Arp防火墙反欺骗策略详细介绍 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/474/2021_2022_Arp_E9_98_B2_E7_81_AB_E5_c67_474164.htm 近来与Arp相关恶意软件越来越猖獗，受害者的也不少，国内的各大杀毒厂商也纷纷推出Arp防火墙。但大部分防火墙虚有其表，原因下面会具体介绍。这篇文章不是科普，主要是思路，更想起到抛砖引玉的作用。让世界清静一点。此外，从从未接触到熟悉Arp协议到写出Arp欺骗和反欺骗的test code，前前后后也不过一个星期多一点的时间。经验有限，疏漏之处，再所难免，各位见谅。 Arp协议和Arp欺骗这里就不做介绍了。网络这方面的文章比比皆是。 为了便于理解，下面构造一些名词： 假如局域网内，有网关，发起欺骗的主机（以下简称欺骗主机），受骗主机 双向欺骗：欺骗主机使得网关认为欺骗主机是受骗主机同时让受骗主机认为欺骗主机是网关； 单向欺骗网关：欺骗主机只使网关认为欺骗主机是受骗主机； 单向欺骗目标主机：欺骗主机只使受骗主机认为它是网关； Arp除了能sniffer之外，现在比较流行的做法就是利用Arp进行HTTP挂马的情况了。所以下面考虑的影响基本以这个角度的方面来衡量。 由于环境不同，继续往下分，一个机房被Arp欺骗的情，机房一般以服务器为主，对外发的数据多以http应答包为主，此时单向欺骗目标主机的危害比较大。另外一个普通的公司，家庭，及网吧之类的局域网环境，对外发的数据多以http请求为主，接收的数据多以http应答包为主，此时单向欺骗网关危害比较大。 还有的就是和网关有关了，网关简单的先分两种： 1、支持IP和mac绑定的； 2、不支持IP和mac绑定。 支持IP

和mac绑定的网关都好办，所以这里就不讨论这种情况了，主要讨论不支持IP和mac绑定的情况：下面举的例子都是Arp双向欺骗已经存在的情况，装上Arp FW后FW将处理情况。 第一种情况普通公司，家庭，及网吧之类局域网环境下，网关不支持IP和mac绑定：先说欺骗策略，说到这里不得不提Arpspoof（以下简称as），最近流行这个工具，并且开源，好分析，也确实写的不错。我手头拿到的3.1版本的源代码。若不修改as代码，在当前情况下，并处在双向欺骗时，只要把配置文件稍微改改，就能够实现利用ARP挂马。但如果受骗主机绑定了正确网关的mac，就不灵了。但如果有人修改了as代码，使其能支持gzip解码，并且把本应发给受害主机的包，重组并解码然后再发给受害主机。就又能欺骗了。 然后再回来看看现在国内的Arp FW.比较弱的，FW一进去，连正确的网关mac都检测不出来，需要手动填。好点的能自动检测正确的网关的mac.一般步骤是：1. 获取当前网关mac（如利用sendARP函数等等）；2. 利用网关IP发一个广播包，获取网关的mac；3. 抓包对比，如果第一步和第二步获得网关的mac相同，则认为网关mac不是伪造的。如过第二步获得两个Arp reply，则把这两个包与第一步的mac对比，相同的说明是伪造的。如果第二步只获得一个Arp reply，以第二步获得mac为准。 检测到正确网关mac后，就静态的绑定网关IP和mac，防止别人伪造网关。 基本上都这么搞，这个思路是有缺陷的。没错，是可以防的住现在的as.因为as发Arp欺骗包间隔是3s，如果不改源代码的话。在这个的时间间隔下，这三步是有能力获得正确的网关，但是如果把间隔设短，甚至没有间隔发Arp欺骗包的话。现在国内市面上的Arp FW几乎全都倒下。碍于

面子这里就不详细说明那些厂商。 先说为什么间隔3s的话，能检测到正确网关mac，在执行第二步时，在发广播包之前必须先发一个Arp reply给网关，告诉网关自己正确的mac，然后网关才能把它本身的mac发给受骗主机。这个过程必须在3s内完成。因此如果as的spoof不设间隔的话。那么网关在接收了你的ip和mac之后。发起欺骗的主机马上就去网关那把它改回来。这样受骗主机虽然发了广播包，但是网关根据mac，会把它本身的mac发给欺骗主机而不是发给受骗主机，这样受骗主机依然得不到正确网关的mac.另外，哪怕受骗主机得到了正确的网关mac，也只能保证自己对外发包不受欺骗，但是收到的包还是会被欺骗的。当然FW可以和as玩拉锯，二者都争先恐后的去网关那边刷自己的mac.但是这样导致是容易丢包。其实这种状况还是有一个相对的解决方案。就是彻底的改头换面掉。同时改自己的IP和mac，不论FW用什么添加ndis虚拟网卡，或者通过代码直接就把当前IP和mac替掉。获得正确网关mac才有保证，否则连正确网关mac都拿不到。其它的就更不用说了（至于什么手动填网关mac之类的。就先不讨论了。知道网关是什么东西的用户原没有想象中的那么多）。 说这是一个相对的解决方案，是因为前提是局域网内得有富余的IP资源。另外它还有一些弊端。就是如果有些机器关机的话，而受害者替换了它的IP之后，以后将造成冲突。当然也是有解决方案了。比较多，这里就先不讨论了。 因此，先要确定哪些IP是未被使用的，可以广播Arp request 局域网各个IP的mac，如果有人应答的话说明这个IP被用，没人应答的话，就是富余的IP了。 只要把自己的IP和mac一改 改了之后，迅速刷新网关，获得正确网关的mac之后，可以询问用户是否改

回来，改回来，因为无法避免丢包。网速也容易受影响。 第二种关于机房Arp欺骗的情况这里就不多说，参考上面文字。有几点要说明的是，机房里，外网IP和内网IP是映射的，同时改IP和mac是会导致断网的，有一定危险性。另外获得正确网关的mac后，IP和mac必须改回来。也就是说在机房这种情况下，丢包是免不了的。 