

eLearnsecurity
Certified eXploit
Development
Preparation by Joas

LinkedIn

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

Ret2libc

<https://www.programmersought.com/article/2475157601/>

<https://www.youtube.com/watch?v=cLLR-ZeTss>

<https://www.youtube.com/watch?v=HjiiY8AXi8>

https://github.com/nnamon/linux-exploitation-course/blob/master/lessons/7_bypass_nx_ret2libc/lessonplan.md

<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/babys-first-nxplusaslr-bypass/>

<https://pdfcoffee.com/lab10-linux-nx-bypass-pdf-free.html>

<https://pdfcoffee.com/lab11-linux-x64-nx-bypass-pdf-free.html>

<https://sploitfun.wordpress.com/2015/05/08/bypassing-nx-bit-using-return-to-libc/>

<https://nandynarwhals.org/ret2libc-namedpipes/>

<https://petruknisme.com/2019/07/09/smashthetux-chapter-0x00-basic-buffer-overflow-ret2libc/>

Linux Stack Smashing

<https://stackoverflow.com/questions/1345670/stack-smashing-detected>

<https://pt.stackoverflow.com/questions/305310/erro-stack-smashing-detected-em-c>

<https://www.educative.io/presso/what-is-the-stack-smashing-detected-unknown-terminated>

<https://www.vivaolinux.com.br/topico/C-C++/-stack-smashing-detected-unknown-terminated>

<https://wiki.gentoo.org/wiki/Stack-smashing-debugging-guide>

<https://www.exploit-db.com/papers/24085>

<https://www.thegeekstuff.com/2013/02/stack-smashing-attacks-gcc/>

<https://access.redhat.com/blogs/766093/posts/3548631>

<https://www.programmersought.com/article/40995878204/>

<https://www.sans.org/blog/stack-canaries-gingerly-sidestepping-the-cage/>

<http://cileseerx.lst.psu.edu/viewdoc/download?doi=10.1.1.135.2.164&rep=rep1&type=pdf>

<https://devconnected.com/how-to-show-hidden-files-on-linux/#:-text=The%20easiest%20way%20to%20show%E2%80%9D%20option%20for%20%E2%80%9Ccall%E2%80%9D.&text=For%20example%2C%20in%20order%20to%20show%20hidden%20files%20on%20Linux.>

<https://serverfault.com/questions/2817/hidden-features-of-linux>

https://www.youtube.com/watch?v=AO4_M-18B5U

Reviews

<https://osandamalth.com/2020/06/25/my-journey-into-ecx-d-learnsecurity-certified-exploit-developer/>

<https://medium.com/kminthein/ecx-d-review-813960dfc07b>

<https://itnext.io/xds-v1-learnsecurity-course-review-cda5bb12f95b>

https://www.reddit.com/r/eLearnSecurity/comments/wh1kt1/review_of_ecxd_and_ecre_learnsecurity_courses/

<https://mayaseven.com/learnsecurity-certified-exploit-developer-ecx-d-review/>

C Language

<https://www.youtube.com/watch?v=QpAhX-gsHMs>

<https://www.youtube.com/watch?v=oZeezrNHxVo>

<https://www.edx.org/learn/c-programming>

<https://www.udemy.com/course/the-complete-c-programming/>

<https://medium.com/javarevisited/9-free-c-programming-courses-for-beginners-2486dff74065>

<https://www.java67.com/2020/07/5-free-courses-to-learn-c-programming.html>

<https://cppinstitute.org/free-c-and-c-courses>

<https://github.com/trending/c>

<https://github.com/topics/c-programming>

<https://github.com/PacktPublishing/Learn-C-Programming>

<https://github.com/gouravthakur39/beginners-C-program-examples>

<https://github.com/Heatwave/The-C-Programming-Language-2nd-Edition>

<https://github.com/roa1ienza/C-Programming>

<https://www.thegeekstuff.com/2013/06/buffer-overflow/>

<https://www.talain.com/blog/2019/04/04/exploring-buffer-overflows-in-c-part-two-the-exploit/>

<https://www.youtube.com/watch?v=yIGATjX3nqc>

<https://www.youtube.com/watch?v=CQ6pGrXY1Us>

<https://www.youtube.com/watch?v=chJ4UkzcKwU>

<https://www.ired.team/offensive-security/code-injection-process-injection/writing-and-compiling-shellcode-in-c>

<https://adrianicitu.com/2015/08/31/introduction-to-linux-shellcode-writing-part-1/>

<https://www.programmersought.com/article/186042228/>

<https://security.stackexchange.com/questions/176495/executing-a-msfvenom-shellcode-in-c-program>

<https://bufferoverflows.net/developing-custom-shellcode-x64-linux/>

<https://0x00sec.org/t/linux-shellcoding-part-1-0/289>

Shellcode Development

<https://www.youtube.com/watch?v=tID6qwl9IN4>

https://www.youtube.com/watch?v=0_-WtzSL9ZY

https://www.youtube.com/watch?v=74Y_w2_MgpY

<https://www.youtube.com/watch?v=Xvh8FkcZNUc>

<https://www.youtube.com/watch?v=QEKjHunT5Cs>

<https://www.youtube.com/watch?v=nZsvSH2pXo>

https://www.youtube.com/watch?v=6MnCC3CIT_tc

<https://www.youtube.com/watch?v=CMJqeDqghws>

<https://www.youtube.com/watch?v=DZKjduIqak>

<https://www.pluralsight.com/courses/exploit-development-execution-metasploit-framework>

<https://www.youtube.com/watch?v=oS2078H57qU>

Assembly Language

<https://github.com/topics/assembly-language>

<https://github.com/Apress/modern-x86-assembly-language-programming>

<https://github.com/0xAX/asm>

<https://github.com/Nxumalo/Assembly-Code>

<https://github.com/topics/assembly-programming>

<https://github.com/topics/assembly-x86>

<https://assembly-area55.github.io/nasm>

<https://www.cin.ufpe.br/~eaa3/Arquivos/Assembly/Assembly%20x86%20NASM.pdf>

<https://www.youtube.com/watch?v=W8UTCqWb2eQ>

<https://www.youtube.com/watch?v=JjnJrQla3k>

<https://github.com/7h3w4lk3r/x86-nasm>

<https://rudamoura.com/x86.html>

<https://www.youtube.com/watch?v=wLXIWKUwPsS>

<https://www.youtube.com/watch?v=HgEGAAyDABA>

<https://www.youtube.com/watch?v=dKjZyJv00I>

<https://www.cs.virginia.edu/~evans/cs216/guides/x86.html>

<https://software.intel.com/content/www/us/en/develop/articles/introduction-to-x64-assembly.html>

<https://www.youtube.com/watch?v=rxsBgHsrVpI>

https://cs.brown.edu/courses/cs033/docs/guides/x64_cheatsheet.pdf

<https://docs.microsoft.com/pt-br/cpp/assembly/masm/masm-for-x64-m64-exe?view=msvc-160>

Awesome Exploit Development

<https://github.com/CyberSecurityUP/AWESOME-EXPLOIT-DEVELOPMENT>

<https://git.plocienik.info/barszczuch/hakowanie/master/2/awesome-exploit-development.pdf>

<https://github.com/FabioBaroni/awesome-exploit-development>

<https://www.offensive-security.com/category/vulndev/>

<https://onehack.us/t/awesome-exploit-development-massive-resources-collection/189926>

<https://0x00sec.org/t/material-for-learning-exploit-development/1727>

<https://github.com/wetw0rk/Exploit-Development>

<https://github.com/SkyBulk/exploit-development>

<https://github.com/jpraveen/exploit-development>

<https://github.com/freddiebarrrsmith/Advanced-Windows-Exploit-Development-Practice>

<https://github.com/freddiebarrrsmith/Buffer-Overflow-Exploit-Development-Practice/blob/master/README.md>

<https://github.com/RackunSec/Exploit-Development>

<https://github.com/tagnullide/Exploit-Development>

<https://github.com/so87/Exploit-Development-and-Pentesting>

https://github.com/gh0x0st/Buffer_Overflow

<https://github.com/johnhacking/Buffer-Overflow-Guide>

<https://github.com/Trib3r3x/Pentest-Cheatsheets/blob/master/exploits/buffer-overflows.rst>

<https://github.com/joshua17sc/Buffer-Overflows>

https://github.com/helviojunior/live_bufferoverflow

<https://github.com/shashijangra22/Buffer-Overflow-Attack>

<https://github.com/Andy53/BufferOverflowExample>

<https://github.com/npapernot/buffer-overflow-attack>

<https://github.com/freddiebarrrsmith/Buffer-Overflow-Exploit-Development-Practice>

What is Shellcode

<https://pt.wikipedia.org/wiki/Shellcode>

<https://searchsecurity.techtarget.com/answer/What-is-the-relationship-between-shellcode-and-exploit-code>

<https://www.firewalls.com/blog/security-terms/shellcode/>

<https://www.yourdictionary.com/shellcode>

<https://translate.google.com/translate?hl=pt-BR&sl=en&u=https://www.easytechjunkie.com/what-is-a-shellcode.htm&prev=search&pto=au>

<https://www.exploit-db.com/docs/english/13019-shell-code-for-beginners.pdf>

<https://www.pcmag.com/encyclopedia/term/shellcode>

<https://security.stackexchange.com/questions/167579/what-is-the-difference-between-a-payload-and-shellcode>

<https://pentest.blog/tag/shellcode/>

Windows SEH

<https://medium.datadriveninvestor.com/exploiting-millennium-mp3-studio-2-0-with-shellcode-payload-82f815bc809b>

<https://pdfcoffee.com/lab4-windows-seh-overflow-mp3-pdf-free.html>

<https://github.com/killvkx/Windows-Exploit-Development-practice/blob/master/Millennium-MP3-Studio-seh-calc.py>

<https://www.exploit-db.com/exploits/9298>

<https://packetstormsecurity.com/files/90291/MP3-Studio-1.0-Buffer-Overflow.html>

<https://vulners.com/exploitdb/EDB-ID:9286>

<https://www.exploit-db.com/exploits/42155>

<https://www.onsecurity.io/blog/buffer-overflow-easy-chat-server-31/>

<https://pdfcoffee.com/lab5-windows-seh-overflow-easychat-pdf-free.html>

https://www.rapid7.com/db/modules/exploit/windows/http/easychatserver_seh/

<https://www.youtube.com/watch?v=WyY5kOCFjo>

<https://www.doyler.net/security-not-included/easy-chat-server-exploit>

<https://www.digitalmunition.me/seh-buffer-overflow-in-easy-chat-server-1/>

<https://sec4us.com.br/treinamentos/desenvolvimento-de-exploits-32-bits/>

Fuzzing

<https://www.udemy.com/course/hands-on-exploit-development-advanced/>

<https://www.exploit-db.com/docs/english/18924-uncovering-zero-days-and-advanced-fuzzing-slides.pdf>

<https://qwarecademy.com/cyber-security-training/exploit-development>

https://www.youtube.com/watch?v=3Kc_joW2YgM

<https://www.youtube.com/watch?v=ItYE6kEasM>

<https://www.youtube.com/watch?v=50qk4Pm5ic>

<https://www.offensive-security.com/metasploit-unleashed/writing-simple-fuzzer/>

<https://www.hackers-arise.com/post/2017/06/21/exploit-development-part-3-finding-vulnerabilities-by-fuzzing-with-spike>

<https://www.deepcode.ca/index.php/2017/03/20/software-exploit-development-fuzzing-with-ai/>

<https://resources.infosecinstitute.com/topic/intro-to-fuzzing/>

<https://github.com/guilhermeferreira/spikepp>

<https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-atel-spike.ppt>

ASLR Bypass

<https://www.youtube.com/watch?v=mPbHroMVepM>

<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://github.com/cryptolok/ASLRay>

<http://hmarco.org/cyber-security/attacks/bypass64bitsASLRLinux/offset2lib-attack.html>

<https://www.hacking.land/2017/10/aslr-lin-elf-x32-and-x64-aslr.html?m=1>

<https://codingvision.net/bypassing-aslr-dep-getting-shells-with-pwntools>

<https://www.youtube.com/watch?v=Pht6y4p63SE>

<https://www.youtube.com/watch?v=gxU3e7Gbc-M>

Shellcode Resource

<https://github.com/alphaSecLab/shellcode-resources>

<https://drive.google.com/drive/folders/12Mwq6KE2HJDUwN2CzHEGwzyW87YunkU>

<https://medium.com/@coturnix97/exploit-exercises-protostar-stack-5-963731ff4b71>

<https://github.com/helviojunior/shellcodetester>

<https://github.com/hellman/shtest>

<https://github.com/NullByteGtK/Shellcode-Tester>

<https://github.com/NytorRST/ShellcodeCompiler>

<https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/>

<https://github.com/shayanzare/obj2shellcode>

<https://reverseengineering.stackexchange.com/questions/15925/how-can-i-export-only-the-opcodes-from-objdump-or-any-other-program>

<https://www.commandlinefu.com/commands/view/6051/get-all-shellcode-on-binary-file-from-objdump>

<https://daemoniolabs.wordpress.com/2012/03/17/transformar-saida-do-objdump-para-shellcode/>

<https://stackoverflow.com/questions/52369994/get-shellcode-from-object-dump-the-right-way>

http://www.tecland.com.br/palestras/01/01-construindo_shellcodes_por_victor.pdf

<https://www.exploit-db.com/docs/english/21013-shellcoding-in-linux.pdf>

Shellcode x32

<http://shell-storm.org/shellcode/files/shellcode-827.php>

<http://shell-storm.org/shellcode/files/shellcode-811.php>

<https://www.exploit-db.com/exploits/44321>

<https://vulners.com/zdt/1337DAY-ID-27788>

<https://github.com/MrEcco/lzw-shellcode>

<https://www.offensive-security.com/metasploit-unleashed/alphanumeric-shellcode/>

https://github.com/SkyBulk/exploit-development/blob/master/codes/easy_rm_2.7_3_700_cal_esp_jump_esp.py

<https://www.exploit-db.com/exploits/42428>

<https://reverseengineering.stackexchange.com/questions/25672/reason-of-padding-in-exploit>

<https://packetstormsecurity.com/files/156478/Windows-x86-Null-Free-WinExec-Calcul-Shellcode.html>

<https://br-n.github.io/OSCE-Prep-Vulnserver-KSTET-Win32-API/>

<https://www.vividmachines.com/shellcode/shellcode.html>

<https://www.oreilly.com/library/view/metasploit-for-beginners/9781788295970/2717da98-f9c0-4901-e43e-6e4bac4841d.xhtml>

<https://snowscan.io/custom-encoder/>

https://owasp.org/www-pdf-archive/HackPhasars_Rooting_Your_Internals_..Michele_Orru.pdf

<https://forum.hackthebox.eu/discussion/4593/shellcode-crashes-after-made-connection-to-netcat-in-stack-base-buffer-overflow-tutorial>

<https://www.ired.team/offensive-security/code-injection-process-injection/executing-shellcode-with-createlfiber>

<https://www.codeproject.com/Articles/5304605-Creating-Shellcode-From-any-Code-Using-Visual-Studio>

<https://systemoverlord.com/2014/06/05/minimal-x86-64-shellcode-for-binsh/>

<https://github.com/PacktPublishing/Penetration-Testing-with-Shellcode>

Shellcode x64

<https://github.com/MrEcco/lzw-shellcode>

<https://www.exploit-db.com/exploits/42179>

<https://www.exploit-db.com/exploits/46907>

<http://shell-storm.org/shellcode/files/shellcode-806.php>

<https://bufferoverflows.net/developing-custom-shellcode-x64-linux/>

<https://packetstormsecurity.com/files/162210/Linux-x64-execve-bin-sh-Shellcode.html>

<https://zeromux0x.blogspot.com/2014/12/there-are-many-versions-of-execve.html>

<https://gist.github.com/matterpreter/03e2bd3cf8b26d570443b494e73bbea>

<https://ciberseguridad.blog/como-automatizar-la-extraccion-del-shellcode-de-cobalt-strike/>

<https://es/052.gtiab.io/notes-to-self/blog/2018-08-04-x64-linux-metasploit-execve-bin-sh-shellcode-analysis/>

<https://wajid-nawazish.medium.com/developing-custom-shellcode-in-x64-57172a85d77>

https://owasp.org/www-pdf-archive/Introduction_to_shellcode_development.pdf

<https://www.tosone.cn/ExploitDatabase/index.htm?type=shellcode>

<https://mytrosecurity.com/2019/06/30/writing-shellcodes-for-windows-x64/>

<https://sec4us.com.br/cheatsheet/shellcoding>

<https://hackerulture.com.br/?p=1059>

<https://www.youtube.com/watch?v=rML5DWgIfIM>

<https://silviavali.github.io/blog/2019-05-01-blog-SLAES1/>

<https://www.programmersought.com/article/23716896022/>

[https://www.pwnwiki.org/index.php/Linux/x64_._execve_._cat_./etc/shadow_._Shellcode_\(66_bytes\)](https://www.pwnwiki.org/index.php/Linux/x64_._execve_._cat_./etc/shadow_._Shellcode_(66_bytes))

<https://docs.pwntools.com/en/stable/shellcraft/amd64.html>

<https://crypto.stanford.edu/~blynn/rop/>

<https://mmquant.net/analysis-of-metasploit-linux-x64-exec-shellcode/>

<https://systemoverlord.com/2014/06/05/minimal-x86-64-shellcode-for-binsh/>