信息安全导论

一．简述ping指令，ipconfig指令，netstat指令，net指令，at指令的功能和用途？

PING (Packet Internet Grope)，因特网包探索器，用于测试网络连接量的程序。Ping发送一个ICMP回声清求消息给目的地并报告是否收到所希望的ICMP回声应答。
□□它是用来检查网络是否通畅或者网络连接速度的命令。作为一个生活在网络上的管理员或者黑客来说，ping命令是第一个必须掌握的DOS命令，它所利用的原理是这样的：网络上的机器都有唯一确定的IP地址，我们给目标IP地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包我们可以确定目标主机的存在，可以初步判断目标主机的操作系统等。□□Ping是Windows系列自带的一个可执行命令。利用它可以检查网络是否能够连通，用好它可以很好地帮助我们分析判定网络故障。应用格式：Ping IP地址。该命令还可以加许多参数使用，具体是键入Ping按回车即可看到详细说明。□□

IPconfig 查看ip 掩码 网关 更多用来做故障分析□

net：功能很强大，内容很复杂，一下子说不清楚，简单而言就是本机与其它的机子建立各种各样的网络链接的命令。

netstat：查看当前本地计算机的网络连接状态□

二． 黑客攻击的一般流程及其技术与方法。

黑客是利用技术手段进入其权限以外的计算机系统。

一般流程：隐藏自身-踩点—扫描—查点—分析并入侵—获取权限—提升权限—扩大范围—安装后门—清除日志。

攻击行为：1.预攻击探测2.密码破解攻击3.缓冲区溢出攻击4.欺骗攻击5.DOS/DDOS攻击

6.SOL注入攻击7.木马攻击8.网络蠕虫9.CGI攻击10.恶意软件

三． Windows 系统日志有哪些？如何清除这些日志？

应用程序日志，安全日志、系统日志、DNS服务器日志、FTP日志、WWW日志。

FTP日志和WWW日志:先停掉相关服务，然后再删日志！

安全日志:打开“控制面板”的“管理工具”中的“事件查看器”，在菜单的“操作”项有一个名为“连接到另一台计算机”的菜单，输入远程计算机的IP，然后选择远程计算机的安全性日志，右键选择它的属性：
点击属性里的“清除日志”按钮，OK！安全日志清除完毕！

四．信息安全所受的威胁？信息保障的主要内容。

威胁：服务干扰、恶意访问、自身失误、信息泄露、破坏信息的完整性、拒绝服务、非法使用、窃听、业务流分析、假冒、旁路控制、内部攻击、特洛伊木马、陷阱门、抵赖、重放、计算机病毒、员工泄露、媒体废弃、物理侵入、窃取、业务欺骗

内容：关信息安全学关注信息本身的安全，而不管是否应用了计算机作为信息处理的手段。信息安全的任务是保护信息财产，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等。这样可以使得我们在最大限度地利用信息为我们服务的同时而不招致损失或使损失最小。

五． 什么是计算机病毒？按感染对象的方式可将病毒分为哪几类？

1）编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒（Computer
Virus）。具有破坏性，复制性和传染性。算机病毒是人为制造的具有破坏性的程序，计算机病毒运行时非授权入侵，计算机病毒可以隐藏在可执行文件或数据文件中。

2）分类：源码型病毒、嵌入型病毒、外壳型病毒、操作系统性病毒。

六． 简述DES加密过程和解密过程的区别.

Des加密将64位明文经初始换位后,在密钥的参与下进行了16轮次非线性变换.
再进行和初始换位相逆的位置变换,便得出密文，实际上就是解密过程的逆运算。

 DES算法的入口参数有3个：Key，Data和Mode。其中Key为8个字节共64位，

是DES算法的工作密钥。Data也为8个字节64位，是要被加密或被解密的数据。Mode为DES的工作方式有两种：加密或解密。

 DES算法的原理是：如Mode为加密，则用Key把数据Data进行加密，生成Data

的密码形式（64位）作为DES的输出结果；如Mode为解密，则用Key把密码形式的数据Data解密，还原为Data的明码形式（64位）作为DES的输出结果。

七． 简述网络蜜罐技术的原理。

定义：蜜罐原理核心价值就是在于对黑客攻击活动进行监视、监测和分析。蜜罐是一种资源，它的价值是被攻击或攻陷。这就意味着蜜罐是用来被探测、被攻击甚至最后被攻陷的，蜜罐不会修补任何东西，这样就为使用者提供了额外的、有价值的信息。蜜罐不会直接提高计算机网络安全，但是它却是其他安全策略所不可替代的一种主动防御技术。蜜罐系统最为重要的功能是对系统中所有操作和行为进行监视和记录，可以网络安全专家通过精心的伪装，使得攻击者在进入到目标系统后仍不知道自己所有的行为
已经处于系统的监视下。为了吸引攻击者，通常在蜜罐系统上留下一些安全后门以吸引攻击者上钩，或者放置一些网络攻击者希望得到的敏感信息，当然这些信息都是虚假的信息。另外一些蜜罐系统对攻击者的聊天内容进行记录，管理员通过研究和分析这些记录，可以得到攻击者采用的攻击工具、攻击手段、攻击目的和攻击水平等信息，还能对攻击者的活动范围以及下一个攻击目标进行了解。同时在某种程度上，这些信息将会成为对攻击者进行起诉的证据。不过，它仅仅是一个对其他系统和应用的仿真，可以创建一个监禁环境将攻击者困在其中，还可以是一个标准的产品系统。无论使用者如何建立和使用蜜罐，只有它受到攻击，它的作用才能发挥出来。 八． 网络后门和木马？及其区别？

什么是木马

“木马”全名叫“特洛伊木马”，它的使用者是黑客，更确切的说是“骇客”，它主要是“骇客”

通过欺骗用户的方法（包含捆绑，利用网页等）让用户不知不觉的安装到他们系统中的一类软件，主要功能有远程控制，盗密码等。木马的名字就指出了它的特征，那就是具有欺骗性，软件的分类不应该看它的功能，而是应该看它的特征。现在有些木马的开发者不喜欢把自己开发的木马叫作“木马”，而是叫“远程控制软件”。原因很简单，“木马”是贬义的，“远程控制软件”就是褒义的了，这样做也可以理解，因为毕竟 “木马”也包含在扩充了意义的“远程控制软件”中了。

木马的特征也是好多人讨厌它的原因，因为被人欺骗了总是很痛苦的，特别是被人欺骗了感情；好多木马都有盗密码功能，这是让人讨厌它的另一个原因.

什么是后门

“后门”是黑客在入侵了计算机以后为了以后能方便的进入该计算机而安装的一类软件，它的使用者是水平比较高的黑客，他们入侵的机器都是一些性能比较好的服务器，而且这些计算机的管理员水平都比较高，为了不让管理员发现，这就要求“后门”必须很隐蔽，因此后门的特征就是它的隐蔽性。木马的隐蔽性也很重要，可是由于被安装了木马的机器的使用者一般水平都不高，因此相对来说就没有后门这么重要了。后门和木马的区别就是它更注重隐蔽性但是没有欺骗性，因此它的危害性没有木马大，名声介于“远程控制软件”和“木马”之间。

所谓“后门”就是程序开发者为了完善自己设计的程序这一目的开设的特殊接口（通道），便于自己对程序进行修改，一般都拥有最高权限。而木马是利用后门或已发现的漏洞非法入侵用户的计算机，从事侵害用户利益的活动。至于远程控制，则是更广泛的概念，它是一种技术，包括使用木马或者别的手段，也包括正当用途的远程管理和维护。所以说，远程控制技术是把双刃剑。木马可以说是远程控制的一种，其实质只是一个网络客户/服务程序。网络客户/服务模式的原理是一台主机提供服务（服务器），另一台主机接受服务（客户机）。作为服务器的主机一般会打开一个默认的端口并进行监听（Listen），如果有客户机向服务器的这一端口提出连接请求（Connect
Request），服务器上的相应程序就会自动运行，来应答客户机的请求，这个程序

称为守护进程。就我们前面所讲的木马来说，被控制端相当于一台服务器，控制端则相当于一台客户机，被控制端为控制端提供服务。

九．简述缓冲区溢出攻击的原理

缓冲区溢出是由编程错误引起的。如果缓冲区被写满，而程序没有去检查缓冲区边界，也没有停止接收数据，这时缓冲区溢出就会发生。缓冲区边界检查被认为是不会有收益的管理支出，计算机资源不够或者内存不足是编程者不编写缓冲区边界检查语句的理由，然而摩尔定律已经使这一理由失去了存在的基础，但是多数用户仍然在主要应用中运行十年甚至二十年前的程序代码。 □□
缓冲区溢出之所以泛滥，是由于开放源代码程序的本质决定的。一些编程语言对于缓冲区溢出是具有免疫力的，例如Perl能够自动调节字节排列的大小，Ada95能够检查和阻止缓冲区溢出。但是被广泛使用的C语言却没有建立检测机制。标准C语言具有许多复制和添加字符串的函数，这使得标准C语言很难进行边界检查。C＋＋略微好一些，但是仍然存在缓冲区溢出。一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误，但是，如果输入的数据是经过“黑客”或者病毒精心设计的，覆盖缓冲区的数据恰恰是“黑客”或者病毒的入侵程序代码，一旦多余字节被编译执行，“黑客”或者病毒就有可能为所欲为，获取系统的控制权。

十．安全审计的目的和功能。

目的：使信息系统自动记录下网络中机器的使用时间、敏感操作和违纪操作等；

功能：为系统进行事故原因查询、定位、事故发生前的预测、报警以及为事故发生后的实时处理提供详细可靠的依据或支持。

十一．恶意代码是什么？它的具体内容有哪些？

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。

它包括计算机病毒、蠕虫、特洛伊木马、逻辑炸弹、病菌、用户级RootKit、核心级RootKit、脚本恶意代码和恶意ActiveX 控件等。

十二．简述容灾和备份之间的关系。

1）容灾和备份的目的不同

容灾系统的目的在于保证系统数据和服务的“在线性”，即当系统发生故障时，仍然能够正常地向网络系统提供数据和服务，以使系统不致停顿。

而备份技术的目的与此并不相同，备份是“将在线数据转移成离线数据的过程”，其目的在于应付系统数据中的逻辑错误和历史数据保存。

2）备份是基石

备份是指为防止系统出现操作失误或系统故障导致数据丢失，而将全系统或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程。

备份是数据高可用的最后一道防线，其目的是为了系统数据崩溃时能够恢复数据。

3）容灾不可少

那么建设了备份系统，是否就不需要容灾系统？这还要看业务部门对RTO（恢复所需的时间指标）/RPO（能够恢复到的最新状态）指标的期望值，如果允许1TB的数据库RTO = 8小时，RPO = 1天，那备份系统就能满足要求。同时，备份的目的在于应付系统数据中的逻辑错误和历史数据保存。只能够满足数据丢失、数据破坏时的数据恢复目的，而不能提供实时的业务接管功能。

因此容灾系统对于某些关键业务而言也是必不可少的。人们谈及容灾往往是针对当生产系统，不能正常工作时，其业务可由容灾系统接替这些业务，继续进行正常的工作。
能够提供很好的RTO和RPO指标。同时远程容灾系统具备应付各种灾难，特别是区域性与毁灭性灾难的能力，具备较为完善的数据保护与灾难恢复功能，保证灾难降临时数据的完整性及业务的连续性，并在最短时间内恢复业务系统的正常运行，将损失降到最小。

4）容灾不能替换备份

容灾系统会完整地把生产系统的任何变化复制到容灾端去，包括不想让它复制的工作，比如不小心把计费系统内的用户信息表删除了，同时容灾端的用户信息表也会被完整地删除。如果是同步容灾，那容灾端同时就删除了；如果是异步容灾，那容灾端在数据异步复制的间隔内就会被删除。这时就需要从备份系统中取出最新备份，来恢复被错误删除的信息。因此容灾系统的建设不能替代备份系统的建设。

相关文档：