

Video Tutorials: New BeEF Hotness with Metasploit and Samurai

A new version of the Browser Exploitation Framework (BeEF) has been released. This new release incorporates both my code from my Security B-Sides update of the ChicagoCon Talk "Cain Beef Hash: Snagging Hashes without Popping Boxes" as well as RSnake and Jabra's modules presented at Defcon. Enclosed in this update are some videos describing how to use the modules that I created which allow for realtime interaction with Metasploit. These modules directly communicate with Metasploit to setup the modules which will be used in further browser exploitation. These videos demonstrate how to use the Samurai WTF distribution's initial setup of BeEF, and to upgrade it to the latest version. Once you are upgraded to the latest version, there are 2 more videos, one to utilize the integration to do "point and click" browser autopwn from a browser hooked via XSS. The other example demonstrates how to leverage a domain's "Local Intranet" policy to capture NTLM/LM Challenge credentials with a static challenge, which can then be turned into usable credentials. The Metasploit code required for this to work is in the 3.3 dev trunk and was added in August after Defcon, so you may need to pull out of the dev trunk to have all of the pieces you need.

Wade Alcorn is the author and maintainer of BeEF and was a great help in getting these added. If you haven't checked out BeEF before watching these videos, hopefully you will check it out now. If you have more great ideas for ways to extend and contribute to the framework please do so. I also appreciate H D Moore's help in getting the Metasploit code to make all of this work seamlessly into the Metasploit trunk. You can find some additional videos of RSnake and Jabra's content on Vimeo.

del.icio.us

Discuss in Forums {mos_smf_discuss:Linn}

Updating BeEF in Samurai WTF

Metasploit's AutoPWN in BeEF

Capturing NTLM Challenge Credentials

with Metasploit and BeEF

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.