了解交换机漏洞保护网络核心部分 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/278/2021_2022__E4_BA_86_E8_A7_A3_E4_BA_A4_E6_c101_278277.htm 交换机在企业网中占有重要的地位，通常是整个网络的核心所在，这一地位使它成为黑客入侵和病毒肆虐的重点对象，为保障自身网络安全，企业有必要对局域网上的交换机漏洞进行全面了解。以下是利用交换机漏洞的五种攻击手段。 VLAN跳跃攻击 虚拟局域网（VLAN）是对广播域进行分段的方法。VLAN还经常用于为网络提供额外的安全，因为一个VLAN上的计算机无法与没有明确访问权的另一个VLAN上的用户进行对话。不过VLAN本身不足以保护环境的安全，恶意黑客通过VLAN跳跃攻击，即使未经授权，也可以从一个VLAN跳到另一个VLAN. VLAN跳跃攻击（VLAN hopping）依靠的是动态中继协议（DTP）。如果有两个相互连接的交换机，DTP就能够对两者进行协商，确定它们要不要成为802.1Q中继，洽商过程是通过检查端口的配置状态来完成的。 VLAN跳跃攻击充分利用了DTP，在VLAN跳跃攻击中，黑客可以欺骗计算机，冒充成另一个交换机发送虚假的DTP协商消息，宣布他想成为中继；真实的交换机收到这个DTP消息后，以为它应当启用802.1Q中继功能，而一旦中继功能被启用，通过所有VLAN的信息流就会发送到黑客的计算机上。 中继建立起来后，黑客可以继续探测信息流，也可以通过给帧添加802.1Q信息，指定想把攻击流量发送给哪个VLAN. 生成树攻击 生成树协议（STP）可以防止冗余的交换环境出现回路。要是网络有回路，就会变得拥塞不堪，从而出现广播风暴

，引起MAC表不一致，最终使网络崩溃。 使用STP的所有交换机都通过网桥协议数据单元（BPDU）来共享信息，BPDU每两秒就发送一次。交换机发送BPDU时，里面含有名为网桥ID的标号，这个网桥ID结合了可配置的优先数（默认值是32768）和交换机的基本MAC地址。交换机可以发送并接收这些BPDU，以确定哪个交换机拥有最低的网桥ID，拥有最低网桥ID的那个交换机成为根网桥（root bridge）。 根网桥好比是小镇上的社区杂货店，每个小镇都需要一家杂货店，而每个市民也需要确定到达杂货店的最佳路线。比最佳路线来得长的路线不会被使用，除非主通道出现阻塞。 根网桥的工作方式很相似。其他每个交换机确定返回根网桥的最佳路线，根据成本来进行这种确定，而这种成本基于为带宽所分配的值。如果其他任何路线发现摆脱阻塞模式不会形成回路（譬如要是主路线出现问题），它们将被设成阻塞模式。 恶意黑客利用STP的工作方式来发动拒绝服务（DoS）攻击。如果恶意黑客把一台计算机连接到不止一个交换机，然后发送网桥ID很低的精心设计的BPDU，就可以欺骗交换机，使它以为这是根网桥，这会导致STP重新收敛（reconverge），从而引起回路，导致网络崩溃。 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