안녕하세요 여러분!
아름다운 버퍼 오버플로우의 세계에 오신 것을 환영합니다.

지금 읽고 계신 이 서적은 버퍼 오버플로우 강좌 시리즈 중 첫 번째인 “왕기초편”으로서, 버퍼 오버플로우의 개념 이해를 시작으로 가장 기본적인 테크닉을 이용한 리눅스 최고관리자(root) 권한 획득까지의 내용을 다루고 있습니다.

이 왕기초편의 특징은 버퍼 오버플로우 및 그와 관련된 “기본 개념을 이해하는 것”을 목표로 둔다는 점입니다. 그렇기 때문에 너무 어렵거나 기술적인 내용보다는 기초 개념 설명에 중점을 두고 있습니다.

특히 초보분들이 처음에 많이 어려워하시는 “어셈블리어”를 다루지 않고 버퍼 오버플로우를 설명하고 있습니다. 그렇기 때문에 이 서적은 아직 어셈블리어와 버퍼 오버플로우를 동시에 소화하기에는 버거운 분들께 적합할 것입니다.

하지만 결국 어셈블리어와 같은 고급 지식들은 버퍼 오버플로우를 비롯한 다양한 해킹 기술의 깊은 이해에 있어 필수 요소이기 때문에 이에 대해선 “쉘코드 제작편” 및 “심화편”에서 상세하게 다루게 됩니다.

보통 버퍼 오버플로우 공부의 시작점으로서 “aleph1의 smashing the stack for fun and profit” 문서를 권합니다. 이 서적은 위 문서를 아직 읽어보지 못하셨거나, 혹은 읽어는 보았으나, 선뜻 잘 이해가 되지 않으셨던 분들께 추천해 드립니다.

부디 이 서적이 버퍼 오버플로우의 완전한 이해를 향한 기분 좋은 첫 걸음이 되길 바랍니다. ^.^

프롤로그

이 책의 목표

./vuln.c

```
int main(int argc, char *argv[])  // 프로그램의 시작
{
	// 80바이트 크기의 지역 변수 선언
	char buffer[80];

	// 프로그램으로 전달 된 인자 확인
	if(argc < 2)
	{
		printf("argument error₩n");
		exit(-1);
	}

	// 프로그램의 첫 번째 인자를 지역 변수 buffer로 복사
	strcpy(buffer, argv[1]);

	// 복사된 내용 출력
	printf("your input is %s₩n", buffer);
}
```

위는 전형적인 버퍼 오버플로우 취약점을 가지고 있는 프로그램의 소스 코드입니다.
이 책을 다 읽을 때 즈음 여러분은 위 프로그램에 존재하는 취약점을 이해하고,
이를 공격하여 최고관리자 권한인 root 권한을 획득할 수 있게 될 것입니다!

해킹핸드북-버퍼오버플로우 시리즈의 구성

버퍼 오버플로우 – 왕기초편
버퍼 오버플로우 해킹 기술과 관련된 여러 기초 개념들을 설명하며, 일반사용자에서 관리자로 권한을 상승시키는 실습을 해봅니다. 모든 실습은 리눅스 OS 환경에서 진행됩니다.

버퍼 오버플로우 – 쉘코드 제작편
어셈블리 언어에 대해 배워보고, 이를 이용하여 다양한 목적의 쉘코드를 만드는 연습을 해봅니다. 그리고 쉘코드가 버퍼 오버플로우 공격에 어떻게 활용되는지 알아봅니다.

버퍼 오버플로우 – 심화편
버퍼 오버플로우 공격 과정 뒤에 숨어 있는 근본 원리에 대해 심도있게 다루며, 공부 과정에서 흔히 발생하는 문제점 및 해결책에 대해서도 알아봅니다.

버퍼 오버플로우 – 문제풀이편
The Lord of the BOF(버퍼오버플로우)라는 해커스쿨에서 만든 버퍼오버플로우 전용 워게임의 풀이법을 상세하게 설명합니다.

버퍼 오버플로우 – Windows편
윈도우즈 운영체제 환경에서의 버퍼 오버플로우에 대해 알아보며, 리눅스 OS 환경에서와의 차이점을 이해합니다.

버퍼 오버플로우 – 실전편
과거에서 최근까지 실제 발생했던 버퍼오버플로우 관련 공개 취약점을 분석하고 exploit을 구현해 봅니다.

프롤로그

이 책을 읽기 전에 기본으로 알고 있어야 할 것들

이 서적은 왕초보를 대상으로 하기 때문에 가능한한 자세한 설명을 전달하고자 노력했습니다. 하지만 여러분이 이 책을 읽기 전에 필수적으로 선행 학습하셔야 할 것이 있으니, 그것은 바로 "C언어"입니다.

버퍼 오버플로우는 프로그래밍 실수로 인해 발생하기 때문에, 프로그래밍에 대한 기본 지식 없이는 제대로 이해할 수가 없습니다. 그렇기 때문에 혹시 아직 C언어를 공부하지 않은 상태라면, C언어 공부를 먼저 한 후에 이 책을 학습해 주시길 바랍니다.

아직 마땅한 C언어 서적을 선택하지 못하였다면, 윤성우님이 집필하신 "난 정말 C언어를 배운 적이 없다고요" 혹은 "열혈강의 C언어" 서적을 추천해 드립니다. 이 두 서적은 제가 시중에 출판된 많은 C언어 서적을 벤치마킹하여 선별한 서적들입니다.

그리고 버퍼 오버플로우를 너무 빨리 공부하고 싶어서 C언어를 오래 잡고있지 못하겠다하시는 분들은 최소한 다음의 단원들만이라도 꼭 학습한 후에 시작해주시기 바랍니다.

- 컴파일(compile)이란?
- 변수와 상수란?
- 함수(function)란?
- 배열과 포인터(pointer)란?