Beginner's Introduction to Reverse Engineering

Nancy Snoke

Overview

- Reverse Engineering Tools
- IDA Pro
  - Basics
  - Hello World Example
  - Simple Password Example
  - Not So Simple Password Example
- Takeaway points
- Practice Ideas

Reverse Engineering Tools

- Tools on Backtrack Linux
  - edb-debugger
  - flasm
  - gdb.py
  - install ida-pro free
  - ollydbg
  - strace.py

Reverse Engineering Tools Continued

- .Net C# or VB
  - ILSpy
- Java
  - Java Decompiler
- Other Unix Tools
  - nm
  - ldd
  - Objdump
- Other Windows Tools
  - dumpbin

IDA Pro

- Why use IDA Pro?
  - Runs on multiple platforms
  - There is a free version
  - Extensible
  - Works with a variety of file types
  - Interactive Debugger as well as dissembler

IDA Pro Basics

- Load The File
  - Drag the file, and IDA autodetects
  - Select file type and binary through the menus
- Navigation
  - Use the space bar to switch between graphical and linear view
  - Press esc to go back
  - Mouse over a name or address for summary information
  - Double click on a name or address to follow it
  - Highlight a hex value and right click to see its value in different forms
  - Add a comment by selecting the line and hitting semi colon
  - Rename a function by highlighting, right clicking, and selecting rename
  - For help with the assembly go to Options -> General and turn on Auto Comments

- Reverse Engineer Hello World Example

IDA Pro "Hello World" Example

- For loops
- While loops
- Function calls
- If Then Structures

IDA Pro Understanding Assembly

- Find main
- Recognize assembly patterns
- Recognize calls to standard libraries
- Recognize function calls and parameters passed
- Recognize complex structures
- Use IDA dynamically to see how the code is executed

Reverse Engineering Strategy

Type	8 bit	16 bit	32 bit
Instruction Pointer			EIP
Stack Pointer		SP	ESP
Base Pointer		BP	EBP
Destination Index		DI	EDI
Source Index		SI	ESI
Accumulator	AL, AH	AX	EAX
Base Index	BL, BH	BX	EBX
Count	CL, CH	CX	ECX
Data	DL, DH	DX	EDX

Register List

- Reverse Engineer Simple Password Example

IDA Pro
Simple Password Example

- Reverse Engineer the Not So Simple Password

IDA Pro
Not So Simple Password

Expand Your Knowledge

- Practice
  - Go through my simple examples
  - Find examples in online courses / tutorials
  - Find other examples in CTFs
- Read interesting sections of the IDA Pro Book
- Continue Practicing

Questions