실습1

|  |
| --- |
| .global main  main:  push %ebp  mov %esp, %ebp  sub $50, %esp  mov $3, %eax  mov $0, %ebx  mov %esp, %ecx  mov $50, %edx  int $0x80  mov $4, %eax  mov $1, %ebx  mov %ecx, %ecx  mov $50, %edx  int $0x80  mov $1, %eax  int $0x80 |

텍스트이(가) 표시된 사진

자동 생성된 설명

실습2

|  |
| --- |
| .global main  main:  push %ebp  mov %esp, %ebp  sub $28, %esp  push $0x0  push $0x41414141  mov $5, %eax  mov %esp, %ebx  mov $2, %ecx  int $0x80  mov $3, %eax  mov $3, %ebx  mov %esp, %ecx  mov $28, %edx  int $0x80  mov $4, %eax  mov $1, %ebx  mov %esp, %ecx  mov $28, %edx  int $0x80  mov $1, %eax  int $0x80 |

텍스트이(가) 표시된 사진

자동 생성된 설명

실습3

텍스트이(가) 표시된 사진

자동 생성된 설명

Shell.c 생성 -> gdb -> disas execve

텍스트이(가) 표시된 사진

자동 생성된 설명

어셈블리 코드로 변환 myshell.s

텍스트이(가) 표시된 사진

자동 생성된 설명

Shellc.c

텍스트이(가) 표시된 사진

자동 생성된 설명

정상작동됨

텍스트이(가) 표시된 사진

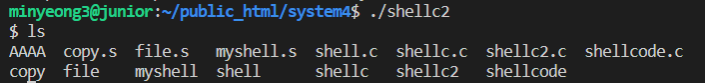
자동 생성된 설명

Null 제거함

텍스트이(가) 표시된 사진

자동 생성된 설명

Shellc2.c 생성



정상작동됨!

Prob8

|  |
| --- |
| #include<stdio.h>  #include <stdlib.h>  int main(int argc, char\*\* argv) {  int\* a;  FILE\* b, \* c;  long d;  int e;  if (2 >= argc) {  puts("Usage:. / prob8 input\_file.txt output\_file.txt");  exit(1);  }  b = fopen(argv[1], "rb");  c = fopen(argv[2], "wb");  fseek(b, 0, 2);  d = ftell(b); // <+108>  fseek(b, 0, 0);  e = fgetc(b); //<+129>  if (feof(b)!=0) {  fputc(e, c);  a = malloc(d); //<+173>  while (feof(b) == 0); {  fputc(e, c);  fread(a, 1, 1, b);  fwrite(a, 1, 1, c);  e = fgetc(b);  }  puts("gogo~!");  }  fclose(b); //<+281>  fclose(c);  free(a);  return 0;  } |

텍스트이(가) 표시된 사진

자동 생성된 설명

Prob9

|  |
| --- |
| #include<stdio.h>  #include <time.h>  #include<stdlib.h>  #include<string.h>  int main(int argc, char\*\* argv) {  char buf[256];  FILE\* a;  char\* b;  if (argc < 2) {  puts("Usage : ./prob9 [passwd]");  }  if (time(0) == atoi(argv[1])) {  printf("passwd = %d\n", atoi(argv[1]));  a = fopen("key\_09.txt", "r");  fscanf(a, "%s", buf);  b = malloc(strlen(buf)+1);  strcpy(b, buf);  printf("key = %s", b);  }  else  puts("Try Again~~!");  return 0;  } |

**#3. 파일을 쓰고 그 파일을 다시 읽는 프로그램 만들기**

|  |
| --- |
| .global main  main:          push %ebp          mov %esp, %ebp          sub $30, %esp          push $0x0          push $0x41414141          mov $5, %eax          mov %esp, %ebx          mov $2, %ecx          int $0x80          mov $3, %eax          mov $0, %ebx          mov %esp, %ecx          mov $30, %edx          int $0x80          mov $4, %eax          mov $3, %ebx          mov %esp, %ecx          mov $32, %edx          int $0x80          mov $4, %eax          mov $1, %ebx          mov %esp, %ecx          mov $28, %edx          int $0x80          mov $1, %eax          int $0x80 |

텍스트이(가) 표시된 사진

자동 생성된 설명

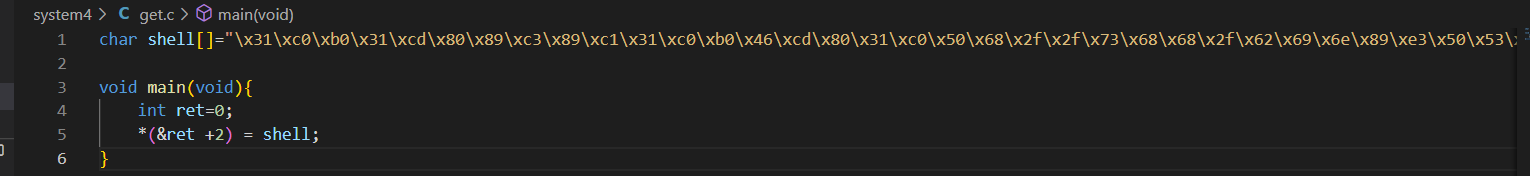


**#4. Shellcode에 getuid setreuid 추가해서 만들기**

텍스트이(가) 표시된 사진

자동 생성된 설명

Set.c



Get.c

텍스트, 장치, 측정기, 게이지이(가) 표시된 사진

자동 생성된 설명

정상작동됨