

Video: The 15-Minute Network Pen Test Part 2

There are numerous tools used in the Penetration Testing (pen testing) process, and there are plenty of books that go into how to use the individual tools. There are very few resources that discuss how the tools are used and how to approach the process. Parts 1 and 2 encompass the basic outline of what was presented at a talk given to the Duke University ACM Chapter with some minor changes.

In Part 1, we took the viewer through the initial network recon stage through actual exploitation using Metasploit. Initially the network is scanned through Nmap, and then continued with Nessus. We importing the Nessus vulnerabilities directly into Metasploit, determined the corresponding modules for the specific host, then used the module to compromise a remote Microsoft Windows XP box.

Part 2 covers some of the post-exploitation tasks that a pen tester may use. It begins with some basic Meterpreter tasks. Meterpreter is a specialized pen testing shell that is included in Metasploit as a payload. Using Meterpreter, password hashes are obtained from the exploited machine, and Ophcrack is used to crack the obtained passwords. While the passwords are cracking offline, the viewer is taken back to Meterpreter in order to create a hidden cmd.exe shell on the remote host. Finally we create a new user and add that user to the Administrators group. Ready to see it in action?

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

While these are just a few of the tasks that a pen tester will perform, these videos should whet the appetite for more

knowledge. Many of these tools are covered in-depth and with an emphasis on the process, skills, and mindset necessary to become a pen tester in the SANS Security 560 class: Network Penetration Testing and Ethical Hacking. I highly recommend this class if you are interested in learning more about these tools and how to effectively leverage them. Another well received course is the Offensive Security 101 AKA OSCP class which uses the Backtrack Live distribution . The Backtrack Live distribution contains many of the tools discussed in the videos and the course is designed by the designers of Backtrack. Other great resources can be found on the home pages for each of the tools listed below, and of course, The Ethical Hacker Network.

Nmap: <http://nmap.org>

Metasploit: <http://www.metasploit.com/>

Nessus: <http://www.nessus.org/>

Ophcrack: <http://ophcrack.sourceforge.net>

Microsoft Windows: <http://www.microsoft.com/>

SANS: <http://www.sans.org/>

Offensive Security: <http://www.offensive-security.com/>

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.