Mid-Term Exam Notes

CSE4830 : Reverse Engineering

Mid-Term Exam Topics

The mid-term exam includes all topics up to and including the Reversing Networking Lesson. You should feel comfortable with the following topics.

1. Explain the purpose of each register for a Linux System Call. Given a small snippet of assembly, describe the system call being made and the value of each parameter (Intro to x64 Assembly Lesson, Introduction to x64 Assembly Reading)

2. Dynamically analyze a program in a debugger (setting breakpoints, stepping through execution, examining registers/memory). Given a small snippet of code, be able to identify a place to insert a break-point to reveal a textitflag. (Reversing Machine Code Part 1 Lesson)

3. Describe the impact of compile time options (symbol stripping, static/dynamic linking) on a binary. (Reversing Machine Code Part 2 Lesson)

4. Perform static analysis of a binary using a disassembler or decompiler to produce a LLIL/HLIL representation of a binary. (Reversing Machine Code Part 2 Lesson, Binary Ninja Blog & API)

5. Given a symbol stripped binary, identify the address of the main() function. (Reversing Machine Code Part 2 Lesson, Live Overflow Video)

6. Describe the purpose of ELF sections, including the .ini, .fini, .bss, .data, .rodata, .plt, and .got.plt (Portable Formats Specification 1.1, Elf Executable File Format Lesson)

7. Write a script/plugin to assist in static analysis of binaries (Scripting Decompiler Sample Code, String Decryption Blog Post, Binary Ninja Blogs)

8. Describe how opaque predicates are used to obfuscate binaries and remove opaque predicates. (Obfuscation Lesson, Tigress Obfuscator)

9. Describe the control flow flattening technique for obfuscation. (Obfuscation Lesson, Tigress Obfuscator)

10. Describe how an attacker mnight leveraging ptrace() to prevent dynamically analyzing a binary. Given a binary with anti-debugging technique using a call to ptrace, remove the anti-debugging functionality by patching the binary (Anti-Reverse Engineering Lesson, Linux Journal Article, Hiding Calls to Ptrace Blog Post)

11. Describe the purpose of networking wrapper functions (bind, listen, accept, connect, send & receive). Given a binary with networking, describe the address and port the binary is listening on or connecting to (Reversing Networking Lesson, Linux manpages)