REVERSE ENGINEERING 101

HIMANSHU KHOKHAR

AGENDA

- Intro to Reverse Engineering
- The tools – disassembler, debuggers and decompilers
- Reversing on Linux
- Break
- Reversing on Windows

INTRODUCTION TO REVERSE ENGINEERING

REVERSE ENGINEERING

- Noun - The reproduction of another manufacturer's product following detailed examination of its construction or composition.
- Wikipedia – "*Reverse engineering*, also called back *engineering*, is the process by which a man-made object is deconstructed to reveal its designs, architecture, or to extract knowledge from the object; similar to scientific research, the only difference being that scientific research is about a natural phenomenon."

TOOLS OF THE TRADE

- **Disassembler** – "A **disassembler** is a computer program that translates machine language into assembly language—the inverse operation to that of an assembler. A **disassembler** differs from a decompiler, which targets a high-level language rather than an assembly language."
- **Debugger** – "A **debugger** or **debugging tool** is a computer program that is used to test and debug other programs (the "target" program). "
- **Decompiler** – "A **decompiler** is a computer program that takes an executable file as input, and attempts to create a high level source file which can be recompiled successfully. It is therefore the opposite of a compiler, which takes a source file and makes an executable."
- All stolen from Wiki ;)

REVERSING ON LINUX

TOOLS OF THE TRADE

- objdump
- gdb
- DDD
- radare2
- Cutter (GUI for radare2)
- IDA Pro
- Hopper
- Binary Ninja

DEBUGGING WITH GDB

TARGET – IOLI CRACKMES

INTRODUCTION TO RADARE2 FRAMEWORK

RADARE2

- “r2 is a rewrite from scratch of radare in order to provide a set of libraries and tools to work with binary files. Radare project started as a forensics tool, a scriptable commandline hexadecimal editor able to open disk files, but later support for analyzing binaries, disassembling code, debugging programs, attaching to remote gdb servers, ..” - https://github.com/radare/radare2
- Super powerful and supports ton of architectures, file formats, OS, and has bindings for several programming languages.
- Has a built-in package manager.
- Can be extended by writing own plugins, or just use bindings to automate tasks with your fav programming lang ☺

CAPABILITES

- Architectures currently supported - Supported architectures - i386, x86-64, ARM, MIPS, PowerPC, SPARC, RISC-V, SH, m68k, AVR, XAP, System Z, XCore, CR16, HPPA, ARC, Blackfin, Z80, H8/300, V810, V850, CRIS, XAP, PIC, LM32, 8051, 6502, i4004, i8080, Propeller, Tricore, Chip8 LH5801, T8200, GameBoy, SNES, MSP430, Xtensa, NIOS II, Dalvik, WebAssembly, MSIL, EBC, TMS320 (c54x, c55x, c55+, c66), Hexagon, Brainfuck, Malbolge, DCPU16
- File formats support - ELF, Mach-O, Fatmach-O, PE, PE+, MZ, COFF, OMF, TE, XBE, BIOS/UEFI, Dyldcache, DEX, ART, CGC, Java class, Android boot image, Plan9 executable, ZIMG, MBN/SBL bootloader, ELF coredump, MDMP (Windows minidump), WASM (WebAssembly binary), Commodore VICE emulator, Game Boy (Advance), Nintendo DS ROMs and Nintendo 3DS FIRMs, various filesystems.
- You can use radare2 on - Windows (since XP), GNU/Linux, OS X, [Net|Free|Open]BSD, Android, iOS, OSX, QNX, Solaris, Haiku, FirefoxOS.

REVERSING WITH RADARE2

IOLI-CRACKME

BREAK

REVERSING ON WINDOWS

TOOLS OF THE TRADE

- Immunity Debugger
- Olly Debugger
- x64dbg
- Windbg
- IDA Pro
- radare2
- Cutter (radare2 GUI)

USING CUTTER

CRACKMES

INTRODUCTION TO IDA PRO

THANK YOU ☺