额外打印 for zlt

第一章

1、 中国计算机安全等级划分为 5 个，各是什么？

第一级：用户自主保护级（TCSEC 的 C1 级） 第二级：系统审计保护级（TCSEC 的 C2 级） 第三级：安全标记保护级（TCSEC 的 B1 级） 第四级：结构化保护级（TCSEC 的 B2 级） 第五级：访问验证保护级（TCSEC 的 B3 级

2、 信息安全划分为三个级别：计算机安全、网络安全、信息系统安全。

3、 网络面临各种各样的威胁，其中最主要的威胁是 恶意攻击、软件漏洞、网络结构缺陷、安全缺陷和自然灾害。

4、 计算机安全包括设备安全、操作系统安全、数据库安全、介质安全等方面。

5、 橙皮书：1985 年美国国防部 NCSC 制定的计算机安全标准——可信计算机系统评价准则 TCSEC。TCSEC 标准定义了系统安全的 5 个要素：安全策略、可审计机制、可操作性、生命期保证、建立并维护系统安全的相关文件。4 个方面：安全政策、可说明性、安全保障、文档。7 个安全级别： D 、C1、C2、B1、B2、B3、A1。

6、 网络安全的基本目标：就是能够具备安全保护能力、隐患发现能力、应急反应能力、信息对抗能力。

第二章

7、 三类安全威胁：外部攻击、内部攻击和行为滥用。

8、 从攻击目的的角度来讲可分为 5 类：破坏型攻击、利用型攻击、信息收集型攻击、网络欺骗型攻击、垃圾信息攻击。

9、 网络欺骗攻击：DNS 欺骗、电子邮件欺骗、Web 欺骗、IP 欺骗。

10、利用向目标主机发送非正常消息而导致目标主机崩溃的攻击方法主要有哪些？

PingOfDeath IGMP Flood Teardrop UDP flood SYN flood Land Smurf Fraggle 畸形消息攻击 分布式拒绝服务攻击

目的地不可达攻击 电子邮件炸弹 对安全工具的拒绝服务攻击

拒绝服务攻击，网络远程拒绝服务攻击，本地拒绝服务攻击

11、简要叙述 IP 欺骗的原理与过程。

IP 欺骗，简单地说，就是伪造数据包源 IP 地址的攻击，其实现的可能性基于两个前提：第一，目前的 TCP/IP 网络在路由选择时，只判断目的 IP 地址，并不对源 IP 地址进行进行判断，这就给伪造 IP 包创造了条件；第二，两台主机之间，存在基于 IP 地址的认证授权访问，这就给会话劫持创造了条件。

12、叙述攻击的一般目的。

破坏目标工作、窃取目标信息、控制目标计算机、利用假消息欺骗对方，从本质上讲就是入侵与破坏。

13、简要叙述攻击的一般过程及注意事项。

攻击的准备阶段、攻击的实施阶段、攻击的善后阶段。注意：①确定攻击目的、准备攻击工具、收集目标信息；②隐藏自己的位置、利用收集到的信息获取账号和密码，登陆主机、利用漏洞或者其他方法获得控制权并窃取网络资源和特权；③清理痕迹如 Web 服务器的日志，事件日志等，可用以下方法：禁止日志审计、清除事件日记、清除 IIS 服务日记。

14、简要叙述口令猜测的方法与步骤

一、获取账号

利用目标主机的 Finger 功能、利用目标主机的 X.500 服务、从电子邮件地址中收集、查看主机是否有习惯性的账号。

二、获取密码

通过网络监听非法得到用户密码、在知道用户的账号后、利用一些专门的软件强行破解用户密码、利用系统管理员的失误。

第三章

15、网络侦察技术：网络扫描、网络监听、口令破解。

16、什么是网络扫描？什么是扫描器？

扫描是通过向目标主机发送数据报文，然后根据相应获得目标主机的情况。

扫描器是一种自动检测远程或本地主机安全性弱点的程序。

17、扫描有几种类型？简述它们的功能。

地址扫描、端口扫描、漏洞扫描；

地址扫描：是最简单、最常见的一种扫描方式。简单的做法就是通过 Ping 这样的程序判断某个 IP 地址是否有活动的主机，或者某个主机是否在线。

端口扫描：判断运行服务的方法就是通过端口扫描，因为常用的服务时使用标准的端口，只要找到相应的端口，就能知道目标主机上运行着什么服务。

漏洞扫描：指使用漏洞扫描程序对目标系统进行信息查询。通过漏洞扫描，可以发现系统中存在的不安全的地方。

18、什么是网络监听？

网络监听作为一种发展比较成熟的技术，在协助网络管理员检测网络传输数据及排除网络故障等方面具有不可替代的作用。目的是截获通信的内容，监听的手段是对协议进行分析。（是一种见识网络状态、数据流程以及网络上信息传输的管理工具，它可以将网络界面设定成监听模式，并且可以截获网络上锁传输的信息。）

19、简述 Sniffer 的工作原理

正当用处主要是分析网络的流量，以便找出所关心的网络中潜在的问题。可以捕获网络报文，它把包抓取下来，然后查看其中的内容，可以得到密码等。Sniffer 只能抓取一个物理网段内的包。如果想要完成监听，捕获网络上的所有报文，前提条件是，网络必须是共享以太网，把本机上的网卡设置为混杂模式。大多数至少能够分析下面的一些一些协议：标准以太网，TCP/TP,IPX，DECNet。

20、什么是字典文件？简述其在攻击中的作用。

所谓字典文件就是根据用户的各种信息建立一个用户可能使用的口令的列表文件，对攻击者来说，攻击的口令在这字典文件中的可能性很大，而且因为字典条目相对较少，在破解速度上也远快于穷举法口令攻击。

第四章

21、什么是拒绝服务攻击？如何分类？

Dos 是阻止或拒绝合法使用者存取网络服务器的一种破坏性攻击方式。

内部用户通过长时间占用系统的内存、cpu 处理时间，外部用户通过占用网络连接使其它用户得不到网络服务。外部几种模式：消耗资源、破坏或改变配置信息、物理破坏或者改变网络部件、利用服务程序中的处理错误使服务失效。

根据攻击者是从一个位置发起攻击还是从多个位置发起攻击，拒绝服务攻击又可以分成传统的拒绝服务攻击和分布式拒绝服务攻击。

Dos 攻击的具体实现方式主要包括：资源消耗、服务中止、物理破坏等。

22、简述电子邮件轰炸拒绝服务攻击的原理。它会造成什么样的危害？怎样防止这种攻击？

电子邮件轰炸是最早的一种拒绝服务攻击，它的表现形式是在很短时间内受到大量无用的电子邮件。

原理：连接到邮件服务器的 SMTP（25）端口，按照 SMTP 协议发送几行信息加上一堆文字垃圾，就算只发送了一封邮件，反复多次，就形成了邮件炸弹。

危害：因为所有的邮件都需要空间来保存，同时受到的邮件需要系统来处理，所以过多的邮件会加剧网络连接负担、消耗大量的存储空间；过多的投递会导致系统日志文件变得巨大，甚至溢出文件系统，这将给许多操作系统带来危险。而且大量的邮件将消耗大量的处理器时间，占用大量的带宽，延缓甚至阻止系统的正常处理活动。

防止：可以识别邮件炸弹的源头，配置路由器，不使其通过。

可以配置防火墙，但防火墙最多只能防止从攻击者源头发来的信息。

使用最新版本的电子邮件服务软件，提高系统记账能力。

23、什么是分布式拒绝服务攻击？它有什么特点？为什么它的危害性更强？怎样防止这种攻击？

分布式拒绝服务 DDos 攻击是对传统 DoS 攻击的发展，攻击者首先侵入并控制一些计算机，然后在控制这些计算机的同时向一个特定的目标发起拒绝服务攻击。

特点：克服了传统拒绝服务攻击的两个缺点（受网络资源的限制、隐蔽性差），其隐蔽性更强，突破了传统攻击方式从本地攻击的局限性和不安全性。

分布式拒绝服务可以根据情况扩大攻击的规模，使目标系统完全失去服务的功能。目前，DDoS 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。

DDOS 引人了分布式攻击和 Client\Server 结构，使 DOS 的威力激增，同时，DDOS 囊括了已经出现的各种重要的 DOS 攻击方法，比 DOS 的危害性更大。

防止攻击：允许管理员设置一些限制，如限制可以使用的最大的内存、CPU 时间以及生成的最大文件等。

24、对付分布式拒绝服务攻击的方法有哪些？举例说明。

一、在数据流中搜寻特征字符，攻击者在传达攻击命令或发送数据时，进行搜寻特征字符，就可以确定攻击服务器和攻击者的位置。

二、利用攻击数据包的某些特征，例如超长或畸形的 ICMP 或 UDP 包等存在某种加密特性时，很可能就是攻击控制器向攻击器发布的攻击命令；

三、设置防火墙监视本地主机端口的使用情况，对本机敏感端口仅此能够监视；

四、对通信数据量进行统计也可获得有关攻击系统的位置和数量信息。例如在攻击之前目标网络的域名服务器往往会接受到远远超过正常数量的反向和正向的地址查询，在攻击时，攻击数据的来源地址会发出超出正常极限的数据量。

第五章

25、简述缓冲区溢出的基本原理。

缓冲区溢出攻击是一种通过往程序的缓冲区写入超出其长度的内容，造成缓冲区溢出，从而破坏程序的堆栈，使程序转而执行其他预设指令，以达到攻击目的的攻击方法。

26、缓冲区溢出攻击的一般目标是什么？

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使得攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了，攻击者必须达到如下的两个目标：

① 在程序的地址空间里安排适当的代码。

② 通过适当的初始化寄存器和内存，让程序跳转到入侵者安排的地址空间执行。

第六章

27、程序攻击的方法有哪些？试说明什么叫逻辑炸弹？什么叫病毒？什么叫后门？什么叫特洛伊木马？

逻辑炸弹、病毒、后门、特洛伊木马

逻辑炸弹：一种隐藏于计算机系统中以某种方式触发后对计算机系统硬件、软件或数据进行恶意破坏的程序代码。

病毒：计算机病毒是一段附着在其他程序上的、可以自我繁殖的程序代码。

后门：是计算机入侵者攻击网上其他计算机成功后，为方便下次再进入而采取的一些欺骗手段和程序。

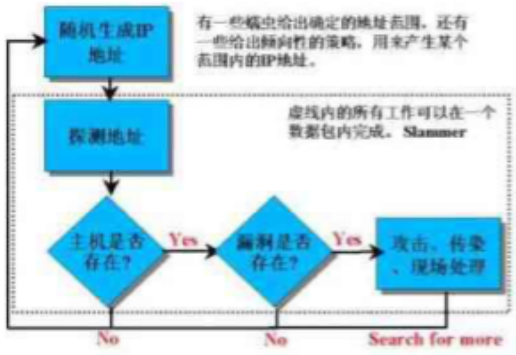
特洛伊木马：指附着在应用程序中或者单独存在的一些恶意程序，它可以利用网络远程响应网络另一端的控制程序的控制命令，实现对感染木马程序的计算机的控制，或者窃取感染木马程序的计算机上的机密资料。

28、蠕虫与病毒有哪些相同点和不同点？

和病毒类似，蠕虫也可以自我复制。蠕虫能够利用电子邮件和网络设施来扩散并且创建新的拷贝。通过分布式网络来扩散传播特定的信息或错误，进而造成网络服务遭到拒绝并发生死锁。“蠕虫”程序不一定是有害的，病毒类似，蠕虫也在计算机与计算机之间自我复制，与病毒相比，蠕虫可消耗内存或网络带宽，并导致计算机停止响应。蠕虫也是一种病毒，因此具有病毒的共同特征。

蠕虫一般不采取利用 pe 格式插入文件的方法，而是复制自身在互联网环境下进行传播，病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。局域网条件下的共享文件夹，电子邮件 email，网络中的恶意网页，大量存在着漏洞的服务器等都成为蠕虫传播的良好途径。

29、试画出模拟 Morris 蠕虫病毒主体程序代码的工作流程图。



30、按照特洛伊木马的发展过程把特洛伊木马分成哪几类？这几类木马的主要特点分别是什么？

最初网络还处于以 UNIX 平台为主的时期，木马就产生了，当时的木马程序的功能相对简单，往往是将一段程序嵌入到系统文件中，用跳转指令来执行一些木马的功能。随着 WINDOWS 平台的日益普及，一些基于图形操作的木马程序出现了，用户界面的改善，使使用者不用懂太多的专业知识就可以熟练的操作木马，相对的木马入侵事件也频繁出现，而且由于这个时期木马的功能已日趋完善，因此对服务端的破坏也更大了。

第一代木马：控制端 —— 连接 —— 服务端

特点：属于被动型木马。能上传，下载，修改注册表，得到内存密码等。

典型木马：冰河，NetSpy，back orifice（简称：BO）等。

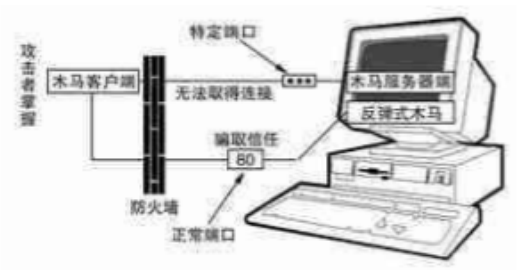
第二代木马：服务端 —— 连接 —— 控制端

特点：属于主动型木马。隐蔽性更强，有利用 ICMP 协议隐藏端口的，有利用 DLL（动态连接库）隐藏进程的，甚至出现能传播的木马。

典型木马：网络神偷，广外女生等。（反弹端口型木马）

31、为什么后来的木马制造者制造出反弹式木马？反弹式木马的工作原理是什么？试画出反弹式木马的工作流程图 p134

因为随着防火墙技术的发展，基于 IP 包过滤规则可以很有效的防止从外部来的连接，因此黑客在无法连接装有木马程序的计算机的情况下，就无法实施攻击。于是发明了一种反向连接技术，即所谓的反弹式木马。利用防火墙对内部发起的连接请求无条件信任的特点假冒是系统的合法网络请求与木马的客户端建立连接，从而达到对北攻击计算机控制的目的。



32、木马技术包括哪些，这些技术有什么特点？

自动启动技术、隐藏技术、远程监控技术。

自动启动技术，木马程序第一次运行需要用户来执行，以后会启动系统时候自动装在服务端程序。

隐藏技术，木马程序不同于普通程序的最大特定就是想尽一切办法隐藏自己。

远程监控技术，木马的最主要功能，也是木马的最终目的。

第七章

33、常见的欺骗方式有哪些？共同特点是什么？除了文中所讲述的那几种方式外，你还知道哪些欺骗攻击的方式？

DNS 欺骗攻击，Email 欺骗攻击，Web 欺骗攻击，IP 欺骗攻击。共同特点是利用假消息欺骗对方为主要目标，用来攻击目标配置不正确额消息。

ARP 欺骗、源路由欺骗（通过指定路由，以假冒身份与其他主机进行合法通信或发送假报文，使受攻击主机出现错误动作）、地址欺骗（包括伪造源地址和伪造中间站点）等。

34、简述 DNS 的工作原理，并指出在整个 DNS 解析过程中，可能存在的被欺骗的地方。

DNS 实现了一种分布式的、层次式的模型结构，每个登记的域都将自己的数据库列表提供给整个网络复制。当客户在浏览器输入要访问的主机名时，一个ＩＰ地址的查询请求就会发往ＤＮＳ服务器，ＤＮＳ服务器中的数据库提供所需的ＩＰ地址。在ＤＮＳ体统中提供所需地址解析数据的ＤＮＳ服务器称为域名服务器。

可能存在的被欺骗的地方：在当提交给某个域名服务器的域名解析请求的数据包被捕获，然后按截获者的意图将一个虚假的ＩＰ地址作为应答信息返回给请求者。

35、简述 DNS 欺骗攻击的原理和过程。

原理：假设当提交给某个域名服务器的域名解析请求的数据包被捕获，然后按截获者的意图将一个虚假的ＩＰ地址作为应答信息返回给请求者。这时，原始请求者就会把这个虚假的 IP 地址作为它所要请求的域名而进行连接，显然它被欺骗到了别处而根本连接不上自己想要的那个域名。这样对那个客户想要连接的域名而言，它就算是被黑掉了，因为客户由于无法得到它的正确的 IP 地址而无法连接上它。这就是 DNS 欺骗的基本原理。

（如果可以冒充域名服务器，然后把查询的 IP 地址设为攻击者的 IP 地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了，这就是 DNS 欺骗的基本原理。）

过程：在进行欺骗之前获得正确的查询 ID 值，伪造出客户端无法辨认的 DNS 应答包，并在服务器给出应答之前将欺骗信息发送出去。第一次向要欺骗的 DNS 服务器发一个查询包并监听到该 ID 值，随后再发一个用于干扰的查询包，紧接着马上发送事先构造好的应答包，包内的查询 ID 为预测的可能的值。

36、简述 E-mail 欺骗攻击的原理和过程。

主要表现为邮件炸弹和电子邮件欺骗。电子邮件轰炸和电子邮件滚雪球（邮件炸弹）指用伪造的ＩＰ地址和电子邮件地址向同一个信箱发送数以千计或数以万计升值无穷多次的内容相同的垃圾邮件，致使受害人的邮箱被“轰炸”，严重者可能会给电子邮件服务器操作系统带来危险，甚至导致系统瘫痪。

电子邮件欺骗，攻击者佯称自己为系统管理员，给用户发送邮件要求用户修改口令或在貌似正常的附件总加载病毒或其他木马程序。

具体过程：①构造自己的 SMTP 服务器，并不需要安装额外的邮件服务器；②伪造该公司的发信人和发信地址；③需要编写后台脚本接受用户输入表单。

37、Web 欺骗攻击有哪些具体形式？请简述其原理。

具体形式有：改写 URL、特殊的网页假象，如 web 病毒，web 木马，图片格式文件的病毒。

（①改写ＵＲＬ：在ＵＲＬ重写中，攻击者能够把网络流量转到攻击者控制的另一个站点上。利用ＵＲＬ地址，是地址都指向攻击者的Ｗｅｂ服务器。

②特殊的网页假象：攻击者制造一些特殊的网页来攻击用户。有 Web 病毒、Web 木马、图片格式文件的病毒。）

原理：是攻击者通过伪造某个 www 站点的影像拷贝，使该影像 web 的入口进入到攻击者的 web 服务器，并经过攻击者计算机的过滤作用，从而达到攻击者监控受攻击者的任何活动以获取有用信息的目的，这些信息当然包括用户的口令账户。

38、简述 IP 欺骗的原理和过程。

原理：IP 欺骗是在服务器不存在任何漏洞的情况下，通过利用 TCP/IP 协议本身存在的一缺陷进行攻击的方法，既然 hosta 和 hostb 之间的信任关系是基于 ip 地址而建立起来的，假如可以冒充 hostb 的 ip，就可以使用 rlogin 登录到 hosta。而不需任何口令验证。

过程：（1）首先使被信任主机的网络暂时瘫痪，以免对攻击造成干扰；

（2）连接到目标机的某个端口来猜测 ISN 基值和增加规律；

（3）接下来把源地址伪装成被信任主机，发送带有 SYN 标志的数据段请求连接；

（4）等待目标机发送 SYN+ACK 包给已经瘫痪的主机；

（5）再次伪装成被信任主机向目标主机发送 ACK，此时发送的数据段带有预测的目标主机的 ISN+1；

（6）连接建立，发送命令请求。

第九章

39、访问控制包含哪些内容？请分别举例说明

访问控制包含：用户身份的识别和认证；对访问的控制；审计跟踪。

用户身份的识别和认证：是访问控制的第一道设防，鉴别合法用户和非法用户，从而有效地阻止非法用户访问系统。

对访问的控制：包括 3 种控制，授权；确定访问权限；实施访问权限。

审计跟踪：它对用户使用何种系统资源、使用时间、执行操作等问题进行完整的记录，以备非法事件发生后能进行有效的追查。

40、身份认证包含哪些信息？这些认证信息主要用于什么方面？

身份认证过程指的是当用户试图访问资源的时候，系统启动用户的身份是否真实的过程。通常可根据以下信息认证：

①用户所知道的：密码认证过程 PAP。

②用户所拥有的：基于智能卡的认证系统。

③用户本身的认证：用户的一些生物学上的属性，如指纹、虹膜特征等。

④根据特定地点（或特定时间）：Bellcore 的 S/KEY 一次一密系统。

⑤通过信任的第三方：Kerberos 认证

41、简述口令认证技术的认证方法，用哪些方法可以提高口令认证技术的安全性。

口令认证也成通行字认证，是一种根据已知事物验证身份的方法。

需要考虑和规定选择方法，使用期限，字符长度，分配和管理以及在计算机系统内的保护等。

提高安全性：每个用户需分配有专用的同行字，系统可以知道哪些用户在联机；采用随时间变化的通行字；采用通行短语代替通行字；在通行字后填充随机数。

42、网络的物理隔离技术包含那几个方面，他们各自采用了什么样的技术。

客户端的物理隔离，把用户的硬盘分为两个区，一个是公共区，一个是安全区。每次只能进入其中之一，可以保证安全区不暴露在 Internet 上。

集线器级的物理隔离，在客户端的内外双网的布线上使用一条网络线来通过远端切换器连接内外双网，实现一台工作站连接内外两个网络的目的，并在布线上避免了客户端技算计要用两条网络线连接内外两个网络的目的；

服务器端的物理隔离，采用的是一种新的高级隔离技术，它可以通过复杂的软硬件技术实现在服务器端的数据过滤和传输任务。

43、什么叫自主访问控制，自主访问控制的方法有哪些，自主访问控制有哪几种类型？

自主访问控制：由客体自主地确定各个主体对它的直接访问权限（又称访问模式）。

方法：①基于行的 DAC 有权利表、前缀表、口令；②基于列的 DAC 有保护位、访问控制表。　　类型：等级型，有主型，自由型。

44、为什么自主访问控制无法抵御特洛伊木马的攻击？请举例说明。

DAC 技术存在着一些明显的不足：资源管理比较分散，用户间关系不能在体统镇南关体现出来，不易管理；信息容易泄露，无法抵御特洛伊木马的攻击。特洛伊木马是一段计算机程序，它镶嵌在一个合法用户使用的程序中，当这个合法用户在系统中运行这个程序是，他悄无声息的进行非法操作。在自主访问控制下，一旦带有特洛伊木马的应用程序被激活，特洛伊木马可以任意泄露和破坏所接触到的信息，甚至改变这些信息的访问授权模式，而系统无法区别这种修改时用户自己的合法操作还是特罗伊木马的非法操作。

45、什么是强制访问控制方式，如何防止特洛伊木马的非法访问？

在强制访问控制下，用户与文件都有一个固定的安全属性，系统利用安全属性来确定一个用户是否可以访问某个文件。它通过无法回避的访问限制来防止某些对系统的非法入侵。要防止特洛伊木马偷窃某个文件，就必须采用强制访问控制手段，基本方法有：限制访问控制和过程控制。

第十章

46、防火墙规则的处理方式中，reject 和 drop 的区别是什么？

Reject 拒绝数据包或信息通过，并且通知信息源该信息被禁止。

Drop 直接将数据包或信息丢弃，并且不通知信息源。

47、防火墙产品的两条基本原则是什么？

①一切未被允许的就是禁止的，“默认拒绝”；②一切未被禁止的就是允许的，“默认允许”。

48、包过滤防火墙和应用级网关《代理服务器》二者有何区别？

包过滤防火墙工作在网络协议 IP 层，它只对 IP 包的源地址、目标地址及相应端口进行处理，因此速度比较快，能够处理的并发连接比较多，缺点是对应用层的攻击无能为力。

代理服务器防火墙将收到的 IP 包还原成高层协议的通讯数据，比如 http 连接信息，因此能够对基于高层协议的攻击进行拦截。缺点是处理速度比较慢，能够处理的并发数比较少。

代理服务器是防火墙技术的发展方向，众多厂商都在提高处理速度的同时基于代理开发防火墙的更高级防护功能。P234

49、防火墙有哪些功能，存在哪些问题？

防火墙主要用于逻辑隔离外部网络与受保护的内部网络。对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

（防火墙是网络安全的屏障：防火墙可以强化网络安全策略：对网络存取和访问进行监控审计：防止内部信息的外泄： 内部网络和外部网络之间的所有网络数据流都必须经过防火墙，只有符合安全策略的数据流才能通过防火墙，防火墙自身应具有非常强的抗攻击免疫力。）

问题：防火墙不能防止内部攻击，不能防止未经过防火墙的攻击，不能取代杀毒软件，不易防止反弹端口木马攻击。

第十一章

50、入侵检测系统检测的入侵内容主要是什么？

外部攻击检测和内部特权滥用检测。

外部攻击检测：重点在于检测来自外部的攻击或入侵。

内部特权滥用检测：重点集中在观察授权用户的活动。

51、入侵检测系统按引擎类别分，可以划分为几种类型，这些引擎实现的方法是什么？

异常检查和模式匹配。异常检查，以历史数据或期望值为基础，为各个主体、对象的行为定义变量与该变量的基本值，利用加权函数组合变量，得出中和变量值，在此基础上，将入侵定义为出现了任何与期望值相比较有不可接受的偏差。

模式匹配，首先根据已知的入侵定义有独立的时间、时间的序列、时间临界值等通用规则组成的入侵模式，然后观察能与入侵模式相匹配的事件，达到发现入侵的目的。

52、商业 IDS 系统主要采用的技术有哪些？这些技术的特点是什么？

1.基于统计分析的入侵检测技术：稳定，但经常虚假报警。

2.基于神经网络的入侵检测技术：系统精简，成本低，但是十分不成熟。

3.基于专家系统的入侵检测技术：离成熟的实际应用还有一定距离。

4.基于模型推理的入侵检测技术：又称模式匹配，是应用较多的入侵检测方法。

第十三章

53、计算机病毒的定义和特征？

计算机病毒是一段附着在其他程序上的、可以自我繁殖的程序代码。

特征：传染性、非授权性、隐蔽性、潜伏性、破坏性、百科预见性和可触发性

54、计算机病毒一般有那几个部分构成？各自负责哪些功能？他们之间有什么联系？

构成：感染模块，触发模块，破坏模块，主控模块，相应为感染机制，触发机制，破坏机制。感染模块：是病毒进行感染动作的部分，负责实现感染机制。触发模块：主要检查预定触发条件是否满足，如果满足，返回真值，否则，返回假值。破坏模块：复责实施病毒的破坏动作。主控模块： 在总体上控制病毒程序的运行。

联系：病毒程序是一种特殊的程序，其最大特点是具有感染能力，病毒的感染动作受到触发机制的控制，同时触发机制还控制了病毒的破坏动作。但是不是所有病毒都具备有所有的模块。

55、蠕虫和病毒在定义上有什么区别？

凡能够引起计算机故障，破坏计算机数据的程序统称为计算机病毒。所以从这个意义上说，蠕虫也是一种病毒！网络蠕虫病毒，作为对互联网危害严重的 一种计算机程序，其破坏力和传染性不容忽视。与传统的病毒不同，蠕虫病毒以计算机为载体，以网络为攻击对象。

蠕虫：一种能够自动通过网络进行自我传播的恶意程序。它不需要附着在其他程序上，而是独立存在的。当形成规模、传播速度过快时会极大地消耗网络资源导致大面积网络拥塞甚至瘫痪。

病毒：一种具有隐蔽性、破坏性、传染性的恶意代码。病毒无法自动获得运行的机会，必须附着在其他可执行程序代码上或隐藏在具有执行脚本的数据文件中才能被执行。

56、阐述病毒检测的主要技术。

特征值检测技术，校验和检测技术，行为监测技术，启发式扫描技术，虚拟机技术等。

57、根据自己的感受，写出病毒预防的基本策略。

1）检查外来文件 2)局域网预防 3）购买正版软件 4）小心运行可执行文件 5）使用确认和数据完整性工具 6)周期性备份工作文件 7）留心计算机出现的异常 8）及时升级抗病毒工具的病毒特征库和有关的杀毒引擎 9）建立健全的网络系统安全管理制度，严格操作规程和规章制度。

其他预防措施有：不需要每次从软盘启动，不要依赖于 BIOS 内置的病毒防护，不要过分相信文档编辑器内置的宏病毒保护，因为内置病毒防护容易被用户和病毒关闭。

第十六章

58、什么是计算机取证？

指对能够为法庭接受的、足够可靠和有说服性的，存在于数字犯罪场景（计算机和相关外设）中的数字证据的确认、保护、提取和归档的过程。

59、和传统的物证想比，电子证据有什么相同点和不同点？

相同点：可信的、准确的、完整的、使法官信服的、符合法律法规的。

不同点：表现形式和存储格式的多样性、高科技性和准确性、脆弱性和易毁坏性、数据的“挥发性”

优点：可以被精确地复制；用适当的软件工具和原件对比，很容易鉴别当前的电子证据是否有改变；一些情况下，犯罪嫌疑人完全销毁电子证据是比较困难的；

60、试述计算机取证的原则和步骤？

原则：a 尽早收集证据，并保证没有收到任何破坏；

b 必须保证取证过程中计算机病毒不会被引入目标计算机；

c 不要在为作为证据的计算机上执行无关的程序

d 必须保证“数据连续性”

e 整个检查、取证过程必须是受到监督的；

f 要妥善保存得到的无证，必须保证提取出来的可能有用的证据不会收到机械或电磁损害；

g 详细记录所有的取证活动。

步骤： A 在取证检查中，保护目标计算机系统，使之远离磁场，避免发生任何的改变、伤害、数据破坏或者病毒感染，并对系统进行数据备份；

B 搜索目标系统中的所有文件

C 全部恢复所发现的已删除文件

D 最大程度的现实操作系统或应用程序的隐藏文件、临时文件和交换文件的内容

E 法律允许的情况下，访问被保护或加密文件的内容

F 分析获得的各种数据及在磁盘的特殊区域中发现所有相关数据

G 打印目标对计算机系统的全面分析结果，以及所有可能有用的文件和被挖掘出来的文件数据清单；

H 给出必须的专家证明/或在法庭上的正词。

过程：数据获取、数据分析、证据陈述

61、试述计算机取证有哪些常用技术？

数据获取技术、数据分析技术、数据获取、保全、分析技术。

（数据获取技术：对计算机系统和文件的安全获取技术；对数据和软件的安全搜集技术；对磁盘或其他存储介质的安全无损备份技；对已删除文集的恢复、重建技术；对磁盘空间、未分配空间和自由空间中包含的信息的发掘技术；对交换文件、缓存文件临时文件中包含的信息的复原技术；计算机在某一特定时刻活动内存中的数据的搜集技术；网络流动数据的获取技术、

数据分析技术：文件属性分析技术、文件数字摘要分析技术、日志分析技术；根据已获得的文件或数据的用词语法和写作风格，推断出其可能的作者的分析技术；发掘同一事件的不同证据间的联系的分析技术；数据解密技术；密码破译技术；对电子介质中的保护信息的强行访问技术。

数据获取、保全、分析技术：
电子数据证据保全技术：数据加密技术、数字摘要技术、数字签名技术、数字证书
电子数据证据分析技术：操作系统日志分析、防火墙日志分析、IDS 软件日志分析、
应用软件日志分析
电子数据证据鉴定技术：设备来源鉴定，软件来源鉴定，IP 地址来源鉴定
电子数据证据内容分析技术：文件系统的本地数据或网络数据，周边数据）

62、简述蜜罐的目的和蜜罐系统的工作原理

蜜罐技术是一种主动防御技术，是入侵检测技术的一个重要发展方向。
目的： 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。
工作原理：是一个包含漏洞系统的诱骗系统，通过模拟一个或多个易受攻击的主机，给攻击者提供一个容易攻击的目标，同时，让所有试图与其进行连接的攻击者浪费时间，延缓对真正目标的攻击，从而使目标系统得到保护。

63、现阶段计算机的取证技术的局限和不足，如何解决？

虽然计算机取证的理论和软件在计算机安全领域内取得了重大的成就，但是当前的计算机取证技术还存在着一定的局限性，在实践中适用的计算机取证工具还比较少。
当前国内外计算机取证技术还存在很大局限性。这主要表现在两方面：

（1）计算机取证所面临的入侵者的犯罪手段和犯罪技术的变化。这主要是指反取证技术的发展。反取证技术就是删除或隐藏证据使取证调查失效，包括数据擦除、数据隐藏和数据加密等 3 类，这些都给取证工作带来新的挑战。

（2）计算机取证技术是一个新的研究领域，致力于专业技术研发的机构还比较少。尽管个别公司投入了大量的人力物力在研究上，但由于国内没有相关的专业技术认证标准，因此不仅使得我国研发公司在获证方面困难重重，也让取证部门在选择工具时缺乏可比性，这就使得取证权威性受到质疑。

由于自身的局限性和计算机犯罪手段的变化，现有的取证技术还必须不断地发展，如取证的领域扩大，取证工具向着专业化和自动化方向发展，融合其他理论和技术如磁盘数据恢复技术、反向工程，取证的工具和过程标准化等，从而在不久的将来缔造出一个更加安全、纯净的信息和网络安全空间。

64、常规密钥体制与公开密钥体制分别有何特点和优缺点？请举例说明

常规密钥体制：优点是加密解密速度快，加密算法简单高效，保密度强。不足：密钥必须通过安全途径传送,因此密钥管理至关重要。密钥的保密相当重要。

传统的加密方法是加密、解密使用同样的密钥，由发送者和接收者分别保存，在加密和解密时使用，采用这种方法的主要问题是密钥的生成、注入、存储、管理、分发等很复杂，特别是随着用户的增加，密钥的需求量成倍增加。在网络通信中，大量密钥的分配是一个难以解决的问题。例如，若系统中有 n 个用户，其中每两个用户之间需要建立密码通信，则系统中每个用户须掌握(n-1)/2 个密钥，而系统中所需的密钥总数为 n*(n-1)/2 个。对 10 个用户的情况，每个用户必须有 9 个密钥，系统中密钥的总数为 45 个。对 100 个用户来说，每个用户必须有 99 个密钥，系统中密钥的总数为 4950 个。这还仅考虑用户之间的通信只使用一种会话密钥的情况。如此庞大数量的密钥生成、管理、分发确实是一个难处理的问题。

公开密钥体制，使用不同的加密密钥与解密密钥，优点：可以适应网络的开放性要求。且密钥管理问题也比较简单，尤其可以方便地实施数字签名和身份验证。不足：其算法复杂，加密速度低。实际中经常将常规密钥体制和公开密钥体制结合在一起使用,如利用 DES 加密信息,用 RSA 来传递会话密钥。

在公开密钥密码体制中，加密密钥（即公开密钥）PK 是公开信息，而解密密钥（即秘密密钥）SK 是需要保密的。加密算法 E 和解密算法 D 也都是公开的。虽然秘密密钥 SK 是由公开密钥 PK 决定的，但却不能根据 PK 计算出 SK。与传统的加密方法不同，该技术采用两个不同的密钥来对信息加密和解密，它也称为“非对称式加密方法”。每个用户有一个对外公开的加密算法 E 和对外保密的解密算法 D，
公开密钥体制特点： (1) 发送者用加密密钥 PK 对明文 X 加密后，在接收者用解密密钥 SK 解密，即可

恢复出明文，或写为： Dsk(Epk(X)) = X 解密密钥是接收者专用的秘密密钥，对其他人都保密。此外，加密和解密的运算可以对调，即 Epk(Dsk(X)) = X (2) 加密密钥是公开的，但不能用它来解密，即 Dpk(Epk(X)) X (3) 在计算机上可容易地产生成对的 PK 和 SK。 (4) 从已知的 PK 实际上不可能推导出 SK，即从 PK 到 SK 是“计算上不可能的”。 (5) 加密和解密算法都是公开的。

（RSA 算法解决了大量网络用户密钥管理的难题。RSA 并不能替代 DES，它们的优缺点正好互补。 RSA 的密钥很长，加密速度慢，而采用 DES，正好弥补了 RSA 的缺点。即 DES 用于明文加密，RSA 用于 DES 密钥的加密。由于 DES 加密速度快，适合加密较长的报文；而 RSA 可解决 DES 密钥分配的问题。美国的保密增强邮件（PEM）就是采用了 RSA 和 DES 结合的方法，目前已成为 E-MAIL 保密通信标准。）