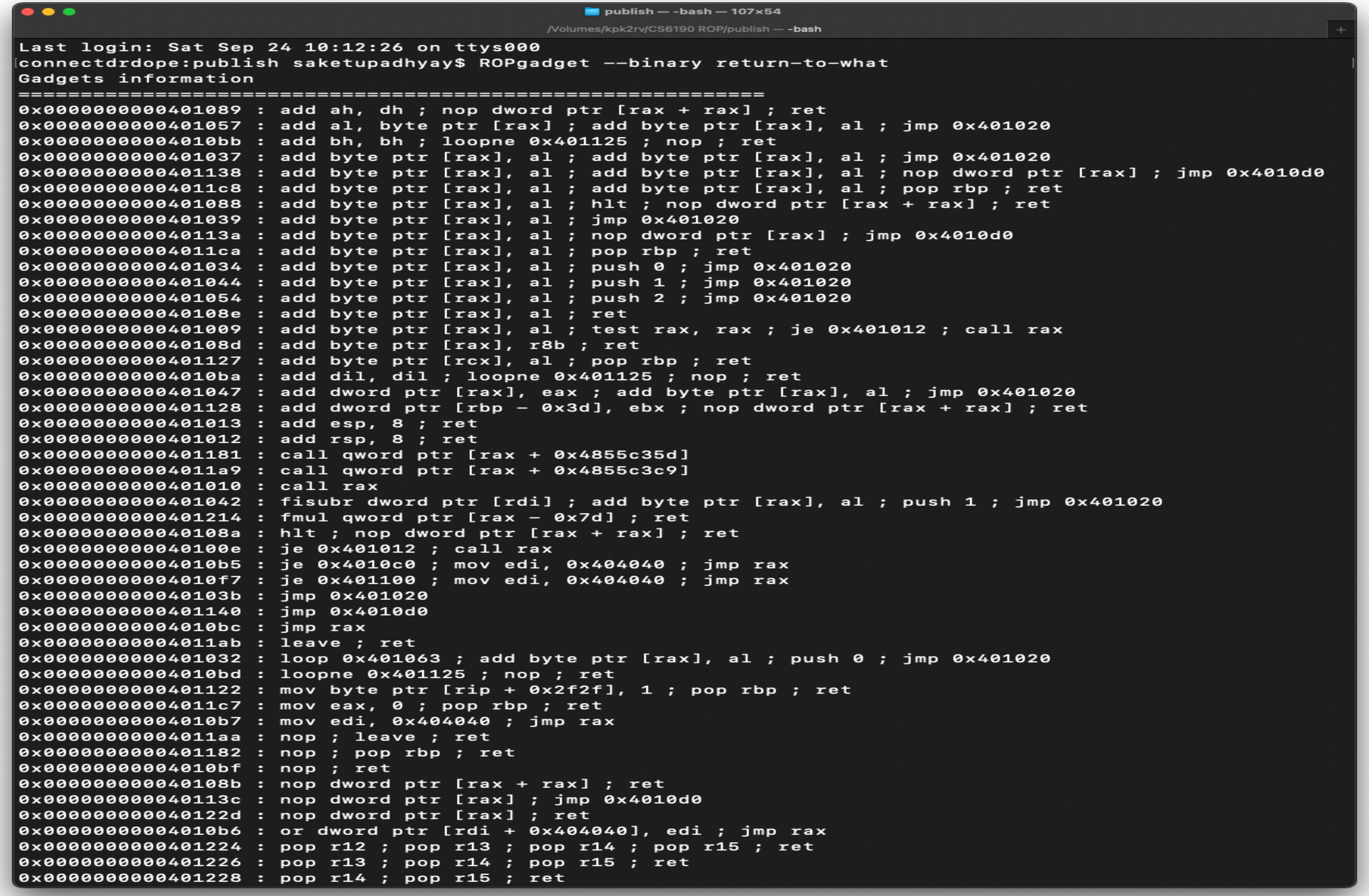
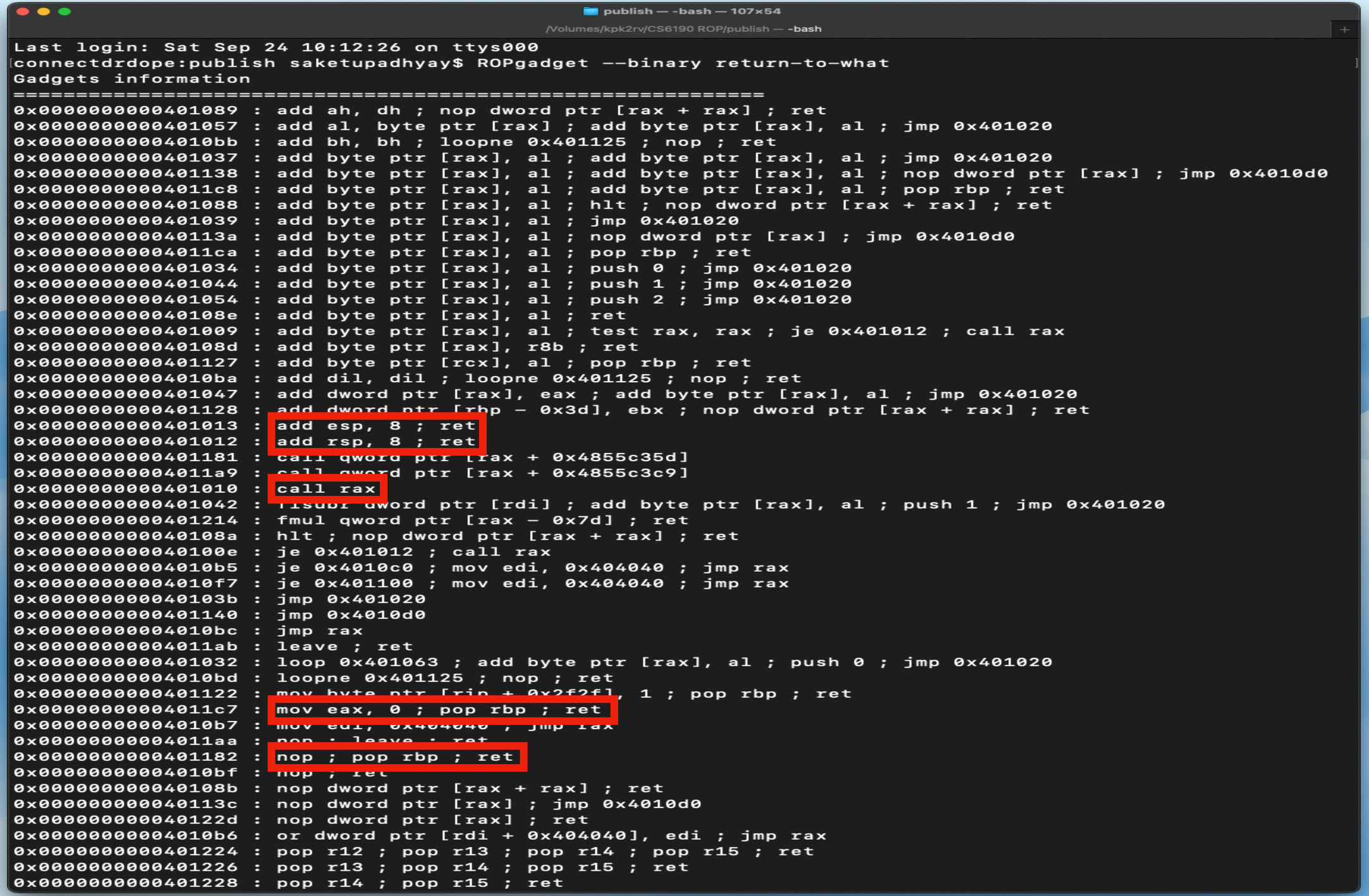

publish — -bash — 107×54
/Volumes/kpk2rv/CS6190 ROP/publish — -bash
Last login: Sat Sep 24 10:12:26 on ttys000
connectdrdope:publish saketupadhyay$ ROPgadget --binary return-to-what
Gadgets information
0x0000000000401089 : add ah, dh ; nop dword ptr [rax + rax] ; ret
0x0000000000401057 : add al, byte ptr [rax] ; add byte ptr [rax], al ; jmp 0x401020
0x00000000004010bb : add bh, bh ; loopne 0x401125 ; nop ; ret
0x0000000000401037 : add byte ptr [rax], al ; add byte ptr [rax], al ; jmp 0x401020
0x0000000000401138 : add byte ptr [rax], al ; add byte ptr [rax], al ; nop dword ptr [rax] ; jmp 0x4010d0
0x00000000004011c8 : add byte ptr [rax], al ; add byte ptr [rax], al ; pop rbp ; ret
0x0000000000401088 : add byte ptr [rax], al ; hlt ; nop dword ptr [rax + rax] ; ret
0x0000000000401039 : add byte ptr [rax], al ; jmp 0x401020
0x000000000040113a : add byte ptr [rax], al ; nop dword ptr [rax] ; jmp 0x4010d0
0x00000000004011ca : add byte ptr [rax], al ; pop rbp ; ret
0x0000000000401034 : add byte ptr [rax], al ; push 0 ; jmp 0x401020
0x0000000000401044 : add byte ptr [rax], al ; push 1 ; jmp 0x401020
0x0000000000401054 : add byte ptr [rax], al ; push 2 ; jmp 0x401020
0x000000000040108e : add byte ptr [rax], al ; ret
0x0000000000401009 : add byte ptr [rax], al ; test rax, rax ; je 0x401012 ; call rax
0x000000000040108d : add byte ptr [rax], r8b ; ret
0x0000000000401127 : add byte ptr [rcx], al ; pop rbp ; ret
0x00000000004010ba : add dil, dil ; loopne 0x401125 ; nop ; ret
0x0000000000401047 : add dword ptr [rax], eax ; add byte ptr [rax], al ; jmp 0x401020
0x0000000000401128 : add dword ptr [rbp - 0x3d], ebx ; nop dword ptr [rax + rax] ; ret
0x0000000000401013 : add esp, 8 ; ret
0x0000000000401012 : add rsp, 8 ; ret
0x0000000000401181 : call qword ptr [rax + 0x4855c35d]
0x00000000004011a9 : call qword ptr [rax + 0x4855c3c9]
0x0000000000401010 : call rax
0x0000000000401042 : fisubr dword ptr [rdi] ; add byte ptr [rax], al ; push 1 ; jmp 0x401020
0x0000000000401214 : fmul qword ptr [rax - 0x7d] ; ret
0x000000000040108a : hlt ; nop dword ptr [rax + rax] ; ret
0x000000000040100e : je 0x401012 ; call rax
0x00000000004010b5 : je 0x4010c0 ; mov edi, 0x404040 ; jmp rax
0x00000000004010f7 : je 0x401100 ; mov edi, 0x404040 ; jmp rax
0x000000000040103b : jmp 0x401020
0x0000000000401140 : jmp 0x4010d0
0x00000000004010bc : jmp rax
0x00000000004011ab : leave ; ret
0x0000000000401032 : loop 0x401063 ; add byte ptr [rax], al ; push 0 ; jmp 0x401020
0x00000000004010bd : loopne 0x401125 ; nop ; ret
0x0000000000401122 : mov byte ptr [rip + 0x2f2f], 1 ; pop rbp ; ret
0x00000000004011c7 : mov eax, 0 ; pop rbp ; ret
0x00000000004010b7 : mov edi, 0x404040 ; jmp rax
0x00000000004011aa : nop ; leave ; ret
0x0000000000401182 : nop ; pop rbp ; ret
0x00000000004010bf : nop ; ret
0x000000000040108b : nop dword ptr [rax + rax] ; ret
0x000000000040113c : nop dword ptr [rax] ; jmp 0x4010d0
0x000000000040122d : nop dword ptr [rax] ; ret
0x00000000004010b6 : or dword ptr [rdi + 0x404040], edi ; jmp rax
0x0000000000401224 : pop r12 ; pop r13 ; pop r14 ; pop r15 ; ret
0x0000000000401226 : pop r13 ; pop r14 ; pop r15 ; ret
0x0000000000401228 : pop r14 ; pop r15 ; ret


publish — -bash — 107×54
/Volumes/kpk2rv/CS6190 ROP/publish — -bash
Last login: Sat Sep 24 10:12:26 on ttys000
connectdrdope:publish saketupadhyay$ ROPgadget --binary return-to-what
Gadgets information
0x0000000000401089 : add ah, dh ; nop dword ptr [rax + rax] ; ret
0x0000000000401057 : add al, byte ptr [rax] ; add byte ptr [rax], al ; jmp 0x401020
0x00000000004010bb : add bh, bh ; loopne 0x401125 ; nop ; ret
0x0000000000401037 : add byte ptr [rax], al ; add byte ptr [rax], al ; jmp 0x401020
0x0000000000401138 : add byte ptr [rax], al ; add byte ptr [rax], al ; nop dword ptr [rax] ; jmp 0x4010d0
0x00000000004011c8 : add byte ptr [rax], al ; add byte ptr [rax], al ; pop rbp ; ret
0x0000000000401088 : add byte ptr [rax], al ; hlt ; nop dword ptr [rax + rax] ; ret
0x0000000000401039 : add byte ptr [rax], al ; jmp 0x401020
0x000000000040113a : add byte ptr [rax], al ; nop dword ptr [rax] ; jmp 0x4010d0
0x00000000004011ca : add byte ptr [rax], al ; pop rbp ; ret
0x0000000000401034 : add byte ptr [rax], al ; push 0 ; jmp 0x401020
0x0000000000401044 : add byte ptr [rax], al ; push 1 ; jmp 0x401020
0x0000000000401054 : add byte ptr [rax], al ; push 2 ; jmp 0x401020
0x000000000040108e : add byte ptr [rax], al ; ret
0x0000000000401009 : add byte ptr [rax], al ; test rax, rax ; je 0x401012 ; call rax
0x000000000040108d : add byte ptr [rax], r8b ; ret
0x0000000000401127 : add byte ptr [rcx], al ; pop rbp ; ret
0x00000000004010ba : add dil, dil ; loopne 0x401125 ; nop ; ret
0x0000000000401047 : add dword ptr [rax], eax ; add byte ptr [rax], al ; jmp 0x401020
0x0000000000401128 : add dword ptr [rbp - 0x3d], ebx ; nop dword ptr [rax + rax] ; ret
0x0000000000401013 : add esp, 8 ; ret
0x0000000000401012 : add rsp, 8 ; ret
0x0000000000401181 : call qword ptr [rax + 0x4855c35d]
0x00000000004011a9 : call qword ptr [rax + 0x4855c3c9]
0x0000000000401010 : call rax
0x0000000000401042 : fisubr dword ptr [rdi] ; add byte ptr [rax], al ; push 1 ; jmp 0x401020
0x0000000000401214 : fmul qword ptr [rax - 0x7d] ; ret
0x000000000040108a : hlt ; nop dword ptr [rax + rax] ; ret
0x000000000040100e : je 0x401012 ; call rax
0x00000000004010b5 : je 0x4010c0 ; mov edi, 0x404040 ; jmp rax
0x00000000004010f7 : je 0x401100 ; mov edi, 0x404040 ; jmp rax
0x000000000040103b : jmp 0x401020
0x0000000000401140 : jmp 0x4010d0
0x00000000004010bc : jmp rax
0x00000000004011ab : leave ; ret
0x0000000000401032 : loop 0x401063 ; add byte ptr [rax], al ; push 0 ; jmp 0x401020
0x00000000004010bd : loopne 0x401125 ; nop ; ret
0x0000000000401122 : mov byte ptr [rip + 0x2f2f], 1 ; pop rbp ; ret
0x00000000004011c7 : mov eax, 0 ; pop rbp ; ret
0x00000000004010b7 : mov edi, 0x404040 ; jmp rax
0x00000000004011aa : nop ; leave ; ret
0x0000000000401182 : nop ; pop rbp ; ret
0x00000000004010bf : nop ; ret
0x000000000040108b : nop dword ptr [rax + rax] ; ret
0x000000000040113c : nop dword ptr [rax] ; jmp 0x4010d0
0x000000000040122d : nop dword ptr [rax] ; ret
0x00000000004010b6 : or dword ptr [rdi + 0x404040], edi ; jmp rax
0x0000000000401224 : pop r12 ; pop r13 ; pop r14 ; pop r15 ; ret
0x0000000000401226 : pop r13 ; pop r14 ; pop r15 ; ret
0x0000000000401228 : pop r14 ; pop r15 ; ret

ROP Chain

- We combine multiple micro-operations to set the environment according to our needs.

- This process is called chaining.