2013년 01회

216. 컴퓨터에 대한 공격 방법 중에서 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소(return address)를 조작, 궁극적으로 공격자가 원하는 코드를 실행하도록 하는 공격은?

① 버퍼 오버플로우 공격 ② Race Condition

③ Active Contents ④ Memory 경합

정답	1

2014년 04회

217. 다음 중 버퍼오버플로우 대한 설명으로 올바르지 못한 것은?

① 버퍼에 저장된 프로세스 간의 자원 경쟁을 야기해 권한을 획득하는 기법으로 공격하는 방법이다.

② 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소를 조작하는 기법을 사용하여 해킹을 한다.

③ 스택 버퍼오버플로우와 힙 오버플로우 공격이 있다.

④ 버퍼오버플로우가 발생하면 저장된 데이터는 인접한 변수영역까지침범하여 포인터 영역까지 침범하므로 해커가 특정코드를 실행하도록 하는 공격기법이다.

정답	1

레이스 컨디션(Race Condition) 공격

- Race Condition 상태는 Unix 시스템에서 다수의 프로세스가 서로 동일한 자원을 할당받기 위해 경쟁하는 상태를 나타내는 말이다.
- 다수의 프로세스 간 자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능하게 하는 공격 기법이다.
- 두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다.

(1) C언어에서 버퍼 오버플로우에 취약한 함수

① 버퍼 오버플로우 공격은 프로세스가 정해진 크기의 버퍼 한계를 벗어나 이웃한 메모리 위치에 데이터를 겹쳐 쓰려고 시도하는 것과 같은 프로그래밍 오류의 결과로 발생하는 것으로 아래와 같이 취약한 함수를 썼을 때에는 추가적인 코딩을 해줘야 한다.

- **strcpy(char *dest, char *src);** 문자열 src의 내용을 문자열 desc에 복사한다. src문자열의 길이를 체크하지 않으므로 desc 버퍼를 초과하는 결과가 발생할 수 있다.
- strcat(char *dest, char *src); 문자열 src의 내용을 문자열 desc에 붙인다.
- getwd(char *buf);
- **gets**(char *s); 표준 입력에서 줄을 읽고 호출에 의해 버퍼로 불러와 저장하는 C 표준 라이브러리의 기능으로 매우 위험한 함수로 손꼽힌다. 심지어 리눅스 매뉴얼에는 저주받은 함수라는 표현되어 있을 정도이다. 따라서 초보자는 fget()를 이용해야 한다.
- scanf(const char *format, ...); 주어진 문자열 스트림 소스에서 지정된 형식으로 데이터를 읽어내는 함수
- **sscanf**(char *str, const char *format, ...); **scanf()함수와 비슷하지만 메모리 공간에 입력해주는 함수**.
- vscanf(), vsscanf()
- realpath(char *path, char resolved_path[]);
- sprintf(char *str, const char *format);
- vsprintf();

(2) C언어에서 사용을 권장하는 함수

- **strncat**(복사받을 변수, 복사할 변수, 복사할 길이): 입력한 길이만큼만 덧붙이는 함수
- **strncpy**(복사받을 변수, 복사할 변수, 복사할 길이): 원하는 길이만큼 복사받을 수 있는 함수
- **strcmp(str1, str2)**: 함수는 두 문자열 str1과 str2를 비교하여, 같으면 0을, str1이 더 크면 양수를, str2가 더 크면 음수를 반환한다.
- **fgets**(입력받을 변수명, 문자열 최대길이, 스트림): stream에서 문자열을 최대 num-1개 만큼 받아서 str이 기리키는 메모리에 저장하는 함수
- **fscanf();**
- **vfscanf();**
- **snprintf();**
- **vsnprintf();**

(3) 안전한 코딩(Secure Coding) 기술

③ **안전한 소프트웨어 개발을 위해 소스코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 보안 활동이다.**

2018년 11회

218. 다음 중 C언어 함수 중에서 버퍼 오버플로우 취약점이 발생하지 안도록 하기 위해 권장하는 함수가 아닌 것은?

① strncat() ② strncpy()

③ snprintf( ) ④ gets()

정답 4

2016년 07회

219. 다음 중 프로그래머의 관점에서 버퍼 오버플로우 공격에 취약하지 않도록 사용 자제를 권고하는 함수는 무엇인가?

① snprintf() ② strcpy()

③ gets() ④ strcat()

정답 1

2013년 02회

220. 다음 중 버퍼 오버플로우 취약점이 존재하는 함수가 아닌 것은?

① strcpy ② strcat

③ scanf ④ snprintf

정답 4

2018년 12회

221. 권장하는 함수에 속하는 것은?

① strcat() ② gets()

③ sprintf() ④ strncpy()

정답 4

strncpy(복사받을 변수, 복사할 변수, 복사할 길이): 원하는 길이만큼 복사받을 수 있는 함수

2017년 09회

222. 권장하는 함수에 속하는 것은?

① strcat( ) ② gets( )

③ sprintf( ) ④ strncpy( )

정답 4

2019년 14회

223. 버퍼 오버플로우에 취약한 함수가 아닌 것은?

① strcpy()　② fgets　③ gets()　④ scanf

정답 2

fgets(입력받을 변수명, 문자열 최대길이, 스트림): stream에서 문자열을 최대 num-1개 만큼 받아서 str이 기리키는 메모리에 저장하는 함수이다.

2019년 14회

224. 다음 중 버퍼 오버플로우에 취약한 함수가 아닌 것은?2

① strcpy　② fgets

③ getbyhostname　④ scanf

정답 2

2016년 08회

225. 스택 버퍼 오버플로우 공격의 수행절차를 순서대로 바르게 나열한 것은?

ㄱ. 특정 함수의 호출이 완료되면 조작된 반환 주소인 공격 셸 코드의 주소가 반환된다. ㄴ. 루트 권한으로 실행되는 프로그램 상에서 특정 함수의 스택 버퍼를 오버플로우시켜서 공격 셸 코드가 저장되어 있는 버퍼의 주소로 반환 주소를 변경한다. ㄷ. 공격 셸 코드를 버퍼에 저장한다. ㄹ. 공격 셸 코드가 실행되어 루트 권한을 획득하게 된다.

① ㄱ→ㄴ→ㄷ→ㄹ　② ㄱ→ㄷ→ㄴ→ㄹ

③ ㄷ→ㄴ→ㄱ→ㄹ　④ ㄷ→ㄱ→ㄴ→ㄹ

정답 3

2016년 08회

226. 버퍼 오버플로우 공격의 대응수단으로 적절하지 않은 것은?

① 스택상에 있는 공격자의 코드가 실행되지 못하도록 한다.

② 프로세스 주소 공간에 있는 중요 데이터 구조의 위치가 변경되지 않도록 적재 주소를 고정시킨다.

③ 함수의 진입(entry)과 종료(exit) 코드를 조사하고 함수의 스택 프레임에 대해 손상이 있는지를 검사한다.

④ 변수 타입과 그 타입에 허용되는 연산들에 대해 강력한 표 기법을 제공하는 고급수준의 프로그래밍 언어를 사용한다.

정답 2

공격에 대응하기 위한 방어수단

- 문자열 조작 루틴과 같은 불안전한 표준 라이브러리 루틴을 안전한 것으로 교체한다.
- 함수의 진입과 종료 코드를 조사하고 함수의 스택 프레임에 손상이 있는지를 검사한다.
- 한 사용자가 프로그램에 제공한 입력이 다른 사용자에게 출력되면 공격자는 이를 악용해 정보를 빼낼 수 있으므로 다른 사용자에게는 입력값이 출력되지 않도록 해야 한다.
- 매 실행 시마다 각 프로세스 안의 스택이 다른 곳에 위치하도록 한다.(randomization)

2016년 07회
227. 다음 중 버퍼 오버플로우(Buffer Overflow)에 대한 대책으로 옳지 않은 것은?
① 경계를 검사하는 함수를 사용한다.
② 운영체제 커널 패치를 실시한다.
③ 경계 검사를 하는 컴파일러 및 링크를 사용한다.
④ 최대 권한으로 프로그램을 실행한다.

정답	4

2014년 03회
228. 다음 중 버퍼 오버플로우 대응책으로 올바르지 못한 것은?
① 버퍼 오퍼플로우 취약점이 생기지 않도록 패치를 정기적으로 한다.
② 문자길이를 검사하지 않는 함수를 사용하지 않고 안전한 프로그래밍을 해야 한다.
③ 함수로부터 복귀할 때 스택의 무결성을 검사한다.
④ 사용자의 스택 혹은 힙 영역의 쓰기 및 실행권한을 준다.

정답	4

2013년 02회
229. 다음 중 버퍼 오버플로우를 막기 위해 사용하는 방법이 아닌 것은?
① Non-executable 스택
② ASLR(Address Space Layout Randomization)
③ RTL(return to libc)
④ 스택 가드(Stack Guard)

정답	3

"return-to-libc" 공격은 보통(NX 비트가 존재하는 경우 이것을 우회함으로써), 콜 스택의 서브루틴 반환 주소를 이미 프로세스의 실행 가능 메모리에 위치한 서브루틴의 주소로 교체되게 하는, 버퍼 오버플로 시에 사용되는 컴퓨터 보안 공격이다.

2014년 03회
230. 버퍼오버플로우에 대한 설명으로 올바르지 않은 것은?
① 버퍼에 저장된 프로세스 간의 자원 경쟁을 야기해 권한을 획득하는 기법으로 공격하는 방식이다.
② 오버플로우에는 힙오버플로우와 스택오버플로우가 있다.
③ 버퍼오버플로우가 발생하면 데이터는 인접한 포인트 영역까지 침범한다.
④ 대응책은 데이터가 들어가는 배열의 읽기, 쓰기가 배열 범위를 벗어나지 않는지 검사한다.

정답	1

포맷 스트링(Format String) 공격 p.596

2) 포맷 스트링(Format String) 공격

(1) 개념

① 버퍼 오버플로우 공격과 유사하며 C언어가 생기면서부터 존재했지만, 발견에 많은 시간이 소요되었다.
② 포맷 스트링 공격은 데이터의 형태와 길이에 대한 불명확한 정의로 인한 문제점 중 '데이터 형태에 대한 불명확한 정의'로 인한 것이다.
③ 일반적으로 다음 formatstring.c 함수와 같이 buffer에 저장된 문자열은 printf 함수를 이용하여 출력한다.
④ 포맷 스트링을 인자로 하는 함수의 취약점을 이용한 공격으로 외부로부터 입력된 값을 검증하지 않고 입출력 함수의 포맷 스트링을 그대로 사용하는 경우 발생할 수 있는 취약점이다.
⑤ ormatstring.c와 같이 포맷 스트링을 작성하는 것은 정상적인 경우이며 포맷 스트링에 의한 취약점은 발생하지 않는다. 여기서 사용된 %s와 같은 문자열을 가리켜 포맷 스트링이라고 하며 그 종류는 다음과 같다.

파라미터	특징	파라미터	특징
%d	정수형 10진수 상수 (integer)	**%o**	양의 정수 (8 진수)
%f	실수형 상수 (float)	**%x**	양의 정수 (16 진수)
%lf	실수형 상수 (double)		
%s	문자 스트링 ((const)(unsigned) char *)	**%n**	* int (이전까지 출력한 총 바이트 수)
%u	양의 정수 (10 진수)	**%hn**	%n의 반인 2바이트 단위

표 302 포맷 스트링 파라미터 종류

(2) 공격방법

① 포맷스트링 인자로 하는 함수의 취약점(입력값을 검증하지 않음)을 이용한 공격방법이다.
② 공격자는 취약한 프로세스를 공격하거나, 메모리 내용을 read/write가능하다.
③ 결과적으로 프로세스 권한획득 및 임의의 코드 실행할 수 있다.
④ 포맷스트링을 지정하지 않았을 경우 공격자는 메모리 내용을 참조하여 값 변조가 가능
⑤ 예를 들면 공격자는 주소값을 원하는 위치로 변조하여 악성코드를 실행할 수 있다.
· 대응방안 : 포맷스트링을 함수의 입력 파라미터로 직접사용하지 않는다.(외부입력X)
⑥ ex)printf(argv[1]); => printf("%s" ,argv[1]);

2014년 04회
231. 다음 공격기법을 무엇이라 하는가?

▪ 데이터의 형태와 길이에 대한 불명확한 정의로 인한 문제점 중 '데이터 형태에 대한 불명확한 정의'로 인한 것이다. ▪ 일반적으로 buffer에 저장된 문자열은 printf 함수를 이용하여 출력한다. ▪ 외부로부터 입력된 값을 검증하지 않고 입출력 함수의 포맷 스트링을 그대로 사용하는 경우 발생할 수 있는 취약점이다.

① 버퍼오버플로우공격 ② 스니핑 공격
③ 포맷스트링공격 ④ 세션하이젝킹 공격

정답 3

2015년 05회
232. 다음 지문의 빈칸에 알맞은 단어는 무엇인가?

(A)은(는) printf 등의 함수에서 문자열 입력 포맷을 잘못된 형태로 입력하는 경우 나타나는 버그이다. (B) 특정 프로그램을 이용하여 네트워크상의 데이 터를 몰래 캡처하는 행위를 말한다.

① ⓐ 포맷 스트링, ⓑ 스니핑
② ⓐ 버퍼 오버플로우, ⓑ 하이젝킹
③ ⓐ 스니핑, ⓑ 버퍼 오버플로우
④ ⓐ 스니핑, ⓑ 스푸핑

정답 1

2018년 12회
233. 다음 중 포맷 스트링(Format String)공격에 대해 잘못 설명한 것은?
① 시스템 자원을 고갈시켜 가용성을 공격하는 기법이다.
② 대표적으로 printf() 함수를 공격 대상으로 삼는다.
③ 포맷 스트링을 취약점으로 stack에 비정상적으로 접근한다.
④ Write가 허용된 Memory Segment에 원하는 값을 삽입할수 있다.

정답 1

2017년 09회
234. 형식에 대한 매개변수를 적절하게 고른 것은?

매개변수 형식
%d 정수형 10진수 상수
ㄱ. 문자스트링
ㄴ. 16진수 양의 정수
ㄷ. %n의 반인 2바이트 단위

① ㉠ %s, ㉡ %o, ㉢ %lf
② ㉠ %s, ㉡ %x, ㉢ %hn
③ ㉠ %c, ㉡ %x, ㉢ %hn
④ ㉠ %c, ㉡ %o, ㉢ %lf

정답 2

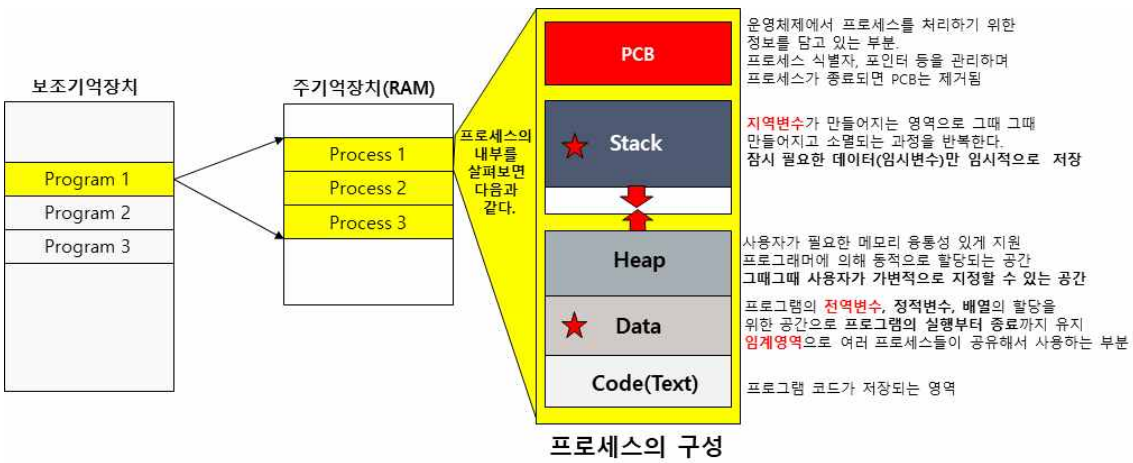
2017년 10회
235. 다음 지문에서 설명하는 공격은?

- 메모리는 런 타임 시에 애플리케이션에 의해 동적으로 할당되며 일반적으로 프로그램 데이터를 포함한다.
- 동적 메모리 할당 연결(malloc 메타 데이터 같은)을 겹쳐 쓰고 프로그램 함수 포인터를 겹쳐 쓰기 위해 결과로 나온 포인터를 교환하는 기법이다.
- 이 공격에 사용되는 메모리 영역은 malloc, free 등의 함수로 제어함
- 쉘 코드를 사용하기 위하여 함수의 반환 주소를 단순히 덮어 쓰는 방법은 사용할 수 없고, 버퍼에 할당된 포인터 값을 덮어 쓰는 방법이 일반적으로 사용됨

① 스택 버퍼 오버플러우 ② 레이스 컨디셔닝
③ 힙 버퍼 오버플로우 ④ RTL(Return To Libc)

정답 3

heap(힙): 응용 애플리케이션에 의해 동적으로 할당되는 메모리 영역이다.



프로세스의 구성

레이스 컨디션(Race Condition) 공격 p.598

3) 레이스 컨디션(Race Condition) 공격

가) 개념

① Race Condition 상태는 Unix 시스템에서 다수의 프로세스가 서로 동일한 자원을 할당받기 위해 경쟁하는 상태를 나타내는 말이다.

② 다수의 프로세스 간 **자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능**하게 하는 공격 기법이다.

③ **두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다**.

④ 시스템 프로그램과 공격 프로그램이 서로 자원을 차지하기 위한 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로 파일에 접근을 가능하게 하는 공격방법을 말한다.

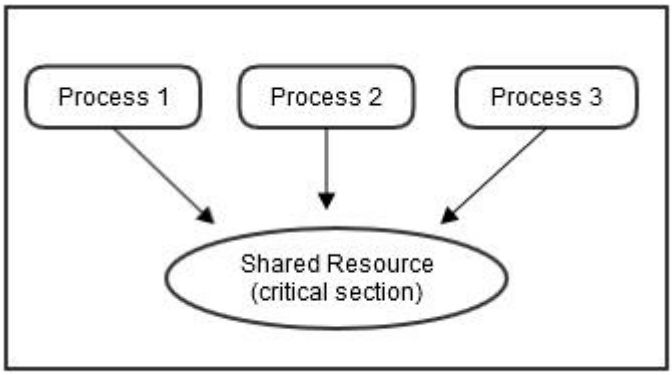


그림 35 Race Condition 상태

나) 경쟁조건 발생원인

① 시스템의 중요 자원의 integrity를 보증하기 위하여 중요 자원을 access 하는 경우에 자원을 locking하고, 사용 후에 release 시킨다.

② 한 프로세스가 자원을 lock하고 있는 경우에, 이 자원을 얻으려는 다른 프로세스들은 wait 해야 한다.

③ 자원을 lock한 프로세스가내부적인 문제로 release가 길어지는 경우에 프로세스 대기 행렬이 길어지고, 교착상태(deadlock)의 발생가능성이 커지고, 시스템의 performance에 심각한 영향을 준다.

다) 공격방법

① 다른 계정의 권한에 접근해야 하므로 **공격 파일에 root권한의 SetUID가 설정되어야 한다**.

② 프로세스 중에 임시로 파일을 만드는 프로세스가 있을 경우가 있어야 한다.

③ 임시 파일을 읽어 들여 파일을 삭제하거나 전혀 엉뚱한 파일과 연결하여 백도어를 만든다.

2019년 14회

236. 다음에서 설명하는 취약점(또는 공격 메커니즘)은 무엇인가?3

• 공유 자원에 대해 여러 개의 프로세스가 동시에 접근을 시도할 때 접근의 타이밍이나 순서 등이 결과값에 영향을 줄 수 있는 상태로, 프로세스 간의 자원 경쟁을 유발하여 권한을 획득하는 기법으로 활용된다. • 다수의 프로세스 간 자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능하게 하는 공격 기법이다. 두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다.

① Drive by download
② Exploit
③ Race Condition
④ Buffer Overflow

정답	3

Race Condition 상태는 Unix 시스템에서 다수의 프로세스가 서로 동일한 자원을 할당받기 위해 경쟁하는 상태를 나타내는 말이다.

2017년 10회

237. 여러 프로세스가 자원의 이용을 위해 경쟁을 벌이는 현상을 이용하는 공격은 무엇인가?

① SQL 인젝션 공격 ② LADP 인젝션 공격
③ XML 인젝션 공격 ④ 레이스 컨디션 공격

정답	4

2015년 06회

238. 다음 중 레이스 컨디셔닝 공격에 대한 설명으로 올바르지 않은 것은?

① Setuid가 설정되어 있어야 한다.
② Symbolic Link의 사용 주의한다.
③ 임시파일 사용 시 링크상태, 파일의 종류, 파일의 변경여부 등을 점검한다.
④ 임시 파일 이름을 공격자가 몰라도 된다.

정답	4