1. 사회공학이 무엇인지 서술하시오

사회공학의 사전적 정의는'컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여, 정상 보안 절차를 깨뜨리고 비기술적인 수단으로 정보를얻는행위'이다. 사회공학은 조직의 특성에 따라 보안에 큰 문제를 야기하기도 하는데 주변을 살펴보면 조직의 구성원에 의해 정보가 상당히 쉽게 유출되는 모습을 볼 수 있다. 일례로 정보를 얻기 위해 '혹시 어디어디에 아는 사람 있어?'라고 묻는 것도 사회공학을 이용한 사례에 해당한다. 실제로 조직 내에서 패스워드 점검 차원 등을 이유로 개인 패스워드를 물으면 상당수의 직원이 자신의 패스워드를 바로 알려주곤 한다. 그리고 약 2/3에 해당하는 사람이 업무상 패스워드와 개인용 이메일 혹은 인터넷뱅킹 패스워드를 동일하게 사용한다. 이런 사실을 악용할 경우 상당히 위험해 진다. 사회공학은 첩보/해킹의 한 분야가 학술적으로 정립된 것이라고도 할 수 있다. 사회공학 공격을 행하는 사람들은 어떤 학자나 기술자라고 보기는 어렵고, 컴퓨터 보안을 깨는 사기꾼이다. 고도의 컴퓨터 기술을 필요로 하는 다른 해킹의 분야와 달리 사회공학은 인간의 심리를 이용하는 경우가 많다. 필연적으로 사회공학만을 사용하기보다는 다른 해킹의 분야와 같이 사용되는 경우가 많다. 사회공학이라는 단어는 컴퓨터가 존재하기 이전부터 존재했을 정도로 유서가 깊다. 그 특성 상 해킹이 아닌 다른 인간의 심리를 다루는 분야와도 관련이 많은 편이다. 고로 일상생활에서도 유용한 기술이다.

2. 사회공학적 해킹이란 무엇인지 서술하시오

일반적으로 사회공학은 사람들의 심리적, 사회적 관계를 이용하여 사기를 치는 아주 오래된 수법으로서 사회공학이란 용어가 새롭고 어렵게 느껴질 뿐 결코 새로운 것이 아니며 우리 곁에서는 빈번히 일어나고 있는 현상이다. 사회공학의 사전적 의미는 사회 행동의 과학적 연구로 얻어진 기초적인 식견이나 법칙을 응용하여 사회생활에서 당면하는 여러 가지의 실천 상의 특수 문제를 해결하고 또 그 때문에 필요한 기술적 제 문제에 관하여 연구하는 학문이라 설명된다. 하지만 정보 보안에서의 사회공학이란 좀 다르다. 정보 보안에서의 사회공학은 설득과 감언이설을 통해 자신의 신분을 속이거나 사람들을 교묘히 조종하는 것을 의미한다. 그 결과, 사회 공학자는 기술에 대한 특별한 지식이 없어도 사람들을 이용해 정보를 입수할 수 있다. 따라서 사회공학적 해킹은 시스템이 아닌 사람의 취약점을 공략하여 원하는 정보를 얻는 공격 기법을 통칭한다. 불확실성이 내포되어 있는 보안 대비책은 취약성을 지닐 수밖에 없음을 고려할 때, 많은 변수를 가지고 있는 인간이라는 요소는 시스템 체인 내에서 취약점으로 작용할 수 있다. 전화사기, 이메일 피싱, 우편물 등을 통한 개인 정보 도난 등 특별한 기술 없이도 손쉽게 기본 정보를 얻어내는 비 기술적인 침임 방법이라고도 한다. 1990년대 가장 유명한 해커였던 케빈 미트닉은 사회공학적 해킹법을 가장 잘 사용하기로 유명하였다. 그는 시스템을 이루는 노드들 중 인간을 공략하는 사회공학적 기법이 가장 효과적인 공격법이었다고 회고한다. 실제로 그가 저지른 해킹의 상당수가 전화

통화로 시작되었으며, 모토로라의 최신 핸드폰의 핵심 소스코드를 전화 몇 통화 만으로 탈취해 낸 것은 매우 유명한 실화이다. 사회공학은 해킹보다 더욱 심각한 문제로 원래 사람이란 예측 불가능한데다 조작이나 설득에 걸려들기 쉬운 점을 악용한다. 보안 침해 피해를 당했으며 지속적으로 당할 가능성이 있는 대다수 경우는 기술적인 해킹이나 크래킹 때문이 아니라 사회공학에 기인한 것하고 있다. 최근에 피싱(Phishing), 파밍(Pharming), 문자메시지를 이용한 스미싱(SMiShing), 불특정 다수에게 전화를 걸어 개인 정보를 빼내는 비싱(Vishing) 등 사회공학적 위협이 증가하면서 사회공학에 대한 관심도 높아지고 있다. 현재 다양하고 정교해진 보안장비로 기술적 침입이 어려워지고 있어 해커들이 특별한 기술이나 지식 없이도 쉽게 사용할 수 있는 사회공학이 보안에 있어 향후 그 어떤 것보다 심각한 문제가 될 것이다.

3. 사회공학 공격 대상을 서술하시오

사회공학을 이용한 공격의 흐름은 다음과 같다. 가장 먼저 공격 대상의 가족 관계나 직장 생활, 사회적 활동 등의 다양한 자료를 수집하고, 수집된 자료를 가지고 관계를 형성하여, 오프라인 모임이나 온라인을 통해 대상에게 접근한 후, 신뢰감을 형성하였다고 판단될 경우, 그동안 수집된 정보를 바탕으로 공격을 감행하는 순서를 갖는다. 공격 대상은 공격자를 믿기 때문에, 공격자의 요청을 직접적으로 수행함으로써 실질적인 피해를 입게 되고, 공격자는 확보한 유무형의 자산을 이용하여 실질적인 목적을 수행한다. 이와 같은 공격 대상의 특징으로는 정보의 가치를 모르는 사람, 특별한 권한을 가진 사람, 제조사 또는 판매사, 조직에 새로 들어온 사람 등을 들 수 있다.