有关TCP_IP协议族存在的脆弱性剖析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/454/2021_2022__E6_9C_89_E5_85_B3TCP__c98_454828.htm 基于TCP/IP协议的服务很多，人们比较熟悉的有WWW服务、FTP服务、电子邮件服务，不太熟悉的有TFTP服务、NFS服务、Finger服务等等。这些服务都存在不同程度上的安全缺陷，当用户构建安全可信网络时，就需要考虑，应该提供哪些服务，应该禁止哪些服务。同时，在使用这些服务的时候，你可能没有想到，TCP/IP从一开始设计的时候就没有考虑到安全设计。 TCP/IP存在脆弱性IP层的主要曲线是缺乏有效的安全认证和保密机制，其中最主要的因素就是IP地址问题。TCP/IP协议用IP地址来作为网络节点的惟一标识，许多TCP/IP服务，包括Berkeley中的R命令、NFS、X Window等都是基于IP地址对用户进行认证和授权。当前TCP/IP网络的安全机制主要是基于IP地址的包过滤（Packet Filtering）和认证(Authentication)技术，它的有效性体现在可以根据IP包中的源IP地址判断数据的真实性和安全性。然而IP地址存在许多问题，协议的最大缺点就是缺乏对IP地址的保护，缺乏对IP包中源IP地址真实性的认证机制与保密措施。这也就是引起整个TCP/IP协议不安全的根本所在。由于UDP是基于IP协议之上的，TCP分段和UDP协议数据包是封装在IP包中在网络上传输的，因此同样面临IP层所遇到的安全威胁。现在人们一直在想办法解决，却仍然无法避免的就是根据TCP连接建立时“ 三次握手 ”机制的攻击（如图1）。这些攻击总结起来包括： 源地址欺骗（Source Address Spoofing）或IP欺骗（IP Spoofing）；源路由选择欺骗

（Source Routing Spoofing）；路由选择信息协议攻击（RIP Attacks）；鉴别攻击（Authentication Attacks）；TCP序列号欺骗（TCP Sequence number spoofing）；TCP/IP协议数据流采用明文传输；TCP序列号轰炸攻击（TCP SYN Flooding Attack），简称SYN攻击；易欺骗性（Ease of spoofing）。 图1 比如网管员都熟悉的因特网控制信息协议（ICMP），它是TCP/IP协议组的一个基本网络管理工具，在帮助网络管理人员排除网络故障中立下了汗马功劳，同时ICMP攻击却十分猖狂。最明显的是ICMP重定向报文，它被网关用来为主机提供好的路由，却不能被用来给主机的路由表进行主动的变化。如果入侵者已经攻破一个对目标主机来说可利用的次要网关，而不是基本网关，入侵者就可以通过有危险的次要网关给信任主机设置一个错误的路由。多数的服务主机在TCP重定向报文上不实行有效检查，这种攻击的影响和基于RIP的攻击相似。 另外，ICMP也可以被用来进行拒绝服务攻击（如图2）。个别的报文如目标不可达或者超时，就可以用来重置目前的连接，如果入侵者知道TCP 连接的本地及远端的端口号，将生成该连接的ICMP 报文。有时这样的信息可以通过NETSTAT服务来实现。一个更普遍的拒绝服务攻击是发送伪造的子网掩码回应报文。无论主机是否查询，它们都将接受该报文，一个错误的报文就可能阻塞目标主机的所有连接。 图2 