ARP病毒攻击技术分析与防御 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/224/2021_2022_ARP_E7_97_85_E6_AF_92_E6_c101_224572.htm 一、ARP Spoofing攻击原理分析 在局域网中，通过ARP协议来完成IP地址转换为第二层物理地址（即MAC地址）的。ARP协议对网络安全具有重要的意义。通过伪造IP地址和MAC地址实现ARP欺骗，能够在网络中产生大量的ARP通信量使网络阻塞或者实现“ man in the middle ”进行ARP重定向和嗅探攻击。 用伪造源MAC地址发送ARP响应包，对ARP高速缓存机制的攻 击。 每个主机都用一个ARP高速缓存存放最近IP地址到MAC硬件地址之间的映射记录。MS Windows高速缓存中的每一条记录（条目）的生存时间一般为60秒，起始时间从被创建时开始算起。 默认情况下，ARP从缓存中读取IP-MAC条目，缓存中的IP-MAC条目是根据ARP响应包动态变化的。因此，只要网络上有ARP响应包发送到本机，即会更新ARP高速缓存中的IP-MAC条目。 攻击者只要持续不断的发出伪造的ARP响应包就能更改目标主机ARP缓存中的IP-MAC条目，造成网络中断或中间人攻击。 ARP协议并不只在发送了ARP请求才接收ARP应答。当计算机接收到ARP应答数据包的时候，就会对本地的ARP缓存进行更新，将应答中的IP和 MAC地址存储在ARP缓存中。因此，B向A发送一个自己伪造的ARP应答，而这个应答中的数据为发送方IP地址是192.168.10.3（C的IP地址），MAC地址是DD-DD-DD-DD-DD-DD（C的MAC地址本来应该是CC-CC-CC-CC-CC-CC，这里被伪造了）。当A接收到B伪造的ARP应答，就会更新本地的ARP缓存（A可不

知道被伪造了）。 当攻击源大量向局域网中发送虚假的ARP信息后，就会造成局域网中的机器ARP缓存的崩溃。 Switch上同样维护着一个动态的MAC缓存，它一般是这样，首先，交换机内部有一个对应的列表，交换机的端口对应MAC地址表Port n Mac记录着每一个端口下面存在那些MAC地址，这个表开始是空的，交换机从来往数据帧中学习。因为MAC-PORT缓存表是动态更新的，那么让整个 Switch的端口表都改变，对Switch进行MAC地址欺骗的Flood，不断发送大量假MAC地址的数据包，Switch就更新MAC-PORT缓存，如果能通过这样的办法把以前正常的MAC和Port对应的关系破坏了，那么Switch就会进行泛洪发送给每一个端口，让Switch基本变成一个 HUB，向所有的端口发送数据包，要进行嗅探攻击的目的一样能够达到。也将造成Switch MAC-PORT缓存的崩溃，如下下面交换机中日志所示：
Internet 172.20.156.10000b.cd85.a193 ARPAVlan256Internet 172.20.156.50000b.cd85.a193 ARPAVlan256Internet 172.20.156.254 0000b.cd85.a193 ARPAVlan256Internet 172.20.156.53 0000b.cd85.a193 ARPAVlan256Internet 172.20.156.33 0000b.cd85.a193 ARPAVlan256Internet 172.20.156.130000b.cd85.a193 ARPAVlan256Internet 172.20.156.150000b.cd85.a193 ARPAVlan256Internet 172.20.156.140000b.cd85.a193 ARPAVlan256 二、ARP病毒分析
当局域网内某台主机运行ARP欺骗的木马程序时，会欺骗局域网内所有主机和路由器，让所有上网的流量必须经过病毒主机。其他用户原来直接通过路由器上网现在转由通过病毒主机上网，切换的时候用户会断一次线。切换到病毒主机上

网后，如果用户已经登陆了传奇服务器，那么病毒主机就会经常伪造断线的假像，那么用户就得重新登录传奇服务器，这样病毒主机就可以盗号了。 由于ARP欺骗的木马程序发作的时候会发出大量的数据包导致局域网通讯拥塞以及其自身处理能力的限制，用户会感觉上网速度越来越慢。当ARP欺骗的木马程序停止运行时，用户会恢复从路由器上网，切换过程中用户会再断一次线。 在路由器的“ 系统历史记录 ”中看到大量如下的信息： MAC Chged 10.128.103.124MAC Old 00:01:6c:36:d1:7fMAC New 00:05:5d:60:c7:18 这个消息代表了用户的MAC地址发生了变化，在ARP欺骗木马开始运行的时候，局域网所有主机的MAC地址更新为病毒主机的MAC地址（即所有信息的MAC New地址都一致为病毒主机的MAC地址），同时在路由器的“ 用户统计 ”中看到所有用户的MAC地址信息都一样。 如果是在路由器的“ 系统历史记录 ”中看到大量MAC Old地址都一致，则说明局域网内曾经出现过ARP欺骗（ARP欺骗的木马程序停止运行时，主机在路由器上恢复其真实的MAC地址）。 BKDR_NPFECT.A病毒引起ARP欺骗之实测分析 Part1. 病毒现象 中毒机器在局域网中发送假的APR应答包进行APR欺骗, 造成其他客户机无法获得网关和其他客户机的网卡真实MAC地址,导致无法上网和正常的局域网通信. Part2. 病毒原理分析: 病毒的组件 本文研究的病毒样本有三个组件构成: %windows%\SYSTEM32\LOADHW.EXE(108,386 bytes) ….. ”病毒组件释放者 ” %windows%\System32\drivers\npf.sys(119,808 bytes) ….. ”发ARP欺骗包的驱动程序 ” %windows%\System32\msitinit.dll (39,952 bytes)… ”命令驱动程

序发ARP欺骗包的控制者 ”病毒运作基理: 1.LOADHW.EXE 执行时会释放两个组件npf.sys 和msitinit.dll . LOADHW.EXE释放组件后即终止运行. 注意: 病毒假冒成winPcap的驱动程序,并提供winPcap的功能. 客户若原先装有winPcap, npf.sys将会被病毒文件覆盖掉.[1] [2] 下一页