# 网络协议欺骗攻防小结



在网络的虚拟环境中和现实中一样，各种各样的人都有，各种各样的欺骗技术也都横行。笔者最近闲来无事总结了一下常见的欺骗技术和防范的方法。希望对广大读者有所帮助。

一、ARP 欺骗

ARP 协议用于 IP 地址到 MAC 地址的转换，此映射关系存储在 ARP 缓存表中，若 ARP 缓存表被他人非法修改，则会导致发送给正确主机的数据包发送给另外一台由攻击者控制的主机。ARP 欺骗（ARP spoofing），也叫 ARP 毒药（ARP poison），即可完成这些功能。

假设攻击者和目标主机在同一个局域网中，并且想要截获和侦听目标主机到网关间的所有数据。当然，对于使用集线器的局域网环境，攻击者只需要把网卡设置为混杂模式即可。但是现在的局域网都是交换机了，不仅可以提高局域网的容量，而且可以提高安全性。在这种情况下，攻击者首先会试探交换机是否存在失败保护模式（fail-safe mode），是交换机所处的特殊模式状态。交换机维护 IP 地址和 MAC 地址的映射关系时会花费一定处理能力，当网络通信时出现大量虚假 MAC 地址时，某些类型的交换机会出现过载情况，

从而转换到失败保护模式。若交换机不存在失败保护模式，则需要使用 ARP 欺骗技术。

攻击者主机需要两块网卡，IP 地址分别是 192.168.0.5 和 192.168.0.6，插入交换机的两个端口，准备截获和侦听目标主机 192.168.0.3 和路由器 192.168.0.1 之间的所有通信。另外攻击者主机还需要有 IP 数据包转发功能，此项功能在 Linux 下只需要执行命令 echo 1> /proc/sys/net/ipv4/ip_forward 就可以。以 192.168.0.4 的网络通信为例，正常的 ARP 转换如下：

1.主机 A192.168.0.4 想要与路由器 192.168.0.1 通信，从而接入 Internet。

2.主机 A 以广播的方式发送 ARP 请求，希望得到路由器的 MAC。

3.交换机收到 ARP 请求，并把此请求发送给连接到交换机的各个主机。同时，交换机将更新它的 MAC 地址和端口之间的映射表，即将 192.168.0.4 绑定它所连接的端口。

4.路由器收到 A 的 ARP 请求后，发出带有自身 MAC 地址的 ARP 响应。

5.路由器更新 ARP 缓存表，绑定 A 的 IP 地址和 MAC 地址。

6.交换机收到了路由器对 A 的 ARP 响应后，查找它的 MAC 地址和端口之间的映射表，把此 ARP 响应数据包发送到相应

的端口。同时，交换机更新它的 MAC 地址和端口之间的影射表，即将 192.168.0.1 绑定它所连接的端口。

7.主机 A 收到 ARP 响应数据包，更新 ARP 缓存表，绑定路由器的 IP 地址和 MAC 地址。

8.主机 A 使用更新后的 MAC 地址信息把数据发送给路由器，通信通道就此建立。

ARP 欺骗需要攻击者迅速地诱使目标主机 192.168.0.3 和路由器 192.168.0.1 都和它建立通信，从而使自己成为中间人 MiM（Man in Middle)。换句话说，攻击者的主机此时相当于一个被攻击者完全控制的路由器，目标主机和路由器之间的所有数据通信都要由攻击者主机转发，攻击者也就能对数据作各种处理。要达到同时欺骗目标主机和路由器的目的，攻击者应打开两个命令界面，执行两次 ARP 欺骗：一次诱使目标主机认为攻击者的主机有路由器的 MAC 地址，这可以利用 IP 地址欺骗技术，伪造路由器的 IP 地址，从攻击者主机的一块网卡上发送给目标主机ARP请求包,则错误的MAC地址和 IP 地址的映射将更新到目标主机；另一次使路由器相信攻击者的主机具有目标主机的 MAC 地址，方法和前面相似。

ARP 欺骗的防范：

中毒的网络，就会一直有发送 arp 病毒包的，这些 arp 病毒包会误导你的机器对网关 mac 地址的解析。所以需要绑

定 mac 地址。两种方法：

1、列出局域网内所有机器的 MAC 地址。

# arpAddress HWtype HWaddress Flags Mask Iface

192.168.1.1 ether 00:07:E9:2A:6F:C6，然后，绑定 MAC 地址， #arp -s 192.168.1.1 00:07:E9:2A:6F:C6

注意：假如用户的网关设置了 hostname 的话，这里 192.168.1.1 就有可能需要换成 hostname。

2、创建一个/etc/ethers 文件，比如你要绑定网关，那就在/etc/ethers 里写上:192.168.1.1 00:07:E9:2A:6F:C6，然后执行 #arp -f ，每次重启机器后需要重新绑定 MAC 地址。

另外，mac 地址的绑定需要双向的，即机器 a 绑定了机器 b，机器 b 也要绑定机器 a，这样 arp 病毒才会被彻底挡住。

二、IP 地址欺骗

IP 地址欺骗就是攻击者假冒他人 IP 地址，发送数据包。因为 IP 协议不对数据包中的 IP 地址进行认证，因此任何人不经授权就可以伪造 IP 包的源地址。

IP 包一旦从网络中发送出去，源 IP 地址就几乎不用，仅在中间路由器因某种原因丢弃它或到达目标端后，才被使用。这使得一个主机可以使用别的主机的 IP 地址发送 IP 包，只要它能把这类 IP 包放到网络上就可以。因而，如果攻击

者把自己的主机伪装成被目标主机信任的好友主机，即把发送的 IP 包中的源 IP 地址改成被信任的友好主机的 IP 地址，利用主机间的信任关系和这种信任关系的实际认证中存在的脆弱性（只通过 IP 确认），就可以对信任主机进行攻击。注意其中所说的信任关系是指一个被授权的主机可以对信任主机进行方便的访问。例如 Unix 中的所有的 R*命令都采用信任主机方案，所以一个攻击主机把自己的 IP 改为被信任主机的 IP，就可以连接到信任主机，并能利用 R*命令开后门达到攻击的目的。

想要实现 IP 地址欺骗要注意以下两个问题：

1.因为远程主机只向伪造的 IP 地址发送应答信号，攻击者不可能收到远程主机发出的信息，即用 C 主机假冒 B 主机 IP，连接远程主机 A，A 主机只向 B 主机发送应答信号，C 主机无法收到；

2.要在攻击者和被攻击者之间建立连接，攻击者需要使用正确的 TCP 序列号。

攻击者使用 IP 地址欺骗的目的主要有两种：

1.只想隐藏自身的 IP 地址或伪造源 IP 和目的 IP 相同的不正常包，而并不关心是否能收到目标主机的应答，例如 IP 包碎片、Land 攻击等；

2.伪装成被目标主机信任的友好主机得到非授权的服务。解决办法：目前最理想的方法是使用防火墙，防火墙决

定是否允许外部的 IP 数据包进入局域网，对来自外部的 IP 数据包进行检验。假如来自外部的数据包声称有内部地址，它一定是欺骗包。如果数据包的 IP 地址不是防火墙内的任何子网，它就不能离开防火墙。

三、路由欺骗

TCP/TP 网络中，IP 包的传输路径完全由路由表决定。若攻击者通过各种手段改变路由表，使目标主机发送的 IP 包到达攻击者能控制的主机或路由器，就可以完成侦听，篡改等攻击方式。

1.RIP 路由欺骗

RIP 协议用于自治系统内传播路由信息。路由器在收到 RIP 数据报时一般不作检查。攻击者可以声称他所控制的路由器 A 可以最快的到达某一站点 B，从而诱使发往 B 的数据包由 A 中转。由于 A 受攻击者控制，攻击者可侦听、篡改数据。

RIP 路由欺骗的防范措施主要有：路由器在接受新路由前应先验证其是否可达。这可以大大降低受此类攻击的概率。但是 RIP 的有些实现并不进行验证，使一些假路由信息也能够广泛流传。由于路由信息在网上可见，随着假路由信息在网上的传播范围扩大，它被发现的可能性也在增大。所以，对于系统管理员而言，经常检查日志文件会有助于发现此类问题。

2.IP 源路由欺骗

IP 报文首部的可选项中有“源站选路”，可以指定到达目的站点的路由。正常情况下，目的主机如果有应答或其他信息返回源站，就可以直接将该路由反向运用作为应答的回复路径。

主机 A（假设 IP 地址是 192.168.100.11）是主机 B（假设 IP 地址为 192.168.100.1）的被信任主机，主机 X 想冒充主机 A 从主机 B 获得某些服务。首先，攻击者修改距离 X 最近的路由器 G2，使用到达此路由器且包含目的地址 192.168.100.1 的数据包以主机 X 所在的网络为目的地；然后，攻击者 X 利用 IP 欺骗（把数据包的源地址改为 192.168.100.11）向主机 B 发送带有源路由选项（指定最近的 G2）的数据包。当 B 回送数据包时，按收到数据包的源路由选项反转使用源路由，传送到被更改过的路由器 G2。由于 G2 路由表已被修改，收到 B 的数据包时，G2 根据路由表把数据包发送到 X 所在的网络，X 可在其局域网内较方便地进行侦听，收取此数据包。

防范 IP 源路由欺骗的好方法主要有：

1.配置好路由器，使它抛弃那些由外部网进来的、声称是内部主机的报文；

2.关闭主机和路由器上的源路由功能。

四、TCP 欺骗

实现 TCP 欺骗攻击有两种方法：

1.非盲攻击

攻击者和被欺骗的目的主机在同一个网络上，攻击者可以简单地使用协议分析器（嗅探器）捕获 TCP 报文段，从而获得需要的序列号。以下是其攻击步骤：

（1）攻击者 X 要确定目标主机 A 的被信任主机 B 不在工作状态，若其在工作状态，也使用 SYN flooding 等攻击手段使其处于拒绝服务状态。

（2）攻击者 X 伪造数据包：B->A：SYN（ISN C），源 IP 地址使用 B，初始序列号 ISN 为 C，给目标主机发送 TCP 的 SYN 包，请求建立连接。

（3）目标主机回应数据包：A->B：SYN（ISN S），ACK（ISN C），初始序列号为 S，确认序号为 C。由于 B 处于拒绝服务状态，不会发出响应包。攻击者 X 使用嗅探工具捕获 TCP 报文段，得到初始序列号 S。

（4）攻击者 X 伪造数据包：B->A:ACK(ISN S),完成三次握手建立 TCP 连接。

（5）攻击者 X 一直使用 B 的 IP 地址与 A 进行通信。

2.盲攻击

由于攻击者和被欺骗的目标主机不在同一个网络上，攻击者无法使用嗅探工具捕获 TCP 报文段。其攻击步骤与非盲攻击几乎相同，只不过在步骤（3）中无法使用嗅探工具，

可以使用 TCP 初始序列号预测技术得到初始序列号。在步骤（5）中，攻击者 X 可以发送第一个数据包，但收不到 A 的响应包，较难实现交互。

从攻击者的角度来考虑，盲攻击比较困难，因为目的主机的响应都被发送到不可达的被欺骗主机，攻击者不能直接确定攻击的成败。然而，攻击者可使用路由欺骗技术把盲攻击转化为非盲攻击。

对 TCP 欺骗攻击的防范策略主要有：

（1）使用伪随机数发生工具产生 TCP 初始序号；

（2）路由器拒绝来自外网而源 IP 是内网的数据包；

（3）使用 TCP 段加密工具加密。

五、DNS 欺骗

在网上，用户可以利用 IE 等浏览器进行各种各样的 WEB 站点的访问，如阅读新闻、订阅报纸、电子商务等。攻击者可以将用户想要浏览的网页的 URL 改写成指向攻击者自己的服务器，当用户浏览目标网页的时候，实际上是向攻击者服务器发出请求，那么攻击者就可以达到欺骗或攻击的目的了。例如，可以利用 Webserver 的网页给客户端机器传染病毒。这种攻击的效果是通过 DNS 欺骗技术得到的。DNS 协议不对转换或信息性的更新进行身份认证，这就使得攻击者可以将不正确的信息掺进来，并把用户引向攻击者自己的主机。

用一个简单的例子说明

假如 cn.wy.com 向 xinxin.com 的子域 DNS 服务器 120.2.2.2 询 www.xinxin.com 的 IP 地址时，用户冒充 120.2.2.2 给 www.xinxin.com 的 IP 地址，这个 IP 地址是一个虚拟的地址，列如 202.109.2.2，这 cn.wy.com 就会把 202.109.2.2 当 www.xinxin.com 的地址返还给 hk.wy.com 了。当 hk.wy.com 连 www.xinxin.com 时，就会转向我们提供的那个虚假的 IP 地址了，这样对 www.xinxin.com 来说，就算是给黑掉了。因为别人根本连接不上这个域名。 这就是 DNS 欺骗的基本原理，但正如同 IP 欺骗一样。DNS 欺骗在技术上实现上仍然有一些困难，为了理解这些需要看一下 DNS 查询包的结构。在 DNS 查询包中有一个重要的域叫做做标识 ID。用来鉴别每个 DNS 数据包的印记，从客户端设置。由服务器返回，它可以让客户匹配请求与响应。

如 cn.wy.com120.2.2.2 这时黑客只需要用假的 120.2.2.2 进行欺骗，并且在真正的 120.2.2.2 返回 cn.wy.com 信息之前，先于它给出所查询的 IP 地址。cn.wy.com←120.2.2.2 ，www.xinxin.com 的 IP 地址是 1.1.1.1 。在 120.2.2.2 前 cn.wy.com 送出一个伪造的 DNS 信息包，如果要发送伪造的 DNS 信息包而不被识破，就必须伪造正确的 ID，但是，如果无法判别这个标识符的话，欺骗将无法进行。这在局域网上是很容易实现的，只要安装一个

sniffer,通过嗅探就可以知道这个 ID。但如果是在 Internet 上实现欺骗，就只有发送大量的一定范围的 DNS 信息包，通过碰运气的办法来提高给出正确标识 ID 的机会。

DNS 欺骗的真实过程

如果已经成功的攻击了 120.2.2.2 子网中任意一台主机，并且通过安装 sniffer 的方法对整个子网中传输的包进行嗅探，可以设置只对进出 120.2.2.2 的包进行观察，从而获得我们需要的标识 ID。当 DNS 服务器 120.2.2.2 发出查询包时，它会在包内设置标识 ID，只有应答包中的 ID 值和 IP 地址都正确的时候才能为服务器所接受。这个 ID 每次自动增加 1，所以可以第一次向要欺骗的 DNS 服务器发一个查询包并监听到该 ID 值，随后再发一个查询包，紧接着马上发送构造好的应答包，包内的标识 ID 为预测的值。为了提高成功效率可以指定一个范围，比如在前面监听到的哪个 ID+1 的范围之间。接上列，如 cn.wy.com 向 120.2.2.2 发来了要求查 www.xinxin.com 的 IP 地址的包，此时，120.2.2.2 上的黑客就要欺骗 cn.wy.com。

cn.wy.com→120.2.2.2 [Query]

NQY：1 NAN：0 NNS：0 NAD：0 QID：6573

QY：www.xinxin.com A

其中 NQY，NAN 等是查询包的标志位。当这两个标志位为“1”时表示是查询包，这时我们就可以在 120.2.2.2 上

监听到这个包，得到他的 ID 为 6573.然后紧接着我们也向 120.2.2.2 发出一次查询，使它忙于应答这个包。

1.1.1.1→120.2.2.2 [Query]

NQY：1 NAN：0 NNS：0 NAD：0

QY：other.xinxin.com A

紧接着发带预测 QID 的应答包

120.2.2.2→cn.wy.com [Answer]

NQY：1 NAN：0 NNS：0 NAD：0 QID：6574

QY www.xinxin.com PTR

AN www.xinxin.com PTR 111.222.333.444

111.222.333.444 就是由攻击者来指定的 IP 地址。注意发这个包时标识 ID 为前面监听到的 ID 值加 1 既 6574+1=6575。这样，DNS 欺骗就完成了 cn.wy.com 就会把 111.222.333.444 当 www.xinxin.com 的 IP 地址了。假如 111.222.333.444 是一台已经被用户控制的计算机，可以把它的主页改成想要的内容，这时当被欺骗的其他用户连接 www.xinxin.com 时，他就以为这个网站已经被黑掉了。

防范 DNS 欺骗的方法是用 DNS 转换得到的 IP 地址或域名再次作反向转换进行验证，用户可以通过一些软件来实现。