**源路由**

**目 录**

1源路由基本概念

2源路由选项

3源路由攻击和地址欺骗

**1****源路由基本概念**

源路由的用户可以指定他所发送的数据包沿途经过的部分或者全部[路由器](http://baike.baidu.com/view/1360.htm)。它区别于有主机或者路由器的互联层软件自行选择路由后得出的路径。

源路由是一种基于源地址进行[路由选择](http://baike.baidu.com/view/632880.htm" \t "_blank)的策略，可以实现根据多个不同[子网](http://baike.baidu.com/view/65511.htm)或内网地址，有选择性地将[数据包](http://baike.baidu.com/view/25880.htm)发往不同目的地址的功能。

例如有某路由器连接有两个内网和两个外网

接口A：192.168.1.0/24 和接口B：192.168.2.0/24，接口C：10.10.10.10/30，接口D：20.20.20.20/30

要求网络A的请求访问发往网络C，而网络B的请求访问发往网络D，可以这样的设置源路由：

SourceIP/NetMask GateWay Interface

192.168.1.0/24 10.10.10.09 接口C

192.168.2.0/24 20.20.20.19 接口D

**源路由(source route)**

先从源路由如何向连接在外地链路上的移动[节点](http://baike.baidu.com/view/47398.htm" \t "_blank)发送[数据包](http://baike.baidu.com/view/25880.htm)开始。 I P版本4在I P报头中定义了一个可选项：Loose Source and Record Route Option。这个可选项列出了一个或多个中间目的地址，要求[数据包](http://baike.baidu.com/view/25880.htm" \t "_blank)在到达最终的目的地址前必须经过这几个中间地址。

例如，考虑一台源主机要向一台目的主机发送[数据包](http://baike.baidu.com/view/25880.htm" \t "_blank)，但它还想让数据包经过从源到目的地的路径上的一台特定[路由器](http://baike.baidu.com/view/1360.htm)，这台源主机将“下一个中间目的”地址，即那台路由器的地址，放在目的 I P地址域中，而将目的主机的 I P地址放在 Loose Source and Record Route Op t i o n中，这时，数据包将按[网络前缀](http://baike.baidu.com/view/1667469.htm" \t "_blank)路由被送到目的 I P地址域中标示的那台路由器上。

当那台[路由器](http://baike.baidu.com/view/1360.htm)接收到数据包后，它检查可选项，发现自己只是一个中间目的地，于是，将Loose Source and Record Route Option 中所指示的地址取出， 也就是将目的[主机](http://baike.baidu.com/view/23880.htm)的地址取出，然后将数据包送给去往目的主机的[下一跳](http://baike.baidu.com/view/1686120.htm)地址。在转发该数据包前，[路由器](http://baike.baidu.com/view/1360.htm)将自己的 I P地址记录在Loose Source and Record Route Option中，实际上记录的是它将数据包转发出去的那个端口的I P地址。

当[数据包](http://baike.baidu.com/view/25880.htm)到达目的主机时，目的主机检查可选项，发现自己就是包的最终目的地，因此目的主机将数据包送交 I P协议域所指示的高层协议处理。 I P报头中定义的这个可选项还要求。当目的[主机](http://baike.baidu.com/view/23880.htm" \t "_blank)对源主机进行回答时，也要在它的[数据包](http://baike.baidu.com/view/25880.htm)中包含 Loose Source and Record Route O p t i o n。当然，目的主机应包含的是“反向”的源路由。在这个例子中，目的主机在向原来的源主机发送[数据包](http://baike.baidu.com/view/25880.htm" \t "_blank)时，会在Loose Source and Record Route Option 中包含作为中间目的地的那台[路由器](http://baike.baidu.com/view/1360.htm)的地址。

**2****源路由选项**

源路由选项是IP数据报选项的其中之一，可用于测试某特定网络的吞吐率，也可以是数据报绕开出错的网络。

源路由可以分为两类，一类是严格源路由选项（Strict Source Route），一类是松散源路由选项（Loose Source Route）。

严格源路由选项：规定IP数据报要经过路径上的每一个路由器，相邻路由器之间不得有中间路由器，并且所经过的路由器的顺序不可更改。

松散源路由选项：只是给出IP数据报必须经过的一些“要点”，并不给出一条完备的路径，无直接连接的路由器之间的路由尚需IP软件的寻址功能补充。[1]

**3****源路由攻击和地址欺骗**

源地址欺骗(Source Address Spoofing)、IP欺骗(IP Spoofing)其基本原理:是利用IP地址并不是出厂的时候与MAC固定在一起的，攻击者通过自封包和修改[网络节点](http://baike.baidu.com/view/1266538.htm" \t "_blank)的IP地址，冒充某个可信节点的IP地址，进行攻击。

1. 瘫痪真正拥有IP的可信[主机](http://baike.baidu.com/view/23880.htm" \t "_blank)，伪装可信[主机](http://baike.baidu.com/view/23880.htm)攻击服务器;

2. [中间人攻击](http://baike.baidu.com/view/1531871.htm);

(2) 源[路由选择](http://baike.baidu.com/view/632880.htm" \t "_blank)欺骗(Source Routing Spoofing)。原理:利用IP[数据包](http://baike.baidu.com/view/25880.htm)中的一个选项-IP Source Routing来指定路由，利用可信用户对服务器进行攻击，特别是基于UDP协议的由于其是[面向非连接](http://baike.baidu.com/view/2077319.htm" \t "_blank)的，更容易被利用来攻击;

(3) [路由选择信息协议](http://baike.baidu.com/view/876127.htm)攻击(RIP Attacks)。原理:攻击者在网上发布假的路由信息，再通过ICMP重定向来欺骗服务器[路由器](http://baike.baidu.com/view/1360.htm" \t "_blank)和主机，将正常的路由器标志为失效，从而达到攻击的目的。

(4) TCP序列号欺骗和攻击(TCP Sequence Number Spoofing and Attack),基本有三种：

1. 伪造TCP序列号，构造一个伪装的TCP[封包](http://baike.baidu.com/view/111761.htm)，对网络上可信[主机](http://baike.baidu.com/view/23880.htm)进行攻击;

2. SYN攻击(SYN Attack)。这类攻击手法花样很多，蔚为大观。但是其原理基本一致，让TCP协议无法完成[三次握手协议](http://baike.baidu.com/view/2494361.htm" \t "_blank);

3. Teardrop攻击(Teardrop Attack)和Land攻击(Land Attack)。原理:利用系统接收IP[数据包](http://baike.baidu.com/view/25880.htm)，对数据包长度和偏移不严格的[漏洞](http://baike.baidu.com/view/93544.htm)进行的。

[ip地址欺骗](http://baike.baidu.com/view/1168316.htm) 这是一种[黑客](http://baike.baidu.com/view/1960.htm)的攻击形式，黑客使用一台计算机上网,而借用另外一台机器的IP地址,从而冒充另外一台机器与服务器打交道。[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)可以识别这种ip欺骗。

IP地址欺骗是指行动产生的IP[数据包](http://baike.baidu.com/view/25880.htm)伪造的源IP地址，以便冒充其他系统或保护发件人的身分。 欺骗也可以是指伪造或使用伪造的标题就以[电子邮件](http://baike.baidu.com/view/1524.htm)或网络新闻-再次-保护发件人的身分和误导接收器或网络，以原产地和有效性发送数据。

基本的IP地址欺骗

[Internet协议](http://baike.baidu.com/view/696497.htm)或IP是根本议定书发送/接收数据通过计算机网络和互联网。 与网际网路通讯协定，每包发送或接收包含有关的资料的运作，例如来源地和目的地的数据包。 与IP地址欺骗，信息放置在源字段是不实际的来源，该数据包。 通过使用不同的地址在源领域的数据包，实际发件人可以使像包，被送往由另一台计算机上，从而反应目标计算机将被发送到假地址中指定的数据包-除非攻击者要重定向的反应，他自己的电脑。

影响IP地址欺骗

IP地址欺骗是非常有益的，特别是在案件拒绝服务（ DoS ）攻击，如大量的信息被发送到目标计算机或系统没有肇事者关心的反应，目标系统。 这种类型的攻击，特别是有效的，因为攻击[数据包](http://baike.baidu.com/view/25880.htm)，似乎即将从不同的来源，因此，肇事者是难以追查。

[黑客](http://baike.baidu.com/view/1960.htm)使用的IP地址欺骗，经常利用随机选择的IP地址从整个频谱的IP地址空间的同时，一些更先进的黑客仅使用未经注册的部分IP地址范围。 IP地址欺骗，但是，是不那么有效，比使用[僵尸网络](http://baike.baidu.com/view/297306.htm" \t "_blank)为DoS攻击，因为它可以被监控互联网当局利用散射技术可以判断DoS攻击的基础上，有多少无效的IP地址使用的攻击。 不过，它仍然是一个可行的替代办法，为[黑客](http://baike.baidu.com/view/1960.htm)的攻击。

IP地址欺骗，也是一个非常有用的工具，在网络的渗透和克服[网络安全](http://baike.baidu.com/view/17495.htm" \t "_blank)保密措施。 发生这种情况时， IP地址spoofers使用受信任的IP地址，内部网络，从而规避需要提供一个使用者名称或密码登录到该系统。 这类攻击通常是基于一组特定的[主机](http://baike.baidu.com/view/23880.htm)控制（如rhosts ）是不安全的配置。

IP地址欺骗的防御

侵入过滤或[包过滤](http://baike.baidu.com/view/150853.htm)传入的交通，从体制外的使用技术是一种有效方式，防IP地址欺骗，因为这种技术可以判断如果[数据包](http://baike.baidu.com/view/25880.htm)是来自内部或外部的制度。 因此，出口过滤也可以阻止假冒IP地址的[数据包](http://baike.baidu.com/view/25880.htm)从退出制度和发动攻击，对其他网络。

上层协议，如TCP连接或传输控制协议，其中序列号码是用来建立了一个安全的连接与其他系统也是一个有效的方法，防IP地址欺骗。

关闭源路由（松散和严格的）对您的[网络路由器](http://baike.baidu.com/view/189192.htm)也可协助防止[黑客](http://baike.baidu.com/view/1960.htm)利用欺骗的许多功能。 源路由是一个技术的广泛使用，在过去，以防止一个单一的网络故障造成的重大网络故障，但目前的[路由协议](http://baike.baidu.com/view/7031.htm)互联网上的今天使得这一切，但不必要的。