

27 May 2008

By: Marius Oiaga, Technology News Editor



[Microsoft: How to Hack Vista via Linux in Just a Few Minutes](#)

Video tutorial

Windows has never been an epitome of security and alternatives - the open source Linux and Apple's Mac OS X are considered superior in this aspect. However, Windows Vista was built as an apex of security compared to its predecessors. Featuring examples of technology as the Windows BitLocker Drive Encryption, and a revamped architecture for safeguarding sensitive user data including account passwords, Vista is certainly designed to be an evolution in comparison to Windows XP. And yet Microsoft's latest and most secure operating system can be completely yours in a matter of minutes via an attack launched from Linux. Out of all the people, [Roger Halbheer](#), Chief Security Advisor of Microsoft EMEA is the one who highlighted the Windows Vista hack. "No, no. For sure. I am not going to give you advice how to hack," Halbheer stated, but then pointed to a video tutorial put together by Offensive Security, demonstrating a Windows Vista hack using nothing more than a BackTrack distro of Linux. "BackTrack is the result of the merging of two Innovative Penetration Testing live Linux distributions - Whax and Auditor," reads the description of the open source operating system tailored to perform penetration testing actions. "Based on SLAX (Slackware), BackTrack provides user modularity. This means the distribution can be easily customized by the user to include personal scripts, additional tools, customized kernels, etc." The [video demonstration](#) authored by Jesse Varsalone involves a Windows Vista hack which spans no more than a couple of minutes, and this only because a reboot is necessary. You will be able to see that the Logon screen in Windows Vista, with the user name and password, provides no barrier at all against this hack. In fact, it might as well not have existed at all. Of course, the scenario is only valid if the attacker has physical access to the Vista machine. In this context, BackTrack Linux will not permit a remote attacker to hack Vista. "I am always amazed about this kind of videos, which still surprise people. If look years back, we published the 10 Immutable Laws of Security, which contains Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore. The hack shown above needs physical access," Halbheer emphasized. Halbheer's solution is rather simple. Windows BitLocker Driver Encryption provides strong protection against hacks using the BackTrack Linux operating system. Still, while BitLocker is indeed shipped as part of Windows Vista, it is only featured in the Ultimate and Enterprise SKUs. This means that all the remaining Vista editions are exposed to the BackTrack Linux hack which bypasses the Logon screen completely, without requiring the attacker to know, guess, use brute force or even enter a password.