# 1 해킹 기술의 진화

## 1 국내 해커의 역사

### 1986년

- KAIST의 김창범이 '유니콘'이라는 해커 동아리를 만든 것이 시초

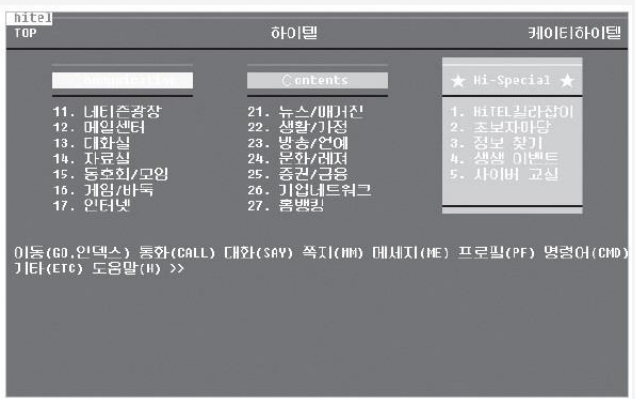
### 1991년

- KAIST에 해커 그룹 '쿠스'가 만들어지고 포항공과대학교에 '플러스'가 생김
- KAIST와 포항공과대학교 간의 유명한 해킹 전쟁이 일어난 후 쿠스 해체
- 쿠스 멤버 중 하나였던 김휘강은 보안을 강조한 시큐리티카이스트를 만듦

## 1 국내 해커의 역사

### 1990년대

- 당시 통신 프로그램이 전화 모델을 이용했기 때문에 시스템과 네트워크의 취약점을 공략하는 공격 기법이 거의 대부분임(응답하라 1988, 시스템 보안, 네트워크 보안)




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 1 국내 해커의 역사

### 1990년대 후반

- 국내 1세대 해커들이 보안 전문 회사를 만들고,
  언더그라운드에서 오버그라운드로 전환하여
  본격적으로 활동 전개
- 수많은 보안 회사가 생겨나고,
  널루트, 와우해커와 같은 언더해커 그룹 등장

### 2000년

- 제1회 세계정보보호올림페어
  (일명 국제해킹왕중왕대회) 개최

## 1 국내 해커의 역사

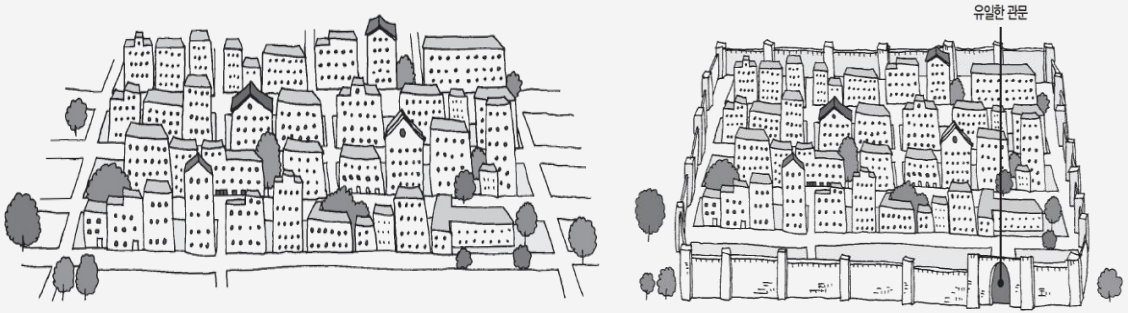
### 2001년

- 제2회 해킹왕중왕대회 개최
- truefinder, Xpl017Elz(X82) 등의 해커가 큰 활약을 함
- P2P 메신저 프로그램이 처음 나오면서 사람들의 호기심과 관심을 불러일으킴
- (Server vs. P2P)


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 웹 해킹의 발전 배경

- 1990년대 중반부터 방화벽, IDS와 같은 네트워크 보안 장비가 개발되면서 웹해킹 발전(IPS, FDS)
- 닷컴 열풍이 불면서 해커들이 점차 웹에 관심을 가지면서 웹의 취약점 연구도 활발하게 진행




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 웹 해킹의 발전 배경

### 포트(Port)

- 영어로 '항구'라는 뜻
- '인터넷의 바다', '인터넷 항해'라는 말이 쓰인 것도 한 시스템의 포트에서 데이터가 출발하여 인터넷이라는 바다를 건너 다른 시스템의 포트에 도달하는 흐름이었기 때문
- 2000년 중반부터는 거의 모든 시스템이 방화벽으로 보호되어 80번 웹 포트 외에는 모두 닫혀 있는 경우가 많아져 웹 해킹이라는 주제가 많이 연구됨(Port, HTTP, FTP, SMTP)

# 2 일반적인 웹 해킹 과정

# 2 | 일반적인 웹 해킹 과정

## 1 웹 해킹 방법

- 취약점의 존재 여부를 확인한 후 그곳을 통해 침투를 시도하는 방법(위협)
- 발견 가능한 모든 공격 표면을 찾아 매트릭스를 작성한 후 하나씩 시도하는 방법(kill chain)

## 2 시스템에 침투하는 일반적인 해킹 과정


과거에는 해커가 자신의 명성을 높이기 위해
공격 성공 후 웹 페이지를 변조하는 경우가 많았으나
요즘은 **흔적을 교묘히 숨기는 경우**가 많아짐(**APT, 사전조사, 제로데이공격, 사회공학, 은닉, 적응, 지속**)

## 2 시스템에 침투하는 일반적인 해킹 과정

### 공격 대상 선정

- 일반적으로 방문자가 많은 대표적인 웹 사이트를 주요 공격 대상으로 선정(웜을 심어놈)
- 기업과 계약하여 모의해킹을 할 때는 주로 공격 대상 목록을 사전에 선정
- 외부에서 접근할 수 있는 모든 대상을 선정해도 무방할 경우 관련 도메인을 모두 검색한 후 가장 취약한 곳을 대상으로 함

## 2 시스템에 침투하는 일반적인 해킹 과정

### 정보 수집

- 공격 대상이 보유하고 있는 외부 접점 중에서 웹 사이트를 통해 웹 애플리케이션을 개발할 때 사용한 언어, 웹 사이트 내 주요 공격 대상의 기능, 웹 서버의 종류 등을 알아보는 것(툴 존재, 실습)
- 공격 대상의 특성과 취약한 표면을 찾음

## 2 시스템에 침투하는 일반적인 해킹 과정

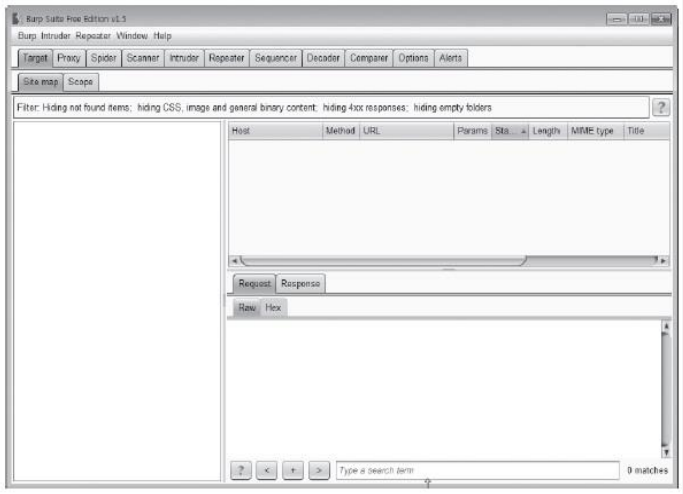
### 자동화 도구를 이용한 웹 사이트 탐색 및 분석

- 공격할 웹 사이트에 접속한 후 취약점이 가장 많이 발생하고 영향력이 큰 영역을 먼저 조사(Exploit, 제로데이공격)
- 웹 사이트를 탐색하면서 사용자 로그인 부분, 게시판이나 자료실처럼 파일을 업로드 할 수 있는 부분이 있는지 살펴봄(취약점)
- 웹 사이트의 디렉터리 구조나 소스코드 간의 연관성과 같은 기본 정보를 얻을 수 있는지 파악(하드코드된 비밀번호)

## 2 시스템에 침투하는 일반적인 해킹 과정

### 자동화 도구를 이용한 웹 사이트 탐색 및 분석

**① Burp Suite 실행**




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### 자동화 도구를 이용한 웹 사이트 탐색 및 분석

**② 웹 사이트 접속**

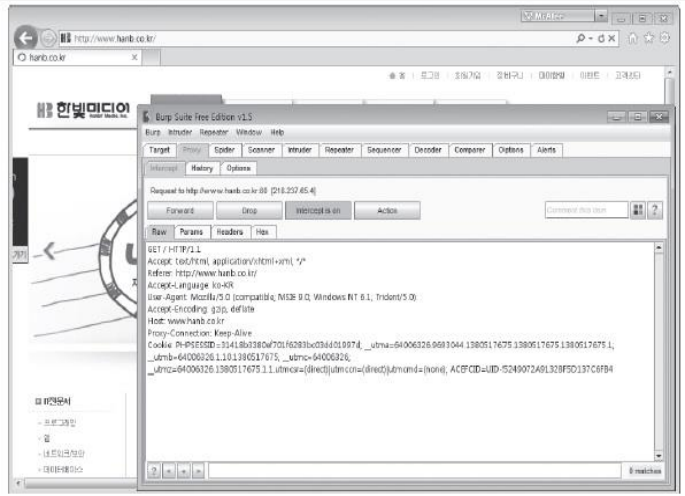
**③ ~ ④ 프록시 설정 후 동작 확인**

- 브라우저의 [도구]-[인터넷 옵션]-[연결]을 선택 후 〈LAN 설정〉 클릭
- 브라우저를 '새로 고침'하여 프록시가 제대로 동작하는지 확인

## 2 시스템에 침투하는 일반적인 해킹 과정

### 자동화 도구를 이용한 웹 사이트 탐색 및 분석

**③ ~ ④ 프록시 설정 후 동작 확인**



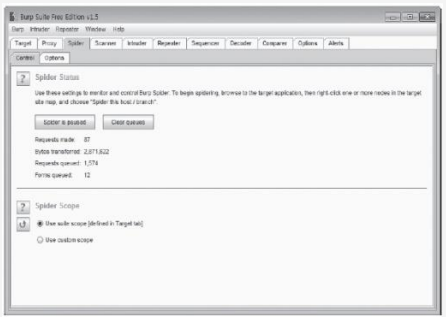

※ 출처 : 인터넷 해킹과 보안,
김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### 자동화 도구를 이용한 웹 사이트 탐색 및 분석

#### ⑤ Intercept 설정 해제

- [Proxy]-[Intercept] 탭에서 〈Intercept is on〉을 클릭하여 〈Intercept is off〉로 변경되면 정상적으로 패킷이 흘러가게 한 후 [Spider] 탭을 클릭



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### 자동화 도구를 이용한 웹 사이트 탐색 및 분석

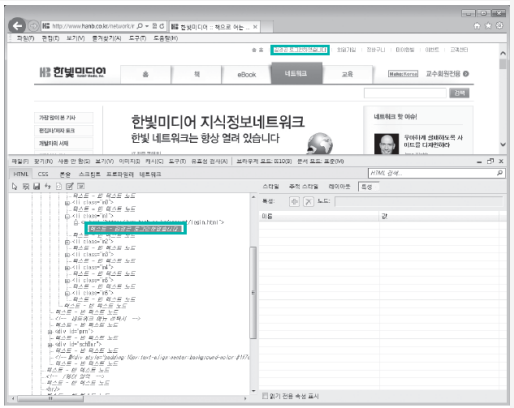
#### ⑥ Spider 실행

- [Spider] 탭에서 〈Spider is paused〉를 클릭하면 Spider가 실행되고 Requests made와 Bytes transferred가 증가하면서 웹 사이트의 정보를 가져옴
- [Target] 탭에 들어가면 방문한 사이트의 디렉터리 구조와 파일 목록, HTML 소스코드 구조 등을 파악할 수 있음

## 2 시스템에 침투하는 일반적인 해킹 과정

### 브라우저의 확장 기능을 이용한 웹 사이트 탐색 및 분석

- 인터넷 익스플로러의 [도구] 메뉴에 웹 애플리케이션 개발자가 웹 사이트의 구조를 쉽게 파악하기 위해 만들어놓은 [F12 개발자 도구] 메뉴가 있음




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### 검색 엔진을 이용한 정보 수집

- 가장 쉽게 많은 정보를 수집할 수 있는 방법
- 구글의 고급 검색 기능

| 검색 인수 | 설명 |
|---|---|
| site: | 특정 도메인으로 지정한 사이트에서 검색하려는 문자열이 포함된 사이트를 찾는다. |
| filetype: | 특정 파일 타입에 한해 검색하려는 문자가 포함된 사이트를 찾는다. |
| link: | 링크에 검색하려는 문자가 포함된 사이트를 찾는다. |
| cache: | 특정 검색어에 해당하는 캐시된 페이지를 보여준다. |
| intitle: | 페이지의 제목에 검색하려는 문자가 포함된 사이트를 찾는다. |
| inurl: | 페이지의 URL에 검색하려는 문자가 포함된 사이트를 찾는다. |

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### 검색 엔진을 이용한 정보 수집

**site:**

- 특정 사이트만 선택해서 집중적으로 검색할 때 사용
- 예 ) site:co.kr admin

## 2 시스템에 침투하는 일반적인 해킹 과정

### 검색 엔진을 이용한 정보 수집

**filetype:**

- 특정 파일 타입을 검색할 때 사용(PDF, PPT)


※ 출처 : 인터넷 해킹과 보안,
김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### 검색 엔진을 이용한 정보 수집

**link:**

- 특정 링크가 포함된 페이지를 검색할 때 사용
- 예) link:korea.ac.kr

**cache:**

- 백업된 데이터를 볼 때 사용(cache?)
- 예) cache:korea.ac.kr

## 2 시스템에 침투하는 일반적인 해킹 과정

### 검색 엔진을 이용한 정보 수집

**intitle:**

- 디렉터리 리스팅에 취약한 사이트를 검색할 때 사용(디렉터리 리스팅)
- 예) intitle:index.of name size
- intitle의 위험성이 많이 알려져 요즘은 intitle로 검색해도 결과가 예전만큼 많이 나오지 않음

## 2 시스템에 침투하는 일반적인 해킹 과정

### 검색 엔진을 이용한 정보 수집

**inurl:**

- site와 유사한 기능으로, 특정 URL만을 대상으로 검색
- 예) ‘inurl:admin/login.asp .com’으로 검색하면 URL이 .com이면서 admin/login.asp 페이지가 있는 사이트를 검색
- admin 디렉터리에 접근하지 못하게 하려면 [Disallow: /admin/] 입력(서버쪽)

## 2 시스템에 침투하는 일반적인 해킹 과정

### 스캐닝 도구를 이용한 정보 수집

- 웹 스캐닝 도구를 이용하면 웹 서버의 종류와 버전, 디렉터리 정보나 중요한 파일 정보가 존재하는지 여부, 웹 서버 자체의 취약점 등을 검사할 수 있음(창과 방패)

## 2 시스템에 침투하는 일반적인 해킹 과정

### ▶ 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

실습 환경

- 윈도우 기반의 운영체제
- 필요 프로그램 : 웹 서버가 설치된 서버, Wikto

## 2 시스템에 침투하는 일반적인 해킹 과정

### ▶ 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

#### ① Wikto 스캐너 준비

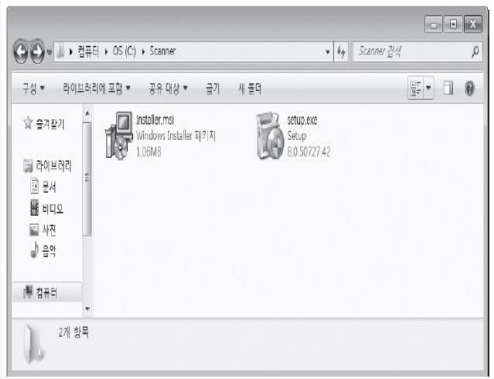
- Wikto는 공개 웹 스캐닝 도구로, 다양한 플랫폼에서 동작하고 수천 개의 웹 취약점을 스캐닝 할 수 있음(Nikto)

## 2 시스템에 침투하는 일반적인 해킹 과정

### ▶ 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

② 압축 해제



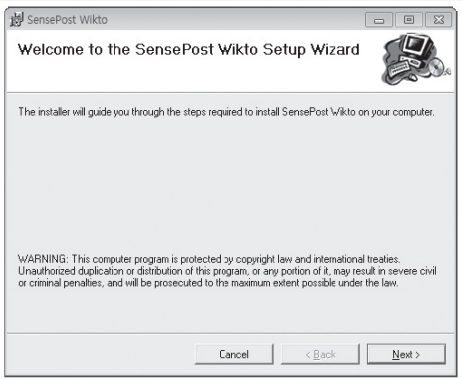

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

#### ③ Wikto 스캐너 설치




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### ▶ 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

④ Wikto 스캐너 실행

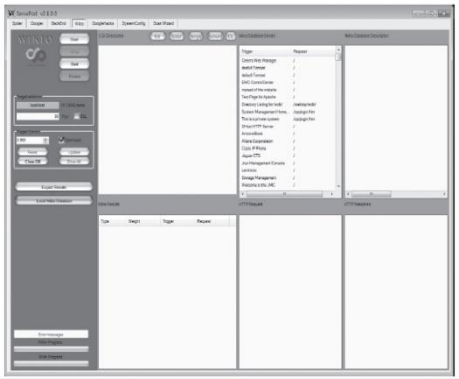
- [시작]-[모든 프로그램]-[SensePost]-[Wikto]에서 Wikto를 선택
- Wikto를 실행한 후 왼쪽에 있는 <Load Nikto Database>를 클릭하여 데이터베이스 파일을 불러옴

## 2 시스템에 침투하는 일반적인 해킹 과정

### ▶ 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

④ Wikto 스캐너 실행



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 시스템에 침투하는 일반적인 해킹 과정

### ▶ 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

⑤ 주의사항

- 현행법상 스캐닝만 해도 공격으로 간주하여 처벌받으니 개인 테스트용 컴퓨터나 허가 받은 컴퓨터만을 대상으로 웹 스캐닝을 해야 함

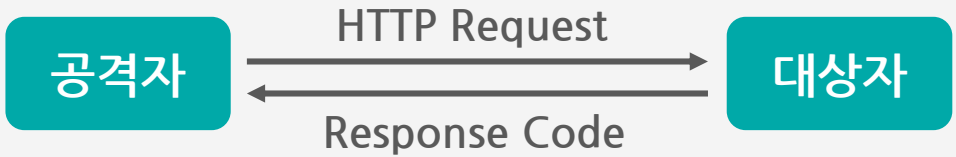
## 2 시스템에 침투하는 일반적인 해킹 과정

### ▶ 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

⑤ 주의사항

- 웹 스캐닝 도구의 원리(반송 - 프로토콜)



## 2 시스템에 침투하는 일반적인 해킹 과정

### ▶ 스캐닝 도구를 이용한 정보 수집

**웹 스캐닝으로 웹 사이트 정보 수집하기**

#### ⑤ 주의사항

- 취약점 검색을 위한 HTTP Request의 내용

```
1913 "iis","/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir","<DIR>","GET","IIS Unicode command exec problem, see
     http://www.wiretrip.net/rfp/p/doc.asp?id=57&face=2 and http://www.securitybugware.org/NT/1422.html. CVE-2000-0884"
1914 "iis","/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\"","boot.ini","GET","IIS Unicode command exec problem, see
     http://www.wiretrip.net/rfp/p/doc.asp?id=57&face=2 and http://www.securitybugware.org/NT/1422.html. CVE-2000-0884"
1915 "iis","/scripts/admin.pl","200","GET","Default FrontPage CGI found."
1916 "iis","/scripts/Carello/Carello.dll","200","GET","Carello 1.3 may allow commands to be executed on the server by replacing
     hidden form elements. This could not be tested by Nikto."
1917 "iis","/scripts/cfgwiz.exe","200","GET","Default FrontPage CGI found."
1918 "iis","/scripts/CGImail.exe","200","GET","Default FrontPage CGI found."
1919 "iis","/scripts/contents.htm","200","GET","Default FrontPage CGI found."
```

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017