

정보시스템보안

2018년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 임의의 데이터를 해쉬값으로 변환하는 해쉬 함수(hash function)는 일방향성과 충돌 회피성을 가져야 하며, 데이터 무결성을 증명할 목적으로 사용된다. 다음 물음에 답하시오. (총 15점)

- 1) 해쉬 함수의 일방향성과 충돌 회피성을 설명하시오. (3점)
- 2) 사용자가 해쉬 함수를 이용하여 저장하려는 데이터의 무결성을 확보할 수 있는 방법을 설명하시오. (6점)
- 3) 리눅스는 사용자 패스워드의 해쉬값을 shadow 파일에 저장한다. 해쉬 함수를 이용한 저장 방식은 shadow 파일이 외부로 유출되더라도, 패스워드 노출을 막을 수 있다. 해쉬 함수의 일방향성과 충돌 회피성의 관점에서 패스워드 안전성을 설명하시오. (6점)

제 2 문. 정보시스템 관리자는 정보시스템의 안전성을 확보하는 방법으로 시스템 내부에 설치된 백도어를 탐지해야 한다. 다음 물음에 답하시오. (총 10점)

- 1) 백도어의 상당수는 표적 시스템의 원격제어를 위해 특정 네트워크 포트를 사용한다. Unix/Linux 계열 시스템, Windows 시스템에서 백도어 존재여부를 확인할 수 있는 방법에 대하여 각각 설명하시오. (4점)
- 2) 네트워크 포트 스캐닝을 통한 백도어 탐지 기법 이외에, 백도어를 탐지하는 기법 3가지를 설명하시오. (3점)
- 3) Windows 시스템에서 실행 중인 프로세스 중 csrss.exe, svchost.exe의 주요 기능을 설명하고 백도어 탐지와 연관성을 설명하시오. (3점)

제 3 문. 지능형 지속 공격(APT, Advanced Persistent Threat)에 대한 다음 물음에 답하시오. (총 10점)

- 1) APT 공격의 특성을 공격대상, 공격목적 및 공격방법의 관점에서 기술하고, 대표적인 사례인 스텅스넷(Stuxnet)의 공격기법에 대해서 설명하시오. (5점)
- 2) APT에 활용가능한 풋프린팅(Footprinting)과 사회공학(Social Engineering)에 대하여 설명하시오. (5점)

제 4 문. 다음은 정보시스템의 접근제어에 대한 문제이다. 물음에 답하시오.

(총 15점)

- 1) 접근제어행렬(access control matrix)은 정보시스템의 접근제어규칙을 표현하는 수단이다. 정보시스템은 3명의 사용자(A, B, C)와 3개의 파일(File1, File2, File3)을 가진다고 가정한다. 3개의 파일(File1, File2, File3) 중 File1은 시스템의 중요 설정파일이며, 3명의 사용자(A, B, C) 중 사용자 A는 모든 파일에 대해 모든 권한을 가지고 있다. 사용자 B와 C는 일반 사용자이며 시스템의 중요설정 파일(File1)에 어떤 권한도 없고, File2와 File3에 대해 읽기/쓰기 권한을 가지고 있다. 접근제어행렬을 활용하여 위의 상황을 기술하고, 기술한 접근제어행렬을 활용하여 접근가능목록(capability list)과 접근제어목록(access control list)을 도출하시오. (단, 권한은 읽기가능은 r, 쓰기가능은 w, 실행가능은 x로 표현함. 문제의 제약조건 이외의 사항은 가정이 가능하며 해당 가정은 답안에 설명되어야 함) (8점)
- 2) 보안모델의 정의를 통해 정보시스템은 접근제어를 좀 더 체계적으로 할 수 있다. 여기서는 1)의 접근제어행렬을 기반으로 사용자 A와 File1은 높은 보안 등급을 소유하고 사용자 B, C와 File2, File3는 낮은 보안등급을 소유한다고 가정한다. 이때 보안 모델의 중요 규칙 중 하나인 ‘No-write-down’이 보장되지 않을 때의 문제점을 위 가정을 기반으로 설명하고, 이 문제점을 해결하기 위한 ‘No-write-down’의 구현방법을 서술하시오. (7점)

인사혁신처 시험출제과장