What is Reverse Engineering (RE)?

Refresher

Know your tools
A basic RE algorithm

Introduction to Reverse Engineering Software
Fine-granularity class topics covered

Frank Poz
CC BY AT licensed
hosted at OpenSecurityTraining.info

Click on green nodes to jump to that topic in the videos

Debugging
Day 1
review 1
Analyzing
Day 1
review 2
C++
About the next class
Other languages
Day 2
review

Applying the RE algorithm to the bomb lab

Phase 1
Labs
Outline
Setting a bomb lab
answers file

Phase 2
introduction

Phase 3
introduction

Phase 4
introduction

Phase 5
introduction

Phase 6
introduction 1

IDA Pro
Intro x86
PE Files
Algorithms
Data Types
& Structures

What kind of questions can you answer with RE?
For loops
Array accesses
Multiple/variable argument functions

Phase 2 walkthrough
Phase 3 walkthrough
Recursion
Phase 4 walkthrough
String decoding
Phase 5 walkthrough
Nested loops
Structures
Phase 6 introduction 2

Structs example:

Defining structs in IDA
Applying structs to assembly in IDA
Applying structs to memory in IDA

Phase 6 walkthrough 1
Loop collapsing in IDA
Identifying a linked list in memory
Defining the struct in IDA
Applying a struct to a memory block in IDA

Phase 6 walkthrough 2

Java
The "this" pointer and virtual function tables ("vtables")
Object member access
Constructors and Destructors
Example:
class_0.ex_
Example:
class_1.ex_
Inheritance
Example:
class_2.ex_

Understanding the first nested loops
Understanding the next set of nested loops
Understanding the last loop
Analyzing the pseudo-code

Linked lists
Reminder:
What is "dl" (or al or bl or cl)?

Why use a debugger?
Types of breakpoints
IDA as a debugger
Single stepping
Conditional jumps in IDA
EFLAGS register in IDA
Passing command line arguments to a debugged program in IDA

Stack frame explanation