

정보보호론

2018년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 디지털 포렌식(Digital Forensic)에 대하여 다음 물음에 답하시오. (총 14점)

- 1) 포렌식의 기본 원칙 5가지를 나열하시오. (4점)
- 2) 디지털 데이터는 법적인 증거력을 확보하기 위해서 증거 능력의 요건을 충족해야 한다. 이를 위해 디지털 증거가 가져야 할 특성 4가지를 나열하시오. (4점)
- 3) 2)의 특성을 가지는 디지털 증거를 확보하기 위한 디지털 포렌식 수행 절차를 6단계로 나누고, 각 단계에서 수행해야 할 업무를 기술하시오. (6점)

제 2 문. 블록암호 CBC(Cipher Block Chaining) 운영모드에 대하여 다음 물음에 답하시오. (총 15점)

- 1) CBC 운영모드의 암호·복호화 동작과정을 그림과 수식으로 나타내시오. (5점)
- 2) CBC 운영모드에서 발생할 수 있는 오류전과 현상을 설명하시오. (4점)
- 3) CBC 운영모드와 OFB(Output Feedback) 운영모드의 특성과 장·단점을 비교 설명하시오. (6점)

제 3 문. 프로그램이 데이터를 입력받아 처리하는 과정에서 입력 데이터의 크기나 데이터의 의미 해석이 프로그램 실행을 위태롭게 할 수 있다. 다음 물음에 답하시오. (총 11점)

- 1) 프로그램에 입력되는 데이터의 크기를 확인하지 않았을 때 발생하는 보안 취약점과 이를 해결하기 위한 방안을 설명하시오. (5점)
- 2) 프로그램에 입력되는 데이터의 의미 해석 문제를 악용하는 공격과 이를 예방하기 위한 안전한 프로그래밍 방법을 기술하시오. (6점)

제 4 문. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제7호에 의거 “침해사고”란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다. 침해사고의 유형은 공통, 웹사이트변조, 악성코드 유포지/경유지, 봇넷 C&C(Command & Control), 해킹 경유지로 구분된다. 다음 물음에 답하시오. (총 10점)

- 1) 윈도우(Windows) 운영체제에서 공통 사고유형의 조사 항목(계정, 로그파일, 웹셀, 백도어, 루트킷)에 대한 분석 방법을 기술하시오. (7점)
- 2) 윈도우 운영체제에서 ‘봇넷 C&C’ 침해사고 유형의 ‘네트워크 연결’ 조사 항목에 대한 분석 방법을 기술하시오. (3점)

인사혁신처 시험출제과장