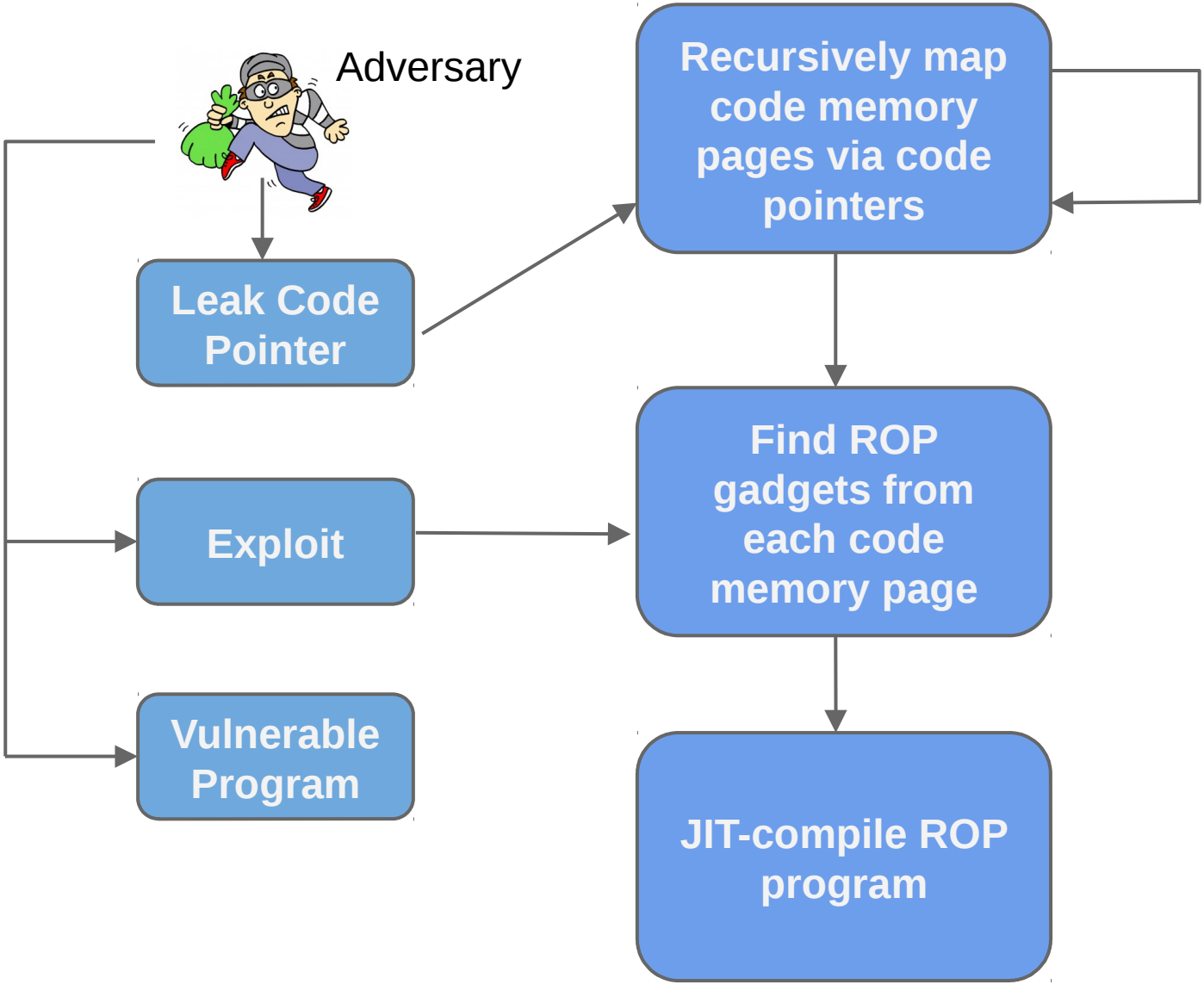
Adversary
Leak Code Pointer
Exploit
Vulnerable Program
Recursively map code memory pages via code pointers
Find ROP gadgets from each code memory page
JIT-compile ROP program