FabioBaroni / awesome-exploit-development

A curated list of resources (books, tutorials, courses, tools and vulnerable applications) for learning about Exploit Development

8 commits **1** branch **0** releases **1** contributor MIT

Branch: **master** New pull request Find File Clone or download

FabioBaroni Add article link — Latest commit `17aee3f` on Jan 28, 2016

LICENSE	Initial commit	4 years ago
README.md	Add article link	4 years ago

README.md

awesome-exploit-development

A curated list of resources (books, tutorials, courses, tools and vulnerable applications) for learning about Exploit Development

A project by Fabio Baroni.

Read the full article here! http://www.pentest.guru/index.php/2016/01/28/best-books-tutorials-and-courses-to-learn-about-exploit-development/

BOOKS

- Hacking - The art of exploitation
- A bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes
- Sockets, shellcode, Porting, and coding: reverse engineering Exploits and Tool coding for security professionals
- Writing Security tools and Exploits
- Buffer overflow attacks: Detect, exploit, Prevent
- Metasploit toolkit for Penetration Testing, exploit Development, and vulnerability research

TUTORIALS

Corelan.be

- https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/
- https://www.corelan.be/index.php/2009/07/23/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-2/
- https://www.corelan.be/index.php/2009/07/25/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-3-seh/
- https://www.corelan.be/index.php/2009/07/28/seh-based-exploit-writing-tutorial-continued-just-another-example-part-3b/
- https://www.corelan.be/index.php/2009/08/12/exploit-writing-tutorials-part-4-from-exploit-to-metasploit-the-basics/
- https://www.corelan.be/index.php/2009/09/05/exploit-writing-tutorial-part-5-how-debugger-modules-plugins-can-speed-up-basic-exploit-development/
- https://www.corelan.be/index.php/2009/09/21/exploit-writing-tutorial-part-6-bypassing-stack-cookies-safeseh-hw-dep-and-aslr/
- https://www.corelan.be/index.php/2009/11/06/exploit-writing-tutorial-part-7-unicode-from-0x00410041-to-calc/
- https://www.corelan.be/index.php/2010/01/09/exploit-writing-tutorial-part-8-win32-egg-hunting/
- https://www.corelan.be/index.php/2010/02/25/exploit-writing-tutorial-part-9-introduction-to-win32-shellcoding/
- https://www.corelan.be/index.php/2010/06/16/exploit-writing-tutorial-part-10-chaining-dep-with-rop-the-rubikstm-cube/
- https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/
- https://www.corelan.be/index.php/2010/01/26/starting-to-write-immunity-debugger-pycommands-my-cheatsheet/

- https://www.corelan.be/index.php/2010/03/22/ken-ward-zipper-exploit-write-up-on-abysssec-com/
- https://www.corelan.be/index.php/2010/03/27/exploiting-ken-ward-zipper-taking-advantage-of-payload-conversion/
- https://www.corelan.be/index.php/2011/01/30/hack-notes-rop-retnoffset-and-impact-on-stack-setup/
- https://www.corelan.be/index.php/2011/05/12/hack-notes-ropping-eggs-for-breakfast/
- https://www.corelan.be/index.php/2011/07/03/universal-depaslr-bypass-with-msvcr71-dll-and-mona-py/
- https://www.corelan.be/index.php/2011/11/18/wow64-egghunter/
- https://www.corelan.be/index.php/2012/02/29/debugging-fun-putting-a-process-to-sleep/
- https://www.corelan.be/index.php/2012/12/31/jingle-bofs-jingle-rops-sploiting-all-the-things-with-mona-v2/
- https://www.corelan.be/index.php/2013/02/26/root-cause-analysis-memory-corruption-vulnerabilities/
- https://www.corelan.be/index.php/2013/01/18/heap-layout-visualization-with-mona-py-and-windbg/
- https://www.corelan.be/index.php/2013/02/19/deps-precise-heap-spray-on-firefox-and-ie10/
- https://www.corelan.be/index.php/2013/07/02/root-cause-analysis-integer-overflows/

Opensecuritytraining.info

- http://opensecuritytraining.info/Exploits1.html
- http://opensecuritytraining.info/Exploits2.html

Securitytube.net

- http://www.securitytube.net/groups?operation=view&groupId=7 exploit research megaprimer
- http://www.securitytube.net/groups?operation=view&groupId=4 buffer overflow exploitation for linux megaprimer
- http://www.securitytube.net/groups?operation=view&groupId=3 Format string vulnerabilities megaprimer

Massimiliano Tomassoli's blog

- http://expdev-kiuhnm.rhcloud.com/2015/05/11/contents/

Samsclass.info

- https://samsclass.info/127/127_F15.shtml

Securitysift.com

- http://www.securitysift.com/windows-exploit-development-part-1-basics/
- http://www.securitysift.com/windows-exploit-development-part-2-intro-stack-overflow/
- http://www.securitysift.com/windows-exploit-development-part-3-changing-offsets-and-rebased-modules/
- http://www.securitysift.com/windows-exploit-development-part-4-locating-shellcode-jumps/
- http://www.securitysift.com/windows-exploit-development-part-5-locating-shellcode-egghunting
- http://www.securitysift.com/windows-exploit-development-part-6-seh-exploits
- http://www.securitysift.com/windows-exploit-development-part-7-unicode-buffer-overflows

COURSES

Corelan

- https://www.corelan-training.com

Offensive Security

- https://www.offensive-security.com/information-security-training/advanced-windows-exploitation/ AWE (Advanced Windows exploitation)

SANS

- https://www.sans.org/course/advance-exploit-development-pentetration-testers SANS SEC760: Advanced Exploit Development for Penetration Testers

Udemy

- https://www.udemy.com/windows-exploit-development-megaprimer/learn/#/ Windows exploit Development Megaprimer by Ajin Abraham

TOOLS

- IDA Pro
- OllyDbg
- WinDbg
- Mona.py

VULNERABLE APPLICATIONS

Exploit-exercises.com

- https://exploit-exercises.com/protostar/ Protostar
- https://exploit-exercises.com/fusion/ Fusion

EXPLOITS DATABASE

- https://www.exploit-db.com
- https://www.milw00rm.com
- http://0day.today
- https://packetstormsecurity.com
- http://www.windowsexploits.com
- http://iedb.ir
- http://www.macexploit.com