ODCS Cheatsheet - December 28, 2022

Dynamic Analysis - GDB/PWNGDB

b *addr	set a software breakpoint at address **addr**
hb *addr	set a hardwarre breakpoint at address **addr**
b *addr if $reg == val	set a software breakpoint at address **addr** if condition is satisfied
del br-num	delete breakpoint with number br-num
w *addr	set a watchdog for write at address **addr**
rw *addr	set a watchdog for read at address **addr**
rw *addr	set a watchdog for read at address **addr**
search WORD	show the address of the memory location containing **word**

Binary utilities

gcc -fPIC FILENAME.c -o FILENAME.so -shared	compile a shared library from c file
ldd **binary_file**	print the list of shared libraries that the binary needs
LD_PRELOAD=./FILENAME.so ./EXECUTABLE	preload your custom shared library into the binary and execute it eventually with arguments
checksec FILENAME	show mitigations applied to the binary
file FILENAME	show information about the file (i.e.: 32/64 bit, dynamically linked etc.)

ROP tools

ropper -f BIN_FILE	show the gadgets of a statically linked binary
ropper –nocolor -f BIN_FILE > GADGETS.TXT	create a file called GADGETS.TXT containing the information about the gadgets contained inside BIN_FILE
ropper –nocolor -f BIN_FILE | grep "WORD1 |WORD12"	show the gadget of a binary + select the rows which contain WORD1 and/or WORD2
ropper –nocolor -f BIN_FILE | grep "WORD1" | "WORD2"	show the gadget of a binary + select the rows which contain WORD1 and WORD2