

정보보호론

2022년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. SSH(Secure Shell)에 대한 다음 물음에 답하시오. (총 15점)

- 1) SSH를 구성하는 3가지 프로토콜에 대해 설명하시오. (9점)
- 2) SSH가 제공하는 2가지 유형의 포트 포워딩에 대해 설명하시오. (6점)

제 2 문. 이상거래 탐지시스템(FDS, Fraud Detection System)에 대한 다음 물음에 답하시오. (총 10점)

- 1) FDS의 주요한 4가지 기능을 설명하시오. (4점)
- 2) FDS의 오용탐지 모델을 설명하시오. (6점)

제 3 문. 대표적인 하드웨어 보안 취약점인 스펙터(Spectre)와 멜트다운(Meltdown)에 대한 다음 물음에 답하시오. (총 10점)

- 1) 스펙터 취약점의 근본 원인과 해당 취약점을 이용한 공격의 영향을 설명하시오. (5점)
- 2) 멜트다운 취약점의 근본 원인과 해당 취약점을 이용한 공격의 영향을 설명하시오. (5점)

제 4 문. 패딩된 평문 M 이 l 개의 128비트 블록 연접 $M = M_1 || M_2 || \cdots || M_l$ 로 표현될 때, ECB(Electronic CodeBook), CBC(Cipher Block Chaining) 및 CFB(Cipher FeedBack) 운용(Operation) 모드에 의하여 생성되는 암호문 C 는 l 개의 128비트 블록 연접 $C = C_1 || C_2 || \cdots || C_l$ 로 표현된다. C_1, \dots, C_l 은 운용 모드에 따라 다음과 같이 정의될 때, 물음에 답하시오. (총 15점)

- ECB 운용 모드: $i = 1, \dots, l$ 에 대하여 $C_i = AES_K(M_i)$
 - CBC 운용 모드: $C_0 = IV$,
 $i = 1, \dots, l$ 에 대하여 $C_i = AES_K(M_i \oplus C_{i-1})$
 - CFB 운용 모드: $C_0 = IV$,
 $i = 1, \dots, l$ 에 대하여 $C_i = AES_K(C_{i-1}) \oplus M_i$
- ※ $AES_K(\cdot)$, $AES_K^{-1}(\cdot)$ 는 각각 비밀키 K 에 의하여 정의되는 AES의 암호화, 복호화 연산이고, IV 는 고정된 초기 벡터

- 1) ECB 운용 모드가 가지는 보안 취약성에 대하여 설명하시오. (4점)
- 2) CBC 운용 모드와 CFB 운용 모드의 복호화 과정을 설명하시오. (6점)
- 3) CBC 운용 모드와 CFB 운용 모드의 병렬 연산 가능성을 설명하고, CFB 운용 모드의 장점을 CBC 운용 모드와 비교하여 설명하시오. (5점)

인사혁신처 시험출제과장