

# Game Hacking with Rust

# Target Audience

- You should know how to program
- Systems Programming basics

# You need to download:

- [AssaultCube](#)
- [Rust](#)
- [VSCode](#) with Rust Analyzer extension

# Source Code

Available here:

<https://github.com/not-matthias/game-hacking-workshop>

or

<https://shorturl.at/jmqrV>

# About Rust

- Types: `i16` vs `u16`
- Functions: `fn foo(bar: u32) -> i16 {}`
- Variables: `let mut temp = 42;`
- Run with: `cargo r` or `cargo run`

# What is a pointer?

- Points to a memory location
- 64 Bit Process => 64 Bit pointers
- 32 Bit Process => 32 Bit pointers

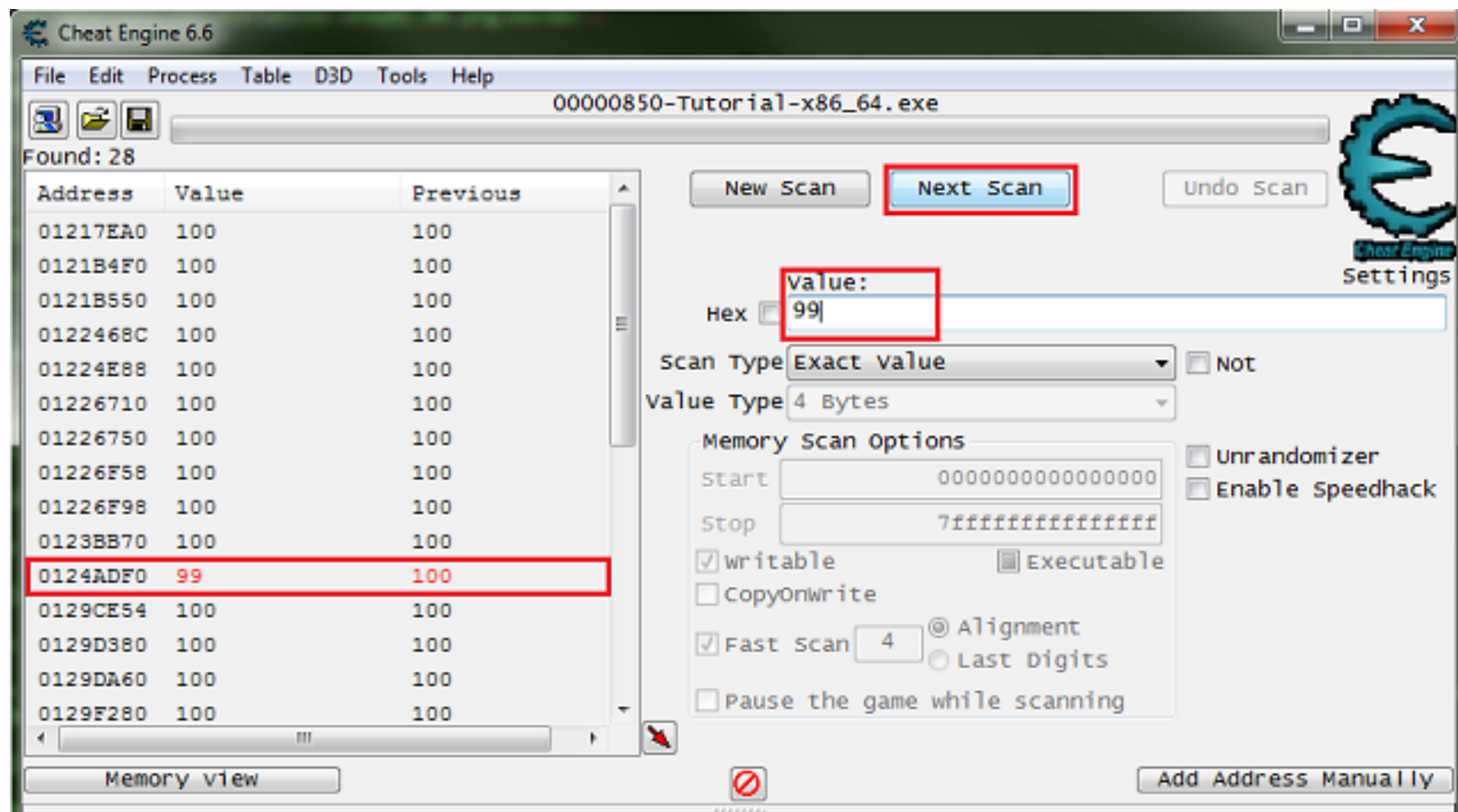
**Let's get started**

**And this is just the start...**



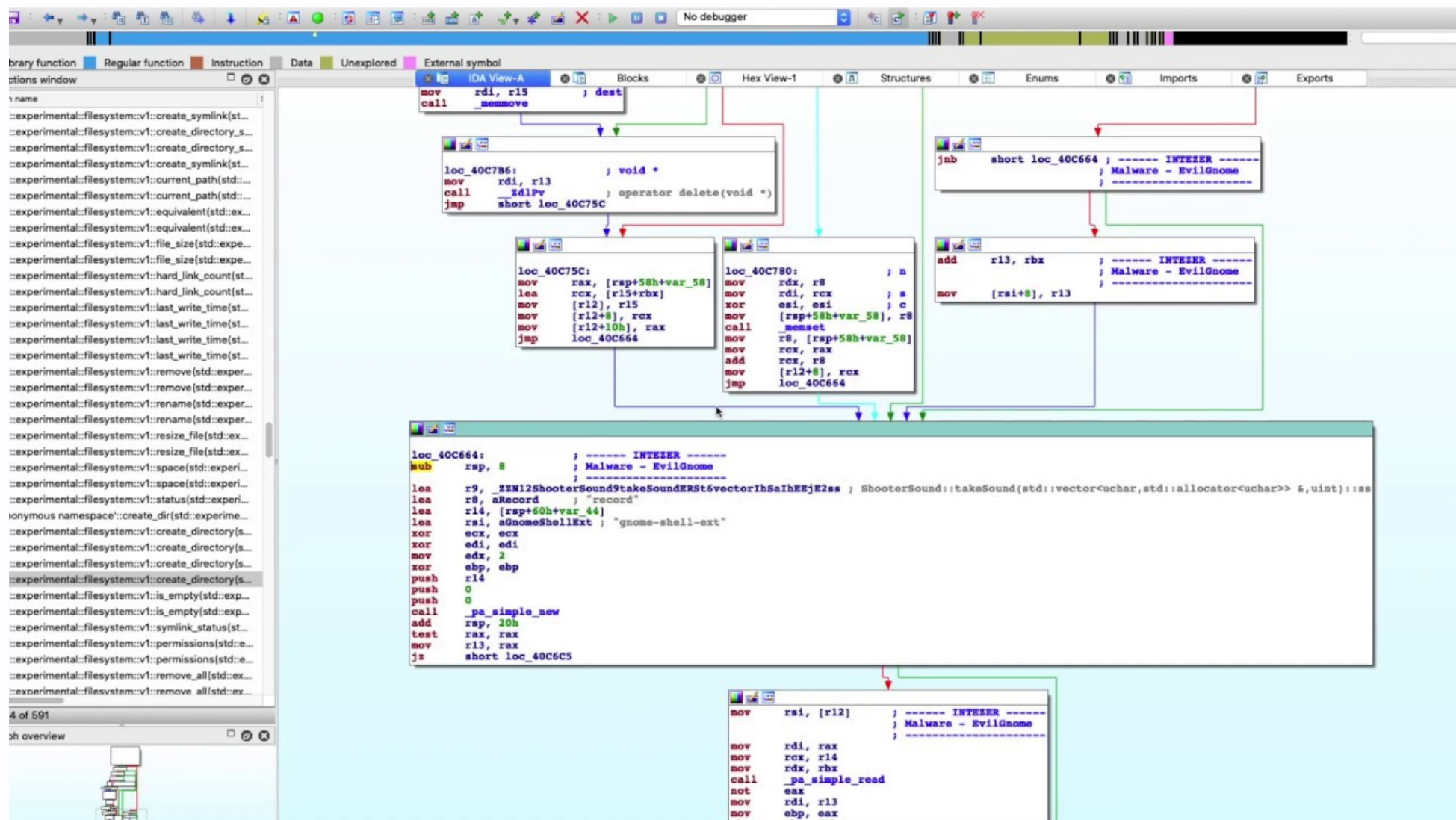
# Useful tools

# Cheat Engine





# IDA



x64dbg.exe - PID: 4054 - Module: x64dbg.exe - Thread: Main Thread 4080 - x64dbg

File View Debug Trace Plugins Favourites Options Help Jul 1 2018

CPU Graph Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source Threads Snowman Handles Trace Log

00007FF6880423D8 CC int3  
00007FF6880423DC sub rsp,38 crtexe.c:372  
00007FF6880423E0 lea rcx,qword ptr ds:[<RTC\_Terminate>] crtexe.c:374  
00007FF6880423E7 E8 88FFFFFF call <x64dbg.atexit>  
00007FF6880423EC mov eax,dword ptr ds:[<\_newmode>] crtexe.c:384  
00007FF6880423F2 mov r9d,dword ptr ds:[<\_dowildcard>] crtexe.c:392  
00007FF6880423F9 mov dword ptr ds:[<startinfo>],eax  
00007FF6880423FF lea rax,qword ptr ds:[<startinfo>]  
00007FF688042406 lea r8,qword ptr ds:[<envp>]  
00007FF68804240D lea rdx,qword ptr ds:[<argv>] rdx:WinMainCRTStartup  
00007FF688042414 lea rcx,qword ptr ds:[<argc>]  
00007FF68804241B mov qword ptr ss:[rsp+20],rax  
00007FF688042420 call qword ptr ds:[<\_getmainargs>]  
00007FF688042426 mov dword ptr ds:[<argret>],eax  
00007FF68804242C test eax,eax crtexe.c:396  
00007FF68804242E jns x64dbg.7FF68804243A crtexe.c:397  
00007FF688042430 mov ecx,8 crtexe.c:400  
00007FF688042435 call <x64dbg.\_amsg\_exit>  
00007FF68804243A add rsp,38  
00007FF68804243E ret  
00007FF68804243F int3  
00007FF688042440 CC crtexe.c:456  
00007FF688042444 E8 83EC28 call <x64dbg.\_security\_init\_cookie> crtexe.c:463  
00007FF688042449 E8 83C428 add rsp,28 crtexe.c:466  
00007FF68804244D E9 02000000 jmp <x64dbg.\_tmainCRTStartup> crtexe.c:465  
00007FF688042452 CC int3  
00007FF688042453 CC int3  
00007FF688042454 E8 88C428 mov rax,rsp crtexe.c:473  
00007FF688042457 E8 895808 mov qword ptr ds:[rax+8],rbx rbx:WinMainCRTStartup  
00007FF68804245B E8 897010 mov qword ptr ds:[rax+10],rsi  
00007FF68804245F 57 push rdi  
00007FF688042460 E8 83EC30 sub rsp,30  
00007FF688042464 E8 8360F0 and qword ptr ds:[rax-10],0 crtexe.c:475

Hide FPU  
RAX 0000000000000000  
RBX 00007FF688042440 <x64dbg.WinMainCRTStartup>  
RCX 00007FF68797F000  
RDX 00007FF688042440 <x64dbg.WinMainCRTStartup>  
RBP 0000000000000000  
RSP 0000005F21E0F7D8  
RSI 00007FF68797F000  
RDI 00007FF68797F000  
R8 00007FF68797F000  
R9 0000000000000000  
R10 0000000000000000  
R11 0000000000000000  
R12 0000000000000000  
R13 0000000000000000  
R14 0000000000000000  
R15 0000000000000000  
RIP 00007FF688042440 <x64dbg.WinMainCRTStartup>  
RFLAGS 0000000000000244  
ZF 1 PF 1 AF 0  
OF 0 SF 0 DF 0  
CF 0 TF 0 IF 1  
LastError 0000000F (ERROR\_PROC\_NOT\_FOUND)  
LastStatus C0000139 (STATUS\_ENTRYPOINT\_NOT\_FOUND)

Default (x64 fastcall) 5 Unlocked  
1: rcx 00007FF68797F000  
2: rdx 00007FF688042440 <x64dbg.WinMainCRTStartup>  
3: r8 00007FF68797F000  
4: r9 0000000000000000

.text:00007FF6880423D9 x64dbg.exe:\$23D9 #17D9

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals

Address	Hex	ASCII
00007FFAF3011E0	90 AD 02 00 F0 AF 02 00 C0 B9 02 00 F0 B9 02 00	...ð...À...ð...
00007FFAF3011F0	90 BA 02 00 D0 BB 02 00 C0 BD 02 00 D0 C6 02 00	...ð...À...ð...
00007FFAF301200	20 C8 02 00 90 C9 02 00 E0 C9 02 00 A0 CE 02 00	...ð...À...ð...
00007FFAF301210	20 CF 02 00 A0 F0 02 00 C0 07 03 00 E0 08 03 00	...ð...À...ð...
00007FFAF301220	60 09 03 00 70 0C 03 00 90 0C 03 00 D0 56 03 00	...ð...À...ð...
00007FFAF301230	80 76 03 00 A0 76 03 00 10 8A 03 00 E0 A7 03 00	...ð...À...ð...
00007FFAF301240	50 A7 03 00 A0 AB 03 00 20 AD 03 00 50 AD 03 00	...ð...À...ð...
00007FFAF301250	40 B1 03 00 80 83 03 00 B0 84 03 00 10 B6 03 00	...ð...À...ð...
00007FFAF301260	70 B6 03 00 00 87 03 00 60 B9 03 00 10 BA 03 00	...ð...À...ð...
00007FFAF301270	A0 BF 03 00 20 C0 03 00 30 C5 03 00 D0 CF 03 00	...ð...À...ð...
00007FFAF301280	20 D3 03 00 F0 D7 03 00 F0 D9 03 00 D0 DC 03 00	...ð...À...ð...
00007FFAF301290	D0 DC 03 00 10 DF 03 00 60 DF 03 00 F0 E1 03 00	...ð...À...ð...

Command: Default

Paused The data has been copied to clipboard. Time Wasted Debugging: 7:03:49:07

x64Dbg

# More ideas

- Read enemy positions -> Radar or ESP
- Aimbot
- Movement Speed multiplier
- No Recoil / Spread

# Anticheats

- EasyAntiCheat
- Battleye
- Vanguard
- ...



# Binary Analysis

- Deobfuscation
- Devirtualization
- ...



# Recommended Resources

- [gamehacking.academy](https://gamehacking.academy)
- [unknowncheats.me](https://unknowncheats.me)
- [github.com/hax-rs](https://github.com/hax-rs)
- [/r/ReverseEngineering](https://r/reverseengineering)
- Discord Servers
  - [Rust RE](#)
  - [hax-rs](#)
  - [Reverse Engineering](#)