ANYCon 2017 Talk – VLAN Hopping, ARP Poisoning and Man-In-The-Middle Attacks in Virtualized Environments

---

ANYCon Invited Talk

I have been invited to give a talk on my research at the upcoming ANYcon InfoSec and Hacking conference which will be held in Albany, NY from June 16th – 18th. This is a new conference bursting into the InfoSec scene, and is shaping up to be similar in size and spirit to other family oriented mainstream InfoSec conferences like DerbyCon and BSides. The talk abstracts are starting to pop up on the Agenda page, and my talk is listed in the Offensive Track.

While your hanging in Albany that weekend you may also want to stay a few extra days and check out the Dead & Company concert that will be at SPAC on June 20th!

DEF CON 24 Presentation: VLAN

Hopping, ARP Poisoning, & Man-in-the-Middle Attacks in Virtualized Environments

---

DEF CON 24 Talk Resources – VLAN Hopping, ARP Poisoning and Man-in-the-Middle Attacks in Virtualized Environments

We are aware that our presentation slides and white paper somehow went missing from the DEF CON 24 CD. They have been submitted for inclusion on the Media Server, but until then you can find the talk information, white paper, and slides at the following links:

Talk Abstract & Speaker Bios

White Paper

Presentation Slides

Also note that all of the demo videos are below. Scroll down for detailed explanations of each test scenario, and links to all of the fully narrated YouTube videos.

Enjoy, and if you have any questions, or are looking for someone to assist in evaluating your environment against these attacks feel free to use the contact form to reach me.

Edit:

The materials are now available on the DEFCON media server:

White Paper

Presentation Slides

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:

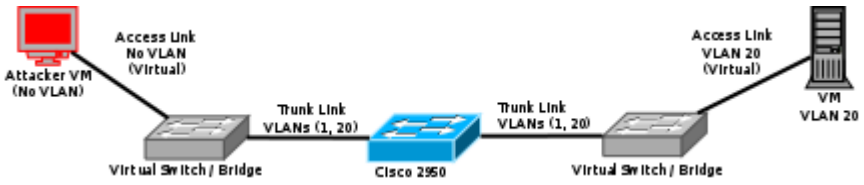
The following video walks through the attack process and results.

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

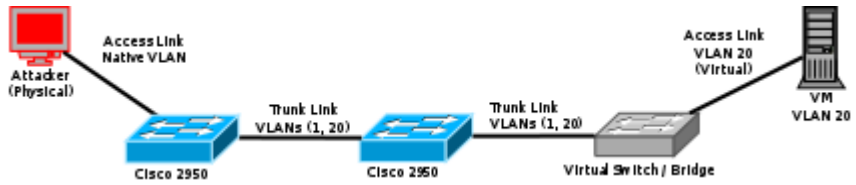
network diagram illustrates the configuration used for each of the experiments:



The following video walks through the attack process and results.

DEF CON 24 DEMO: Double Tagging VLAN Hopping Attack Against the Proxmox Virtual Network Using Two Physical Switches

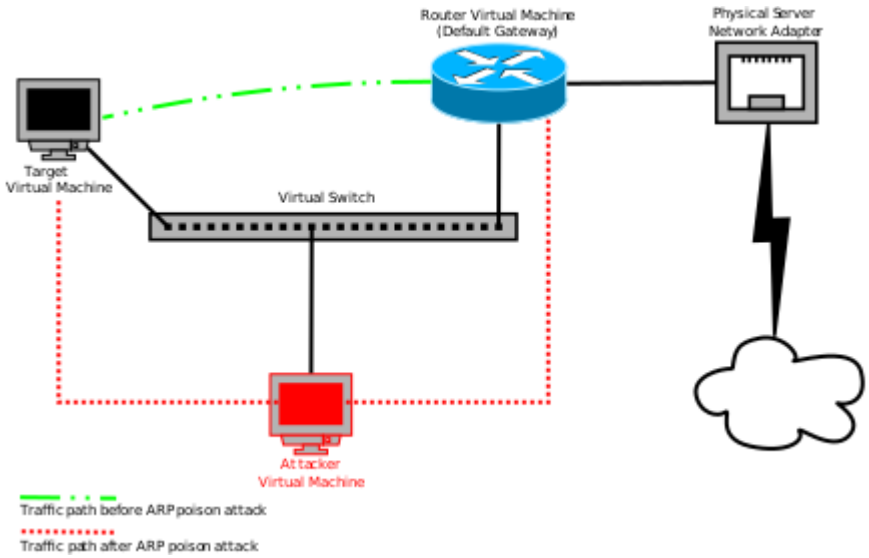
This post demonstrates the effects of running a Double Tagging VLAN Hopping attack against the ProxMox hypervisor environment. In this scenario there are two Cisco 2950 switches in between the attacker and the virtual network. The experiment was performed on seven different hypervisor/virtual network 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 process and results against a virtual machine hosted within the ProxMox hypervisor environment.

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.

DefCon 23 Presentation: Exploring Layer 2 Network Security in Virtualized Environments

---

DefCon 23 Video Demo: Rogue DHCP/DNS server on Citrix XenServer 6.2 with Open vSwitch 1.4.6