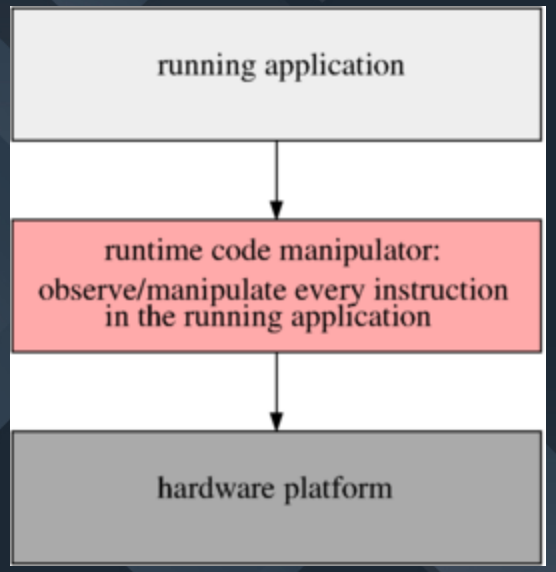
Reverse engineering with ease 😎

DynamoRIO tool to trace function calls based on .pdb symbols

DBI? Never heard of it 🤔

https://dynamorio.org/overview.html#sec_intro



What? 👀

- Let's say you wanna find cmd.exe's text parser for fuzzing purposes
- You have .pdb for free
- Where you start?
  - Search functions by name ➡️ apply breakpoint ➡️ look around

    -- or --
  - Use presented tool 🎯

```
...
 -> BatLoop
     -> OpenPosBat
         -> Copen_Work
         <- Copen_Work (0x0000000000000003)
     <- OpenPosBat (0x0000000000000003)
     -> Parser
         -> _intrinsic_setjmp
         <- _intrinsic_setjmp (0x0000000000000000)
         -> GeToken
             -> Lex
                 -> _intrinsic_setjmp
                 <- _intrinsic_setjmp (0x0000000000000000)
                 -> FillBuf
                     -> ResetCtrlC
                     <- ResetCtrlC (0x0000000000000000)
                     -> ResetCtrlC
                     <- ResetCtrlC (0x0000000000000000)
                     -> ReadBufFromFile
                         -> IsMBTWCConversionTypeFlagsSupported
                         <- IsMBTWCConversionTypeFlagsSupported (0x0000000000000001)
                     <- ReadBufFromFile (0x000000000000001f)
                     -> FileIsDevice
                     <- FileIsDevice (0x0000000000000000)
                     -> SubVar
                         -> FreeStr
                         <- FreeStr (0x0000000000000001)
                     <- SubVar (0x0000000000000001)
                 <- FillBuf (0x00007ff627e949f2)
             <- Lex (0x0000000000004000)
         <- GeToken (0x0000000000004000)
         -> ParseS0
             -> BinaryOperator
                 -> ParseS1
                     -> BinaryOperator
                         -> ParseS2
                             -> BinaryOperator
                                 -> ParseS3
                                     -> BinaryOperator
                                         -> ParseS4
                                             -> ParseRedir
                                             ...
```

Parsing .bat/.cmd file

- ReadBufFromFile()
- BatLoop()
- Parser()
- PraseS...() & BinaryOperator()

Live Demo 😍

Thanks 

Reach out @expend20