**문항 1. 사회공학이 무엇인지 서술하시오. (30점)** 사회공학이란 ‘컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 바탕으로 사람을 속여, 정상 보안 절차를 깨트리고, 비기술적 수단으로 정보를 얻는 행위’를 말한다.

공격 과정 속에서 기술적인 부분 보다는 인간적 상호 작용에 기대어 이루어지는 부분이 더 많다. 개인의 신뢰를 저버리는 방법으로 공격하거나, 의심 없이 접근 가능한 루트에 기대어 공격이 이루어 지기 때문에 방어가 어렵다.

 **문항 2. 사회공학적 해킹이란 무엇인지 서술하시오. (40점)** 사람의 취약점을 공략하여 원하는 정보를 얻는 해킹방법. 지인으로 위장하여 원하는 정보를 얻어내는 방법이 가장 일반적인 방법이다. 가장 대표적인 방법으로는 ‘피싱’을 들을 수 있다. 가까운 지인이 보낸 메일이나 링크를 가장하여 악성 코드를 유포하거나, 개인정보를 빼내는 수법이 있다. 이는 복잡한 컴퓨터 시스템보다 사람의 마음이 더 접근하기 쉽다는 점을 이용한 해킹 방법이다.

 이를 위해서는 정보 수집-관계형성-공격-실행 단계로 구성이 되는데, 이는 대단히 상식적인 인간관계 성립 단계와 비슷하여 완벽한 방어를 하는 것은 대단히 어렵다.

 **문항 3. 사회공학 공격 대상을 서술하시오. (30점)**

사회 공학적 공격의 대상으로는 크게 네 가지를 꼽을 수 있다. 정보의 가치를 잘 모르는 사람, 특별 권한을 가진 사람, 제조사, 해당 조직에 새로 들어온 사람이다. 정보의 가치를 제대로 알지 못하지만 접근가능한 범위에 있는 사람은 해당 정보의 손 쉬운 유출을 초래할 수 있다. 또한 회사의 IT 팀과 같이 직원들의 패스워드 변경 권한이나 업무 정보에 쉽게 접근 할 수 있는 사람도 공격 대상 중에 하나다. 회사의 시스템과 서비스를 제공하거나 유지 보수하는 제조사 또한 쉬운 공격 대상이다. 이러한 제조업체의 경우 한번 뚫으면 다양한 고객사의 정보까지 접근 할 수 있다. 마지막으로는 해당 조직에 새로 들어온 사람이 있는데, 새로운 규칙과 환경에 적응하기 위하여 노력하는 동안은 경계심이 낮아져 인사팀 혹은 IT 팀인 척 메일을 보내 공격하기 손쉬운 대상이다.