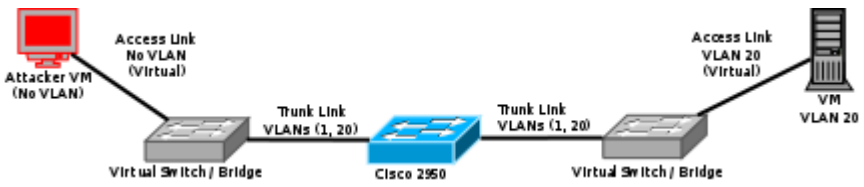
# DEF CON 24 DEMO: Double Tagging VLAN Hopping Attack Between Two Virtual Networks With a Cisco 2950 Switch in the Middle

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.

---

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

---

## DefCon 23 Video Demo: Rogue DHCP/DNS server gaining root access to target

---

## DefCon 23 Video Demo: Rogue DHCP/DNS server ShellShock exploit proof of concept

---

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

---

# DefCon 23 Video Demo: MAC Flooding on Citrix XenServer 6.2 with Open vSwitch 1.4.6

---

# Exploring Layer 2 Network Security In Virtualized Environments – DerbyCon 4.0

I gave a talk this past weekend on part of my Ph.D. dissertation research at the DerbyCon 4.0 “Family Rootz” Computer Security conference in Louisville, KY. Take a look at the following video to view the talk in its entirety. The rest of the conference videos are available here.

# Xen Cloud Platform (XCP) – Cloning Hard Drive Woes

The main hard drive seems to be flaky in one of my XCP servers. I decided to use Clonezilla to clone sda to another drive to see if it is in fact the hard drive. After cloning over the drive I found that my LVM storage group VG_XenStorage-xxx was not mounting, and XenCenter was giving off the following error when trying to connect to the server: **“This server cannot see any storage”**

Turns out the LVM volume group was inconsistent after the clone, my guess is because the hard drives were of the same capacity but different brands so there may have been some differences. Using the lvs and vgs commands did not show the LVM volume information, but instead displayed a kernel dump with a plethora of information. The main error being about the inconsistency of the volume group. In order to solve the problem I had to perform the following command:

Then restart the xapi service:

Time to see if we can make it crash again with the new drive!

# Xen Cloud Platform (XCP) – Assigning A VLAN An IP Address

Once you create VLAN's on your XCP server you will find that the physical interface you used to be able to hit by an IP address no longer responds. This is because you have trunked the interface into multiple VLAN's and need to assign IP's to the VLAN interfaces rather than the physical interface.

In order to do this first remove the static IP from the physical interface if it was assigned one. Then do the following:

(Note this example uses eth1 as the physical interface the VLAN's are assigned to.)

First lets check the settings on the VLAN interface you need to assign an IP to.

This should return a list of the VLAN interfaces parameters for VLAN201

Notice the following parameters are all empty:

Lets assign an IP address to this VLAN:

Now we can confirm the setting by listing the parameters again:

Which should show:

Now try to ping the address it should respond again.

You can also set it to use DHCP instead of assigning a Static address by using

---

# Xen Cloud Platform (XCP) – Setting Up A VLAN

One very useful feature of XCP is the ability to setup VLAN networks for your virtual machines to use. This gives an administrator fine grained control on what network a machine belongs on. This will work as long as the network interface that is assigned to your VM's is plugged into a trunked port on a switch that has been setup with VLAN tags.

In order to start assigning VLAN's to a physical interface or pif in Xen terms do the following:

Get a list of the physical network interfaces and their corresponding UUID's:

This should return something similar to this:

This shows us the 2 network interfaces that are installed in the server. ETH0 is assigned as the management interface and ETH1 is assigned to the virtual machines.

Now we need to create a new network for our VLAN:

This creates a new network named network201 that corresponds to the VLAN tag 201 on the switch. When running this command you will get a uuid as output.

Now we need to assign the VLAN tag 201 to this network, and bind it to a physical interface (eth1 in this case):

Thats it the new VLAN201 is created and can be selected for use by your virtual machines. You can confirm it’s presence by doing:

Which now will display your 2 physical interfaces as well as the new VLAN201 interface: