

## 정보보호론

### 2017년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 사회공학 기법을 사용한 공격에 대하여 다음 물음에 답하시오. (총 12점)

- 1) 피싱(phishing)과 파밍(pharming)에 대하여 각각 설명하시오. (6점)
- 2) 피싱과 파밍 중 DNS(Domain Name System) 스푸핑(spoofing)을 이용하는 공격은 무엇이며, 그 공격 과정에 대하여 설명하시오. (6점)

제 2 문. AES(Advanced Encryption Standard)에 대하여 다음 물음에 답하시오. (총 12점)

- 1) AES 알고리즘은 DES(Data Encryption Standard) 알고리즘과 비교하여 총 라운드 수, 평문 블록의 크기, 키의 길이에 변화가 있었다. 각 파라미터 수치가 어떻게 변화됐는지 각각 기술하시오. (4점)
- 2) AES 알고리즘의 한 라운드는 네 단계로 구성되어 있다. 각 단계별 동작 과정에 대하여 설명하시오. (8점)

제 3 문. 통계 분석을 이용하여 침입 여부를 탐지하는 방법에는 임계값 탐지(threshold detection)와 프로파일 기반 탐지(profile-based detection) 기술이 있다. 다음 물음에 답하시오. (총 11점)

- 1) 임계값 탐지 기술에 대하여 설명하고, 이 기술을 이용한 침입 여부 판단 방법에 대하여 설명하시오. (4점)
- 2) 프로파일 기반 탐지 기술에 대하여 설명하고, 이 기술에서 사용 가능한 평가 지수(metrics)의 예를 세 가지 들고, 그 의미를 설명하시오. (7점)

제 4 문. 무선 LAN 보안 방식으로 사용되는 IEEE 802.11i 표준 기술에 대하여 다음 물음에 답하시오. (총 15점)

- 1) WEP(Wired Equivalent Privacy) 프로토콜에서 사용되었던 CRC(Cyclic Redundancy Check) 변조 문제에 대하여 설명하시오. (4점)
- 2) 1)에서 제기된 CRC 변조 문제를 해결하기 위하여 IEEE 802.11i에서 적용한 기법에 대하여 설명하시오. (3점)
- 3) IEEE 802.11i 인증 방식에 대하여 설명하시오. (4점)
- 4) IEEE 802.11i 암호 방식에 대하여 설명하시오. (4점)

## 인사혁신처 시험출제과장