커널해킹의 이해 중간고사 (2016)

이름:
학번:

1. Bug 와 Vulnerability 의 차이점이 무엇인가?
2. 잘 개발된 Exploitation 이 가져야 할 조건 세가지를 설명하여라.
3. User-land exploitation 이 점점 힘들어짐에 따라 Kernel-land exploitation 이 주목을 받고 있다. User-land exploitation 이 힘들어지고 있는 이유와 Kernel-land exploitation 의 장단점을 설명하여라.
4. Kernel Path 의 두가지 종류를 설명하여라.
5. Interrupt 의 종류 세가지를 설명하고, Interrupt 가 발생하면 해당 코드를 실행하는데 필요한 Kernel data structure 가 무엇인지 설명하여라.
6. Return-to-Libc 공격을 설명하여라
7. 다음 코드의 실행 결과를 설명하여라.

```
#include <stdio.h>
#include <strings.h>

void big_stack_usage() {
    char big[200];
    memset(big,'A', 200);
}

void ptr_un_initialized() {
    char *p;
    printf("Pointer value: %p\n", p);
}

int main()
{
    big_stack_usage();
    ptr_un_initialized();
}
```