

정보시스템보안

2019년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 시스템 해킹에 사용되는 레이스 컨디션(race condition) 공격에 대한 다음 물음에 답하시오. (총 13점)

- 1) 레이스 컨디션 공격의 기본 개념을 설명하시오. (3점)
- 2) 유닉스(리눅스) 시스템에서 심볼릭 링크(symbolic link)를 이용하여 레이스 컨디션 공격을 수행하기 위한 조건과 절차에 대하여 설명하시오. (6점)
- 3) 심볼릭 링크를 이용하는 레이스 컨디션 공격에 대한 대응책에 대해서 설명하시오. (4점)

제 2 문. 인증 과정에서 패스워드 크래킹은 직접적인 보안 위협이다. 윈도우 인증 과정과 패스워드 크래킹 기법에 대한 다음 물음에 답하시오. (총 12점)

- 1) 윈도우의 인증 과정에서 사용하는 구성요소인 LSA(Local Security Authority), SAM(Security Account Manager), SRM(Security Reference Monitor)에 대해 각각 설명하시오. (6점)
- 2) 패스워드 크래킹 방법에는 사전 대입 공격(dictionary attack), 무작위 대입 공격(brute force attack), 레인보우 테이블(rainbow table)을 이용한 공격이 있다. 이에 대해 각각 설명하시오. (6점)

제 3 문. 버퍼 오버플로우(buffer overflow) 공격에 대한 다음 물음에 답하시오. (총 15점)

- 1) 스택 버퍼 오버플로우 공격과 힙 버퍼 오버플로우 공격에 대하여 각각 설명하시오. (4점)
- 2) 다음은 스택 버퍼 오버플로우 공격에 취약한 예제 프로그램이다. 스택 버퍼 오버플로우 공격에 취약한 행 번호와 그 이유에 대하여 설명하시오. (7점)

행 번호	프로그램 소스
1	#include <stdio.h>
2	#include <string.h>
3	int main(int argc, char *argv[]) {
4	char buffer[10];
5	strcpy(buffer, argv[1]);
6	printf("%s\n", buffer);
7	return 0;
8	}

- 3) 버퍼 오버플로우 공격에 대한 대응책에 대해서 설명하시오. (4점)

제 4 문. 정보시스템을 안전하게 관리하기 위해서는 다양한 로그를 수집하고 분석하여야 한다. 정보시스템이 저장하는 로그에 대한 다음 물음에 답하시오. (총 10점)

- 1) 윈도우 시스템이 각종 이벤트 로그를 저장할 때 적용하는 윈도우 로그 감사 정책 5가지를 나열하고 각각 설명하시오. (5점)
- 2) 유닉스(리눅스) 시스템이 저장하는 로그 파일명 5가지를 나열하고 각각 설명하시오. (5점)

인사혁신처 시험출제과장