GDB Cheatsheet

Thursday, September 14, 2023 5:37 PM

GDB / PEDA

Wednesday, January 12, 2022 12:14 PM

- Useful Commands
  - disass $FUNCTION
    - dump assembly instructions for the function
  - break $FUNCTION
    - break *$ADDR
    - pauses execution when function is reached
    - info break
      - list all breaks
    - del $num
      - delete a break
    - break main+39
      - set at a breakpoint + 39 offset
  - print $VAR
    - prints contents of a register or other variable
    - print eip
  - x/$LENi$ADDR
    - examine memory locations
    - x/i $eip
      - examine EIP
    - x/2i $eip
      - look at the next two instructions
    - x/wx $ebp+4
      - look at instruction of ebp + offset4
    - x/20gx $rsp
      - giant register for 64bit
  - info
    - print contents of state registers and other vars
    - info registers
  - c | continue
    - continues execution after break
  - si
    - step one instruction / step *into*
    - ni (step over)
  - run program with a script/command as an argument
    - (gdb) run `python -c 'print("AAAA")'`
  - run program that prompts you for input
    - (gdb) run < <(python -c 'print("AAAA")')
  - run shell commands
    - shell python -c 'print(0x260)'
- gdb (--nx) ./$EXEC
  - --nx disables PEDA/plugins
- PEDA
  - (in gdb) help peda
  - xrefs $FUNC
    - show where in the program there are references to $FUNC
  - pattern_create 300
    - same as msf_pattern_create

  - pattern_offset $VALUE
    - same as msf_pattern_offset
  - jmpcall
    - looks at jmp & call instructions
  - run < <(python -c 'print("A"*612 + "B"*4)')
  - Look for a specific ROP chain:
    - ropsearch "pop rdi; ret"
  - Look for calls & references to system library
    - xrefs sys