**사회공학이 무엇인지 서술하시오.**

사회공학이란 보안학적 측면에서 기술적인 방법이 아닌 사람들 간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 기법, 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 침입 수단이다. 즉 첩보/해킹의 한 분야가 학술적으로 정립된 것이라고도 할 수 있다. 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.

사실 아무리 기술적인 보안을 완벽히 하더라도, 물리적이거나 인간적인 부분까지 완벽히 막기는 어렵다. 제아무리 서버에 고도의 암호화를 했다고 하더라도, 직원을 속여 직원의 계정과 암호를 빼돌리면 답이 없기 때문이다.

컴퓨터 해킹이 아닌 분야에서 사람을 속이거나 정보를 얻어내는 방법에 대해서는 사회공학 문서보다는 심리전, 독심술 문서 참조바람. 사실상 기술정보 말고 휴민트를 수집하는 FBI나 CIA 같은 정보기관들은 밥먹고 하는게 사회"공학"이라 하기 민망할 정도로 자주하는 첩보기술이긴 하다.

## 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, 파밍, 문자메시지를 이용한 스미싱 불특정 다수에게 전화를 걸어 개인 정보를 빼내는 비싱등 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.

## 사회공학 공격 대상을 서술하시오.

사회 공학 기법을 사용하는 공격자는 공격 대상이 되는 특정 인물을 선정하였다면 다음과 같은 흐름으로 사회 공학 기법의 공격을 진행하게 된다.

① 정보 수집

공격자는 제일 먼저 공격 대상과 관련된 가족 관계, 직장 생활 그리고 사회 모임 등의 개인적이거나 사회적인 활동 등과 관련된 다양한 정보들의 수집을 시도하게 된다. 공격자는 이 단계에서 수집한 다양한 정보들을 다음 단계인 관계 형성을 위해서 사용하게 된다.

​

② 관계 형성

1 단계인 정보 수집 단계에서 공격자는 공격 대상과 관련된 다양한 정보들을 충분히 수집하였다고 판단할 경우, 공격자는 이제 공격 대상과 직접적인 관계를 형성하기 위해 2 단계인 관계 형성 단계로 발전하게 된다. 인간 기반 또는 컴퓨터 기반의 수단 들을 공격자는 적절하게 활용하여 공격 대상에게 접근하게 된다. 이 관계 형성 단계에서는 사회 공학 기법에서는 절대 빼놓을 수 없는 '가장이라는 것이 공격자에 의해 발생하게 된다.

'가장' 이라는 의미 자체에서 알 수 있듯이 공격자는 공격 대상에게 자신의 본 모습을 숨기고 다른 누군가로 위장하여 접근하게 된다. 이렇게 다른 누군가로 가장하여 공격 대상에게 접근하는 것은 공격 대상이 가질 수 있는 경계심을 없애고 신뢰할 수 있는 사람이라는 신뢰감을 형성하기 위한 것이다. 이 신뢰감을 바탕으로 공격자는 자신이 가진 특수한 목적을 달성하기 위한 사항을 다음 단계인 공격에서 요청하게 된다.

​

③ 공격

세 번째 단계인 공격은 공격자가 수집한 다양한 정보들을 바탕으로 공격 대상과 충분한 신뢰감을 형성하였다고 판단할 경우에 진행하게 된다. 특히 이 세 번째 단계로 넘어가기 위해서는 공격자 자신을 공격 대상이 더 이상 의심하지 않는다는 판단이 중요하게 작용하게 된다. 이러한 신뢰 관계가 충분히 형성이 되면 공격자는 자신의 특수한 목적을 이룰 수 있는 사항을 공격이라는 단계에서 공격 대상에게 요청하게 된다.

​

④ 실행

마지막 실행단계에서 공격 대상은 공격자가 요청한 사항에 대해 직접적인 실행으로 옮김으로써 이로 인해 실질적인 피해가 발생하게 된다. 그리고 공격자는 요청 사항으로 인해 확보한 유형의 또는 무형의 자신을 이용하여 실질적인 목적을 수행할 수 있게 된다.

​