

네트워크보안

2017년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. 침입차단시스템(Firewall)은 패킷 필터링(Packet Filtering) 방식, 응용 게이트 (Application Gateway) 방식, 상태기반 감시(Stateful Packet Inspection) 방식으로 분류된다. 다음 물음에 답하시오. (총 20점)

- 1) 패킷 필터링 방식과 비교하여 응용 게이트웨이 방식의 동작특성, 차단범위, 장단점을 예시를 들어 설명하시오. (10점)
- 2) 패킷 필터링 방식과 비교하여 상태기반 감시 방식의 동작특성, 차단범위, 장단점을 예시를 들어 설명하시오. (10점)

제 2 문. 침입탐지시스템(Intrusion Detection System, IDS)은 악의적인 네트워크 트래픽이나 비정상적인 컴퓨터 사용을 탐지하기 위하여 사용되지만, False Negative와 False Positive 오류가 존재한다. 다음 물음에 답하시오. (총 30점)

- 1) IDS에서 False Positive와 False Negative의 의미를 설명하시오. (6점)
- 2) IDS에 의해 분석된 이벤트 횟수가 100,000번이고, 그 중에서 100번이 실제 침입이었다. 이 때, IDS의 False Positive 비율과 False Negative 비율이 각각 2%와 1%로 확인되었다. IDS가 침입이라고 탐지한 이벤트 횟수를 풀이과정을 포함하여 구하시오. (10점)
- 3) 2)에서 구한 침입 이벤트 횟수 중에서 실제 침입의 비율을 백분율로 나타내시오. (단, 소수점 첫째자리에서 반올림하여 표시하되 풀이과정을 포함한다) (6점)
- 4) 3)에서 구한 비율만을 IDS의 성능 척도로 활용하는 것이 부적합함을 2)의 결과 값을 인용하여 설명하시오. (8점)

제 3 문. 클라이언트와 서버는 TCP를 기반으로 통신할 때 연결설정 절차를 진행한다. 해당 과정에서 중요 요소인 연결설정 테이블, TCP 헤더의 플래그(Flag) 정보, 순서 번호(Sequence Number)가 갖는 특성을 기반으로 발생하게 되는 보안상의 문제점과 관련하여 다음 물음에 답하시오. (총 30점)

- 1) 서버의 TCP 연결설정 테이블의 크기가 고정되어 있을 때, 연결설정이 불가능해지는 서비스 거부 상황이 발생될 수 있다. 이러한 상황을 연결설정 테이블 크기 및 서비스 요청 빈도와 연관지어 설명하시오. (10점)
- 2) 클라이언트 혹은 서버가 아닌 제3의 악의적인 호스트가 현재 진행 중인 TCP 연결설정을 종료시킬 수 있다. 이러한 상황을 TCP 헤더의 플래그 정보를 기반으로 설명하시오. (5점)
- 3) 클라이언트와 서버가 TCP 기반으로 통신 중인 상태에서 공격자가 스니핑을 통해 순서 번호를 획득하였다. 이 후, 공격자의 TCP 세션 하이재킹 공격이 이루어지는 과정을 설명하시오. (15점)

제 4 문. X.509 인증서에 대하여 다음 물음에 답하시오. (총 20점)

- 1) 사용자 A는 특정 CA(Certificate Authority) C의 올바른 인증서를 가지고 있다. C가 발급한 사용자 B의 인증서를 사용자 A가 획득한 후, 이 인증서를 검증하는 과정을 서술하시오. (10점)
- 2) 인증서의 폐기 여부를 확인하기 위한 두 방식인 CRL 방식과 OCSP 방식에 대해 각각 비교하여 설명하시오. (10점)

인사혁신처 시험출제과장