可以把所有传输的数据进行加密，这样“中间人”这种攻击方式就不可能实现了，同时也能够防止 DNS 和 IP 欺骗。另外一个好处是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 telnet，又可以为 ftp、pop、甚至 ppp 提供一个安全的“通道”。

20. 什么是 TCP Wrappers 程序？为什么要使用该程序？

答：TCP Wrappers 软件扩展了 inetd 为受其控制的服务程序实施控制的能力。通过使用这种方法，它能够提供日志支持、返回消息给联入的连接、使得服务程序只接受内部连接。尽管防火墙能够完成其中的某些功能，TCP Wrappers 也提供了防火墙无法提供的功能，但由 TCP Wrappers 所提供的额外安全功能不应被视为好的防火墙的替代品。TCP Wrappers 应结合防火墙或其他安全加强设施一并使用，为系统多提供一层安全防护。

21. 何谓 umask 值？试解释 022、027、077 三种 umask 值的含义。

答：umask 值是指为新建文件或目录预设的三位八进制访问权限。umask 值是一种补权限，即所标明的权限应该从访问控制权限中去除。可以通过修改配置文件（取决于具体系统）或 umask 命令（临时）来设置 umask 值。由于系统不允许文件具有缺省执行权限，因此文件最大权限为 umask 值 0，最小权限为 umask 值 6（x 执行权限被忽略），文件权限=666-umask 值（计算时忽略 x 权限并默认为-）；目录最大权限为 umask 值 0，最小权限为 umask 值 7，目录权限=777-umask 值。

三种 umask 值含义：022：对应文件权限为 666-022=644（rw-r--r--）;对应目录权限为 777-022=755（rwxr-xr-x）;027：对应文件权限为 666-027=640（rw-r-----）；对应目录权限为 777-027=750（rwxr-x---）；077：对应文件权限为 666-077=600（rw-------）；对应目录权限为 777-077=700（rwx------）。

22. Unix 系统中如何保存用户口令？与 Windows 方式有何异同？

答：Unix 系统中的 shadow 文件位于/etc 目录中，用于存放用户口令等重要信息，所以该文件只有 root 用户可以读取。与 passwd 文件类似，shadow 文件中保存的是已加密的口令。Windows 用户口令保存在%SystemRoot%\system32\config\sam 文件中，sam 文件是 Windows NT 的用户账户数据库，所有 2K/NT 用户的登录名及口令等相关信息都会保存在这个文件中。sam 文件可以认为类似于 Unix 系统中的 passwd 文件，不过没有这么直观明了。passwd 使用的是存文本的格式保存信息，每一行都代表一个用户资料，每一个账号都有七项资料。除密码是加密形式外，其他项目非常清楚明了。而 Windows 虽然也是用文件保存账号信息，但将这些资料全部进行了加密处理，一般的编辑器是无法直接读取这些信息的。注册表中的 HKEY_LOCAL_MACHINE\SAM\SAM 和 HKEY_LOCAL_MACHINE\SECURITY\SAM 保存的就是 SAM 文件的内容，在正常设置下仅对 system 是可读写的。

23. 何谓影子口令（shadow）文件？对于系统账户安全有何意义？

答：传统上/etc/passwd 文件在很大范围内是可读的，因为许多程序需要用它来把 UID 转换为用户名。但如果使用口令猜测程序，具有加密口令的可读/etc/passwd 文件表现出巨大的安全隐患。多数近来的 Unix 产品支持一个变通方法：影子口令文件。影子口令系统把口令文件分成两部分：/etc/passwd 和影子口令文件。影子口令文件保存加密的口令：/etc/passwd 中的 coded-password 域都被置为“X”或其它替代符号。影子口令文件只能被 set-uid 程序在需要合法访问时读取，其他所有非授权用户都被拒绝访问。习惯上，影子口令文件保存在/etc/shadow 中，尽管有些系统使用可选的路径和文件名。Linux/Unix 广泛采用了“shadow（影子）”机制，将加密的口令转移到/etc/shadow 文件里，该文件只为 root 超级用户可读；同时/etc/passwd 文件的密文域显示为一个 x，从而最大限度减少密码泄露的机会。

24. X-Window 对于 Linux 系统的安全性能有何影响？

答：在网络环境下，X-Window 允许远程机访问本地的 X-Server，在本地机运行 X-Window 软件并将结果显示到远程机。这无疑有利于资源共享，尤其是当本地服务器存有某些价格昂贵的 X-Window 软件的时候，其优点十分明显。但方便有时会带来安全上的问题：如果某个不怀好意的家伙滥用访问权，运行一个使用 X-Window 协议基本服务的监听程序来监听本地服务器的话，它甚至能够捕捉到本地击键的所有内容。

25. 在 Ubuntu 实验系统中，如何启用 root 账户？说明什么问题？

答：Ubuntu 中默认是关闭 root 账户的，要启用它很简单：1、输入 sudo passwd root 重新设定 root 账户密码；2.允许 root 账户登录，输入 sudo vi /etc/X11/gdm/gdm.conf 打开 gnome 配置文件，找到 AllowRoot＝false 这一行，改为 AllowRoot＝true，保存后退出。Ubuntu 处于安全性的考虑默认关闭了 root 账户，这样可以减少使用 root 权限的时间总耗用，降低了不注意使用 root 执行命令的风险，并提供了有用的审核痕迹。

26. 在 Unix/Linux 系统中，若忘记所有账户密码，该如何恢复？

答：口令的恢复有 2 个方面：一是给用户产生一个新的口令，使用户能够重新登录系统；二是找出用户原来的口令，而不是以新口令代替旧口令。

密码重设法（以 Redhat9.0 为例）：1、系统启动后,在出现 grub 画面时，用上下键选中你平时启动 Linux 的那一项，然后按 e 键；2、再次用上下键选中你平时启动 Linux 的那一项(类似于 kernel/boot mlinuz-2.4.18-14 ro root=LABEL=/)，然后按 e 键;3、修改你现在见到的命令行,加入 single,结果如下:kernel /boot mlinuz-2.4.18-14 single ro root=LABEL=/ single；4、回车返回，然后按 b 键启动，即可直接进入 Linux 命令行；5、用 passwd 命令修改密码。

其它方法：1、紧急修复模式：在无法启动 Linux 时，常常需要通过磁盘、光盘或其他方法启动 Linux 基本环境，进入 Linux 紧急修复模式。在紧急修复模式下，能够访问硬盘上的 Linux 系统文件，恢复系统正常，包括恢复口令等；2、单用户模式：Linux 有多个运行级别，如单用户模式、无网络服务多用户模式、完全多用户模式和 X11 图形多用户模式等运行级别。单用户模式是指系统运行在惟一用户——Root 用户模式下，进入此模式时，系统只是加载了可运行的最低软硬件配置，以 Root 直接进入，没有口令验证。在单用户模式下，可以用 passwd 命令来更改用户口令，也可以直接对/etc/passwd 等账户口令文件进行读写，达到口令恢复的目的；3、修改口令文件：Linux 口令文件有 2 种保存形式：一种是把账户信息和经加密后的口令密文都保存在/etc/passwd 文件中，此形式不够安全，在早期 Unix 中采用；另一种是把账户信息和口令密文分开存放，/etc/passwd 文件用于保存账户信息，/etc/shadow 文件用于保存口令密文。至于采用何种保存形式和加密算法，可以用/usr/sbin/authconfig 程序来设置。对于没有 shadow 的 passwd 文件，只要把相应账户的口令字段删除，即可不经口令验证直接登录系统。如果是有 shadow 的 passwd 文件，可以删除 passwd 文件中的“x”字母，或者删除 shadow 文件中的口令密文，都可以使相应用户不经口令验证直接登录系统，达到口令恢复的目的；4、口令还原：有些情况下，想找出被丢失的原始口令，而不是登录系统去产生一个新的口令。但是，Linux 使用的是 DES（加密函数式是 Crypt）

或MD5（函数式是Md）加密算法，由于计算量大，它们几乎都没有可能被逆向破解。可用的Linux口令破解工具较多，如John the Ripper、Crack by Alex Muffett和Cracker Jack等等；5、系统攻击破解：如果能够关闭电源重新启动系统，那么很容易恢复口令，但有时Linux系统上运行着非常重要的服务，不能直接关闭电源，否则会对系统和数据产生破坏。像这种在系统运行的情况下获得系统口令，往往是比较困难的，但由于系统管理员对操作系统和应用程序的版本、配置等情况有着全面的了解，加上没有防火墙和入侵检测系统等的防护，那么发现和利用系统漏洞的机会还是不少的，口令恢复的成功机会还是有的。

第三章　漏洞扫描技术

1. 简述 TCP 连接的建立和终止过程？概括其对不同标志位的响应。

   答：建立连接协议需要通过三次握手完成。1、客户端发送一个 SYN 报文到服务器；2、服务器回应客户端 ACK 和 SYN 报文；3、客户再次回应服务器一个 ACK 报文。

   连接中止协议需要通过四次分手完成。1、客户端发送一个 FIN 报文，用来关闭客户端到服务器的数据传送；2、服务器收到这个 FIN 报文，它回送一个 ACK 报文；3、服务器关闭客户端的连接，发送一个 FIN 报文给客户端；4、客户段发回 ACK 报文确认。

   若端口处于监听状态：丢弃 FIN、RST、非 SYN 数据包；丢弃 ACK 数据包，回送 RST 数据包；响应 SYN 数据包，回送 SYN|ACK 数据包。若端口处于关闭状态：丢弃 RST 数据包；丢弃 SYN 或 FIN 数据包，回送 RST 数据包。

2. 何谓信息收集技术？主要作用是什么？试列举几种常用方法。

   答：信息收集技术是指对目标系统相关信息(包括硬件型号、操作系统、网络配置、运行服务等等)的搜集和整理，主要被攻击者用于攻击前的勘查准备或被管理员用于发现系统的漏洞和弱点并进行修补。常用方法或途径包括社会信息、网站信息、社交工程、电话簿、网络搜索引擎、whois 和 DNS 查询、网络勘查、网络扫描等等。

3. Traceroute 主要用于何种目的？试简述其工作原理。

   答：Traceroute 主要用来发现实际的路由路径，为勾画出网络拓扑图提供最基本的依据。工作原理：发送一系列 UDP 包(缺省大小为 38 字节)，其 TTL 字段从 1 开始递增，然后监听来自路径上网关发回来的 ICMP Time Exceeded 应答消息；UDP 包的端口设置为一个不太可能用到的值(缺省为 33434)，因此目标会送回一个 ICMP Destination Unreachable 消息，指示端口不可达。

4. 如何防范网络勘查？试列举几种常见的应对方法。

   答：可以使用以下应对措施：1、部署防火墙，通过设置过滤规则禁止探测网络数据包通过；2、部署入侵监测系统，识别网络勘查行为并采取必要的反制措施；3、使用其它工具：如 rotoroutor，它可以记录外来的 traceroute 请求，产生虚假的应答。

5. 何谓网络扫描技术？对于网络安全有何意义？

   答：互联网在最初设计时并未充分考虑安全需求，不仅自身存在安全缺陷，TCP/IP 协议也并不安全，因此互联网存在诸多安全威胁。扫描技术主要包括 ping 扫描、操作系统探测、端口扫描三部分：ping 扫描帮助探测操作系统的存活状态；操作系统探测可以识别目标主机上运行的操作系统类型和版本；端口扫描则通过与目标系统的 TCP/IP 连接查看该系统处于监听或运行的系统服务。

网络扫描技术一方面可用于检查网络主机或网络，发现其安全缺陷，便于对系统进行修补和加固，提高其安全性；另一方面可被攻击者用于探测系统弱点或安全漏洞，以便有针对性地发起网络攻击。无论处于何种目的，网络扫描对于提升网络安全都有积极的促进意义。

6. 根据扫描目标的不同，扫描技术可分为几大类别？

答：扫描技术可分为三大类别：1、主机扫描：确定在目标网络上的主机是否可达，同时尽可能多映射目标网络的拓扑结构，主要利用 ICMP 数据包；2、端口扫描：发现远程主机开放的端口以及服务；3、操作系统扫描：根据协议栈指纹判别操作系统。

7. 何谓主机扫描技术？试列举几种常见的主机扫描方式。

答：主机扫描技术是指通过 ICMP 协议判断远程主机存活状态，从而跳过非激活主机提高扫描效率的扫描方式。常见的方式包括：ICMP Echo、ICMP Sweep、Broadcast ICMP、Non-Echo ICMP、异常 IP 包头、无效字段 IP 头、超长 IP 包、反向映射等等。

8. 何谓反向映射探测扫描？简述其主要工作原理及防范措施。

答：反向映射探测扫描是一种主机扫描技术，主要用于探测被过滤设备或防火墙保护的网络或主机。攻击者构造可能的内部 IP 地址列表，并向这些地址发送数据包。当对方路由器接收到这些数据包时，会进行 IP 识别并路由，对不在其服务的范围的 IP 包发送 ICMP Host Unreachable 或 ICMP Time Exceeded 错误报文，没有接收到相应错误报文的 IP 地址可被认为在该网络中。其防范措施包括调整防火墙策略，使用状态机制丢弃错误状态的数据包；关闭过滤设备应答，无论地址正确与否均不发送回应；内部网络采用不可路由的保留地址等等。

9. 如何防范主机扫描？试列举几种常见的应对方法。

答：可以使用以下应对措施：1、使用可以检测并记录 ICMP 扫描的工具；2、使用入侵检测系统；3、在防火墙或路由器中设置允许进出自己网络的 ICMP 分组类型。

10. 何谓端口扫描技术？试列举几种常见的端口扫描方式。

答：端口扫描技术是一项自动探测本地和远程系统端口开放情况的策略及方法，它使用户了解系统目前向外界提供了哪些服务，从而为管理网络提供了一种手段。端口扫描向目标主机的 TCP/IP 服务端口发送探测数据包，并记录目标系统的响应，通过分析响应来判断服务端口是打开还是关闭，从而得知端口提供的服务或信息。常见的端口扫描方式包括开放扫描、半开放扫描和秘密扫描等等。

11. 简述开放扫描、半开放扫描和秘密扫描及各自特点。

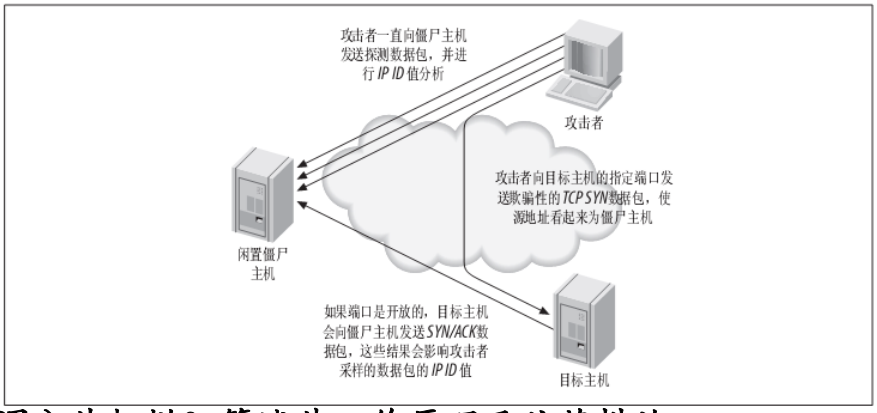
答：开放扫描是指通过三次握手过程与目标主机建立完整 TCP 连接的扫描方式。开放扫描具有很高的可靠性和可行性，不需要任

何系统特权；但会产生大量审计数据，很容易被发现。半开放扫描不需要完成整个三次握手过程，由于连接没有建立，所以称之为半开放扫描。半开放扫描通常不会被对方审计，隐蔽性有所提高；但部分扫描方式需要系统特权。秘密扫描或隐蔽扫描不包含标准 TCP 三次握手协议的任何部分，主要通过各种特殊标记位的数据包或其它方式实现。秘密扫描隐蔽性最好，但其数据包在通过网络时容易被丢弃，从而产生错误的探测信息，相对于其它两种扫描方式可靠性和可信度最低。

优缺点 / 端口扫描技术		优点	缺点
全连接扫描		扫描迅速、准确而且不需要任何权限	易被目标主机发觉而被过滤掉
半连接扫描		一般不会被目标主机记录连接，有利于不被扫描方发现	在大部分操作系统下，扫描主机需要构造适用于这种扫描的IP包，而通常情况下，构造自己的SYN数据包必须要有root权限
秘密扫描		能躲避 IDS、防火墙、包过滤器和日志审计，从而获取目标端口的开放或关闭的信息。没有包含 TCP 三次握手协议的任何部分，所以无法被记录下来，比半连接扫描要更为隐蔽	扫描结果的不可靠性增加，而且扫描主机也需要自己构造 IP 包
其它扫描	FTP 反弹攻击	能穿透防火墙，难以跟踪	速度慢且易被代理服务器发现并关闭代理功能
	UDP ICMP 端口不可到达扫描	可以扫描非 TCP 端口，避免了 TCP 的 IDS	由于是基于简单的 UDP 协议，扫描相对困难，速度很慢而且需要 root 权限

12. 何谓 IP ID 头扫描？简述其工作原理及防范措施。

答：由 Antirez 首先使用并在 Bugtraq 上公布。工作原理为：扫描主机通过伪造第三方主机 IP 地址向目标主机发起 SYN 扫描，并通过观察第三方主机 IP 序号的增长规律获取目标主机端口的状态。优点：不直接扫描目标主机也不直接和它进行连接，隐蔽性较好；缺点：对第三方主机的要求较高，并且要求 IP 序号有规律递增。防范措施包括使用防火墙或入侵检测系统禁止攻击者的探测数据包，或者采用随机生成 IP 包序号的 TCP/IP 实现方式。



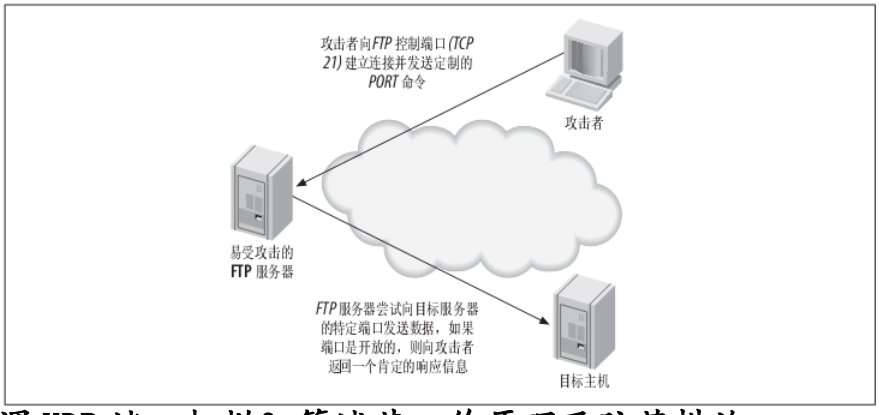
13. 何谓分片扫描？简述其工作原理及防范措施。

答：具有明显特征的探测包可能会被入侵检测系统拦截，因此可以将探测包分为若干个分片：既可以掩盖攻击特征，又可以逃避入侵检测系统拦截，因为处理过多数据包分片将大量消耗传感器

层的内存和 CPU 资源。等所有分片到达目标主机后，又会重新组装成为完整的探测包，实现扫描功能。防范措施包括直接丢弃分片数据包，或者采用代理检测防火墙重组、识别并丢弃探测包等等。

14. 何谓 FTP 跳板端口扫描？简述其工作原理及防范措施。

答：指利用 FTP 服务器在使用 PORT 命令处理连接时的漏洞对远程主机进行端口扫描的攻击方式。其过程如下：1、攻击者连接到准备用作跳板的存在漏洞的 FTP 服务器控制端口（TCP 21）并进入被动模式，迫使服务器使用 DTP（data transfer process，数据传输进程）发送数据到特定主机的特定端口；2、执行 PORT 命令，并向 FTP 服务传递一个参数，该参数指令向目标服务器的指定 TCP 端口建立连接；3、执行 PORT 命令之后，发送一个 LIST 命令，之后 FTP 服务器尝试与 PORT 命令中指定的目标主机建立连接；4、如果响应信息中包含 226，则表明目标主机的该端口是开放的；如果响应信息包含 425，则表明连接被拒绝。防范措施包括修补 FTP 服务器漏洞、在目标主机上配置防火墙禁止非法 FTP 流量等等。



15. 何谓 UDP 端口扫描？简述其工作原理及防范措施。

答：UDP 是一种无连接协议，可以采用两种方式有效枚举网络内可访问的 UDP 服务：1、发送 UDP 探测数据包到所有的 65535 个 UDP 端口，之后等待“ICMP 目的端口不可达”消息以识别不可达的 UDP 端口；2、使用特定的 UDP 服务客户端（如 snmpwalk、dig 或 tftp）发送 UDP 数据包到目标 UDP 网络服务，之后等待确定性的响应信息。UDP 端口扫描是一种反转扫描类型：开放端口没有响应信息；而关闭端口会由目标主机给出 ICMP 目标端口不可达信息。

16. 如何防范端口扫描？试列举几种常见的应对方法。

答：可以采用以下措施（包括但不限于）防范端口扫描：1、在边界路由器和防火墙处对入站的 ICMP 消息类型进行过滤，这将

迫使攻击者不得不对网络内的所有 IP 地址进行全方位的 TCP 端口扫描；2、在边界路由器和防火墙处过滤所有出站的 ICMP 类型 3 不可达消息，以防止 UDP 端口扫描和 firewalking 有效工作；3、考虑对 Internet 防火墙进行有效配置，使其能够识别端口扫描并据此阻断连接；4、进行扫描和探测演练，以评估网络防火墙和入侵检测系统等设备对分片 IP 数据包的处理方式；5、确保你的路由和过滤机制（防火墙和路由器）不会被攻击者使用特定的源端口或源路由技术绕过；6、确保防火墙对那些使用畸形的 PORT、PASV 等命令进行的状态欺骗攻击是无漏洞的。

17. 何谓操作系统扫描技术？试列举几种操作系统扫描方法。

答：指通过扫描方式确定目标主机的操作系统类型和版本的攻击技术。由于很多漏洞都是和操作系统密切相关的，准确识别操作系统既可以确定系统存在的漏洞，又可以有针对性地进行扫描提高效率。相关扫描方法只要包括获取标识信息、Windows API、TCP/IP 协议栈指纹以及其它识别方式（TTL）等等。

18. 何谓栈指纹技术？主动和被动栈指纹技术有何区别？

答：指利用 TCP/IP 协议栈实现上的特点来辨识一个操作系统。主动栈指纹技术寻找不同操作系统之间在处理网络数据包上的差异，并且把足够多的差异组合起来，以便精确地识别出一个系统的 OS 版本；被动栈指纹技术和主动栈指纹识别方法类似，但不是向目标系统发送分组，而是被动监测网络通信，以确定所用的操作系统。

19. 如何防范操作系统扫描？试列举几种常见的应对方法。

答：可以使用以下应对措施：1、端口扫描监测工具监视操作系统检测活动；2、让操作系统识别失效的补丁：修改 OS 的源代码或改动某个 OS 参数以达到改变单个独特的协议栈特征的目的；3、防火墙和路由器的规则配置；4、使用入侵检测系统。

20. 何谓延时扫描和分布式扫描？有何实际意义？

答：各 IDS 常采用判断在某个时间段内特定主机对本地端口的访问频度是否大于事先预定阈值的方法来识别入侵。延时扫描加大各连接之间的时间间隔来逃避检测，虽然比较有效但是延缓了扫描速度。分布式扫描通过把扫描任务分配到不同地理位置和网络拓扑分布的扫描主机上，在解决连接数问题的同时也加速了扫描进度，另外还避免了大量信息收集时单机扫描面临的主机负载和网络负载过重的问题。

21. 何谓查点（Enumeration）？查点和扫描有何区别？

答：如果黑客从一开始的目标探测中没有找到任何可以直接利用的入侵途径，他就会转向收集目标有效的用户账号或保护不当的共享资源，这就是查点(enumeration)。与扫描不同，查点通常针对特定操作系统进行，要对目标系统进行连接和查询，有可能会被目标系统记录。

22. 在 Windows 和 Unix 系统中如何防止查点?

答: 对于 Windows 系统，需要在路由器、防火墙或其他网络关口设置，不允许对 TCP 和 UDP 的 135～139 端口的访问; 在 Windows 2000 系统中，还要禁止 445 端口; 限制匿名连接; 隐藏应用程序标记中的厂商和版本信息; 定期使用端口扫描和 netcat 工具连接活动端口进行网络系统检查，确保没有泄露信息; 锁定注册表，禁止对其进行远程访问。对于 Unix 系统，需要在防火墙或路由器中阻塞对特定端口如(79)的访问; 清除服务程序的标记; 尽可能对服务程序进行升级。

23. 简述 IPC$空会话攻击的一般过程及攻击成功的前提条件。

答: 攻击过程一般如下: 1、利用扫描器得知对方已打开 139 端口; 2、考虑用空会话进行远程密码猜测; 3、映射驱动器，安装后门服务器; 4、远程启动后门服务器，并添加每日运行计划; 5、获取服务器 IP 地址，通过客户端与之建立连接，提升权限并进行后续工作。根据上述过程可知，攻击成功的前提条件包括: 目标主机开放 139 端口; 远程密码复杂度不高易于猜解; 共享驱动器资源(包括管理共享); 缺乏或配置不当的安全机制(防火墙、入侵检测系统)等等。

24. 何谓载波侦听/冲突检测(CSMA/CD)? 何谓网卡的混杂模式?

答: 载波侦听指站点在传输数据前首先监听信道是否空闲: 如果信道空闲就传输自己的数据; 如果信道被占用就等待信道空闲后再传输。冲突检测指为防止两个站点同时监测到网络空闲时可能产生的数据传输冲突，可以采用某种退避算法延迟数据传输从而避开冲突。在正常模式(非混杂模式)下，网卡只接收广播包和 MAC 地址与自己相匹配的数据帧; 但在混杂模式下，无论数据帧中的地址是否与自己匹配，网卡会接收所有的数据帧。为了实现网络监听，网卡必须被配置为混杂模式。

25. 共享网络和交换网络在实现数据包转发上有何区别?

答: 在共享网络中，由于每个数据包被发送到所有站点，因此很容易实现网络监听: 只需要将网卡设置为混杂工作模式即可; 但在交换网络中，交换机通过 MAC-端口映射表将数据包只发送到特定端口上，此时为实现网络监听，除了要配置网卡为混杂模式外，还要采用 ARP 重定向技术实施 ARP 欺骗。

26. 何谓 ARP 重定向技术? 如何在交换网络上实现监听?

答: ARP 重定向技术是一种改变数据包正常流向的中间人攻击方法。假使两台主机 A、B 通过交换机 G 连接，由于交换机 G 通过 MAC-端口映射表转发数据包，此时主机 A、B 均无法监听对方的通信流量。假设主机 B 需要监听主机 A，除了将网卡设为混杂模式外，还需按以下步骤实施 ARP 欺骗: 1、主机 B 打开 IP 转发功能; 2、主机 B 发送假冒的 ARP 包给主机 A，声称自己是交换机 G 的 IP 地址; 3、如果欺骗成功，主机 A 发往外部的数据包会首先

发给主机 B;4、主机 B 监听后再将数据包转发给真正的交换机 G。

27. 如何防范网络监听？试列举几种常见的检测手段。

答：处于混杂模式的网卡和操作系统会有一些不同的行为，利用这些特征可以判断机器是否运行在混杂模式下。常见的检测手段包括：1、观测 DNS：很多网络监听软件会尝试进行地址反向解析，可以观测 DNS 上是否有明显增多的解析请求；2、操作系统特征：Linux 内核在正常情况下只处理本机 MAC 地址或者以太广播地址的包，在混杂模式下许多版本的 Linux 内核只检查数据包中的 IP 地址以确定是否送到 IP 堆栈。因此可以构造无效以太地址而 IP 地址有效的 ICMP ECHO 请求，看机器是否返回应答包(混杂模式)，或忽略(非混杂模式)。Windows 9x/NT 在混杂模式下检查一个包是否为以太广播包时只看 MAC 地址前八位是否为 0xff，可根据类似原理进行检测；3、网络和主机性能：向本地网络发送大量的伪造数据包，然后看目标主机的响应时间是否大于基准或平均值；4、利用反监听软件工具，例如 L0pht 的 AntiSniff 产品等等。

第四章　网络防火墙技术

1. 简述防火墙在安全方面的主要功能和局限性。

   答：从防火墙的功能来说，主要包含以下几个方面：访问控制，（如应用 ACL 进行访问控制）、攻击防范（如防止 SYN FLOOD 等）、NAT、VPN、路由、认证和加密、日志记录、支持网管等。防火墙的功能为：通过防火墙可以定义一个关键点以控制网络访问；监控网络的安全并在异常情况下给出报警提示，必要时应做日志登记；提供网络地址转换（NAT）功能，有助于缓解 IP 地址资源紧张的问题；同时可以避免当一个内部网更换 ISP 时需重新编号的麻烦；防火墙可查询或登记因特网的使用情况，可以确认因特网连入的代价、潜在的带宽瓶须，以使费用的耗费满足企业内部财政模式；防火墙是为客户提供服务的理想位置，即在其上可以配置相应的 WWW 和 FTP 服务，使因特网用户仅可以访问此类服务，而禁止对保护网络的其他系统的访问。局限性：存在着一些防火墙不能防范的安全威胁，如防火墙不能防范不经过防火墙的攻击，也防火墙很难防范来自于网络内部的攻击以及病毒的威胁。

2. 按照保护对象的不同，防火墙可分为哪几种主要类别？

   答：按照保护对象的不同可以分为网络防火墙和单机防火墙。

3. 何谓主机防火墙和网络防火墙？试对比二者主要区别。

   答：主机防火墙是以软件形式运行在普通计算机之上的保护单台主机的安全，是一个软件程序；网络防火墙是一个基于网络的防火墙设备，其从未被授权的访问中保护一个计算机网络。网络防火墙可能是硬件设备，软件程序或两者的结合。通常，一个网络防火墙保护一个内部计算机网络不受外界的恶意访问，也可能也被设定来限制内部用户到外部的访问。最常用形式的网络防火墙是一个代理服务器。区别：主机防火墙是保护单台主机，安全策略分散，安全功能简单，可以普通用户维护，虽然策略设置灵活，但安全隐患较大。网络防火墙是保护整个网络，安全策略集中，安全功能复杂多样，需要专业管理员维护，虽然策略设置复杂，但安全隐患小。

4. 何谓硬件防火墙和软件防火墙？试对比二者主要区别。

   答：硬件防火墙：硬件和软件都需要单独设计，有专用网络芯片来处理数据包；同时采用专门的操作系统平台，从而避免通用操作系统的安全性漏洞。对软硬件的特殊要求，使硬件防火墙的实际带宽与理论值基本一致，有着高吞吐量、安全与速度兼顾的优点。具体特点：1、安全性完全取决于专用的 OS；2、网络适应性强（支持多种接入模式）；3、稳定性较高；4、升级、更新不太灵活。软件防火墙：安装在 PC 平台的软件产品，它通过在操作系统底层工作来实现网络管理和防御功能的优化吞吐量不高，容易造成带宽瓶颈。并且 pc 架构本身就不稳定，更不可能长时间运行。这种防火墙一般只能满足中低带宽的安全要求，在高流量环境下往往会造成网络堵塞甚至系统崩溃。具体特点：1、仅获得

Firewall 软件，需要准备额外的 OS 平台；2、安全性依赖低层的 OS；3、网络适应性弱（主要以路由模式工作）；4、稳定性高；5、软件分发、升级比较方便。

5. 按照体系结构的差异，防火墙可分为哪几种主要类别？

答：按照体系结构的差异，防火墙可以分为以下四种类型：1、分组过滤防火墙，仅仅根据 TCP/IP 层策略实现简单的分组过滤功能；2、双宿主机防火墙，通过双宿主机实现分组过滤和转发处理；3、屏蔽主机防火墙，通过路由器策略将进出内网的通信流量全部集中到双宿堡垒主机上，再由后者转发至路由器或其它内网主机；4、屏蔽子网防火墙：在内外网之间分别设置内网防火墙和外网防火墙，堡垒主机置于内外防火墙之间。

6. 何谓分组过滤防火墙？试简述其优缺点。

答：分组过滤防火墙也称包过滤防火墙，作用在网络层和传输层，根据分组包头源地址、目的地址、端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的地出口端，其余数据包则被从数据流中丢弃。包过滤防火墙的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其弱点也很明显：据以过滤判别的只有网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大地影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC 一类的协议；另外，大多数过滤器中缺少审计和报警机制，且管理方式和用户界面较差；对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统。

7. 何谓双宿主机防火墙？试简述其优缺点。

答：双宿主机防火墙是指用一台装有两个网络适配器的双宿主机做防火墙。双宿主机用两个网络适配器分别连接两个网络，又称堡垒主机。堡垒主机上运行着防火墙软件（通常是代理服务器），可以转发应用程序，提供服务等。双宿主机网关有一个致命弱点，一旦入侵者侵入堡垒主机并使该主机只具有路由器功能，则任何网上用户均可以随便访问有保护的内部网络。

8. 何谓屏蔽主机防火墙？试简述其优缺点。

答：屏蔽主机防火墙由包过滤路由器和堡垒主机（Bastion Host）组成，它所提供的安全性能要比包过滤防火墙系统要强，因为它实现了网络层安全（包过滤）和应用层安全（代理服务）的结合。当入侵者在破坏内部网络的安全性之前，必须首先突破这两种不同的安全系统。优点：1、配置更为灵活，它可以通过配置过滤路由器将某些通信直接传到内部网络的其它站点而不是堡垒主机；2、包过滤路由器的规则较简单。缺点：一旦堡垒主机被攻破，内部网络将完全暴露。

9. 何谓屏蔽子网防火墙？试简述其优缺点。

答：屏蔽子网防火墙是在屏蔽主机网关防火墙的配置上加上另一个包过滤路由器，利用两台屏蔽路由器把子网与内外部网络隔离开，堡垒主机、信息服务器、Modem 组，以及其他公用服务器放在该子网中，这个子网称为“停火区”或“非军事区”（DeMilitarised Zone，DMZ）。优点:提供多层保护，一个入侵者必须通过两个路由器和一个应用网关，是目前最为安全的防火墙系统；缺点:1、价格较贵；2、整个系统的配置较为困难。该防火墙适合大、中型企业以及对安全性要求高的单位。

10. 何谓非军事区（DMZ）？试简述其主要用途。

答：全称 Demilitarized Zone(隔离区或非军事化区)。在技术领域，DMZ 最初被定义为防火墙外部接口与外部（往往是 Internet）路由器的内部接口之间的网段。另外还有个新的含义是：给不可信系统的隔离网段提供服务。这种术语被 IT 专业人士用来指代两个防火墙之间的网段，或者是与防火墙相连的“死端”（Dead-end）或“侧翼”（Wing）网络。该功能主要是为了解决安装防火墙之后外部网络不能访问局域网服务器的问题，比如 FTP 服务器、视频会议、网络游戏等，DMZ 其实就相当于一个网络缓冲区，通过该区域可以有效保护内部网络。

11. 按照实现技术的不同，防火墙可分为哪几种主要类型？

答：按照实现技术的不同，防火墙可以分为以下五种类型：1、分组过滤防火墙，根据 TCP/IP 层策略对分组进行过滤；2、状态分组过滤防火墙，在分组过滤的基础上建立动态连接状态表；3、应用代理防火墙，根据应用层策略对分组数据进行检查过滤；4、复合型防火墙，同时根据 TCP/IP 层策略和应用层策略分别对分组报头和分组数据进行检查过滤；5、核检测防火墙，在复合型防火墙的基础上增加了对完整会话的检测。

12. 何谓数据包过滤防火墙技术？试简述其优缺点。

答：包过滤技术是防火墙最基本的实现技术，具有包过滤技术的装置是用来控制内、外网络数据流入和流出。包过滤技术的数据包大部分是基于 TCP/IP 协议平台的，对数据流的每个包进行检查，根据数据报的源地址、目的地址、TCP 和 IP 端口号，以及 TCP 的其它状态来确定是否允许数据包通过。优点：1、速度快性能高；2、对应用程序透明。缺点：1、安全性低；2、不能根据状态信息进行控制；3、不能处理网络层以上的信息；4、伸缩性差；5、维护不直观。

13. 何谓应用代理防火墙技术？试简述其优缺点。

答：应用代理型防火墙是工作在 OSI 的最高层，即应用层。其特点是完全"阻隔"了网络通信流，通过对每种应用服务编制专门的代理程序实现监视和控制应用层通信流的作用。优点：1、安全性高；2、提供应用层的安全。缺点：1、性能差；2、伸缩性差；

3、只支持有限的应用；4、不透明。

14. 何谓状态检测防火墙技术？试简述其优缺点。

答：状态检测技术主要是通过对 IP 层或 TCP 层的部分状态标志进行检测，来决定是拒绝还是允许数据包通过。状态检测技术采用的是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。优点：1、安全性高：a)能够检测所有进入防火墙网关的数据包；b)根据通信和应用程序状态确定是否允许包的通行；2、性能高：在数据包进入防火墙时就进行识别和判断；3、伸缩性好：a)可以识别不同的数据包；b)已经支持 160 多种应用；c)用户可方便添加新应用；4、对用户、应用程序透明。缺点：应用层控制很弱。

15. 何谓复合型防火墙技术？试简述其优缺点。

答：复合型防火墙将包过滤和代理服务两种方法结合起来，形成新的防火墙，由堡垒主机提供代理服务。优缺点：可以检查整个数据包内容，根据需要建立连接状态表，网络层保护强，应用层控制细，会话控制较弱。

16. 何谓核检测防火墙技术？试简述其优缺点。

答：核检测技术是一种基于操作系统内核的会话检测技术。来自网络的数据包经底层网络设备到达本地主机后，在操作系统内核进行高层应用协议的还原。在会话检测方面，当客户端发起一个访问请求提交给防火墙以后，防火墙可以模拟成服务器端在必要的时候利用内核对高层协议进行还原，并与预先制定的安全策略进行匹配，如果符合就将数据重新封包转发给服务器，同样对于服务器返回的数据信息也是经过上述过程转发给客户端。由此来看，应用核检测技术的防火墙在操作系统内核模拟出典型的应用层协议，在内核实现了对应用层协议的过滤。优缺点：1、网络层保护强；2、应用层保护强；3、会话保护很强；4、在操作系统内核完成应用协议的还原，极大的提高了系统的整体性能。

17. 何谓网络地址转换（NAT）技术？试简述其主要用途。

答：NAT 英文全称是 Network Address Translation，是网络地址转换。作为 IETF 标准，NAT 允许一个机构以一个地址出现在目前 Internet 上。NAT 将每个局域网节点的地址转换成一个 IP 地址，反之亦然。应用到防火墙技术中，把个别 IP 地址隐藏起来不被外界发现，使外界无法直接访问内部网络设备；同时还有助于缓解网络 IP 地址趋于紧张的局面，合理安排网络中的公有 Internet 地址和私有 IP 地址的使用。

18. 何谓端口地址转换（PAT）技术？试简述其主要用途。

答：PAT(Port Address Translation)也称为 NAPT，是一种动态地址转换，允许多个内部本地地址共用一个外部合法地址，用不同的协议端口号映射不同内部网络地址。PAT 理论上可以支持

64500 个 TCP／IP、UDP／IP 连接，但实际可以支持的工作站数约 4000。因为许多 Internet 应用如 HTTP，实际上由许多小的连接组成。PAT 大量应用在远程访问中，特别是在远程拨号用户使用的设备中。使用 PAT 时，所有不同的 TCP 和 UDP 信息流仿佛都来源于同一个 IP 地址。虽然这样会导致信道的拥塞，但由于节省了上网费用、注册 IP 地址、易管理的特点，对只申请到少量 IP 地址但却经常同时有多个用户上外部网络的情况，这种转换是十分有用的。

19. 何谓静态地址转换（SNAT）和动态地址转换（DNAT）？

答：静态转换是一种简单的转换方式，它在 NAT 表中为每一个需要转换的内部地址创建了固定的转换条目，映射了唯一的全局地址。内部地址与全局地址一一对应，每当内部节点与外界通信时，内部地址就会转化为对应的全局地址。动态转换提供了很大的灵活性，它将可用的全局地址地址集定义成 NAT 池（NAT pool）。对于要与外界进行通信的内部节点，如果还没有建立转换映射，边缘路由器或者防火墙将会动态的从 NAT 池中选择全局地址对内部地址进行转化。每个转换条目在连接建立时动态建立，而在连接终止时会被回收。这样网络的灵活性大大增强了，所需要的全局地址进一步减少。值得注意的是，当 NAT 池中的全局地址被全部占用以后，以后的地址转换的申请会被拒绝。这样会造成网络连通性的问题。所以应该使用超时操作选项来回收 NAT 池的全局地址。

20. 何谓源网络地址转换和目标网络地址转换？简述其应用场合。

答：源网络地址转换修改数据报 IP 头部中的数据源地址（通常是把私有地址译为合法的因特网地址）。源地址转换主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。目标网络地址转换修改数据报 IP 头部中的数据目的地址（通常发生在防火墙之后的服务器上）。目的地址转换可分为目标地址映射、目标端口映射、服务器负载均衡等。目的地址转换也称为反向地址转换或地址映射。目的地址转换是一种单向的针对目标地址的映射，主要用于内部服务器向外部提供服务的情况，它与静态地址转换的区别在于它是单向的。外部可以主动访问内部，内部却不可以主动访问外部。另外，可使用目的地址转换实现负载均衡的功能，即可以将一个目标地址转换为多个内部服务器地址，也可以通过端口的映射将不同的端口映射到不同的机器上。

21. 何谓通信日志、命令日志、访问日志、内容日志？简述其特点。

答：通信日志即传统日志，记录通信源地址、目的地址、源目端口、通信时间、通信协议、字节数、是否允许通过；应用层命令日志：在通信日志的基础之上记录各个应用层命令及其参数，如 HTTP 请求及其要取的网页名；访问日志在通信日志的基础上记录用户对网络资源的访问，它和应用层命令日志的区别在于：应用层命令日志可以记录下大量的数据，有些用户可能不需要，如协商通信参数过程等。例如针对 FTP 协议，访问日志只记录下读、

写文件的动作；内容日志在应用层命令日志的基础上还记录用户传输的内容，如用户发送的邮件，用户取下的网页等。因为涉及隐私问题，在普通的防火墙中并不包含这一功能。

22. 何谓状态传输协议（STP）？什么时候需要防火墙支持该协议？

答：STP 的全称是 State Transport Protocol。若防火墙部署为双机热备模式，两台防火墙之间通过 STP 协议保持连接状态表同步。这样当一台防火墙故障时，这台防火墙的连接不需要重新建立就可以透明地迁移到另一台防火墙上，用户不会察觉到。

23. 何谓防火墙与入侵检测系统的安全联动？简述其工作过程。

答：防火墙是访问控制设备，安置在不同安全领域的接口处，其主要目的是根据网络的安全策略，按照经过的网络流量，而这种控制通常基于 IP 地址、端口、协议类型或应用代理。包过滤、网络地址转换、应用代理和日志审计是防火墙的基本功能。IDS 不同于防火墙，它不是网络控制设备，不对通信流量做任何限制。它采用的是一种动态的安全防护技术，通过监视网络资源（网络数据包、系统日志、文件和用户活动的状态行为），主动寻找分析入侵行为的迹象，一旦发现入侵，立即进行日志、告警和安全控制操作等，从而给网络系统提供对外部攻击、内部攻击和误操作的安全保护。防火墙不识别网络流量，只要是经过合法通道的网络攻击，防火墙无能为力。防火墙和 IDS 的功能特点和局限性决定了它们彼此非常需要对方，且不可能相互取代，原因在于防火墙侧重于控制，IDS 侧重于主动发现入侵的信号。而且，它们本身所具有的强大功效仍没有充分发挥。例如，IDS 检测到一种攻击行为，如不能及时有效地阻断或者过滤，这种攻击行为仍将对网络应用造成损害；没有 IDS，一些攻击会利用防火墙合法的通道进入网络。因此，防火墙和 IDS 之间十分合适建立紧密的联动关系，以将两者的能力充分发挥出来，相互弥补不足，相互提供保护。从信息安全整体防御的角度出发，这种联动是十分必要的，极大地提高了网络安全体系的防护能力。工作过程：互联网上的黑客开始对受保护网络内的主机发动攻击，这时位于网络监听状态的入侵检测系统检测到黑客对内网主机的攻击行为后，入侵检测系统通过它与防火墙之间的‘公共语言’发送通知报文通知防火墙，防火墙收到并验证报文后生成动态规则实现对攻击行为的控制和阻断。联动控制是基于客户服务器模式，通过扩展入侵检测系统和防火墙的功能，在防火墙中驻留一个 Server 程序，在 IDS 端驻留一个 Client 端程序，Client 端在发现需防火墙阻断的攻击行为后，产生控制信息，将控制信息传送给 Server 端，Server 端接到 Client 的控制消息后，动态生成防火墙的过滤规则，最终实现联动，拦截攻击后且攻击停止时，添加的防火墙规则自动超时删除。

24. 何谓防火墙与病毒检测服务器的安全联动？简述其工作过程。

答：防火墙通常被用来进行网络安全边界的防护。事实证明，在内网中不同安全级别的安全域之间采用防火墙进行安全防护，不

但能保证各安全域之间相对安全，同时对于网络日常运行中，各安全域中访问的权限的调整提供了便利条件。但防火墙不识别网络流量，只要是经过合法通道的网络攻击，防火墙无能为力。利用网关防病毒系统将病毒尽最大可能的拦截在网络外部，同时在网络内部采用全方位的病毒检测服务器进行全网的病毒防范，对网络中病毒的防护状况做实时监控，针对服务器采用专有的服务器防病毒客户端，同时保证全网病毒防护系统做到统一管理和病毒防护策略的统一。防火墙与病毒检测服务器的工作过程：1、病毒检测服务器作为防病毒软件的控制中心，及时通过 INTERNET 更新病毒库，并强制局域网中已开机的终端及时更新病毒库软件；2、记录各个终端的病毒库升级情况 3、记录局域网中计算机病毒出现的时间、类型对防火墙的策略进行修改阻止黑客的入侵。

25. 何谓源目地址路由技术？什么时候需要防火墙支持该协议？

答：一般的路由技术只根据目标地址来做出路由选择，而目标地址在互联网是唯一的，只是访问的源地址不一样。然而防火墙可以根据通讯的源地址和目标地址来做出路由选择。这种源和目的双地址路由技术可以很好的适应有多个网络出口的环境，从而大大的降低了网络安全建设的成本。防火墙根据数据包的源地址和目的地址，匹配防火墙路由表，决定数据包的下一跳网关，这样可以保证网络资源的充分利用。同时，防火墙的源目的双地址路由功能还有一个特点，就是防火墙的路由表里在不包含防火墙自身接口的源地址路由的情况下，防火墙可以为内部网络与互联网搭起桥梁。也就是说，防火墙为内网提供了到互联网的访问，而互联网却不能访问到防火墙，这也是防火墙实现自身保护的一个很好措施。

26. 何谓 IP/MAC 地址绑定技术和 IP/用户绑定技术？简述其特点。

答：IP/MAC 地址绑定技术：为了防止内部人员进行非法 IP 盗用(例如盗用权限更高人员的 IP 地址，以获得权限外的信息)，可以将内部网络的 IP 地址与 MAC 地址绑定，盗用者即使修改了 IP 地址，也因 MAC 地址不匹配而盗用失败。由于网卡 MAC 地址的唯一确定性，可以根据 MAC 地址查出使用该 MAC 地址的网卡，进而查出非法盗用者。特点：绑定 MAC 地址和 IP 地址可以防止内部 IP 地址被盗用，但实际上由于各层协议以及网卡驱动等实现技术，MAC 地址与 IP 地址的绑定存在很大的缺陷，还不能真正防止内部 IP 地址被盗用。IP/用户绑定技术：在用户上网的认证过程中，可以通过设置 DHCP Relay 来控制用户获得 IP 地址的过程，实现将用户与 IP 地址绑定，防止手工配置 IP 地址来上网等手段的欺骗。在一些二层交换机上也可实现用户的 IP 地址与用户进行绑定，达到标识和管理用户的目的。

27. 何谓端口映射（MAP）功能？对于网络安全性有何意义？

答：端口映射可以实现从 Internet 到局域网内部机器的特定端口服务的访问。利用端口映射功能可以为内部的服务器建立静态

映射，以方便外部用户访问该服务器，同时对一些知名端口如80、21可以被映射到服务器上任意一个端口，以提高安全性。

28. 何谓SYN代理技术？解释其防御SYN洪泛攻击的工作过程。

答：SYN代理技术是指防火墙作为TCP连接代理，既代表服务器响应客户机连接请求，又代表客户机向服务器发起请求并最终完成连接过程。其工作过程如下：1、当客户机向服务器发送SYN连接请求包时，该包首先被防火墙截获；2、防火墙代表服务器向客户机返回SYN+ACK确认包；3、若防火墙没有在规定时间间隔内收到客户端的ACK确认包，则删除半连接状态；否则代表客户机向服务器发送SYN连接请求包；4、服务器向防火墙返回SYN+ACK确认包；5、防火墙向服务器发送最终ACK确认包完成连接过程。SYN洪泛攻击通常向服务器滥发SYN连接请求包，使后者维持大量半连接状态并消耗过多资源，可能导致服务质量降低甚至DoS攻击。通过SYN代理技术，防火墙可以处理并过滤绝大多数攻击性SYN连接请求包，保证服务器不受攻击，从而保证其可用性和可靠性。

29. 何谓防火墙的透明接入模式和路由接入模式？简述各自特点。

答：在透明接入模式：防火墙作为一个实际存在的物理设备，要想放入已存在地网络中又不对网络有任何影响，即以网桥的方式置入网络，用户将不必重新设定和修改路由，也不需要知道防火墙的位置，防火墙就可以直接安装和放置到网络中使用。与路由模式相同，IP报文同样经过相关的过滤检查（但是IP报文中的源或目的地址不会改变），内部网络用户依旧受到防火墙的保护。路由模式：当防火墙位于内部网络和外部网络之间时，需要将防火墙与内部网络、外部网络以及DMZ三个区域相连的接口分别配置成不同网段的IP地址，重新规划原有的网络拓扑，此时相当于一台路由器，采用路由模式时，可以完成ACL包过滤、ASPF动态过滤、NAT转换等功能。然而，路由模式需要对网络拓扑进行修改（内部网络用户需要更改网关、路由器需要更改路由配置等）。

30. 防火墙备份和均衡有何异同？对于状态同步有何具体要求？

答：防火墙备份指两台或多台防火墙中只有一台主防火墙在工作，当其出现故障时由其它备份防火墙接替工作，因此主防火墙和备份防火墙之间需要保持状态同步，以便实现透明的连接迁移和处理。防火墙均衡指两台或多台防火墙同时处于工作状态，当其中一台防火墙失效后其通信连接全部中断，需要重新通过其它防火墙建立网络连接，因此均衡防火墙之间无需进行状态同步。

31. 简述Iptables防火墙的表、链组织结构及各表、链主要功能。

答：Iptables是基于内核的防火墙，内置了filter，nat和mangle三张表：1、filter表负责数据包过滤，包括INPUT、OUTPUT和FORWARD三条规则链；2、nat表涉及网络地址转换，包括PREROUTING、POSTROUTING和OUTPUT三条规则链；3、mangle

表主要用于修改数据包内容进行流量整形，默认的规则链有INPUT，OUTPUT，NAT，POSTROUTING，PREROUTING。INPUT 链：当收到访问防火墙本机的数据包(入站)时，应用此链中的规则；OUTPUT 链：当防火墙本机向外发送数据包（出站）时，应用此链中的规则；FORWARD 链：收到需要通过防火墙发送给其他地址的数据包，应用此链；PREROUTING 链：做路由选择之前，应用此链；POSTROUTING 链：对数据包做路由选择之后，应用此链。

32. 简述 Iptables 防火墙对本机非转发数据包的处理流程。

答：来自外界的数据包到达防火墙，首先被 PREROUTING 规则链处理（是否被修改地址），之后会进行路由选择（判断该数据包应该发往何处），如果数据包的目标地址是防火墙本机，那么内核将其传递给 INPUT 链进行处理，通过以后再交给上次的应用程序进行响应。

33. 写出仅允许开放本机 http 服务的 Iptables 配置指令。

答：
```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
```

34. 写出禁止外网 ping 通本机的 Iptables 配置指令。

答：
```
iptables -A OUTPUT -p icmp -d 127.0.0.1/24 -j DROP
```

35. 简述 Iptables 防火墙的状态机制及状态转换过程。

答：Iptables 防火墙的状态机制其实是一种连接跟踪机制。该机制中数据包共分为四种状态：NEW 状态：当防火墙第一次看到某个数据包时，该数据包为 NEW 状态；ESTABLISHED 状态：若防火墙看到对某个 NEW 状态数据包的应答包（包括否定应答）时，该应答包及该连接上的后续数据包均为 ESTABLISHED 状态；RELATED 状态：如果数据包与现有某个连接存在关联关系，该数据包即为 RELATED 状态；INVALID 状态：若防火墙不能识别数据包属于哪个连接或者不能确定数据包状态，该数据包即为 INVALID 状态。

就状态转换而言：第一次看到的数据包为 NEW 状态；看到对该数据包的应答即转换为 ESTABLISHED 状态；由某个现有 ESTABLISHED 状态的连接创建或与之相关联的新连接为 RELATED 状态；其它均为 INVALID 状态。

36. 写出禁止本机主动向外发起 TCP 连接的 Iptables 配置指令。

答：
```
iptables -A OUTPUT -p tcp -j DROP
```

37. 何谓主动 FTP 模式和被动 FTP 模式？试对比其特点。

答：主动 FTP 模式是指由 FTP 服务器主动向客户端发起数据连接，一般使用 20 端口；被动 FTP 模式是指 FTP 服务器被动接受客户端发起的数据连接，一般使用随机端口。主动模式因为要自外向内主动穿透防火墙，可能会被防火墙拦截；被动模式则自内向外

发起连接，一般不存在上述问题。

38. 写出允许开放本机 ftp 服务的 Iptables 配置指令。

答: iptables -A INPUT -p tcp -m multiport --dports 20,21 -j ACCEPT

iptables -A OUTPUT -p tcp -m multiport --sports 20,21 -j ACCEPT

39. 写出允许本机访问 ftp 服务的 Iptables 配置指令。

答: iptables -A INPUT -p tcp -d 127.0.0.1/24 --dports 20,21 -j ACCEPT

iptables -A OUTPUT -p tcp -d 127.0.0.1/24 --sports 20,21 -j ACCEPT

第五章　入侵检测技术

1. 何谓入侵检测系统？与防火墙系统有何异同？

   答:入侵检测系统指对网络或计算机通信或活动进行监视和分析，借以发现已知或未知的入侵、攻击及滥用行为，并采取一定反制措施的一系列硬件或软件子系统的有机组合。入侵检测系统是对防火墙的有益补充，二者都用于保障网络或系统安全，部分功能是允许冗余的。二者的主要区别在于防火墙属于被动防御措施，而入侵检测系统属于主动防御措施；此外防火墙只能够防止外来攻击，对内部攻击无能为力；入侵检测系统不仅能够防御外来攻击，也同样能够检测内部攻击。

2. 简述入侵检测系统的三大功能组件。

   答：入侵检测系统包括三大功能组件：1、信息收集部件：按照某种安全策略或设置，从其所监控的网络或主机收集各种相关的通信及系统活动信息，形成初始的事件纪录；2、信息分析部件：对原始事件纪录进行整理和分析，按照某种方法（异常检测或误用检测）判断是否存在入侵行为；3、结果处理部件：按照既定安全策略，根据分析结果进行相应处理，包括对入侵行为的记录、告警、反制等措施。

3. 入侵检测系统有哪些主要功能？

   答：入侵检测系统主要包含以下功能：监控用户和系统的活动、查找非法用户和合法用户的越权操作、检测系统配置的正确性和安全漏洞、评估关键系统和数据的完整性、识别攻击的活动模式并向网管人员报警、对用户的非正常活动进行统计分析，发现入侵行为的规律、操作系统审计跟踪管理，识别违反政策的用户活动以及检查系统程序和数据的一致性与正确性等等。

4. 简述 Denning 入侵检测模型，并分析其特点。

   答：1987 年 Dorothy E.Denning 提出了异常入侵检测系统的抽象模型，首次将入侵检测概念作为一种计算机系统安全防御的措施提出，是谓之 Denning 入侵检测模型。Denning 模型包含六个主要元素：主体：系统活动的发起者，用户或进程；客体：主体的操纵对象，资源或设备；审计记录：主体对客体的操作过程在目标系统上产生的对应纪录，是由<主体、活动、客体、异常条件、资源使用、时间戳>构成的六元组；行为轮廓：指描述主体对客体正常行为的模型，包含系统正常活动的各种相关信息；异常纪录：指当系统检测到异常行为时产生的纪录，由事件、时间戳、行为轮廓组成；活动规则：指系统判断是否是入侵行为的准则，以及当满足入侵条件时系统所采取的相应对策。Denning 模型是典型的异常检测原型，在入侵行为是异常行为子集的前提条件下，具有漏检率低、误检率高的明显特点。

5. 简述 CIDF 入侵检测模型，并分析其特点。

答：CIDF 模型是由 CIDF（Common Intrusion Detection Framework）工作组提出的通用入侵检测模型，它将入侵检测系统分为四个单元：1、事件产生器：负责从整个计算环境中获得事件，并向系统其它部分提供此事件；2、事件分析器：负责分析所得到的事件，并产生分析结果；3、响应单元：负责对分析结果作出反应的单元，可以只是简单的报警或是联动其它安全子系统实施反击；4、事件数据库：负责存放各种中间结果和最终数据，可以是复杂的数据库或是简单的文本文件。各功能单元之间的数据交换采用通用入侵描述语言（Common Intrusion Specification Language）实现。CIDF 模型给出了入侵检测系统的基本框架，并不涉及任何具体的检测技术，实际结构则因各种网络环境的差异和安全需求的不同而有所差别。

6. 常见的入侵检测系统分类标准有哪些？简单列举其分类结果。

答：通常存在以下分类标准：1、按照防护对象，可分为网络入侵检测系统和主机入侵检测系统；2、按照检测时效，可分为在线入侵检测系统和离线入侵检测系统；3、按照系统结构，可分为集中式入侵检测系统和分布式入侵检测系统；4、按照检测技术，可分为基于异常检测的入侵检测系统和基于误用检测的入侵检测系统。

7. 何谓集中式 IDS 和分布式 IDS？简单对比二者特点。

答：集中式 IDS 有多个分布于不同主机上的审计程序，但只有一个中央入侵检测服务器。审计程序把当地收集到的数据踪迹发送给中央服务器进行分析处理；其可伸缩性和可配置性较差，但监控主机负载较轻，对性能影响不大。分布式 IDS 则将中央入侵检测服务器的任务分配给多个 HIDS 执行，各 HIDS 不分等级，各自负责监控当地主机的可疑活动；其可伸缩性和可配置性较好，安全性高，但维护成本高，并且监控主机的负载较重。

8. 何谓在线 IDS 和离线 IDS？简单对比二者特点。

答：在线 IDS 工作在实时状态，在数据产生或发生改变的同时对其进行分析处理，特点是反应迅速、能够及时保护系统，但当系统规模较大时实时性难以得到实际保障。离线 IDS 工作在非实时状态，在行为发生后对产生的数据进行分析处理，特点是成本低，可以分析大量事件和长期情况，但无法提供及时保护，具有滞后性。

9. 何谓网络 IDS 和主机 IDS？简单对比二者特点。

答：网络 IDS 通常部署在网络入口处、防火墙之后，一般安装为旁路模式，避免成为系统瓶颈，其保护范围为整个内部网络。网络 IDS 能够来自网络的外部攻击和来自内部的滥用行为，既不需要改变其它设备的配置也无需在其它主机中安装额外软件，因此不会影响业务系统的性能。网络 IDS 主要存在以下局限：无法检测多网段通信，存在监测范围的局限；采用特征检测的方法很难检测复杂和未知的攻击形式；对于大数据流量检测存在困难，可

能因为性能瓶颈造成漏检；无法检测加密通信流量。主机 IDS 通常安装在被重点检测的主机上，主要对该主机的网络实时连接以及系统审计日志进行智能分析和判断，发现并应对可能的入侵或滥用行为。主机 IDS 误报率较网络 IDS 低，也可以检测系统级攻击和加密通信流量，但存在以下弱点：会降低被防护主机的运行效率并引入额外的安全问题；依赖于服务器固有的日志和监视能力；全面部署代价较大，但未安装的主机可能成为攻击突破口；缺乏全面信息，对网络入侵行为无法检测。

10. 简述入侵检测系统的三类主要技术，并就其特点作简单对比。

答：入侵检测通常采用以下技术：特征检测技术：对已知的攻击或入侵方式作出确定性描述，当被审计事件与已知入侵事件模式相匹配时即判断为入侵行为。该方法类似于病毒特征检测，准确率较高，但对无先验知识的入侵或攻击行为无能为力；统计检测技术：通过统计模型对审计事件的数量、间隔时间、资源消耗等统计量进行统计，如果出现异常即判断为入侵行为。该方法可以学习并适应用户的使用习惯，具有较高的检测率和可用性；但其学习能力也给入侵者提供了逐步训练入侵检测系统，使入侵行为符合正常的统计规律，从而穿透入侵检测系统的机会；专家系统：建立入侵特征知识库，将入侵知识表述为 if-then 结构，其中 if 为入侵特征，then 部分为系统防范措施。入侵特征的抽取和表达是专家系统的关键：专家系统依赖于知识库的完备性，而后者又取决于审计系统的完备性和实时性。专家系统的有效性完全取决于其知识库的完备性。

11. 何谓特征检测技术？简单分析其特点。

答：特征检测对已知的入侵或攻击方式作出确定性的描述，形成相应的事件模式。当被审计事件与已知的入侵事件模式相匹配时即报警。原理上与专家系统相仿，检测方法上与计算机病毒的检测方式类似，目前基于对包特征描述的模式匹配应用较为广泛。该方法检测的准确率较高，但对于无经验知识的入侵或攻击行为无能为力，漏报率高。

12. 何谓统计检测技术？简单分析其特点。

答：统计模型常用异常检测，通过统计若干测量参数形成正常活动的行为轮廓，当实际测量结果与行为轮廓发生一定偏差时即判定存在入侵行为。统计方法的最大优点是可以学习用户的使用习惯，从而具有较高的检出率和可用性；但其学习能力也给入侵者以机会，通过逐步训练使入侵事件符合正常操作的统计规律，从而可以透过入侵检测系统。

13. 何谓专家系统检测技术？简单分析其特点。

答：不同的系统与设置具有不同的规则，且规则之间往往无通用性，因此在系统实现中，常将有关入侵的知识转化为 if-then 结构（也可以是复合结构）：条件部分为入侵特征，then 部分是系统防范措施。入侵的特征抽取与表达是入侵检测专家系统的关

键。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性。

14. 何谓文件完整性检查技术？简单分析其特点。

答：指检查计算机中自上次检查后文件的变化情况。首先保存被保护文件的信息摘要数据库，每次检查时重新计算文件的数字摘要并与数据库进行比较：若不相同则表明文件被篡改过。其优点在于方法本身几乎不可能被破解，安全性好，也较为灵活；缺点在于摘要数据库本身也可能被入侵者篡改，做完整的文件系统检查非常耗时，而且只能检测文件篡改攻击。

15. 何谓入侵诱骗技术？对于入侵检测系统有何意义？

答：指用特有的特征吸引攻击者，同时对攻击者的各种行为进行分析，进而找到有效应对措施的技术方法。作为一种主动防御技术，该技术试图将攻击者从关键系统引开从而对其进行保护，同时从现存的各种威胁中提取有用信息已发现新型攻击工具、确定攻击模式并研究攻击者动机和攻击应对措施。

16. 何谓蜜罐技术？其特点如何？对于入侵检测系统有何意义？

答：蜜罐是一种在互联网上运行的计算机系统，它是专门为吸引并诱骗那些试图非法闯入他人计算机系统的人而设计的。蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机给攻击者提供一个明显且易受攻击的目标。由于蜜罐并没有向外界提供真正有价值的服务，因此所有连接的尝试都将被视为是可疑的。蜜罐系统的另一个用途是拖延攻击者对真正目标的攻击，让攻击者在蜜罐上浪费时间。这样，最初的攻击目标得到了保护，真正有价值的内容没有受到侵犯。

17. 何谓蜜罐的弱化系统和强化系统配置？就其特点作简单对比。

答：弱化系统是一个配置有已知攻击弱点的操作系统，这样攻击者更容易进入系统，从而可以收集到有关攻击的数据。为确保攻击者没有删除蜜罐的日志纪录，需要运行其它额外审计系统实现对日志的异地存储和备份。弱化系统的优点在于可以提供的是入侵者试图入侵的实际服务，缺点在于对于绝大多数攻击方式已经有了防范措施，因此维护费用高但收益很小。强化系统是对弱化系统配置的改进，并不配置一个看似有效的系统，管理员为基本操作系统提供所有已知的安全补丁，使系统中每个无掩饰的服务变得足够安全。一旦攻击者闯入足够安全的服务中，一方面可以为加强防御提供依据，另一方面可以为执法机关提供证据。强化系统是在短时间内收集最多有效数据的最好方法，但要求管理员具有比恶意入侵者更高的专业技术，否则可能会失去对蜜罐的控制。

18. 何谓低交互、中交互、高交互蜜罐？就其特点作简单对比。

答：根据蜜罐与攻击者间的交互程度可将蜜罐分为三种类型：1、低交互蜜罐：只通过特殊端口监听提供一些特殊的虚假服务，识别并存储所有的输入数据流，但无法获取复杂的协议传输数据。低交互蜜罐最大的特点是模拟，由于并不提供真正的系统，因此降低了对应的安全风险，安全程度最高；此外低交互蜜罐还无法观察到攻击者和操作系统间的交互信息，检测方式较为被动；2、中交互蜜罐：提供了更多的交互信息，但仍然没有提供一个完整的操作系统。由于对攻击者更具诱惑性和吸引力，因而可以记录和分析更复杂的攻击手段。中交互蜜罐的设计目标是吸引攻击者的注意力并保护真正系统。由于有可能被入侵，因此需要定期检查了解其状态。建立中交互蜜罐比较复杂，需要花费大量时间，因为要设置各种服务并保证其安全性；3、高交互蜜罐：具有一个真实的操作系统，随着复杂程度的提高其危险性也随之加大；但同时收集信息的可能性和对攻击者的诱惑性也大大提高。高交互蜜罐的最大特点就是真实，其设计目标就是为了对各种网络攻击行为进行研究；但缺点在于被入侵的可能性很高，而且容易成为攻击跳板。另外因为长期监视系统的关系，使用高交互蜜罐也非常费时。

	Low	Mid	High
包含等级	低	中	高
真实操作系统	--	–	√
危险性	低	中等	高
信息收集	连接	请求	所有
被攻陷期望值	--	–	√
运行所需知识	低	低	高
建立所需知识	低	高	中等
维护的时间	低	低	很高

19. 何谓牺牲型、外观型、测量型蜜罐？就其特点作简单对比。

答：牺牲型蜜罐是一台为某种特定供给设定的简单计算机，假扮为供给受害者被部署于易受攻击地点，从而为攻击者提供了极好的攻击目标。管理员需要定期检查防止蜜罐被入侵并成为攻击跳板，同时采用防火墙等措施隔离并控制牺牲型蜜罐。牺牲型蜜罐提取攻击数据较为耗时，并且不提供全套的行为规范和控制设备。外观型蜜罐通常由应用服务仿真程序构成，仅仅对网络服务进行仿真而不会导致机器真正被攻击。当外观型蜜罐受到侦听或攻击时，它会迅速收集有关入侵者的信息。外观型蜜罐的性能取决于它能够仿真什么样的系统和应用以及它的配置和管理。外观型蜜罐采集到的数据量较牺牲型蜜罐小，而且只能够提供潜在威胁的基本信息。测量型蜜罐建立在牺牲型蜜罐和外观型蜜罐的基础之上，提供了类似于牺牲型蜜罐的高度可信系统和类似于外观型蜜罐的攻击信息记录。由于测量型蜜罐非常容易访问但很难被绕过，目前已经成为一种行之有效的网络防御方法。高级的测量型蜜罐还可防止攻击者将系统作为进一步攻击的跳板。

20. 何谓蜜网技术？其主要功能如何？与蜜罐技术有何区别？

答：蜜网是一种特殊类型的蜜罐系统，但有两点不同：1、蜜网

并非一个单独系统而是由多个系统和攻击检测应用构成的完整网络。该网络部署于防火墙之后，用以捕获网络数据并分析攻击者的攻击方式、策略和动机；2、蜜网中任何一部分都不是模拟应用，而是与真实系统有着完全相同的安全等级。因此在蜜网中发现的漏洞和弱点就是在真实存在的组织所需改进的问题，用户只需将系统从产品环境移植到蜜网中即可。蜜网的主要功能包括：信息控制：对入侵行为的规范，降低入侵者所能造成的威胁程度；信息捕获：捕获并分析所有的攻击行为，得知攻击者的攻击工具、策略和动机等等；信息收集：对于在逻辑或物理上有多个蜜网的组织来说，必须将所有的捕获数据全部集中存储到预定的中心单元中，只针对分布式环境中具有多个蜜网的组织。

21. 简述入侵检测系统的主要响应方式，就其特点作简单对比。

答：主要响应方式包括：实时响应：在检测到入侵行为的第一时间进行响应，可以是主动响应或被动响应，强调响应的实时性；主动响应：在检测到入侵行为后主动采取实际反制措施的响应方式，包括撤销连接、隔离、与防火墙或病毒服务器联动等等，强调响应的自动化和智能化；被动响应：在检测到入侵行为后只向用户提供信息，依靠用户采取下一步行动的响应，包括屏幕告警、时间日志、语音报警等等，强调响应方式的灵活性；人工响应：依赖管理人员监控检测结果并做出响应行为。

22. 何谓异常检测技术？简单分析其特点。

答：异常检测假设入侵者活动异常与正常主体的活动，其前提是入侵行为是异常活动的子集。根据这一理念，首先建立主体的正常活动模板，然后将当前主体的活动状况与正常模板相比较，当违反其统计规律时则认为该活动是入侵行为。异常检测的难题在于如何建立正常模板以及如何设计统计算法，从而不把正常的操作误判为入侵或者忽略真正的入侵行为。异常检测的误检率较高但漏检率较低，可以检测未知入侵或攻击方式。

23. 简述异常检测模型及相应的检测过程。

答：异常检测模型首先建立用户轮廓，然后对测量参数量化后与用户轮廓进行比较：若低于阈值则为正常活动，否则即为入侵行为。检测过程一般包括监控、量化、比较、判定及修正（训练或学习）各环节。

24. 何谓误用检测技术？简单分析其特点。

答：误用检测又称特征检测或模式匹配。假设入侵活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。误用检测可以检测已知的入侵方法，但对未知或无明显特征的入侵方式无能为力。误用检测的难点在于设计既能够表达入侵特征又不会包含正常活动的模式库，同时确保入侵模式库的及时更新。误用检测的误检率较低但漏检率较高。

25. 简述误用检测模型及相应的检测过程。

答：误用检测模型首先建立入侵行为特征库，然后将系统或用户行为与特征库中的记录进行匹配：若特征匹配时即认为是入侵行为，否则即为正常行为。检测过程一般包括监控、特征提取、匹配及判定各环节。

26. 举例说明入侵检测系统的部署位置对于网络安全性能的影响。

答：通常考虑与防火墙的相对位置关系。若入侵检测系统部署在防火墙外侧，则可以监测到所有进出网络的通信流量。此时由于检测结果不受防火墙影响，信息量大检测结果准确，还能够检测到被防火墙过滤掉的部分攻击形式；但入侵检测系统需要处理大量原本被防火墙过滤掉的部分非法通信流量，工作负荷较重，此外对于内部滥用的检测由于防火墙的阻隔也无能为力，性能损失较大。若入侵检测系统部署在防火墙内侧，则相当一部分非法通信流量可以由防火墙过滤掉，入侵检测系统只需有针对性的检测目标为内网的入侵行为，工作负荷较轻，避免产生漏检；内部滥用行为也可以正常检测。综上所述，一般将入侵检测系统部署在防火墙之后。

第六章　恶意代码防范技术

1. 何谓计算机病毒？有哪些主要特征？试简单列举其传播途径。

答：计算机病毒是一种特殊的计算机程序，由于计算机病毒具有与生物学病毒相类似的特征(潜伏性、传染性、发作期等)，所以人们就用生物学上的病毒来称呼它。特征：计算机病毒程序比较小，一般不会超过 5 KB。与计算机其它合法程序一样，可以存储，可以执行，但是它没有文件名，不能在磁盘中以文件的形式独立存在。传播途径：1、无线网络传播；2、有线网络传播；3、直接投放病毒；4、其他媒介设备传播。

2. 名词解释：源码型病毒、嵌入型病毒、外壳型病毒、OS 型病毒。

答：源码型病毒：这种病毒攻击高级语言编写的程序，病毒在高级语言编写的程序编译之前插入到源程序中，经编译成功后成为合法程序的一部分。嵌入型病毒：在感染时往往对宿主程序进行一定的修改，将自身嵌入到攻击目标中，代替宿主程序中不常用到的堆栈区或功能模块，而不是链接在它的首部或尾部。这种计算机病毒是难以编写的，一旦侵入程序体后也较难消除。外壳型病毒：寄生在宿主程序的前面或则后面，并修改程序的第一个执行指令，使病毒先于宿主程序执行，并随着宿主程序的使用而传染扩散。该类病毒易于编写，数量最多。OS 型病毒：用自己的逻辑部分取代操作系统的合法程序模块，根据病毒自身的特点和被替代的操作系统中合法程序模块在操作系统中运行的地位与作用以及病毒取代操作系统的取代方式等，对操作系统进行破坏。

3. 何谓特洛伊木马？有哪些主要特征？简述其工作过程。

答：特洛伊木马在计算机领域中指的是一种后门程序，是黑客用来盗取其他用户的个人信息，甚至是远程控制对方的计算机而加壳制作，然后通过各种手段传播或者骗取目标用户执行该程序，以达到盗取密码等各种数据资料等目的。与病毒相似，木马程序有很强的隐秘性，随操作系统启动而启动。工作过程：一般的木马程序都包括客户端和服务端两个程序，其中客户端是用于攻击者远程控制植入木马的机器，服务器端程序即是木马程序。首先要把木马程序植入系统，攻击者要通过客户端攻击你的系统，当服务端程序在被感染的机器上成功运行以后，攻击者就可以使用客户端与服务端建立连接，并进一步控制被感染的机器。当服务端在被感染机器上运行以后，它一方面尽量把自己隐藏在计算机的某个角落里面，以防被用户发现；同时监听某个特定的端口，等待客户端与其取得连接;并为了下次重启计算机时仍然能正常工作。木马程序一般会通过修改注册表或者其他的方法让自己成为自启动程序。

4. 何谓计算机蠕虫？有哪些主要特征？简述其工作过程。

答：通过分布式网络来扩散传播特定信息或错误，破坏网络中的信息或造成网络服务中断的病毒。主要特征包括：1、传染方式多：蠕虫病毒入侵网络的主要途径是通过工作站传播到服务器硬盘

中，再由服务器的共享目录传播到其他的工作站。但蠕虫病毒的传染方式比较复杂；2、传播速度快：在单机上，病毒只能通过软盘从一台计算机传染到另一台计算机，而在网络中则可以通过网络通信机制，借助高速电缆进行迅速扩散。由于蠕虫病毒在网络中传染速度非常快，使其扩散范围很大，不但能迅速传染局域网内所有计算机，还能通过远程工作站将蠕虫病毒在一瞬间传播到千里之外；3、清除难度大：在单机中，再顽固的病毒也可通过删除带毒文件、低级格式化硬盘等措施将病毒清除，而网络中只要有一台工作站未能杀毒干净就可使整个网络重新全部被病毒感染，甚至刚刚完成杀毒工作的一台工作站马上就能被网上另一台工作站的带毒程序所传染，因此，仅对工作站进行病毒杀除不能彻底解决网络蠕虫病毒的问题；4、破坏性强：网络中蠕虫病毒将直接影响网络的工作状态，轻则降低速度，影响工作效率，重则造成网络系统的瘫痪，破坏服务器系统资源，使多年的工作毁于一旦。工作过程：蠕虫程序的工作流程可以分为漏洞扫描、攻击、传染、现场处理四个阶段。蠕虫程序扫描到有漏洞的计算机系统后，将蠕虫主体迁移到目标主机。然后，蠕虫程序进入被感染的系统，对目标主机进行现场处理。现场处理部分的工作包括：隐藏、信息搜集等。同时，蠕虫程序生成多个副本，重复上述流程。

5. 计算机病毒一般由哪些模块构成？简单说明各模块功能。

答：计算机病毒一般由引导模块、传染模块和破坏与表现模块组成。引导模块将病毒从外存引入内存，激活传染模块和表现模块；传染模块负责病毒的传染和扩散，将病毒传染到其他对象上；表现或破坏模块为计算机病毒中最关键的部分，实现病毒的破坏作用，如删除文件、格式化硬盘、显示或发声等。

6. 何谓引导型病毒？有哪些主要特征？简述工作过程及预防措施。

答：引导型病毒指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时，不对主引导区的内容正确与否进行判别的缺点，在引导型系统的过程中侵入系统，驻留内存，监视系统运行，待机传染和破坏。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区引导记录病毒。引导型病毒的主要特点为：1、引导型病毒是在安装操作系统之前进入内存，寄生对象又相对固定，因此该类型病毒基本上不得不采用减少操作系统所掌管的内存容量方法来驻留内存高端.而正常的系统引导过程一般是不减少系统内存的；2、引导型病毒需要把病毒传染给软盘，一般是通过修改 INT 13H 的中断向量，而新 INT 13H 中断向量段址必定指向内存高端的病毒程序；3、引导型病毒感染硬盘时，必定驻留硬盘的主引导扇区或引导扇区，并且只驻留一次，因此引导型病毒一般都是在软盘启动过程中把病毒传染给硬盘的.而正常的引导过程一般是不对硬盘主引导区或引导区进行写盘操作的；4、引导型病毒的寄生对象相对固定，把当前的系统主引导扇区和引导扇区与干净的主引导扇区和引导扇区进行比较，如果内容不一致，可认定系统引导区异常。预防引导型病毒，通常采用以下一些方法：1、坚持从不带病毒的硬盘引导系统；2、安装能够实时监

控引导扇区的防杀病毒软件，或经常用能够查杀引导型病毒的防杀病毒软件进行检查；3、某些底板上提供引导扇区病毒保护功能（Virus Protect），启用它对系统引导扇区也有一定的保护作用。

7. 何谓文件型病毒？有哪些主要特征？简述工作过程及预防措施。

答：文件型病毒数目最大、传播最广、采用技巧也最多。文件型病毒是对原文件进行修改，使其成为新的文件。文件型病毒分两类：一种是将病毒加在 COM 前部，一种是加在文件尾部。文件型病毒传染的对象主要是.COM 和.EXE 文件。当执行被传染的.COM 或.EXE 可执行文件时，病毒驻入内存。一旦病毒驻入内存，便开始监视系统的运行。当发现被传染目标时进行如下操作：1、首先对运行的可执行文件特定地址的标识位信息进行判断是否已感染了病毒；2、当条件满足，利用 INT 13H 将病毒链接到可执行文件的首部或尾部或中间，并存入磁盘中；3、完成传染后，继续监视系统的运行，试图寻找新的攻击目标。文件型病毒的预防方法是在源程序中增加自检及清除病毒的功能。这种方法可以使得可执行文件从一生成就具有抗病毒的能力，从而可以保证可执行文件的干净。自检清除功能部分和可执行文件的其它文件融为一体，不会和程序的其他功能冲突，也使得病毒制造者无法造出针对性的病毒来。可执行文件无法传染病毒，文件型病毒就无法传播了。

8. 何谓宏病毒？有哪些主要特征？简述其工作过程。

答：宏病毒是一种专门感染 Office 系列文档的恶性病毒，是利用了一些数据处理系统内置宏编程指令的特性而形成的一种特殊病毒。它和其它一般个体病毒不同，是依附在正常的 Word 文件上，利用 Word 文档可执行其内宏命令代码的方式，在 Word 文档在打开或关闭时来控制并感染系统。宏病毒的传播方法与其它病毒不同，在 Office 目录下的“Templates”子目录里有一个名为 Normal.dot 的常规模板文件，每次我们启动 Word 的时候，该文件都会先被 Word 启动并执行里面的 VBA 语句(宏语句)。通常来说，一般用户的 Normal.dot 里面是没有 VBA 语句的，大多数宏病毒都会采用感染 Normal.dot，把自身的恶意 VBA 语句复制到 Normal.dot 里面，使 Word 每次启动时都执行里面的恶意 VBA 语句，并将自己的代码复制到其它 Word 文档里面的方法来达到传染的目的。当用户打开一个感染了 Word 宏病毒的文档时，就等于激发了 Word 宏病毒的运行，它将组成宏病毒的其它几个宏复制到 Word 的通用模板 Normal.dot 中，这就相当于感染了用户的 Word 本身，使得以后新建或打开的文档都将被宏病毒感染。其中有些宏与文件的保存和关闭有关，如 FileSaveAs、FileSave、FileClose 等。当用户保存或关闭文档时激发这些宏的运行，将当前的文档转换成模板形式保存，并将宏病毒代码添加在文档中，使其成为原先宏病毒的复制品，从而完成了病毒的复制并为其再次传播提供了可能。

9. 何谓病毒寄生技术？解释头寄生、尾寄生、插入寄生和空洞寄生。

答：病毒在感染的时候通常将病毒代码加入正常程序之中，原来

程序的功能部分或者全部被保留。根据病毒代码加入的方式不同，寄生病毒可以分为“头寄生”、“尾寄生”、“中间插入”和“空洞利用”四种。头寄生：实现将病毒代码放到程序的头上有两种方法，一种是将原来程序的前面一部分拷贝到程序的最后，然后将文件头用病毒代码覆盖；另外一种是生成一个新的文件，首先在头的位置写上病毒代码，然后将原来的可执行文件放在病毒代码的后面，再用新的文件替换原来的文件从而完成感染；尾寄生：由于在头部寄生不可避免的会遇到重新定位的问题，所以最简单也是最常用的寄生方法就是直接将病毒代码附加到可执行程序的尾部；插入寄生：病毒将自己插入被感染的程序中，可以整段的插入，也可以分成很多段。有的病毒通过压缩原来的代码的方法，保持被感染文件的大小不变；空洞利用：对于 Windows 环境下的可执行文件，还有一种更加巧妙的方法：由于 Windows 程序的结构非常复杂，一般里面都会有很多没有使用的部分，一般是空的段或者每个段的最后部分。病毒寻找这些没有使用的部分，然后将病毒代码分散到其中，这样就实现了神不知鬼不觉的感染，CIH 病毒就是用了这种方法。

10. 何谓病毒驻留技术？病毒为什么要驻留内存？

答：病毒驻留技术是指那些在内存中寻找合适的页面并将病毒自身拷贝到其中且在系统运行期间能够始终保持病毒代码的存在。病毒驻留比那些直接感染（Direct-action）型病毒更具隐蔽性，它通常要截获某些系统操作来达到感染传播的目的。病毒要达到传染的目的必须首先驻留内存之中，这样才能获得对系统的控制权。病毒获得控制权后想办法驻留内存，一般都是病毒码自己从感染程序中分析出来，在系统中找一块内存作为病毒码的老家，把自己搬过去。然后是把系统的一些服务，主要是 INT21 的文件操作或者 INT13 的磁盘操作拦截下来，自己做成一个钩子函数的形式挂接上去，然后就是恢复被感染程序的运行环境，把控制权交还被感染程序。由于系统的文件、磁盘的服务被病毒下了钩子，要进行文件或者磁盘的操作都要经过病毒的代码，由此可见驻留内存的病毒的传播效率是十分高的。

11. 何谓加密变形技术？病毒为什么要加密变形？

答：加密变形技术：在加密病毒的基础上改进，使解密子的代码对不同传染实例呈现多样性。随着病毒技术的发展，出现了所谓的加密变形病毒，其入口处具有解密子(decryptor)，而病毒主体代码被加了密。运行时首先得到控制权的解密代码将对病毒主体进行循环解密，完成后将控制交给病毒主体运行，病毒主体感染文件时会将解密子用随机密钥加密过的病毒主体和保存在病毒体内或嵌入解密子中的密钥一同写入被感染文件。由于同一种病毒的不同传染实例的病毒主体是用不同的密钥进行加密，因而不可能在其中找到唯一的一段代码串和偏移来代表此病毒的特征，似乎静态扫描技术对此即将失效。但不同传染实例的解密子仍保持不变机器码明文，所以使用特征码虽然有误报风险，但仍为一种有效的方法。由于加密病毒还没有能够完全逃脱静态特征

码扫描，所以病毒设计者在加密病毒的基础之上进行改进，使解密子代码对不同传染实例呈现出多样性，这就出现了加密变形病毒。它和加密病毒非常类似，唯一的改进在于病毒主体在感染不同文件会构造出一个功能相同但代码不同的解密子，也就是不同传染实例的解密子具有相同的解密功能，但代码却截然不同。例如，原本的一条指令却被拆成几条指令来完成，中间可能会被插入无用的垃圾代码，这样由于无法找到不变的特征码，静态扫描技术就彻底失效了。

12. 何谓压缩病毒技术？病毒为什么要压缩？解释其感染过程。

答：目前的大部份病毒都是在原生病毒的基础上，经压缩变形而成。压缩后的病毒内容虽然同原生病毒一模一样，但病毒特征代码已经完全改变，相当于产生了一个新的变种病毒。压缩算法是公开的技术，而压缩文件格式是不公开的。利用这些公开的技术，可以生成无数种他人短期内无法破解的压缩格式，进而也就可以利用原生的病毒，轻松产生出无穷多种新病毒。

13. 何谓病毒检测比较法？有哪些主要特征？

答：比较法是用原始的或正常的与被检测的进行比较。比较法包括长度比较法、内容比较法、内存比较法、中断比较法等。比较时可以靠打印的代码清单（比如 DEBUG 的 D 命令输出格式）进行比较，或用程序来进行比较（如 DOS 的 DISKCOMP、COMP 或 PC-TOOLS 等其他软件）。这种比较法不需要专用的查病毒程序，只要用常规 DOS 软件和 PCTOOLS 等工具软件就可以进行，而且还可以发现那些尚不能被现有查病毒程序发现的计算机病毒。长度比较法和内容比较法不能区别程序的正常变化和病毒攻击引起的变化，不能识别保持宿主程序长度不变的病毒，无法判定为何种病毒。通过对内存的检测，观察其空间变化，与正常系统内存的占用和空间进行比较，可以判定是否有病毒驻留空间，但无法判定为何种病毒。此法对于那些隐蔽型病毒无效。病毒为实现其隐蔽和传染破坏之目的，常采用“截留盗用”技术，更改、接管中断向量，让系统中断向量转向执行病毒控制部分。将正常系统的中断向量与有病毒系统的中断向量进行比较，可以发现是否有病毒修改和盗用中断向量。

14. 何谓病毒检测校验和法？有哪些主要特征？

答：将正常文件的内容，计算其校验和，写入文件中保存。定期检查文件的校验和与原来保存的校验和是否一致，可以发现文件是否感染病毒，这种方法叫校验和法。它既可发现已知病毒又可发现未知病毒。由于病毒感染并非文件内容改变的惟一的非它性原因，文件内容的改变有可能是正常程序引起的，所以校验和法常常误报警，而且也会影响文件的运行速度。因而用监视文件的校验和来检测病毒，不是最好的方法。校验和法的优点是：方法简单能发现未知病毒、被查文件的细微变化也能发现。其缺点是：对文件内容的变化过于敏感、会误报警、不能识别病毒名称、不能对付隐蔽型病毒。

15. 何谓病毒检测特征代码法？有哪些主要特征？

答：特征代码法是使用最为普遍的病毒检测方法，国外专家认为特征代码法是检测已知病毒的最简单、开销最小的方法。特征码查毒就是检查文件中是否含有病毒数据库中的病毒特征代码。采用病毒特征代码法的检测工具，必须不断更新版本，否则检测工具便会老化，逐渐失去实用价值。病毒特征代码法对从未见过的新病毒无法检测。

16. 何谓病毒检测行为监测法？有哪些主要特征？

答：利用病毒的特有行为特征性来监测病毒的方法，称为行为监测法。通过对病毒多年的观察、研究，有一些行为是病毒的共同行为，而且比较特殊。当程序运行时监视其行为，如果发现了疑似病毒行为立即报警。行为监测法的长处：可发现未知病毒、可相当准确地预报未知的多数病毒。行为监测法的短处：可能误报警、不能识别病毒名称、实现时有一定难度。

17. 何谓病毒检测软件模拟法？有哪些主要特征？

答：为了检测多态性病毒，研制了新的检测法-软件模拟法。它是一种软件分析器，用软件方法来模拟和分析程序的运行。新型检测工具纳入了软件模拟法，该类工具开始运行时，使用特征代码法检测病毒。如果发现隐蔽性病毒或多态性病毒嫌疑时，启动软件模拟模块，监视病毒的运行，待病毒自身的密码译码以后，再运用特征代码法来识别病毒的种类。

18. 何谓病毒检测感染实验法？有哪些主要特征？

答：感染实验是一种简单实用的检测病毒方法。由于病毒检测工具落后于病毒的发展，当病毒检测工具不能发现病毒时，如果不会用感染实验法便束手无策。如果会用感染实验法，可以检测出病毒检测工具不认识的新病毒，可以摆脱对病毒检测工具的依赖，自主地检测可疑新病毒。这种方法的原理是利用了病毒的最重要的基本特征：感染特性。所有的病毒都会进行感染，如果不会感染，就不称其为病毒。如果系统中有异常行为，最新版的检测工具也查不出病毒时，就可以做感染实验：运行可疑系统中的程序后，再运行一些确切知道不带毒的正常程序，然后观察这些正常程序的长度和校验和，如果发现有的程序增长，或者校验和变化，就可断言系统中有病毒。

19. 何谓病毒检测类属解密法？有哪些主要特征？

答：病毒检测类属解密法是对付多态加密病毒的一种技术，类属解密（Generic Decryption,GD）：此反病毒方法使得反病毒程序可以容易地检测出甚至是最复杂的多形病毒，同时保持快速的扫描速度。当包含了变形病毒的文件执行时，病毒必须对自身进行解密来激活它的功能。为了检测这样的结构，可执行文件要通过GD扫描才能运行。

20. 何谓病毒免疫技术？其实现原理如何？

答：“计算机病毒免疫”发源于生物免疫技术，就像为动物注射某种病毒的免疫疫苗后可以对此病毒产生自然抵抗能力一样。“计算机病毒免疫”就是一种具有类似特点的技术，它的设计目标是不依赖于病毒库的更新而让电脑具有对所有病毒的抵抗能力。普通防毒软件的最大缺点是总要等到病毒出现后才能制定出清除它的办法，并且还要用户及时的升级到新的病毒库。这就让病毒有更多的机会去蔓延传播，而病毒免疫则完全打破这种思路，它可以让电脑具有自然抵抗新病毒的能力，当有新病毒感染计算机系统时不用升级病毒库而同样可以侦测出它。

21. 在清除磁盘病毒时，一般都要求内存不带病毒，为什么？

答：病毒感染内存，其实是病毒感染了硬盘引导区，电脑每次在启动时首先读取硬盘引导区，这时候，病毒就被载入内存里了，再伺机感染其它的可执行程序，达到传播的目的。杀毒软件如果只清除文件中的病毒而没有清除内存中的病毒,则病毒在系统退出前仍有机会感染文件。

22. 结合实际经验，谈谈应对计算机病毒的一般性措施和方法。

答：一、未雨绸缪——做好预防措施

1.一个好，两个妙

杀毒软件和网络防火墙都是必需的。上网前或启动机器后马上运行这些软件，就好像给你的机器“穿”上了一层厚厚的“保护衣”，就算不能完全杜绝网络病毒的袭击，起码也能把大部分的网络病毒“拒之门外”。目前杀毒软件非常多，功能也十分接近，大家可以根据需要去购买正版的,也可以在网上下载免费的共享杀毒软件,但千万不要使用一些破解的杀毒软件,以免因小失大。安装软件后，要坚持定期更新病毒库和杀毒程序，以最大限度地发挥出软件应有的功效，给计算机“铁桶”般的保护。

2.下载文件仔细查

网络病毒之所以得以泛滥，很大程度上跟人们的惰性和侥幸心理有关。当你下载文件后，最好立即用杀毒软件扫描一遍，不要怕麻烦，尤其是对于一些 Flash、MP3、文本文件同样不能掉以轻心,因为现在已经有病毒可以藏身在这些容易被大家忽视的文件中了。

3.拒绝不良诱惑

很多中了网页病毒的朋友，都是因为访问不良站点惹的祸，因此，不去浏览这类网页会让你省心不少。另外，当你在论坛、聊天室等地方看到有推荐浏览某个 URL 时，要千万小心，以免不幸“遇害”，或者尝试使用以下步骤加以防范:

1)打开杀毒软件和网络防火墙;

2)把 Internet 选项的安全级别设为“高”;

3)尽量使用以 IE 为内核的浏览器(如 MyIE2)，然后在 MyIE2 中新建一个空白标签，并关闭 Script、javaApple、ActiveX 功能后再输入 URL。

小提示:该方法不但能有效对付网页病毒,而且对“蠕虫病毒”也有一定作用。

4.免费午餐: 在线查毒

虽然目前网络上的“免费午餐”越来越少，但仍有一些网站坚持向网民们提供免费的在线查毒服务，实在是值得表扬哦。对于没有安装查毒软件、又担心会“中招”的朋友，可以利用在线查毒服务为自己的“爱姬”来一个全身“扫描”:

小提示:

1)各网站的在线查毒服务都有所不同,使用前要仔细阅读网站上的相关说明后再进行操作，争取把病毒赶尽杀绝;

2)由于查毒时需要调用浏览器的 ActiveX 控件,因此查毒前要先在 IE 的“Internet 选项”\“安全”页面中检查该功能是否打开,并相应降低安全级别(一般“中等”即可)再查毒。

5.千呼万唤终不应

如果你发现有“你中奖啦!”、“打开附件会有意外惊喜哦!”这些话，可千万别信!看到类似广告的邮件标题，最好马上把它删掉。对于形迹可疑的邮件(特别是 HTML 格式)，不要随便打开，如果是你熟悉的朋友发来的，可以先与对方核实后再作处理。同时，也有必要采取一定措施来预防邮件病毒:

1)尽量不要用 Outlook 作为你的邮件客户端,改以 Foxmail 等代替，同时以文本方式书写和阅读邮件，这样就不用担心潜伏在 HTML 中的病毒了;

2)多使用远程邮箱功能，利用远程邮箱的预览功能(查看邮件 Header 和部分正文)，可以及时找出垃圾邮件和可疑邮件，从而把病毒邮件直接从服务器上赶走;

3)不要在 Web 邮箱中直接阅读可疑邮件,因为这种阅读方法与浏览网页的原理一样,需要执行一些脚本或 Applet 才能显示信息,有一定危险性。

6.修修补补，填充漏洞

当前各种各样的安全漏洞给网络病毒开了方便之门(其中以 IE 和 PHP 脚本语言的漏洞最多)，我们平时除了注意及时对系统软件和网络软件进行必要升级外,还要尽快为各种漏洞打上最新的补丁。其中一个检测漏洞的简易方法就是直接使用系统中自带的“Windows Update”功能，让微软为你的电脑来一次“全身检查”并打上安全补丁。当然也可以使用其他软件对计算机进行安全检测(例如东方卫士的“系统漏洞检测精灵”就是一个不错的软件)，

以便及早发现漏洞。

7.给危险文件加把“锁”

不管网络病毒如何“神通广大”，它要对计算机进行破坏，总是要调用系统文件的执行程序(例如 format.exe、delete.exe、deltree.exe 等)，根据这个特点，我们可以对这些危险文件采用改名、更改后缀、更换存放目录、用软件进行加密保护等多种方法进行防范，让病毒无从下手。

8.有“备”无患，打造最后防线

正所谓“智者千虑，必有一失”，为保证计算机内重要数据的安全，定时备份少不了。如果我们能做好备份工作，即使遭受网络病毒的全面破坏，也能把损失减至最小。当然，前提条件是必须保证备份前数据没被感染病毒，否则只能是徒劳无功。另外，要尽量把备份文件刻录到光盘上或存放到隐藏分区中，以免“全军覆没”。

二、见招拆招——杀毒软件的常见问题

安装杀毒软件后与其他软件发生冲突怎么办?

1)由于多数杀毒软件和防火墙在默认设置中都是开机后自动运行的,因此当发生软件冲突时先检查是否开启了杀毒软件和防火墙，然后尝试暂时关闭杀毒软件和防火墙的监测功能，再看看问题是否已经解决;

2)到杀毒软件的主页网站看看是否出了相关补丁或升级版本,有则打上补丁或升级到最新版本;

3)如果以上措施还不能解决问题，可以通过 E-mail 联系作者，寻求解决方法。

不能正常升级怎么办?

1)如果使用的是正版软件，可以先试着完全卸载旧版本，再安装新版本(为安全起见，建议卸载前先进行备份);

2)检查是否安装了多种杀毒软件，卸载其他杀毒软件后再安装;

3)检查输入的序列号是否正确、钥匙盘(A 盘)有没有损坏，有问题的请与经销商联系解决;

4)尝试以下操作方法：清空 Temp 文件夹→关闭打开的杀毒软件→换路径重新安装→把安装光盘中的安装目录拷贝到硬盘上，然后运行目录里的“Setup.exe”。

无法清除病毒怎么办?

1)先升级病毒库再杀毒;

2)用一张干净的系统引导盘启动机器后，在 DOS 状态下进行杀毒;

3)备份染毒文件并隔离，然后把病毒样本寄给作者，得到新病毒库后再杀毒。

三、亡羊补牢——病毒发作后的急救措施

虽然已经做足了防范措施，但正所谓：“天有不测之风云”，万一中招了，我们还有什么急救措施呢？

1.软件方面

1)首先断开全部网络连接，以免病毒向其他在线电脑传播，然后马上用杀毒软件进行扫描杀毒工作(记得要先扫描内存、引导区)；

2)赶快备份和转移重要文档到安全地方(软盘、光盘)，记录账号、密码等资料，等病毒清除完毕后再作处理；

3)平时曾用 GHOST 备份的，可以利用映像文件来恢复系统，这样不但能马上恢复工作，而且连同所有病毒也一并清除了，当然，这要求你的 GHOST 备份是没有感染病毒的。另外，恢复系统前同样要先做好备份重要资料的工作。

4)没有进行 GHOST 备份，并且机器中数据并不重要的，可以用干净的引导盘启动机器后格式化硬盘，然后再重新安装系统和程序。

2.硬件方面

1)BIOS 或 CMOS 被破坏的，需要找寻相同类型的主板，然后用热插拔的方法进行恢复。此方法存在着极大的危险性，最好找专业技术人员代你进行恢复。

2)硬盘引导区或主引导扇区被破坏的，可以尝试用 KV 杀毒王、金山毒霸等硬盘修复工具进行修复。

第七章　虚拟专用网技术

1. 何谓 IP 安全？主要提供哪些安全服务？

答：IP 安全或 IPSec 泛指一系列标准，为基于 IP 的网络提供全方位的安全性服务。IPSec 对信息的传输与交换提供机密性、完整性与认证服务。

2. IP 安全解决方案主要包括哪些安全元素？分别实现什么功能？

答：包括的内容及功能：1、认证头（Authentication Header，AH）：提供认证与数据完整性服务；2、封装安全协议（Encapsulating Security Protocol，ESP）：保证 IP 净载（或净荷）的机密性；3、ISAKMP/Oakley（IKE）：安全密钥管理，包括密钥的产生、分发与交换；4、PKI：用于证书管理的公钥体系；5、安全策略：一个安全政策数据库，密钥管理协议与 IPSec 相结合，为 IP 分组提供合适级别的安全性。

3. 何谓认证头？分别简述其在传输模式和隧道模式下的工作原理。

答：认证头 AH（IP 协议号为 51）提供数据源认证、数据完整性校验和防报文重放功能，位于 IP 报头与上层协议之间。它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报文头，此报文头插在标准 IP 包头后面，对数据提供完整性保护。可选择的认证算法有 MD5（Message Digest）、SHA-1（Secure Hash Algorithm）等。MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。隧道模式将整个 IP 分组封装到 AH 中，而传输模式将上层协议（如 TCP）部分封装到 AH 中。隧道（tunnel）模式：用户的整个 IP 数据包被用来计算 AH 头，AH 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通讯。传输（transport）模式：只是传输层数据被用来计算 AH 头，AH 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯。

4. 何谓封装安全载荷？分别简述其在传输模式和隧道模式下的工作原理。

答：ESP (RFC1827, RFC1829)通过对所有分组的数据或净载加密，保证传输信息的机密性。主流的 ESP 标准是 DES(Data Encryption Standard)，它支持的密钥长度达 56bits。而三重 DES(3DES)使用三个系列的密钥加密，这等效于使用 168 bits 的密钥。ESP 操作的两种模式：隧道模式操作允许网络设备为后台主机提供 IPsec，这样对原系统不必作任何改动。但对于隧道模式操作，需产生新的 IP 头，即使用私有 IP 地址。这种模式对基于 ISP 的 VPN 最有用。传输模式允许主机直接加入 IPSec 操作。对于隧道，信源主机的 IP 头必须使用，且只有数据被加密。

5. 何谓组合 IPSEC 协议？简述其工作原理。

答：IPSec 提供了两种安全机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭篡改。加密机制通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被窃听。IPSec 协议组包含 Authentication Header（AH）协议、Encapsulating Security Payload（ESP）协议和 Internet Key Exchange（IKE）协议。其中 AH 协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP 协议定义了加密和可选认证的应用方法，提供可靠性保证。在实际进行 IP 通信时，可以根据实际安全需求同时使用这两种协议或选择使用其中的一种。AH 和 ESP 都可以提供认证服务，不过 AH 提供的认证服务要强于 ESP。IKE 用于密钥交换。

6. 为什么需要 IPSEC 密钥管理？简述其主要功能。

答：对小规模的安全需求，密钥可以人工管理。通常对密钥进行集中管理，然后再分发给远程用户。对大规模的安全需求，集中与安全的密钥管理系统负责动态地、透明地、自动地确定与分发密钥。为协调所有网络设备及其与密钥管理系统的相互关系与作用，必须制定相应标准。Oakley（一个密钥确定协议）定义如何确定密钥，而 Internet 安全连接和密钥管理协议（ISAKMP）是 IPsec 体系结构中的一种主要协议，ISAKMP（Internet Security Association Key Management Protocol，Internet 安全关联与密钥管理协议 ）定义分发密钥的方法允许实体双方协商其安全参数并建立安全关联关系，ISAKMP 与 Oakley 的结合，即 IKMP（Internet Key Management Protocol），提供了完整的、自动的端到端密钥管理体系。

7. 何谓虚拟专用网？为什么要发展 VPN？简述其主要功能。

答：VPN（Virtual Private Networks）是一个私有数据通信网络。它使用一个公共的 IP 网络（如 Internet）来完成公司数据中心、移动职员、远程办公室、用户、提供商及商业伙伴之间的信息传输。可以以不同的方式访问 VPN，包括模拟拨号、ISDN、专线或 xDSL 等。典型地：VPN 定义的安全技术包括加密或（和）认证及 IP 隧道内私有数据的封装。此外，可以使用宽带分组交换服务（如 ATM、Frame Relay 或 X.25）来提供 VPN。现在随着 Internet 的发展，实现基于 IP 的 VPN 服务逐渐成为一种趋势。

8. 构建虚拟专用网可以采取哪些方法？简单对比其特点。

答：可以采取以下方法：1、路由控制：选择确定仅到同一 VPN 路由器的路径；如使用私有地址空间，可能需要 FW/NAT；可使用路由政策或 BGP 公共属性，控制路由分配过程。优点：使用现有的基于路由器的基础设施。缺点：配置复杂；如不使用加密，则无数据保护；难于管理；如使用加密，性能可能下降；2、隧道：拨号 VPN 使用隧道技术使远程访问服务器把用户数据“打包”在 IP 信息包中，这些信息包通过电信服务提供商的网络传递。在 Internet 里，则需要穿过不同的网络，最后到达隧道终点，然后数据拆包，转换成最初的形式。公司网进行远程访问通信时，从长距离的本

地电信服务提供商到 ISP 和 Internet 需要采用隧道技术。隧道技术使用点对点通信协议代替了交换连接，通过路由网络来连接数据地址，这代替了电话交换网络使用的电话号码连接。隧道技术允许授权移动用户或已授权的用户在任何时间任何地点访问企业网络。VPN 隧道技术所具备的优点有以下几点：最小成本：无须购买网络设备和专用线路覆盖所有远程用户；责任共享：通过购买公用网的资源，部分维护责任迁移至 provider（更专业，有经验，是操作，维护成本降低）；安全性；保障 QoS；可靠性：如果一个 VPN 节点坏了，可以一个替换 VPN 建立起来绕过，这种恢复工作是得 VPN 操作可以尽可能的延续；可扩展性：可以通过从公用网申请更多得资源达到非常容易的扩展 VPN，或者协商重构 VPN。

9. 隧道可以分为哪几种类型？分别适用于什么环境？

答：可以分为以下类型：1、服务提供商－服务提供商(SP-SP)：隧道起始于并终止于提供商的网络；服务提供商增值；2、服务提供商－企业 (SP-E)：隧道起始于提供商网络，终止于企业网；服务提供商增值；3、企业－企业 (E-E)：隧道起始于并终止于企业网络；无服务提供商增值，除非作为“打包”式或整体服务。

10. 何谓点对点协议（PPP）？简述其工作原理及特点。

答：点对点协议（PPP）为在点对点连接上传输多协议数据包提供了一个标准方法。PPP 最初设计是为两个对等节点之间的 IP 流量传输提供一种封装协议。在 TCP/IP 协议簇中它是一种用来同步调制连接的数据链路层协议（OSI 模式中的第二层），替代了原来非标准的第二层协议，即 SLIP。除了 IP 以外 PPP 还可以携带其它协议，包括 DECnet 和 Novell 的 Internet 网包交换（IPX）。工作原理：为了建立点对点链路上的通信连接，发送端 PPP 首先发送 LCP 帧，以配置和测试数据链路。在 LCP 建立好数据链路并协调好所选设备之后，发送端 PPP 发送 NCP 帧，以选择和配置一个或多个网络层协议。当所选的网络层协议配置好后，便可以将各网络层协议的数据包发送到数据链路上。配置好后的链路一直保持通信状态，直到 LCP 帧或 NCP 帧明确提示关闭链路，或者有其它的外部事件发生。特点：PPP 协议是一种点-点串行通信协议。PPP 具有处理错误检测、支持多个协议、允许在连接时刻协商 IP 地址、允许身份认证等功能。

11. 何谓点对点隧道协议（PPTP）？简述其工作原理及特点。

答：点对点隧道协议（PPTP）是一种主要用于 VPN 的传输层网络协议。点对点隧道协议(PPTP)是由包括微软和 3Com 等公司组成的 PPTP 论坛开发的一种点对点隧道协，基于拨号使用的 PPP 协议使用 PAP 或 CHAP 之类的加密算法，或者使用 Microsoft 的点对点加密算法 MPPE。其通过跨越基于 TCP/IP 的数据网络创建 VPN 实现了从远程客户端到专用企业服务器之间数据的安全传输。PPTP 支持通过公共网络（例如 Internet）建立按需的、多协议的、虚拟专用网络。PPTP 允许加密 IP 通讯，然后在要跨越公司 IP 网络或公共 IP 网络（如 Internet）发送的 IP 头中对其进行

封装。

12. 何谓第二层隧道协议（L2TP）？简述其工作原理及特点。

答：L2TP(Layer-2 Tunneling Protocol，第二层隧道协议)是一个建议的工业标准，它结合了 L2F 及 PPTP 的最好特性。L2TP 第 2 层隧道协议(L2TP)是 IETF 基于 L2F(Cisco 的第二层转发协议）开发的 PPTP 的后续版本，是一种工业标准 Internet 隧道协议，可以为跨越面向数据包的媒体发送点到点协议 (PPP) 框架提供封装。PPTP 和 L2TP 都使用 PPP 协议对数据进行封装，然后添加附加包头用于数据在互联网络上的传输。PPTP 只能在两端点间建立单一隧道，L2TP 支持在两端点间使用多隧道，用户可以针对不同的服务质量创建不同的隧道。L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。但是当 L2TP 或 PPTP 与 IPSEC 共同使用时，可以由 IPSEC 提供隧道验证，不需要在第 2 层协议上验证隧道使用 L2TP。PPTP 要求互联网络为 IP 网络，L2TP 只要求隧道媒介提供面向数据包的点对点的连接。L2TP 可以在 IP（使用 UDP）、帧中继永久虚拟电路（PVCs）、X.25 虚拟电路(VCs）或 ATM VCs 网络上使用。

13. 何谓第二层转发协议（L2F）？简述其工作原理及特点。

答：L2F(Layer-2 Forwarding，第二层转发)是由 Cisco Systems 发布的隧道化协议：1、第二层转发协议（L2F）用于建立跨越公共网络（如因特网）的安全隧道来将 ISP POP 连接到企业内部网关。这个隧道建立了一个用户与企业客户网络间的虚拟点对点连接；2、第二层转发协议（L2F）允许高层协议的链路层隧道技术。使用这样的隧道，使得把原始拨号服务器位置和拨号协议连接终止与提供的网络访问位置分离成为可能；3、L2F 允许在 L2F 中封装 PPP/SLIP 包。ISP NAS 与家庭网关都需要共同了解封装协议，这样才能在因特网上成功地传输或接收 SLIP/PPP 包。特点：1、是因为 L2F 只需要本地拨号功能，可以减少企业远程访问成本；2、可以提供与专用网络相同的安全等级并且可以支持多条连接的 L2F 隧道；3、对终端用户来说是透明的。

14. 何谓多协议标签交换（MPLS）技术？简述其工作原理及特点。

答：多协议标签交换(Multi-Protocol Label Switch，简称 MPLS）是一种在开放的通信网上利用标签引导数据高速、高效传输的新技术。它的价值在于能够在一个无连接的网络中引入连接模式的特性；其主要优点是减少了网络复杂性，兼容现有各种主流网络技术，能降低网络成本，在提供 IP 业务时能确保 QoS 和安全性，具有流量工程能力。此外，MPLS 能解决 VPN 扩展问题和维护成本问题。MPLS 是集成式的 IP Over ATM 技术，即在 Frame Relay 及 ATM Switch 上结合路由功能，数据包通过虚拟电路来传送，只须在 OSI 第二层（数据链结层）执行硬件式交换（取代第三层（网络层）软件式 routing)。它整合了 IP 选径与第二层标记交换为单一的系统，因此可以解决 Internet 路由问题，使数据包传送的延迟时间减短，增加网络传输的速度，更适合多媒体讯息

的传送。因此，MPLS 最大技术特色为可以指定数据包传送的先后顺序。MPLS 使用标记交换（Label Switching），网络路由器只需要判别标记后即可进行转送处理。

15. 何谓远程用户拨号认证系统（RADIUS）？可以提供哪些安全服务功能？简述其特点。

答：远程用户拨号认证系统（RADIUS）是 VPN 的一个关键组成部分。远程授权拨号上网用户服务(RADIUS)提供三个主要的功能：认证、授权与计费。RADIUS 是一个非专用的协议，它使用户能够管理一个系统中多个厂商提供的拨号远程服务设备。RADIUS 主要功能：1、认证：通过用户名及口令对用户身份进行鉴别；2、授权：基于预先设置的用户配置文件等制定数据访问参数；3、计费：通过不间断的审计追踪每个基于 RADIUS 的会话，以便 ISP 进行准确的收费。RADIUS 的主要特点如下：1、客户/服务模式；2、网络安全；3、灵活的认证机制；4、扩展协议。