网络时代黑客攻击的主要方式及防范手段 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/462/2021_2022__E7_BD_91_E7_BB_9C_E6_97_B6_E4_c97_462527.htm 攻击探索 下面介绍下网络攻击的主要方式及如何防范：ip地址欺骗、源路由攻击、端口扫描、DoS拒绝服务、窃听报文、应用层攻击等。一、IP地址伪装 攻击者通过改变自己的IP地址来伪装成内部网用户或可信的外部网用户，以合法用户身份登录那些只以IP地址作为验证的主机；或者发送特定的报文以干扰正常的网络数据传输；或者伪造可接收的路由报文（如发送ICMP报文）来更改路由信息，来非法窃取信息。 防范方法： 1、当每一个连接局域网的网关或路由器在决定是否允许外部的IP数据包进入局域网之前，先对来自外部的IP数据包进行检验，如果该IP包的IP源地址是其要进入的局域网内的IP地址，该IP包就被网关或路由器拒绝，不允许进入该局域网。虽然这种方法能够很好的解决问题，但是考虑到一些以太网卡接收它们自己发出的数据包，并且在实际应用中局域网与局域网之间也常常需要有相互的信任关系以共享资源，因此这种方案不具备较好的实际价值。 2、另外一种防御这种攻击的较为理想的方法是当IP数据包出局域网时检验其IP源地址。即每一个连接局域网的网关或路由器在决定是否允许本局域网内部的IP数据包发出局域网之前，先对来自该IP数据包的IP源地址进行检验。如果该IP包的IP源地址不是其所在局域网内部的IP地址，该IP包就被网关或路由器拒绝，不允许该包离开局域网,因此建议每一个ISP或局域网的网关路由器都对出去的IP数据包进行IP源地址的检验和过滤。如果每一个网

关路由器都做到了这一点，IP源地址欺骗将基本上无法奏效。 二、源路由攻击 路由器作为一个内部网络对外的接口设备，是攻击者进入内部网络的第一个目标。如果路由器不提供攻击检测和防范，则也是攻击者进入内部网络的一个桥梁。防范方法： 1、可靠性与线路安全。 2、对端路由器的身份认证和路由信息的身份认证。 3.、访问控制对于路由器的访问控制，需要进行口令的分级保护；基于IP地址的访问控制；基于用户的访问控制。 4、信息隐藏 ：与对端通信时，不一定需要用真实身份进行通信。通过地址转换，可以做到隐藏网内地址、只以公共地址的方式访问外部网络。除了由内部网络首先发起的连接，网外用户不能通过地址转换直接访问网内资源。 5、数据加密。 6、在路由器上提供攻击检测，可以防止一部分的攻击。 三、端口扫描 利用一些端口扫描工具来探测系统正在侦听的端口，来发现该系统的漏洞；或者是事先知道某个系统存在漏洞，而后通过查询特定的端口，来确定是否存在漏洞，最后利用这些漏洞来对系统进行攻击，导致系统的瘫痪。 防范方法： 1、关闭闲置和有潜在危险的端口，它的本质是将所有用户需要用到的正常计算机端口外的其他端口都关闭掉。因为就黑客而言，所有的端口都可能成为攻击的目标。换句话说“ 计算机的所有对外通讯的端口都存在潜在的危险 ”，而一些系统必要的通讯端口，如访问网页需要的HTTP（80端口）；QQ（4000端口）等不能被关闭。 在Windows NT核心系统（Windows 2000/XP/ 2003）中要关闭掉一些闲置端口是比较方便的，可以采用“ 定向关闭指定服务的端口 ”和“ 只开放允许端口的方式 ”。计算机的一些网络服务会有系统分配默认的端口，将一些闲置的服务关

闭掉，其对应的端口也会被关闭了进入“ 控制面板 ”、“ 管理工具 ”、“ 服务 ” 项内，关闭掉计算机的一些没有使用的服务（如FTP服务、DNS服务、IIS Admin服务等等），它们对应的端口也被停用了。至于“ 只开放允许端口的方式 ”，可以利用系统的“ TCP/IP筛选 ” 功能实现，设置的时候，“ 只允许 ” 系统的一些基本网络通讯需要的端口即可。 2.检查各端口，有端口扫描的症状时，立即屏蔽该端口。这种预防端口扫描的方式显然用户自己手工是不可能完成的，或者说完成起来相当困难，需要借助软件。这些软件就是我们常用的网络防火墙。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com