Reverse Engineering – Content Study #1

Joas Antonio

https://www.linkedin.com/in/joas-antonio-dos-santos

X86 Architecture

- https://tc.gts3.org/cs6265/tut/tut01-warmup1.html
- https://cs.lmu.edu/~ray/notes/x86overview/
- https://mulcas.com/what-is-x86-architecture/
- https://www.seeedstudio.com/blog/2020/02/24/what-is-x86-architecture-and-its-difference-between-x64/
- https://www.csie.ntu.edu.tw/~cyy/courses/assembly/10fall/lectures/handouts/lec12_x86arch.pdf
- https://www.mindshare.com/files/ebooks/x86%20Instruction%20Set%20Architecture.pdf
- https://csit.ust.edu.sd/files/2018/10/lec2-COAsm2018.pdf

X64 Architecture

- https://www.intel.com/content/dam/develop/external/us/en/documents/introduction-to-x64-assembly-181178.pdf
- https://cs.brown.edu/courses/cs033/docs/guides/x64_cheatsheet.pdf
- https://www.ic.unicamp.br/~rodolfo/Cursos/mo401/2s2005/Trabalho/041438-x86.pdf
- https://www.cs.princeton.edu/courses/archive/spr18/cos217/reading/x86-64-1.pdf
- https://phoenixnap.com/kb/x64-vs-x86
- https://www.cs.princeton.edu/courses/archive/spr18/cos217/reading/x86-64-1.pdf
- https://courses.cs.washington.edu/courses/csep590/06au/projects/history-64-bit.pdf
- https://www.blackhat.com/docs/us-15/materials/us-15-Herath-These-Are-Not-Your-Grand-Daddys-CPU-Performance-Counters-CPU-Hardware-Performance-Counters-For-Security.pdf

ARM and CISC

- https://indico.ictp.it/event/a01127/session/7/contribution/6/material/0/0.pdf
- https://developer.arm.com/documentation/den0013/d/Introduction-to-Assembly-Language/Comparison-with-other-assembly-languages
- https://www.extremetech.com/computing/323245-risc-vs-cisc-why-its-the-wrong-lens-to-compare-modern-x86-arm-cpus
- https://prezi.com/rxq9scmjbijh/cisc-x-risc-x-arm/
- https://www.microcontrollertips.com/risc-v-vs-arm-vs-x86-whats-the-difference/
- https://www.makeuseof.com/risc-vs-arm-what-is-the-difference/

Reverse Engineering in Kernel

- https://www.kernel.org/doc/ols/2002/ols2002-pages-191-196.pdf
- https://dslab.epfl.ch/pubs/reveng.pdf
- https://www.blackhat.com/presentations/bh-usa-07/Lindsay/Presentation/bh-usa-07-lindsay.pdf
- https://aclanthology.org/D09-1012.pdf
- https://syssec.kaist.ac.kr/~yongdaek/courses/ee515/2014/Slides/12-3-1.pdf
- https://users.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_chipounov.pdf
- http://www.cse.hut.fi/fi/opinnot/T-110.6220/2015_Reverse_Engineering_Malware_AND_Software_Security/luennot-files/t1106220.pdf
- https://recon.cx/2015/slides/recon2015-20-steven-vittitoe-Reverse-Engineering-Windows-AFD-sys.pdf
- https://sambaxp.org/fileadmin/user_upload/sambaxp2021-slides/Aptel_Reverse_engineering_the_windows_SMB_server.pdf

Debugging

- https://www.techtarget.com/searchsoftwarequality/definition/debugging
- https://0xinfection.github.io/reversing/pages/part-15-debugging-hello-world.html
- https://www.geeksforgeeks.org/software-engineering-debugging/
- https://www.tutorialspoint.com/what-is-a-debugger-program
- https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/getting-started-with-windows-debugging
- https://www.elprocus.com/what-is-debugging-types-techniques-in-embedded-systems/
- https://questhenkart.medium.com/debugging-the-power-of-reverse-engineering-d659214da3a
- https://www.youtube.com/watch?v=PTCKXTPUeqY&ab_channel=AppleProgramming (Introduction Debugging)

Sysinternals and Windows API

- https://www.apriorit.com/dev-blog/364-how-to-reverse-engineer-software-windows-in-a-right-way
- https://cybergeeks.tech/reverse-engineering-psexec-for-fun-and-knowledge/
- https://infosecwriteups.com/getting-started-with-reverse-engineering-609a42e86cc1
- http://www.ahsanworld.com/debugging-reverse-engineering-windows-applications/
- https://int0x33.medium.com/day-59-windows-api-for-pentesting-part-1-178c6ba280cb
- https://mentebinaria.gitbook.io/engenharia-reversa/windows-api
- https://github.com/microsoft/Windows-classic-samples

Memory Management

- https://www.techtarget.com/whatis/definition/memory-management
- https://www.geeksforgeeks.org/memory-management-in-operating-system/
- https://www.dca.fee.unicamp.br/~marco/cursos/ea879_11_2/referencias/so_cap04.pdf
- https://www.ifsc.usp.br/~lattice/oldlattice/mod9.1.pdf
- https://sites.ualberta.ca/~smartynk/Resources/CMPUT%20379/beck%20notes/memory.pdf
- https://cseweb.ucsd.edu/classes/su09/cse120/lectures/Lecture7.pdf
- https://people.umass.edu/tongping/teaching/cs3733/lecture-07-MemoryManagement.pdf
- https://www.utc.edu/sites/default/files/2021-04/2800-lecture8-memeory-management.pdf
- https://www.cs.princeton.edu/courses/archive/spr19/cos217/lectures/20_DynamicMemory.pdf
- https://research.cs.wisc.edu/areas/os/Qual/papers/mach-memory.pdf
- https://www.inf.ed.ac.uk/teaching/courses/os/slides/09-memory18.pdf

C Language

- https://www.geeksforgeeks.org/c-language-set-1-introduction/
- https://www.sitepoint.com/fundamentals-of-c/
- https://www.guru99.com/c-programming-language.html
- https://microchipdeveloper.com/tls2101:start
- https://skills.microchip.com/fundamentals-of-the-c-programming-language
- https://www.ijirt.org/master/publishedpaper/IJIRT142685_PAPER.pdf
- https://www.javatpoint.com/c-programming-language-tutorial
- https://www.w3resource.com/c-programming-exercises/
- https://codeforwin.org/c-programming-examples-exercises-solutions-beginners
- https://www.tutorialspoint.com/cprogramming/c_memory_management.htm
- https://www.codecademy.com/resources/docs/c/memory-management
- https://www.geeksforgeeks.org/memory-layout-of-c-program/
- https://github.com/oz123/awesome-c

Assembly Language

- https://github.com/Maijin/awesome-asm
- https://www.investopedia.com/terms/a/assembly-language.asp
- https://www.ic.unicamp.br/~pannain/mc404/aulas/pdfs/Art%20Of%20Intel%20x86%20Assembly.pdf
- https://sectigostore.com/blog/what-is-assembly-language/
- https://cs.lmu.edu/~ray/notes/x86assembly/
- https://bcastudyguide.com/unit-6-assembly-language-2/
- https://flint.cs.yale.edu/cs421/papers/x86-asm/asm.html
- https://go.dev/doc/asm
- https://kb.iu.edu/d/aewk
- http://www.cburch.com/books/arm/

Disassemblers

- https://www.apriorit.com/dev-blog/366-software-reverse-engineering-tools
- https://resources.infosecinstitute.com/topic/kali-linux-top-8-tools-for-reverse-engineering/
- https://www.alchemy.com/dapps/capstone-disassembler
- https://www.techopedia.com/definition/6860/disassembler
- https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/disassembly-window