第 1 章 网络安全概述与环境配置

1. 网络攻击和防御分别包括哪些内容？

答：攻击技术主要包括以下几个方面。

（1）网络监听：自己不主动去攻击别人，而是在计算机上设置一个程序去监听目标计算机与其他计算机通信的数据。

（2）网络扫描：利用程序去扫描目标计算机开放的端口等，目的是发现漏洞，为入侵该计算机做准备。

（3）网络入侵：当探测发现对方存在漏洞后，入侵到目标计算机获取信息。

（4）网络后门：成功入侵目标计算机后，为了实现对“战利品”的长期控制，在目标计算机中种植木马等后门。

（5）网络隐身：入侵完毕退出目标计算机后，将自己入侵的痕迹清除，从而防止被对方管理员发现。

防御技术主要包括以下几个方面。

（1）安全操作系统和操作系统的安全配置：操作系统是网络安全的关键。

（2）加密技术：为了防止被监听和数据被盗取，将所有的数据进行加密。

（3）防火墙技术：利用防火墙，对传输的数据进行限制，从而防止被入侵。

（4）入侵检测：如果网络防线最终被攻破，需要及时发出被入侵的警报。

（5）网络安全协议：保证传输的数据不被截获和监听。

2. 从层次上，网络安全可以分成哪几层？每层有什么特点？

答：从层次体系上，可以将网络安全分成 4 个层次上的安全：物理安全，逻辑安全，操作系统安全和联网安全。

物理安全主要包括 5 个方面：防盗，防火，防静电，防雷击和防电磁泄漏。

逻辑安全需要用口令、文件许可等方法来实现。

操作系统安全，操作系统必须能区分用户，以便防止相互干扰。操作系统不允许一个用户修改由另一个账户产生的数据。

联网安全通过访问控制服务和通信安全服务两方面的安全服务来达到。（1）访问控制服务：用来保护计算机和联网资源不被非授权使用。（2）通信安全服务：用来认证数据机要性与完整性，以及各通信的可信赖性。

第 2 章 网络安全协议基础

1. 简述 OSI 参考模型的结构

答：

OSI 参考模型是国际标准化组织（International Standards Organization，ISO）制定的模

型，把计算机与计算机之间的通信分成 7 个互相连接的协议层，自顶向下分别为应用层、表示层、会话层、传输层、网络层、数据链路层、物理层。

2. 简述 TCP/IP 协议族的基本结构，并分析每层可能受到的威胁及如何防御

答：

TCP/IP 协议族包括 4 个功能层，自顶向下分别为：应用层、传输层、网络层、网络接口层。

应用层中很多应用程序驻留并运行在此层，并且依赖于底层的功能，使得该层是最难保护的一层。简单邮件传输协议（SMTP）容易受到的威胁是：邮件炸弹，病毒，匿名邮件和木马等。保护措施是认证、附件病毒扫描和用户安全意识教育。文件传输协议（FTP）容易受到的威胁是：明文传输、黑客恶意传输非法使用等。保护的措施是不许匿名登录，单独的服务器分区，禁止执行程序等。超文本传输协议（HTTP）容易受到的威胁是：恶意程序（ActiveX 控件，ASP 程序和 CGI 程序等）。

传输层可能受到的威胁是拒绝服务（DOS）和分布式拒绝（DDOS）服务的攻击，其中包括 TCP SYN 淹没攻击、SSL 中间人攻击、Land 攻击、UDP 淹没攻击、端口扫描攻击等，保护措施是正确设置客户端 SSL，使用防火墙对来源不明的有害数据进行过渡等。

网络层可能受到的威胁是 IP 欺骗攻击，保护措施是使用防火墙过滤和打系统补丁。

网络接口层又可分为数据链路层和物理层。

数据链路层可能受到的威胁是内容录址存储器表格淹没、VLAN 中继、操纵生成树协议、MAC 地址欺骗、ARP 攻击、专用 VLAN、DHCP 耗竭等。保护措施是，在交换机上配置端口安全选项可以防止 CAM 表淹没攻击。正确配置 VLAN 可以防止 VLAN 中继攻击。使用根目录保护和 BPDU 保护加强命令来保持网络中主网桥的位置不发生改变，可防止操纵生成树协议的攻击，同时也可以强化生成树协议的域边界。使用端口安全命令可以防止 MAC 欺骗攻击。对路由器端口访问控制列表（ACL）进行设置可以防止专用 VLAN 攻击。通过限制交换机端口的 MAC 地址的数目，防止 CAM 表淹没的技术也可以防止 DHCP 耗竭。

物理层可能受到的威胁是未授权用户的接入（内部人员、外部人员）、物理盗窃、涉密信息被复制或破坏等等。保护措施主要体现在实时存档和监测网络，提高通信线路的可靠性（线路备份、网管软件、传输介质）、软硬件设备安全性（替换设备、拆卸设备、增加设备）、防干扰能力，保证设备的运行环境（温度、湿度、烟尘），不间断电源保障，等等。

5. 简述常用的网络服务及提供服务的默认端口。

答：

常见服务及提供服务的默认端口和对应的协议如下表所示

端　　口	协　　议	服　　务
21	TCP	FTP 服务
25	TCP	SMTP 服务

53	TCP/UDP	DNS服务
80	TCP	Web服务
135	TCP	服务
137	UDP	NetBIOS域名服务
138	UDP	NetBIOS数据报服务
139	TCP	NetBIOS会话服务
443	TCP	基于 SSL的 HTTP服务
445	TCP/UDP	Microsoft SMB 服务
3389	TCP	Windows终端服务

6. 简述 ping 指令、ipconfig 指令、netstat 指令、net 指令和 at 指令的功能和用途。

答：

（1）ping 指令：ping 指令通过发送 ICMP 包来验证与另一台 TCP/IP 计算机的 IP 级连接。应答消息的接收情况将和往返过程的次数一起显示出来。ping 指令用于检测网络的连接性和可到达性。

（2）ipconfig 指令：ipconfig 指令显示所有 TCP/IP 网络配置信息、刷新动态主机配置协议（Dynamic Host Configuration Protocol, DHCP）和域名系统（DNS）设置。使用不带参数的 ipconfig 可以显示所有适配器的 IP 地址、子网掩码和默认网关。

（3）netstat 指令：netstat 指令显示活动的连接、计算机监听的端口、以太网统计信息、IP 路由表、IPv4 统计信息（IP，ICMP，TCP 和 UDP 协议）。使用“netstat -an”命令可以查看目前活动的连接和开放的端口，是网络管理员查看网络是否被入侵的最简单方法。

（4）net 指令：net 指令的功能非常的强大，在网络安全领域通常用来查看计算机上的用户列表、添加和删除用户、与对方计算机建立连接、启动或者停止某网络服务等。

（5）at 指令：使用 at 命令建立一个计划任务，并设置在某一时刻执行。

第 3 章　网络安全编程基础

1. 简述 Windows 操作系统的内部机制。

答：

Windows 操作系统的内部机制如下：Windows 是一个“基于事件的，消息驱动的”操作系统。在 Windows 下执行一个程序，只要用户进行影响窗口的动作（如改变窗口大小或移动、单击鼠标等）该动作就会触发一个相应的“事件”。系统每次检测到一个事件时，就会给程序发送一个“消息”，从而使程序可以处理该事件。每次检测到一个用户事件，程序就对该事件做出响应，处理完以后，再等待下一个事件的发生。

2. 简述学习 Windows 下编程的注意点。

答：

（1）根据实际情况选择一门语言，精通使用，切勿看到一种语言学一种，到最后都只是略知一二。

（2）编程是一个循序渐进的过程，需要在学习的过程中一点一滴积累，遇到困难大可不必灰心丧气。

（3）从一开始写程序要养成良好的编程习惯，如变量命名规则、缩进规范、编写文档和注释等，以提高程序的可读性和可扩展性。

第 4 章 网络扫描与网络监听

1. 简述黑客的分类，以及黑客需要具备哪些基本素质。

答：

目前将黑客分成 3 类：第 1 类为破坏者，第 2 类为红客，第 3 类为间谍。

要成为一名好的黑客，需要具备 4 种基本素质：“Free”精神，探索与创新精神，反传统精神和合作精神。

2. 黑客在进攻的过程中需要经过哪些步骤？目的是什么？

答：

黑客一次成攻的攻击，可以归纳成基本的五个步骤：

第一， 隐藏 IP；

第二， 踩点扫描；

第三， 获得系统或管理员权限；

第四， 种植后门；

第五， 在网络中隐身。

以上几个步骤根据实际情况可以随时调整。

3. 简述黑客攻击和网络安全的关系。

答：

黑客攻击和网络安全是紧密结合在一起的，研究网络安全不研究黑客攻击技术等同于纸上谈兵，研究攻击技术不研究网络安全等同于闭门造车。某种意义上说没有攻击就没有安全，系统管理员可以利用常见的攻击手段对系统进行检测，并对相关的漏洞采取措施。

网络攻击有善意也有恶意的，善意的攻击可以帮助系统管理员检查系统漏洞，恶意的攻击可以包括：为了私人恩怨而攻击，为了商业或个人目的获得秘密资料而攻击，为了民族仇恨而攻击，利用对方的系统资源满足自己的需求、寻求刺激、给别人帮忙，以及一些无目的攻击。

4. 为什么需要网络踩点？

答：

踩点就是通过各种途径对所要攻击的目标进行尽可能的了解。常见的踩点方法包括：在域名及其注册机构的查询，公司性质的了解，对主页进行分析，邮件地址的搜集和目标

IP 地址范围查询。

踩点的目的就是探察对方的各方面情况，确定攻击的时机。摸清对方最薄弱的环节和守卫最松散的时刻，为下一步的入侵提供良好的策略。

5. 扫描分成哪两类？每类有什么特点？可以使用哪些工具进行扫描、各有什么特点？

答：

扫描，一般分成两种策略：一种是主动式策略，另一种是被动式策略。被动式策略是基于主机之上，对系统中不合适的设置、脆弱的口令及其他同安全规则抵触的对象进行检查，不会对系统造成破坏。主动式策略是基于网络的，它通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞，但是可能会对系统造成破坏。

常见的扫描工具包括：

第一，系统自带的扫描工具如 windows 和 linux 中的 ping，linux 中的 namp。这类工具操作简单，大多工作在命令行模式下。

第二，开源的和免费的扫描工具如 Nessus，X-scan，Netcat，X-port 以及 Google 在 2010 年新推出的 Skipfish 等。这类扫描工具一般具有单一、独特的功能，因此扫描速度极快、更新速度快、容易使用，由于其开源、免费的特点，使其具有更广泛的影响力。

第三，商用的扫描工具，如 eEye 公司的 Retina，Network Associates 的 CyberCop Scanner 以及 Symantec 的 NetRecon 等。基本上大部分商业扫描器都工作在黑盒模式，在这种模式下无法看到源代码，以一个近似于渗透者或攻击者的身份去看待需要评估的。在商业化应用中，对误报、漏报的容忍程度比较低。商用扫描器在精确扫描之后，会给出一些建议和手段来屏蔽。最初是提供一些修补建议，这种方式对专业人员来说有相当价值，但对于一些较薄弱或者比较懒惰的用户，修补建议的作用就被忽略了。在新一代的商用扫描器中，提出了修补联动的概念，通过发送注册表去提示用户，用户双击注册表，就可以导入需要修改、升级补丁的信息，并且还可以和 WSUS 进行联动。这样就可以基本上达到自动化的修补。

6. 网络监听技术的原理是什么？

答：

监听器 Sniffer 的原理是：在局域网中与其他计算机进行数据交换时，数据包发往所有的连在一起的主机，也就是广播，在报头中包含目的机的正确地址。因此只有与数据包中目的地址一致的那台主机才会接收数据包，其他的机器都会将包丢弃。但是，当主机工作在监听模式下时，无论接收到的数据包中目的地址是什么，主机都将其接收下来。然后对数据包进行分析，就得到了局域网中通信的数据。一台计算机可以监听同一网段所有的数据包，不能监听不同网段的计算机传输的信息。

第 5 章 网络入侵

1. 简述社会工程学攻击的原理。

答：

社会工程是使用计谋和假情报去获得密码和其他敏感信息的科学。研究一个站点的策略，就是尽可能多地了解这个组织的个体，因此黑客不断试图寻找更加精妙的方法从他们希望渗透的组织那里获得信息。

另一种社会工程的形式是黑客试图通过混淆一个计算机系统去模拟一个合法用户。

2. 登录系统以后如何得到管理员密码？如何利用普通用户建立管理员账户？

答：

用户登录以后，所有的用户信息都存储在系统的一个进程中，这个进程是“winlogon.exe”，可以利用程序将当前登录用户的密码解码出来。

用普通用户账号登录后，可以利用 GetAdmin.exe 等权限提升工具将自己加到管理员组或者新建一个具有管理员权限的用户。

3. 简述暴力攻击的原理。暴力攻击如何破解操作系统的用户密码、如何破解邮箱密码、如何破解 Word 文档的密码？针对暴力攻击应如何防御？

答：

暴力攻击的原理：黑客使用枚举的方法，使用运算能力较强的计算机，尝试每种可能的字符破解密码，这些字符包括大小写、数字和通配符等。

字典文件为暴力破解提供了一条捷径，程序首先通过扫描得到系统的用户，然后利用字典中每一个密码来登录系统，看是否成功，如果成功则显示密码。

邮箱的密码一般需要设置为 8 位以上，7 位以下的密码容易被破解。尤其 7 位全部是数字的密码，更容易被破解。使用相应暴力破解软件可以每秒 50 到 100 个密码的速度进行匹配。

破解 Word 文档的密码方法与破解邮箱密码相似。

进行适宜的安全设置和策略，通过结合大小写字母、数字和通配符组成健壮的密码可以防御暴力攻击。

4. 简述 Unicode 漏洞的基本原理。

答：

漏洞描述：攻击者可通过 IE 浏览器远程运行被攻击计算机的 cmd.exe 文件，从而使该计算机的文件暴露，且可随意执行和更改文件。

Unicode 标准被很多软件开发者所采用，无论何种平台、程序或开发语言，Unicode 均为每个字符提供独一无二的序号，如向 IIS 服务器发出包括非法 Unicode UTF-8 序列的 URL，攻击者可使服务器逐字“进入或退出”目录并执行任意程序，该攻击即称为目录转换攻击。

Unicode 用“%2f”和“%5c”分别代表“/”和“ ”字符，但也可用“超长”序列来代替这些字符。“超长”序列是非法的 Unicode 表示符，如用“%c0%af”代表“/”字符。由于 IIS 不对超长序列进行检查，因此在 URL 中添加超长的 Unicode 序列后，可绕过微软的安全检查，如在一个标记为可执行的文件夹发出该请求，攻击者即可在服务器上运行可执行文件。

5. 简述缓冲区溢出攻击的原理。

答：

当目标操作系统收到了超过了它的能接收的最大信息量时，将发生缓冲区溢出。这些多余的数据使程序的缓冲区溢出，然后覆盖实际的程序数据。缓冲区溢出使目标系统的程序被修改，经过这种修改的结果将在系统上产生一个后门。最常见的手段是通过制造缓冲区溢出使程序运行一个用户 shell，再通过 shell 执行其他命令，如果该 shell 有管理员权限，就可以对系统进行任意操作。

6. 简述拒绝服务的种类与原理。

答：

DoS（Denial of Service，拒绝服务）攻击，其目的是使目标计算机或网络无法提供正常的服务。最常见的 DoS 攻击是计算机网络带宽攻击和连通性攻击。带宽攻击是以极大的通信量冲击网络，使网络所有可用的带宽都被消耗掉，最后导致合法用户的请求无法通过。连通性攻击指用大量的连接请求冲击计算机，最终导致计算机无法再处理合法用户的请求。

9. 简述 DDos 的特点以及常用的攻击手段，如何防范？

答：

分布式拒绝服务攻击的特点是先使用一些典型的黑客入侵手段控制一些高带宽的服务器，然后在这些服务器上安装攻击进程，集数十台，数百台甚至上千台机器的力量对单一攻击目标实施攻击。在悬殊的带宽力量对比下，被攻击的主机会很快因不胜重负而瘫痪。分布式拒绝服务攻击技术发展十分迅速，由于其隐蔽性和分布性很难被识别和防御。

常用攻击手段及防范措施如下：

第一，破坏物理设备。这些物理设备包括：计算机、路由器、电源、冷却设备、网络配线室等。防范这种破坏的主要措施有：例行检查物理实体的安全；使用容错和冗余网络硬件的方法，必要时迅速实现物理设备切换，从而保证提供正常的应用服务。

第二，破坏配置文件。错误配置也会成为系统的安全隐患，这些错误配置常常发生在硬件装置、系统或应用程序中。如果攻击者侵入目标系统，更改了某些配置信息，目标系统很可能因配置不当而无法继续提供正常的服务。因此，管理员首先应该正确设置系统及相关软件的配置信息，并将这些敏感信息备份到软盘等安全介质上；利用 Tripwire 等工具的帮助及时发现配置文件的变化，并快速恢复这些配置信息保证系统和网络的正常运行。

第三，利用网络协议或系统的设计弱点和实现漏洞。SYN flooding 攻击即是利用 TCP/IP 协议的设计弱点，即建立连接时的三次握手协议和该过程中资源的非对称分配，及 IP 欺骗。若要从根本上克服这些弱点，需要重新设计协议层，加入更多的安全控制机制。

若要在现有的网络构架中弥补这些弱点，可以采取上面介绍的半通明网关或主动监视技术。

第四，消耗系统资源。系统资源包括 CPU 资源，内存资源，磁盘空间，网络带宽等，攻击者利用资源有限的特点，恶意消耗系统资源，使系统无法提供正常的服务。Smurf，DDoS 等都属于该类型。随着攻击技术的日新月异，智能型协作型的攻击工具的不断开发，信息的可用性面临着更为严峻的考验。安全专家对此深感忧虑，因为一旦发动 DDoS 攻击，目前没有什么快速有效的解决办法。

另外，全球网络管理员要管理好自己的网络，可以采取下面这些行之有效的防范措施：

1）及时地给系统打补丁，设置正确的安全策略；

2）定期检查系统安全：检查是否被安装了 DDoS 攻击程序，是否存在后门等；

3）建立资源分配模型，设置阈值，统计敏感资源的使用情况；

4）优化路由器配置：（1）配置路由器的外网卡，丢弃那些来自外部网而源 IP 地址具有内部网络地址的包；（2）配置路由器的内网卡，丢弃那些即将发到外部网而源 IP 地址不具有内部网络地址的包；（3）设置 TCP 拦截；（4）限制 TCP 连接超时阈值；（5）禁止 IP 广播包流入内部网络；（6）禁止外出的 ICMP 不可达消息；

5）由于攻击者掩盖行踪的手段不断加强，很难在系统级的日志文件中寻找到蛛丝马迹。因此，第三方的日志分析系统能够帮助管理员更容易地保留线索，顺藤摸瓜，将肇事者绳之以法；

6）使用 DNS 来跟踪匿名攻击；

7）对于重要的 WEB 服务器，为一个域名建立多个镜像主机。

第 6 章 网络后门与网络隐身

1. 留后门的原则是什么？

答：

后门的好坏取决于被管理员发现的概率，留后门的原则就是不容易被发现，让管理员看了没有感觉、没有任何特别的地方。

2. 如何留后门程序？列举三种后门程序，并阐述原理及如何防御。

答：网络攻击经过踩点、扫描、入侵以后，如果攻击成功，一般就可以拿到管理员密码或者得到管理员权限。

第一，Login 后门。在 Unix 里，login 程序通常用来对 telnet 来的用户进行口令验证。入侵者获取 login。c 的原代码并修改，使它在比较输入口令与存储口令时先检查后门口令。如果用户敲入后门口令，它将忽视管理员设置的口令让你长驱直入。这将允许入侵者进入任何账号，甚至是 root。由于后门口令是在用户真实登录并被日志记录到 utmp 和 wtmp 前产生一个访问的，所以入侵者可以登录获取 shell 却不会暴露该账号。管理员注意到这种后门后，便用“strings”命令搜索 login 程序以寻找文本信息。许多情况下后门口令会原形毕露。入侵者就开始加密或者更好的隐藏口令，使 strings 命令失效。所以更多的管理员是

用 MD5 校验和检测这种后门的。

第二，线程插入后门。这种后门在运行时没有进程，所有网络操作均播入到其他应用程序的进程中完成。也就是说，即使受控制端安装的防火墙拥有“应用程序访问权限”的功能，也不能对这样的后门进行有效的警告和拦截，也就使对方的防火墙形同虚设！这种后门本身的功能比较强大，是现在非常主流的一种，对它的查杀比较困难，很让防护的人头疼。

第三，网页后门。网页后门其实就是一段网页代码，主要以 ASP 和 PHP 代码为主。由于这些代码都运行在服务器端，攻击者通过这段精心设计的代码，在服务器端进行某些危险的操作，获得某些敏感的技术信息或者通过渗透，提权获得服务器的控制权。并且这也是攻击者控制服务器的一条通道，比一般的入侵更具有隐蔽性。

防御后门的方法主要有：建立良好的安全习惯，关闭或删除系统中不需要的服务，经常升级安全补丁，设置复杂的密码，迅速隔离受感染的计算机，经常了解一些反病毒资讯，安装专业的防毒软件进行全面监控等。

3. 简述终端服务的功能，如何连接到终端服务器上？如何开启对方的终端服务？

答：

终端服务是 Windows 操作系统自带的，可以通过图形界面远程操纵服务器。

可通过以下三种方式连接到终端服务器上：

第一，利用 Windows 2000 自带的终端服务工具 mstsc.exe。该工具中只需设置要连接主机的 IP 地址和连接桌面的分辨率即可。

第二，使用 Windows XP 自带的终端服务连接器 mstsc.exe。它的界面比较简单，只要输入对方主机的 IP 地址就可以了。

第三，使用 Web 方式连接，该工具包含几个文件，需要将这些文件配置到 IIS 的站点中去。

假设对方不仅没有开启终端服务，而且没有安装终端服务所需要的软件，使用工具软件 djxyxs.exe 可以给对方安装并开启该服务。

4. 简述木马由来，并简述木马和后门的区别。

答：

“木马”一词来自于“特洛伊木马”，英文名称为 Trojan Horse。传说希腊人围攻特洛伊城，久久不能攻克，后来军师想出了一个特洛伊木马计，让士兵藏在巨大的特洛伊木马中，部队假装撤退而将特洛伊木马丢弃在特洛伊城下，让敌人将其作为战利品拖入城中，到了夜里，特洛伊木马内的士兵便趁着夜里敌人庆祝胜利、放松警惕的时候从特洛伊木马里悄悄地爬出来，与城外的部队里应外合攻下了特洛伊城。由于特洛伊木马程序的功能和此类似，故而得名。

本质上，木马和后门都是提供网络后门的功能，但是木马的功能稍微强大一些，一般还有远程控制的功能，后门程序则功能比较单一，只是提供客户端能够登录对方的主机。

网络代理跳板作用如下：当从本地入侵其他主机时，本地 IP 会暴露给对方。通过将某一台主机设置为代理，通过该主机再入侵其他主机，这样就会留下代理的 IP 地址而有效地保护自己的安全。本地计算机通过两级代理入侵某一台主机，这样在被入侵的主机上，就不会留下自己的信息。可以选择更多的代理级别，但是考虑到网络带宽的问题，一般选择两到三级代理比较合适。

6. 系统日志有哪些？如何清楚这些日志？

答：

系统日志包括 IIS 日志，应用程序日志、安全日志和系统日志等。

清除日志最简单的方法是直接到该目录下删除这些文件夹，但是文件全部删除以后，一定会引起管理员的怀疑。一般入侵的过程是短暂的，只会保存到一个 Log 文件，只要在该 Log 文件删除所有自己的记录就可以了。

使用工具软件 CleanIISLog.exe 可以删除 IIS 日志。使用工具软件 clearel.exe 可以方便地清除系统日志，首先将该文件上载到对方主机，然后删除这 3 种主机日志。清除命令有 4 种：Clearel System，Clearel Security，Clearel Application 和 Clearel All。

第 7 章 恶意代码分析与防治

1. 简述研究恶意代码的必要性。

答：

在 Internet 安全事件中，恶意代码造成的经济损失占有最大的比例。如今，恶意代码已成为信息战、网络战的重要手段。日益严重的恶意代码问题，不仅使企业及用户蒙受了巨大经济损失，而且使国家的安全面临着严重威胁。

2. 简述恶意代码长期存在的原因。

答：

在信息系统的层次结构中，包括从底层的操作系统到上层的网络应用在内的各个层次都存在着许多不可避免的安全问题和安全脆弱性。而这些安全脆弱性的不可避免，直接导致了恶意代码的必然存在。

3. 恶意代码是如何定义，可以分成哪几类？

答：

恶意代码的定义随着计算机网络技术的发展逐渐丰富，Grimes 将恶意代码定义为，经过存储介质和网络进行传播，从一台计算机系统到另外一台计算机系统，未经授权认证破坏计算机系统完整性的程序或代码。

它可以分成以下几种类型：计算机病毒(Computer Virus)、蠕虫(Worms)、特洛伊木马

逻辑炸弹(Logic Bombs)、病菌(Bacteria)、用户级 RootKit、核心级 RootKit、脚本恶意代码(Malicious Scripts)和恶意 ActiveX 控件。

6 个方面，并图示恶意代码攻击模型。

答：

恶意代码的整个作用过程分为 6 个部分：

①侵入系统。侵入系统是恶意代码实现其恶意目的的必要条件。恶意代码入侵的途径很多，如：从互联网下载的程序本身就可能含有恶意代码；接收已经感染恶意代码的电子邮件；从光盘或软盘往系统上安装软件；黑客或者攻击者故意将恶意代码植入系统等。

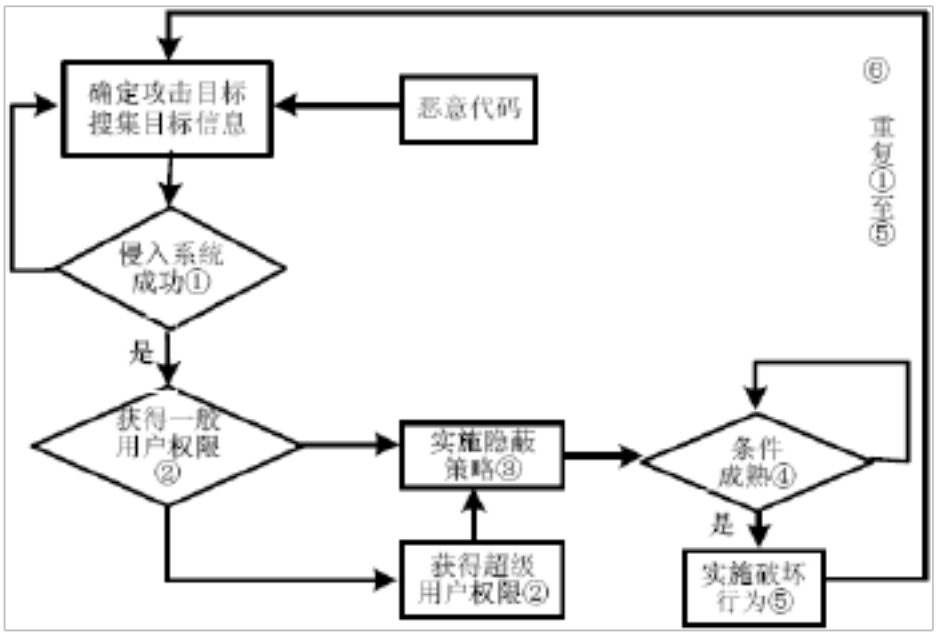
②维持或提升现有特权。恶意代码的传播与破坏必须盗用用户或者进程的合法权限才能完成。

③隐蔽策略。为了不让系统发现恶意代码已经侵入系统，恶意代码可能会改名、删除源文件或者修改系统的安全策略来隐藏自己。

④潜伏。恶意代码侵入系统后，等待一定的条件，并具有足够的权限时，就发作并进行破坏活动。

⑤破坏。恶意代码的本质具有破坏性，其目的是造成信息丢失、泄密，破坏系统完整性等。

⑥重复①至⑤对新的目标实施攻击过程。恶意代码的攻击模型如下图所示。



5. 简述恶意代码的生存技术是如何实现的。

答：

恶意代码生存技术通过以下 4 个方面实现：反跟踪技术、加密技术、模糊变换技术和自动生产技术。

第一，反跟踪技术。恶意代码采用反跟踪技术可以提高自身的伪装能力和防破译能力，增加检测与清除恶意代码的难度。目前常用的反跟踪技术有两类：反动态跟踪技术和反静态分析技术。

第二，加密技术。加密技术是恶意代码自我保护的一种手段，加密技术和反跟踪技术的配合使用，使得分析者无法正常调试和阅读恶意代码，不知道恶意代码的工作原理，也无法抽取特征串。从加密的内容上划分，加密手段分为信息加密、数据加密和程序代码加密三种。

主程序的代码互不相同。同一种恶意代码具有多个不同样本，几乎没有稳定代码，采用基于特征的检测工具一般不能识别它们。随着这类恶意代码的增多，不但使得病毒检测和防御软件的编写变得更加困难，而且还会增加反病毒软件的误报率。

第四，自动生产技术。恶意代码自动生产技术是针对人工分析技术的。“计算机病毒生成器”，使对计算机病毒一无所知的用户，也能组合出算法不同、功能各异的计算机病毒。“多态性发生器”可将普通病毒编译成复杂多变的多态性病毒。多态变换引擎可以使程序代码本身发生变化，并保持原有功能。

恶意代码通过以下几种技术实现攻击技术：进程注入技术、三线程技术、端口复用技术、超级管理技术、端口反向连接技术和缓冲区溢出攻击技术。

第一，进程注入技术。当前操作系统中都有系统服务和网络服务，它们都在系统启动时自动加载。进程注入技术就是将这些与服务相关的可执行代码作为载体，恶意代码程序将自身嵌入到这些可执行代码之中，实现自身隐藏和启动的目的。

第二，三线程技术。在 Windows 操作系统中引入了线程的概念，一个进程可以同时拥有多个并发线程。三线程技术就是指一个恶意代码进程同时开启了三个线程，其中一个为主线程，负责远程控制的工作。另外两个辅助线程是监视线程和守护线程，监视线程负责检查恶意代码程序是否被删除或被停止自启动。

第三，端口利用技术。端口复用技术，系指重复利用系统网络打开的端口（如 25、80、135 和 139 等常用端口）传送数据，这样既可以欺骗防火墙，又可以少开新端口。端口复用是在保证端口默认服务正常工作的条件下复用，具有很强的欺骗性。

第四，超级管理技术。一些恶意代码还具有攻击反恶意代码软件的能力。为了对抗反恶意代码软件，恶意代码采用超级管理技术对反恶意代码软件系统进行拒绝服务攻击，使反恶意代码软件无法正常运行。

第五，端口反向连接技术。防火墙对于外部网络进入内部网络的数据流有严格的访问控制策略，但对于从内网到外网的数据却疏于防范。端口反向连接技术，系指令恶意代码攻击的服务端（被控制端）主动连接客户端（控制端）。

第六，缓冲区溢出攻击技术。缓冲区溢出漏洞攻击占远程网络攻击的 80%，这种攻击可以使一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权，代表了一类严重的安全威胁。恶意代码利用系统和网络服务的安全漏洞植入并且执行攻击代码，攻击代码以一定的权限运行有缓冲区溢出漏洞的程序，从而获得被攻击主机的控制权。

7. 简述恶意代码如何实现隐藏技术。

隐藏通常包括本地隐藏和通信隐藏，其中本地隐藏主要有文件隐藏、进程隐藏、网络连接隐藏、内核模块隐藏、编译器隐藏等。网络隐藏主要包括通信内容隐藏和传输通道隐藏。

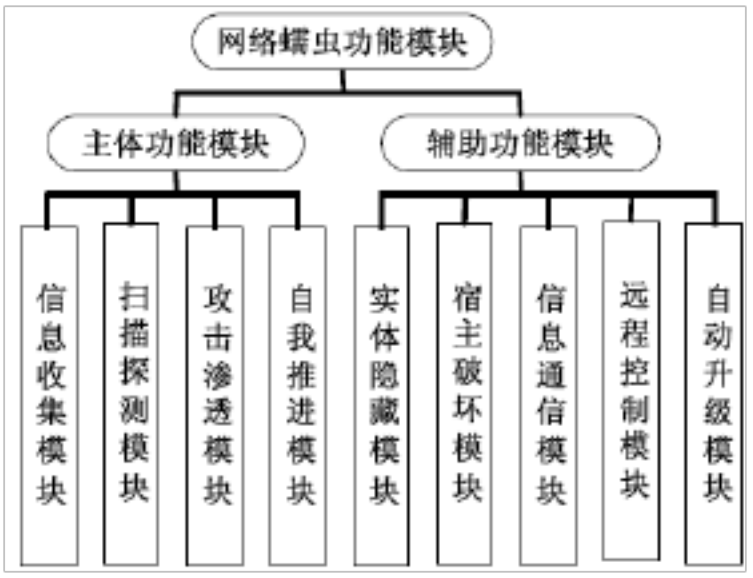
本地隐蔽是指为了防止本地系统管理人员觉察而采取的隐蔽手段。隐蔽手段主要有三

命令的检查；另一类方法是如果恶意代码能够修改或替换相应的管理命令，也就是把相应管理命令恶意代码化，使相应的输出信息经过处理以后再显示给用户，就可以很容易地达到蒙骗管理人员，隐蔽恶意代码自身的目的；还有一类方法是分析管理命令的检查执行机制，利用管理命令本身的弱点巧妙地避过管理命令，可以达到既不修改管理命令，又达到隐蔽的目的。从上述隐蔽方法看来，恶意代码植入的位置越靠近操作系统低层越不容易被检测出来，对系统安全构成的威胁也就越大。

使用加密算法对所传输的内容进行加密能够隐蔽通信内容。隐蔽通信内容虽然可以保护通信内容，但无法隐蔽通信状态，因此传输信道的隐蔽也具有重要的意义。对传输信道的隐蔽主要采用隐蔽通道技术。隐蔽通道是允许进程违反系统安全策略传输信息的通道。

答：

网络蠕虫的功能模块可以分为主体功能模块和辅助功能模块。实现了主体功能模块的蠕虫能够完成复制传播流程，而包含辅助功能模块的蠕虫程序则具有更强的生存能力和破坏能力。网络蠕虫功能结构如下图所示。



9. 简述目前恶意代码的防范方法。

答：

恶意代码防范方法主要分为两方面：基于主机的恶意代码防范方法和基于网络的恶意代码防范方法。

第一，基于主机的恶意代码防范方法。主要包括：基于特征的扫描技术、校验和、沙箱技术和安全操作系统对恶意代码的防范，等等。

第二，基于网络的恶意代码防范方法。基于网络的恶意代码防范方法包括：恶意代码检测防御和恶意代码预警。其中常见的恶意代码检测防御包括：基于 GrIDS 的恶意代码检测、基于 PLD 硬件的检测防御、基于 HoneyPot 的检测防御和基于 CCDC 的检测防御。

8章 安全操作系统基础

简述操作系统账号密码的重要性，有几种方法可以保护密码不被破解或者被盗取？

标识与鉴别是涉及系统和用户的一个过程，可将系统账号密码视为用户标识符及其鉴别。标识就是系统要标识用户的身份，并为每个用户取一个系统可以识别的内部名称——用户标识符。用户标识符必须是惟一的且不能被伪造，防止一个用户冒充另一个用户。将用户标识符与用户联系的过程称为鉴别，鉴别过程主要用以识别用户的真实身份，鉴别操作总是要求用户具有能够证明他的身份的特殊信息，并且这个信息是秘密的，任何其他用户都不能拥有它。

较安全的密码应是不小于6个字符并同时含有数字和字母的口令，并且限定一个口令的生存周期。另外生物技术是一种比较有前途的鉴别用户身份的方法，如利用指纹、视网膜等，目前这种技术已取得了长足进展，逐步进入了应用阶段。

2. 简述审核策略、密码策略和账户策略的含义，以及这些策略如何保护操作系统不被入侵。

答：

审核策略：安全审核是 Windows 2000 最基本的入侵检测方法。当有人尝试对系统进行某种方式（如尝试用户密码，改变账户策略和未经许可的文件访问等）入侵时，都会被安全审核记录下来。

密码策略：密码对系统安全非常重要，密码策略用于保证密码的安全性。其策略包括：“密码复杂性要求”是要求设置的密码必须是数字和字母的组合；“密码长度最小值”是要求密度长度至少为6位；“密码最长存留期15天”是要求当该密码使用超过15天以后，就自动要求用户修改密码；“强制密码历史”是要求当前设置的密码不能和前面5次的密码相同。

账号策略：开启账户策略可以有效防止字典式攻击。账号策略包括：复位账户锁定计数器，账户锁定时间，账户锁定阈值等策略。如账户锁定阈值等于 5，账户锁定时间等于30 分钟，则当某一用户连续尝试 5 次登录都失败后将自动锁定该账户，30 分钟后自动复位被锁定的账户。

3. 如何关闭不需要的端口和服务？

答：

用端口扫描器扫描系统所开放的端口，在 文件中有知名端口和服务的对照表可供参考。用记事本打开该文件，如图1所示。