3 / 9 - 컴퓨터 보안 수업

중간고사 보고서 - 4월 20일 휴강, 중간고사 보고서 제출일 → 4월 26일

1. 다음의 그림을 보고 구성해야 하는 보안 시스템을 구성하라.
2. 네트워크가 지역마다 다 쪼개져 있을 때, 지역간의 네트워크에서 막 넘나들면 안되기 때문에 보안이 걸려있을 것이다. 그렇게 했을 때, 어떤 시스템이 적용 될 수 있는지 그림으로 그려라

수업시간에 배운 내용을 토대로 작성하되, 잘못 이해하고 적으면 감점.

기말고사 - 객관식, 주관식으로 평가가 된다. 객관식이 어려울 가능성이 높다.

- Ex)
    - 보안이란?
    - 기술
    - 법
    - 융합 기술
    - 시스템 보안
    - 네트워크 보안
- 정보 보안의 역사
    - 애니그마와 콜로서스 - 1950년 이전
        - 1918년 폴란드의 암호 보안 전문가들이 개발한 장치 | 평문 → 암호문
        - 은행의 통신 보안 강화를 위해 개발 → 2차 세계대전 독일군의 군사 통신 보안용으로 사용
        - 문자판의 키 하나를 누르면, 원판 3개가 회전해 복잡한 암호가 만들어짐
        - 애니그마를 해독한 것은 앨런 튜링이 만든 최초의 컴퓨터 콜로서스
        - 브루트하게 암호문이 애니그와의 암호와 일치할 때 까지 비교
    - 최초의 컴퓨터 연동망 ARPA - 1970년 이전
        - 1967년 미국 국방부는 기관의 정보 공유 지원하는 ARPA 프로젝트를 통해 컴퓨터 연결망 개발
        - IMPS 네트워크라고 불린 이 연동망은 오늘날 인터넷의 뿌리
    - 유닉스 운영체제의 개발
        - 1969년 켄 톰프슨과 데니스는 UNIX를 개발
        - 개발자 툴 및 컴파일러에 접근하기 쉽고, 동시에 여러 사용자가 사용가능한 특성이 있다. (해커 친화적)
    - 최초의 이메일 전송
        - 1971년 레이먼드 톰린슨은 최초의 이메일 프로그램을 개발
        - 64노드의 아르파넷에서 @을 사용한 최초의 이메일

- 마이크로소프트 설립
    - 1974년 MITS가 세계 최초 조립식 개인용 컴퓨터 앨테어 8800판매
    - 소프트웨어가 없고, 토글 스위치의 불빛을 보고 결과를 해독
    - 빌 게이츠는 앨테어 8800에서 동작하는 앨테어 베이직 작성
    - 마이크로스프트 설립
- 애플 컴퓨터 탄생
    - 1979년 탄생
    - 데스크톱 PC가 보급되어 일부 사용자들이 하드웨어를 사용해 원격 시스템 해킹
- 네트워크 해킹의 시작(방화벽의 등장) - 1990년 이전
    - FireWall - 들어오는 것은 블락킹, 중요한건 정책 - 중간고사 과제 - (업무의 특수성 왜 엄격하게 하지않냐, 엄격하게 하면 불편해 진다. 보안은 불편하게 만들수밖에 없다. 편의성이 낮아진다. 해커를 불편하게 하기 위해 방화벽 정책을 엄격하게 모두다 하면, 각 네트워크 사이에서 환경이 다르기 때문에 복잡해질 것이다. 따라서 각 네트워크에 맞는 정책에 따라 방화벽을 바꿔주어야 한다.)
    - 1980년 초 네트워크 해커라는 개념 탄생
    - 414Gang은 대표적인 네트워크 해킹 사건
    - BBS의 일원 들이 만든 해커 그룹으로 60개 컴퓨터 침입 및 삭제
    - 1981년 캡틴 잽이라는 별명을 가진 이언 머피가 AT&T의 컴퓨터 시스템에 침입 후 전화 요금을 조작
- 정보 권리 논쟁의 시작
    - 1981년 독일 해커 그룹 CCC 카오스 컴퓨터 그룹 결성
    - 정보에 대한 자유로운 접근 권리를 주장
- 해킹 문화의 등장
    - 해킹 문화로 인해 영화, 해커 잡지가 탄생했으며, 컴퓨터 범죄 처벌 규정이 생겨나게 되었다.
- 해커의 등장
    - 1980년 해킹이 발전하면서, 역사적으로 유명한 해커들이 본격적으로 등장
- 데포콘 해킹 대회
    - 최초의 해킹 대회
- 해킹 도구의 개발
    - 1994년 인터넷 브라우저인 넷스케이프가 개발되어 웹 정보에 대한 접근이 가능해짐.
    - 해커들은 노하우를 BBS에서 웹 사이트로 옮기고, 해킹 툴을 공개
    - 일부 사용자는 해킹 툴을 이용해 은행을 해킹
    - 이 때 부터 해커는 컴퓨터 광이 아닌 해킹하는 사람을 가르킴
- 아메리카 온라인 해킹

        - 1997년 AOL침입만을 목적으로 고안된 AOHell공개
        - 이후 수백만 명의 온라인 사용자가 공격을 받음
    - 트로이 목마, 백 오리피스 (백신 등장)

- 분산 서비스 거부 공격 (DDOS) - 2000년 이후
    - 네트워크 스캔 후 trojans라는 것으로 많은 패킷을 전송
    - ICMP 패킷을 이용한 스머프 공격으로 마비
- 웜과 바이러스
    - 2000년에는 러브 버그 바이러스가 등장
    - MS-SQL-2000 서버를 공격하는 슬래머 웜이 전국 네트워크를 마비
    - 2004년에는 베이글 웜, 마이둠 웜, 넷스카이 웜 등장
- 개인 정보 유출과 도용
    - 2005 ~ 2006사이 우리나라에서 주민 번호가 유출
    - 2005년 11월 금융 정보를 이용해 은행 계좌에서 잔고를 인출한 사건 발생
- 전자 상거래 교란
    - 2006년 7월에는 안심클릭의 허점을 이용한 해킹 사기 사건 발생
    - 정보 검색 순위를 조작한 광고업체 입건
- APT 공격의 등장
    - 2008년 해커 8명으로 구성된 캐시어가 RBS 은행의 침입 후 복제 카드 제작
    - 신용카드의 한도를 올리고, 12시간 동안 세계 49개 도시의 2100개 ATM 기기에서 인출
    - APT 공격 : 오랜 시간을 들여 사이트를 분석하고, 취약점을 찾아 해킹하는 것을 APT라 함
- 농협 사이버 테러
    - 2011년 4월 대규모 데이터 삭제로 전산 시스템이 멈춤
    - 북한의 사이버 테러로, 국내 기업의 보안 인식 자체를 바꿈
- 스마트폰 해킹
    - IOS와 구글의 안드로이드는 모두 유닉스와 유사
    - 리눅스에 기반을 둔 안드로이드는 리눅스 해킹툴을 비교적 쉽게 설치
    - 스마트폰은 긴 시간 전원 공급이 되고, 와이파이, 3G, LTE 이용가능 한 최고의 해킹 도구
- 가상 화폐 해킹
    - 현재 가상 화폐는 큰 돈이 되고 있기 때문에 관련 해킹 사건도 증가
- 보안의 3대 요소
    - 기밀성 - 접근
        - 인가된 사용자만 정보 자산에 접근할 수 있다는 것으로, 일반적인 보안의 의미와 가장 가까움
        - 허가되지 않은 사람 (비인가자)이 정보에 접근하는 것을 막는 자물쇠

        - 보안과 관련된 많은 시스템과 소프트웨어는 기밀성과 밀접한 관련이 있음
        - 방화벽, 암호, 패스워드 등은 기밀성의 대표적인 예
    - 무결성 - 권한
        - 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것
        - 무결성은 일상생활에서 중요하게 작용
    - 가용성 - 편의성 (보안을 엄격하게 걸면, 가용성이 낮아진다.)
        - 필요한 시점에 정보 자산에 대한 접근이 가능하도록 하는 것을 의미
        - 일상생활에서 가용성을 상품화한 대표적인 예는 24시 편의점
        - 현대 사회에서 정보의 가용성이 훼손되는 것은 필수 불가결한 요소의 가용성이 훼손되는 것과 마찬가지
- 보안 전문가의 자격 요건

    - 윤리 의식을 가지고(방어 체계를 만든 사람이 해커가 된다면?), 정보통신기반 보호법, 클라우드 컴퓨팅법, 전자공부법을 알아야한다.
    - 운영체제, 네트워크, 프로그래밍, 서버, 보안 솔루션, 모니터링 시스템, 정책과 절차에 대해 알아야한다.
- ISMS

    - 보안과 관련된 법을 잘 준수하고있는지 확인하는 제도
    - 인증심사원의 자격을 가지는 것도 보안의 한 분야

Next → 다양한 보안 분야와 진로