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

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:

Xen Cloud Platform (XCP) – Add A Disk To The Default LVM Volume Group

If you initially install XCP using only one disk you can still add more drives later if you find you need more room. XCP uses LVM storage to manage the partitions created for new Virtual Machines which allows you to extend the default volume group at your leisure among other things.

In order to add a new disk to your default volume group perform the following steps.

Install the new drive into the computer

Partition it using fdisk

After you create the partition change it’s type to Linux LVM:

Enter the menu option T to change the partition type:

Enter the menu option 1 to choose the first partition:

Enter the menu item 8e to choose Linux LVM:

Enter the menu item p to print the partition output to verify that it is set to Linux LVM:

Enter the menu item w to save the partition information:

Enter the menu item q to quit:

Now we can add the partition to the volume group.

Set the partition as a physical volume:

Find out the name of the existing volume group:

This should output something like this:

We are interested in this line:

Add the new physical volume to the existing volume group

Now you can verify that it worked by typing:

This should list the volume group and display it’s current size, which should indicate the size of the old volume group + the size of the added disk.

Xen Cloud Platform (XCP) – Local ISO Storage

Repositories

XCP supports local ISO storage on an internal hard drive. It is not available as an option in the xsconsole – Disk and Storage Repositories menu. However you can set one up with a little bit of command line magic.

The best way to do this is by using a second hard drive in the server. Once installed use fdisk to create the partition.

Proceed to follow the prompts and create a new partition using the ext3 file system.

Once the partition is created format it:

Now make the directory that will be the mount point for the volume.

Mount it.

Then add the following entry in /etc/fstab so that the partition is mounted at boot.

Now let Xen know it’s there.

That’s it. You can now place ISO images in /var/opt/xen/iso_import and they should automatically show up in XenCenter under local storage. You will also be able to use them to install new virtual machines via the drop down menu.

Xen Cloud Platform (XCP) – Linux Templates Will Not Boot To CD/DVD

It seems that the Linux templates in XCP 1.0 & 1.1 are all bugged and will not boot to a CD/DVD drive upon first boot of the virtual machine. This makes it very difficult to start up your installation media. In order to work around this you can either use the “Other Installation Media” template and fill in the blanks, or you can do a little command line magic once you create your virtual machine from one of the Linux templates. The problem is that the boot order does not get set from the template upon VM creation, so once you have the VM created do the following:

List all of the Virtual Machines currently on the server:

You should see a list that contains all of your virtual machines in this format:

Next check the current boot order setting by issuing the following command:

You will see something like this:

Notice there is no boot order setting listed, add one by issuing the following command:

Now check the boot order setting again:

And we see that it is now set to “dc” a.k.a. CDROM/DISK

That’s it! You should now be able to start the virtual machine and have it boot to it’s installation media.