

Video Tutorial: Pass-The-Hash Toolkit

Ryan Linn is back with another video for your learning pleasure. This time he gives a video tutorial of an existing toolset, the Pass-The-Hash Toolkit by Hernan Ochoa (Core Security Technologies). Core describes it as, "The Pass-The-Hash Toolkit contains utilities to manipulate the Windows Logon Sessions maintained by the LSA (Local Security Authority) component. These tools allow you to list the current logon sessions with its corresponding NTLM credentials (e.g.: users remotely logged in thru Remote Desktop/Terminal Services), and also change in runtime the current username, domain name, and NTLM hashes (YES, PASS-THE-HASH on Windows!)."

So what does all that mean? As with his other videos, Ryan tackles this topic in a very easy to follow process. So watch along as he integrates the PTH Toolkit in a makeshift penetration test, and shows how an attacker can utilize credentials without ever having to crack a single password. Oh by the way, he cracks them, too. This way he can impersonate a legitimate user without knowing their password, and then again while knowing their password. Ryan then goes one step further with his talk at ChicagoCon 2009s on May 9 with fellow EH-Net Columnists, Brian Wilson, when they team up for Cain BeEF Hash: Snagging Passwords without Popping Boxes. They not only show you some of their cutting-edge research results, but also perform it in a live demo! [Click for Conference Details.](#)

del.icio.us

Discuss in Forums {[mos_smf_discuss:Linn](#)}

Ryan Linn is a Scheduled Speaker for the Spring ChicagoCon

The \$100 Ethical Hacking Conference is May 8 - 9, 2009

Ryan Linn, CISSP, MCSE, GPEN - Ryan is currently an Information Security Engineer at SAS Institute. Employed in the computer industry since 1997, he has held positions ranging from web developer to Unix Systems Programmer at a large university to his current position in Information Security. Ryan has been responsible for working with large scale deployments of various flavors of *nix, high availability web and database clusters, as well as for application programming in high availability environments. In the past few years, Ryan has incorporated Windows security into his responsibilities, and is now part of the team responsible for information security globally in one of the largest privately held software companies in the world.