9과목 (소프트웨어 개발 보안 구축)

Chapter 01 소프트웨어 개발 보안 설계

1. SW 개발 보안
   ↘ 소프트에어 개발 과정에서 지켜야 할 일련의 보안 활동
2. SW 개발 보안 생명주기
   ↘ 요구사항 명세 > 설계 > 구현 > 테스트 > 유지보수
3. SW 개발 보안 3대 요소 (무기가)
   - 무결성 : 시스템 내의 정보는 오직 인가된 사용자만 수정할 수 있음
   - 기밀성 : 시스템 내의 정보와 자원은 인가된 사용자에게만 접근이 허용
   - 가용성 : 인가받은 사용자는 시스템 내의 정보와 자원을 언제라도 사용할 수 있음
4. ***DoS*** (Denial of Service) 공격
   ↘ ==시스템을 악의적으로 공격해서 해당 시스템의 자원을 부족하게 ==하여 원래 의도된 용도로 사용하지 못하게 하는 공격
   - DoS 공격 종류
     - ***SYN 플러딩*** : 서버의 동시 가용 사용자수를 SYN 패킷만 보내 점유하여 다른 사용자가 서버를 사용 불가능하게 하는 공격
     - ***UDP 플러딩*** : 대량의 UDP 패킷을 만들어 임의의 포트번호로 전송하여 응답 메시지를 생성하게 하여 지속해서 자원을 고갈 시키는 공격
     - ***스머핑(Smurfing)*** : 출발지 주소를 대상의 IP로 설정하여 네트워크 전체에게 ICMP Echo 패킷을 직접 브로드캐스팅하여 마비시키는 공격
     - ***Ping of Death*** : ICMP 패킷을 정상적인 크기보다 아주 크게 만들어 전송하여 정상적인 서비스를 못하도록 하는 공격
     - ***랜드 어택(Land Attack)***: 출발지 IP와 목적지 IP를 같은 패킷 주소로 만들어 보내 시스템의 가용성을 침해하는 공격
     - ***티어 드롭(Tear Drop)*** : IP패킷의 재조합 과정에서 잘못된 정보로 인해 수신 시스템이 문제를 발생하도록 만드는 공격
     - Boink : 프로토콜의 오류제어를 이용한 공격기법
5. DDoS (Distributed Denial of Service)
   ↘ 여러대의 공격자를 분산 배치하여 동시에 동작하게함으로써 특정 사이트를 공격하는 기법
   - DDoS 공격도구
     - Trinoo : 많은 소스로부터 통합된 UDP flood 서비스 공격을 유발하는데 사용되는 도구
     - Tribe Flood Network : 많은 소스에서 하나 혹은 여러개의 목표 시슽메에 대해 서비스 거부 공격을 수행할 수 있는 도구
     - Stacheldraht : 분산 서비스 거부 에이전트 역할을 하는 Linux 및 Solaris 시스템용 멀웨어 도구
   - DDoS 공격 구성요소 (HAMAD)
     - Handler : 마스터 시스템의 역할을 수행하는 프로그램

- Agent : 공격 대상에 직접 공격을 가하는 시스템
- Master : 공격자에게서 직접 명령을 받는 시스템
- Attacker : 공격을 주도하는 해커의 컴퓨터
- Daemon : 에이전트 시스틈의 역할을 수행하는 프로그램

6. DoS와 DDoS 차이
   ↘ DoS는 직접공격, DDoS 공격하도록 지시
7. DRDoS
   ↘ 공격자는 출발지 IP를 공격대상 IP로 위조하여 다수의 반사 서버로 요청정보를 전송, 공격 대상자는 반사 서버로부터 다량의 응답을 받아서 서비스 거부(DoS)가 되는 공격
8. 세션 하이재킹(Session Hijacking)
   ↘ TCP의 세션 관리 취약점을 이용한 공격 기법, 케빈 미트닉
9. 애플리케이션 공격기법
   - ***HTTP GET 플러딩*** : 과도한 Get메시지를 이용하여 웹서버의 과부하를 유발시키는 공격
   - ***Slowloris*** : HTTP GET 메서드를 사용하여 헤더의 최종 끝을 알리는 개행 문자열을 전송하지 않고, 대상 웹 서버와 연결 상태를 장시간 지속시키고 연결 자원을 모두 소진 시키는 서비스 거부 공격
   - ***RUDY*** : 요청 헤더의 Content-Length를 비상장으로 크게 설정하여 메시지 바디 부분을 매우 소량으로 보내 계속 연결 상태를 유지 시키는 공격
   - ***Slow HTTP Read DoS*** : 다수 HTTP 패킷을 지속적으로 전송하여 웹서버의 연결상태가 장시간 지속, 연결자원을 소진 시키는 서비스 거부 공격
   - ***Hulk DoS*** : 공격자가 웹페이지 주소를 지속적으로 변경하면서 다량으로 GET요청을 발생시키는 서비스 거부 공격
   - Hash DoS : 많은 수의 파라미터를 POST방식으로 웹서버로 전달하여 다수의 해시 충돌을 발생시켜서 자원을 소모시키는 서비스 거부 공격
10. 네트워크 공격
    - 스니핑 : 공격대상의 데이터만 몰래 들여다보는 수동적 공격 기법
    - 네트워크 스캐너 : 네트워크 하드웨어 및 소프트웨어 구성의 취약점 파악을 위해 공격자가 취약점을 탐색하는 공격 도구
    - 패스워드 크래킹
      - 사전 크래킹 : ID, PW가 될 가능성이 있는 단어를 파일로 만들어 파일의 단어를 대입하여 크랙하는 공격 기법
      - 무차별 크래킹 : 무작위로 패스워드 자리에 대입하여 패스워드를 알아내는 공격 기법
      - 패스워드 하이브리드 공격 : 사전 + 무차별
    - IP 스푸핑: 침입자가 인증된 컴퓨팅 시스템인 것 처럼 속여서 인증된 호스트의 IP주소로 위조하여 타깃에 전송하는 공격 기법
    - ARP 스푸핑 : 공격자가 특정 호스트의 MAC주소를 자신의 MAC주소로 위조한 ARP Reply를 만들어 희생자에게 지속적으로 전송
    - ICMP Redirect 공격 : 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격 기법
    - 트로이 목마 : 악성 루틴이 숨어 있는 프로그램, 실행하면 악성 코드를 실행

11. 버퍼 오버플로우 (Buffer Overflow) 공격
    ↘ 메모리에 할당된 버퍼 크기를 초과하는 양의 데이터를 입력하여 프로세스의 흐름을 변경시켜서 악성 코드를 실행 시키는 공격 기법
    - 버퍼 오버플로우 공격 대응 방안
        - 스택가드 활용 : 카나리라고 불리는 무결성 체크용 값을 복귀 주소와 변수사이에 삽입
        - 스택쉴드 활용 : 함수 시작시 복귀 주소를 Global RET라는 특수 스택에 저장
        - ASLR 활용 : 메모리 공격을 방어하기 위해 주소 공간 배치를 난수화
12. 백도어
    ↘ 정상적인 인증 절차를 우회하는 기법
    - 백도어 탐지기법
        - 프로세스 및 열린 포트 확인
        - Setuid 파일 검사
        - 백신 및 백도어 탐지 툴 활용
        - 무결성 검사
        - 로그 분석
13. 주요시스템 보안 공격 기법
    - 포맷 스트링 공격 : 포맷 스트링을 인자로 하는 함수의 취약점을 이용한 공격
    - 레이스 컨디션 공격 : 둘 이상의 프로세스나 스레드가 공유 자원을 동시에 접근할 때 접근 순서에 따라 비정상적인 결과가 발생하는 조건
    - 키로거 공격 : 컴퓨터 사용자의 키보드 움직임을 탐지해서 저장
    - 루트킷 : 침입 사실을 숨긴채 차후 침입을 위한 프로그램 모음
14. 보안 관련 용어
    - 스피어 피싱(Spear Phising): 발송 메일의 본문 링크나 첨부된 파일을 클릭하도록 유도 공격
    - 스미싱(Smishing) : 문자메시지를 이용하여 신뢰할 수 있는 사람 또는 기업이 보낸것 처럼 가장 피싱 공격
    - 큐싱(Qsing) : 스마트폰을 이용하여 금융업무를 처리하는 사용자에게 인증이 필요한 것처럼 속여 피싱 공격
    - APT 공격 : 특정 타깃을 목표로하여 다양한 수단을 통한 지속적이고 지능적인 맞춤형 공격 기법
    - 제로데이 공격 : 보안 취약점이 발견되어 널리 공표되기 전에 해당 취약점을 악용하여 이루어지는 보안 공격
    - 사이버 킬체인 : 룩히드 마틴, 공격형 방위시스템
    - 이블트윈 공격 : 무선 wifi 피싱 기법
    - 웜 : 스스로를 복제하여 네트워크 연결을 통하여 전파
    - 랜섬웨어 : 사용자의 컴퓨터에 침입 내부문서 파일 등 암호화해서 못열게 하고 돈을 요구
    - Tripwire : 크래커가 침입하여 백도어를 만들어 놓거나 설정 파일을 변경했을때 분석 하는 도구
15. 인증 기술의 유형 (지소생특)
    - 지식기반 인증 : 사용자가 기억하고 있는 지식 (ID, PW)
    - 소지기반 인증 : 소지하고 있는 사용자 물품 (OTP)
    - 생체기반 인증 : 고유한 사용자의 생체 정보 (지문)
    - 특정기반 인증 : 사용자의 특징을 활용 (서명, 몸짓)

16. 서버 접근 통제 유형
    - ***임의적 접근 통제 (DAC)*** : 신분에 근거하여 객체에 접근 제한
    - ***강제적 접근 통제 (MAC)*** : 주체가 찾는 접근 허가 권한에 근거하여 객체에 접근 제한
    - ***역할 기반 접근 통제 (RBAC)*** : 중앙 관리자가 조직 내 맡은 역할에 기초하여 접근 제한

정책	DAC	MAC	RBAC
권한부여	데이터 소유자	시스템	중앙관리자
접근 결정	신분	보안등급	역할
정책 변경	변경 용이	고정적	변경 용이
장점	구현 용이, 유연함	안정적, 중앙 집중적	관리 용이

17. 접근 통제 보호 모델 (벨기비무)
    - 벨-라파듈라 모델 : 미국방부 지원 보안 모델로 기밀성 강조
    - 비바 모델 : 벨-라파듈라 모델의 단점을 보완한 무결성 보장
18. 암호 알고리즘
    ↘ 데이터의 무결성 및 기밀성 확보를 위해 정보를 쉽게 해독할 수 없는 형태로 변환하는 기법
    - 양방향 방식
        - 대칭키 암호 방식 : 암호화와 복호화에 같은 암호키
            - 블록 암호 방식 : EDS, AES, SEED
            - 스트림 암호 방식 : RC4
        - 비대칭 키 암호 방식 : 개인키를 나눠 가지지 않은 사용자들이 안전하게 통신하는 방식 (RSA, 디피-헬만)
    - 일방향 해시함수 방식 : 임의 길이 정보를 입력받아, 고정된 길이의 암호문(해시값)을 출력하는 암호방식
        - MDC : 키를 사용하는 메시지 인증 코드
        - MAC : 키를 사용하지 않는 변경 감지 코드
19. 대칭키 암호화 알고리즘
    - DES : 1975, IBM, 대칭 키
    - SEED : 1999, 한국인터넷진흥원(KISA)
    - AES : 2001, 미국 표준 기술 연구소(NIST)
    - ARIA : 2004, 국가정보원, 산학연구협회
    - IDEA : DES 대체, 스위스 연방 기술기관
    - LFSR : 선형함수로 계산되는 구조
20. 비대칭키 암호화 알고리즘
    - 디피-헬만 : 최초의 공개키 알고리즘
    - RSA : 1977, MIT
    - ElGamal : 1984 ElGamal
    - ECC : 1985, RSA 대안'
21. 해시 암호화 알고리즘
    - MD5 : MD4 개선

    - SHA-1 : 1993 NSA 미국 정부 표준
    - SHA-256/384/512 : 256비트 해시값 생성하는 해시 함수
    - HAS-160 : 국내 표준 서명 알고리즘
    - HAVAL : 메시지를 1024 bit 블록으로 나눔

- IPSec : IP 보안 프로토콜
- SSL/TLS : 클라이언트와 서버간의 웹데이터 암호화, 상호 인증 및 전송 시 데이터 무결성을 보장하는 보안 프로토콜
- S-HTTP : 웹상 네트워크 트래픽 암호화

Chapter02 소프트웨어 개발 보안 구현

1. 시큐어 코딩
   ↘ 설계 및 구현 단계에서 해킹 등의 공격을 유발할 가능성이 있는 잠재적인 보안 취약점을 사전에 제거하고, 외부 공격으로부터 안전한 소프트웨어를 개발하는 기법
2. 입력 데이터 검증 및 표현 취약점
    - XSS : 검증되지 않은 외부 입력 데이터가 포함된 웹페이지를 사용자가 열람함으로써 포함된 부적절한 스크립트가 실행되는 공격
    - 사이트 간 요청 위조 (CSRF) : 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격
    - SQL 삽입(Injection) : 악의적인 SQL 구문을 삽입, 실행 시켜 데이터베이스의 접근, 정보 탈취 조작 행위 공격
3. 네트워크 보안 솔루션
    - 방화벽(firewall) : 기업 내부, 외부 간 트래픽을 모니터링하여 시스템의 접근을 허용하서나 차단하는 시스템
    - 웹 방화벽(WAF) : 웹 애플리케이션 보안에 특화된 보안 장비
    - 네트워크 접근 제어(NAC) : 단말기가 내부 네트워크에 접속을 시도할 때 이를 제어하고 통제하는 기능을 제공
    - 침입 탐지 시스템(IDS) : 네트워크에 발생하는 이벤트를 모니터링, 침입을 실시간으로 탐지
    - 침입 방지 시스템(IPS) : 네트워크에 대한 공격이나 침입을 실시간으로 차단, 능동적으로 처리하는 시스템
    - 무선 침입 방지 시스템(WIPS) : 인가되지 않은 무선 단말기의 접속을 자동으로 탐지 및 차단 보안에 취약한 무선 공유기 탐지
    - 통합 보안 시스템(UTM) : 방화벽, IDS, IPS, VPN 등 다양한 보안 기능을 하나의 장비로 통합하여 제공
    - 가상사설망 (VPN) : 인터넷과 같은 공중망에 사설망을 구축하여 마치 전용망을 사용하는 효과를 가지는 보안 솔루션
4. 시스템 보안 솔루션
    - 스팸 차단 솔루션 : 메일 서버 앞단에 위치하여 Proxy 메일 서버로 동작
    - 보안 운영체제 (Secure OS): 컴퓨터 운영체제의 커널에 보안기능을 추가한 솔루션
5. 취약점 분석 절차 (자진 제진결보)

- 자산 조사 및 분석
- 진단 대상 선정
- 제약사항 확인
- 진단 수행
- 결과분석/ 보고서 작성