[문항1] 로그의 개념에 대해 간단히 서술하시오.

로그는 특정 사건이 발생했을 때, 사건의 발생 시점, 내용, 주체 등을 기록한 정보이다. 이는 장애 분석, 정책 위반 탐지, 보안 사고 대응 등에 활용된다.

[문항2] 오탐 유형 중 FRR(False Reject Ratio)에 대해 간단히 서술하시오.

FRR은 악의적 공격을 정상 접근으로 잘못 판단하여 허용하는 오류를 의미한다. 이는 보안 요구 수준이 높은 조직에서 과도한 예외처리나 탐지 규칙 부재 시 발생할 수 있다.

[문항3] 로그 분석 시 IP Packet 구조를 이해하면 도움이 되는 이유에 대해 간단히 서술하시오.

IP Packet은 공격자 정보나 공격 기법, 전송 경로 등의 정보를 담고 있어 로그 분석 시 필수적인 요소이다. 각 계층별 정보(L2~L4)를 통해 공격 원리와 경로를 정확히 파악할 수 있다.

[문항4] 보안시스템 중 방화벽(Firewall)에 대해 간단히 서술하시오.

방화벽은 네트워크 트래픽을 제어하여 비인가 접근을 차단하고, 내부 시스템을 보호하는 보안장비이다. 접근 정책에 따라 트래픽을 허용하거나 차단함으로써 위협을 사전에 방지할 수 있다.

[문항5] 보안로그의 기록 방식 분류는 크게 저장 Type과 저장 위치에 따라 구분되는데 이 중 저장 Type에 대해 간단히 서술하시오.

저장 Type은 보안로그가 저장되는 방식으로, 일반적으로 파일(File) 저장과 데이터베이스(Database) 저장으로 나뉜다. 파일 저장은 소규모 로그에 적합하고, 데이터베이스 저장은 대규모 로그의 검색과 관리에 유리하다.

[문항6] 공격경로 확인 방법 중 기본 공격경로 확인기법에 대해 간단히 서술하시오.

기본 기법은 traceroute 등을 이용해 단순한 네트워크 라우팅 경로를 파악하는 방법이다. 이를 통해 공격자가 목적지까지 도달한 흐름을 시각적으로 추적할 수 있다.

[문항7] 공격 경로를 확인하기 위한 명령어를 서술하시오.

공격 경로 확인에는 Windows의 tracert 또는 Linux의 traceroute 명령어를 사용할 수 있다. 이 명령어는 네트워크 패킷이 지나가는 경유지를 단계별로 표시해준다.

[문항8] 탐지패턴을 개발하는 목적에 대해 간단히 서술하시오.

탐지패턴 개발은 보안시스템이 알려진 위협을 신속하게 인식하고 차단하도록 돕는 것이 목적이다. 이를 통해 침해사고를 조기에 발견하고 자동화된 대응이 가능해진다.

[문항9] 보안이벤트 탐지를 위한 탐지 모형은 크게 이상 탐지와 오용 탐지로 분류되는데 이 중 이상 탐지의 개념에 대해 간단히 서술하시오.

이상 탐지는 정상적인 활동 패턴을 기준으로 이탈 행위를 탐지하는 방식이다. 이는 알려지지 않은 새로운 공격이나 제로데이 공격 탐지에 효과적이다.

[문항10] 탐지패턴 최적화 목적에 대해 간단히 서술하시오.

탐지패턴 최적화는 오탐과 누락 탐지를 줄여 정확도를 높이고, 보안시스템의 효율적인 운영을 위해 수행된다. 이는 리소스 낭비를 방지하고 대응 속도를 개선하는 데 기여한다.