网络常见攻击方式及对应防御方式概述 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022__E7_BD_91_E7_BB_9C_E5_B8_B8_E8_c101_181847.htm 崩溃型攻击 死亡之ping （ping of death） 概览：由于在早期的阶段，路由器对包的最大尺寸都有限制，许多操作系统对TCP/IP栈的实现在ICMP包上都是规定64KB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区，当产生畸形的，声称自己的尺寸超过ICMP上限的包也就是加载的尺寸超过64K上限时，就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使接受方当机。 防御：现在所有的标准TCP/IP实现都已实现对付超大尺寸的包，并且大多数防火墙能够自动过滤这些攻击，包括：从windows98之后的windows,NT(service pack 3之后)，linux、Solaris、和Mac OS都具有抵抗一般ping ofdeath攻击的能力。此外，对防火墙进行配置，阻断ICMP以及任何未知协议，都讲防止此类攻击。泪滴（tear0drop） 概览：泪滴攻击利用那些在TCP/IP堆栈实现中信任IP碎片中的包的标题头所包含的信息来实现自己的攻击。IP分段含有指示该分段所包含的是原包的哪一段的信息，某些TCP/IP（包括servicepack 4以前的NT）在收到含有重叠偏移的伪造分段时将崩溃。 防御：服务器应用最新的服务包，或者在设置防火墙时对分段进行重组，而不是转发它们。 UDP洪水（UDP flood） 概览：各种各样的假冒攻击利用简单的TCP/IP服务，如Chargen和Echo来传送毫无用处的占满带宽的数据。通过伪造与某一主机的Chargen服务之间的一次的UDP连接，回复地址指向开着Echo服务的一台主机，这样

就生成在两台主机之间的足够多的无用数据流，如果足够多的数据流就会导致带宽的服务攻击。 防御：关掉不必要的TCP/IP服务，或者对防火墙进行配置阻断来自Internet的请求这些服务的UDP请求。 SYN洪水（SYN flood） 概览：一些TCP/IP栈的实现只能等待从有限数量的计算机发来的ACK消息，因为他们只有有限的内存缓冲区用于创建连接，如果这一缓冲区充满了虚假连接的初始信息，该服务器就会对接下来的连接停止响应，直到缓冲区里的连接企图超时。在一些创建连接不受限制的实现里，SYN洪水具有类似的影响。 防御：在防火墙上过滤来自同一主机的后续连接。 未来的SYN洪水令人担忧，由于释放洪水的并不寻求响应，所以无法从一个简单高容量的传输中鉴别出来。 Land攻击 概览：在Land攻击中，一个特别打造的SYN包它的原地址和目标地址都被设置成某一个服务器地址，此举将导致接受服务器向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接，每一个这样的连接都将保留直到超时掉，对Land攻击反应不同，许多UNIX实现将崩溃，NT变的极其缓慢（大约持续五分钟）。 防御：打最新的补丁，或者在防火墙进行配置，将那些在外部接口上入站的含有内部源地址滤掉。（包括10域、127域、192.168域、172.16到172.31域） Smurf攻击 概览：一个简单的smurf攻击通过使用将回复地址设置成受害网络的广播地址的ICMP应答请求（ping）数据包来淹没受害主机的方式进行，最终导致该网络的所有主机都对此ICMP应答请求作出答复，导致网络阻塞，比pingof death洪水的流量高出一或两个数量级。更加复杂的Smurf将源地址改为第三方的受害者，最终导致第三方雪崩。 防御：为

了防止黑客利用你的网络攻击他人，关闭外部路由器或防火墙的广播地址特性。为防止被攻击，在防火墙上设置规则，丢弃掉ICMP包。 Fraggle攻击 概览：Fraggle攻击对Smurf攻击作了简单的修改，使用的是UDP应答消息而非ICMP 防御：在防火墙上过滤掉UDP应答消息 电子邮件炸弹 概览：电子邮件炸弹是最古老的匿名攻击之一，通过设置一台机器不断的大量的向同一地址发送电子邮件，攻击者能够耗尽接受者网络的带宽。 防御：对邮件地址进行配置，自动删除来自同一主机的过量或重复的消息。 畸形消息攻击 概览：各类操作系统上的许多服务都存在此类问题，由于这些服务在处理信息之前没有进行适当正确的错误校验，在收到畸形的信息可能会崩溃。 防御：打最新的服务补丁。 利用型攻击 利用型攻击是一类试图直接对你的机器进行控制的攻击，最常见的有三种： 口令猜测 概览：一旦黑客识别了一台主机而且发现了基于NetBIOS、Telnet或NFS这样的服务的可利用的用户帐号，成功的口令猜测能提供对机器控制。 防御：要选用难以猜测的口令，比如词和标点符号的组合。确保像NFS、NetBIOS和Telnet这样可利用的服务不暴露在公共范围。如果该服务支持锁定策略，就进行锁定。 特洛伊木马 概览：特洛伊木马是一种或是直接由一个黑客，或是通过一个不令人起疑的用户秘密安装到目标系统的程序。一旦安装成功并取得管理员权限，安装此程序的人就可以直接远程控制目标系统。 最有效的一种叫做后门程序，恶意程序包括：NetBus、BackOrifice和BO2k,用于控制系统的良性程序如：netcat、VNC、pcAnywhere。理想的后门程序透明运行。 防御：避免下载可疑程序并拒绝执行，运用网络扫描软件定期监视内部主机

上的监听TCP服务。 缓冲区溢出 概览：由于在很多的服务程序中大意的程序员使用象strcpy(),strcat()类似的不进行有效位检查的函数，最终可能导致恶意用户编写一小段利用程序来进一步打开安全豁口然后将该代码缀在缓冲区有效载荷末尾，这样当发生缓冲区溢出时，返回指针指向恶意代码，这样系统的控制权就会被夺取。 防御：利用SafeLib、tripwire这样的程序保护系统，或者浏览最新的安全公告不断更新操作系统。 信息收集型攻击 信息收集型攻击并不对目标本身造成危害，如名所示这类攻击被用来为进一步入侵提供有用的信息。主要包括：扫描技术、体系结构刺探、利用信息服务 扫描技术 地址扫描 概览：运用ping这样的程序探测目标地址，对此作出响应的表示其存在。 防御：在防火墙上过滤掉ICMP应答消息。 端口扫描 概览：通常使用一些软件，向大范围的主机连接一系列的TCP端口，扫描软件报告它成功的建立了连接的主机所开的端口。 防御：许多防火墙能检测到是否被扫描，并自动阻断扫描企图。 反响映射 概览：黑客向主机发送虚假消息，然后根据返回“ hostunreachable ”这一消息特征判断出哪些主机是存在的。目前由于正常的扫描活动容易被防火墙侦测到，黑客转而使用不会触发防火墙规则的常见消息类型，这些类型包括：RESET消息、SYN-ACK消息、DNS响应包。 防御：NAT和非路由代理服务器能够自动抵御此类攻击，也可以在防火墙上过滤“ hostunreachable ”ICMP应答?. 慢速扫描 概览：由于一般扫描侦测器的实现是通过监视某个时间桢里一台特定主机发起的连接的数目（例如每秒10次）来决定是否在被扫描，这样黑客可以通过使用扫描速度慢一些的扫描软件进行扫描。 防御：通过引诱服务来对慢速扫描

进行侦测。 体系结构探测 概览：黑客使用具有已知响应类型的数据库的自动工具，对来自目标主机的、对坏数据包传送所作出的响应进行检查。由于每种操作系统都有其独特的响应方法（例NT和Solaris的TCP/IP堆栈具体实现有所不同），通过将此独特的响应与数据库中的已知响应进行对比，黑客经常能够确定出目标主机所运行的操作系统。 防御：去掉或修改各种Banner，包括操作系统和各种应用服务的，阻断用于识别的端口扰乱对方的攻击计划。 利用信息服务 DNS域转换 概览：DNS协议不对转换或信息性的更新进行身份认证，这使得该协议被人以一些不同的方式加以利用。如果你维护着一台公共的DNS服务器，黑客只需实施一次域转换操作就能得到你所有主机的名称以及内部IP地址。 防御：在防火墙处过滤掉域转换请求。 Finger服务 概览：黑客使用finger命令来刺探一台finger服务器以获取关于该系统的用户的信息。 防御：关闭finger服务并记录尝试连接该服务的对方IP地址，或者在防火墙上进行过滤。 LDAP服务 概览：黑客使用LDAP协议窥探网络内部的系统和它们的用户的信息。 防御：对于刺探内部网络的LDAP进行阻断并记录，如果在公共机器上提供LDAP服务，那么应把LDAP服务器放入DMZ。 假消息攻击 用于攻击目标配置不正确的消息，主要包括：DNS高速缓存污染、伪造电子邮件。 DNS高速缓存污染 概览：由于DNS服务器与其他名称服务器交换信息的时候并不进行身份验证，这就使得黑客可以将不正确的信息掺进来并把用户引向黑客自己的主机。 防御：在防火墙上过滤入站的DNS更新，外部DNS服务器不应能更改你的内部服务器对内部机器的认识。 伪造电子邮件 概览：由于SMTP并不对邮件的发送者的身

份进行鉴定，因此黑客可以对你的内部客户伪造电子邮件，声称是来自某个客户认识并相信的人，并附带上可安装的特洛伊木马程序，或者是一个引向恶意网站的连接。 防御：使用PGP等安全工具并安装电子邮件证书。 