EXPLOIT DEVELOPMENT BY JOAS

Reverse Engineering

- https://github.com/tylerha97/awesome-reversing
- https://www.mentebinaria.com.br/forums/topic/212-awesome-lists/
- https://awesomeopensource.com/projects/reverse-engineering
- https://gitmemory.com/alphaSeclab/awesome-reverse-engineering
- https://repo.telematika.org/project/tylerha97_awesome-reversing/
- https://repo.telematika.org/project/tylerha97_awesome-reversing/
- https://github.com/mytechnotalent/Reverse-Engineering
- https://github.com/wtsxDev/reverse-engineering
- https://github.com/mentebinaria/retoolkit
- https://github.com/0xZ0F/Z0FCourse_ReverseEngineering
- https://github.com/hax0rtahm1d/Reverse-Engineering

Shellcode Development

- https://hackerculture.com.br/?p=1059
- https://www.helviojunior.com.br/it/security/criacao-de-exploits/como-realizar-stack-buffer-overflow/
- https://www.youtube.com/watch?v=rvZsvSH2pXo
- https://www.youtube.com/watch?v=qSjxR8tfokg
- https://www.youtube.com/watch?v=Xvh8FkczNUc
- https://github.com/anjelikasah/Shellcode-Development-Lab
- https://github.com/topics/shellcode-development
- https://github.com/topics/shellcode-development?l=c
- https://github.com/topics/shellcode-development?l=python
- https://github.com/wetw0rk/Sickle
- https://medium.com/mii-cybersec/tagged/shellcode
- http://www.alanwar10.com/tag/shellcode/archive?source=topics_v2-------------------------------------
- https://posts.specterops.io/going-4-a-run-eb263838b944
- https://www.tenouk.com/Bufferoverflowc/Bufferoverflow5.html
- https://seedsecuritylabs.org/Labs_20.04/Files/Shellcode/Shellcode.pdf
- https://h0mbre.github.io/Win32_Reverse_Shellcode/
- https://blog.usejournal.com/red-team-diary-entry-3-custom-malware-development-establish-a-shell-through-the-browser-bed97c6398a5
- https://towardsdatascience.com/20-best-vs-code-extensions-for-productive-web-development-in-2020-95bf904ceb69
- https://www.exploit-db.com/docs/english/13610-building-your-own-ud-shellcodes-part-1.pdf
- https://www.coresecurity.com/sites/default/files/private-files/publications/2016/05/TheShellcodeGeneration.pdf
- https://www.blackhat.com/presentations/bh-europe-09/Caillat/BlackHat-Europe-09-Caillat-Wishmaster-slides.pdf
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3153488
- https://www.iaik.tugraz.at/wp-content/uploads/2020/07/04-exploits.pdf
- https://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-aitel.pdf
- https://www.blackhat.com/presentations/bh-europe-09/Caillat/BlackHat-Europe-09-Caillat-Wishmaster-whitepaper.pdf
- https://www.blackhat.com/presentations/bh-asia-03/bh-asia-03-chong.pdf
- https://www.blackhat.com/presentations/win-usa-04/bh-win-04-aitel.pdf

Awesome Buffer Overflow

- https://github.com/gh0x0st/Buffer_Overflow
- https://github.com/johnjhacking/Buffer-Overflow-Guide
- https://github.com/joshua17sc/Buffer-Overflows
- https://github.com/justinsteven/dostackbufferoverflowgood
- https://github.com/V1n1v131r4/OSCP-Buffer-Overflow
- https://github.com/the-c0d3r/buffer-overflow
- https://gist.github.com/apolloclark/6cffb33f179cc9162d0a
- https://github.com/sradley/overflow
- https://github.com/hyperreality/OSCP-Buffer-Overflow-in-30-minutes
- https://github.com/art049/simple-buffer-overflow-server
- https://github.com/npapernot/buffer-overflow-attack
- https://github.com/EmreOvunc/Buffer-Overflow-PoC
- https://github.com/freddiebarrsmith/Buffer-Overflow-Exploit-Development-Practice
- https://github.com/kevinkong91/buffer-overflow-exploit
- https://github.com/helviojunior/live_bufferoverflow
- https://github.com/Andy53/BufferOverflowExample
- https://github.com/hackutk/overflow-example

The exploit development lab environment

- https://www.youtube.com/watch?v=7PMw9GIb8Zs
- https://www.anitian.com/a-study-in-exploit-development-part-1-setup-and-proof-of-concept/
- http://zeroknights.com/getting-started-exploit-lab/
- https://blog.exploitlab.net/
- https://www.shogunlab.com/blog/2017/08/11/zdzg-windows-exploit-0.html
- https://github.com/CyberSecurityUP/Buffer-Overflow-Labs
- https://iratoon.medium.com/exploit-development-windows-part-2-4b0d17fe8d40
- https://theguly.github.io/2020/02/eLearnSecurity-eXploit-Development-Student/
- https://epi052.gitlab.io/notes-to-self/blog/2020-05-13-osce-exam-practice-part-one/

Application x64 work in 32 Bits

- https://www.howtogeek.com/194119/why-are-most-programs-still-32-bit-on-a-64-bit-version-of-windows/#:~:text=The%2032%2Dbit%20program%20can,don't%20worry%20about%20it.
- https://www.youtube.com/watch?v=LCGhg-RfDDE
- https://www.youtube.com/watch?v=Kyoyorh-YGQ
- https://docs.microsoft.com/en-us/windows/win32/winprog64/running-32-bit-applications
- https://medium.com/codixlab/what-happens-when-a-32-bit-program-runs-on-a-64-bit-machine-c231ac3ddb2f
- https://appuals.com/how-to-install-32-bit-software-on-64-bit-windows/
- https://www.alphr.com/make-32-bit-apps-work-64-bit-windows/

Sysinternals

- http://index-of.co.uk/Malware/WINDOWS%20SYSINTERNALS%20ADMINISTRATOR'S%20REFERENCE.pdf
- https://ptgmedia.pearsoncmg.com/images/9780735684447/samplepages/9780735684447.pdf
- https://neprisstore.blob.core.windows.net/sessiondocs/doc_c67d889c-039a-4977-8266-3e025c1408e3.pdf
- https://docs.microsoft.com/en-us/sysinternals/downloads/
- https://www.ebooks.com/en-us/book/95824138/troubleshooting-with-the-windows-sysinternals-tools/mark-e-russinovich/
- https://repo.zenk-security.com/Linux%20et%20systemes%20d.exploitations/Windows%20Internals%20Part%201_6th%20Edition.pdf
- http://index-of.es/Linux/Other/Windows%20Internals%20Part%202_6th%20Edition.pdf

Assembly

- https://www.ic.unicamp.br/~pannain/mc404/aulas/pdfs/Art%20Of%20Intel%20x86%20Assembly.pdf
- https://www.ic.unicamp.br/~ducatte/mc404/2009/docs/beginner_avr.pdf
- https://www.tutorialspoint.com/assembly_programming/assembly_tutorial.pdf
- http://www.ece.utep.edu/courses/web3376/Notes_files/ee3376-assembly.pdf
- http://www.egr.unlv.edu/~ed/assembly64.pdf
- https://docs.oracle.com/cd/E19457-01/801-7045/801-7045.pdf
- http://www.staroceans.org/kernel-and-driver/The.Art.of.Assembly.Language.2nd.Edition.pdf
- http://index-of.co.uk/Assembly/Assembly_Language_Step_by_Step_en.pdf
- https://www.cs.princeton.edu/courses/archive/spr18/cos217/lectures/13_Assembly1.pdf
- http://arantxa.ii.uam.es/~gdrivera/sed/docs/ARMBook.pdf
- https://en.wikipedia.org/wiki/X86_assembly_language

Windows Memory Management

- https://www.cs.sjtu.edu.cn/~kzhu/cs490/9/9_MemMan.pdf
- http://mit.bme.hu/~micskeiz/opre/files/eng/03-operating-systems-windows-memory-management.pdf
- https://madoc.bib.uni-mannheim.de/3148/1/InternalsOfWindowsMemoryMangement2.pdf
- https://www.intellectualheaven.com/Articles/WinMM.pdf
- http://efreidoc.fr/L3/Operating%20System/Cours/PDF/2010-11/2010-11.cours.13.memory-management-in-windows-and-linux.op.pdf
- https://www.dc.fi.udc.es/~so-grado/2020-21/Temas/SO-Memoria.pdf
- https://warwick.ac.uk/fac/sci/physics/research/condensedmatt/imr_cdt/students/david_goodwin/teaching/operating_systems/l12_realos.pdf
- http://www.tfzr.uns.ac.rs/Content/files/0/Lab08.pdf
- https://www2.latech.edu/~box/os/ch08.pdf
- https://dcc.ufrj.br/~valeriab/SO-VirtualMemory.pdf
- http://www.cs.umsl.edu/~sanjiv/classes/cs4760/lectures/memory.pdf
- http://www.ifsc.usp.br/~lattice/oldlattice/mod9.1.pdf

Buffer Overflow Concept

- https://www.imperva.com/learn/application-security/buffer-overflow/
- https://economictimes.indiatimes.com/definition/buffer-overflow
- https://owasp.org/www-community/vulnerabilities/Buffer_Overflow
- https://www.veracode.com/security/buffer-overflow
- https://searchsecurity.techtarget.com/definition/buffer-overflow
- https://avinetworks.com/glossary/buffer-overflow/
- https://www.cloudflare.com/pt-br/learning/security/threats/buffer-overflow/
- https://journals.indexcopernicus.com/api/file/viewByFileId/134652.pdf
- https://www.sans.org/reading-room/whitepapers/threats/paper/481
- https://www.ajrsp.com/en/Archive/issue-19/The%20Buffer%20Overflow%20Attack.pdf
- https://web.ecs.syr.edu/~wedu/Teaching/CompSec/LectureNotes_New/Buffer_Overflow.pdf
- https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture21.pdf
- http://technologeeks.com/Courses/BO.pdf
- https://www.cs.utexas.edu/~shmat/courses/cs380s_fall09/cowan.pdf
- http://www.dcc.fc.up.pt/~edrdo/QSES1819/lectures/qses-08-buffer-overflows_part2.pdf
- https://www.youtube.com/watch?v=zeX2ZLzgPOA
- https://www.youtube.com/watch?v=HrFZ6ry6roQ
- https://www.youtube.com/watch?v=59_gjX2HxyA
- https://www.youtube.com/watch?v=VX27nq6EcjI&t=2s
- https://www.youtube.com/watch?v=1S0aBV-Waeo
- https://www.youtube.com/watch?v=1X2JGF_9JGM
- https://www.youtube.com/watch?v=2ZZPwwXOH08
- https://www.youtube.com/watch?v=GAcmECMYAkY

Labs Reverse Engineering and Exploit Development

- https://github.com/renyxa/re-lab
- https://github.com/OpenToAllCTF/REsources
- https://github.com/jsoverson/workshop-reverse-engineering
- https://github.com/rustymagnet3000/Reverse-Engineering-C-challenges
- https://github.com/AravGarg/Bomb-Lab
- https://github.com/momalab/ICSREF
- https://infosecwriteups.com/linux-reverse-engineering-ctfs-for-beginners-4cf03ff2cfb4
- https://ctf101.org/reverse-engineering/overview/
- https://www.hackthebox.eu/
- vulnhub.com
- https://github.com/VictorAlonsoCM/CTFs
- https://github.com/apsdehal/awesome-ctf
- https://github.com/j00ru/ctf-tasks
- https://github.com/JustBeYou/ctfs
- https://github.com/teambi0s/secREtary
- https://www.youtube.com/watch?v=Hvfwtffpnho
- https://www.youtube.com/watch?v=ou_4msS5ZW8
- https://github.com/firmianay/Life-long-Learner/blob/master/SEED-labs/buffer-overflow-vulnerability-lab.md
- https://github.com/Jeffery-Liu/Buffer-Overflow-Vulnerability-Lab
- https://github.com/wadejason/Buffer-Overflow-Vulnerability-Lab
- https://github.com/wadejason/Buffer-Overflow-Vulnerability-Lab/blob/master/stack.c
- https://github.com/cranelab/exploit-development
- https://github.com/0xdutra/exploitation-labs
- https://github.com/globocom/secDevLabs
- https://github.com/wtsxDev/Exploit-Development/blob/master/README.md
- https://github.com/topics/exploit-development
- https://github.com/VoidSec/Exploit-Development
- https://github.com/midnightslacker/exploit_training

Buffer Overflow OSCP

- https://www.youtube.com/watch?v=4rUN1F6_Mhk
- https://www.youtube.com/watch?v=_EYoYiSInSA
- https://assume-breach.medium.com/oscp-prep-buffer-overflows-made-super-easy-with-the-brainpan-1-vm-e5ccaf7d3f0c
- https://github.com/V1n1v131r4/OSCP-Buffer-Overflow
- https://www.udemy.com/course/practical-buffer-overflows-for-oscp/
- https://thelistsec.com/2020/06/23/oscp-like-buffer-overflow-walkthrough/
- https://steflan-security.com/complete-guide-to-stack-buffer-overflow-oscp/
- https://www.trenchesofit.com/2020/09/12/oscp-buffer-overflow-write-up/
- https://www.youtube.com/watch?v=RmpNQQwhDms
- https://www.youtube.com/watch?v=8So2XCateS8
- https://www.tripwire.com/state-of-security/security-data-protection/passing-offensive-security-certified-professional-exam-oscp/
- https://github.com/3isenHeiM/OSCP-BoF
- https://github.com/xMilkPowderx/OSCP/blob/master/Buffer%20Overflow.md
- https://github.com/fredisanmar/OSCP-Buffer-Overflow

My LinkedIn and E-books

- https://www.linkedin.com/in/joas-antonio-dos-santos
- https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU

Awesome Exploit Development

- https://github.com/FabioBaroni/awesome-exploit-development
- https://github.com/secfigo/Awesome-Fuzzing
- https://github.com/gold1029/awesome-exploit-development
- https://github.com/dineshkumarc987/awesome_exploit_development
- https://github.com/roninAPT/awesome-exploit-development
- https://awesomeopensource.com/projects/exploit-development
- https://0x00sec.org/t/material-for-learning-exploit-development/1727
- https://sec4us.com.br/cheatsheet/

Exploit Development and Buffer Overflow

- https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/
- https://www.corelan.be/index.php/articles/
- https://ccsecuritytraining.com/training/exploit-development-bootcamp/
- https://medium.com/stolabs/tagged/exploit-development
- https://iratoon.medium.com/exploit-development-windows-part-3-4c420652c840
- https://infosecwriteups.com/tagged/exploit-development
- https://www.coalfire.com/the-coalfire-blog/january-2020/the-basics-of-exploit-development-1
- https://www.crowdstrike.com/blog/state-of-exploit-development-part-1/
- https://tcm-sec.com/category/exploit-development/
- https://www.helviojunior.com.br/
- https://betterprogramming.pub/an-introduction-to-buffer-overflow-vulnerability-760f23c21ebb
- https://blog.devgenius.io/buffer-overflow-tutorial-part3-98ab394073e3
- https://blog.offensive-shield.com/lets-talk-about-buffer-overflow-54764101030b
- https://academy.hackthebox.eu/course/preview/stack-based-buffer-overflows-on-linux-x86
- https://i.blackhat.com/us-18/Thu-August-9/us-18-Rikansrud-Mainframe-[zOS]-Reverse-Engineering-and-Exploit-Development.pdf
- https://i.blackhat.com/USA-19/Thursday/us-19-Hawkes-Project-Zero-Five-Years-Of-Make-0day-Hard.pdf
- https://www.blackhat.com/docs/us-17/thursday/us-17-Ablon-Bug-Collisions-Meet-Government-Vulnerability-Disclosure-Zero-Days-Thousands-Of-Nights-RAND.pdf
- https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-sutton.pdf
- https://www.blackhat.com/docs/us-16/materials/us-16-Oh-The-Art-of-Reverse-Engineering-Flash-Exploits.pdf
- https://blackhat.com/us-14/video/hands-on-exploit-development.html
- https://www.youtube.com/watch?v=opBLBYAR8tU

System Architecture

- http://web.mit.edu/6.976/www/notes/Notes1.pdf
- https://www.incose.org/docs/default-source/wasatch-chapter-documents/the-big-happy-family-of-architectures-r0.pdf?sfvrsn=613696c6_2
- https://www.gaudisite.nl/SystemArchitectureProcessPaper.pdf
- https://mitocw.ups.edu.ec/courses/aeronautics-and-astronautics/16-842-fundamentals-of-systems-engineering-fall-2015/lecture-notes/MIT16_842F15_Ses4_Con_Syn.pdf
- https://www.regjeringen.no/contentassets/0de9ab36c5244c3ba9cbafa74c1876a2/securityarchitecture-ecountingofpvotesv1_1.pdf
- https://www.kean.edu/~gchang/tech2920/http___professor.wiley.com_CGI-BIN_JSMPROXY_DOCUMENTDIRECTORDEV+DOCUMENTID&0471715425+DOCUMENTSUBID&1+PRFVALNAME&pdfs_ch02.pdf
- https://incoseuk.org/Documents/zGuides/Z8_System_Architecture.pdf
- https://hal.archives-ouvertes.fr/hal-01407372/document
- https://en.wikipedia.org/wiki/Systems_architecture#:~:text=A%20system%20architecture%20is%20the,and%20behaviors%20of%20the%20system.
- https://thenewstack.io/primer-understanding-software-and-system-architecture/
- https://www.sebokwiki.org/wiki/System_Architecture