RE for CTF 101

Registers

Register	Purpose
rax	Register a extended
rbx	Register b extended
rcx	Register c extended
rdx	Register d extended
r8-r15	64-bit mode General Purpose Registers

Register	Purpose
rbp	Register base ptr (start of stack)
rsp	Register stack ptr (current location in stack, growing down)
rsi	Register source index
rdi	Register data index

GDB

Command	Function
start	sets a temporary breakpoint at the beginning of the main procedure and `run`s it registers are loaded and addresses are correct
continue	resumes program execution after encountering a breakpoint
disassemble	dumps assembler code for current function, and tells us where we are in the instructions

RE for CTF 101

Assembly

Assembly	Meaning
add rax, 0x12	Add 0x12 to RAX
sub rbx, 0x12	Subtract 0x12 from RBX
snd r8, 0x10111111	Logical AND Operation
xor r9, 0x00000010	Logical XOR operation
add rax, 0x12	Add 0x12 to RAX
mov r9, rax	Store the value 0x1 into RAX
add [rax], 0x4	Operate on address stored in RAX
cmp rax, 0x4 jeq 0x118b	Jump if RAX contains 0x4
cmp rax, 0x4 jne 0x118b	Jump if RAX does not contain 0x4

Assembly	Meaning
cmp rax, 0x4 jl 0x118b	Jump if RAX is less than 0x4
cmp rax, 0x4 jg 0x118b	Jump if RAX is greater than 0x4
cmp rax, 0x4 jge 0x118b	Jump if RAX is greater or equal than 0x4
call 0x800117e <foo>	Call a function

push rbp
mov rbp, rsp
sub rsp, 0x20
	Function prologue (instructions to start a function)

leave ret	Function epilogue
push 0x491c	Push 0x491c onto the stack
pop rax	Pop the value on the stack into rax