

## Video Review: Cobalt Strike Penetration Testing Software

By Ryan Linn

Cobalt Strike is the latest tool that Raphael Mudge (@Armitagehacker) has released at <http://www.advancedpentest.com/> to help penetration testers optimize their workflow and pen testing tasks. Cobalt Strike is a commercially supported version of Armitage, Cyber Attack Management for Metasploit, with a whole slew of new features added to aid in social engineering attacks, phishing, and targeted exploitation. As described on their own site:

"Cobalt Strike is threat emulation software. Red teams and penetration testers use Cobalt Strike to demonstrate the risk of a breach and evaluate mature security programs. Cobalt Strike exploits network vulnerabilities, launches spear phishing campaigns, hosts web drive-by attacks, and generates malware infected files from a powerful graphical user interface that encourages collaboration and reports all activity."

Stay with us after the break as we examine more details of this new software package, thoughts on how it might fit into your arsenal of tools and also an exclusive video by Ryan Linn offering a first look at Cobalt Strike to all EH-Netters.

Discuss in Forums {mos\_smf\_discuss:Linn}

Cobalt Strike offers great features such as a teamserver that allows multiple people to work on a single Metasploit instance and share shells between consultants as well as IRC features to chat. The new features for social engineering and phishing allow a simple workflow for creating web-based attacks similar to the Social Engineering Toolkit (SET), and then leads you all the way to mass mailing the phishing emails to get your targets to click the link. While some of the attacks may be similar, Cobalt Strike has written this functionality from scratch to integrate more closely within the Cobalt Strike workflow.

With an easy to use GUI, Cobalt Strike simplifies many of the testing tasks including allowing bulk attacks by selecting multiple hosts and choosing attacks. To round out the features which are required for a penetration testers, Cobalt Strike has added reporting capabilities to allow the activity, vulnerabilities, and other information to be exported into PDF files. Additional work has been done to allow for browser and application fingerprinting remotely to allow initial recon as part of a social engineering attack before targeting the application versions that you know are in use. With all of the features of Metasploit plus the additions that Rafael has added to the tool, this new software package is a great alternative to other pen testing tools out there.

We could talk about all of the new features and use cases, but it would not do it justice. One of the great things that sets Rafael and his company, Strategic Cyber, LLC, apart is that they have done a lot of work to explain how to use Cobalt Strike and how to get the most out of the product. If you head over to <http://www.advancedpentest.com/training>, there are tons of videos discussing the new features and focusing on each step in the pen testing process. The site has tons of documentation, and, even though this is a new release, already has a lot of support information. Cobalt Strike has an entry price of \$2,500 a year, which is much lower than many other tools. It comes with commercial support, no restrictions on the number of IPs, and no installation limits allowing a lot of flexibility as to how you use it.

Now that you know a little bit about Cobalt Strike, I've done a quick video showing some of the basic features. In this video, we utilize some of the web attack vectors as well as network attacks to go from un-authenticated to Domain Admin in 15 minutes and talk a bit about some of the cool features that Cobalt Strike offers. Be sure to see our written conclusions below the video.

Ryan Linn's First Look at Cobalt Strike

Overall, I enjoyed getting to learn Cobalt Strike. It's a new release, and it wasn't perfect. On the other hand, it did all of the things that I needed to do quickly, and it made pass-the-hash a lot easier than going through the

console. Having different tables was another nice feature, so that multiple tasks could be done at once and compartmentalized so that the text wasn't intermixed. As it continues to mature and add features, Cobalt Strike is going to be a good tool for individual testers and teams who aren't looking to spend \$100k on tools. Raphael Mudge is a great contributor to the community as well, so as you support this project, you will also be allowing him to spend his full time developing Cobalt Strike as well as other contributions to the security community. Cobalt Strike is also available with a 7-day free trial, so go download it, play and let us know what you think!

Ryan Linn, CISSP, MCSE, GPEN - Ryan is a Senior Security Consultant for Trustwave SpiderLabs Network Penetration Testing practice with a passion for making security knowledge accessible. In addition to being a columnist with The Ethical Hacker Network, co-author of "Coding for Penetration Testers", and a frequent presenter at security conferences, Ryan has contributed to open source tools including Metasploit, Dradis and the Browser Exploitation Framework (BeEF).