

ARP欺骗攻击原理和防范思科认证 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022_ARP_E6_AC_BA_E9_AA_97_E6_c101_644155.htm ARP欺骗/

MITM(Man-In-The-Middle)攻击原理和防范

MITM(Man-In-The-Middle) 攻击原理 按照 ARP 协议的设计，为了减少网络上过多的 ARP 数据通信，一个主机，即使收到的 ARP 应答并非自己请求得到的，它也会将其插入到自己的 ARP 缓存表中，这样，就造成了“ARP 欺骗”的可能。如果黑客想探听同一网络中两台主机之间的通信（即使是通过交换机相连），他会分别给这两台主机发送一个 ARP 应答包，让两台主机都“误”认为对方的 MAC 地址是第三方的黑客所在的主机，这样，双方看似“直接”的通信连接，实际上都是通过黑客所在的主机间接进行的。黑客一方面得到了想要的通信内容，另一方面，只需要更改数据包中的一些信息，成功地做好转发工作即可。在这种嗅探方式中，黑客所在主机是不需要设置网卡的混杂模式的，因为通信双方的数据包在物理上都是发送给黑客所在的中转主机的。这里举个例子，假定同一个局域网内，有 3 台主机通过交换机相连：A 主机：IP 地址为 192.168.0.1，MAC 地址为 01:01:01:01:01:01；B 主机：IP 地址为 192.168.0.2，MAC 地址为 02:02:02:02:02:02；C 主机：IP 地址为 192.168.0.3，MAC 地址为 03:03:03:03:03:03。B 主机对 A 和 C 进行欺骗的前奏就是发送假的 ARP 应答包。在收到 B 主机发来的 ARP 应答后，A 主机应知道：到 192.168.0.3 的数据包应该发到 MAC 地址为 02:02:02:02:02:02 的主机；C 主机也知道：到 192.168.0.1 的数据

包应该发到 MAC 地址为 020202020202 的主机。这样，A 和 C 都认为对方的 MAC 地址是 020202020202，实际上这就是 B 主机所需得到的结果。当然，因为 ARP 缓存表项是动态更新的，其中动态生成的映射有个生命期，一般是两分钟，如果再没有新的信息更新，ARP 映射项会自动去除。所以，B 还有一个“任务”，那就是一直连续不断地向 A 和 C 发送这种虚假的 ARP 响应包，让其 ARP 缓存中一直保持被毒害了的映射表项。现在，如果 A 和 C 要进行通信，实际上彼此发送的数据包都会先到达 B 主机，这时，如果 B 不做进一步处理，A 和 C 之间的通信就无法正常建立，B 也就达不到“嗅探”通信内容的目的，因此，B 要对“错误”收到的数据包进行一番修改，然后转发到正确的目的地，而修改的内容，无非是将目的 MAC 和源 MAC 地址进行替换。如此一来，在 A 和 C 看来，彼此发送的数据包都是直接到达对方的，但在 B 来看，自己担当的就是“第三者”的角色。这种嗅探方法，也被称作“Man-In-The-Middle”的方法。攻击实例目前利用 ARP 原理编制的工具十分简单易用，这些工具可以直接嗅探和分析 FTP、POP3、SMB、SMTP、HTTP/HTTPS、SSH、MSN 等超过 30 种应用的密码和传输内容。下面是测试时利用工具捕获的 TELNET 过程，捕获内容包含了 TELNET 密码和全部所传的内容：不仅仅是以上特定应用的数据，利用中间人攻击者可将监控到数据直接发给 SNIFFER 等嗅探器，这样就可以监控所有被欺骗用户的数据。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com