Offensive Security Exploit Development - Windows

Joas Antonio

Details

- This ebook is just a content guide for OSED certification. It's just an overview of the certification.
- My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

OSED - About

- WinDbg tutorial
- Stack buffer overflows
- Exploiting SEH overflows
- Intro to IDA Pro
- Overcoming space restrictions: Egghunters
- Shellcode from scratch
- Reverse-engineering bugs
- Stack overflows and DEP/ASLR bypass
- Format string specifier attacks
- Custom ROP chains and ROP payload decoders

Windbg

- https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/getting-started-with-windbg
- https://www.youtube.com/watch?v=QuFJpH3My7A
- https://www.codeproject.com/Articles/6084/Windows-Debuggers-Part-1-A-WinDbg-Tutorial
- https://github.com/microsoft/WinDbg-Samples/blob/master/TTDQueries/tutorial-instructions.md
- https://reactos.org/wiki/WinDbg_Tutorial
- https://riptutorial.com/windbg
- https://www.youtube.com/watch?v=8zBpqc3HkSE
- https://www.youtube.com/watch?v=KKZ_IaAGVks
- https://riptutorial.com/windbg/example/19170/important-commands
- https://www.tenforums.com/tutorials/5558-windbg-basics-debugging-crash-dumps-windows-10-a.html
- https://usermanual.wiki/Document/BeginnersGuidetoWinDBGPart1.2093398295/help
- https://github.com/repnz/windbg-cheat-sheet
- https://sites.google.com/site/taesaza0/etc/windbgcheatsheet
- https://www.stefangeiger.ch/2019/05/11/windbg-cheat-sheet.html
- https://oalabs.openanalysis.net/2019/02/18/windbg-for-malware-analysis/

Stack Buffer Overflow

- https://en.wikipedia.org/wiki/Stack_buffer_overflow
- https://pt.wikipedia.org/wiki/Transbordamento_de_dados
- https://www.rapid7.com/blog/post/2019/02/19/stack-based-buffer-overflow-attacks-what-you-need-to-know/
- https://cwe.mitre.org/data/definitions/121.html
- https://www.imperva.com/learn/application-security/buffer-overflow/
- https://sghosh2402.medium.com/understanding-exploiting-stack-based-buffer-overflows-acf9b8659cba
- https://www.freecodecamp.org/news/buffer-overflow-attacks/
- https://owasp.org/www-community/vulnerabilities/Buffer_Overflow
- https://embeddedartistry.com/fieldmanual-terms/stack-buffer-overflow/
- https://www.youtube.com/watch?v=1S0aBV-Waeo
- https://web.ecs.syr.edu/~wedu/Teaching/CompSec/LectureNotes_New/Buffer_Overflow.pdf
- https://infosecwriteups.com/stack-based-buffer-overflow-practical-for-windows-vulnserver-8d2be7321af5

Stack Buffer Overflow

- https://securityinformationnews.files.wordpress.com/2014/02/bufferoverflow.pdf
- http://www.cs.ucr.edu/~csong/cs255/l/stack-overflow.pdf
- http://repositorio.ufla.br/bitstream/1/31316/1/TCC_Buffer_overflow_teoria_e_exploracao.pdf
- https://arxiv.org/pdf/2012.15116.pdf
- https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS11/Alex%20Van%20Margraf%20_%20TCC_BufferOverflow_Mecan_Defesa.pdf
- https://www.dcc.fc.up.pt/~edrdo/QSES1819/lectures/qses-08-buffer-overflows_part2.pdf
- https://www.cs.colostate.edu/~massey/Teaching/cs356/RestrictedAccess/Slides/356lecture21.pdf
- https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture21.pdf
- https://www.exploit-db.com/docs/english/28475-linux-stack-based-buffer-overflows.pdf

Exploiting SEH overflows

- https://www.coalfire.com/the-coalfire-blog/march-2020/the-basics-of-exploit-development-2-seh-overflows#:~:text=In%20order%20to%20exploit%20an,current%20SEH%20records%20exception%20handler
- https://resources.infosecinstitute.com/topic/seh-exploit/
- https://www.exploit-db.com/docs/english/17505-structured-exception-handler-exploitation.pdf
- https://www.youtube.com/watch?v=UVtXaDtIQpg
- https://www.youtube.com/watch?v=ZCNv0hwd58c
- https://www.coalfire.com/the-coalfire-blog/march-2020/the-basics-of-exploit-development-2-seh-overflows
- https://www.corelan.be/index.php/2009/07/25/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-3-seh/
- https://sghosh2402.medium.com/vulnserver-gmon-command-exploit-1cdde13d2d64
- https://memn0ps.github.io/2020/01/27/Stack-Based-Buffer-Overflows-SEH-Part-2.html
- https://blog.devgenius.io/seh-overflow-with-multi-staged-jumps-95a0ae9438da
- https://www.youtube.com/watch?v=qc5-Yt2kCu8
- https://www.rapid7.com/resources/structured-exception-handler-overwrite-explained/
- https://www.fuzzysecurity.com/tutorials/expDev/3.html

Exploiting SEH overflows

- https://www.ffri.jp/assets/files/research/research_papers/SEH_Overwrite_CanSecWest2010.pdf
- https://www.securitysift.com/windows-exploit-development-part-6-seh-exploits/
- https://www.ins1gn1a.com/exploitation-of-seh/
- https://frostylabs.net/projects/vulnserver-seh-overflow/
- https://www.ethicalhacker.net/features/root/tutorial-seh-based-exploits-and-the-development-process/
- https://www.cyberark.com/resources/threat-research-blog/a-modern-exploration-of-windows-memory-corruption-exploits-part-i-stack-overflows
- https://www.shogunlab.com/blog/2017/11/06/zdzg-windows-exploit-4.html
- https://samsclass.info/127/proj/p15-seha.htm
- https://medium.datadriveninvestor.com/exploiting-millennium-mp3-studio-2-0-with-shellcode-payload-82f815bc809b
- https://techjoomla.com/blog/beyond-joomla/seh-buffer-overflow-exploitation-using-egghunter-payload
- https://msrc-blog.microsoft.com/2009/02/02/preventing-the-exploitation-of-structured-exception-handler-seh-overwrites-with-sehop/
- http://zeroknights.com/windows-exploit-dev-part-2-seh-buffer-overflows/
- https://sec4us.com.br/cheatsheet/bufferoverflow-seh

Intro to IDA Pro

- https://www.youtube.com/watch?v=Rk98rsmHbIg
- https://www.youtube.com/watch?v=N_3AGB9Vf9E
- https://www.youtube.com/watch?v=vb18UVF4a_o
- https://www.youtube.com/watch?v=zvWc-XsBKrA
- http://web.cse.msstate.edu/~hamilton/Forensics/resources/4%20-Intro%20to%20IDA%20Pro.pdf
- https://www.hackers-arise.com/post/2017/06/22/reverse-engineering-malware-part-3-ida-pro-introduction
- https://www.secpod.com/blog/introduction-to-ida-pro/
- https://resources.infosecinstitute.com/topic/basics-of-ida-pro-2/
- https://flylib.com/books/en/4.287.1.25/1/
- https://securityxploded.com/reversing-basics-ida-pro.php

Overcoming space restrictions: Egghunters

- https://www.ins1gn1a.com/exploiting-minimal-buffer-overflows-with-an-egghunter/
- https://github.com/r0r0x-xx/OSED-Pre
- https://www.securitysift.com/windows-exploit-development-part-5-locating-shellcode-egghunting/
- https://www.qa.com/course-catalogue/products/offensive-security-windows-user-modeexploit-development-exp-301-90-days-qaosed90/
- https://fluidattacks.com/blog/vulnserver-lter-seh/
- https://www.coalfire.com/the-coalfire-blog/may-2020/the-basics-of-exploit-development-3-egg-hunters
- https://www.purpl3f0xsecur1ty.tech/
- https://pt.slideshare.net/ajin25/exploit-research-and-development-megaprimer-win32-egghunter
- https://conceptofproof.wordpress.com/2014/01/07/egghunting-for-fun-and-profit-w-bison-ftp-server/
- https://bigb0ss.medium.com/expdev-winamp-5-12-exploitation-using-egghunter-b12383f7a449
- https://iwantmore.pizza/posts/quickzip-seh-win10-wow64.html

Egghunters

- https://www.exploit-db.com/docs/english/18482-egg-hunter---a-twist-in-buffer-overflow.pdf
- https://www.exploit-db.com/docs/arabic/44880-buffer-overflow-for-windows---egghunter.pdf
- http://www.hick.org/code/skape/papers/egghunt-shellcode.pdf
- https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/Exploit%20writing%20tutorial%20part%208-Win32%20Egg%20Hunting.pdf
- https://defcon.org/images/defcon-16/dc16-presentations/defcon-16-aharoni.pdf
- https://media.defcon.org/DEF%20CON%20China%201/DEF%20CON%20China%201%20presentations/DEF%20CON%20China%201.0%20-%20Workshops/DEF%20CON%20China%201.0%20-%20Dino-Covostos-Hack-to-Basics.pdf
- https://synapse-labs.com/sced.pdf
- http://index-of.es/Failed-attack-techniques/Exploit%20writing%20tutorial%20part%208-Win32%20Egg%20Hunting.pdf

Egghunters

- https://medium.com/syscall59/on-eggs-and-egg-hunters-linux-x64-305b947f792e
- https://www.youtube.com/watch?v=Znrvsf8Trvg
- https://www.youtube.com/watch?v=2o3t16ED8g0
- https://www.youtube.com/watch?v=OTP3TuzxqlM
- https://www.youtube.com/watch?v=CB625M1lWoo
- https://www.youtube.com/watch?v=5CEAJTANsZk
- https://osandamalith.com/2013/10/29/egg-hunting-fun/
- https://hackerculture.com.br/?p=1059
- https://www.fuzzysecurity.com/tutorials/expDev/4.html
- https://www.helviojunior.com.br/it/security/criacao-de-exploits/criacao-de-exploits-parte-3-estudo-de-caso-vulnserver-kstet-com-egghunter/
- https://www.corelan.be/index.php/2010/01/09/exploit-writing-tutorial-part-8-win32-egg-hunting/

Egghunters

- https://memn0ps.github.io/2020/04/01/Stack-Based-Buffer-Overflows-Egghunter-Part-3.html
- https://m0chan.github.io/2019/08/21/Win32-Buffer-Overflow-SEH.html
- https://philkeeble.com/exploitation/windows/Vulnserver-Walkthrough-Part-3/
- https://cr0wsplace.wordpress.com/2020/08/04/exploit-development-part-1-winamp-5-12-buffer-overflow-in-python-with-egghunters/
- https://medium.com/@rafaveira3/exploit-development-kolibri-v2-0-http-server-egg-hunter-example-1-5e435aa84879
- https://www.offensive-security.com/metasploit-unleashed/egghunter-mixin/
- https://shellcode.blog/Windows-Exploitation-Egg-hunting/
- https://xavibel.com/2019/06/26/exploit-development-vulnserver-kstet-method-1/

Egghunters

- https://h0mbre.github.io/Badchars_Egghunter_SEH_Exploit/
- https://www.rapid7.com/blog/post/2012/07/06/an-example-of-egghunting-to-exploit-cve-2012-0124/
- http://sh3llc0d3r.com/vulnserver-kstet-command-exploit-with-egghunter/
- https://www.abatchy.com/2017/05/skapes-egg-hunter-null-freelinux-x86
- https://securityimpact.net/2017/02/15/exploit-development-4-egg-hunting/
- https://mnorris.io/slae32/assignment_3/
- https://githubmemory.com/repo/freddiebarrsmith/Advanced-Windows-Exploit-Development-Practice

Shellcode from scratch

- https://vividmachines.com/shellcode/shellcode.html
- https://www.exploit-db.com/docs/english/21013-shellcoding-in-linux.pdf
- https://www.exploit-db.com/papers/13224
- https://0x00sec.org/t/linux-shellcoding-part-1-0/289
- https://sec4us.com.br/cheatsheet/shellcoding
- https://medium.com/purple-team/buffer-overflow-c36dd9f2be6f
- https://seedsecuritylabs.org/Labs_16.04/PDF/Shellcode.pdf
- https://marcosvalle.github.io/re/exploit/2018/10/20/windows-manual-shellcode-part1.html
- https://www.fuzzysecurity.com/tutorials/expDev/6.html
- https://github.com/lorenzoinvidia/Raw-Windows-Shellcode
- https://github.com/giovannyortegon/shellcode-x86_x64
- https://www.youtube.com/watch?v=u3COf_kJ8sk
- http://www.securitytube.net/video/7001
- https://phackt.com/slae-tcp-bind-shell

Shellcode from scratch

- https://github.com/anjelikasah/Shellcode-Development-Lab
- https://seedsecuritylabs.org/Labs_16.04/Software/Shellcode/
- https://www.youtube.com/watch?v=upjB4UU6e58
- https://www.youtube.com/watch?v=Z1gSZThlbWY
- https://securitycafe.ro/2015/10/30/introduction-to-windows-shellcode-development-part1/
- https://www.coresecurity.com/sites/default/files/private-files/publications/2016/05/TheShellcodeGeneration.pdf
- https://www.exploit-db.com/docs/english/13610-building-your-own-ud-shellcodes-part-1.pdf
- https://www.blackhat.com/presentations/bh-europe-09/Caillat/BlackHat-Europe-09-Caillat-Wishmaster-slides.pdf
- https://www.exploit-db.com/docs/english/13019-shell-code-for-beginners.pdf

Reverse Engineering

- https://www.youtube.com/watch?v=mwrhRP2PswA
- https://www.youtube.com/watch?v=f1wp6wza8ZI
- https://www.youtube.com/watch?v=puNkbSTQtXY
- https://github.com/tylerha97/awesome-reversing
- https://gitmemory.com/alphaSeclab/awesome-reverse-engineering
- https://repo.telematika.org/project/tylerha97_awesome-reversing/
- https://githubmemory.com/repo/0xT11/awesome-reversing
- https://github.com/mytechnotalent/Reverse-Engineering
- https://github.com/wtsxDev/reverse-engineering
- https://github.com/mentebinaria/retoolkit
- https://github.com/hax0rtahm1d/Reverse-Engineering
- https://github.com/NationalSecurityAgency/ghidra
- https://github.com/OpenToAllCTF/REsources

Stack overflows and DEP/ASLR bypass

- https://security.stackexchange.com/questions/147002/how-to-bypass-dep-and-aslr-at-the-same-time
- https://www.usenix.org/legacy/events/sec09/tech/slides/sotirov.pdf
- https://www.youtube.com/watch?v=Pht6y4p63SE
- https://codingvision.net/bypassing-aslr-dep-getting-shells-with-pwntools
- https://msrc-blog.microsoft.com/2010/12/08/on-the-effectiveness-of-dep-and-aslr/
- https://info.armis.com/rs/645-PDC-047/images/Armis-CDPwn-ASLR-Bypass-WP.pdf
- https://cwinfosec.org/Intro-ROP-DEP-Bypass/
- https://blog.securityevaluators.com/asuswrt-buffer-overflow-format-string-aslr-bypass-2bbf9736fe46
- https://github.com/FULLSHADE/OSCE/blob/master/README.md
- https://bananamafia.dev/post/binary-aslr-dep-32/
- https://www.corelan.be/index.php/search/aslr+bypass/
- https://www.exploit-db.com/docs/english/17914-bypassing-aslrdep.pdf

Stack overflows and DEP/ASLR bypass

- http://index-of.es/Failed-attack-techniques/DEP-ASLR%20bypass%20without%20ROP-JIT.pdf
- https://www.bordergate.co.uk/dep-aslr-bypass/
- https://www.codeproject.com/Articles/5163529/Bypassing-ASLR-and-DEP-Getting-Shells-with-pwntool
- https://mh4x0f.github.io/exploration/2014/10/14/Bypass-Protect-winndows-Linux-metasploit-DEP.html
- https://www.youtube.com/watch?v=Lxjw9OhF6w4
- https://github.com/cryptolok/ASLRay
- https://tekwizz123.blogspot.com/2014/02/bypassing-aslr-and-dep-on-windows-7.html
- http://ith4cker.com/content/uploadfile/201601/716b1451824309.pdf?hufovg=tk4ek3
- https://www.ccn-cert.cni.es/pdf/documentos-publicos/xi-jornadas-stic-ccn-cert/2575-m11-06-rockandropeando/file.html
- http://index-of.co.uk/Reversing-Exploiting/Defeating%20DEP%20and%20ASLR.pdf
- https://www.digitalwhisper.co.il/files/Zines/0x0F/DW15-3-Win7DEPnASLR.pdf
- https://www.blackhat.com/presentations/bh-usa-08/Sotirov_Dowd/bh08-sotirov-dowd.pdf

Stack overflows and DEP/ASLR bypass

- https://i.blackhat.com/briefings/asia/2018/asia-18-Marco-return-to-csu-a-new-method-to-bypass-the-64-bit-Linux-ASLR-wp.pdf
- https://www.blackhat.com/presentations/bh-europe-09/Fritsch/Blackhat-Europe-2009-Fritsch-Bypassing-aslr-slides.pdf
- https://www.blackhat.com/presentations/bh-europe-09/Fritsch/Blackhat-Europe-2009-Fritsch-Bypassing-aslr-whitepaper.pdf
- https://www.blackhat.com/docs/asia-16/materials/asia-16-Marco-Gisbert-Exploiting-Linux-And-PaX-ASLRS-Weaknesses-On-32-And-64-Bit-Systems.pdf
- https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Pan-Scavenger-Misuse-Error-Handling-Leading-To-QEMU-KVM-Escape.pdf
- https://www.blackhat.com/docs/us-15/materials/us-15-Yason-Understanding-The-Attack-Surface-And-Attack-Resilience-Of-Project-Spartans-New-EdgeHTML-Rendering-Engine-wp.pdf
- https://www.blackhat.com/presentations/bh-usa-08/Sotirov_Dowd/bh08-sotirov-dowd-slides.pdf

ROP and ROP Decoders

- https://www.exploit-db.com/docs/english/28479-return-oriented-programming-(rop-ftw).pdf
- http://www.cse.psu.edu/~trj1/cse598-f11/slides/BH_US_08_Shacham_Return_Oriented_Programming.pdf
- https://people.eecs.berkeley.edu/~daw/papers/rop-usenix14.pdf
- https://www.hackthezone.com/wp-content/uploads/2019/11/Weaponizing-ROP-with-PwNtools-ANDREI-GRIGORAS-18oct2019HTZ.pdf
- https://www.cs.bu.edu/~goldbe/teaching/HW55813/rop.pdf
- https://scholars.unh.edu/cgi/viewcontent.cgi?article=2376&context=thesis
- https://www.doc.ic.ac.uk/~livshits/classes/CO445H/reading/smashing-rop.pdf
- https://www.acsac.org/2020/workshops/laser/111-AutomaticExploitGeneration-Paper.pdf
- https://www.blackhat.com/presentations/bh-usa-08/Shacham/BH_US_08_Shacham_Return_Oriented_Programming.pdf