User Mode Linux: Maximizing performance, jailing attackers

By *srlinuxx*
Created *12/07/2006 - 8:13am*
Submitted by srlinuxx on Wednesday 12th of July 2006 08:13:28 AM Filed under Interviews [1]

User Mode Linux (UML)has ideal security features for controlling and jailing hackers once they've taken the sweetened bait of a 'honeypot,' says User Mode Linuxauthor and project architect Jeff Dike. UML can log all terminal traffic to the host in a way that's invisible and impossible to interfere with from inside the UML unlike Xen and VMware.

Take a tour of UML with Dike as he offers best practices, explains how to boot from an empty jail, talks about jailing attackers and more.

What are some unique issues of server consolidation with User Mode Linux?

Jeff Dike: From my point of view, server consolidation doesn't differ greatly from any other virtualization workload. So, the advantages of UML apply here the same as in other areas.

One aspect of server consolidation that may distinguish it from other virtualization workloads is that the host administrator may not trust the UML administrators. In this case, the UML administrators won't have shell access on the host, and the host administrator will need to decide how they will be allowed to access their UMLs.

The easy solution is to allow only network access. But this will increase the support burden when UML owners make their UMLs inaccessible by misconfiguring their networks. In this case, allowing the equivalent of logging in on a hardwired terminal would be nice, so that the UML admins still have access to their UMLs and can fix the network themselves.

So how should host administrators determine access criteria for UML?

Full Story [2].

Interviews

Links:
[1] http://www.tuxmachines.org/taxonomy/term/119

[2] http://searchopensource.techtarget.com/tip/0,289483,sid39_gci1197366,00.html