

해커의 길

보안 전문가의 길

2011.7.23
전 상훈 (바다란)

p4ssion@kaist.ac.kr
p4ssion@gmail.com

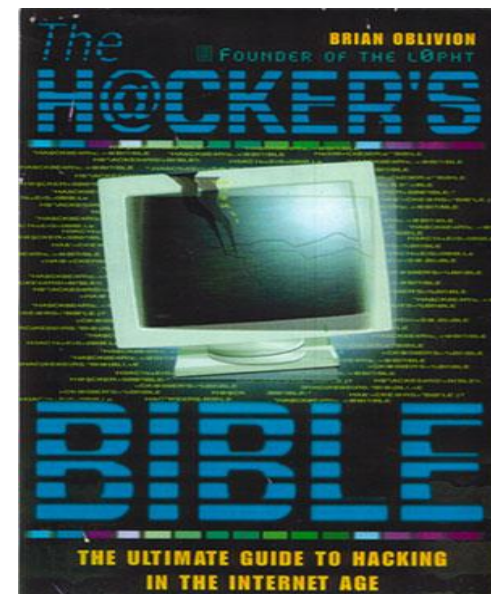
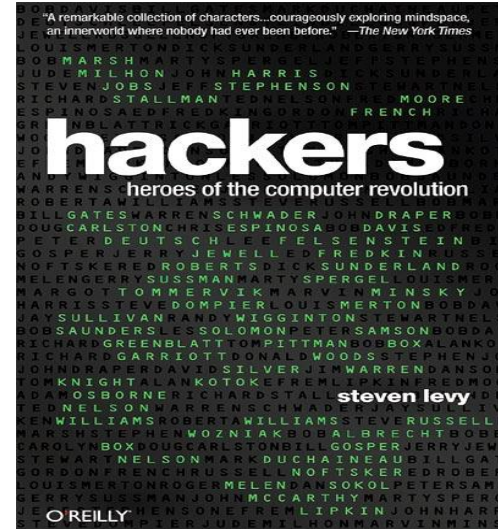
해커란?

- ▶ 해킹이란? 해커란 무엇인가?
 - 연상단어 - 불법, 몰입, 열정, 우월한 지식
- ▶ 룰즈섹, Anonymous ?
- ▶ 무엇을 위한?
 - 연상단어 - 명예, 금전적 보상, 성취감, 과시
- ▶ 해킹을 한다고 보안을 잘 할까?
 - 아직도 갈길은 멀고도 험하다.
- ▶ 해커의 길, 보안 전문가의 길
- ▶ 전문가는 그만큼의 책임을 질 수 있을때 전문가



Bible은 어디에?

- ▶ 무엇을 어떻게 해야 하는가?
- ▶ 프로그래밍만 할줄 알면?
- ▶ Exploit을 만들 수 있으면 될까?
- ▶ 유명 해킹 프로그램을 이용하면 해커 ?
- ▶ 영화속에 나오는 10초만에 성공하는 해킹은 ---
- ▶ 전지전능한 사람은 없다.
- ▶ 인내 하지 못하고 즐기지 못하는자 절대 도달 할 수 없다.



해커의 길 -1

기성자는 왕을 위해 싸움닭을 훈련시키는 사람이었다.
그는 훌륭한 닭 한 마리를 골라 훈련을 시켰다.
열흘이 지나자 왕은 닭이 싸움할 준비가 되었는가를 물었다.

[단계 1]

조련사는 대답했다.

“아직 안 됐습니다. 아직 불 같은 기운이 넘치고 어떤 닭과도 싸울 자세입니다. 공연히 뽐내기만 하고 자신의 기운을 너무 믿고 있습니다.”

[단계 1] Becoming a user

- 확실한 사용자가 되라. 사용해 보고 익히고 즐기기를 두려워 마라
- 기법은 항상 지나간다. 근본을 익히려고 노력하라. 인내 (프로그래밍)
- 네트워크, 시스템, 어플리케이션을 부지런히 익히라.
- 공격 기법은 중요하지 않다. 어설픈 흥내는 독이다.

해커의 길 -2

[단계 2]

다시 열흘이 지나 왕이 또 문자 그는 대답했다.

“아직 안 됐습니다. 아직도 다른 닭의 울음소리가 들리면 불끈 성을 냅니다.”

[단계 2] Becoming a Admin

- 시스템을 통제하라. (여러 종류의 운영체제)
- **자신의 전문분야를 설정하고 노력하라.**
- 남이 하지 못한 시도에 도전하고 영역을 만들어라
- 지식의 한계를 넘어서라 (영어권역)

해커의 길 3

[단계 3]

또다시 열흘이 지났으나 왕의 물음에 여전히 그는 대답했다.

“아직 멀었습니다. 아직도 상대를 보기만 하면 노려보고 깃털을 곤두세웁니다.”

[단계 3] Programming your style

- 당신의 전문분야에서 세계적인 최고가 되도록 하라. (좁은 범위에서 점진확대)
- 스스로가 필요에 의해 도구를 만들고 활용하라.
- 절대 자만하지 마라. 세상은 넓고 인재는 많다. 당신의 특징을 만들어 가라

해커의 길 -4

[단계 4]

또 열흘이 지나서 왕이 묻자 기성자는 마침내 대답했다.

“이제 거의 준비가 되었습니다. 다른 닭이 울어도 움직이는 빛이 안 보이고, 먼 데서 바라보면 마치 나무로 조각한 닭과도 같습니다.

이제 성숙한 싸움닭이 되었습니다. 어떤 닭도 감히 덤비지 못할 것이며, 아마 바라보기만 해도 도망칠 것입니다.”

[단계 4] Becoming a guru

- **각 분야를 아우르는 존재가 되라.** (시스템, 네트워크, 어플리케이션)
- 전략적인 통찰을 하라.
- **새로운 주제에 도전하고 항상 새로움의 영역을 만들어라.**
- 스스로의 성과를 널리 공유하고 활용 할 수 있도록 하라.
- 끊임 없는 노력만이 그대를 Guru에 이르게 한다.

- 1998 해커의 길 I 에서

진짜가 되려면?

▶ 프로그래밍

- C , C++ , Perl , CGI, Script [asp, jsp, php 등] , Assembly 지식 및 코딩 역량
- Exploit에 대한 작성, 취약성에 대한 이해, 대책을 위한 부분

▶ 시스템 지식

- Windows계열 , Linux, Unix, SunOS, MacOS에 대한 이해
- 시스템에 대한 지식과 프로그래밍, 네트워크가 결합된 종합적인 인식 능력

▶ 네트워크

- TCP/IP, 유무선 프로토콜에 대한 이해, 라우터, 스위치에 대한 이해와 설정
- 네트워크상에서 일어나는 위험과 리스크에 대한 분석 경험과 역량

▶ 보안 장비에 대한 이해

- ID/PS , Firewall, WebFW, ESM 등에 대한 이해 및 활용 능력
- 문제 해결 역량 (침해사고 대응에 대한 경험), 공격이 가능해야 방어도 가능하다.

▶ 영어능력

- 습득해야 될 지식의 절반 이상은 영어 권역에 존재한다. 익히지 못하면 반쪽이 된다.

***최소한 세가지 이상은 익혀야 중간은 간다.**

로드맵

▶ IT 보안 전문가

- 보안 전문가는 무엇이고 보안 관리자는 무엇인가?
- 시스템 보안
- Application 보안
 - Programming 능력
 - 구조에 대한 이해
 - 각 Application별 [상용 또는 자체개발] 보안 취약성의 동향과 이해, 정보 생산 능력
 - Reverse Engineering
- 네트워크 보안
- 모의해킹 역량
- 침해사고 대응 역량 (위의 지식을 알고 있어야 가능함)

각 개별 분야별 전문가가 될 수도 있다.
(모의해킹, 취약성 리서쳐, 포렌식, CERT, 관제등)

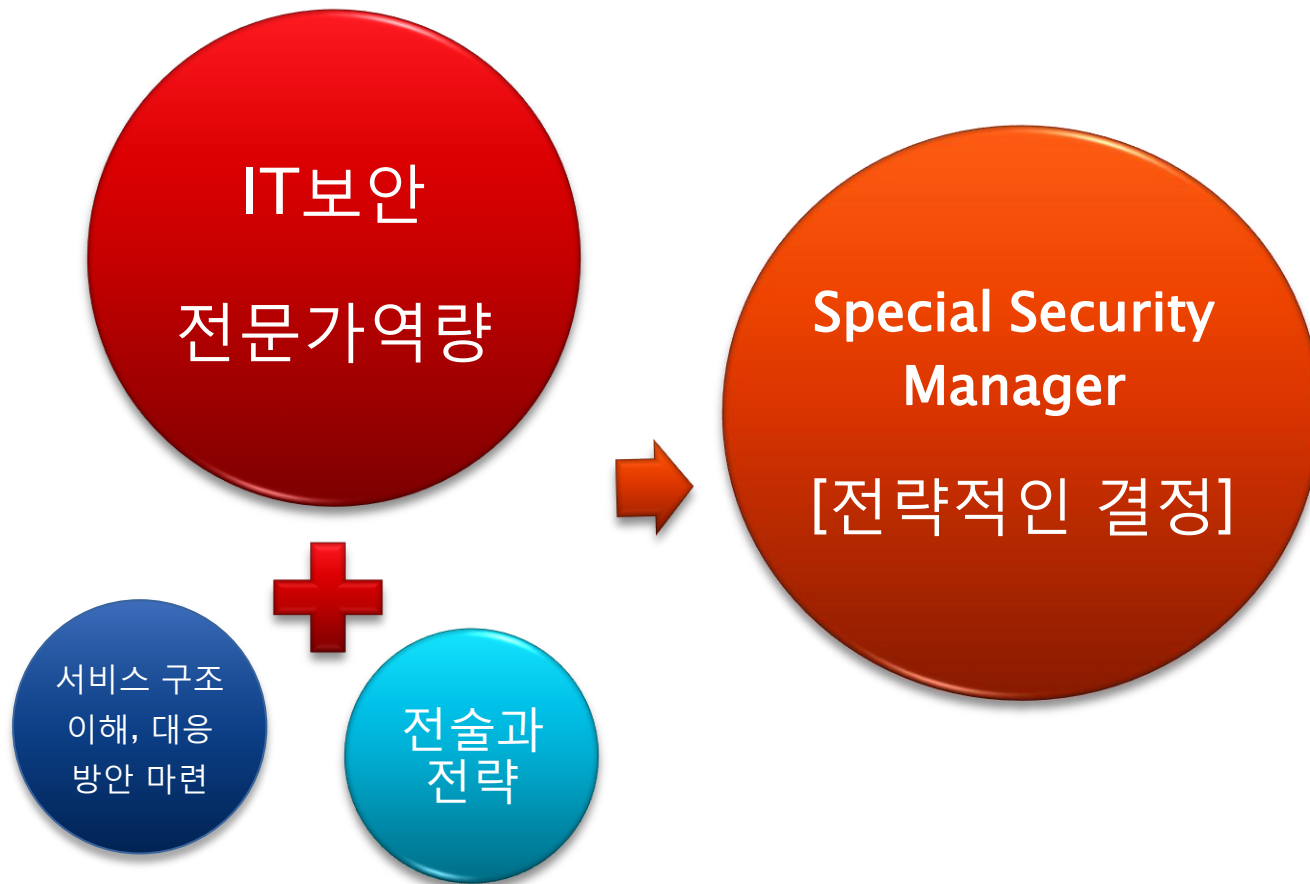
로드맵 -2

▶ 보안 관리자 (일반 보안- GSM)

- 보안 정책의 수립
- 관리 체계의 정립
 - ISO 및 ISMS 인증
 - 프로세스에 대한 이해와 보안성 강화
 - 문서 보안 및 사내보안 체계 수립
 - 법령 및 규정의 변화에 따른 대비
- 비즈니스 연속성 계획 (BCP)
- 물리적 보안 체계 구성 및 관리
- CISA, CISSP 등의 자격증이 도움이 됨 , 깊이 보다는 넓이에 치중

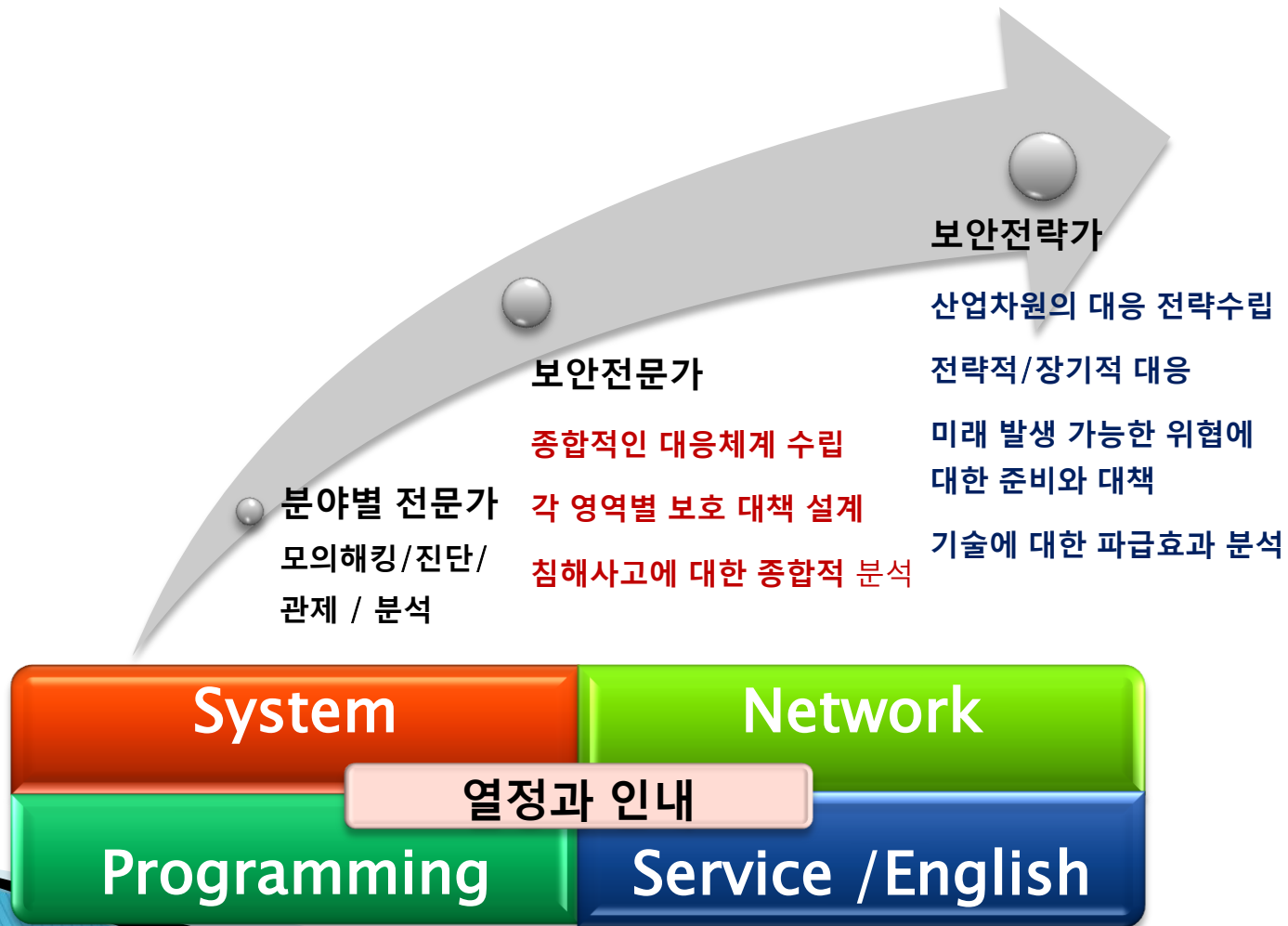
로드맵 -3

▶ 보안 관리자 (SSM- Special Security Manager)



Vision

- Stuxnet의 공격 코드 분석보다 더 중요한 것은 파급효과와 장기적 대응 전략이 아닐까?
- 지금 우리에게 정말 필요한 것은 전문가와 전략이 아닐까?



- ▶ 끊임 없는 노력과 날마다 새로워 지려는 노력
- ▶ 당신을 믿어라.
- ▶ 당신의 지식을 과시하는 순간 퇴보가 시작된다.
- ▶ 기술은 항상 변화하고 지나간다. 안주하지 마라
- ▶ 미치지 못하면 도달하지 못하는 법.

- ▶ 참고 (p4ssion.com Guide for guru: 해커의 길 I,II, 보안관리자..)

- 바다란 세상 가장 낮은 곳의 또 다른 이름 -