Session 5

GDB and Buffer Overflows

GDB basics

- gdb [executable-file]
- disas [function name or memory address]
- break [LOCATION] [thread THREADNUM] [if CONDITION]
- info breakpoints
- delete breakpoints [breakpoint_number]
- run
- continue
- stepi
- nexti
- set

GDB basics (cont)

- x/nfu [address]
    - n: How many units to print
    - f: Format character
        - a Pointer
        - c Read as integer, print as character
        - d Integer, signed decimal
        - f Floating point number
        - o Integer, print as octal
        - s Treat as C string (read all succesive memory addresses until null character and print as characters)
        - t Integer, print as binary (t="two")
        - u Integer, unsigned decimal
        - x Integer, print as hexadecimal
    - u: Unit
        - b: Byte
        - h: Half-word (2 bytes)
        - w: Word (4 bytes)
        - g: Giant word (8 bytes)
        - i: Instruction (read n assembly instructions from the specified memory address)

GDB basics (cont)

- p/f [what]
  - f: Formant character
    - a Pointer
    - c Read as integer, print as character
    - d Integer, signed decimal
    - f Floating point number
    - o Integer, print as octal
    - s Treat as C string (read all succesive memory addresses until null character and print as characters)
    - t Integer, print as binary (t="two")
    - u Integer, unsigned decimal
    - x Integer, print as hexadecimal
    - i Instruction (read n assembly instructions from the specified memory address)

PEDA

- pdis
- stepi
- nexti
- context [reg|code|stack|all]
- telescope
- patch [address] “string”

Stack

- Stack frames

- Local variables

- Calling functions

- Buffer Overflows