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.

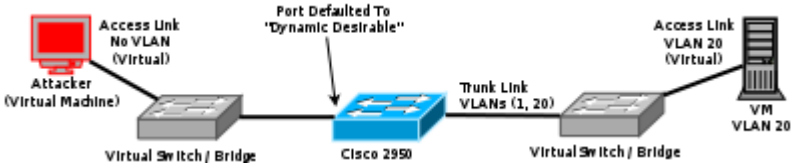
This experiment was performed on seven different hypervisor/virtual network configurations in order to perform

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: Switch Spoofing Attack Against a Cisco 2950 Switch from the VMWare ESXi 6.0 Hypervisor Environment

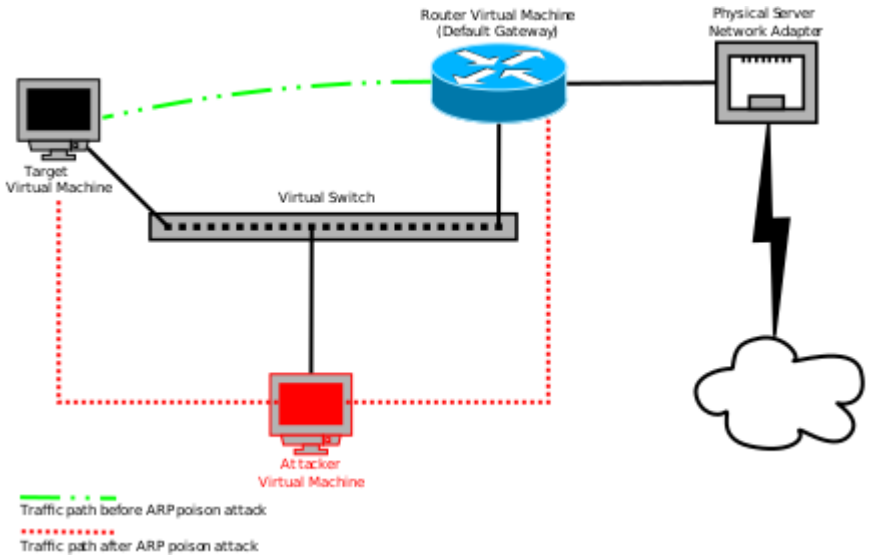
This post includes a demo video which illustrates the effects of a Switch Spoofing attack launched from within a virtualized networking environment. The experiment was performed on seven different hypervisor/virtual network configurations in order to perform a systematic evaluation of the effects across 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.

How To: CentOS 7 Router

I have had to create a few CentOS 7 minimal router systems over the past few weeks for my research environments and decided to document the process. CentOS 7 makes use of systemd and firewalld which is a change from previous versions which were openrc and iptables based. The process of creating a minimal router system is fairly straight forward and can be completed in a very short amount of time after the initial installation with minimal dependencies.

In order to create a router the system will need multiple network interface cards assigned to it. In this article we will focus on a system with two network interfaces. Once will be considered the public interface and the other will be the

private interface. Network Address Translation (NAT) will be used in order to pass traffic from the public interface through the router to the systems located on the private LAN.

First install CentOS 7 to the system from the minimal installation media. You can set the hostname and address information during installation or wait until after and edit the configuration files manually. Once the installation is complete perform the following actions:

Change the hostname:

Change the IP address of the first network interface:
(Note: your network interface may be named something different than eth0)

Add the following information to the file:

Change the IP address of the second network interface:

Add the following information to the file:

Run the following command to restart the networking service:

Now the firewall service has to be configured to support NAT:

First create the following file to allow IP forwarding:

In the file add the following line:

Then run the following command to activate IP forwarding:

Now we need to create a firewall rule to allow IP masquerading between the public and private interfaces:

Now assign eth0 to the external firewall zone:

Set the default zone to the internal zone:

Reload the firewall service:

Now restart the networking and firewall services:

Verify that the firewall settings persisted through the reload:

That’s it! Now test to see if it works by connecting a system to the private side of the router. Then assign it an IP address and subnet mask on the private LAN, and set the default gateway to the private interface on the router. DNS should be set to the same DNS server that the router is using unless you are running a private DNS server on your LAN.

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