Monday, April 23. 2007

### Breachable virtual machines?

The regular reader of my blog may have detected that i´m not really a fan of virtualisation in the Unix sphere. Server virtualisation is selled by it´s proponents as the cure-for-all-datacenter problems, but with a competent administration it solves a problem that doesn´t exist. You were able to split a machine for several tasks since the invention of Unix.

But there is another problem: Many user believe, that the seperation of a VM is comparable to real metal from a security standpoint. But: All virtualisation technologies are just large heaps of code, and it would be foolish to assume, that the hypervisor is more secure or less buggy than any other software of comparable size. But exactly this belief seems to exists, at least when you talk with many users of virtualisation, as most of them don´t take the hypervisor really into consideration from a security standpoint.

For a long time i had this suspicion, that there is no exploit to evade virtual machines only for the reason, that nobody searched for it and not out of a theoretical impracticality, because as i said it before: It´s just software. Well, this dim feeling was confirmed by a paper of Tavis Ormandy of Google with the title "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments". He found strong indices for the possibility to break out of virtual machines. The linked paper is a really interesting read.

To make it clear: I think, that virtualisation has some use cases, but they are not nescessarily those the media, analysts and other experts want tell you. At the end, i would like to put a question. You can´t think of them as really separated systems and virtual machines don´t really solve the problems of managing hundreds of operating system instances. But: What´s the remaining value proposition of virtual machine based virtualisation, when you take all this into consideration? Besides of herding Windows systems, you weren´t able to consolidate on a single operating environment ?

Posted by Joerg Moellenkamp in English, The IT Business at 19:47