리팩토링 01

2020.03.07

권문정

목차

해킹과 정보보안의 개념

- “해킹”이란?
- “정보보안”이란?

“해킹”이란?

- Hacking is about finding inventive solutions
  using the properties and laws of a system
  in ways not intended by its designer
- 해킹이란 디자이너에 의하여 의도되지 않았던 방법으로
  어떤 시스템의 특성과 법을 이용한 창의적인 해결책을 찾는 것
- 즉, **시스템 제작자가 생각하지 못한 사용 방법을 찾는 것**

“정보보안”이란?

- 정보보안(情報保安, information security)

  : 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에

  정보의 **훼손, 변조, 유출 등을 방지**하기 위한 **관리적, 기술적** 방법

- 정보보호(情報保護, information protection)

  : 정보를 제공하는 공급자 측면과 사용자 측면에서

  논리적이고 물리적인 장치를 통해 **미연에 방지**

보안의 3대 요소

- 기밀성(Confidentiality)
- 무결성(Integrity)
- 가용성(Availability)

보안의 3대 요소_ 기밀성(Confidentiality)

- **인가(authorization)된 사용자**만 정보 자산에 **접근 가능**
- 일반적인 보안의 의미와도 가장 가깝다.

  ex) **자물쇠** - 허가되지 않은 사람, 즉 비인가자의 정보에 대한 접근을 막는 역할
- 보안과 관련된 많은 시스템과 소프트웨어가 기밀성과 밀접한 관련

  ex) 방화벽, 암호, 패스워드

보안의 3대 요소_ 무결성(Integrity)

- **적절한 권한**을 가진 사용자에 의해 **인가된 방법**으로만 정보 **변경 가능**
- ex) **지폐** – 오직 정부(적절한 권한을 가진 사용자)만이
  한국은행을 통해(인가된 방법으로만) 만들거나 바꿀 수 있고,
  그렇지 않은 경우(무결성이 훼손될 경우)에는 위조지폐로 취급된다
- ex) PC카톡을 켜고 자리를 비운 사이, 누군가가 대화명을 임의로 변경함
  -> 대화명은 공개되는 정보이므로 기밀성은 영향 X,
  무결성은 잃게 된다.

보안의 3대 요소_ 가용성(Availability)

- 정보 자산에 대해 **적절한 시간에 접근 가능함**
- 사전적 정의 : 가용(可用) – 사용할 수 있음.
- ex) **24시간 편의점** – 무엇인가 필요할 때 항상 얻을 수 있다

  -> 언제나 '가용' 하다
- 가용성은 정보화 사회에서 매우 중요함

  ex) 카드사에서 23:50~24:00 동안 결제 불가

  -> 해당 시간 동안 카드로 결제할 돈의 가용성이 훼손됨

보안 관련 직업

- 보안 시스템 개발자
- 보안 프로그램 개발자
- 보안 컨설턴트
- 보안 관리자

보안 관련 직업1_ 보안 시스템 개발자

- 방화벽과 IDS 등의 **시스템을 만듬**
- 하드웨어에 대한 지식을 가진 프로그래머
- 보안에 종사하나, 기본적으로 **프로그래머**
- 해킹 기법에 대한 지식 많이 필요하지 X

보안 관련 직업2_ 보안 프로그램 개발자

- 네트워크와 시스템, 해킹 기법에 대한 이해 필요
- 프로그래밍 실력 갖춰야 함
- 일반적으로 이미 알려진 **해킹 기법에 대한 대응책**을 강구하고, 이를 **프로그램에 반영**

보안 관련 직업3_ 보안 컨설턴트

- 크게 **관리적 / 기술적 보안**으로 나뉨
- 관리적 보안 : 사무실에서의 출력물 관리,
  통제 시스템에 대한 접근 권한 등에 대한 감사
- 기술적 보안 : 모의 해킹, 취약점 분석

보안 관련 직업4_ 보안 관리자

- 회사의 한 부서 내 보안팀에 소속
- 회사의 **특정 시스템에 대한 보안 관리**

  -> 여러 시스템에 대한 지식 X
- 시스템 관리자와 비슷한 업무

보안 전문가의 자격 요건

- 윤리 의식
- 다양한 분야의 전문성
  - 운영체제
  - 네트워크
  - 프로그래밍
  - 서버
  - 보안 시스템
  - 모니터링 시스템
  - 암호
  - 정책과 절차

보안 전문가의 자격 요건_ 윤리 의식

- **해킹은 절대 하면 안 된다!**
- 해킹 관련 기술을 배워 좋은 곳에 활용하는 전문가가 되자
  잠깐의 실수로 평생 범죄자라는 꼬리표를 달 수도 있다!
- **합법적인 모의해킹**의 경우에도 **처벌 가능**

  ex) 개인적인 용도로 모의해킹 이용

  애인의 개인정보 엿보기
- 윤리 강령 - https://bit.ly/2xbSlsE

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **운영체제(Operating System)**
  - 운영체제는 정보를 저장하고 처리하는 하나의 틀
  - 운영체제의 종류 : 윈도우, 유닉스, 리눅스, 맥 OS

1) 윈도우 - 실무적으로 가장 중요한 운영 체제

Why? 클라이언트로 많이 사용됨. 대부분의 악성코드가 윈도우를 목표.
게임회사나 포털의 경우 윈도우 서버의 비중이 매우 높음

2) 유닉스 - 금융권과 공공기관의 중요 시스템의 서버

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **운영체제(Operating System)**

  3) 리눅스 - 유닉스를 공부하기 좋다

  Why? 유닉스와 비슷한 환경 제공

  소스가 공개. 쉽게 구하고, 자유롭게 배울 수 있음.

  보안 장비나 스마트폰의 운영체제로 선택 (ex. 안드로이드)

  맥 OS의 경우에도 뿌리는 유닉스에 두고 있음

  - BUT 리눅스는 **버전에 따라 보안 설정 및 운영 방법이 상이**한 경우가 많음

    -> 유닉스의 표준화된 체계를 별도로 살펴보고 이해 필요

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **네트워크**
  - 하나의 시스템에서 데이터를 처리한 뒤,
    다른 시스템으로 전달하는 **"길"**과 같은 역할
  - **TCP/IP**
    1973년대에 만들어져 지금까지 네트워크의 기본이 되는 프로토콜
    매우 중요하기 때문에 동작 하나하나까지 이해 필요

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **프로그래밍**
  - 일반적인 수준의 보안 전문가에게 프로그래밍 능력이 그리 중요하지는 않다.
  - 기본적인 **C 프로그래밍과 객체지향 프로그래밍**에 대한 이해,
    HTML 정도면 충분
  - 웹 해킹의 경우에도 **JAVA와 JSP, ASP**를 이해하는 것이 도움,
    사실상 **자바스크립트와 HTML**을 정확히 이해하는 것이 훨씬 더 도움

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- 프로그래밍 능력이 중요한 경우
  - 수준 높은 보안 전문가
  - 보안 시스템 개발자 : 방화벽, 침입 탐지 시스템(IDS) 등의 개발
  - 응용 프로그램 취약점 분석 테스터 : 리버스 엔지니어링(Reverse Engineering)을 이용한 게임, 상용 프로그램 테스터/취약점 분석가
    -> 특히 어셈블리어에 대한 깊은 이해 필요
  - 자신만의 해킹 또는 보안 툴을 만들고 싶다면, C 언어를 충분히 알아야 한다.

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **서버**
  - 웹, 데이터베이스, WAS, FTP, SSH, Telnet 등의 서비스 프로그램
  - 기본적인 보안 전문가의 업무
    : 기업에서 안전하고 신뢰할 수 있는 서비스를 제공할 수 있는 서버의 운용
    -> 서버를 이해하는 것은 필수적!
  - 일반적으로 사용하는 모든 서버 프로그램의 설치와 기본적인 설정,
    각 서버별 인증 및 접근 제어 암호화 수준과 여부를 이해 필요.
  - 데이터베이스 : 기본적인 SQL 숙지

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **보안 시스템**
  - 보안 솔루션의 경우, 각 시스템별 기본 보안 통제와 적용 원리,
    네트워크상에서의 구성, 목적 등을 이해해야 한다.
  - ex) 방화벽, 침입 탐지 시스템, 침입 방지 시스템, 단일 사용자 승인(SSO),
    네트워크 접근 제어 시스템(NAC), 백신

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **모니터링 시스템**
  - 모니터링 시스템에 대해서도 기본적인 개념 숙지 필요
  - ex) 네트워크 관리 시스템(NMS), 네트워크 트래픽 모니터링 시스템(MRTG)

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **암호**
  - 암호와 해시의 차이, 대칭키 알고리즘과 비대칭키 알고리즘의 종류와 강도, 공개키 기반 구조에 대한 이해 필요

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **정책과 절차**
  - 보안 전문가의 전문성은 **기술적인 전문성만을 의미하는 것은 아니다.**
    큰 조직의 보안 전문가일수록 **보안 정책(Security Policy)**을 이해하고,
    해당 기업의 핵심적인 **업무 프로세스**를 잘 이해하고 있어야 한다.
    -> 최고보안책임자(CSO: Chief Security Officer)가 되기 위한 요건

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **정책과 절차**
  - 보안 거버넌스(Security Governance)
    : “조직의 보안을 달성하기 위한 구성원들 간의 지배 구조”
  - 보안 정책에서 가장 핵심적인 요소.
  - 최근 발생한 대규모 보안 사고의 원인 – 대부분 이러한 지배 구조의 부재

보안 전문가의 자격 요건_ 다양한 분야의 전문성

- **정책과 절차 – 보안 거버넌스의 중요성**
  - IT 부서의 엔지니어의 노력만으로는 보안 달성 불가
  - 대부분의 현실에서는 이사회 및 최고 경영층과 보안 관리자 사이의 괴리 존재, 보안에 대한 관심이나 기업 전략과의 연계 미약
  - 마치 보안 관리자의 책임만 있고 권한은 부재한 상황
  - 적절한 보안 거버넌스를 확보하지 못한 보안은 실패한다

IT 업체를 무너뜨린 악명높은 해킹 사례 20선

- MS 윈도우 2000 소스코드, 온라인 공개
- 룰즈섹, 해킹으로 HB게리 CEO 사퇴시키다
- 네트워크 침입 당한 RSA, 시큐ID 토큰 교체
- 보안업체 비트9, 자사 제품을 쓰지 않아 코드 서명 인증서 탈취당하다
- ……
- http://www.itworld.co.kr/print/86870

References

- [네이버 지식백과] 기밀성 (정보 보안 개론, 2013. 6. 28., 양대일)
- [네이버 지식백과] 정보보안 [Information Security] (학문명백과 : 공학, 김태달)