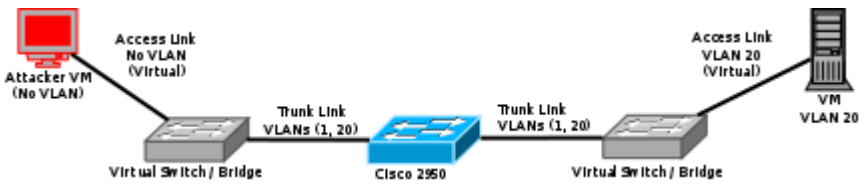
DEF CON 24 DEMO: Double Tagging VLAN Hopping Attack Between Two Virtual Networks With a Cisco 2950 Switch in the Middle

This post demonstrates the effects of using a double tagging vlan hopping attack to send an ICMP packet from a virtual machine located in one hypervisor environment to another virtual machine located in a separate hypervisor environment connected to the same physical switch. In this scenario the attacker is using a virtual Kali 2.0 system located within the Citrix XenServer hypervisor environment and targeting a virtual machine located on a separate VLAN within the ProxMox hypervisor environment.

This experiment was performed on seven different hypervisor/virtual network configurations in order to perform a systematic evaluation of the effects across all of the major enterprise level virtualization platforms. The following network diagram illustrates the configuration used for each of the experiments:



The following video walks through the attack process and results.