复习题

第一章

1．从操作系统本身而言，Windows NT系统主要具有哪些特点？
2．Windows NT系统在系统和网络安全性上引入了哪些新的概念？
3．请考虑以下说法是否正确：Windows 2000系统是Windows产品系列发展中的一个飞跃，因此它的内核完全不同于其前身——Windows NT系统的内核。
4．Windows 2000系统包含哪几个版本，它们各自的特性和适用对象是什么？
5．在Windows 2000系统中，引入了哪些新的安全特性？
6．Windows 2000系统安全模型灵活性与可扩展性的核心是什么？
7．活动目录的概念和作用分别是什么，包括哪些组成部分？
8．试简述活动目录如何创建一种层次结构来组织网络资源。
9．请解释以下三个概念：域，站点，组织单元。它们之间的相互关系是什么？
10．请说明Windows NT系统和Windows 2000系统在域间信任关系上的不同点。
11．请说明Windows NT系统和Windows 2000系统在域控制器上的不同点。
12．请解释使用公钥基础结构（PKI）来提高安全性的必要性。
13．Windows 2000系统中的PKI包含有哪些组件？它们各自的作用是什么？
14．Windows 2000系统中的组策略可以设置哪些内容？
15．请简述Kerberos协议的思想，并描述一次典型的操作过程。
16．配置IPSec协议可以完成哪些安全功能？
17．如果某用户在Windows 2000系统上试图安装未签名的驱动程序，系统就会通知该用户采取哪三种反应？这说的是Windows 2000的哪一种安全特性？
18．Windows Server 2003系统包含哪几个版本，它们各自的特性和适用对象是什么？
19．Windows Server 2003系统为身份验证引入了什么新的安全特性？试对该特性进行说明。
20．Windows Server 2003系统在增强网络安全性上提供了哪些新的特性？

第二章

1. 请解释Windows NT系统安全体系结构中内核模式和用户模式之间的区别。
2. Windows NT系统的用户模式中包含哪些安全子系统？
3. 什么是执行服务？组成执行服务的组件有哪些？
4. 查阅《可信计算机系统评估准则》（TCSEC，即“橘皮书”），了解操作系统安全等级的划分和相关指标。
5. 根据《可信计算机系统评估准则》，Windows NT系统达到的系统安全等级是什么？达到该级别的重要安全性指标有哪些？
6. 请说明FAT文件系统和NTFS文件系统的不同点。
7. 简述NTFS文件系统主要提供了哪些安全特性。
8. Windows NT系统创建的两个默认账户是什么？它们各自的用户权限是什么？
9. Windows NT Server系统有哪些内置的组账户？它们各自被赋予了什么特殊的权限？
10. 试说明通过“用户管理器”和“域用户管理器”创建不同用户类型时的用户作用域有何不同。
11. 请说明工作组和域之间的不同之处。
12. 两个域之间的信任关系有哪两种？Window NT系统的工作组和域之间能否建立起信任关

系？

13. 根据域之间的信任关系，我们可以创建哪些域模型？各种域模型的特点和适用对象是什么？
14. 请解释以下名词：安全标识符，安全访问令牌，访问控制项，访问控制列表。
15. 在Windows NT系统中，当删除某账户后再次创建具有相同用户名的账户，那么新账户是否具有与老账户相同的访问控制权限？
16. 请描述在Windows NT系统中，如何结合安全访问令牌和安全访问控制列表用以完成一次对资源的访问控制。
17. 试简述Windows NT系统中安全审核的功能。

第三章

1. Windows 2000 系统的核心是处于体系结构中核心模式下的软件，它们可以分成哪些组，各组完成的功能是什么？
2. 请简述 Windows 2000 系统试图达到的安全性目标。
3. 请简述 Windows 2000 系统安全模型的底层原理。
4. Windows 2000 系统的安全性在用户模式和内核模式下是分离的，试对此说法进行解释。
5. 本地安全授权机构为基于 Windows 2000 系统的计算机维护所有本地的安全信息，它提供了哪些功能？
6. Windows 2000 系统允许哪几种网络安全协议来提供身份验证服务？
7. Windows 2000 系统默认的身份验证协议是什么？
8. 在 Windows 2000 安全程序开发协议中的哪个组件用来获得验证、信息完整性、信息隐私等集成安全服务，以及用于所有分布式应用程序协议安全方面的服务。

第四章

1. 活动目录服务出现的背景是什么？它的主要作用是什么？
2. 活动目录包含哪两方面的内容？它们各自的定义是什么？两者之间的区别在哪里？
3. Windows 2000 活动目录具有智能的信息复制能力，为什么？
4. 请简述活动目录采用什么方式和 DNS 集成？
5. 如何理解 Windows 2000 环境中 DNS 与活动目录名称空间之间的差异？
6. 请描述一下活动目录客户机定位活动目录服务器的过程。
7. 为了保证活动目录的正常运行，DNS 服务器必须支持哪些特性？
8. Windows 2000 域控制器之间是“ 对等 ”关系还是“ 主从 ”关系？如何理解这种关系？
9. 请简述全局编录服务器的作用。
10. 在一个目录林中增加全局编录服务器对用户查询响应时间的影响如何，对网络通讯量的影响又如何？
11. 以下哪几种类型的操作主机角色在整个目录林中只能有一个。
    （1）架构主机
    （2）域命名主机
    （3）相对标识符主机
    （4）主域控制器模拟器
    （5）基础结构主机
12. 请解释何谓“ 架构 ”。

13. 活动目录架构中所有类别的对象的属性都应该满足哪些条件？
14. 试列出可以引用架构对象（包括类别和属性）的几种名称类型。
15. 在活动目录中发布对象的主要特征是什么？发布对象的方法有哪些？
16. 请简述使用域能够完成哪些网络管理目标？
17. 基于 Windows 2000 的一个目录林中的多个域树之间的名称空间是否连续？
18. 基于 Windows 2000 的一个目录林中的所有域之间具有以下何种信任关系。
    （1）单向不可传递
    （2）单向可传递
    （3）双向不可传递
    （4）双向可传递
19. 请解释一下名词：组织单元，站点。
20. 请说明混和模式域与本地模式域有何不同。
21. 在 Windows 2000 系统中，站点提供哪些服务？
22. 请说明站点和域之间的区别。
23. 请说明利用站点是如何来提高处理客户机请求以及复制目录数据操作的效率。
24. 请简述规划活动目录时需要考虑的内容。
25. 请在自己所在的网络环境中练习创建第一台域控制器。
26. 请在上一题完成的基础上，在自己所在的网络环境中练习创建第二台域控制器。

第五章

1. Windows 2000 系统的身份验证包括哪两部分？分别完成什么功能？
2. 何谓 Windows 2000 系统的单一登录特性？
3. Windows 2000 系统提供了哪些身份验证机制来抵抗中间人攻击？
4. 用户交互式登录到本地计算机和登录到域账户有何不同？
5. Windows 2000 系统的交互式登录需要哪三个系统组件？它们各自的功能是什么？
6. MSGINA.dll 实现了默认的 Windows 登录界面，提供了 Winlogon 用于标识和验证用户的输出函数，请查阅 MSDN 了解实现 GINA 的技术细节。
7. 请说明本地安全授权机构在用户登录的身份验证过程中所起的作用。
8. 请描述一下 Windows 2000 系统中交互式登录到本地计算机的过程。
9. 在 Windows 2000 系统中，除了 Kerberos v5 之外，为什么还需要 NTLM 身份验证协议？
10. 考虑 Windows NT 4.0 Workstation 客户端向 Windows 2000 域控制器验证身份的情况，这时候所使用的身份验证协议是什么？
11. 在 Kerberos 身份验证过程中，Active Directory 所起的作用是什么？
12. 请解释一下何谓 Kerberos 的身份验证委派？
13. 请列举 Kerberos 协议的优缺点。
14. 请简述智能卡所具有的功能。
15. 请简述基于智能卡的交互式登录过程和基于口令的交互式登录过程有何不同？

第六章

1. 请解释以下名词：主体，客体，访问控制技术。
2. 试从访问控制的主体和客体两方面分别说明 Windows 2000 系统中的访问控制机制。
3. 请分别说明自由访问控制列表（DACL）和系统访问控制列表（SACL）在访问控制机制中

的作用。

4. 安全标识符（SID）值的一般格式为：S-R-X-Y^1-Y^2…Y^{n-1}-Y^n，请解释各部分字段的含义。其中哪部分字段是用来标识域内特定的账户和组的？
5. 访问令牌包含进程或线程的安全上下文的完整描述，请说明其中包含有哪些信息？
6. 什么叫做“模拟令牌”？它的作用是什么？
7. 请简要描述一下“安全描述”的结构。
8. 请说明“空 DACL”和“没有 DACL”的区别。
9. 在 Windows 2000 的访问控制中有哪六种访问控制项？其中有哪几种一般类型访问控制项，有哪几种特殊对象类型访问控制项？一般类型访问控制项和特殊对象类型访问控制项之间的基本区别是什么？
10. 在 Windows 2000 系统中有哪三种组作用域？它们之间的区别是什么？
11. 什么是 Windows 2000 的本地组？它与具有域本地作用域的 Active Directory 组有何根本区别？
12. 请列举在 Windows 2000 系统中默认的 Administrators 组、Users 组以及 Power Users 组用户所分别具有的权限。
13. 请说明 RunAs 服务的作用。在 Windows 2000 系统中如何使用 RunAs 服务？
14. 属于 Power Users 组的用户能否创建本地用户和组？他能否删除其创建的本地用户和组？他能否删除其他组创建的本地用户和组？
15. 在安装 Windows 2000 系统的时候是否定义根目录的访问控制权限？为什么？
16. 在 Windows 2000 系统中可用来配置注册表安全权限的命令工具是什么？
17. 在 Windows 2000 系统中，请练习对“用户权利指派”进行配置。

第七章

1．FAT 文件系统较之 NTFS 文件系统，谁的安全性更好？FAT 文件系统能否转换成 NTFS 文件系统？若能，请问该如何操作？NTFS 文件系统能否转换成 FAT 文件系统？若能，请问又该如何操作？

2．在基于 NTFS 文件系统的 Windows 2000 中，如果一个用户即是 A 组的成员，又是 B 组的成员，A 组拥有对某文件夹的“读取”权限，而 B 组拥有对该文件夹的“写入”权限，那么该用户对该文件夹具有什么权限？

3．举例说明以下说法：在 Windows 2000 的 NTFS 文件系统中，“拒绝”权限优先于其他权限。

4．在基于 NTFS 文件系统的 Windows 2000 中，假设以下情况：某普通用户先将一个文件（该用户是这个文件的所有者）的访问权限设置为只有他才能完全控制，而其他任何人均没有任何访问权限。此后，因为某种原因从系统中删除了该用户的账户。这时候，系统中就没有任何人能够直接访问该文件了。请问：应该如何操作才能恢复对该文件的访问。

5．在基于 NTFS 文件系统的 Windows 2000 中，请使用命令行工具 Cacls.exe 为 cmd.exe 设置如下访问权限：Administrators 组——完全控制，SYSTEM 组——完全控制。

6．关于 Windows 2000 文件加密系统（EFS），下列哪种说法是不正确的：

（1）EFS 所采用的加密技术是基于公私钥体制的。

（2）EFS 是作为综合系统服务运行的，比较容易管理、而且很难攻击。

（3）EFS 对于用户是透明的。

（4）不拥有文件密钥的用户无法访问使用 EFS 加密的文件，而新安装系统的管理员则可以。

7．请简述 Windows 2000 EFS 的组成结构。

8．什么是“故障恢复代理”？它在文件加密系统中的作用是什么？
9．请简述文件加密系统的局限性。
10．在以下关于复制加密文件的描述中，正确的有哪些：
（1）源文件及其所在的目录都加密，而目标目录未加密，则目标文件不加密。
（2）源文件及其所在的目录都加密，而目标目录未加密，则目标文件加密。
（3）源文件及其所在的目录都未加密，而目标目录加密，则目标文件不加密。
（4）源文件及其所在的目录都未加密，而目标目录加密，则目标文件加密。
11．在 Windows 2000 系统中，对文件及文件夹进行 EFS 加密的命令行工具是什么？
12．请练习“将默认的恢复代理备份到软盘”这一操作过程。
13．请简述磁盘配额的好处。
14．什么是 Windows 2000 系统的“空会话”漏洞？该漏洞的危害是什么？采取什么方法能够弥补该漏洞？
15．请解释以下名词：常规备份，增量备份，差异备份，拷贝备份，每日备份。

第八章

1．请描述一下在网络上能够对数据及正常服务造成危害的几种常用攻击技术。
2．使用 IPSec 协议对于安全的保证意义在于：
（1）数据的完整性。
（2）数据的保密性。
（3）数据的可用性。
（4）数据的来源验证。
3．IPSec 是在 OSI 参考模型中哪一层上所进行的加密操作？这样有什么好处？
4．IPSec 的传输模式和隧道模式有何区别？
5．请分别描述一下封装安全载荷（ESP）协议和验证报头（AH）协议的实现原理。
6．在 IPSec 中，安全联盟（SA）的作用是什么？
7．什么是 IKE？请简述 RFC2409 为 IKE 所定义的一个两阶段的过程。
8．Windows 2000 在实现 IKE 的时候提供了三种用以在计算机之间建立信任的身份验证方法（基于 IETF 标准），它们分别是什么？
9．请描述一下当 IPSec 策略发挥作用时的一个典型数据交换过程。
10．在 Windows 2000 中实现 IPSec 时，有哪些预定义的 IP 安全策略？它们分别对应于什么级别的安全性？
11．如果计算机是域的成员，那么应用于域的 IPSec 安全策略和本地的活动 IPSec 策略，哪一种安全策略的优先级更高？
12．指派给活动目录中组织单位的 IPSec 策略将覆盖该组织单位中所有成员的域级策略，请问指派给低级组织单位的 IPSec 策略将如何影响指派给较高级别组织单位的 IPSec 策略？
13．请在自己的 Windows 2000 主机上配置 IPSec 策略来完成以下目的：
- 屏蔽外界对本机 ICMP 数据包的访问
- 屏蔽外界对本机 135/tcp, 139/tcp, 445/tcp 端口的访问。

14．什么是 SSL 协议？它实质上包括哪两层协议？
15．SSL 协议和 S-HTTP 协议之间的关系是什么？
16．请描述在使用 SSL 机制时，客户端和服务器之间建立一个安全通道的典型过程。
17．什么是 VPN？最常用于 VPN 的隧道协议有哪些？

18．请在 Windows 2000 系统中配置并启用一台 VPN 服务器，并使用 VPN 客户端连接该服务器、以验证是否成功。

第九章

1．什么是 IIS？它包含哪些重要的组件？为什么说它的安全性非常重要？
2．IIS 有哪些基本的安全需求？
3．请简述 IIS 5.0 所具备的安全特性。
4．IIS 5.0 有哪些身份验证机制？请比较各种身份验证机制在安全性上的差异。
5．对于通过任何类型 Web 浏览器来访问你所设置的 Web 服务器的用户，你想要对他们进行身份验证。下列那种身份验证方法最适合你的需求？
   （1）匿名访问
   （2）基本身份验证
   （3）摘要身份验证
   （4）集成 Windows 身份验证
6．请描述在 IIS 5.0 中如何使用证书来对 Web 客户端进行身份验证和账户映射。
7．在 IIS 5.0 中，对客户访问进行控制的组件有哪些？请描述一下 IIS 5.0 的访问控制流程。
8．可用来帮助管理员从一个中心位置检查网络中所有 Windows 2000 主机补丁状态的工具有哪些？下载这些工具并练习使用它们。
9．为什么需要使用 syskey 加密系统账户数据库？在进行加密的时候，可以选择的密钥选项有哪些？为了保证最大的安全性，你会选择哪一种选项？
10．为了保证 IIS 服务器的安全性，在配置网络协议时请务必关闭 NetBIOS 协议。请在 Windows 2000 系统中进行必要的操作来完成该功能。
11．请查询和分析一些经典漏洞的资料，说明为什么需要在 IIS 中①合理设置 Web 服务的主目录；②删除示例程序；③删除虚拟目录 IISADMPWD；④删除不必要的应用程序映射关联。
12．IIS 日志文件的默认位置在哪里？应对其设置什么样的访问权限？
13．IIS Lockdown 工具的功能是什么？URLScan 工具的功能是什么？
14．什么是终端服务技术？它的优势在哪里？
15．终端服务器有哪两种具体的运行模式？其中哪一种模式对服务器的性能影响较小？
16．通过终端服务管理器可以对控制会话、侦听会话以及正常会话分别进行哪些操作？
17．更改终端服务的默认端口号可以在一定程度上提高终端服务的安全性，请在 Windows 2000 系统中练习该操作。

第十章

1．什么是组策略？什么是组策略对象？
2．为了给一个选定的活动目录站点、域或组织单元设置组策略，需要满足什么要求？
3．请分析 Windows NT 系统和 Windows 2000 系统在策略编辑和设置上的不同之处。
4．请举例说明组策略配置的默认应用顺序。
5．请举例说明组策略的继承关系。
6．请解释以下与特殊的组策略应用顺序和继承相关的名词：禁止替代，锁定策略继承，反向。
7．请描述一下组策略对计算机启动和用户登录的影响情况。
8． 访问组策略管理单元有哪两种基本的方法？

第十一章

1．请简要叙述在 Windows 2000 系统中提供安全配置工具集的好处。
2．安全配置工具集允许管理员配置的内容有哪些？
3．安全配置工具集包含哪些组件？各自的功能是什么？
4．Windows 2000 提供了许多预定义的安全模板，它们在计算机上的存放目录在哪里？在该目录下面有哪些预定义的安全模版文件？
5．Windows 2000 默认提供的安全模板被设计成对应哪五种不同的安全等级？
6．通过 Microsoft 管理控制台（MMC）的“安全配置和分析”管理单元能够完成哪几项功能？
7．请解释以下密码策略的含义：密码必须符合复杂性要求；密码长度最小值；密码最长存留期；密码最短存留期。
8．请解释以下账户锁定策略的含义：账户锁定时间；账户锁定阀值。
9．计算机上的本地策略设置包括哪几类安全区域？
10．事件日志策略为三种默认的日志（分别是应用程序、安全和系统）定义了哪些设置？这些设置的含义分别是什么？
11．使用 secedit.exe 分析系统安全性的语法是什么？

第十二章

1．Windows 2000 系统中包含哪 6 种事件日志？其中又有哪几种日志在所有的 Windows 2000 系统中都存在？
2．审核事件中的成功事件和失败事件该如何正确的理解？
3．在 Windows 2000 系统中可以审核哪些事件类型？
4．在哪些情况下会在服务器的安全日志中生成登录事件日志？
5．请解释为什么需要先将各个域控制器上的安全日志合并，然后再来分析域中的所有账户登录事件？
6．网络非法攻击的一种手段是在系统中添加管理员用户账号，为了能够察觉这种攻击手段，请问应该在 Windows2000 系统中添加何种审核策略？
7．什么是对象的 SACL？它是怎么组成的？它在 Windows 2000 审核对象访问事件的时候所起的作用是什么？
8．如果启用了相关的审核策略，那么关闭计算机或更改系统时间会生成哪种类型的事件？
9．请分别通过“事件查看器”工具和组策略单元设置以下事件日志属性：
   - 安全日志最大值：10240KB。
   - 安全日志保留天数：30 天。
   - 系统日志最大值：10240KB。
   - 系统日志保留天数：30 天。
   - 应用程序日志最大值：5120KB。
   - 应用程序日志保留天数：15 天。
10．请在事件查看器中设置筛选器来查看安全日志中的成功审核和失败审核事件。
11．请在事件查看器中设置筛选器来查看事件 ID 为 608（授予了用户权限）和 609（删除了用户权限）的审核事件。
12．请使用 Dumpel 工具专储过去一个月内所生成的安全事件、系统事件和应用程序事件到专用的日志服务器上（假设服务器主机名为 LogServer）。

第十三章

1．公钥基础结构（PKI）的基础是公钥加密算法，这种算法的基本属性是什么？它的安全性体现在哪里？
2．使用公钥加密算法能够完成哪些安全功能？
3．既然公钥加密算法很安全，那么为什么还需要构建公钥基础结构？
4．什么是数字证书？数字证书的作用是什么？
5．公钥基础结构包含哪些组件？它们各自的作用是什么？
6．Windows 2000 系统提供了那些特性用来支持公钥基础结构？
7．在 Windows 2000 系统上安装证书颁发机构（CA）时可以选择哪几种 CA 类型？其中哪几种类型的 CA 需要活动目录，并且能够在域中发布证书？
8．默认情况下，CA 所颁发的证书存储于系统中的哪个文件夹下面？在何种情况下，该文件夹会被系统设置为共享？
9．在 Windows 2000 系统中，有哪两种申请证书的主要方法？分别适用于向何种证书颁发机构申请证书？
10．在处理证书申请的环节上，企业证书颁发机构和独立证书颁发机构有何不同？
11．Windows 2000 中有多种导出证书的格式，而其中哪一种格式允许导出私钥？
（1）加密消息语法标准 (PKCS #7)
（2）DER 编码的二进制 X.509
（3）Base64 编码的 X.509
（4）个人信息交换 (PKCS #12)
12．什么是 CRL？它的作用是什么？
13．什么是 CRL 的发布期？什么是 CRL 的有效期？两者有何关系？
14．如果 CA 已经发布了新的 CRL（到了“发布期”），则无论客户的 CRL 是否到了“有效期”，都使用新的 CRL 代替旧的 CRL。这种说法是否正确？为什么？
15．证书服务也需要备份吗？假设证书服务遭受到硬件破坏而无法正常运作，那么会引发什么后果？

第十四章

1．请简述 Windows 2003 系统在文件系统的访问控制安全性上的改进。
2．在 Windows Server 2003 系统中，对于新创建的共享资源，Everyone 组具有什么访问权限？
3．在 Windows Server 2003 系统中，不仅可以拥有文件系统对象（文件或文件夹）的所有者权限，是否还可以将对象的所有者权限授予任何人？如果可以的话，那么该如何操作？
4．请简述 Windows 2003 系统在服务配置上的安全性改进。
5．以 Local Service 账户运行的服务和以 Network Service 账户运行的服务有何不同？
6．Windows Server 2003 系统对于本地系统的身份验证，新增了什么措施来保证安全性？
7．Windows Server 2003 系统在活动目录上的改进突出显示在跨越林的信任方面，请简述林信任具有哪些优点？
8．假设以下系统均为 Windows Server 2003，如果在林 1 和林 2 之间创建了一个林信任，在林 2 和林 3 之间也创建了一个林信任，那么林 1 和林 3 之间是否有隐式的信任关系？
9．Windows Server 2003 系统中的 IIS 版本为 IIS 6.0，请简述它在安全性上的改进。