# DEF CON 24 Presentation: VLAN Hopping, ARP Poisoning, & Man-in-the-Middle Attacks in Virtualized Environments

---

# DEF CON 24 DEMO: Double Tagging VLAN Hopping Attack Against the Microsoft Server 2012 Hyper-V Cisco Nexus 1000v Virtual Network Using One Physical Switch

This post demonstrates the effects of using a double tagging VLAN hopping attack to send an ICMP packet to a virtual machine located on a separate VLAN than the physical attacking system. In this scenario the attacker is using a physical Kali 2.0 system connected to a native vlan access port on a Cisco 2950 switch and targeting a virtual machine located on a separate VLAN within the Microsoft Server 2012 Hyper-V hypervisor environment using the Cisco Nexus 1000v virtual switch.

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.

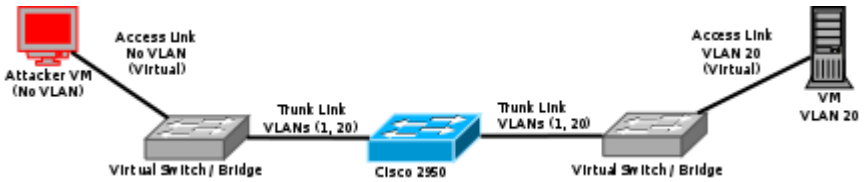
---

# 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:

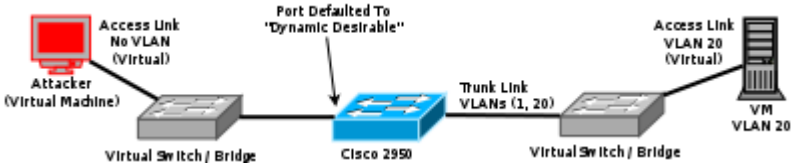



The following video walks through the attack process and results.

---

# DEF CON 24 DEMO: Switch Spoofing Attack Against a Cisco 2950 Switch from the VMWare ESXi 6.0 Hypervisor Environment

This post includes a demo video which illustrates the effects of a Switch Spoofing attack launched from within a virtualized networking environment. The 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:

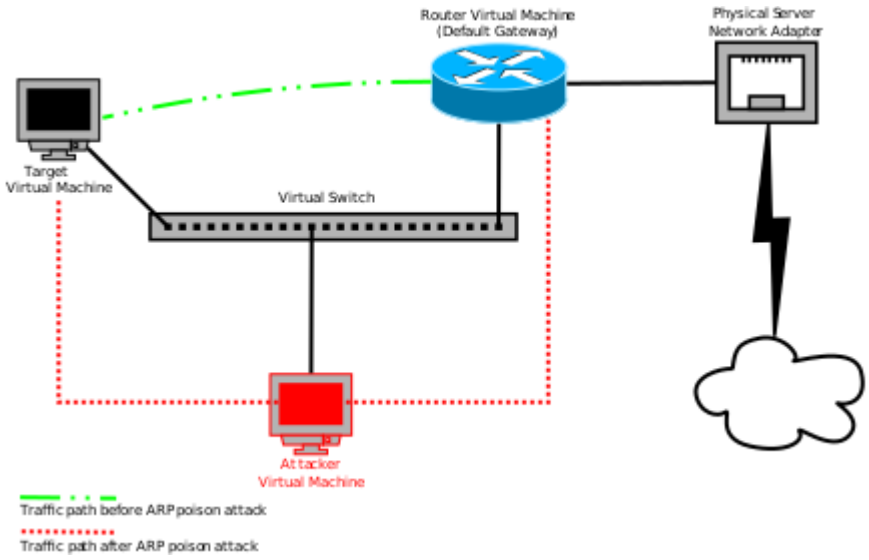



The following video walks through the attack and results under VMWare ESXi 6.0 using the standard ESXi virtual switch.

---

# DEF CON 24 DEMO: ARP Poisoning Attacks in Virtual Networks

This post includes demo videos which illustrate the effects of an ARP poisoning Man-in-the-Middle attack within a virtualized networking environment. The 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 videos walk through the attack and results under VMWare ESXi 6.0 using the standard ESXi virtual switch as well as Microsoft Server 2012 HyperV using the Cisco Nexus 1000v virtual switch.