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_ti2020/142/2021_2022_ARP_E7_97_85_E6_AF_92_E6_c101_142600.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 