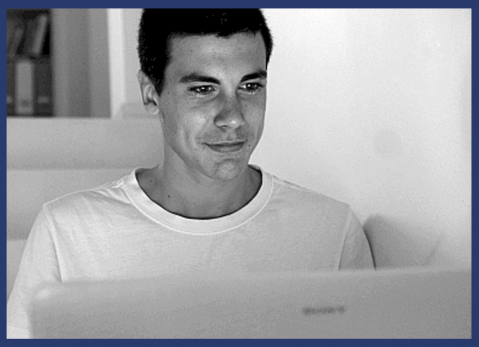
Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 1
BEING A HACKER

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

Warning – WORLD

Hacker Highschool Project(HHS)는 학습 도구로 만들어졌지만, 일부 내용의 경우 오용될 시 물리적 피해가 발생할 수 있습니다. 또한 특정 기술들로 인한 파급력과 영향력을 충분히 숙지하고 있지 못할 시 추가적인 문제가 발생할 수 있습니다. 학생들이 배운 내용들을 활용하는데 있어 주의가 필요하지만 적극적으로 배우고 연습할 수 있도록 지도해 주시기 바랍니다. 하지만 배운 내용들을 악의적으로 사용해 발생한 문제들에 대해 ISECOM은 책임을 지지 않습니다.

해당 교제에서 배울 내용들과 연습문제들은 공개되어 있으며 ISECOM에서 제시하는 다음의 조건들을 따를 시 누구나 사용할 수 있습니다:

HHS의 자료들은 초등학생, 중학생, 고등학생들에게 무료로 제공됩니다. 해당 자료들은 판매를 목적으로 생산될 수 없습니다. 대학, 직업학교, 단기과정, 방학특강 등에서 실시하는 어떤 학습 과정에서도 허가 없이 학생들에게 해당 자료들로 인한 비용을 부과해서는 안 됩니다. 허가증을 받기 위해서는 HHS 홈페이지의 http://www.hackerhighschool.org/licensing.html를 방문하여 라이센스 섹션을 참조하시기 바랍니다.

HHS는 공개 참여를 통한 오랜 노력과 여러 사람들의 지원으로 만들어졌습니다. 해당 프로젝트에 도움을 주고 싶으시다면 허가증 구매, 기부, 후원을 통해 HHS에 일조 하실 수 있습니다.

Warning – KOREA

HHS 는 ISECOM의 프로젝트입니다.
HHS 외 ISECOM의 모든 프로젝트의 한국 내에서의 관리 및 감독 등의 모든 권한은 ISECOM Korea 에 있습니다.
본 문서의 용도는 개인 학습용이며 무료 공개자료입니다.
해당 용도 외 사용 시 법적인 처벌을 받으실 수 있습니다.
해당 용도 외 문의는 ISECOM Korea 에 문의해 주시기 바랍니다.

목차

도움을 주신 분들

Pete Herzog, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Shaun Copplestone, ISECOM
Greg Playle, ISECOM
Jeff Cleveland, ISECOM
Simone Onofri, ISECOM
Tom Thomas, ISECOM
Dzen Hacks

ISECOM Korea

왕응석 EungSeok Wang
정진우 JinWoo Jung
박영후 YongHoo Park
최홍선 HongSeon Choe

해킹을 향한 열정

Introduction by Pete Herzog

여러분은 해커에 대해 많이 들어보았을 것이다. 그 중 분명한 사실은 해커들이 정말 잘하는 것은 "무언가를 발견해내는 것"이다. 해커들은 자발적으로 활동하며 자신이 가진 것을 잘 활용하여 문제를 해결해 내는 능력과 창의력을 가지고 있다. 해커들은 어떤 대상에 집중하면 그것을 통제하는 방법과 어떻게 다른 것으로 변화 시키는지를 알아낼 수 있을 때 까지 작동 방식을 철저히 탐구한다. 이렇게 특정 대상의 기능을 깊이 있게 파고드는 적극성을 기반으로 아무리 새롭고 대단한 아이디어라도 자기들 방식으로 다시 한 번 파고든다. 그뿐 아니라 과학적 호기심을 해소하기 위해 또다시 실수를 하는 것을 전혀 겁내지 않고 같은 실수라도 동일한 결과를 내는지 확인 할 수 있는 기회로 삼는다. 이러한 사고방식으로 인해 해커들은 실수를 커다란 실패나 시간 낭비로 여기지 않고 다른 새로운 것을 배울 수 있는 과정으로 여긴다. 해커들의 이러한 특징들은 진보를 이뤄내기 위해 사회가 필요로 하는 능력들이다.

> "언론에서 해커라고 불리는 사람들이나 해킹으로 인해 문제에 처한 사람들은 사실 진짜 해커라고 볼 수 없다."

해커는 현장에서 일하는 실험 과학자와 유사하다. 이들은 일반적으로 알려진 가설을 따르기보다는 자신의 감정에 따라 일을 진행하는 경우가 많기 때문에 가끔은 “매드 사이언티스트”라 불리는 것이 더 잘 어울리기도 한다. 이렇게 직관을 따르는 것은 전혀 잘못된 일이 아니다. 일반적인 통념에 따르지 않은 사람들이 있어왔기 때문에 여러 흥미로운 물건들이 탄생 할 수 있었다.

수학자 조지 칸토어(Georg Cantor)는 무한과 집합이론을 처음 제시하여 많은 동료 수학자들의 분노를 받게 되었다. 이들은 이 새로운 이론을 수학을 감염시킨 “심각한 질병”이라고 부를 정도였다.

니콜라 테슬라(Nikola Tesla) 역시 자신의 시대에 “매드 사이언티스트”로 여겨졌지만 그 누구보다도 전기의 흐름에 대해 많은 것을 알고 있었다. 테슬라는 AC전류에서 사용할 수 있는 브러시리스 모터를 거의 최초로 만들었지만 테슬라 이펙트와 테슬라 코일만 알려져 있다.

젠메르와이스(Ignaz Philipp Semmelweis)는 질병의 확산을 막기 위해서는 의사가 환자를 치료한 후 손을 씻어야 한다는 것을 발견했다. 이 아이디어를 직접 실행해 본 결과 실제로 질병의 전파가 감소된다는 것을 알아냈다. 하지만 당시 학계의 세균에 관한 지식 수준으로는 이해 할 수 없는 생각이었고 동료 의사들은 손 소독 과정을 번거로운 절차로 여겼다.

여러분이 해커에 대해 알고 있는 것은 대부분 사실과 거리가 멀다. 흔히들 해커가 여러분의 컴퓨터에 침입해 계정을 탈취하고 이메일을 엿보며 웹캠을 통해 감시하고 소리를 엿들을 수 있다고 여기지만 사실이 아니다.

몇몇 해커들은 네트워크 보안을 그저 하나의 도전으로 여긴다. 이들은 시스템을 속이는 방법에 대해서 취미 삼아 알아보기도 하지만 실제로 하는 것은 네트워크 설치자와 설계자의 생각을 뛰어넘고, 가능한 많은 정보를 알아내기 위해 노력한다. 그럼으로써 시스템의 규칙, 운용방법을 알아내고 OS와 주요 시스템들을 이해하며 누가 시스템 이용자인지 관리자 인지를 파악한다. 이후에도 이 정보들을 발판삼아 정보들을 계속해서 탐색해 나간다. 해킹이란 것은 좀 더 안전하고 향상된 기술들을 만들기 위해 필요한 매우 유익한 활동이라 할 수 있다.

불행히도 가끔은 해킹이 범죄에 사용되어 불법적이고 파괴적으로 사용되기도 한다. 그리고 뉴스에서는 이러한 해커들을 주로 다루기에 해커의 이미지가 이상하게 전파된 것이다.

해커는 다른 사람의 SNS 계정에 접근해 글을 올리거나 **어깨너머로(shoulder-sufs)** 암호를 알아내서 로그인하는 사람이 아니며 이것은 해킹이 아니다. 해킹 툴을 다운 받아**(script kiddie)** 다른 사람의 이메일에 침입하는 사람 또한 해커가 아니며 해킹 또한 아니다. 이러한 사람들은 그저 도둑이거나 범죄자일 뿐이다.

> 해킹은 연구 활동과 같다. 여러분은 어떤 것을 이해하기 위해 지속적으로 반복해서 연구해 본 적이 있는가? 멀쩡한 기계를 뜯어서 어떤 장치들이 들어있고 어떤 작용을 하는지 알아본 적이 있는가? 장비들을 바꾸거나 조정하면 어떤 일이 발생하는지 알아본 적이 있는가? 이처럼 작동 원리를 조사해서 창의적으로 수정하고 원하는 결과를 얻기 위한 시도를 한 적이 있다면 여러분 역시 해킹을 한 적이 있는 것이다.

인터넷, 프로그램, 시스템, 장비, 여러 제작공정들 역시 해킹과 연관이 있다. 이러한 것들을 만든 것이 해커라고 볼 수도 있기 때문에 이런 분야에서 활동하는 해커들을 많이 볼 수 있다. 이 외에, 다양한 분야와 산업에서도 많은 해커들을 만날 수 있고 모든 해커들에게는 한 가지 공통점이 있다. 바로 어떤 것의 작동원리를 이해하기 위해 시간을 투자하고 새로운 방식을 적용할 줄 안다는 것이다. 해커들은 제작자와 같은 방식으로 접근하지 않고 더 큰 잠재력을 발견하여 해킹해 새로운 것을 만들어낸다.

> 해킹으로 많은 성과를 내고 늘 겸손한 태도로 해킹에 몰입해야만 훌륭한 해커가 될 수 있다는 것을 잊지 말자.

돌멩이를 던지는 것과 같이 **해킹 그 자체로는 범죄와 상관이 없다.** 남에게 상해를 입힐 목적으로 돌을 던진 것이 아니라면 그걸 범죄라고 할 수 없다. 하지만 의도가 어떻든 만약에 다른 사람이 돌에 맞았다면 보상을 해줘야 한다. **해커 프로파일링 프로젝트(Hacker Profiling Project)**라고 불리는 ISECOM프로젝트의 조사에 의하면 대부분의 해킹 피해는 어리고 경험 없는 해커들에 의해 발생한다. 이는 길거리에서 재미로 돌멩이를 던졌다가 차에 흠집을 내거나 유리창을 깨는 것과 같다. 의도적으로 피해를 입힌 것은 아니지만 당연히 보상을 해야 한다. 그러니 해킹을 할 때는 다른 사람들의 소유물이 아닌 자신의 것을 해킹 대상으로 한정하자.

하지만 자신이 구입한 것을 해킹 할 때도 범죄가 되는 경우가 있다. 자신이 산 프로그램, 음악, 영화를 해킹했는데도 기소되는 일이 발생하기도 한다. 대부분의 소프트웨어의 경우 아무리 자신이 돈을 내고 구입했다 하더라도 해킹이 허용되지 않는다. 소프트웨어를 구입할 때 함께 오는 계약서와 **최종 사용자 라이센스 동의서(End User License Agreement)**에서 이를 허용하지 않는다. 만약 소프트웨어를 깔 때 읽지 않았거나 설치 후에 읽었다 할지라도 계약 내용에 동의한 것으로 간주된다. 그러니 자신의 물건을 대상으로 혼자 해킹을 하더라도 이러한 사항을 주의해야 한다.

왜 해커가 되는가?

인간 게놈지도를 만드는 과학자들을 주목해보자. 암호화가 적용된 패스워드를 해독하는 것은 힘들기 때문에 이들은 암호해독을 위해 만들어진 특별한 방법을 사용하여 패스워드를 해독한다. 계층적 **무작위 대입(brute-forcing)**을 사용하여 **크랙킹(cracking)** 속도를 높여 패스워드를 획득하는데 이때 **단방향 해시(one-way hash)** 형태로 암호화되어 있는 경우가 많다. 게놈 분석 과학자들은 게놈을 여러 조각으로 나눈 후에 한 번에 그 짝을 찾는 방법을 사용한다. 이 방법을 사용하여 나온 조합들을 사용하여 서로 이어져 있는 게놈 연결체들을 찾아낸다. 여러 개의 대응하는 암호조각들을 동시에 찾아내는 크랙킹 기법을 사용하면 하나씩 찾아내는 것보다 훨씬 더 빠르게 암호화된 패스워드를 해독할 수 있다. 33억 개에 달하는 인간 게놈의 짝을 찾아 배열 순서를 밝힐 때 이러한 동시 판별법을 사용하여 해석 속도를 끌어올린다.

부엌에서 요리사가 맛있는 아이스크림을 만들기 위해 액체 질소를 냉각제로 사용하거나 케첩을 만들기 위해 토마토와 여러 재료들을 활용하는 순간에도 해킹 활동을 목격할 수 있다. 요리사들은 여러 가지 재료들을 사용해서 새로운 요리들을 만들어낸다.

화학자 역시 수 세기동안 여러 화학 성분과 화합물들을 해킹해오고 있다. 분자는 온도, 고도, 수압 등에 의해서 그 움직임의 특성이 변화하는 불규칙적인 성질을 가지고 있기 때문에 화학자는 각 화학 성분들의 특성을 철저하게 이해해야 한다. 이러한 이해 활동은 수없이 많은 식물들의 잎, 줄기, 뿌리, 열매 등이 가진 화학적 성질을 연구하는 약학 분야에서 잘 나타난다. 이 분야의 연구자들은 새로

운 물질을 만들어내기 위해서 화학 성분들을 추출하고 조합하며 끊임없이 새로운 시도들을 하고 있다.

기업에서도 해킹을 사용해서 시장과 구매자들의 행동들을 연구한다. 기업은 관심을 가진 사업 분야를 이끌어가는 요소가 무엇인지 밀도있게 연구하며 원하는 결과를 얻기 위해서 여러 요소들을 변화시키고 영향을 미치는 방법을 이해하려고 끊임없이 노력한다. 때로는 실제 상품을 해킹하기도 하고, 때로는 그들이 당신을 해킹(광고 및 다른 수단을 통하여)하기도 한다. 자세한 내용은 사회공학(Social Engineering) 레슨에서 다룰 것이다.

전쟁에서도 해킹은 점차 그 비중이 커지고 있다. 고도로 훈련된 군인들은 해커들이 그러듯 주변상황을 잘 활용하고 창의력을 발휘하여 임무를 달성한다. 암호 해석요원, 정보 분석가, 지휘관들은 기본적으로 해킹 기술들을 사용하여 적의 정체, 목적, 활동 방법들을 연구하여 이들의 약점을 이용할 방법을 찾아낸다. 컴퓨터와 네트워크에 대한 국가의 의존이 계속해서 커짐에 따라 해킹을 이용한 사이버 공격과 방어는 군대의 전투와 정보 활동에서 필수적인 요소로 자리 잡고 있다. 이러한 심각성을 이해한 여러 국가 보안 기관들은 해커 컨퍼런스에 참여하여 실력 있는 해커들을 스카웃하고 있다.

해커가 되는 진짜 이유는 정말 강력한 힘을 가질 수 있기 때문이다. 훌륭한 해킹 기술을 가지고 있다면 정말 멋진 일들을 할 수 있다. 목표로 한 대상을 조절하고 통제할 수 있을 정도로 그 작동 원리를 이해했다면 어마어마한 능력을 손에 지니고 있다고 볼 수 있다. 무엇보다도, 이러한 능력을 활용하여 자기 자신과 다른 사람들을 보호할 수 있다.

현대에 들어 대부분의 사람들은 인터넷을 이용하여 사람들과 관계를 쌓고, 직업을 찾으며, 돈을 벌고 있다. 정보라는 것은 귀중한 자산이지만 위험 요인이 될 수도 있다. 해커들은 이러한 정보들을 다른 누구보다도 잘 지켜낼 수 있으며 자신들의 데이터에 어떤 일이 발생하고 있는지 알아 낼 수 있다. 또한 자신이 원하는 정보만을 노출시키며 사생활을 지킬 능력을 가지고 있다. 아주 약간이라도 부정적인 정보가 있다면 악용될 여지가 있기 때문에 해커들은 평범한 사람들과 비교할 때 학교와 일터, 생활 곳곳에서 상대적인 우위를 가지고 있다고 볼 수 있다. 이는 절대적인 사실이다.

남에게 피해만 주지 않는다면 어떤 것이든 해킹하라.

어떻게 해킹을 하는가

어떻게 해킹을 하는지 설명하는 것은 평균대에서 백덤블링 하는 방법을 말로 풀어 설명 하는 것과 마찬가지다. 아무리 상세한 설명을 듣는다 해도 처음부터 백덤블링을 해낼 수는 없다. 실제 연습을 통해 기술, 감각, 직관력을 길러야만 땅과 키스하는 것을 피할 수 있다. 하지만 여러분이 연습을 지속하는데 도움을 주기 위해 해줄 말이 있다.

우선, 해킹이 실제로 어떻게 실행되는지에 관한 몇 가지 비밀에 대해서 알 필요가 있다. 이를 위해서 **OSSTMM**(www.osstmm.org)의 자료들을 몇 가지 참고할 예정이다. OSSTMM은 **Open Source Security Testing Methodology Manual**의 약자로 많은 전문 해커들이 공격과 방어를 계획하고 실행할 때 참고하는 주요 문서로 여러분들이 철저하게 익힌다면 해킹의 정수를 이해할 수 있을 것이다.

목표달성을 위한 두 가지 방법

예를 들어, 원하는 것을 얻는 방법에는 크게 두 가지가 있다. 자신이 직접 원하는 것을 취하거나 다른 사람이 얻게 한 후에 자신이 전달받는 방법이 있다. 즉 이 세상에 존재하는 것을 얻기 위해서는 원하는 것과 사람간의 **상호작용(소통:Interactions)**이 필요하다. 동의하는가? 그게 의미하는 것은 보호를 위한 도구는 사람과 특정 자산과의 관계를 단절시켜야 한다는 것이다. 하지만 커다란 금고 안에 보호대상을 넣어두는 것이 아니라면 모든 관계를 끊어내는 것은 불가능하다. 가게는 손님을 위해 자신의 자산이자 보호물을 선반에 진열해야 하고 기업은 정보자산을 전달하기 위해 메일서버를 거쳐야 한다.

이 모든 과정이 바로 상호작용이다. 상호작용을 거치는 몇몇 사람들과 자산들의 경우에는 서로 간에 주기적인 상호작용을 통해 **신뢰관계(Trust)**가 생성된다. 하지만 익숙하지 않은 대상들 간에 상호작용이 있을 경우에는 **접속(Accesses)**과정을 거쳐야 한다. 그러니 자신이 원하는 것을 얻기 위해서는 접속 과정을 거치거나 신뢰관계가 있는 대상을 속여 원하는 자산을 취하게 한 후에 그것을 받아내는 방법을 거쳐야 한다. 이를 기초로 생각해 보자면 보호 시스템은 익숙하지 않은 대상들에게서 자산을 지키는 것과 신뢰관계가 있는 대상들로부터 자산을 지키는 것으로 나눌 수 있다.

Exercise

1.1 검색엔진을 도구로 쓰는 상호작용에는 무엇이 있는가? 접속 과정을 거치는가? 아니면 신뢰관계에 있는가?

1.2 자전거 거치대의 자전거를 얻기 위해 이용해야 하는 접속 정과 신뢰관계의 예를 들어보자.

1.3 다른 사람의 메일 계정에 접속하기 위해 이용해야 하는 접속 과정과 신뢰관계의 예를 들어보자.

Feed Your Head: Espionage

해킹을 사용한 각종 침투방법을 이용해 외국 정부가 가진 정치적, 군사적 정보를 획득하는 것을 **첩보활동(espionage)**이라고 한다. 만약 대상이 외국 정부가 아닌 타국의 기업을 대상으로 한다면 **경제첩보활동(economic espionage)**라고 한다.

사적인 개인정보를 파헤쳐 공개적으로 망신을 주기위해 사용하는 해킹을 **신상털이(DoXing)**라고 한다. 특정 인물이나 회사에 공격을 하기 위해 공적인 정보를 해킹하지만 범죄는 아닌 경우 **다중정보검색(document grinding)**이나 **공개출처정보(OSInt: Open Source Intelligence)**활용이라고 부른다.

특정 회사의 네트워크, 시스템, 애플리케이과 장비들을 이해하기 위해 해킹을 실행하지만 시스템에 실제로 침입하지 않고 정보를 획득하는 방식을 **네트워크 조사(network surveying)**라고 한다.

비록 그 방법이 무례하거나 비열하게 여겨질 수도 있지만 어떠한 법도 어기지 않고 경쟁상대의 정보를 획득하기 위한 해킹 방법을 **경쟁정보(competitive intelligence)** 획득 활동이라고 한다.

그렇다면 합법적이지만 무례한 방법은 과연 무엇일까? 상대방으로부터 정보를 얻기 위해 스트레스를 주거나 걱정을 하도록 하는 상황을 입힌 예를 생각해보자. 상대방에게 직접적인 상해를 입히지 않는 한 거짓말을 한다고 잡혀가지는 않는다. (물론 공공장소에서 큰소리로 불이 났다는 거짓말을 하여 혼란을 야기하는 것을 금지하는 법률은 존재할 수 있다)

한 회사가 공장건설을 계획하고 있을 때 그 위치가 궁금한 해커가 있다면 우선 다중정보검색(document grinding)을 활용해 누가 의사 결정권자인지를 알아내야 한다. 그 후 사무실에 전화해 해당 인물이 그동안 방문한 도시와 공장들이 무엇인지 확인해야 한다. 물론 이러한 민감한 정보를 쉽사리 알려줄 리가 없기 때문에 해커는 상대방을 속여 필요한 정보를 얻어내야 한다. 그런 방법을 생각해 내는 것은 그다지 어렵지 않다.

해커 : 안녕하세요. 여기는 병원입니다. 댁의 따님 때문에 전화 드렸습니다.
상대방 : 아, 그래요? 딸애한테 무슨 일이 생겼나요?
해커 : 그게.. 따님이 계속해서 코피를 흘리는데 멈출 수가 없네요. 최근에 따님이 공장에서 사용하는 화학물질같은 유해물질에 노출된 적이 있나요? 이런 경우는 아주 드문 경우라 그 외의 상황은 생각하기 힘드네요. 혹시 생각나는게 있으신가요?
상대방 : (아는 모든 정보를 말한다.)

이런 방법을 불법이라고는 볼 수 없지만 불필요한 스트레스를 유발하는 것은 사실이다. 또한 부모에게 이러한 걱정을 하게 하는 것은 비열한 방법이기도 하다.

세상을 뒤집기 위한 해킹

해킹은 상호작용이 아니다. 여러분은 그것을 알고 있다. 몇몇 사람들은 정치는 상호작용이라고 말한다. 그럴 수도 있지만 당신은 아마 해킹이라는 것은 단순히 보안을 깨는 것이라고 생각할 것이다. 때때로 그것은 맞는 답이 될 수 있다. 해킹의 진정한 목적은 대상을 완벽하게 통제하고 때로는 변화시키는 방법을 연구하는 것이다. 그동안 배운 기본 개념들을 활용하여 목표물과의 상호작용을 이해하고 그게 실제 세계에서 무엇을 의미하는지 이해하는 것은 침투, 발견, 발명에 있어 필수적인 조건들이다. 이런 방법들을 익힘으로써 우리가 가진 것들을 온전히 활용하여 원하는 목표를 이룰 수 있고 보안이라는 것을 이유로 우리가 소유하고 있는 것을 멋대로 조정하려 하는 것을 막을 수 있다.

여러분이 무언가를 샀을 때 일부 회사들은 강제적이거나 은밀한 방법을 사용하여 자신들이 정한 기준점 이상으로 상품을 커스터마이징하거나 개조하지 못하도록 한다. 그러니 물건이 고장 났을 때 AS나 교환이 불가능하다는 사실을 받아드릴 수 있다면 해킹을 시도하도록 하자. 자신이 소유한 것을 해킹한다는 것은 그저 소유한다는 것 이상의 의미를 가지며 그 누구도 부인할 수 없을 정도로 온전히 자신의 일부로 만드는 것을 의미한다. 어떤 이들에게는 이게 무섭게 들릴 수도 있겠지만 해킹은 분명히 이점을 가지고 있다. 특히 다른 누군가가 자신이 소유한 것에 접근하지 못하게 하고 싶다면 더욱 더 큰 이점을 누릴 수 있다.

대부분의 사람들에게 보안이란 지키고자 하는 대상을 자물쇠, 경보기, 방화벽 등의 각종 보안장비들을 장착한 장소에 집어넣는 것을 의미한다. 하지만 이러한 보안장비들이 언제나 효과를 발휘하는 것은 아니고 오히려 **공격지점(Attack Surface)**을 증가시키는 문제를 가져올 수 있다.(공격지점은 공격자가 활용할 수 있는 모든 지점, 방법, 상호작용을 의미한다.) 여러분은 현재 대량 생산품, 시범상품, 크라우드 소싱을 통한 갖가지 상품들을 쉽게 살 수 있는 세상에서 살고 있다. 그러니 여러분은 자신의 보안을 해킹해야 한다. 시스템을 향상 시키기 위해서는 제품을 세밀히 분석해 어떤 지점에서 오류가 나는지, 변화를 주기 위해서는 어떻게 해야 하는지를 연구해야 한다. 여러 번의 해킹을 통해 제품을 산 회사가 기본 설정으로 초기화 시키지 못하게 막을 수 있다.

해킹을 통해 보안을 무너뜨리는 것은 해킹의 한 분야일 뿐이라는 것을 명심하자. 보안을 해제하는 방법을 모른다면 여러분이 누리는 자유와 지키고자 하는 사생활을 보호할 방법을 알 수 없다. (여러분은 온라인 상에서 자신이 쓰는 글이나 포스팅하는 것에 대해 전혀 주의를 기울이지 않고 있을 것이다. 하지만 인터넷은 여러분의 기록을 결코 잊어버리지 않고 앞으로도 그러한 기능은 점점 더 향상되어 다른

사람들이 그 잔재를 파고들 수도 있다. 그러니 지금은 중요하다 여기지 않더라도 미래의 자신을 위해 인터넷에 기록을 남길 때는 주의하도록 하자.)

이제 상호작용에 대해 좀 더 깊이 있게 알아보자. 여태까지 상호작용의 기본이 되는 접속과정과 신뢰관계에 대해 배웠다. 다음에 배워야 할 세 번째 상호작용은 **가시성(Visibility)**이다. 가시성은 앞의 두 가지 상호작용처럼 중요한 역할을 한다. 경찰 용어에서 가시성은 기회(opportunity)로 단순화 되지만 해킹에서 가시성이란 상호작용의 대상이 있는지 없는지를 확인하는 것과 관련이 있다. 가시성의 기능을 통해 기만(deception), 착각(illusion), 위장(camouflage)과 같은 새로운 보안 기술들 뿐 아니라 이러한 보안 기술들을 피하거나 우회하기 위한 해킹 기술들 역시 탄생했다.

유명한 은행털이범인 제시 제임스(Jesse James)는 왜 은행을 털었냐는 질문을 받았을 때 "그곳에 돈이 있으니까"라고 대답했다. 즉 제시 제임스는 가시성을 통해 은행이 돈을 가지고 있다는 사실을 인지한 것이다. 은행은 가시성을 가지고 있고 모든 사람들이 은행이 돈을 가지고 있다는 것을 알고 있다. 하지만 모든 것이 가시성을 가지고 있는 것은 아니다. 사실상 프라이버시(Privacy)는 가시성과 반대되는 기능을 가지며 타겟이 되는 것을 피할 수 있는 강력한 기능을 가지고 있다고 볼 수 있다. 위험지역이든 정글이든 인터넷상이든 그 어디에서든지 **노출되는 정보(exposure)**를 줄이거나 가시성을 피한다면 공격의 대상이 될 가능성을 줄일 수 있다.

Exercise

1.4 인터넷이라는 공간은 잘못된 정보를 만들고 그것을 영구화시키기 쉬운 곳이기에 무엇이 진실이고 무엇이 거짓인지 확신할 수 없다. 그렇기에 훌륭한 해커가 되고 싶다면 자신이 알고 있는 사실이 진실인지 확인한 후 학습하는 습관을 가져야 한다. 이런 습관을 가지기 위한 첫 단계로 앞에서 인용한 제시 제임스의 답변이 사실인지 알아보자. 단 하나의 웹사이트만을 이용하지 말고 좀 더 여러 웹사이트와 다양한 방법들을 사용해 보자.

여러분은 인터넷에서 무언가를 찾는데 매우 익숙해져 있다. 다음의 일반 상식들에 관한 진실을 찾아보자:

1.5 이누이트 언어의 이글루(igloo)라는 단어의 기원은 무엇이고 실제로 그 단어가 의미하는 것은 무엇인가? 어떤 종류의 상호작용(소통)을 사용하였는가?

1.6 많은 부모들이 자신들의 아이들이 설탕을 먹으면 정신 사나울 정도로 활동적으로 변한다고 믿고 있는데 그게 사실인가? 아이들이 설탕이나 설탕이든 음식을 먹었을 때 위장에서 실제로 일어나는 반응은 무엇인가?

1.7 대부분의 사람들이 설탕이 충치를 유발한다고 알고 있는데 설탕을 먹었을 때 실제로 입에서 어떤 반응이 일어나고 충치를 유발하는 진짜 원인은 무엇인가?
양치질을 할 때 충치의 원인과 싸우기 위해 어떠한 반응이 일어나고 그 원인을 처리하기 위한 성분을 한 가지 이상 찾아보자. (힌트 : 불소는 정답이 아님)

4단계 접근법

앞에서 이야기 한 세 종류의 상호작용(소통)을 다 이해했다면, 이제 공격지점(Attack Surface)의 기본인 보안의 **다공성(Porosity)**에 대해 배워야 한다. 단어가 의미하는 것처럼 여러가지 상호작용을 거치기 위해 나타날 수 밖에 없는 보안의 구멍을 의미한다. 예를 들어 가게에서는 물건을 팔기 위해 자신의 자산을 진열하여 손님들이 만지고, 카트에 넣고, 살 수 있도록 해야 한다. 물건을 팔기 위해서는 이러한 상호소통이 필요하지만 판매 직원이 창고에서 몰래 물건을 빼돌리는 것과 같이 불필요한 상호소통이 일어나는 것을 알지 못할 수도 있다.

자신을 지키거나 해킹을 하기 위해서는 이 보안의 구멍에 대해 알아야 한다. 이를 위해서는 단순히 해킹대상을 분석하는 것 뿐 아니라 여태까지 배운 세 가지 상호소통에 대해 좀 더 구체적으로 배울 필요가 있다. 이 단계는 **4단계 접근법(Four Point Process: FPP)**이라고 불리며 OSSTMM의 해킹 비법 중 하나이다. 이제, 세 가지 상호작용을 활용하는 분석 방법에 대해 알아보자.

메아리 탐색

우리는 상호작용을 통해 새로운 것들을 발견하고 배우면서 성장한다. 어린 아이들은 다람쥐가 죽는지 확인해 보기 위해 날카로운 것으로 찔러보곤 한다. 이런 것을 **메아리 탐색(echo process)**이라고 부른다. 가장 기초적이고 미숙한 분석 방법으로 동굴에 소리를 지른 후에 반응을 기다리는 것과 같다. 메아리 탐색은 여러 종류의 접속 방법을 타겟에게 적용해 본 후에 그 반응을 확인해 어떤 상호작용을 선택하는 것이 좋은지를 알아보는 과정으로 인과관계에 기초를 둔 탐색 방법이다.

이 방법을 이용하면 빠르게 대상을 탐색할 수 있지만 언제나 정확한 결과를 얻을 수 있는 것은 아니기 때문에 좋은 방법이라고 보기 힘들다. 예를 들어, 보안 테스트에 메아리 탐색을 이용했을 때 아무 반응을 보이지 않는다면 가시성(visibility)을 드러내지 않으니 보안 상태가 좋다고 여길 수 있다. 하지만 적용했던 특정 상호작용에는 반응 하지 않는 보안 모델일 수 있고 이는 보안 상태를 제대로 확인한 것으로 보기 힘들다. 메아리 탐색의 결과가 언제나 정확하다면 곰은 죽은 척 하는 사람들을 건들지 않을 것이고 단순히 곰을 보고 기절하는 것만으로 곰의 공격에서 안전할 수 있을 것이다. 하지만 현실은 그렇지 않다. 가시성을 드러내지 않음으로써 일부 해로운 상호작용을 방지할 수 있지만 모든 상황에 적용되는 것은 아니다.

불행하게도, 많은 사람들이 메아리 탐색만을 이용하여 일상에서 만나는 주변 대상들을 분석한다. 이런 일차원적인 분석 방법에서는 정보의 손실이 다량 발생한다. 병원에서도 예전에는 "이렇게 하면 아픈가요?"식의 일차원적 탐색 방법만을 사용했지만 현재에 와서는 다양한 탐색 방법을 사용하고 있다. 병원이 여전히 과거의 탐색 방법만을 사용해 사람들의 건강을 관리한다면 많은 사람들을 도울 수 없을 것이다. 유일하게 긍정적인 부분은 환자들의 대기 시간이 크게 줄어든다는 것뿐이다. 그렇기 때문에 의사, 과학자, 그리고 해커들은 4단계 접근법을 통해 놓치는 부분들을 최소화한다.

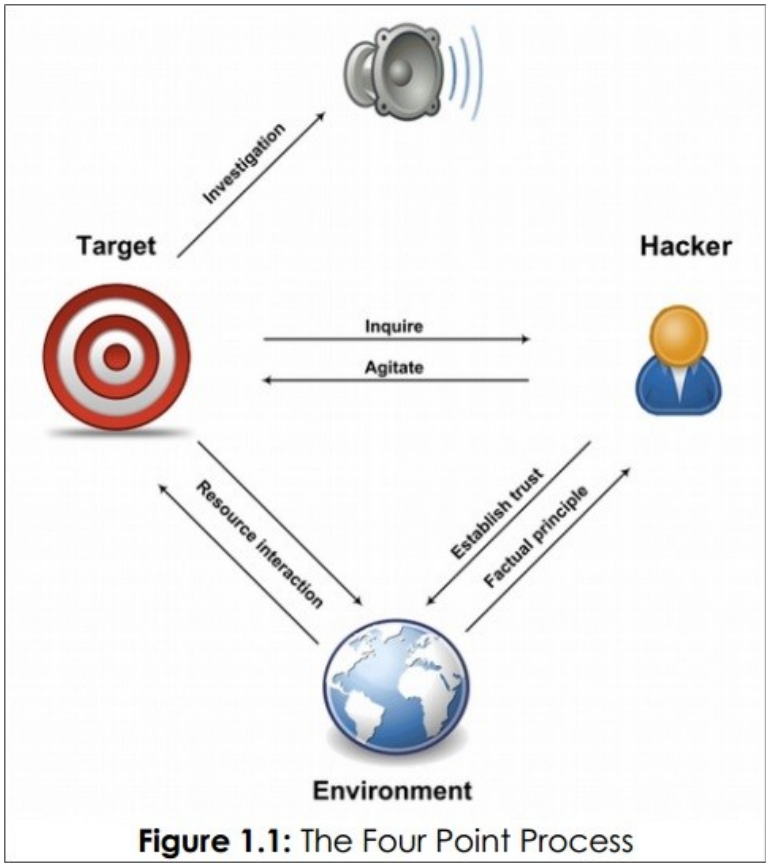


Figure 1.1: The Four Point Process

4단계 접근법은 다음의 네 가지 방법을 활용해 상호작용을 분석한다.

1. 유도 Induction: 목표물이 주변 환경으로부터 어떠한 영향을 받는가? 해당 환경에서 어떻게 행동하는가? 만약 환경에 아무런 영향을 받지 않는다면 아주 흥미로운 상황이다.

2. 검토 Inquest: 목표물이 어떤 흔적을 남기는가? 목표물이 남기는 흔적을 조사하라. 시스템이나 프로세스는 일반적으로 주변 환경과 상호작용할 때 특유의 흔적을 남긴다.

3. 작용 Interaction: 목표물을 찌르면 어떤 반응을 보여주는가? 반응을 유발하기 위한 메아리 탐색법의 일종으로 목표물에게 여러 종류의 상호작용을 시험한다.

4. 조정 Intervention: 목표물을 얼마나 구부려야 부러지는가? 전기와 같이 목표물이 필요로 하는 자원들에 침투해 다른 시스템들과의 상호작용에 간섭한다. 간섭 정도가 어느 정도가 되어야 작동을 멈추는지 확인한다.

병원에서 일어나는 활동에 해당 단계들을 적용해 보겠다.

1. 작용 Interaction: 의사들은 메아리 탐색 방법을 이용해 환자를 진찰하고 그 반응을 살핀다.

팔꿈치와, 무릎 등 여러 곳을 다양한 도구를 이용해 진찰하며 "이렇게 하면 아픈가요?"라고 물으며 탐색한다.

2. 검토 Inquest: 환자의 맥박, 혈압, 뇌파 등에서 나오는 수치(흔적)들을 해석한다.

3. 조정 Intervention: 환자의 항상성, 행동, 일과, 편암함의 정도를 변화시키거나 압박을 주면 어떤 변화가 일어나는지 확인한다.

4. 유도 Induction: 환자가 병에 걸리기 전에 방문한 장소들을 조사한다. 환자가 무엇을 만지고, 먹고, 흡입했는지를 확인해 방문한 곳들이 어떠한 영향을 미칠 수 있는지 조사한다.

Exercises

1.8 앞서 살펴본 것처럼 4단계 접근법은 상호작용을 이해하는데 필수적인 요소들이다. 이제 직접 시도해 보자. 4단계 접근법을 사용해서 시계가 어떻게 작동 하는지와 정확한 시간을 유지하는지 설명해 보자.

무엇을 해킹하는가?

무언가를 해킹하기 위해서는 기본적인 규칙을 정해 놔야 한다. 자신이 해킹하는 것이 무엇인지 확고하게 하기 위한 개념과 용어를 설정해야 한다. **영역(Scope)**은 해킹하고자 하는 대상이 이용할 수 있는 모든 상호작용인, 작업환경(operating environment)을 의미한다.

Feed Your Head: Classes and Channels

해킹의 세계에서 영역(Scope)은 총 세 개의 **분류(Classes)**과 다섯 개의 **채널(Channels)**로 이뤄져 있다.

분류(Class)	채널(Channel)
Physical Security (PHYSSEC)	Human
	Physical
Spectrum Security (SPECSEC)	Wireless
Communications Security (COMSEC)	Telecommunications
	Data Networks

분류(Classes)는 여러분이 걱정할 필요가 없는 부분이며 일반적으로 보안 산업, 정부, 군대에서 공식적으로 사용하는 명칭이다. 분류는 연구(study), 조사(investigation), 운영(operation)분야로 이루어 진다.

채널(Channels)은 특정 자산과 상호소통을 하기 위해 알아둬야 하는 일반적인 용어이다. 무언가를 해킹할 때 각 채널들에 4단계 접근법을 적용하는 것은 아주 흔한 해킹 방법이다. 물론 해야 할 일은 아주 많지만 매뉴얼에는 없는 자신만의 방법을 찾아내고 제작자를 뛰어넘는 일은 아주 즐겁고 흥미로운 일이 될 것이다.

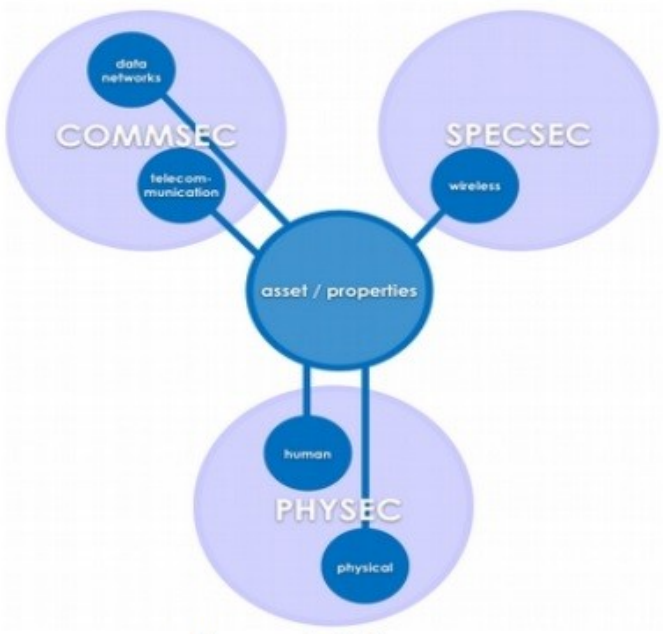


Figure 1.2: Scope

자산(Asset)은 금, 인적자원, 설계도, 노트북, 핸드폰이 전달하는 900 MHz주파수, 돈과 지적자산의 일종인 개인정보, 브랜드 정보, 기업정보, 제조과정, 암호나 핸드폰을 통한 대화 등이 있다.

의존물(Dependencies)은 자산의 소유자가 독자적으로 제공할 수 없는 자원을 말한다. 예를 들어 컴퓨터 소유자는 전기를 만들어낼 수는 없다. 물론 누군가 전력을 끊어버릴 확률은 낮지만 의존물은 해킹 범위에 포함된다.

보안의 목표는 지켜야 하는 자산과 의존물을 위협 요인과 **분리(Separation)**시키는 것이다.

보안은 분리의 기능을 가지고 있다. 이러한 분리를 가능하게 하는 네 가지 방법이 존재한다.

- 자산을 이동시킨 후 위험요인들을 막기 위한 방어막을 형성한다.
- 위험요인들을 무해한 상태로 변화시킨다.
- 위험요인들을 제거한다.
- 자산을 제거한다.(권장하지 않음)

해킹을 하기 위해서는 타겟과 상호작용을 할 수 있는 장소를 알아내야 한다. 건물의 문들을 생각해보자. 각 문들은 근무자용, 손님용, 화재 탈출용 등으로 구분되어 있고 일부는 불필요한 문들일 수도 있다.

종류는 다양하지만 모든 문들이 상호작용(소통)의 위한 장소로 사용되어 긍정적인 기능과 도둑질과 같은 부정적인 기능을 돕는다. 만약 해킹을 위해 이 빌딩에 왔다면 각 문들이 만들어진 이유를 알 필요는 없다. 단지 4단계 접근법을 사용해서 조사를 시작하면 된다.

벼락으로부터 안전해지고 싶어 하는 한 남자를 생각해보자. 자신을 번개로부터 지킬 수 있는 유일한 방법은 번개가 절대로 통과할 수 없는 바위와 흙으로 뒤덮힌 동굴 속으로 들어가는 것이다. 만약 이 남자가 밖으로 나갈 필요가 전혀 없다면 이 방법은 100% 안전하다고 할 수 있다. 하지만 누군가 동굴에 구멍을 뚫는다면 번개는 구멍 수 만큼의 접근 기회를 가지기 때문에 다공성(porosity)은 증가한다. OSSTMM은 **안전(Safe)**한 상황과 **보안(Secure)**이 이뤄진 상황을 구분지어 생각한다. 간단히 말해 보안 구멍이 많아질수록 해커가 대상을 변화시키고 통제할 수 있는 가능성은 증가한다.

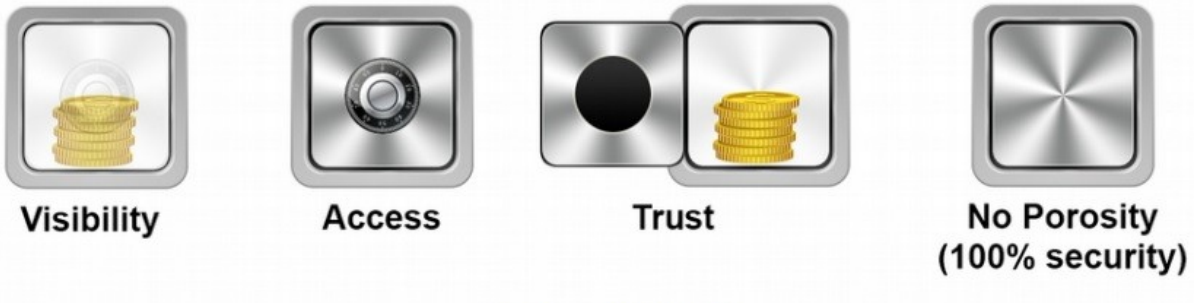


Figure 1.3: Porosity

Feed Your Head: Porosity

해킹의 관점에서 다공성(Porosity)을 구별하고 정의하자면 다음과 같다.

용어	정의
가시성 (Visibility)	경찰이 범죄를 조사할 때는 범죄방법, 범죄동기, 범죄기회를 잘 살펴본다. 자산이 눈에 잘 띄인다면 공격당할 가능성이 높아지고 그 반대로 자산이 숨겨져 있다면 공격대상이 될 확률은 줄어든다. 몇몇 보안 전문가들은 **불명료화(obfuscation)**를 단지 대상을 숨겨줄 뿐 대상을 지켜주는 보안의 기능은 형편없다고 말한다. 하지만 영구적인 보안대책이 늘상 필요한 것은 아니기 때문에 위의 불명료화를 나쁘다고만은 볼 수 없다. **OSSTMM**도 이 주장에 긍정하며 다음과 같이 말했다. “보안이 평생 지속될 필요는 없다. 단지 누군가의 관심이 사라질 때까지만 유지되면 된다.”(“Security doesn't have to last forever, just longer than anything else that might notice it's gone.”)
접근성 (Access)	접근성은 각 영역(scope)의 외부로부터 상호작용(소통)이 발생할 수 있는 곳들을 말한다. 빌딩을 예로 들면 밖으로 나갈 수 있는 문이나 창문이 해당되고, 인터넷 서버의 경우 열려있는 포트 번호나 컴퓨터에서 이용할 수 있는 서비스가 접근을 가능하게 한다.
신뢰성 (Trust)	신뢰성을 이용한다면 영역(scope)내에서 자유롭게 상호작용(소통)을 할 수 있다. 신뢰성이 형성되어 있기 때문에 어머니가 자신을 껴안을 때 신원을 확인할 필요가 없고 음식에 독을 넣지 않았을 거라고 확신할 수 있다. 모두 자신만의 영역에서 누구를, 무엇을 신뢰해야 하는지 자연스럽게 배운다. 만약 어느 날 어머니가 에일리언에게 몸을 빼앗기고 음식에 독을 넣었다면 불행히도 당할 수밖에 없다. 이처럼 신뢰성은 보안의 허점인 동시에 신원을 증명할 수 있는 수단이다. 신뢰는 사회적으로 가치있는 특성이며 누구든 자신만의 신뢰를 가지고 있기 때문에 신뢰란 까다로운 주제이다. 신뢰가 없다면 우리는 자유롭게 소통할 수 있는 능력을 잃게 될 것이다. 하지만 신뢰를 이용하면 누군가를 속이고, 강탈하고, 거짓말하는 것이 더욱 쉬워진다. OSSTMM은 신뢰에 관한 조사를 통해 누군가를 신뢰할 수 있는 10가지 이유인 **신뢰의 특성(Trust Properties)**을 알아내었다. 만약 이 10가지 이유가 충족 된다면 아무런 걱정 없이 상대방을 신뢰할 수 있다. 하지만 한 가지 이유만 충족 되어도 상대방을 신뢰하는 경우가 많고 3가지 이상의 이유가 충족 되었는데도 상대방을 신뢰하지 않는 경우도 있다.

학습 도구

효과적인 연구, 학습, 비판적 사고는 해커가 필수적으로 지녀야 하는 자질이다. 실제로 해킹능력은 수업보다는 일상적인 생활 속에서 개발되는 창의적인 능력이다. 해커가 되기 위해 알아야 하는 모든 것을 알려 줄 수는 없지만 무엇을 배워야 하는지는 알려 줄 수 있다. 기술은 빠르게 발전하고 있고 오늘 배운 내용이 내일은 필요가 없어질 수 있기 때문에 해킹의 가장 필수적인 부분이자 **아마추어 해커(script kiddie**: 해킹의 본질을 이해하지 못하고 해킹 도구들을 사용하는 사람)에서 벗어나게 해줄 수 있는 해커들의 학습 습관을 배우는 것이 훨씬 도움이 될 것이다.

이번 레슨을 공부하다가 이해가 안 되는 단어나 개념을 마주한다면 반드시 그 의미를 찾아봐야 한다. 새로운 개념들을 이해하고 넘어가지 않으면 앞으로의 학습이 더욱 어려워 질 것이다. 앞으로 만날 각종 주제들에 대해 스스로 조사하고 새로 알게 된 정보들을 통해 연습 문제들의 답을 알아내야 한다. 하지만 해당 연습 문제들의 답을 제공하지는 않는다. 그러니 자신에게 맞는 학습 도구들을 이용하여 배우고 익히는데 많은 시간을 투자하기 바란다.

책

아마 처음에 추천하는 것이 인터넷이 아니라서 많이 놀랐을 것이다. 하지만 책은 기초를 배우고 정확한 지식을 배우기 위한 훌륭한 학습 도구이다. 컴퓨터의 하드웨어나 시스템 등의 세세한 부분들을 자세하게 배우기 위해서는 책보다 더 좋은 게 없다. 컴퓨터 관련 책들의 문제점은 기록되어 있는 지식들이 빠르게 구식이 된다는 것이다. 중요한 것은 책이 소개하는 기본 원리들을 보는 방법을 배우는 것이다. MS-DOS와 윈도우는 분명히 다르지만 둘 다 19세기에 에이다 러브레이스(Ada, Countess of Lovelace)가 처음 컴퓨터 프로그램을 작성한 후부터 컴퓨터에 사용되어온 불 로직(Boolean logic)에 기반을 두고 있다. 보안과 프라이버시에 관한 정보들은 지난 2,500년 동안 계속해서 변화해 왔지만 손자가 쓴 **손자병법(The art of war)**은 현대에서도 적용할 수 있는 내용들을 가득 담고 있다.(하지만 손자의 말을 인용하는 것은 자신이 **초보(n00b)**라는 것을 드러내는 것일 뿐이다. 중요한 것은 손자의 말을 인용하는 것이 아니라 현실에 적용하는 것이고 손자가 말했듯 자신이 알고 있는 지식은 비밀로 남겨둬야 한다. 그러니 손자병법의 글을 남에게 읊어대는 것은 책을 제대로 읽지 않았다는 것이다.)

비록 다른 학습 도구들을 통해 얻는 정보들이 책을 통한 정보들보다 업데이트가 빠르긴 하지만 책의 정보들은 아주 잘 작성되어 있고 보다 정확할 확률이 높다. 일 년을 책을 쓰는데 집중한 작가는 하루에 여섯 게 정도의 포스팅을 하는 블로거보다 사실 확인을 훨씬 철저하게 할 것이다.(인터넷 잡지, 블로그편에서 더욱 자세하게 알 수 있다.)

하지만 정확한 정보 역시 편견을 내포하고 있을 수 있고 작가들의 정보 출처 자체가 편견에 치우쳐 있을 수도 있다. "역사는 승자에 의해 기록된다."는 말에서 알 수 있듯이 때로는 해당 시기의 정치와 사회의 규범에 의해서 출판이 되지 못하는 정보들이 존재한다. 교과서의 경우에도 당시의 정치 상황에 의해서 내용이 선별되고 사회적으로 받아들여질 만한 정보들만을 수록한다. 이런 내용들을 책을 통해 알게 된다는게 참 다행이라고 생각하지 않는가? 누구나 책을 쓸 수 있고 저자의 사상에 의해 진실은 변형될 수 있다는 것을 명심하자.

책이 단지 두껍다는 이유만으로 읽는 것을 포기해선 안 된다. 이 두꺼운 책을 전부 다 읽는 사람은 드물다. 그냥 **선사 시대의 웹페이지**라고 생각하고 아무 페이지나 넘기면서 독서를 시작해 보자. 만약 이해가 안 되는게 나온다면 앞쪽의 설명을 읽거나 뒷 부분에서 필요한 내용들을 찾아서 읽어보자. 인터넷에서 여러 웹사이트를 뒤지는 것처럼 책의 여러 부분을 왔다갔다 하면서 읽어도 충분히 도움이 된다. 이런 식의 독서법은 훨씬 재미있고 해커에게 만족감을 줄 것이다.

마지막으로, 독서를 통해 독자들은 글을 잘 쓸 수 있는 능력을 얻을 수 있다. 이 능력은 새로운 분야를 이해하고 참여하는데 큰 도움이 된다. 자신이 말하는 것을 더욱 신뢰가 가게 만들어주며 특정 권한을 가진 사람을 설득할 때도 도움이 된다.

간행물과 신문

간행물과 신문은 자세한 내용을 길게 싣지는 않지만 정확하고, 현실을 반영하는 정보를 주는 유용한 학습 도구이다. 두 매체는 특정 독자들을 대상으로 하며 자신들만의 논점과 주제의식을 가지고 있기 때문에 편견과 공정의 개념을 전혀 고려하지 않고 자신들의 주장을 말할 뿐이다. 만약 리눅스와 관련된 간행물은 경쟁 제품인 윈도우와 관련된 정보는 다루지 않고 독자들 역시 리눅스에 관한 신규 정보들을 원하지 다른 운영매체에 관한 정보를 기대하지는 않는다. 많은 간행물들이 자신들이 집중하고 있는 주제에 대한 긍정적인 면만 강조하고 부정적인 면은 잘 다루지 않는 **체리픽킹(Cherry picking)** 기법을 사용한다.

간행물이 편견 섞인 정보를 줄 수도 있다는 것을 잊지 말자. 간행물들은 진실보다는 자신들의 의견을 개제하는 공간이고 자신들의 입맛에 맞게 몇 가지 진실들을 배제하여 독자들의 주체적인 견해형성을 막을 수 있다. 항상 정보의 출처를 고려하는 습관을 길러야 한다! 아무리 중도를 지향하는 간행물일지라도 편견에 치우칠 수 있고 추측성 기사를 남발 할 수 있다.

의료계에서는 실험의 성패와 관계없이 모든 의학적, 약학적 실험 결과들을 간행물로 만들자는 활발한

움직임이 형성되고 있다. 모든 실험의 결과들이 정리된 간행물이 나온다면 의사들이 치료를 하기 전에 어떤 약이나 치료법을 선택해야 할지 고려하는데 도움이 될 수 있다. 현재 발간되고 있는 의료계의 간행물들은 임상실험에서 나온 "사실"들을 기사로 싣고 있지만 실험의 구체적 내용이나 실험 환경에 관한 내용은 여전히 모호하다. 어떤 주제를 다루든지 특정 결과와 효과를 발생 시키는 근본 원인을 아는 것은 아주 중요하다.

각종 간행물들은 의식적이든 무의식적이든 다양한 트릭을 사용한다. 전문가가 아닌 특정 사람의 의견을 싣는 **일화적 증거(anecdotal evidence)**방식과 해당 분야와 상관없는 전문가의 의견을 싣는 **권위자 증명(authoritative evidence)**방법을 사용하여 기사가 진실처럼 보이게 만든다. 또한 사실 확인 없이 "모두"가 사실이라고 생각한다는 것을 진실의 이유로 간주하여 **추측(speculation)**성 기사를 싣기도 한다.

자신이 마주한 특정 이슈의 정확성과 진실성을 파악하기 위한 최고의 방법은 깊고 넓은 탐색을 실행하는 것이다. 간행물에서 흥미로운 주제를 발견한다면 좀 더 깊이 있게 파고들 필요가 있다. 해당 이슈의 한쪽 관점에서 사실을 확인한 후 다른 쪽 관점에서 진실여부를 파악하여 반박의 여지가 있는지 탐색한다. 일부 문화권에서는 여러 관점에서 문제에 접근하는 것을 기본적인 의견형성 방법으로 여기고 있다. 일상적인 생활에서 추구되는 기본적인 습관으로써 아주 강력한 문화적 특성이며 특히 민주주의를 공고히 하는 최고의 방법이다.

Exercise

1.9 인터넷을 이용해 해킹과 관련된 간행물 세 종류를 찾아보자. 어떤 방식으로 찾아냈는가?

1.10 해당 간행물들이 컴퓨터 해킹만을 다루는가? 해킹 외에도 다른 분야에 관한 유용한 정보를 담고 있는가?

Feed Your Head: Speculation

다음의 뉴스기사는 강도사건을 다루고 있다. 다음 기사에서 추측성(speculation) 정보를 찾아보자.

목요일 오후 레이크 매도우 은행(The Lake Meadow Bank and Mortgage Lender)은 폐점 직전 가면을 쓰고 총기를 들고 온 강도들에 돈을 강탈 당했다. 직원들은 범인들이 최신 SUV를 타고 도주하기 전까지 한 시간 가량 인질로 잡혀있었던 것으로 보인다. 부상자는 없다고 보고되었다.
범인들의 신원은 파악이 되지 않고 있으며 범인들이 사건 직후 은행 뒤에 주차되어 있는 차를 타고 남쪽의 블루그린산맥(the Bluegreen Mountains)의 숲 속으로 들어간 것을 근거로 경찰들은 이들이 전문 범죄자들이라고 믿고 있다. 경찰들은 수감기록이 있는 강도 전과자들과 해당 지역의 시민들과 친분을 가지고 있는 사람들을 조사하고 있을 것이다.
블루그린 시의(Bluegreen country) 인구는 내년에 50,000명을 넘을 것으로 예상되며 하루 평균 57건의 은행 강도사건들이 보고되고 있다. 이는 은행 강도사건의 시발점으로 여겨진다. 경찰국장인 스미스씨는 "이런 현상은 유행의 시작으로 보인다."라고 말했다.

우리는 점점 추측성 기사에 무감각해지고 편향된 통계수치를 무분별하게 받아들이고 있기 때문에 미래의 뉴스들은 단 한 명의 기자에 의한 추측으로 도배될 수도 있다. 위의 짧은 기사에서 나오는 정보들 중 믿을 수 있는 사실은 단 한 가지, 목요일 오후에 한 은행에서 강도 사건이 발생했다는 것 뿐이다. 추측성 정보를 강조하기 위해 위의 기사에서 나온 추측들을 더욱 과장되고 터무니없게 바꿔보겠다.

목요일 오후 레이크 매도우 은행(The Lake Meadow Bank and Mortgage Lender)은 폐점 직전 총기를 들고 닭 가면을 쓴 강도들에 의해 돈을 강탈당했다. 직원들은 범인들이 닭장 모양의 열기구를 타고 도주하기 전까지 십년 가량을 인질로 잡혀있었던 것으로 보인다. 직원들 중 깃털을 뒤집어쓴 사람은 없다고 보고되었다.
닭들의 신원은 파악이 되지 않고 있으며 범인들이 사건 직후 은행 위에 매달려 있던 열기구를 타고 남쪽의 툰드라로 향한 것을 근거로 경찰들은 범인들 중 변장 전문가와 열기구 전문가가 있을 것으로 믿고 있다. 경찰들은 열기구 운전을 취미로 하는 사람들과 친분을 맺고 있는 메이크업 전문가들을 찾고 있을 것이다.
블루그린 시에(Bluegreen country)있는 열기구 산업의 매출은 미래에 47억 원 가량이 될 것으로 예상되며 하루 평균 57건의 도난사고가 보고되고 있다. 이는 열기구를 이용한 은행 강도사건의 시발점으로 여겨진다. 경찰국장인 골든씨는 "이런 현상은 유행의 시작으로 보인다."라고 말했다.

워낙 다양한 산업분야에서 이러한 추측성 정보의 기능을 사용하고 있기 때문에 보안 산업에서도 추측성 정보를 사용한다는 것은 그리 놀라운 일이 아니다. 보안 산업에서 주로 사용하는 용어인 **FUD**는

Fear(공포), Uncertainty(불확실), Doubt(의심)의 약어로 보안에 관한 관심과 보안 솔루션을 팔기 위해 사람들을 주목시키는 용도로 사용하는 추측성 정보와 주관적 위험분석에 적용되는 특성들이다. 불행히도 이러한 특성들은 추측성 정보에 무감각해지고 있는 상황 덕분에 뛰어난 효과를 보여주고 있다. 이런 트릭들로 인해 무분별한 보안솔루션 판매와 부적절한 보안 시스템 적용, 권위자에 대한 맹목적 믿음과 같은 부작용들을 만들어내고 있다. 사람들의 비판적 사고능력은 계속해서 약화되어 결국 상업적으로 이용당할 뿐 아니라 범죄자들의 타겟이 될 수도 있다.

검색 엔진

구글은 검색엔진으로 잘 알려져 있지만 그 이상의 기능을 가지고 있다. 빙(Bing)은 간단한 질문형식의 검색에 유용하고 야후(Yahoo)는 포괄적인 검색능력에 특화되어 있다. 이러한 웹 서비스들은 서비스 이용자들에 관한 정보를 원하고 때로는 필요 이상의 정보를 가져가기도 한다. 이들은 항상 사용자들의 검색 정보와 검색 이후의 접속 사이트에 관한 정보들을 수집하고 있다.

AltaVista와 DuckDuckGo.com처럼 사용자의 검색어를 기록하지 않는 검색엔진들도 존재한다. 불건전한 내용을 검색할 때 활용할 수 있는 검색엔진들이다.

웹사이트들은 온라인에 존재하는 한 언제까지나 검색이 가능하고 **캐시페이지(cached pages)**형태로 자료들을 계속해서 남겨둔다. 캐시페이지에는 웹사이트들의 과거 기록들이 저장되어 있고, 심지어 지금은 사라진 웹사이트들의 정보도 가지고 있다. 검색엔진과 아카이브 사이트들은 정보를 평생 동안 보관한다. 그러니 인터넷에 무언가를 게시하기 전에는 이 사실을 항상 명심해야 한다. 웹페이지들 중에는 캐시페이지로 연결되어 있는 링크들을 올려놓는 곳도 있다. 예를 들어 구글은 과거 일반 링크결과 옆에 "캐시(Cache)"라고 쓰여있는 링크버튼을 만들어 놨었다. 현재는 오른쪽의 매뉴창에 위치해 있지만 여러분이 이 책을 보고 있을 때는 또다시 바뀌었을 수도 있다.

검색엔진 외에도 **Internet Archive(http://www.archive.org)**처럼 캐시정보들을 볼 수 있는 사이트들이 존재한다. 이런 사이트들을 이용하면 수년 동안 변화해온 각종 캐시페이지들을 볼 수 있고, 이를 통해 지금은 사라진 정보들을 검색할 수 있다.

한 가지 주의할 점은 검색엔진을 통해 나타난 웹사이트라는 이유로 무조건 신뢰해서는 안 된다는 것이다. 웹사이트에 접속하고 프로그램을 다운받거나 자료를 공유할 때는 해킹 공격이나 바이러스에 피해를 입을 가능성이 높아진다. 신뢰가 가지 않는 사이트에서는 다운로드를 하지 않거나 **샌드박스(sandbox)**를 이용함으로써 자신을 지킬 수 있지만 이것만으로 충분하지는 않다. 인터넷 브라우저는 창문과 마찬가지로 인터넷과 소통할 수 있는 창구이기 때문에 개방되어 있을 때는 외부의 침입을 받을 수 있다. 이러한 침투는 실제적인 피해가 발생하기 전에는 알아채지 못하는 경우도 있다.

Exercise

1.11 세상에는 많은 종류의 검색엔진이 있고 그 중에는 일반 검색엔진으로는 검색이 안 되는 **투명 웹(Invisible Web)**을 찾아낼 수 있는 검색엔진들이 존재한다.
훌륭한 연구자들은 이러한 검색엔진들을 잘 사용할 줄 안다. 일부 웹사이트들은 검색엔진을 찾아내는데 특화되어 있다. 이제, 그동안 전혀 들어본 적도 사용해 본 적도 없는 검색엔진들을 찾아보자.

1.12 다른 검색엔진들을 찾아내는 검색엔진들 역시 존재한다. 이런 종류의 검색엔진들은 **메타 검색엔진(meta search engines)**으로 불린다. 이제, 메타 검색엔진 한 가지를 찾아내 보자.

1.13 "security and hacking"라는 단어를 검색하고 최상위 3개의 검색결과를 알아보자.
? 마크를 붙였을 경우 다른 검색 결과가 나오는가?

1.14 하나의 주제에 관해 검색하는 것은 단어나 문장을 검색하는 것과 상당히 다른 과정을 거친다. 위의 연습문제에서 문장을 검색했으니 이제 하나의 주제를 검색해보자. 그러기 위해서는 **자신이 찾고 있는 주제를 다루는 웹페이지에 들어갈 만한 문장을 생각해 보**자.
검색엔진을 통해 해킹 관련 간행물의 리스트를 알아내고 싶다면 "a list of online magazines about hacking"를 검색하는 것으로는 충분한 정보를 알아낼 수 없다.
그것보다는 우선 "만약 내가 해킹 관련 간행물을 만든다면 어떠한 문장을 집어넣을까?"라고 생각해 봐야한다. 아래의 문장들을 검색엔진에 입력하고 어떤 결과가 나오는지 알아 보자.

1. my list of favorite magazines on hacking
2. list of professional hacking magazines
3. resources for hackers
4. hacking magazine
5. magazines hacking security list resources

1.15 인터넷 아카이브(Internet Archive)를 통해 Mozilla의 홈페이지 중에서 가장 초기 버전을 찾아보자. 그러기 위해서는 "http://www.archive.org"에 접속해서 "www.mozilla.org"를 검색하면 된다.

1.16 이제 여태까지 알아본 것들을 종합적으로 사용하여 넷스케이프버전 1(Netscape verson 1)을 다운받아 보자. 검색엔진과 인터넷 아카이브를 활용하면 된다.

웹사이트와 웹 애플리케이션

실질적인 정보 공유는 웹브라우저를 통해서 이루어진다. 우리는 모든 것들을 "웹(web)"으로 알고 있지만, 시간이 지나면서 우리들이 사용하는 대부분의 것들은 "웹 애플리케이션(web application)"

으로 바뀌고 있다. 웹에 존재하는게 다 웹사이트는 아니다. 웹 브라우저를 이용해서 메일을 주고받거나 웹 연결형 서비스를 이용해 음악을 듣는다면 웹 애플리케이션을 사용하고 있는 것이다.

웹 애플리케이션을 이용하기 위해서는 권한(privileges)이 필요한 경우가 있다. 권한을 얻기 위해서는 로그인 아이디와 패스워드가 필요하다. 합법적인 권한을 이용하여 접속하였을 경우 **권한(privileges)**을 획득 했다고 할 수 있다. 웹 페이지를 통제하기 위해 해킹을 한 경우에도 접속은 할 수 있지만 합법적인 권한을 가진 것은 아니기 때문에 권한 이용 접속(privileged access)이라고는 볼 수 있다. 웹을 계속해서 이용하다 보면 권한이 필요한 영역(privileged areas)에 접속하게 해주는 보안 허점들을 우연히 발견하는 경우도 있을 것이다.

이런 허점들을 발견할 때 웹 사이트 관리자에게 알려주는 것은 좋은 습관이지만 이때 발생할 수 있는 법적 파급 효과들을 주의해야 한다. 불행히도, 많은 관리자들이 이런 식의 선행을 좋아하지 않는다.

자신을 보호하는 동시에 인터넷을 좀 더 안전한 장소로 만들기 위해서는 Tor이나 anonymous remailers와 같은 **익명서비스(Anonymizer)**를 사용해서 사이트 관리자들에게 취약점 보고를 하는 것이 좋다. 하지만 이런 서비스도 약점이 있고 자기가 생각하는 만큼 익명성이 유지되지 않을 수 있다는 것을 명심하자.(많은 해커들이 안타까운 경험을 한 후에야 이러한 사실을 알게 되는 경우가 많다.)

Excercise

1.17 검색엔진을 사용해 모든 사용자들에게 권한접속을 가능하게 하는 실수를 범한 사이트를 찾아보자. 이를 위해 우리는 해당 자료들을 담고 있는 폴더들을 찾아야 한다. 이는 "디렉토리 리스팅(directory listing)"이라고 불리며 아무대서나 사용할 수 있는 것은 아니다. 다음 명령어를 구글 검색창에 타이핑 해보자.

```
allintitle:"index of" .js
```

해당결과를 통해 디렉토리 리스팅처럼 보이는 것을 찾을 수 있을 것이다. 이런 식의 탐색법을 구글 해킹이라고 부른다.

1.18 이런 방식으로 다른 종류의 문서들을 찾을 수 있는가? .xls files, .doc files, .avi file명령어가 포함된 세 가지 디렉토리 리스팅을 찾아보자.

1.19 “allintitle:”말고도 다른 종류의 검색옵션이 있는가? 어떻게 찾았는가?

인터넷 잡지

잡지(Zine) 또는 **인터넷 잡지(E-Zine)**로 알려진 이것은 팬들에 의해 만들어진 **잡지(Fanzine)**에 의해 시작되었다. 주로 비전문가들에 의해 만들어지는 인터넷 잡지들은 대부분 그 규모가 작고 무료로 독자들에게 공개된다. 잘 알려진 **2600**이나 **Pharck**를 포함한 많은 인터넷 잡지들이 올리는 자료들의 출처는 평범한 인터넷 사용자들이기 때문에 오타체크나 문장교정이 없이 기사가 실리는 경우가 많고 때로는 과격한 언어를 사용하기도 한다.

인터넷 잡지는 과격한 주제들을 다루거나 자신만의 의견에 치우치는 경향이 있다. 하지만 광고주나 독자들에게 자금을 지원 받지 않기 때문에 특정 이슈들에 대해 다양한 의견들을 보여준다.

Excercise

1.20 인터넷을 이용해 해킹을 다루는 인터넷 잡지 세 가지를 찾아보자. 어떻게 해당 인터넷 잡지들을 찾았는가?

1.21 왜 이 잡지들을 인터넷 잡지로 여기는가? 단순히 인터넷 잡지로 제공하거나 “인터넷 잡지”라는 제목을 붙였다는 이유 만으로 인터넷 잡지로 판단해서는 안 된다.

블로그

블로그(blog)는 인터넷 잡지의 진화 버전으로 단 한 명에 의해 작성된다. 블로그의 정보들은 출판물이나 인터넷 잡지에 비해 빠른 속도로 업데이트 되며 특정 주제에 관한 다양한 커뮤니티를 형성한다. 블로그에 올라오는 글들은 인터넷 잡지 보다도 훨씬 즉각적이고 다양한 관점의 개인 의견이 많이 포함된다. 이러한 점이 블로그만이 가지는 특별한 장점이다.

인터넷에는 어마어마하게 많은 블로그가 존재하지만 실제로 꾸준히 운영되는 블로그는 소수에 불가하다. 하지만 대부분의 블로그에 있는 정보들은 언제든지 열람할 수 있다.

Excercise

1.22 인터넷을 이용해 해킹 관련 블로그 세 가지를 찾아보자.

1.23 어떤 단체나 커뮤니티가 관련되어 있는가?

1.24 해당 블로그가 보안, 법집행, 학술정보를 다루는가?

포럼과 메일링리스트

포럼(Forums)과 **메일링리스트(mailing lists)**는 여러 사람들에 의해 만들어진 대중 매체로, 파티에서 여러 사람들이 나눈 대화를 기록한 책자의 인터넷 버전이라고 보면 된다. 여기에서 얻은 정보들은 늘 의심하는 습관을 가지는 게 좋다. 주장들의 논점은 계속해서 변하고 많은 이야기들이 진실인지 아닌지 알 수 없다. 몇몇 사람들은 일부러 **공격적이고 불쾌한 내용을 올리거나(trolling)** 다른 사람들의 주장을 **비방하고 모욕하는 경우(flame war)**도 있다. 포럼과 메일링리스트는 유사한 점이 많다. 정보의 정확성 여부에 상관없이 각자의 주장을 자유롭게 게시하며 익명성을 유지할 수 있다. 다루는 주제나 화제가 빠르게 변화하기 때문에 모든 정보를 수용하기 위해서는 앞의 일부분만을 읽는 게 아니라 내용 전체를 살펴봐야 한다.

포럼은 거의 모든 분야에서 나타날 수 있고 많은 온라인 잡지사와 신문사들은 독자들의 반응을 알기 위해 자신들의 기사에 대한 포럼을 제공한다. 아무리 많은 사람들이 특정 기사를 좋아하더라도 싫어하는 사람들 역시 존재하기 때문에 포럼을 형성하면 발행한 기사들에 대한 여러 의견들을 알 수 있다.

특수한 주제들에 대한 메일링리스트도 많이 존재하지만 찾는 게 쉽지 않다. 자신이 원하는 메일링리스트를 찾기 위해서는 해당 커뮤니티가 다룰만한 특정 정보에 관해 검색해 보는 게 좋다.

해커로서 알아두어야 할 것은 대부분의 포럼과 메일링리스트들이 검색엔진에서 탐색이 안 된다는 것이다. 검색엔진을 통해서 일부를 찾을 수는 있지만 개별적인 정보들을 확인할 수는 없을 것이다. 게시된 정보들은 특정 웹사이트나 포럼에서 직접 검색 해야지만 찾을 수 있기 때문에 포럼과 메일링리스트는 투명웹(invisible web)의 일종으로 여겨진다.

Excercise

1.25 해커와 관련된 포럼 두 가지를 찾아보자. 어떻게 이 둘을 찾았는가?
포럼 웹사이트가 중점을 둔 주제나 화제가 무엇인지 알 수 있는가?
포럼에서 직접 다루는 주제와 웹사이트가 중점을 둔 주제가 일치하는가?

1.26 해커와 보안과 관련된 메일링리스트 두 가지를 찾아보자.
찾아낸 메일링리스트들의 주인들은 누구인가? 멤버들의 목록을 찾을 수 있는가? (멤버목록을 열람하기 위해서는 각 메일링리스트가 사용하는 리스트작성 애플리케이을 알아내서 감춰진 명령어를 찾아내야 한다.)
둘 중 어느 곳이 사견보다 정확한 정보의 비중이 높다고 보는가? 왜 그렇게 생각하는가?

뉴스그룹

뉴스그룹(Newsgroups)은 오랜 시간동안 존재해 왔고 일부 뉴스그룹들은 월드와이드웹이 만들어지기 훨씬 전에도 존재했다. 구글은 뉴스그룹들의 모든 아카이브를 구매해서 http://groups.google.com에 모아두었다. 뉴스그룹은 메일링리스트와 유사하지만 메일을 경유하지 않는다. 누구나 자기가 원하는 내용들을 직접 게시할 수 있고 1990년대부터 현재까지의 포스팅들을 검색할 수 있다.

웹 아카이브와 마찬가지로 뉴스그룹 아카이브는 어떤 아이디어나 상품의 기원이 어디인지 알아내는데 중요한 역할을 한다. 또한 평범한 웹페이지를 통해서는 결코 알아낼 수 없는 정보들을 검색할 수도 있다.

뉴스 그룹은 오랜 시간 사용되어 왔으며, 과거에 비해 오늘날 더 적게 사용되거나 하는 변화가 있지는 않다. 하지만 뉴스 그룹은 어떠한 성장도 하지 않았으며 그 인기는 블로그와 포럼과 같은 새로운 웹 서비스들에게 점차 자리를 내어주고 있는 추세이다.

Excercise

1.27 구글의 뉴스그룹을 이용하여 해킹 관련 포럼이 작성한 가장 오래된 포스팅을 찾아보자.

1.28 뉴스그룹을 이용할 수 있는 다른 방법들을 찾아보자. 뉴스그룹을 사용할 수 있는 애플리케이션이 존재하는가?

1.29 해킹 관련 뉴스그룹이 얼마나 많이 존재하는가?

1.30 현재 운영 중인 뉴스그룹들이 정리된 목록을 찾을 수 있는가?

위키

위키(Wikis)는 인터넷에서 만들어진 새로운 현상 중 하나이다. 여러 종류의 위키가 서비스되고 있고 그 중 가장 잘 알려진 위키로는 위키피디아(www.wikipedia.org)가 있다. 여러 사이트들처럼 위키 역시 커뮤니티들이 합쳐져서 만들어졌다. 위키는 여러 아마추어들에 의해 만들어지기 때문에 정확하지 않다는 주장이 계속되고 있지만 이런 점은 책, 메일링리스트, 잡지나 다른 매체들 역시 마찬가지다. 중요한 점은 전문가만이 훌륭한 아이디어나 정확한 정보를 알고 있는 것은 아니라는 것이다. OSSTMM이 주장하는 것처럼 새로운 개념은 아이디어를 차근차근 검증 하는데서 나오는 것이지 극적인 발견을 통해 나오는 것이 아니다. 이런 이유 때문에 위키는 전문가와 아마추어의 의견이 뒤섞인 훌륭한 정보

출처이고 차근차근 정확성을 높여가고 있다.

위키는 여러 주제들을 다양한 관점에서 논의하며 수정목록을 통해 이용자들이 게시된 정보들이 어떻게 정의되고 반박되며 수정되어 왔는지 알 수 있게 해놓았다. 위키는 정보를 캐내기 위한 훌륭한 장소로 많은 사람들이 애용하는 웹사이트이다.

Excercise

1.31 "Ada Lovelace" 검색해 보자. 검색 결과에 위키정보가 나타나는가?

1.32 위키피디아에서 다시 검색하고 결과를 확인하자. 인터넷 검색 결과에 해당 위키피디아 검색 결과가 포함되어 있는가?

1.33 위키피디아의 편집 목록을 확인해서 수정된 정보들은 무엇인지 확인해 보자.
수정된 정보는 무엇인가? 수정된 내용이 원래 내용으로 돌아간 게 있는가?
이제 좋아하는 영화배우나 가수를 위키피디아로 검색한 후에 수정항목들을 살펴보자.
차이점이 있는가?

1.34 다른 위키사이트를 찾아서 다시 검색해보자.
위키의 검색 결과 중 일반 검색엔진의 검색 결과에 나타나는 게 있는가?

소셜미디어

지금 사용하고 있는 소셜미디어(Social Media)가 있는가? 만약 있다면 몇 가지를 사용하는가? 해커로서 현재 많이 사용되고 있는 소셜미디어의 종류들을 잘 알고 있을 것이다. 과거에 비해 인기가 떨어진 소셜미디어는 어떤 것이 있는가? 비록 인기가 떨어졌다 해도 여전이 운영되고 있고 저장된 데이터들 역시 대부분의 이용할 수 있다.

이게 뜻하는 것은 우리들이 마음껏 뿌리고 다닌 개인 정보들을 보유하고 있는 거대한 정보 저장고가 있다는 것이다. 이 정보들은 앞으로 영원히 저장될 것이다.

소셜미디어 사이트에서 이용자들이 관심을 가지는 주제에 대한 하위 그룹이나 커뮤니티가 생기는 경우도 있다. 전문적인 주제를 다루는 사이트는 대부분 사이버 보안 커뮤니티를 가지고 있고 "어둠의 경로"와 관련된 주제를 다루는 사이트들은 주로 해킹 커뮤니티를 가지고 있다. 전자는 실명을 사용하게 하지만 후자의 경우 주로 익명을 허용한다.

중요한 질문을 하나 하겠다. 여러분은 소셜미디어를 사용할 때 실명을 사용하는가? 아니면 "프로필명(handle)"을 따로 만들어서 사용하는가? 프로필명을 이용해서 실제 이름을 추리할 수 있는 여지가 있는가? 대부분의 사람들이 프로필명의 익명성을 잘 활용하지 못하고 프로필명에는 가명을 사용하지만 자신들의 실제 이름, 주소, 학교, 직업 등 여러 가지 개인정보를 입력해 놓는 경우가 많다. 이런 부주의를 노린 누군가가 프로필명을 기준으로 신상털이(doxing)를 시작한다면 금세 여러 가지 개인정보를 알아낼 수 있다. 그러니 익명을 유지하기 위해 가명을 프로필명으로 사용했다면 자신의 개인정보를 함부로 개시해서는 안 된다. 또한 여러 가지 프로필명을 사용한다면 햇갈리지 않도록 주의하자.

Excercise

1.35 자가 자신을 검색해보자. 검색 결과가 나오는가? 정확한 정보인가?
검색 결과들 중 소셜 미디어를 통한 정보들이 있는가?

1.36 자신이 사용하는 소셜미디어 사이트에 로그인하지 않고 외부인이라 가정한 후 자신에 대한 검색을 해보자. 얼마나 많은 정보들이 나오는가?

1.37 친구가 사용하는 소셜미디어 사이트에 가서 로그인을 하지 않고 친구에 관한 정보를 검색해 보자. 얼마나 많은 정보들이 나오는가?

채팅

인터넷 실시간 채팅(IRC:Internet Relay Chat)과 **인스턴트메시지(IM:Instant Message)**의 형태로 운영되는 **채팅(chat)**은 아주 잘 알려진 소통의 공간이다.

채팅은 여러 사람들과의 실시간 대화에 기반하기 때문에 연구 자료로는 적절하지 않다. 친절한 태도를 보이거나 유쾌한 농담을 하는 사람이 있는 반면, 무례하고 거짓말을 일삼는 사람 역시 존재한다. 지적이고 자신의 정보를 공유하려는 사람도 있지만 무지하면서 정보도 공유하려 하지 않는 인색한 사람도 있다. 채팅 상대가 어떤 유형의 사람인지 아는 것은 어려운 일이다.

하지만, 마음이 맞고 대화하기 편한 상대들을 만난다면 이들이 소속되어 있는 커뮤니티에 합류하여 여러 가지 질문과 답변들을 통해 다양한 지식들을 배울 수 있을 것이다. 결국, 그동안 커뮤니티가 쌓아온 가치 있는 정보와 제로데이(zero day:최근에 발견된 문제점으로 아직 해결책이 없는 문제점) 같은 신규 정보를 얻어 자신의 지식 수준을 향상 시킬 수 있을 것이다.

Excercise

1.38 인스턴트 메시지프로그램 세 가지를 찾아보자. 각각의 차이점이 무엇인가?
세 가지 모두 서로 간의 대화를 위한 프로그램들인가?

1.39 실시간 인터넷 채팅이 무엇인지와 어떻게 접속하는지를 알아보자.
어떤 네트워크가 ISECOM의 채널을 가지고 있는지 알아낼 수 있는가?
해당 네트워크를 찾아냈다면 isecom-discuss 채널에 들어갈 방법은 무엇인가?

1.40 실시간 인터넷 채팅 네트워크에 존재하는 채널들을 어떻게 알 수 있는가?
보안채널과 해킹채널들을 각각 세 개씩 찾아보자. 찾은 채널들에 들어갈 수 있겠는가?
채널에서 대화를 나누는 것은 사람인가 봇(bots)인가?

P2P

Peer to Peer의 약자인 **P2P**는 일종의 인터넷 네트워크다. 중앙 서버를 통해 모든 컴퓨터들이 연결시키는 클라이언트/서버 네트워크(client/server network)와는 달리 P2P네트워크는 이용자들을 직접 연결시켜준다. 대부분의 사람들이 P2P를 음악이나 영화를 다운받을 수 있는 수단 정도로 여기지만 정보를 교환하거나, 분산된 정보들을 취합하여 연구에 사용하기 위한 목적의 다양한 P2P 네트워크들이 존재한다.

하지만 P2P네트워크에는 몇 가지 문제를 가지고 있다. P2P네트워크를 통해 많은 자료들을 찾을 수 있지만 그 중 몇 가지는 네트워크에 존재하는 것 만으로도 범죄로 여겨진다. 법을 어기지 않은 P2P자료들 중에도 제작자가 네트워크에서 공유되는 것을 불편하게 여기고 다운로드 될 때마다 **인터넷 게이트웨이(Internet gateway)** 소유자들에게 돈을 받고 싶어 하는 자료들이 많이 존재한다.

현재, P2P네트워크를 사용하여 자료들을 다운받는 것이 개인에게 책임이 있는지와 이런 사람들을 경찰이 체포해야 하는지에 관한 논의가 계속 되고 있다. 이는 “누군가 내 차를 훔쳐 범죄를 저질렀을 때 차 주인인 내가 감옥에 가야하는가?”의 논제와 비슷하다. 인터넷 법규는 아직 확실하게 규정되어 공정하게 집행되고 있지 않기 때문에 알아서 주의하는 수밖에 없다.

P2P네트워크가 지적 자산을 다운받기 위한 수단으로 사용될 수도 있지만 정보를 찾는데 도움을 주는 훌륭한 도구라는 것은 부인할 수 없는 사실이다. P2P네트워크 자체로는 불법적인 게 전혀 없다. P2P네트워크에는 다양한 라이센스들의 허가로 인해 자유롭게 이용할 수 있는 자료들이 아주 많이 있지만 네트워크에 존재해서는 안 되는 자료들 역시 존재한다. 그러니 P2P네트워크를 이용하는 것을 겁내지 말고 곳곳에 존재하는 위험과 자신이 다운로드 하는 파일이 무엇인지 주의하자.

Excercise

1.41 가장 잘 알려져 있고 많이 사용되는 P2P네트워크 세 가지를 찾아보자.
찾아낸 P2P네트워크들은 어떻게 작동하는가?
각 P2P네트워크들을 사용하기 위해 필요한 프로그램은 무엇인가?

1.42 찾아낸 P2P네트워크들 중 한 개의 P2P네트워크를 선택하여 어떤 프로토콜을 사용하는지 알아보자. 다운로드 속도를 더 빠르게 하기 위해 사용한 방법은 무엇인가?

1.43 "download Linux"를 검색엔진에 쳐보자. P2P를 사용해서 리눅스를 다운받을 수 있는가?

자격증

OSSTMM은 보안분석과 보안테스트능력을 증명하는 자격증과 다양한 종류의 "해커" 자격증을 제공한다. 각 자격증들은 "표준 업무(best practices)"를 기준으로 삼으며 특이한 이니셜을 사용한 명칭들을 가지고 있다.

왜 자격증에 주목해야 한다고 생각하는가? 왜냐하면 자격증은 나이의 제한 없이, 그리고 대학 졸업 여부와 상관없이 언제든지 취득할 수 있기 때문이다. 자격증을 가지게 됨으로써 자신의 능력을 입증할 수 있고 회사 입장에서 특정 업무를 믿고 맡길 수 있는 사람으로 여겨진다.

표준 업무 기반 자격증의 문제점은 표준 업무가 "지금 모든 사람들이 하고 있는 일들"을 의미하기 때문에 계속 변화한다는 것이다. 가끔은 지금 하고 있는 표준 업무가 틀릴 수도 있지만 다음 주가 될 때까지 수정되지 않을 수도 있다.

그래서 나온 것이 인간 행동과 시스템 운영을 효과적인 방법으로 계속 연구하는 능력을 증명하는 연구기반 자격증(research-based certifications)이다. 물론 ISECOM 역시 연구 기반 자격증 교육에 많은 투자를 하고 있다. 이 외에도 기술기반 자격증(skills-based certifications), 분석기반 자격증(analysis-based certifications), **지식융합 자격증(applied knowledge certifications)**을 취득한다면 자신이 지닌 업무수행 능력을 증명할 수 있다. 실제 업무를 할 때 이러한 자격증들은 틀림없이 도움이 될 것이다.

세미나

세미나에 참석하면 각종 이론들을 상세하게 배울 수 있고 여러 기술들의 시연을 볼 수 있다. 제품시연에 중점을 둔 세미나 역시 각종 제품들이 어떻게 작동하고 왜 만들어 졌는지 알 수 있는 좋은 자리이다. 물론 제품 시연 세미나가 마케팅과 제품 판매에 목적을 두고 있다는 것을 알고 가야 한다.

ISECOM 역시 Hacker Highschool 세미나를 여러 지역에서 개최해 왔다. 세미나에서는 HHS의 일부 레슨들을 보다 심도 있게 다루고 프로 해커들이 나와 해킹과 해커가 되는 방법에 대한 강의를 한다. 또한 해커는 어떤 인물들이고 왜 해킹을 하는지 연구하기 위한 UN과의 합작 프로젝트인 **Hacker Profiling Project**의 조사를 통해 도출한, 진정한 해커란 어떤 존재인지에 관해 날카로운 통찰력

을 보여준다. 만약 이 세미나에 참석한다면 해킹의 밝은 면에 대한 이해도를 높일 수 있을 것이다.

늘 지적인 호기심을 가지고 어떤 환경에서도 목표를 이뤄내는 해커가 될 수 있는 방법이 바로 우리가 여러분에게 알려줄 수 있는 가장 중요한 정보들 중 하나 이다. 해커들은 어떻게 스스로 학습해 나가야 하는지 알고 자기가 배운 것 이상을 추구하며 필요한 기술들을 스스로 획득해 나간다.

HHS의 레슨을 당신의 학교에서 시작하는 방법을 배우기 위해 당신은 당신의 부모님 혹은 선생님에게 언제든 물어 볼 수 있다. 자세한 내용은 ISECOM에 문의하면 된다.

앞으로의 학습방향

이제는 지금까지 배운 것들을 계속해서 연습해야 한다. 연습을 많이 할수록 더 많은 정보를 빠르게 찾아내고 배우는 속도를 높일 수 있다. 하지만 비판적 시각을 기르는 것을 게을리 해서는 안 된다. 모든 정보가 진실이 아니라는 것을 명심하자.

늘 다음과 같은 질문들을 스스로에게 하는 습관을 기르자. 왜 저 사람이 거짓말을 하는가? 사람을 속이거나 루머를 퍼트리는 일이 돈과 연관되어 있는가? 진실의 출처는 어디인가? 그리고 가장 중요한 질문인, 진실의 범위가 어느 정도인가?

해킹과 마찬가지로 연구 활동은 특정 조사 범위에서 결과를 도출해내기 때문에 통계치, 퍼센티지, 확률들을 확인할 때는 주의해야 한다. 연구 결과를 보면 그 연구의 조사 범위가 어느 정도인지 항상 확인해야 한다. 주로 범죄나 건강 관련 이슈에서 통계수치를 많이 사용하지만 대부분 샘플의 양이 작고 지역이 한정되어 있는 경우가 많다. 한 도시에 사는 시민 200명의 10%가 어떤 영향을 받았다는 결과가 나라 전체 인구의 10%에 동일하게 적용되는 것은 아니다. 그러니 정보를 이해하고 탐색할 때는 영리해질 필요가 있다. 조사 범위를 확인하느냐 마느냐 하는 단순한 행동이 큰 차이를 이끌어낸다.

Hacker Highshcool 프로그램에 관해 좀 더 추가적인 공부를 하고 싶다면 아래의 개념이나 단어를 추가로 탐색해 보자.

- Meta Search
- The Invisible Web
- Google Hacking
- How Search Engines Work
- The Open Source Search Engine
- The Jargon File
- OSSTMM
- ISECOM Certifications:
  - OPST (OSSTMM Professional Security Tester)
  - OPSA (OSSTMM Professional Security Analyst)
  - OPSE (OSSTMM Professional Security Expert)
  - OWSE (OSSTMM Wireless Security Expert)
  - CTA (Certified Trust Analyst)
  - SAI (Security Awareness Instructor)

오늘날의 십대들은 SNS, 인터넷 등을 통해 전 세계와 연결되어있다.
그러나 그들은 사기, 신원 위조, 개인정보 유출 등의
인터넷을 통한 공격방식과 이에 대한 대처방법을 잘 알지 못한다.
해커하이스쿨은 이러한 학생들을 위한 지침서가 될 것이다.

해커하이스쿨 프로젝트는 중·고등학생들에게 보안과 개인정보에 대한 인식을 제고하고 향상시킬 수 있는 교육자료이다

해커하이스쿨은 올바른 해커양성을 목적으로하며 이론과 실전파트로 구성되어있다. 해커는 지적능력, 창의성, 논리성을 모두 갖춰야한다. 우리는 학생들에게 일반적인 사이버보안 인식 혹은 IT 기술의 교육뿐만 아니라 어떻게 해커의 자질을 기르고 향상시킬 수 있는지를 가르칠 필요가 있다. 이 프로그램은 보안과 개인정보 인식교육 자료를 무상으로 포함하고 있으며 승인받은 중교등학교 선생님들을 위한 백앤드 서비스도 지원중이다. 다양한 언어로 지원되고 있으며 이 수업은 안전한 인터넷 사용, 웹 개인정보, 인터넷검색, 바이러스나 악성코드를 피하는법 윤리와 법 등을 포함한다.

HHS 프로그램은 ISECOM, 비영리단체, 보안 인식과 전문적인 보안 개발과 승인에 초점을 맞춘 오픈소스리서치 그룹에 의해 개발 되었다.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM