通过交换机查找局域网内病毒攻击的方法Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/557/2021_2022__E9_80_9A_E8_BF_87_E4_BA_A4_E6_c101_557836.htm 在局域网内如何查杀攻击病毒呢?以下分两类来详细讲解： ARP 地址攻击查找流程 1、如果客户端PC与网关无法通讯，首先在客户端ping 网关地址后，然后在dos窗口下执行 arp a 查看网关的mac地址，记录下网关MAC地址。到交换机上查找交换机的MAC地址(例如VLAN1接口) 执行 show int vlan 1 查看输出信息中VLAN1接口MAC，同时执行 show standby vlan 1 查看HSRP网关MAC地址。如果客户端显示的mac(假设为00-0d-0a-ac-bc-78)地址与网关地址不同，则可能是网关的MAC遭到ARP 病毒攻击。到交换机上执行show mac-address | in 000d.0aac.bc78 在输入信息中查找关联该MAC地址的端口，如果该端口是直连PC或者SERVER的端口，那么该端口所连客户端可能感染ARP类病毒。如果该端口连接的是另外一台交换机，那么登陆到那台交换机上执行show mac-address | in 000d.0aac.bc78 直到关联端口是直连PC的端口位置。 2、如果客户端PC能够PING 通网关但是与其他VLAN的机器PING(假设该地址为192.168.1.111)不通。首先在客户端ping 192.168.1.111后，然后在dos窗口下执行 arp a 查看对方IP地址对应的mac地址，记录下其MAC地址(有可能没有信息)，同时在目标机器192.168.1.111上执行ipconfig/all查看该机器网卡mac地址并记录下(注意：交换机上显示的MAC地址和PC上显示的MAC地址格式不一样，交换机上为4个16进制数一组并以“ . ”分割，PC机上为2个16进制数为一组以 ” - ” 分割)。在dos窗口下执行 tracert d

192.168.1.111。查看tracert信息最后一跳到达哪台交换机。登陆到那台交换机上执行PING 192.168.1.111，然后执行 show arp | in 192.168.1.111 查看输出信息的mac地址与目标机器(192.168.1.111)的mac地址是否相同。如果不同(假设显示为000a.da87.5bca)，记录下后执行 show mac-address | in 000a.da87.5bca 在输出信息查看该MAC地址关联到哪个端口，如果关联的端口连接到另外一台交换机上则到那台交换机上执行show mac-address | in 000a.da87.5bca，最终找到关联端口连接是最终客户端(PC或者server)的端口，如果该端口不是真正连接192.168.1.111的端口通常该端口既是感染ARP类病毒的机器。在交换机上执行 show arp | in 000a.da87.5bca 输入信息通常会显示该MAC会关联多个IP地址。 流量攻击型病毒的查找流程 如果局域网中通讯不正常、丢包严重，登陆到网关上也会延迟很大，通常是局域网中有机器感染了流量攻击型病毒，该类病毒会发送大量的小字节数据包消耗网络中交换机、路由器的带宽和处理能力。查找该类病毒也是通过流量判断攻击来源。在核心交换机上执行clear count 清除当前各个接口上的流量信息，20秒钟后执行show interface 查看各个接口上的流量(数据包的数量、总字节数)通常会有一个或几个端口的数据包的数量相当夸张，但是总字节数不一定很多。如果这个端口直连PC那么暂时拔下该端口网线查看网络是否回复正常。如果该端口是连接另外一台交换机那么登陆到那台交换机上依次操作，先清空各个端口的统计数字，20秒钟后检查接口流量。直到找到直连PC而且流量相当大的机器。 更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详