정보보안 Path Finder

- 정보보안 개요와 진로, 분야 정리 프로젝트

내용 수정이 필요하시면 paul-lab@naver.com으로 연락주세요.

1. 정보보안 개요 - 해킹과 해킹 방어
2. 정보보안 진로
3. 국가 주도 추천 코스와 자격사항
4. 시스템 보안, 네트워크 보안, 어플리케이션 보안,
   리버스 엔지니어링, 포렌식, 버그헌팅, 암호학
5. 웹 해킹 개요 (XSS, SQL Injection,
   파일 업로드, 디렉터리 노출, 쿠기 변조, DBD, 애러노출과 구글해킹

00부대 서버정비장교, CERT과장 역임
한국공학기술연구원 팀장
삼성전자 주니어소프트웨어 아카데미 메인 강사
신한금융그룹 정보보안 담당
제주 코딩 베이스캠프 외 다수의 사회공헌 활동
제주대학교 컴퓨터공학과 풀스택 강의 강사
튜토리얼로 배우는 Python 외 다수 IT 서적 집필

현) 바울랩 ICT 기술연구원 대표
현) 바울랩 ICT 컴퓨터학원 대표
현) 사도출판 대표
현) 주식회사 위니브 대표
현) 바울랩 미디어 대표
현) 제주스타트업협회 부회장
현) Google Developers Group JEJU 오거나이저

해킹(hacking)은 소프트웨어, 네트워크, 웹 서비스, 앱 등 각종 정보 체계가 본래의 의도를 벗어난 동작을 일으키도록 하거나 주어진 권한 이상의 정보를 열람, 복제, 변경 가능하게 하는 행위를 광범위하게 이르는 말

"침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률, 제2조 7호

파밍과 홈페이지 위변조

보안 취약점을 찾아내어
그 문제를 해결하고 이를 악의적으로 이용하
는 것을 방지하는 행위를 말한다.

해커의 분류

	조직적	혼재	비조직적
합법	화이트 햇 해커		버그바운티
불법	사이버 테러리스트 사이버 갱조직 등	핵티비스트	블랙 햇 해커
그 어딘가	국가 소속 활동가 (Nation State Actors)	사이버 용병 (Cyber Mercenaries)	스크립트 키디 (Script Kiddies) 그래이 햇 해커 국가 지원 해커 (Nationalist hackers)

NASA를 들었다 놓았던 천재해커의 나이

17살

해킹이 발생했을 경우,
해킹이 발생한 것을 인지하기까지의 시간

146일

2200만명의 직원 정보 탈취를 당했던 미국 인사처는 해킹을 인지하는데 343일이 걸렸다. 평균 해킹을 당한 것을 인지하는데 146일이 걸린다고 한다.

2010년 초반 구글 크롬북 해킹 상금은 한화로 1억 2천만원이었으며 테슬라의 모델S 해킹 상금은 한화로 1,137만원이었습니다. 그러나 테슬라는 하루만에 해킹 당했습니다.
지금은 얼마일까요?

150만 달러

구글, 애플(건당 20만달러에서 100만달러로 5배),
삼성(해킹방어대회 개최), **현대**(화이트 햇 해커 조직 운영), **그 외 많은 기업**

연변 모바일 갱

1. 중국 길림성의 연변에 거주하고 있어 연변 모바일 갱이라고 불리며, 이곳은 중국과 북한의 경계에 위치한 도시입니다.

2. 활발히 활동중인 모바일 갱에는 표적과 안티바이러스 애플리케이션에 맞게 악성코드를 신속하게 적용시키기 위한 다양한 역할들이 있습니다. 모바일 갱은 조직책, 통역사, 카우보이, 악성코드 제작자로 구성됩니다.

3. 가짜 뱅킹 어플리케이션, 인기 있는 어플리케이션을 모방한 가짜 어플리케이션, 각종 무료 SW(게임 크랙 등), 음란물 앱

어나니머스

해커 집단

세계적 활동

'익명'

약 3000명

핵티비스트

Anonymous
어나니머스

구글해킹, 프록시 변조

보안 관제실

(CERT 침해사고대응과 함께하는 경우가 많음)

보안 운영

정보보안 R&D

기업 정보보안 팀의 구조

출처 : http://news.bizwatch.co.kr/article/mobile/2018/06/29/0030,
한국인터넷진흥원 정보보안 관제실

공격자와 방어자

공격자와 방어자

공격자

방어자

공격자와 방어자

시스템 & 네트워크 공격	WAF
사회공학적 공격	Anti DDoS(DDX)
제로데이 공격	IDS & IPS
APT 공격	FireWall
...	...
각 종 해킹 공격	해킹 공격의 대응책

1. 정보보안 개요 - 해킹과 해킹 방어
2. **정보보안 진로**
3. 국가 주도 추천 코스와 자격사항
4. 시스템 보안, 네트워크 보안, 어플리케이션 보안,
   리버스 엔지니어링, 포렌식, 버그헌팅, 암호학
5. 웹 해킹 개요 (XSS, SQL Injection,
   파일 업로드, 디렉터리 노출, 쿠기 변조, DBD, 애러노출과 구글해킹

정보보호 인력이란 조직이 보유하고 있는 비즈니스 자산을 다양한 공격으로부터 효과적, 효율적으로 보호하기 위한 **다차원적인 보호 활동**을 수행할 수 있는 지식과 역량을 보유하고 있는 전문 인력을 의미

출처 : KISA 정보보안 진로 가이드

그래서 뭐부터 해야 하죠?

광범위한 분야, 빠른속도로 발전하는 기술,
상당한 깊이의 지식

지금 이시간, 여러분이 공부하고 있는 동안에도 거미줄처럼 얽힌 여러
Code들은 Version은 업데이트 되고 있죠.

맛보기를 통해, 진로를 찾고, 스스로 공부해
가는 시간이 필요합니다.

가능하다면, 가르침에 기대려 하지 마세요.

그것은 이미 낡은 지식일 가능성이 큽니다.

지식에 관련된 얘기는
4장과 5장에서 할 예정이에요.

개발
사전 침투 / 방어
사후 조사
수집 / 해독
진단 / 평가
관리
감독 / 총괄

출처 : KISA 정보보안 진로 가이드

총 7개의 직업군에 대해 살펴봅시다.

1. 보안제품 개발자(개발)

정보보호 관련 사고를 미연에 방지하기 위해서 보안이 필요한 분야에서 요구되는 소프트웨어 프로그램을 개발하는 전문가

출처 : KISA 정보보안 진로 가이드

그러나, 방어쪽만 있는 것은 아닙니다.

2. 침해사고 대응 전문가(사전침투/방어)

보안사고가 발생했을 때 피해규모를 최소화 하기 위해 사고를 보고하고 시스템을 구축하고 예방전략을 수립하는 일을 하는 전문가

출처 : KISA 정보보안 진로 가이드

관제 / CERT, 취약점 분석, 모의해킹

3. 디지털 포렌식 전문가 (사후조치)

정보자산을 위협하여 보안사고를 발생시키는
요인에 대하여 증거를 수집하여 복구하고 추
적하는 활동을 수행하는 일을 합니다.

출처 : KISA 정보보안 진로 가이드

국정원, 경찰청, 검찰청, 군 등

4. 악성코드 분석 전문가 (수집/해독)

새로운 악성코드를 분석하여 감염 경로나 방법-증산-치료 방법 등을 개발하고 치료할 수 있는 백신 프로그램을 제작하는 일을 하는 전문가

출처 : KISA 정보보안 진로 가이드

동적분석과 정적분석 그리고 패턴화

5. 보안 컨설턴트 (진단/평가)

고객의 정보자산과 비즈니스 프로세스에 따른 위협 및 취약점을 분석하여 보안 수준을 파악하고, 요구 수준에 맞는 통합적인(기술 + 관리) 보안 해결책을 설계하는 전문가

출처 : KISA 정보보안 진로 가이드

정보시스템 감리사, 정보시스템 보안 감사, 보안제품 인증 전문가, 보안기술 컨설턴트

6. 보안 관리자 (관리)

조직관점에서 보안이라는 목적을 달성하기 위하여 보안과 관련된 정책-관리체계-시스템 구축-운영(관리) 업무를 실제적으로 수행하는 전문가

출처 : KISA 정보보안 진로 가이드

DB, 시스템, 개인정보보호 관리자 등

7. 최고 보안 관리자 (감독/총괄)

조직의 경영 관점에서 전체적인 보안전략을
총괄적-통합적으로 수립하고 운영하며 조정
하는 전문가

출처 : KISA 정보보안 진로 가이드

정보보호 직무

CEO
(Chief Executive Officer)

CIO
Chief
Information Officer
정보관리책임자

CISO
Chief
Information Security
Officer
정보보안책임자

CFO
Chief
Finance Officer
재무 책임자

COO
Chief
Operating Officer
운영책임자

CSO
Chief
Security Officer
보안담당책임자

CTO
Chief
Technology Officer
최고기술책임자

한 마디로, 보안 총괄!

너무 많고, 복잡하죠?

선택과 집중.

넓고, 얇게 경험해 본 다음, 여러분의 분야를
정하고, 깊게 공부하는 시간이 필요합니다.

만약 정보보안으로 진로를 정하셨다면,

1. 초, 중, 고 학생의 경우 : 관련 대학교 학과가 있습니다.

2. 관련 학과 재학중이거나, 졸업을 한 경우 : 정보보안 기사를 준비하세요.(3강에서 자격사항 언급)

3. 관련 학과를 졸업하지 않은 비전공자 :

1. 정보보안 개요 - 해킹과 해킹 방어
2. 정보보안 진로
3. **국가 주도 추천 코스와 자격사항**
4. 시스템 보안, 네트워크 보안, 어플리케이션 보안,
   리버스 엔지니어링, 포렌식, 버그헌팅, 암호학
5. 웹 해킹 개요 (XSS, SQL Injection,
   파일 업로드, 디렉터리 노출, 쿠기 변조, DBD, 애러노출과 구글해킹

체계적으로 배우고 싶어요.

앞서 말씀드린 것처럼,
스스로 커리큘럼을 빌딩하시는 것이 좋습니다.

정보보안 관련 학교 및 학과

* 출처 : 나무위키, KISA 정보보안 진로 가이드, 대학교 홈페이지

수도권 정보보안 관련학과

고려대학교 사이버국방학과
서울여자대학교 정보보호학과
성신여자대학교 융합보안학과
세종대학교 정보보호학과
상명대학교 해킹방어학과
수원대학교 정보보호학과
경기대 융합보안학과
세종사이버대학교 정보보호시스템전공
건국대학교 정보보안전공
고려대학교 정보보호대학원
단국대 멀티미디어대학원 정보보호학과
고려대학교 정보보호 대학원
서울여자대학교 정보통신공학부(정보보호공학)
세종사이버대학교 정보보호시스템학과
동국대 국제정보대학원 정보보호학과

지방권 정보보안 관련 대학교

건양대학교 정보보호학과
경복대 정보보호학과
경원대학교 소프트웨어학부(정보보호학과)
대전대학교 기초과학부(전산정보보호학과)
대불대학교 정보보안공학과
목원대학교 전자정보보호소학부(정보보호공학)
목포대학교 정보공학부(정보보호공학)
세명대학교 인터넷정보학부(정보보호공학)
순천향대학교 정보보호학과
아주대 정보통신대학원 정보통신학과(정보보안전공)
전주대학교 정보기술컴퓨터공학부(정보보호공학)
한국기술교대 인터넷미디어공학부(정보보호공학)
한국정보통신대학교(카이스트) 공학부(정보보호트랙)
호서대학교 컴퓨터공학부(정보보호전공)
호원대학교(사이버수사경찰학부)
중부대학교(정보보호학과)
우석대학교(정보보안학과)
순천향대학교(정보보호학과)
동양대학교(컴퓨터정보전학과)
동명대학교(정보보호학과)
대구한의대학교(정보보호학과)

정보보안 관련 대학원

건국대학교 정보통신대학원 정보보안학과
고려대학교 정보보호대학원
동국대학교 국제정보보호대학원
서강대학교 정보통신대학원 정보보호전공
성균관대학교 정보통신대학원 정보보호학과
연세대학교 정보대학원 정보보호 트랙
아주대학교 정보통신대학원 사이버보안전공
중앙대학교 일반대학원 융합보안학과
KAIST 정보보호대학원
경기대학교 일반대학원 산업보안학과
한양대학교 일반대학원 정보보안학과
숭실대학교 정보과학대학원 정보보안학과

각 과에 대한 상세 모집요강 확인 必
예시 : 고려대학교 사이버 국방학과
1단계 : 서류 100%
2단계 : 1단계 성적 60% + 면접 20% + 기타 20%
군 면접 + 체력검정)
(수능 전국 0.1%, 코드게이트 해킹 방어대회 1등
수상자 등 가산점)

* 인지도 및 선호도 순이 아닙니다.

학교 말고 배울 수 있는 곳은 없나요?

해킹대회와 컨퍼런스, 커뮤니티, SNS 와 동아리, 워게임, 정보보안 YouTube, 정보보안 유무료 강의, BoB, 주니어 케이쉴드와 같은 국가 주도 정보보안 인력 양성 프로그램 등

차례대로 살펴봅시다.

국내 해킹대회

국외 해킹대회

국내 정보보안 컨퍼런스

국외 정보보안 컨퍼런스

SNS 정보보안 커뮤니티

일반 정보보안 커뮤니티

워게임

정보보안 YouTube

유무료 온오프라인 강좌

K-Shield (정보보안 관련직종 직장인)

주니어 K-Shield (대~일반인)

BoB (중~대)

자격증은 필요한가요?

네, 좋아하진 않지만,
시야가 넓어지는 것은 맞습니다.

직장을 구하실 때,
이직 하실 때 도움이 되기도 해요.

난이도 초급 :

정보보안 산업기사, 정보보안 기사
정보처리기사
빅데이터분석기사
디지털포렌식전문가 2급
네트워크 관리사 2급, 리눅스 마스터, CPPG, SQLD
CCNA, CCNP, CCDA, CCDP, OCJP, CSA, OCNA
MCP, MCSE, MCSD, OCP, CNE, PIP

난이도 중급 :

CISSP, CISA
CISM, CFPS, CFP, CIA
DAP, SQLP
ISMS-P(구 ISMS)

난이도 고급 :

정보통신 기술사, 정보처리 기술사(기술사는 기사 자격증 취득 후 4년 경력)
OCM, CCIE
정보시스템감리사(기사자격증 취득 후 7년 경력)

1. 정보보안 개요 - 해킹과 해킹 방어
2. 정보보안 진로
3. 국가 주도 추천 코스와 자격사항
4. **시스템 보안, 네트워크 보안, 애플리케이션 보안,**
   리버스 엔지니어링, 포렌식, 버그헌팅, 암호학
5. 웹 해킹 개요 (XSS, SQL Injection,
   파일 업로드, 디렉터리 노출, 쿠기 변조, DBD, 애러노출과 구글해킹

1. 시스템 보안
2. 네트워크 보안
3. 어플리케이션 보안
4. 리버스 엔지니어링
5. 포렌식
6. 버그헌팅
7. 암호학

예) 권한 탈취, 상승 해킹 기법　　예) 메모리 삽입이나 오염

패스워드, 접근 제어, 권한, 로그, 취약점, 메모리 조작
DB의 데이터 암호화, 응용프로그램 관리

예) 프로세스 확인

컴퓨터와 시스템을 장학하기 위한
가장 유효한 공격 방법

2010년 이란의 핵 시설을 공격 - 스턱스넷
2014년 한국수력원자력 발전소 해킹 - 한글

....

6개월 이상의 잠복기간

시스템 마비
시스템 정보 탈취
계좌 획득
정보 위변조

언어는 주로 C, Python

Google 에서 취약점 가이드 라고 검색해보세요.

remote exploit, vulnerable exploit

https://www.rapid7.com/
securityvulns.com/files
www.outpost9.com/exploits
https://packetstormsecurity.com/
등

1. 시스템 보안
2. **네트워크 보안**
3. 어플리케이션 보안
4. 리버스 엔지니어링
5. 포렌식
6. 버그헌팅
7. 암호학

DDoS, DoS(Teardrop Attack, LAND Attack, SYN Flooding Attack, smurf Attack, ...), 스니핑, 스푸핑, 세션 하이제킹, Scanning Attack,

7.7 DDoS 공격사건

대규모 공격,
하지만, 진짜 공격을 숨기기 위한 용도로도 사용

공격 코드 : Python
(Python DoS code)

패킷분석 : Wireshark

1. 시스템 보안
2. 네트워크 보안
3. **애플리케이션 보안**
4. 리버스 엔지니어링
5. 포렌식
6. 버그헌팅
7. 암호학

애플리케이션 보안(Application security)은 응용 소프트웨어의 보안 정책에서의 결함이나 시스템 개발에서의 눈에 띄지 않는 위약점들 같은, 코드의 생명주기 전체 과정을 아우른다.

- Wiki

웹, 앱 뿐만 아니라 응용 프로그램

애플리케이션 보안 가이드,
시큐어 코딩 가이드

1. 시스템 보안
2. 네트워크 보안
3. 어플리케이션 보안
4. **리버스 엔지니어링**
5. 포렌식
6. 버그헌팅
7. 암호학

Reverse Engineering
역공학(　　學)

분해, 분석 -> 재조합, 새로운 제품

정보보안에서의 목적?

취약점 분석과 악성코드 분석

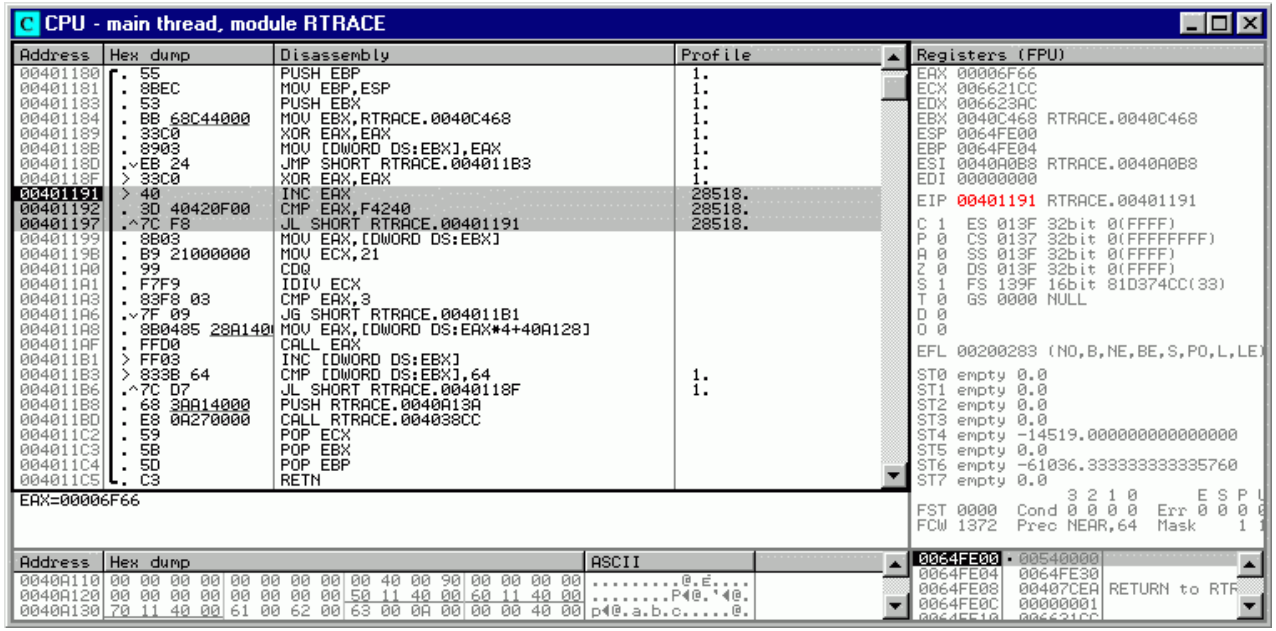
그럼 꼭 분석을 해야만 바이러스인 것을 알까요?

바이러스토탈

프로그래밍 언어, 레지스터, 메모리, CPU, 운영체제 등

ollydbg, IDA 등의 도구

4. 리버스 엔지니어링


CPU - main thread, module RTRACE
Address | Hex dump | Disassembly | Profile
00401180 . 55 PUSH EBP 1.
00401181 . 8BEC MOV EBP,ESP 1.
00401183 . 53 PUSH EBX 1.
00401184 . BB 68C44000 MOV EBX,RTRACE.0040C468 1.
00401189 . 33C0 XOR EAX,EAX 1.
0040118B . 8903 MOV [DWORD DS:EBX],EAX 1.
0040118D .v EB 24 JMP SHORT RTRACE.004011B3 1.
0040118F > 33C0 XOR EAX,EAX 1.
00401191 > 40 INC EAX 28518.
00401192 . 3D 40420F00 CMP EAX,F4240 28518.
00401197 .^7C F8 JL SHORT RTRACE.00401191 28518.
00401199 . 8B03 MOV EAX,[DWORD DS:EBX]
0040119B . B9 21000000 MOV ECX,21
004011A0 . 99 CDQ
004011A1 . F7F9 IDIV ECX
004011A3 . 83F8 03 CMP EAX,3
004011A6 .v 7F 09 JG SHORT RTRACE.004011B1
004011A8 . 8B0485 28A140 MOV EAX,[DWORD DS:EAX*4+40A128]
004011AF . FFD0 CALL EAX
004011B1 > FF03 INC [DWORD DS:EBX]
004011B3 > 833B 64 CMP [DWORD DS:EBX],64 1.
004011B6 .^7C D7 JL SHORT RTRACE.0040118F 1.
004011B8 . 68 3AA14000 PUSH RTRACE.0040A13A
004011BD . E8 0A270000 CALL RTRACE.004038CC
004011C2 . 59 POP ECX
004011C3 . 5B POP EBX
004011C4 . 5D POP EBP
004011C5 . C3 RETN
EAX=00006F66
Registers (FPU)
EAX 00006F66
ECX 006621CC
EDX 006623AC
EBX 0040C468 RTRACE.0040C468
ESP 0064FE00
EBP 0064FE04
ESI 0040A0B8 RTRACE.0040A0B8
EDI 00000000
EIP 00401191 RTRACE.00401191
C 1 ES 013F 32bit 0(FFFF)
P 0 CS 0137 32bit 0(FFFFFFFF)
A 0 SS 013F 32bit 0(FFFF)
Z 0 DS 013F 32bit 0(FFFF)
S 1 FS 139F 16bit 81D374CC(33)
T 0 GS 0000 NULL
D 0
O 0
EFL 00200283 (NO,B,NE,BE,S,PO,L,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty -14519.000000000000000
ST5 empty 0.0
ST6 empty -61036.333333333335760
ST7 empty 0.0
3 2 1 0 E S P U
FST 0000 Cond 0 0 0 0 Err 0 0 0 0
FCW 1372 Prec NEAR,64 Mask 1 1
Address | Hex dump | ASCII
0040A110 00 00 00 00 00 00 00 00 00 40 00 90 00 00 00 00 .....@.É....
0040A120 00 00 00 00 00 00 00 00 50 11 40 00 60 11 40 00 ....P◄@.`◄@.
0040A130 70 11 40 00 61 00 62 00 63 00 0A 00 00 00 40 00 p◄@.a.b.c.....@.
0064FE00 00540000
0064FE04 0064FE30
0064FE08 00407CEA RETURN to RTR
0064FE0C 00000001

4. 리버스 엔지니어링

if, while, function, etc

기계어

```
8B542408 83FA0077 06B80000 0000C383
FA027706 B8010000 00C353BB 01000000
C9010000 008D0419 83FA0376 078BD98B
B84AEBF1 5BC3
```

어셈블리어

```
fib:
    mov edx, [esp+8]
    cmp edx, 0
    ja @f
    mov eax, 0
    ret

    @@:
    cmp edx, 2
    ja @f
    mov eax, 1
    ret

    @@:
    push ebx
    mov ebx, 1
    mov ecx, 1

    @@:
        lea eax, [ebx+ecx]
        cmp edx, 3
        jbe @f
        mov ebx, ecx
        mov ecx, eax
        dec edx
    jmp @b

    @@:
    pop ebx
    ret
```

Python

```
def fibonacci(n):
    if 0 <= n <= 1:
        return n
    else:
        return fibonacci(n-1) + fibonacci(n-2)

def fibolist(n):
    list = []
    for i in range(n):
        list.append(fibonacci(i))
    return list
```

출처 : 위키디피아

1. 시스템 보안
2. 네트워크 보안
3. 어플리케이션 보안
4. 리버스 엔지니어링
5. **포렌식**
6. 버그헌팅
7. 암호학

5. 포렌식

조사/수사, 파일 복구, 재현 등

예) 황우석 박사의 줄기세포 사건 : 김선종 연구원의 노트북에서 포렌식을 통해 증거 획득, 유죄!

But!

예) 2010년 총리실 민간인 불법 사찰 하드디스크 삭제 : 디가우저 장비를 이용, 하드디스크 데이터를 영구 삭제한 안티포렌식 사례

출처 : 해킹 맛보기(강력 추천)

기술, 조사, 법률

증거

1. 정당성 원칙
2. 재현의 원칙
3. 절차 연속성의 원칙
4. 무결성의 원칙
5. 신속성의 원칙

출처 : 해킹 맛보기(강력 추천)

EnCase

간단한 파일 복구라면, 레쿠바 이용하세요.

1. 시스템 보안
2. 네트워크 보안
3. 어플리케이션 보안
4. 리버스 엔지니어링
5. 포렌식
6. **버그헌팅**
7. 암호학

6. 버그헌팅

취약점은 어디에나 존재
완벽한 코드는 없다. -> 풀리지 않는 자물쇠는 없다.

소스코드 감사, 바이너리 감사, 퍼징, 권한 상승 등

6. 버그헌팅

https://www.boho.or.kr/data/noticeView.do?bulletin_writing_sequence=1403

1. 시스템 보안
2. 네트워크 보안
3. 어플리케이션 보안
4. 리버스 엔지니어링
5. 포렌식
6. 버그헌팅
7. **암호학**

실제 전하고자 하는 메시지를 숨기는 것

왜?

전치법, 대체법, DES, AES, RSA, MD5, SHA

예를 들어,

I LOVE YOU

K NQXG AQW

다음세대를 책임질 암호 알고리즘은?

1. 정보보안 개요 - 해킹과 해킹 방어
2. 정보보안 진로
3. 국가 주도 추천 코스와 자격사항
4. 시스템 보안, 네트워크 보안, 애플리케이션 보안,
   리버스 엔지니어링, 포렌식, 버그헌팅, 암호학
5. **웹 해킹 개요 (XSS, SQL Injection,**
   파일 업로드, 디렉터리 노출, 쿠키 또는 프록시 변조,
   DBD, 에러노출과 구글해킹

OWASP TOP 10

1. XSS
2. SQL Injection
3. 파일 업로드
4. 디렉터리 노출
5. 쿠키 또는 프록시 변조
6. DBD
7. 에러노출과 구글해킹

서버를 공격하는 것이 아니라 사용자 공격!

주로 게시판 댓글에 허용되는 HTML이나 JS 코드

1. XSS
2. SQL Injection
3. 파일 업로드
4. 디렉터리 노출
5. 쿠키 또는 프록시 변조
6. DBD
7. 에러노출과 구글해킹

SQL 쿼리를 이용하여 시스템 접근 또는 로그인 우회

1. XSS
2. SQL Injection
3. **파일 업로드**
4. 디렉터리 노출
5. 쿠키 또는 프록시 변조
6. DBD
7. 에러노출과 구글해킹

PHP, JSP, ASP, 이미지, 영상 등을 업로드 하여 시스템 권한 획득 공격

1. XSS
2. SQL Injection
3. 파일 업로드
4. **디렉터리 노출**
5. 쿠키 또는 프록시 변조
6. DBD
7. 에러노출과 구글해킹

directory traversal attack

1. XSS
2. SQL Injection
3. 파일 업로드
4. 디렉터리 노출
5. **쿠키 또는 프록시 변조**
6. DBD
7. 에러노출과 구글해킹

쿠키, 프록시

5000만원 쇼핑하고 1만원 결제

1. XSS
2. SQL Injection
3. 파일 업로드
4. 디렉터리 노출
5. 쿠키 또는 프록시 변조
6. **DBD**
7. 에러노출과 구글해킹

Drive By Download Attack

1. XSS
2. SQL Injection
3. 파일 업로드
4. 디렉터리 노출
5. 쿠키 또는 프록시 변조
6. DBD
7. **에러노출과 구글해킹**

7. 에러노출과 구글해킹

- ✓ Intitle, allintitle
- ✓ Inurl, allinurl
- ✓ Filetype
- ✓ Allintext
- ✓ Site
- ✓ Link
- ✓ Inanchor
- ✓ Daterange
- ✓ Cache
- ✓ Info
- ✓ Related
- ✓ Phonebook
- ✓ Rphonebook
- ✓ Bphonebook
- ✓ Author
- ✓ Group
- ✓ Msgid
- ✓ Insubject
- ✓ Stocks
- ✓ define

1. 구글 검색의 기초
2. 고급 연산자
3. 구글 해킹 기본
4. 문서 파일 분석과 데이터베이스 디깅
5. 정보 수집을 위한 구글의 기능
6. 익스플로잇 그리고 공격 대상 찾기
7. 간단하면서 유용한 검색문 10가지
8. 웹 서버, 로그인 포털, 네트워크 하드웨어 검색
9. 사용자 이름, 비밀번호, 그 외 감추고 싶은 것
10. 구글 서비스로 해킹하기
11. 구글 해킹 쇼케이스
12. 구글 해커로브터 자신 보호하기