

This story appeared on Network World at <http://www.networkworld.com/news/2008/080808-black-hat-spotlights-virtualization.html>

Black Hat spotlights virtualization, DNS issues

By [Ellen Messmer](#), [Tim Greene](#) and Robert McMillan, Network World, 08/08/2008

LAS VEGAS — The 12th Black Hat conference convened at Caesar's Palace last week, where the 4,500 attendees (a 12.5% increase over last year) heard about the security problems that will plague virtualized environments, why [Cisco](#) routers are more of a hacker target than ever and a detailed explanation of DNS attacks.

Attendees also found a conference show floor that was dominated by vendor booths. The booths, once a rarity at the conference, are becoming more prevalent as vendors inject themselves into the Black Hat mix. While he didn't apologize for their presence — and noting that vendor sponsorships are important to the financial success of the conference — Black Hat founder and director Jeff Moss did distance the content of the show from the sponsors. Presenters at the show briefings present vendor-neutral material chosen solely for its value to the security community, he said during his opening remarks.

Vendor booths aside, the audience was tuned to far more weighty topics, such as the security problems that will ultimately arise out of the industry's headlong push into virtualizing everything.

[Virtualization](#) “will not save you money, it will cost you more,” and “virtualized security can seriously impact performance, resilience and scalability,” said Christopher Hoff, chief security architect at Unisys, in an impassioned presentation. Hoff argued the user community is being sweet-talked into virtualization by an industry unmindful of the security consequences.

Related Content

“Over the next 12 to 18 months, there's a very uncomfortable set of circumstances as every vendor rushes out to say we've virtualized,” said Hoff in his talk, entitled “The Four Horsemen of the Virtualization Apocalypse.”

Using strong language directed at the network industry, Hoff argued that “it's getting real messy” as Cisco, Brocade, 3Leaf, Xsigo, among others gallop off toward virtualization of basic switching infrastructures. This is being done without a clear notion of what the security consequences are for enterprise customers accustomed to wholly different topologies that include technologies such as spanning tree and STP.

“A virtual switch is just a piece of code like a hypervisor,” said Hoff about the industry’s new direction. “It’s basically Layer 2 switching modules,” adding it means you’ve collapsed the network into “a single tier” and “it all boils down to three settings in a GUI.”

The virtual security — he called it “VirtSec” — that’s arising in the wake of anticipated changes is ushering in virtual appliances that will become the cornerstone for trying to replicate traditional defenses such as intrusion-prevention systems, antivirus and firewalls, Hoff said. But as security functions compete for virtual-machine resources, there will be a performance hit just as is seen in unified threat management (UTM) devices today that combine IPS, firewall and other functions, he said.

Capacity planning with a virtualized network is “going to be very difficult to predict,” Hoff said, adding he was profoundly skeptical that trying to virtualize a firewall is going to work as DMZs are pushed into going virtual, too.

“If I decide to V-motion a firewall, it won’t work,” said Hoff, alluding to his own research with VMware and its V-Motion capability to rapidly deploy VM images. With virtualization, “you won’t get rid of host-based security software. As we add more solutions, we add complexity,” Hoff said, advising the Black Hat audience “not to be dragged into the environment.”