C1网络攻防(网络侦查获取目标信息,网络攻击抑制/入侵/控制,网络防护防止被攻击),漏洞分析与利用是核心.网络安全指网络系统的硬件\软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭受到破坏\更改\泄露,系统连续可靠正常地运行,网络服务不中断.可分信息系统(主机服务器)\网络边界及网络通信的安全.目标是保护网络系统中信息的机密性(保证信息不能被非授权访问, 通过访问控制阻止非授权用户获得机密信息,通过加密变换阻止非授权用户获知信息内容)\完整性(维护信息的一致性即信息在生成\传输\存储和使用过程中不应发生人为或非人为的非授权篡改.一般通过访问控制阻止篡改行为,同时通过消息摘要算法来检验信息是否被篡改.数据没有被(未授权)篡改或者损坏&系统未被非法操纵,按既定的目标运行)\可用性(保障信息资源随时可提供服务的能力特性,即授权用户可据需随时访问所需信息.是信息资源服务功能和性能可靠性的度量,涉及到物理\网络\系统\数据\应用和用户等多方面的因素,是对信息网络总体可靠性的要求)(信安三要素)\不可抵赖性(信息交互过程中,所有参与者不能否认曾经完成的操作或承诺)\真实性(要求信息所涉事务客观存在,信息要素真实齐全,信息来源真实可靠)\可控性(对信息的传播及内容具有控制能力.也就是可以控制用户的信息流向,对信息内容进行审查,对出现的安全问题提供调查和追踪手段)\可审查性(基于可控性,出现安全问题时提供依据与手段)\保鲜性(信息在时效之内,对物联网安全很重要)等安全属性|网络安全体系结构是安全服务(X.800定义:为了保证系统或数据传输有足够的安全性,开放系统通信协议所提供的服务. RFC2828定义:一种由系统提供的对资源进行特殊保护的进程或通信服务)\安全机制(一种措施或技术,一些软件或实施一个或更多安全服务的过程.常用有认证\访问控制\加密\数据完整性\审计等机制)\安全策略(在某个安全域内,施加给所有与安全相关活动的一套规则)及相关技术(与安\*服务和安\*机制对应的一系列算法\方法或方案,体现在相应的软件或管理规范等之中.如密码\数字签名\防火墙\入侵检测\防病毒\访问控制等)的集合.分层(应用\*HTTPS/SSH/FTPS传输\*SSL/TLS网络\*IPSec网络接口\*PPTP/L2TP)也可将网络安全体系结构看作是网络协议层次\安全功能和安全技术的集合|攻防体系:网络攻击是指采用技术手段,利用目标信息系统的安全缺陷,破坏网络信息系统的(保密性\完整性\真实性\可用性\可控性与可审查性)等的措施和行为.其目的是窃取\修改\伪造或破坏信息,以及降低\破坏网络使用效能.网络防护是指为保护己方网络和设备正常工作\信息数据安全而采取的措施和行动.其目的是保证己方网络数据的(6性)等|计网脆弱性及面临安全威胁: 1)网络基础协议存在安全漏洞TCP/IP协议设计问题,地址欺骗\源路由攻击2)网络硬件存在安全隐患3)软件缺陷和安全漏洞 对程序输入处理不当\缺乏适当的用户身份认证\对程序功能配置不当4)操作系统存在安全隐患(是软件系统\功能过多配置复杂\安全级别不高\国外引进难保证安全)5)网络体系结构的安全风险(传统的/跨域的安全问题);主要威胁(人为/恶意/非←/内外部)1)各种自然因素2)内部窃密和破坏(内部涉密人员有意或无意泄密\更改记录信息;内部非授权人员有意无意偷窃机密信息\更改网络配置和记录信息;内部人员破坏网络系统)3)信息的截获和重演(线路窃听)4)非法访问(非法用户未经授权使用网络资源或合法用户以未授权的方式使用网络资源)5)破坏信息的完整性(改变信息流的时序,更改信息的内容;删除某个消息或消息的某些部分;在消息中插入一些信息,让收方读不懂或接收错误的信息)6)欺骗(冒充合法地址或身份欺骗网络中的其它主机及用户;冒充网络控制程序套取或修改权限\口令\密钥等信息,越权使用网络设备和资源;接管合法用户,欺骗系统,占用合法用户的资源)7)抵赖8)破坏系统可用性;安全威胁主要利用网络与信息系统存在的脆弱性和网络管理中的漏洞|主要技术与分类:系统角度:侦查(网络信息探测,是指运用各种技术手段\采用适当的策略对目标网络进行探测扫描,获得有关目标计算机网络系统的拓扑结构\通信体制\加密方式\网络协议与操作系统\系统功能,以及目标地理位置等各方面的有用信息,并进一步判别其主控节点和脆弱节点,为实施网络攻击提供可靠的情报保障;1)端口探测2)漏洞探测(硬件\软件\协议的具体实现或系统安全策略上不可避免会存在缺陷.如果这些缺陷能被攻击者利用,则这样的缺陷称为漏洞.模拟攻击/信息型漏洞探测.nmap -sV IP)3)隐蔽侦查4)渗透侦查(木马等))/攻击(利用目标漏洞,为窃取/修改/伪造/破坏信息,及降低\破坏网络使用效能而采取的各种措施和行动.目的破坏网络信息系统的安全属性.1)拒绝服务(降低或剥夺目标系统的可用性,使合法用户得不到服务或不能及时得到服务,一般通过耗尽网络带宽或耗尽目标主机资源的方式进行)2)入侵,通过漏洞非法进入系统获得权限3)病毒,具有感染性和寄生性的代码,隐藏在目标系统中自我复制\传播\侵入其他程序4)恶意代码,任何可以在计/网间传播的可执行代码,目的是在未授权的情况下有目的地更改或控制计算机及网络系统.典型的:计算机病毒\木马\后门\逻辑炸弹\蠕虫)5)电子邮件6)诱饵,建立诱饵网站,诱骗用户浏览恶意网页,是被动攻击./防护(为保护己方网络设备正常工作,保护信息数据安全而采取的措施和行动,目的保护网络信息系统的安全属性.走管理和技术相结合的道路,技术上有防火墙(实现网络访问控制的装置,最基本的网络防护措施,使用最广泛的网络安全防护技术.主要有数据包过滤和代理服务技术)\入侵检测(动态安全技术通过对入侵行为的过程与特征的研究,使安全系统对入侵事件和入侵过程能做出实时响应.基于特征的和基于行为的,也称误用检测和异常检测.实现方式上分基于主机/网络的入侵检测系统)\病毒防护(主要方法是特征码及行为分析法)\数据加密(主要研究数据的加密和解密及其应用)\认证(身份认证是验证信息的发送者的真实身份;信息认证验证信息的完整性,即验证信息在传送或存储过料中是否被篡改\重放或延迟等)\蜜罐(将攻击者从关键系统引诱开的诱骗系统),主要目标:1)进不来:用访问控制机制,允许授权用户访问,阻止非授权用户进入网络,从而保证网络系统的可控性和可用性2)拿不走:用授权机制,实现对用户的权限控制,同时结合内容审计机制,实现对网络资源及信息的可控性3)看不懂:使用加密机制,确保信息不暴露给未授权的实体或进程,从而实现信息的保密性4)改不了:使用数据完整性鉴别机制,保证只有得到允许的人才能修改数据,从而确保信息的完整性和真实性5)走不掉:使用审计\监控\防抵赖等安全机制,使破坏者走不脱.并进一步对网络出现的安全问题提供调查依据和手段,实现信息安全可审查性)国家网络空间安全战略:个别国家强化网络威慑战略,加剧网络空间军备竞赛,世界和平收到新的挑战.C2基础知识net启停服务net start/stop servicename启[停]共享net share sharename [/del](net share c=c:\)[删除][映射]磁盘net use drivename [/del] [\\ip\drive /user:username]添[删]用户net user username password /add[/del]将用户加入组net localgroup administrators username /add[/del]激活/关guest账号net user guest /active:yes[no]|telnet IP [Port]|ftp [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-w:windowsize] [-A] [host]|计划任务at [\\computername] [[id] [/DELETE] | [/DELETE [/YES]]或at [\\computername] time［/INTERACTIVE］[/EVERY:date[,…] | [/NEXT:date[,…]] command|查看修改文件夹权限cacls filename [/T][/E][/C] [/G user : perm] [/R user[…]] [/P user : perm […]] [/D user […]]|echo text >[>>] file ^>转义|查看当前系统(仅W2003)用户情况query [process|session|termserver|user]|终止会话logoff [sessionname | sessionid] [server:servername] [/V]|ipconfig [/all][/renew]|tracert查看通信路由|nslookup|netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]|route [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]|Linux:ls/mkdir/chown/chmod/telnet/echo/ping/traceroute/ifconfig/ netstat/grep/ps/export/lsmod(list modules)/insmod(install module)/gzip/tar|Windows的sc命令:用来与服务控制管理器和服务进行通信的命令行程序.sc query枚举活动服务和驱动程序,sc start启动服务,sc pause暂停服务|逻辑意义上的端口一般指TCP/IP协议中的端口即协议(网络)端口.作用:与进程关联的一种数据结构;分类:知名端口\动态端口\协议端口;在入侵中的作用:入侵的门窗;相关工具:netstat和nmap保护:查看\判断\关闭|互联网数据以高位字节优先顺序传输.C3密码学主要保护机密性完整性,基于计算复杂性的计算机密码学迅速发展,要求密码算法公开密钥必须保密.研究如何隐密地传递信息的学科,其首要目的是隐藏信息的涵义.用某种方法伪装消息以隐藏它的内容的过程称为加密把密文转变为原始明文的过程称为解密.除机密性外,密码学需提供三功能:鉴别(消息的接收者应该能够确认消息的来源;入侵者不可能伪装成他人)\完整性(消息的接收者应该能够验证在传送过程中的消息没有被修改;入侵者不可能用假消息代替合法消息)\抗抵赖性(发送消息者事后不可能虚假地否认他发送的消息)对称密码算法有时又叫传统密码算法,加密密钥能够从解密密钥中推算出来,反过来也成立,对称算法的安全性依赖于密钥的保密,最大优势速度快.分组密码算法:对明文的一组位进行加密和解密运算,这些位组称分组,相应算法称分组算法.常见的分组算法有DES(分组64密钥64算法使用其中56)(变换(置换)明文x0=IP(x)=L0R0;按照规则进行16轮迭代Li=Ri-1,Ri=Li⊕f(Ri-1,Ki)(i=1…16),f由S盒置换构成Ki;逆置换L16R16)\DES3\IDEA\AES(分组128密钥长128\192\256);序列(流)密码算法:一次只对明文的单个位(或字节)运算的算法称为序列密码算法或流密码.常见的流密码有RC4\A5\SEAL\PIKE;密码协议:也称作安全协议,是使用密码学的协议,是以密码学为基础的消息交换协议,其目的是在网络环境中提供各种安全服务.常见的安全协议有:认证\不可否认\公平性\身份识别\密钥管理协议.密码编码原则:密码算法应建立在算法的公开不影响明文和密钥的安全.公钥加密算法加密解密密钥不同,解密密钥不能根据加密密钥计算出来,至少在可以计算的时间内不能.有RSA\ElGamal\背包算法\Rabin(RSA的特例)\Diffie－Hellman密钥交换协议中的公钥加密算法\椭圆曲线加密算法ECC.最广泛RSA算法,ElGamal也常用.RSA:密钥计算:选择两个大素数p和q(典型1024bit)计算n=pq和z=(p-1)(q-1)选择一个与z互质的数d,找到e使e×d=1modz,公钥为(e,n)私钥为(d,n);加密:k位块P,k满足2^k<n,C=P^e(mod n)解密:P=C^d (mod n).|消息摘要(高速的完整性鉴别)与数字签名(防止抵赖):前者使用散列函数H计算消息摘要,加密后的消息摘要也称为消息鉴别标签.H需要满足特性:输入任意长,输出固定长;任意给定输入,容易计算;单向性;抗弱碰撞(对给定x要找y≠x且H(y)=H(x)在计算上不可能);抗强碰撞/生日攻击(找到一对(x,y)满足H(y)=H(x)在计算上不可能).常用的MD5(128bit)\SHA序列函数(-1=160bit,-2=256/384/512bit).数字签名指用户用自己的私钥对原始数据的消息摘要进行加密所得的数据,即加密的摘要.可确保消息来源真实性和数据传输完整性|PGP:PGP随机生成密钥,用IDEA算法加密明文,然后用RSA算法加密密钥.既有RSA算法的保密性和认证性,又保持了IDEA算法速度快的优势.提供五种服务:鉴别,机密性,压缩,兼容电子邮件,分段.C4虚拟专用网(VPN)技术即虚拟专用网络是企业网在因特网(或其他公共网络)上的扩展.VPN在因特网上开辟一条安全的隧道,以保证两个端点(或两个局域网)之间的安全通信.VPN构建于廉价的因特网之上,可以实现远程主机与局域网(内网)之间的安全通信,也可以实现任何两个局域网之间的安全连接功能是将因特网虚拟成路由器,将物理位置分散的局域网和主机虚拟成一个统一的虚拟企业网.组成:VPN服务器\VPN连接（公共网络）\协议隧道\VPN客户机原理:VPN综合利用了隧道技术\加密技术\鉴别技术和密钥管理等技术,在公共网络之上建立一个虚拟的安全通道,实现两个网络或两台主机之间的安全连接分类:(应用场合)远程访问VPN,网关-网关VPN;(按隧道协议分类)隧道协议是一个网络协议的载体,使用隧道的原因是在不兼容的网络上传输数据,或在不安全网络上提供一个安全路径,隧道协议可能使用数据加密技术来保护所传输的数据.隧道协议实现在OSI模型或TCP/IP模型的各层协议栈,根据VPN协议在OSI模型的实现层次,VPN大致可以分为:第2层隧道协议(主要包括点到点隧道协议(PPTP)\第二层转发协议(L2F)\第2层隧道协议(L2TP),主要用于实现远程访问VPN)\第3层隧道协议(主要是IP安全(IPSec),用于在网络层实现数据包的安全封装, IPSec主要用于实现网关—网关VPN,也可实现主机-主机的安全连接)\第4层隧道协议((SSL):在传输层上实现数据的安全封装,主要用于保护两台主机的两个进程间的安全通信,安全的Web\安全的电子邮件等均使用了第4层隧道协议)\基于第2,3层隧道协议(MPLS)之间的VPN(也称为2.5层隧道协议,是利用MPLS路由器的标签特性实现的VPN).基于第2层隧道协议的VPN:第2层隧道协议在数据链路层对数据报进行封装,主要用于远程访问VPN.PPTPVPN:点对点隧道协议是实现VPN的方式之一.PPTP使用TCP创建控制通道来传送控制命令,以及利用通用路由封装(GRE)通道来封装点对点协议(PPP)数据包以传送数据.PPTP的协议规范本身并未描述加密或身份验证的部份,它依靠点对点协议(PPP)来实现这些安全性功能.PPTP因为易于设置和使用而流行,路由和远程访问服务中实现.L2TPVPN:第二层隧道协议是一种由数据链路层隧道协议,是一种虚拟隧道协议,通常用于虚拟专用网.L2TP协议自身不提供加密与可靠性验证的功能,可以和安全协议搭配使用,从而实现数据的加密传输.经常与L2TP协议搭配的加密协议是IPsec.Windows2003实现远程访问VPN:1)配置路由器Router2)配置远程访问服务器VPNServer3)配置VPN客户端.基于第3层隧道协议的IPSecVPN:互联网安全协议,是通过对IP协议(互联网协议)的分组进行加密和认证来保护IP协议的网络传输协议族(一些相互关联的协议的集合).IPSec的组成:1)认证头AH:为IP数据报实现无连接的完整性和数据源认证功能,并能抵抗重放攻击2)封装安全有效载荷ESP:实现保密性\数据源认证\无连接的完整性\抗重放攻击的服务\有限的网络流的保密性3)安全联盟SA:给出算法和数据的集合,以向AH或ESP的操作提供必须的参数,安全联盟和密钥管理协议ISAKMP提供了认证和密钥交换的框架.IPSec两种工作模式:传输模式和隧道模式.传输模式用于两台主机之间的连接,在IP层封装主机-主机的分组,对原IP包的地址部分不做处理,仅对数据负载部分进行加密;隧道模式用于两个网关之间的连接,在IP层封装网关—网关的分组,可穿过公共网络实现局域网之间的互联,对整个IP数据包进行加密处理.AH和ESP均支持传输模式和隧道模式,实现认证和加密等安全功能.认证协议AH:AH数据报直接封装在IP数据报中,协议字段为51.AH和ESP同时保护数据时,AH头在ESP头之后.传输模式AH:新IP头拷贝自原IP头,协议字段为51,原协议字段拷贝到AH头的下一个头字段.隧道模式AH:重建IP头,新IP头的IP地址改成网关的IP地址,协议字段为51,AH头中的下一个头为4或41,原始数据包拷贝到AH头之后.AH头的格式:下一个头8‐bits,标识AH头后的载荷类型,在传输模式下可为6(TCP)或17(UDP);在隧道模式下将是4(IPv4)或41(IPv6).序列号抗重放攻击.封装安全载荷ESP:与AH协议一样,ESP数据报也直接封装在IP数据报中,协议字段为50.ESP数据报由四部分组成:头部\加密数据(包括ESP尾)\ESP验证数据.传输模式ESP:新IP头拷贝自原IP头,将协议字段改为50,原协议字段拷贝到ESP尾的下一个头.隧道模式ESP:重建IP头,新IP头的IP地址改成网关的IP地址,协议字段为50,ESP尾中的下一个头为4或41,原始数据包和ESP尾加密后拷贝到ESP头之后.ESP的数据报格式:序列号抗重播攻击.安全关联与安全策略:在AH和ESP头中有一个32bits的安全参数索引SPI,用于标识通信的两端采用的IPSec安全关联SA.安全关联(SA)是两个通信实体协商建立起来的一种安全协定,例如IPSec协议(AH或ESP)\IPSec的操作模式(传输模式和隧道模式)\加密算法\验证算法\密钥\存活时间等,是单工的,输出和输入都需要独立的SA.SA是通过IKE密钥管理协议在通信双方之间来协商的,协商完成后,通信双方都会在它们的安全关联数据库(SAD)中存储该SA参数.安全关联参数:1.安全参数索引号(SPI):一个与SA相关的位串,由AH和ESP携带,使得接收方能选择合适的SA处理数据包2.IP目的地址:目前只允许使用单一地址,表示SA的目的地址3.安全协议标识:标识该SA是AH安全关联或ESP安全关联.安全策略决定了为一个数据包提供的安全服务,它保存在安全策略数据库SPD中.安全策略数据库(SPD)记录了对IP数据流(根据源IP\目的IP\上层协议\流入还是流出)采取的安全策略.每一安全策略条目可能对应零条或多条SA条目,通过使用一个或多个选择符来确定某一个SA条目.Windows 2003实现网关-网关VPN:1)创建ServerA的IPSec策略2)创建ServerB的IPSec策略3)配置远程访问VPN服务器.C5防火墙定义:位于两个(或多个)网络之间执行访问控制的软件和硬件系统,它根据访问控制规则对进出网络的数据流进行过滤.处理方式:根据安全策略,防火墙对数据流的处理方式有三种:1.允许数据流通过2.拒绝数据流通过:通知发送方3.将这些数据流丢弃:不通知发送方.为了配置和管理方便,通常将内部网中需要向外部提供服务的服务器设置在单独的网段,这个网段被称为非军事区(DMZ).DMZ是周边网络,位于内部网之外,使用与内部网不同的网络号连接到防火墙,其中部署了Web服务器\ftp服务器\通信服务器等对外提供公共服务.DMZ隔离内外网络,并为内外网之间的通信起到缓冲作用.本质是一种能够限制网络访问的设备或软件.功能:是执行访问控制策略的系统,它通过监测和控制网络之间的信息交换和访问行为来实现对网络安全的有效管理.其遵循一种允许或禁止业务来往的网络通信安全机制,也就是提供可控的过滤网络通信,只允许授权的通信.因此,对数据和访问的控制\对网络活动的记录是防火墙的基本功能.1)访问控制功能:最基本和重要的功能,通过禁止或允许特定用户访问特定资源,保护内部网络的资源和数据2)内容控制功能:可以防止非法用户进入内部网络,也能禁止内网用户访问外网的不安全服务(比如恶意网站)3)日志功能:记录通过防火墙的信息内容和活动4)对网络攻击的检测和告警:当发生可疑动作时,防火墙能进行适当的报警,并提供网络是否受到监测和攻击的详细信息5)集中管理功能:针对不同的网络情况和安全需要,指定不同的安全策略,在防火墙上集中实施,使用中还可能根据情况改变安全策略.还可有流量控制\网络地址转换(NAT)\虚拟专用网(VPN)等功能.分类:根据防火墙在网络协议栈中的过滤层次不同,可以把防火墙分为三类:1.包过滤防火墙主要根据网络层的信息进行控制2.电路级网关防火墙主要根据传输层的协议信息进行过滤(一般作为代理服务器模块存在,也只检测包头)3.应用级网关防火墙主要根据应用层协议的信息进行过滤.包过滤防火墙也称为分组过滤防火墙,包过滤工作在网络层,也用到了传输层的协议端口号等信息.根据访问控制策略的实现机制的不同,又分为静态包过滤和动态包过滤.网络管理员首先根据企业的安全策略定义一组访问控制规则,然后防火墙在内存中建立一张与访问控制规则对应的访问控制列表.对每个数据包,如在访问控制列表中有对应的项,则防火墙按规则要求允许或拒绝数据包的通过,否则应用默认规则:默认丢弃/默然允许.静态包过滤防火墙的访问控制列表在运行过程中是不会动态变化的,其过滤规则只利用了IP与TCP/UDP报头中的几个字段.对数据包的处理过程:1)接收每个到达的数据包2)对数据包按序匹配过滤规则,对数据包的IP头和传输字段内容进行检查,如果数据包的头信息与一组规则匹配,则根据该规则确定是转发还是丢弃该数据包(3)如果没有规则与数据包头信息匹配,则对数据包施加默认规则.静态包过滤防火墙的判决仅依赖于当前数据包的内容,对数据包的检测是孤立的\无状态的,检查的内容包括:1.源IP地址2.目的IP地址3.应用或协议号4.源端口号5.目的端口号.优点:1)对网络性能的影响较小2)成本较低3)对用户透明.缺点:1)安全性较低2)缺少状态感知能力3)容易遭受IP欺骗攻击4)创建访问控制规则比较困难.动态包过滤防火墙:根据当前所交换的信息动态调整过滤规则表,动态包过滤技术能够通过检查应用程序信息以及连接信息,来判断某个端口是否需要临时打开.当传输结束时,端口又可以马上恢复为关闭状态,可以保证主机的端口没有一个是永远打开的,那么外界也就无从连接主机.只有在主机主动地跟外界连接时,其他的机器才可以跟它连接.工作原理:1.首先检测每一个有效连接的状态并根据这些信息决定网络的数据包是否能够通过防火墙2.然后通过从协议栈低层截取数据包,并将当前数据包及其状态信息和其前一时刻的数据包及其状态信息进行比较,从而得到该数据包的控制信息3.然后动态包过滤模块就开始截获,分析并处理所有试图通过防火墙的数据包,以保证网络的高度安全和数据完整.由于网络和各种应用的通信状态可以被动态存储到动态状态表中,结合预定义好的规则,动态包过滤模块就可以识别出不同应用的服务类型,同时还可以通过以前的通信及其他应用程序分析出目前这个连接的状态信息4.再接下来检验IP地址\端口以及其他需要的信息以便决定该通信包是否满足安全策略5.最后它还把会相关的状态和状态之间的关联信息存储到动态连接表中以随时更新其中的数据,通过这些数据,动态包过滤模块就可以观测到后继的通信信息.优点:1)高安全性2)高性能3)伸缩性和易扩展性4)针对性5)应用范围广.缺点:1)由于没有对数据包的净荷部分进行过滤,因此仍然只具有较低的安全性2)容易遭受IP地址欺骗攻击3)难于创建规则,管理员创建规则时必须要考虑规则的先后次序4)如果动态包过滤防火墙在连接建立时没有遵循RFC建议的三步握手协议,就会引入额外的风险:两次握手导致防火墙在DoS/DDoS攻击时因耗尽所有资源而停止响应.应用级网关防火墙:也称为代理防火墙,是实现内容过滤的主要技术之一.应用级网关防火墙针对每一种应用软件,均由对应的代理软件对其网络载荷进行分析和过滤.工作原理:应用级网关截获进出网络的数据包,对数据包的内容进行检查,如果符合所制定的安全规则,则允许数据通过;否则根据安全策略的要求进行处理.优点:1)在已有的安全模型中安全性较高:避免了服务器和客户机之间的直接连接2)具有强大的认证功能3)具有超强的日志功能4)应用级网关防火墙的规则配置比较简单.缺点:1)灵活性很差2)配置烦琐,增加了管理员的工作量3)性能不高,有可能成为网络的瓶颈.三种典型部署模式:屏蔽主机\双宿/多宿主机\屏蔽子网.堡垒主机是一种配置了较为全面的安全防范措施的网络上的计算机,它为网络间的通信提供了一个阻塞点.通常堡垒主机可以用作应用级和电路级网关的平台,是一个组织机构网络安全的中心主机.堡垒主机特征:1)堡垒主机硬件平台运行较为安全的操作系统,成为可信任的系统2)只有网络管理员认为必要的服务才会安装在堡垒主机上3)当允许一个用户访问代理服务时,堡垒主机可能会要求进行额外认证4)每一个代理都只能支持标准应用服务命令集中的一个子集5)每一个代理只允许访问指定主机的通信,这意味着每一个代理通过对所用的网络流量,每一个连接及其持续时间记录日志,保留了详细的审计信息,审计日志对检测和终止入侵者极为重要6)每一个代理模块都是一个为网络安全设计的一个很小的软件包7)代理之间相互独立8)代理通常无需进行磁盘访问,不需要读取初始配置文件9)堡垒主机是一个组织机构网络安全的中心主机.屏蔽主机模式防火墙:实质就是包过滤和代理服务功能的结合,堡垒主机担任了身份鉴别和代理服务的功能,这样的配置比单独使用包过滤防火墙或应用层防火墙更加安全.双宿/多宿主机模式防火墙:是一种拥有两个或多个连接到不同网络上的网络接口的防火墙,通常用一台装有两块或多块网卡的堡垒主机作为防火墙,每块网卡各自与受保护网络和外部网连接.该模式下,堡垒主机必须关闭了IP转发功能,其网关功能是通过提供代理服务而不是通过IP转发来实现的.屏蔽子网模式防火墙:最为安全的配置模式,采用了两个包过滤路由器:一个位于堡垒主机和外部网络之间,另一个位于堡垒主机和内部网络之间.该配置模式在内部网与外部网络之间建立了一个被隔离的子网:“非军事区”.防火墙存在的问题:1)不能防范不经由防火墙的攻击2)目前还不能防止感染了病毒的软件或文件的传输3)不能防止数据驱动式攻击4)还存在着安装\管理\配置复杂的缺点.性能指标:1)吞吐量2)时延3)丢包率4)背对背:描述网络设备成熟突发数据的能力5)最大位转发率6)最大并发连接数7)最大并发连接建立速率8)有效通过率.选择:1)安全性2)高效性3)适用性4)可管理性5)完善的售后.C6入侵检测入侵:试图破坏网络及信息系统机密性\完整性\可用性等安全属性的行为.入侵方式:1)未授权的用户访问系统资源2)已授权用户企图获得更高权限,或已授权用户滥用所给权限.入侵检测:是监测计算机网络和系统,发现违反安全策略事件的过程,是对企图入侵\正进行的入侵或已发生的入侵行为进行识别的过程.入侵检测系统(IDS):所有能够执行入侵检测任务和实现入侵检测功能的系统,自动监视并分析事件,一般位于内部网络入口处,安装在防火墙后面.IDS组成:数据收集器\检测器\知识库\控制器\用户接口组件.IDS任务:1)信息收集:系统和网络的日志文件\目录和文件中的异常改变\程序执行中的异常行为\网络活动信息2)信息分析:模式匹配\统计分析\完整性分析\安全响应.IDS功能:1)网络流量的跟踪与分析功能:跟踪用户进出网络的所有活动,实时检测并分析用户在系统中的活动状态,实时统计网络流量,检测拒绝服务攻击等异常行为2)已知攻击特征的识别功能:识别特定类型的攻击,并向控制台报警,为网络防护提供依据,根据定制的条件过滤重复告警事件,减轻传输与响应的压力3)异常行为的分析\统计与响应功能:分析系统的异常行为模式,统计异常行为,并对异常行为做出响应4)特征库的在线和离线升级功能:提供入侵检测规则的在线和离线升级,实时更新入侵特征库,不断提高IDS的入侵检测能力5)数据文件的完整性检查功能:检查关键数据文件的完整性,识别并报告数据文件的改动情况6)自定义的响应功能:定制实时响应策略,根据用户定义,经过系统过滤,对告警事件及时响应7)系统漏洞的预报警功能:对新发现或新公布的系统漏洞特征进行预报警8)IDS探测器集中管理功能:通过控制台收集探测器的状态和告警信息,控制各个探测器的行为9)容易配置和管理,自身具有很高的安全性IDS分类:1)基于网络的入侵检测系统(NIDS):数据来自网络上的数据流,能够截获网络中的数据包,提取其特征并与知识库中已知的攻击签名相比较,从而达到检测目的.优点是检测速度快\隐蔽性好\不容易受到攻击\不消耗被保护主机的资源;缺点是有些攻击是从被保护的主机发出的,不经过网络,因而无法识别2)基于主机的入侵检测系统(HIDS):通过对系统日志和审计记录的不断监控和分析来发现入侵.优点是针对不同操作系统捕获应用层入侵,误报少;缺点是依赖于主机及其子系统,实时性差3)分布式入侵检测系统(DIDS):能够同时分析来自多个主机系统的审计日志和来自网络的数据流,一般为分布式结构,由多个部件组成,克服了单一的HIDS和NIDS的不足.典型的DIDS采用控制台/探测器结构.NIDS和HIDS作为探测器放置在网络的关键节点,并向中央控制台汇报情况.攻击日志定时传送到控制台,并保存到中央数据库中,新的攻击特征能及时发送到各个探测器上,每个探测器能够根据所在网络的实际需要配置不同的规则集.CIDF模型:通用入侵检测框架,三个目的:1.IDS构件共享:一个IDS系统的构件可被另一个系统使用2.数据共享:即通过提供标准的数据格式,使得IDS中的各类数据可以在不同的系统之间传递并共享3.完善互用性标准:建立一套开发接口和支持工具,以提供独立开发部分构件的能力.CIDF组成:事件产生器:从整个的计算机环境中获得事件,并向系统的其他部分提供该事件;事件分析器:从事件产生器中获得数据,通过各种分析方法(一般为误用检测和异常检测方法)来分析数据,判定入侵是否已经发生或者正在发生;响应单元:对分析结果作出反应的功能单元;事件数据库:存放各种中间和最终数据的地方的总称,它可以是复杂的数据库也可以是简单的文本文件;目录服务构件:用于各构件定位其他的构件,控制其他构件传递的数据并认证其他构件的使用,以防止IDS系统本身受到攻击,它可以管理和发布密钥,提供构件信息和告诉用户构件的功能接口.IDS三大要素:信息源\分析\响应称作入侵检测系统的处理模式.PPDR模型:一种动态防御模型,包含策略\防护\检测\响应,具有动态\自适应的特性,策略是整个模型的核心.IDS分析引擎分类:误用检测\异常检测.误用检测技术:又称基于知识或特征的检测技术,它假定所有入侵行为和手段(及其变种)都能够表达为一种模式或特征,并对已知的入侵行为和手段进行分析,提取入侵特征,构建攻击模式或攻击签名,通过系统当前状态与攻击模式或攻击签名的匹配判断入侵行为.优点:可以准确地检测已知的入侵行为;缺点:不能检测未知的入侵行为.异常检测技术:又称为基于行为的入侵检测技术,用来检测主机或网络中的异常行为,基本设想是入侵行为与合法的活动有明显差异.异常检测工作原理:首先收集一段时间系统活动的历史数据,再建立代表主机\用户或网络连接的正常行为描述,然后收集事件数据并使用一些不同的方法来决定所检测到的事件活动是否偏离了正常行为模式,从而判断是否发生了入侵.异常检测方法:1)统计异常检测方法2)特征选择异常检测方法3)基于贝叶斯推理异常检测方法4)基于贝叶斯网络异常检测方法5)基于模式预测异常检测方法.Snort是一个基于libpcap的轻量级网络入侵检测系统(包括解码器\预处理器\检测引擎\输出插件\日志/警报子系统).IDS的发展方向:1)宽带高速实时检测技术2)大规模分布式的检测技术3)数据挖掘技术4)更先进的检测算法5)入侵响应技术6)与其他安全技术的结合.反NIDS目标:使NIDS检测不到入侵行为的发生,或无法对入侵行为做出响应,或无法证明入侵行为的责任.NIDS攻击方法:规避NIDS检测,针对NIDS自身发起攻击,借助NIDS的某些响应功能达到入侵或攻击目的.NIDS脆弱性:1)检测的工作量很大:需要高效的检测方法和大量的系统资源,NIDS的检测是资源密集型的,这在某种程度上使其更加容易遭受DoS攻击2)检测方法的局限性:复杂的\智能化方法的作用十分有限,特征匹配作为一种轻量级的检测方法有其固有的缺陷,缺乏弹性(尤其是字符串匹配),如何完备定义匹配特征是决定检测性能的一个关键问题3)网络协议的多样性与复杂性:NIDS须对其中的大部分协议进行模拟分析检测工作,这会使得分析引擎变得臃肿而效率低下4)系统实现的差异:NIDS可能不能完全理解所保护主机对数据的解析,理解不一致导致漏报误报.C7Windows及Linux系统的安全TCSEC受信计算机系统评测标准.四个级别:D最小保护(D1),C自主保护(C1:自主安全保护,C2:受控的访问保护),B强制保护级(B1:标签式安全保护B2:结构化保护B3:安全域),A经过验证的保护(A1:经过验证的设计). 从TCSEC的B2级到A1级,TCSEC要求所有对受信计算基(TCB)的更改必须由配置管理进行控制.受信系统的配置管理包括在开发\维护和设计过程中,对TCB所有更改的识别\控制\记录和审计.TCSEC的主要目的是为受信系统的开发者提供配置管理概念,及其在受信系统开发和生命周期中所需的指导.TCSEC也为其它系统开发者提供配置管理重要性及其实施方式的指导.信息技术安全评价准则(ITSEC)(E3=C2),CC for ITSEC 2.0=>ISO154 08,GB 17859-1999计算机信息系统安全保护等级划分准则.W/U系统安全级别C2,关键要求:①安全登录机制②自主访问控制机制③安全审计机制④对象重用保护机制(残留信息的处理机制,即:阻止一个用户利用或阅读另一个用户已删除的数据,或访问另一个用户曾经使用并释放的内存).WNT及后续还实现了B级要求:信任路径功能,用于防止用户登录时被特洛伊木马程序截获用户名和密码;信任机制管理,支持管理功能的单独账号,例如,给管理员的分离账号\可用于备份计算机的用户账号和标准用户等.Win重要的安全机制:对象的保护机制,安全审计机制,用户管理安全机制.Windows系统的安全防护:1.使用NTFS2.防止穷举法猜测口令3.使用高强度的口令4.正确设置防火墙5.路由和远程访问中的限制6.系统安全策略7.安装第三方安全软件,及时打补丁8.断开重要的工作主机与外部网络的连接.入侵Windows系统:1)口令破解2)利用漏洞入侵:中文版输入法漏洞入侵,获得管理员账号(全拼输入法-帮助-操作指南(右击)-跳至URL-C:\winnt\ system32)创建跳板(激活guest(C2)添加密码(net guest pw)添加权限(net localgroup administrators guest /add))扫除入侵痕迹(快捷方式/日志文件)3)利用黑客工具入侵.SYSTEM用户权限是Windows2000系统上的最高权限.Linux的安全机制:1)用户和口令安全将一个普通用户变成root:修改/etc/passwd文件(需要sudo权限),找到abc,把用户ID修改为0.2)文件许可权3)目录许可4)设置用户ID许可和同组用户ID许可:有效的UID和GID用于系统确定该进程对于文件的存取许可.慎用suid和sgid:当某可执行文件是root创建的,如果设置了SUID,而该可执行文件又被赋予了其他普通用户的可执行权限,则该程序被任何用户运行时,对应的进程的euid是root,该进程可以访问任何文件.Linux的安全防护:1)使用高强度的口令2)用户登录超时注销3)禁止访问重要文件4)允许和禁止远程访问5)禁止不必要的SUID程序6)及时为系统的已知漏洞打上补丁7)保证一些应用服务的安全入侵Linux系统:1)破解口令2)通过系统漏洞进行入侵3)几种典型的数据驱动攻击(指向某个进程(远程或本地)发送将导致非预期结果的数据,从而入侵系统,主要原因在于程序的设计者忽视了对输入数据的校验):1)缓冲区溢出攻击:在某个用户或进程试图往一个缓冲区(即固定长度的数组)中放置比原初分配的空间还要多的数据的时候,就会出现缓冲区溢出条件2)格式化字符串攻击:格式化字符串漏洞是格式化函数(包括printf()和sprintf())中的格式化参数与待输出的变量个数不匹配而导致的,攻击者利用该漏洞可以使进程崩溃,读写某个敏感变量的值,甚至能执行任意的代码3)输入验证攻击:如果进程没有确切地分析并验证所收到输入的有效性,则可能发生输入验证攻击,情况包括:1.程序无法辨认语法上不正确的输入2.模块接受了无关的输入3.模块没有能够处理遗漏的输入域4.发生了域值相关性错误.SQL注入攻击就是典型的输入验证攻击.为了防止输入验证攻击,程序员要认真检查输入,并测试所有的代码.如何在windows2003中禁止某个用户从本地登录:程序->管理工具->本地安全策略->本地策略->用户权限分配->拒绝本地登录->添加要禁止的用户.C8 32位Linux系统的缓冲区溢出缓冲区是一块用于存取数据的内存,其位置和长度(大小)在编译时确定或在程序运行时动态分配.缓冲区可以在栈(stack)和堆(heap)中.当向缓冲区拷贝数据时,若数据的长度大于缓冲区的长度,则多出的数据将覆盖该缓冲区之外的(高地址)内存,从而覆盖了邻近的内存,这就是所谓的缓冲区溢出错误.如果缓冲区溢出错误能被攻击者利用,则称为缓冲区溢出漏洞.如果C语言中的字符串拷贝操作不检查字符串长度,则有可能发生缓冲区溢出错误.危害:1.发生后如果邻近内存空闲(不被进程使用)则对系统的运行无影响;2.如果邻近内存是被进程使用的数据,可能导致进程不正确运行;3.如果被覆盖的是函数的返回地址,攻击者通过精心构造被拷贝的数据(即BigBuffer的内容),有可能执行其期望的代码.所谓编写Shellcode,就是编译一段使用系统调用的简单的C程序,通过调试器抽取汇编代码,并根据需要修改这段汇编代码使之实现攻击者的目的.抵抗:地址随机化机制可迟滞攻击者,关闭:sudo sysctl -w kernel.randomize\_va\_space=0,栈不可执行,堆栈保护等.Win:进程跳转利用动态链接库中的call esp或jmp esp指令.为了进行缓冲区溢出攻击,必须分析目标程序的进程映像(进程在内存中的分布, 与操作系统及版本有关,也与生成该程序的编译器有关)进程4个主要内存区:(低地址)代码区(.text可执行代码)\数据区(.data已初始化的全局变量|.bss未初始化的\*)\堆栈区(Heap(堆,动态内存)|未使用|Stack(栈,局部变量))和环境变量区(高地址),(1)可执行代码fun1, fun2, main存放在内存的低地址,且按照源代码中的顺序从低地址到高地址排列(先定义的函数的代码存放在内存的低地址)(2)全局变量(x, y, z)也存放内存的低地址,位于可执行代码之上(起始地址高于可执行代码的地址)(初始化的全局变量存放在较低的地址,而未初始化的全局变量位于较高的地址) (3)局部变量位于内存高地址区(0xbfff eexx),字符串变量放在高地址,其它变量从低地址到高地址依次(先定义的放在低地址)存放(4)函数的入口参数的地址(> 0xbfff efxx)更高,位于函数的局部变量更高的地址之上,main函数从环境中获得参数,因此,环境变量位于最高的地址.由(3)和(4)可以推断出,栈底(最高地址)位于0xc000 0000,环境变量和局部变量位于进程的栈区,函数的返回地址也位于进程的栈区.三种数据段.text(文本区,不可写(写入会导致段错误)存放程序代码)\.data\.bss.栈:后进先出数据结构,往低地址增长,保存本地变量\函数调用等信息.老版本栈底固定为0xc0000000.堆是先进先出结构,主要用来保存程序信息和动态分配的变量.栈帧包含以下信息①该函数的返回地址②调用函数的栈帧信息,即栈顶和栈底(最高地址)③为该函数的局部变量分配的空间④为被调用函数的参数分配的空间||缓冲区溢出原理:函数里局部变量的内存分配是发生在栈帧里的,所以如在某函数内部定义了局部变量,则这个缓冲区变量所占用的内存空间是在该函数被调用时所建立的栈帧里.由于对缓冲区的潜在操作(如字串的复制)都是从内存低地址到高地址的,而内存中所保存的函数返回地址往往就在该缓冲区的上方(高地址),这是由于栈的特性决定的,这就为覆盖函数的返回地址提供了条件.当用大于目标缓冲区大小的内容来填充缓冲区时,就可以改写保存在函数栈帧中的返回地址,从而改变程序的执行流程,执行攻击者的代码.调试过程:gcc -fno-stack-protector -o [bin] [file.c] $gdb buf (运行)r (反汇编)disas 函数名[main/foo] (在关键位置(foo入口\对strcpy的调用\出口)设置断点)b \*(foo+行数) (程序暂停时自动打印$eip寄存器的值,/i表示机器指令码输出)display/i $eip (/x表示十六进制输出,函数入口处的堆栈指针esp指向的栈(冒号左)保存了函数foo返回到调用函数的地址(冒号右),即函数的返回地址,此时记A=$esp本身的值)x/x $esp (继续执行, 由于C语言默认将参数逆序推入堆栈,因此,C函数strcpy(des, src)的src(全局变量Lbuffer的地址)先进栈(高地址),des(foo()中buff的首地址)后进栈(低地址))c ((这就是低地址的栈,保存后进栈的buff的首地址)0xbfffee80: 0xbfffee90)x/x $esp (0xbfffee84: 0x0804a040) (0x804a040 <Lbuffer>: 0x33323130)x/x 0x0804a040 可见Lbuffer的地址0x804a040 保存在地址为0xbfffee84的栈中,buff的首地址0xbfffee90保存在地址为0xbfffee80的栈中.B = buff的首地址,则buff的首地址与返回地址所在栈的距离=A-B= 0xbfffeeac-0xbfffee90 =0x1c=28因此,若Lbuffer>28字节就会溢出,返回地址将被改写.Lbuf溢出的字节为ABCD,返回地址会被改写为0x44434241(因为IA32默认小端序,低字节存放在低地址)构造attackStr法一:将Shellcode放置在跳转地址(函数返回地址所在的栈)之前:缓冲区足以容纳shellcode,N\*NOP-shellcode-跳转地址-NOP,RETURN=buffer的起始地址+n,0<n<N.否则NOP-RETURN-N\*NOP-shellcode,RETURN=buffer的起始地址+offset+4+n,0<n<N.NOP指令=0x90,对地址随机化可以用大量NOP填充.另一方法是将shellcode放在环境变量中,编译时用-z execstack允许栈可执行,RETURN = 0xbffffffc-(length($path)+1)-(length($shellcode)+1);其中1是结束符0的长度.C9Linux32shellcode技术注入到目标进程中的二进制代码,其功能取决于编写者的意图.编写shellcode步骤1.编写简洁的能完成所需功能的C程序2.反汇编可执行代码,用系统功能调用代替函数调用,用汇编语言实现相同的功能3.提取出操作码,写成shellcode,并用C程序验证.实验:1)编写能执行cat /etc/passwd的程序2)gdb调试(disas execve;disas \_\_kernel\_vsyscall;执行到sysenter;I reg eax ebx ecx edx),eax保存系统调用号11,ebx指name[0],ecx 指向name数组,edx为0;3)name[0]=`/bin/cat`[1]= `/etc/passwd`[2]=NULL用功能调用(填充寄存器指令开始,int $0x80(即sysenter)结束)实现execve(name[0],name, NULL),用xor %edx,%edx代替mov $0x0,%edx以避免\x00,用//bin代替/bin,用lea 0xb(%edx),%eax替换mov $0xb,%eax,(注意是小端序,字符在前字节在后)4)objdump -d [file\_asm]提取shellcode;5)对目标程序进行调试获得buff首地址和offset,修改攻击代码.C10Win32缓冲区溢出攻击实验:1)编译cl/Fd/Zi/GS-src\homework.cpp,并用WinDbg进行调试2)umain查看main函数汇编找到overflow函数并反汇编3)在入口\strcpy调用\返回处设置断点bpaddr 4)g运行程序,ddesp查看esp的值为函数返回地址存放地址A5)继续运行,查看esp指向地址的内容为buff首地址B,A-B得到offset6)继续运行至ret之后,eip变成被覆盖内容,esp+4.**进程跳转**:执行ret指令后eip变成可以控制的内容,此时的esp增加4,指向输入字符串中返回地址所在的单元偏移4字节的地址,把Shellcode放到保存返回地址所在单元的后面(高地址),而把这个返回地址覆盖成一个包含jmpesp或callesp指令的地址,那么执行ret指令之后将跳转到Shellcode.C11Win32shellcode由于ntdll.dll和kernel32.dll总是出现在任何32位进程的地址空间,因此可以在进程空间中找到动态链接库的加载地址,进而找到其中的输出函数地址,这样就可以使用其中的函数了,所以只要找到kernel32. dll中的LoadLibrary和GetProcAddress函数地址,就可以编写实现任何功能的shellcode.有两种方法可以从进程空间中确定动态链接库的加载地址:使用系统结构化异常处理程序和使用PEB(进程环境块).编码后的shellcode需要在目标进程中解码后才能执行,为此需要将解码程序附加在其之前,构建新的shellcode.C11+64位系统缓冲区溢出实验:1)在main入口处设置断点并运行,反汇编main和foo2)在foo函数入口\strcpy调用\ret处设置断点3)运行程序,x/x$rsp指向返回地址所存放的内存地址A 4)继续运行,x/s$rsi查看源字符串内容,x/x$rdi指向buff首地址B,A-B得到offset.与32位区别:1)采用64位寄存器和堆栈2)在传递参数时优先使用rsi和rdi.64位系统如果要成功利用strcpy导致的缓冲区溢出漏洞,则被攻击的缓冲区必须大到足以容纳shellcode.C12格式化字符串原理:对于printf函数,其要打印的内容及格式是由该函数的第一个参数确定的,如果第一个参数指定的格式与其后续参数匹配,则不会发生错误;然而如果指定的格式与其后续参数不匹配,则将会输出错误的结果,在某些情况下还会泄露内存变量的值.如果攻击者可以控制输入的字符串(含打印格式),则有可能利用该漏洞执行shellcode,从而入侵目标系统.若格式化参数个数>给定参数的个数,则printf会从栈的当前位置开始,依次向esp增大的方向获得数据并打印.抵抗方法:不允许用户修改格式串.攻击:%s打印地址对应字符串%n对已输出的字符计数,将数值存入当前栈指针指向的栈单元存储的地址中%m.nx十六进制打印,宽度m精度n,m前加0为左对齐.“0x%08x.”对应读取4字节&打印11个字符.例:改写为26472(0x6768),先输入A的地址,26472-5\*11=26417,格式串0x%08x.0x%08x.0x%08x.0x%08x.0x%08x.%.26417u%n.改写值太大可分2次改写:把要改写的内存地址写到格式串中.实验:1)调试程序在printf处设置断点,查看esp寄存器确定user\_input位于栈顶开始的第7个单元2)关闭地址随机化并记录B的内存地址(地址=0xbfffeb24=3221220132键盘输入3221220132和格式串“%08x.”重复7),第7个单元将会变成该内存地址3)先写数值小的两字节(如0x1234ABCD): \*address=u\_addr+2;\*(address+1)=u\_addr+2;\*(address+2)=u\_addr;格式化字符串%08x.%08x.%08x.%08x.%08x.%.4603u%hn%. 39321u%hn.%08x.%08x.;位置相反(如0xfedcba98)则:\*address=u\_addr;\*(address+1)=u\_addr+2;\*(address+2)= u\_addr+2;格式化字符串%08x.%08x.%08x.%08x.%08x.%.47711u%hn%.17476u%hn.%08x.%08x.;SQL注入攻击原理:非法使用单引号和注释符号,改变SQL语句的语义;防御:1)屏蔽特殊字符:magic\_quotes\_gpc=on(php.ini)\ addslashes()\mysql\_real\_escape\_string() 2)预处理语句机制.格式化字符串配合shellcode①函数的返回地址所在的单元=改写的内存地址=输入的整数②要改写的值=攻击代码的地址=跳转地址③shellcode放置在mystring文件的末端.C13协议和拒绝服务攻击Denial of Service目的是使计算机或网络无法提供正常的服务,导致合法用户无法访问系统资源,从而破坏目标系统可用性,故又称服务阻断攻击.易令目标警觉,在其他攻击无效时才用,分4类:带宽耗尽型(较大的管道淹没较小的管道/征用多个网点集中拥塞受害者的网络)\资源耗尽型(某个进程或用户耗尽了系统的资源(如CPU利用率\内存\文件系统限额和系统进程总数)如对Web站点大量查询)\漏洞利用型(缓冲区溢出/格式化字符串/故意输入错误口令)和路由攻击型(发送伪造的路由信息,产生错误的路由干扰正常的路由过程/DNS攻击通过各种手段,使域名指向不正确的IP地址手法是域名劫持\DNS缓存投毒和DNS欺骗).带宽耗用和资源衰竭攻击是典型的通用DoS攻击,应用层:短期内建立大量合法的TCP连接可以禁止来自同一个IP地址发起的对同一端口的多个连接;传输层(SYN Flood):利用了TCP协议的缺陷,不完成最后一次握手,制造大量半开连接(发送大量伪造IP地址的请求)防御措施:增加连接队列的大小\缩短连接建立超时时限\应用厂家检测及规避潜在SYN Flood攻击的相关软件补丁\应用网络IDS产品\使用退让策略(迅速更换域名所对应的IP地址)避免被攻击\基于DNS解析的负载均衡天然就拥有对SYN Flood的免疫力\Win修改注册表SynAttackProtect\TcpMaxHalfOpen\TcpMaxHalfOpenRetried;网络层:利用了IP协议的脆弱性,滥用IP广播和组播协议,将人为导致网络拥塞.Smurf使用了IP欺骗和ICMP 回应请求,需要攻击者\放大网络(也称为反弹网络或站点)和受害者三部分.过程:A伪装成V的源地址向反弹网络的广播地址发送echo请求,路由器收到请求会广播到整个网段,收到的主机会响应.对策:阻塞源头(访问控制)\阻塞反弹站点(阻塞入站echo/制止广播)\防止攻击目标站点(过滤/防火墙);DNS攻击:DNS主机名溢出\DNS长度溢出;路由重定向攻击.DdoS组成部分:攻击者\主控端\代理端;特点:规模可控\主体分布\攻击隐蔽\后果严重\防范困难;对策:提高软件的安全性,杜绝漏洞的出现\加强计算机用户的安全防护意识,避免成为傀儡计算机\实施控制,降低分布式拒绝服务攻击的危害\建立组织,健全分布式拒绝服务攻击的响应机制.