BUFFER OVERFLOW FOR BEGINNERS by JOAS

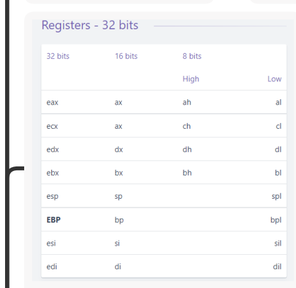
Introduction and Concept

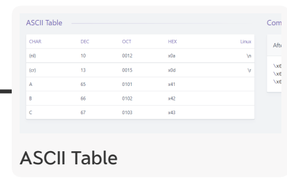
- https://www.triaxiomsecurity.com/introduction-to-buffer-overflow-attacks/
- https://betterprogramming.pub/an-introduction-to-buffer-overflow-vulnerability-760f23c21ebb
- https://www.youtube.com/watch?v=qSnPayW6F7U&ab_channel=TheCyberMentor
- https://www.youtube.com/watch?v=IiOQ-XD3uDw&ab_channel=DionTraining
- https://www.youtube.com/watch?v=54ivE1VZk8I&ab_channel=BittenTech
- https://www.youtube.com/watch?v=4rUN1F6_Mhk&ab_channel=NakerahNetwork
- https://d0nut.medium.com/week-13-introduction-to-buffer-overflows-5f15c0d5b5c1
- https://www.imperva.com/learn/application-security/buffer-overflow/
- https://ijournals.in/wp-content/uploads/2017/07/14.3425-Nilesh.compressed.pdf
- https://searchsecurity.techtarget.com/definition/buffer-overflow
- https://medium.com/techloop/understanding-buffer-overflow-vulnerability-85ac22ec8cd3
- https://www.sans.org/white-papers/481/
- https://www.hackingarticles.in/a-beginners-guide-to-buffer-overflow/
- https://www.coengoedegebure.com/buffer-overflow-attacks-explained/

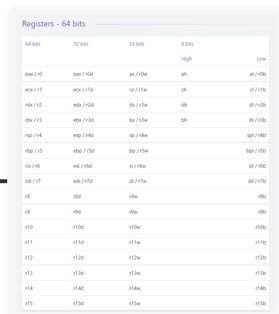
Practice Laboratory

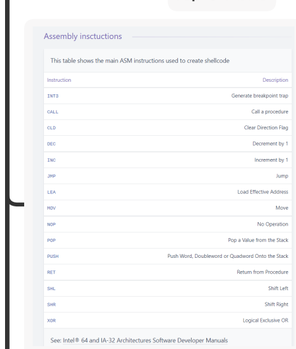
- https://mrmoddom.github.io/ctf/walkthrough-Stack-Overflows-for-Beginners-1/
- https://www.vulnhub.com/entry/stack-overflows-for-beginners-101,290/
- https://medium.com/@iwhoam047/stack-overflows-for-beginners-1-41acf75d230
- https://medium.com/dsc-sastra-deemed-to-be-university/buffer-overflow-vulnserver-4951a4318966
- https://z3r0th.medium.com/a-simple-buffer-overflow-using-vulnserver-86b011eb673b
- https://www.youtube.com/watch?v=yJF0YPd8lDw&ab_channel=JohnHammond
- https://www.youtube.com/watch?v=OOkU7to0Ty4&ab_channel=JesseK
- https://www.youtube.com/watch?v=dCWgoSlni6s&ab_channel=NobodyAtall
- https://www.youtube.com/watch?v=k7EOkalfSKw&ab_channel=timthetinkerer
- https://www.youtube.com/watch?v=qyoALEIAJqo&ab_channel=drprventura
- https://princerohit8800.medium.com/buffer-overflow-exploiting-slmail-email-server-f90b27459911
- https://esseum.com/win-32-buffer-overflow-walkthrough-exploiting-slmail-5-5/
- https://github.com/CyberSecurityUP/Buffer-Overflow-Labs
- https://medium.com/@rafaelrenovaci/exploit-to-pcman-ftp-server-2-0-7-remote-buffer-overflow-cffafb8faddb
- https://medium.com/@mtucunduva98/buffer-overflow-pcman-ftp-server-2-0-7-e143ff3473c
- https://www.hebunilhanli.com/wonderland/bof-101/
- http://www.computersecuritystudent.com/SECURITY_TOOLS/BUFFER_OVERFLOW/WINDOWS_APPS/lesson1/index.html
- https://www.youtube.com/watch?v=h5N0aOZjXDE&ab_channel=raulcpop

Fundamentals Assembly (Sec4US)

- Register is a small space used by CPU to store information.
- Register Description — sp 16 bits — ESP 32 bits — rsp 64 bits
- 

  Register 32 Bits
- IP - Instruction Pointer — Points to next instruction to be executed
  - Register Description
  - ip 16 bits
  - EIP 32 bits
  - rip 64 bits
- Badchars
  - 

    ASCII Table
- https://sec4us.com.br/cheatsheet/bufferoverflow-windows — https://sec4us.com.br/cheatsheet/bufferoverflow-egghunting
- 

  Register 64 Bits
- SP Stacker
  - sp 16 bits
  - esp 32 bits
  - rsp 64 bits
- 

  Assembly Instructions
- https://en.wikipedia.org/wiki/X86_instruction_listings
- https://flint.cs.yale.edu/cs421/papers/x86-asm/asm.html
- https://software.intel.com/content/www/us/en/develop/articles/introduction-to-x64-assembly.html
- https://cs.brown.edu/courses/cs033/docs/guides/x64_cheatsheet.pdf
- https://www.felixcloutier.com/x86/