New Custom vCORE VirtualBox Appliance With EMANE, Quagga OSPF-MANET, & NASA ION-DTN

I have put together a fully updated vCORE VirtualBox appliance based on Debian 9.6 that includes the latest versions of CORE, EMANE, Quagga OSPF-MANET, and NASA's ION.

This version of the virtual appliance includes the following releases:

[CORE 5.2 (git)](#)
[EMANE 1.2.3 (git)](#)
[NRL Quagga mr_0.99.21mr2.2 (source)](#)
[NASA ION-DTN 3.6.2 (sourceforge)](#)

All dependencies were installed via apt-get including all packages required to build the above listed software from source. All source code for the above listed packages is located in /usr/src/ for end user customization and updates. The virtual machine was designed to be used for development purposes, and can be fully customized by the end user.

username: core
password: eroc

The 'core' user has sudo privileges, and core-daemon is set to run on startup. You may want to edit the VirtualBox network settings *(ie. bridge, NAT, host-only)* for the VM to suit your environment.

Download the new vCORE VirtualBox appliance [here](#).
md5 hash: e5a80ee4dd5893ec3bfa63afa54b11b2 vCORE.ova

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!

HackCon#12 Invited Talk Trailer

The kind folks that organize the HackCon#12 conference made a "trailer" for my upcoming talk in Oslo, Norway.

Upcoming Invited Talk: HackCon#12 – Oslo, Norway

I have recently been invited to give a presentation on my research in Layer 2 Network Security in Virtualized Environments at the upcoming [HackCon#12](#) Norwegian Cyber Security Convention which will be held in Oslo, Norway from February 13th-16th. More information about the talk can be found [here](#).

New Publication: International Journal of Communication Networks and Distributed Systems

I recently have had a new article published in the [International Journal of Communication Networks and Distributed Systems](#). The article was submitted to the journal about a year and a half ago, and was released in a [Special Issue on Software Defined Networks and Infrastructures, Network Function Virtualisation, Autonomous Systems and Network Management](#). You can find a copy of the final draft of the article on my [publications](#) page.

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:
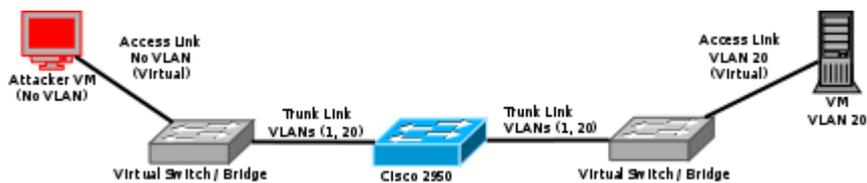

The following video walks through the attack process and results.

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.