흥달쌤과 함께하는

정보처리기사 실기

마무리 특강 학습교안

1억뷰 N잡

YouTube 흥달쌤 (https://bit.ly/3KtwdLG) E-Mail hungjik@naver.com

네이버 카페 흥달쌤의 IT 이야기 (https://cafe.naver.com/sosozl/)

01 정보보안

Section 1. SW개발 보안 설계

1. 정보보안

⑴ 정보보안 개념

- 기업의 정보 및 정보 시스템에 대해서 허가되지 않은 접근, 변경, 삭제 등으로부터 보호하는 것

⑵ 정보보안 요소

1) 기밀성(Confidentiality)
   - 인가된 사용자만 정보 자산에 접근할 수 있도록 한다.
2) 무결성(Integrity)
   - 적절한 권한을 가진 사용자가 인가된 방법으로만 정보를 변경할 수 있도록 접근 통제한다.
3) 가용성(Availability)
   - 원하는 시점에 언제든 정보 자산에 접근이 가능하도록 한다.
4) 인증(Authentication)
   - 접속한 사용자가 허가받은 사용자인지 확인하는 것
5) 부인방지(Non-Repudiation)
   - 정보를 보낸 사람이 나중에 정보를 보냈다는 것을 발뺌(부인)하지 못하도록 하는 것

⑶ AAA(Authentication, Authorization, Accounting)

1) 인증(Authentication)
   - 망, 시스템 접근을 허용하기 전에 사용자의 신원을 검증
2) 권한부여(Authorization)
   - 검증된 사용자에게 어떤 수준의 권한과 서비스를 허용
3) 계정관리(Accounting)
   - 사용자의 자원에 대한 사용 정보를 모아서 과금, 감사, 용량증설, 리포팅 등

⑷ 정보보안 거버넌스(Information Security Governance)

1) 정보보안 거버넌스 정의
   - 정보의 무결성, 서비스의 연속성, 정보자산의 보호를 위한 것
2) 정보보안 거버넌스의 3요소
   ① 데이터 무결성(Integrity of Data)
   ② 서비스 연속성(Service Continuous)
   ③ 정보자산의 보호(Protection of information Asset)

⑸ 인증제도

1) ISMS(정보보호 관리체계 인증)
   - 정보통신망의 안전성 확보를 위하여 수립하는 기술적, 물리적, 관리적 보호조치 등 종합적인 정보보호 관리체계에 대한 인증제도
2) PIMS(개인정보보호 관리체계)
   - 기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적 · 지속적으로 보호 업무를 수행하는지에 대해 객관적으로 심사하여 기준 만족 시 인증 부여

3) ISMS-P(정보보호 및 개인정보보호 관리체계 인증)
- 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

4) ITSEC(Information Technology Security Evaluation Criteria)
- 1980년대 후반 영국, 프랑스, 독일, 네델란드 주축으로 고유의 보안성 평가 기준서 개발

5) TCSEC(Trusted computer System Evaluation Criteria)
- 미국의 신뢰성 있는 컴퓨터 시스템 평가기준

6) CC(Common Criteria)
- 국가마다 상이한 평가 기준을 연동시키고, 평가결과를 상호 인증하기 위해 제정된 국제 평가기준

2. Secure SDLC(Software Development Life Cycle)

⑴ Secure SDLC의 개념
- 보안상 안전한 소프트웨어를 개발하기 위해 SDLC(Software Development Life Cycle)에 보안 강화를 위한 프로세스를 포함한 것

⑵ Secure SDLC 방법론

1) CLASP(Comprehensive, Lightweight Application Security Process)
- SDLC의 초기 단계에서 보안을 강화하기 위해 개발된 방법론

2) MS-SDL
- MS사에서 안전한 소프트웨어 개발을 위해 기존의 SDLC를 개선한 방법론

3) Seven Touchpoints
- 소프트웨어 보안의 모범사례를 SDLC에 통합한 방법론

3. 시큐어 코딩(Secure Coding)

⑴ OWASP(The Open Web Application Security Project)
- 오픈소스 웹 애플리케이션 보안 프로젝트
- OWASP Top 10
  - 웹 애플리케이션 취약점 중 빈도가 많이 발생하고, 보안상 영향을 줄 수 있는 10가지를 선정하여 발표

⑵ 시큐어 코딩 가이드

1) 입력 데이터 검증 및 표현
- 프로그램 입력값에 대한 검증 누락 또는 부적절한 검증, 데이터 형식을 잘못 지정하여 발생하는 보안 약점
- 보안 약점 종류
  - SQL Injection
  - XSS(크로스 사이트 스크립트)
  - 자원 삽입
  - 위험한 형식 파일 업로드
  - 명령 삽입
  - 메모리 버퍼 오버플로

2) 보안기능
- 보안 기능을 부적절하게 구현하는 경우 발생할 수 있는 보안 약점

- 보안 약점 종류
  - 적절한 인증 없이 중요기능 허용
  - 부적절한 인가
  - 취약한 암호화 알고리즘 사용
  - 하드코딩된 패스워드
  - 패스워드 평문 저장
  - 취약한 패스워드 허용

3) 시간 및 상태

- 동시 수행을 지원하는 병렬 시스템이나 하나 이상의 프로세스가 동작하는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안 약점
- 보안 약점 종류
  - 경쟁 조건
  - 종료되지 않는 반복문 또는 재귀 함수

4) 에러 처리

- 에러를 처리하지 않거나 불충분하게 처리하여 에러 정보에 중요 정보가 포함될 때 발생할 수 있는 보안 약점
- 보안 약점 종류
  - 오류 메시지 정보 노출
  - 오류 상황 대응 부재
  - 부적절한 예외 처리

5) 코드 오류

- 개발자가 범할 수 있는 코딩 오류로 인해 유발되는 보안 약점
- 보안 약점 종류
  - 널 포인터 역참조
  - 부적절한 자원 해제
  - 해제된 자원 사용
  - 초기화되지 않은 변수 사용

6) 캡슐화

- 중요한 데이터 또는 기능성을 불충분하게 캡슐화하거나 잘못 사용해 발생하는 보안 약점
- 보안 약점 종류
  - 잘못된 세션에 의한 정보 노출
  - 제거되지 않은 디버그 코드
  - 시스템 정보 노출
  - 잘못된 접근 지정자

7) API 오용

- 의도된 사용에 반하는 방법으로 API를 사용하거나 보안에 취약한 API를 사용하여 발생할 수 있는 보안 약점
- 보안 약점 종류
  - DNS에 의존한 보안 결정
  - 취약한 API 사용

4. 백업과 복구

(1) 재난 복구 전략 시 지표

성과 지표	설명
RP (Recovery Period)	- 실제 업무 기능 복구까지 걸린 시간
RTO (Recovery Time Objective)	- 업무 중단 시점부터 복구되어 가동될 때까지 시간 목표 - 시스템 장애 시 비즈니스가 감당할 수 있는 최대의 시간
RPO (Recovery Point Objective)	- 재해 발생 시 데이터 손실을 감당할 수 있는 데이터의 양
MTD (Maximum Tolerable Downtime)	- 비즈니스 연속성 관리에서 사용되는 지표 - 장애 시 업무가 정지 상태를 허용하는 최대 시간

(2) 백업과 복구를 위한 전략

전략	설명
풀-이미지 백업	- 데이터의 풀(full) 이미지를 백업하여 즉각적으로 이용할 수 있는 복구 시점을 생성한다. - 전체 백업을 수행해야하기 때문에, 가장 오랜 시간이 걸린다.
차등 백업	- 마지막 풀-이미지 백업 이후부터 발생한 모든 변경 사항을 백업한다. - 복구에는 마지막 풀-이미지 백업과 최신 차등 백업이 필요하다.
증분 백업	- 마지막 풀-이미지 복구 시점 이후부터 변경된 사항을 점차적으로 백업한다.
실시간 백업	- 지속적인 백업으로도 불리며 즉각적으로 모든 변경사항을 분리된 스토리지 디바이스에 복사한다.
합성 백업	- 기존의 전체 백업본과 증분 백업을 합하여 새로운 전체 백업을 만드는 작업

Section 2. SW개발 보안 구현

1. 암호 알고리즘

⑴ 대칭키 암호(Symmetric Key)

1) 대칭키 암호 개념

- 암호화할 때의 키와 복호화할 때의 키가 동일한 암호 시스템
- 대칭키 암호는 혼돈과 확산의 성질을 이용하여 평문을 암호화한다.

2) 블록암호 알고리즘

알고리즘	설명
DES	- 64bit 블록, 56bit 암호화 키 사용 - 평문을 32bit로 나눠 각 블록에 치환과 전치를 16Round 반복하여 암호화 - Feistel 암호 방식을 사용한다.
3-DES	- 암호화 키 2개를 사용하여 암호화→복호화→암호화 순으로 암호화
AES	- 128bit 평문을 128/192/256bit로 암호화 - 키 크기에 따라 10/12/14회 Round 수행 - SPN 암호 방식을 사용한다.
SEED	- 순수 국내기술로 개발한 128bit 및 256bit 대칭 키 블록의 암호 알고리즘
ARIA	- 국가 보안 기술 연구소(NSRI) 필두로 학계, 국가 정보원 등의 암호 기술 전문가들이 개발한 국가 암호화 알고리즘 - AES 알고리즘과 똑같이 128/192/256bit 암호화키를 지원한다.
IDEA	- 1990년 스위스에서 만들어진 PES를 개량하여 만들어진 블록 암호 알고리즘 - 키 길이가 128bit, 블록 길이가 64bit, 8Round - Feistel 방식과 SPN의 중간형태 구조
SKIPJACK	- 미국의 NSA에서 개발한 Clipper 칩에 내장되는 블록 알고리즘 - 64bit 입출력에 80bit의 키 총 32Round

3) 스트림암호 알고리즘

알고리즘	설명
LFSR	- LFSR은 현재 상태에서 선형 연산을 통해 다음 상태를 생성하는 레지스터 - 스트림 암호의 난수를 생성하는 용도로 많이 사용한다. - 블록암호에 비해 경량 및 고속 동작이 용이하다.
RC4	- 로널드 라이베스트가 만들었다. - 각 단계에서 키스트림 한 바이트를 생성한다.
A5	- 시프트 레지스터를 기반으로 사용 - GSM 휴대폰 체계에 사용

⑵ 비대칭키 암호

1) 비대칭키 암호 개념

- 암호화와 복호화에 이용하는 키가 다른 방식

- 공개 키 암호 방식이라고도 한다.

2) 키의 종류

① 공개키(Public Key)

- 대중에게 공개된 키

② 개인키(Private Key)

- 개인이 가지고 있으면서 관리하는 키

3) 비대칭키 알고리즘

구분		설명
소인수 분해 기반	RSA	- 대표적인 공개키 암호 알고리즘
	Robin	- 1979년 Robin이 개발, RSA보다 빠르다.
이산대수 기반	Diffie-Hellman	- 키관리 센터 없이 공개키 전달 가능
	DSA	- 미국의 전자서명 표준
	ELGamal	- 같은 평문에서 다른 암호문의 생성이 가능
	KCDSA	- KISA에서 개발한 인증서 기반 부가형 전자서명 알고리즘
타원 곡선	ECC	- 타원 곡선상의 이산대수를 이용

4) 전자서명

- 인증서 형태로 발급되는 자신만의 디지털 인감 도장이며 안전한 디지털 서명

⑶ 단방향 암호화

1) 단방향 암호화 개념

- Hash를 이용하여 암호화하는 과정
- 평문을 암호화할 수는 있지만, 복호화는 불가능하다.

2) 해시 함수 특성

특성	설명
역상 저항성	- 해시 값이 주어졌을 때, 그 해시 값을 생성하는 입력값을 알아내기가 불가능하다는 특성
제 2역상 저항성	- 어떤 입력 값과 동일한 해시 값(결과 값)을 가지는 다른 입력 값을 찾을 수 없어야 한다는 특성
충돌 저항성	- 해시 값(결과 값)이 같은 두 개를 찾을 수 없다는 특성

3) 해시 함수 종류

- MD5
- SHA
- HAS-160

4) 암호학적 해시 함수의 결점

① 무차별 대입 공격(Brute-Force Attack)

- 해시 함수는 빠르기 때문에 무차별적 데이터를 넣다보면 암호화가 깨질 수 있다.

② Rainbow Table 공격

- 사용자의 암호유형을 정의한 Rainbow Table을 만들어 하나씩 대입해 보면서 암호를 발견해 낼 수 있다.

5) 암호학적 해시 함수의 보완

① 키 스트레칭(Key Stretching)

- 해시 암호화를 여러 번 반복하여 암호학적 문제가 발생하는 점을 줄일 수 있다.
- 무차별 대입 공격을 방지하는 효과가 있다.

② 솔팅(Salting)

- 데이터 앞/뒤에 임의의 값을 넣어 해시값을 만든다.
- Rainbow Table 공격을 방지하는 효과가 있다.

⑷ 전자우편 보안

1) 암호화 프로토콜

종류	설명
PGP	- Phil Zimmermann에 의해 개발, 전자우편 보안의 표준 - 전자우편을 암호화하고, 받은 전자우편의 암호를 해석해 주는 보안 프로그램
PEM	- PGP와 같이 메시지의 내용을 암호화하고, 특정 키가 있어야만 내용을 볼 수 있다. - 기밀성, 메시지 무결성, 사용자인증, 부인방지 기능 제공
S/MIME	- 표준 보안 메일 규약으로 송/수신자를 인증하고 메시지의 무결성을 증명 - 첨부물에 대한 보안이 목적
DKIM	- 메일 발신자가 발송 정보를 위장할 수 없도록 하는 기술 표준

2. 코드 오류

⑴ 코드의 유형

- 순차 코드(Sequence Code)
- 블록 코드(Block Code)
- 10진 코드(Decimal Code)
- 그룹 분류 코드(Group Classification Code)
- 연상 코드(Mnemonic Code)
- 표의 숫자 코드(Significant Digit Code)
- 합성 코드(Combined Code)

⑵ 코드의 오류 발생 형태

- 생략 오류(Omission Error)
- 필사 오류(Transcription Error)
- 전위 오류(Transposition Error)
- 이중 오류(Double Transposition Error)
- 추가 오류(Addition Error)
- 임의 오류(Random Error)

Section 3. 인증과 접근통제

1. 인증과 인가

⑴ 인증(Authentication)

1) 인증의 개념

- 로그인을 요청한 사용자의 정보를 확인하고 접근 권한을 검증하는 보안 절차

2) 인증 유형

- 지식 기반 인증
- 소유 기반 인증
- 생체 기반 인증
- 행위 기반 인증
- 위치 기반 인증

⑵ 인가(Authorization)

- 로그인 후, 인증된 사용자에게 권한을 부여한다.

⑶ 인증방식

- 계정 정보를 요청 헤더에 넣는 방식
- Cookie/Session 방식
- 토큰 기반 인증 방식(JWT, JSON Web Token)
- SSO(Single Sign-On)
- 커버로스(Kerberos)
- 아이핀(i-PIN)

2. 접근 통제

⑴ 접근 통제 개념

- 정당한 사용자에게는 권한을 부여하고 그 외의 다른 사용자는 거부하는 것

⑵ 접근 통제 과정

1) 식별(Identification)

- 사용자 ID를 확인하는 과정

2) 인증(Authentication)

- 패스워드가 정확한지 확인

3) 인가(Authorization)

- 읽고, 쓰고, 실행시키는 권한을 부여

⑶ 접근 통제 원칙

- 최소 권한의 원칙
- 직무분리

⑷ 접근 통제 정책

1) 강제적 접근통제(MAC, Mandatory Access Control)

- 자원의 보안 레벨과 사용자의 보안 취급인자를 비교하여 접근 제어한다.
- 기밀성이 강조되는 조직에서 사용된다.

2) 임의적 접근통제(DAC, Discretionary Access Control)

- 주체가 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한한다.
- 자원의 소유권을 가진 사람이 다른 사람의 접근을 허용하거나 제한할 수 있다.

3) 역할기반 접근통제(RBAC, Role Based Access Control)

- 사용자의 역할에 기반을 두고 접근을 통제하는 모델이다.

⑸ 접근 통제 모델

1) 벨-라파둘라 모델(BLP, Bell-LaPadula Confidentiality Model)

- 미 국방부 지원 모델로 기밀성을 강조한 모델이다.
- No Read Up, No Write Down

2) 비바 모델(Biba Integrity Model)

- 무결성을 위한 상업용 모델이다.
- No Read Down, No Write Up

3) 클락-윌슨 모델(Clark-Wilson Integrity Model)

- 무결성 중심의 상업용 모델이다.

4) 만리장성 모델(Chinese Wall Model, Breswer-Nash Model)

- 충돌을 야기하는 어떠한 정보의 흐름도 차단해야 한다는 모델로 이익 충돌 회피를 위한 모델

Section 4. 시스템 보안 구현

1. 취약점 분석

⑴ 보안 취약점

- 정보시스템에 불법적인 사용자의 접근을 허용할 수 있는 위협

⑵ 보안 취약점 점검 분류

- 관리적 관점
- 기술적 관점
- 물리적 관점

2. 보안관제

⑴ 보안관제 개념

- 24시간 정보자산을 지키기 위해 모니터링하고, 외부의 공격자가 전달하는 패킷을 관측한다.
- 실제 침해사고 시 CERT(Computer Emergency Response Team)팀이 대응함

⑵ 통합로그 분석 장비

- ESM(Enterprise Security Management)
- SOAR
- SIEM(Security Information & Event Management)

3. 보안 운영체제(Secure-OS), 신뢰성 운영체제(Trusted OS)

⑴ 보안 운영체제 개념

- 컴퓨터 운영체제에 내재된 보안상의 결함으로 인하여 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 기능을 추가한 운영체제

⑵ 보안 운영체제 목적

- 안정성
- 신뢰성
- 보안성

4. 보안 솔루션

⑴ 방화벽(Firewall)

- 침입차단 시스템

⑵ 웹 방화벽(Web Firewall)

- 웹서버 특화 방화벽

⑶ 침입탐지시스템(IDS, Intrusion Detection System)

- 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템

1) 침입탐지 방식에 따른 분류

① 오용탐지

- 미리 입력해 둔 공격 패턴이 감지되면 이를 알려준다.

② 이상탐지

- 평균적인 시스템의 상태를 기준으로 비정상적인 행위나 자원의 사용이 감지되면 알려준다.

2) 침입탐지 대상에 따른 분류

① 네트워크 기반 IDS(NIDS)

- 네트워크 패킷을 분석하여 침입을 탐지한다.

② 호스트 기반 IDS(HIDS)

- 로그 분석과 프로세스 모니터링을 통한 침입을 탐지한다.

⑷ 침입방지시스템(IPS, Intrusion Prevention System)

- 방화벽과 침입 탐지 시스템을 결합한 것

⑸ 데이터유출방지(DLP, Data Leakage/Loss Prevention)

- 내부 정보의 외부 유출을 방지하기 위한 보안 솔루션

⑹ 가상 사설 통신망(VPN, Virtual Private Network)

- 인터넷 등 통신 사업자의 공중 네트워크에 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안 솔루션

⑺ NAC(Network Access Control)

- 네트워크에 접속하는 내부PC의 MAC주소(고유 랜카드 주소)를 IP관리 시스템에 등록한 후 일관된 보안관리 기능을 제공하는 보안 솔루션

⑻ ESM(Enterprise Security Management)

- 다양한 장비에서 발생하는 로그 및 보안 이벤트(방화벽, IDS, IPS, 웹방화벽, VPN 등)를 통합 관리하는 보안 솔루션

⑼ SIEM(Security Information & Event Management)

- ESM의 진화된 형태로 볼 수 있으며, 네트워크 하드웨어 및 응용 프로그램에 의해 생성된 보안 경고의 실시간 분석을 제공
- 기존의 ESM이 단기 이벤트성 위주 분석이었다면, SIEM은 빅데이터 수준의 데이터를 장시간 심층 분석한 인덱싱 기반

⑽ SOAR(Security Orchestration, Automation and Response)

- IT 시스템을 위협으로부터 보호하는 데 사용되는 일련의 기능
- 보안 오케스트레이션, 자동화 및 대응(Security Orchestration, Automation, and Response)

⑾ Sandbox

- 응용 프로그램이 실행될 때 가상 머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 의미한다.

⑿ FDS(Fraud Detection System)

- 전자금융거래에서 사용되는 단말기 정보, 접속 정보, 거래 내용 등을 종합적으로 분석하여 의심 거래를 탐지하고 이상 금융거래를 차단하는 시스템

⒀ Proxy Server

- 클라이언트 대신에 인터넷상의 다른 서버에 접속하는 서버

5. 방화벽(Firewall)

⑴ DMZ 구간(Demilitarized Zone)

- 내부 네트워크에 포함되어 있으나 외부에서 접근할 수 있는 구간

⑵ 구현방식에 따른 유형

유형	설명
패킷 필터링 (Packet Filtering)	- 네트워크 계층과 전송 계층에서 동작한다. - 다른 방화벽에 비해 속도가 빠르다.
애플리케이션 게이트웨이 (Application Gateway)	- 응용계층에서 동작한다. - 로그에서 다양한 정보를 얻어 여러 기능을 추가할 수 있다.
회선 게이트웨이 (Circuit Gateway)	- 응용계층과 세션 계층 사이에서 동작한다.
상태 기반 패킷 검사 (Stateful Packet Inspection)	- OSI의 모든 계층에서 패킷을 분석하여 차단하는 기능 - 방화벽 중 가장 강력하다.
혼합형 타입 (Hybrid Type)	- 서비스 종류에 따라 복합적으로 구성한다.

⑶ 방화벽 시스템 구축 유형

1) 스크리닝 라우터(Screening Router)
   - IP, TCP, UPD의 헤더 부분에 포함된 내용만 분석하여 동작
   - 내부 네트워크와 외부 네트워크 사이의 패킷을 허용/거부하는 라우터
   - 비용이 적게 들지만, 패킷 내의 데이터는 차단 및 관리가 어렵다.
2) 베스천 호스트(Bastion Host)
   - 내부 네트워크로 진입하기 전에 베스천 호스트를 두어 내부 네트워크를 전체적으로 보호
   - 스크린 라우터보다 안전하고, 로그 생성 관리가 용이
3) 듀얼 홈드 호스트(Dual-Homed Host)
   - 2개의 인터페이스를 가진 베스천 호스트로, 하나의 NIC는 내부 네트워크 연결, 다른 NIC는 외부 네트워크와 연결
4) 스크린드 호스트(Screened Host)
   - 패킷 필터 라우터와 베스천 호스트로 구성
   - 네트워크 계층과 응용계층의 2단계 방어로 안전
5) 스크린드 서브넷(Screened Subnet)
   - 스크린드 호스트의 보안성 문제점을 해결한 것
   - 두 개의 스크리닝 라우터와 한 개의 베스천 호스트로 구성되어 있다.

6. 보안 프로토콜

⑴ SSH(Secure Shell Protocol)
- 원격 호스트에 접속하기 위해 사용되는 보안 프로토콜
- 22번 포트를 사용한다.

⑵ SSL(Secure Socket Layer)
- 웹 브라우저와 웹 서버 간에 데이터를 안전하게 주고받기 위한 업계 표준 프로토콜
- SSL이 적용된 웹 페이지는 URL이 https로 시작되며, 443번 포트를 사용한다(http는 80포트).

⑶ TLS(Transport Layer Security)

- 전송계층을 기반으로 개발되었다.
- 데이터의 정보 보호와 무결성을 제공하기 위해 만들어졌다.

⑷ IPSec

- IP계층(네트워크 계층)을 안전하게 보호하기 위한 기법

1) 동작모드

- 전송 모드(Transport Mode) : 헤더를 제외한 페이로드(Payload)만을 보호
- 터널 모드(Tunnel Mode) : IP 패킷 전체를 보호

2) 프로토콜

- AH(Authentication Header) : 무결성, 인증 제공
- ESP(Encapsulating Security Payload) : 무결성, 인증, 기밀성 제공
- IKE(Internet Key Exchange) : 키 교환에 사용되는 프로토콜

⑸ S-HTTP (Secure HTTP)

- 웹상에서 네트워크 트래픽을 암호화하는 주요 방법 중 하나이다.
- 웹상의 파일들이 안전하게 교환될 수 있도록 해주는 HTTP의 확장판이다.

⑹ RedSec

- RADIUS 데이터를 전송 제어 프로토콜(TCP)이나 전송 계층 보안(TLS)을 이용하여 전송하기 위한 프로토콜

7. 고가용성(HA, High Availability)

- 서버와 네트워크, 프로그램 등의 정보 시스템이 오랜 기간 동안 지속적으로 정상 운영이 가능한 성질

Section 5. 서비스 공격 유형

1. DoS(Denial of Service) 공격

⑴ DoS 공격의 개념

- 대상 시스템이 정상적인 서비스를 할 수 없도록 가용성을 떨어뜨리는 공격

⑵ DoS 공격 유형

1) Smurf Attack
- IP와 ICMP의 특성을 이용한다.

2) Ping Of Death
- 규정 크기 이상의 ICMP 패킷으로 시스템을 마비시키는 공격 방법

3) Land Attack
- 출발지 IP와 목적지 IP가 같은 패킷을 만들어 보내는 공격 방법

4) Teardrop Attack
- 재조합을 할 수 있는 Fragment Number를 위조하는 공격 방법

5) SYN Flooding
- TCP의 연결과정(3Way Handshaking)의 취약점을 이용한 공격 방법

6) UDP Flooding
- 다량의 UDP 패킷을 전송하여 네트워크 자원을 고갈시키는 공격 방법

7) Ping Flooding
- 특정 사이트에 매우 많은 ICMP Echo를 보내서 시스템 자원을 모두 사용하게 하는 공격 방법

2. DDoS(Distributed Denial of Service attack) 공격

⑴ DDoS 공격 구성

구성	설명
공격자(Attacker)	- 해커의 시스템
명령 제어 (C&C, Command and Control)	- 공격자로부터 공격 명령을 전달받는 시스템
좀비(Zombie) PC	- C&C의 명령을 받고 실제 공격을 수행하는 다수의 PC
공격 대상(Target)	- 좀비 PC의 공격을 받는 대상 시스템
Exploit	- 공격자의 의도된 명령/프로그램 등

⑵ DDoS 공격 툴의 종류

- 트리누(Trinoo) : UDP Flooding 공격을 수행
- TFN(Tribal Flood Network) : UDP Flooding, TCP Flooding, ICMP 브로드캐스트 공격을 수행
- 슈타첼드라트(Stacheldraht) : Trinoo의 네크워크 구조와 TFN의 다양한 공격방법을 포함

3. 기타 해킹 기법

- 웜(Worm)
  - 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성 프로그램

- 바이러스(Virus)
  - 파일, 부트, 메모리 영역에서 스스로를 복사하는 악성 프로그램으로 파일 속에 숨어 옮겨 다닌다.
- 트로이목마(Trojan)
  - 해를 끼치지 않을 것처럼 보이지만 실제로는 바이러스 등의 위험인자를 포함하고 있는 프로그램
- 스턱스넷(Stuxnet)
  - 공항, 발전소, 철도 등 기간시설을 파괴할 목적으로 제작된 컴퓨터 바이러스
- 루팅(Rooting)
  - 핸드폰 운영체제의 루트(root) 관리자 계정을 획득하는 것
- 루트킷(Rootkit)
  - 시스템에 전반적으로 접근할 수 있는 루트 권한을 쉽게 얻게 해주는 킷(Kit)
- 혹스(Hoax)
  - 남을 속이거나 장난을 친다는 뜻으로, 말 그대로 가짜 바이러스
- 스니핑 공격(Sniffing Attack)
  - 네트워크로 전송되는 패킷을 훔쳐보는 공격
- IP Spoofing
  - 자신의 IP 주소를 속여서 접속하는 공격
- ARP Spoofing
  - 자신의 MAC(Media Access Control) 주소를 다른 컴퓨터의 MAC인 것처럼 속이는 공격
- DNS Spoofing
  - DNS 서버로 보내는 질문을 가로채서 변조된 결과를 보내주는 것으로 일종의 중간자 공격
- 파밍(Pharming)
  - 사용자의 컴퓨터를 악성코드에 감염시켜 정상 홈페이지에 접속하여도 피싱 사이트로 유도하는 피싱공격
- 타이포스쿼팅(Typosquatting)
  - 사용자가 사이트의 URL 주소를 입력할 때 철자를 잘못 입력하거나 빠뜨리는 실수를 이용하여, 해커가 만들어 놓은 유사한 URL로 접속하도록 유도하는 공격
- Smishing(SMS phishing)
  - 문자메시지를 이용한 피싱
- Qshing
  - QR코드를 통해 악성 링크로 접속을 유도하거나 직접 악성코드를 심는 금융범죄 기법
- 포트 스캐닝(Port Scanning)
  - 서버에 열려있는 포트를 확인 후 해당 포트의 취약점을 이용한 공격
- 세션 하이재킹(Session Hijacking)
  - 이미 인증을 받아 세션을 생성, 유지하고 있는 연결을 빼앗는 공격
- Buffer Overflow
  - 프로그램이 실행될 때 입력받는 값이 버퍼를 가득 채우다 못해 넘쳐흘러 버퍼 이후의 공간을 침범하는 현상
  - 방어기법 : 스택가드, 스택쉴드, ASLR (Address Space Layout Randomization)
- Format String Attack
  - 문자열의 출력 포맷을 애매하게 설정할 때의 취약점을 포착하여, 메모리의 RET 위치에 악성코드 주소를 입력하여 공격하는 기법

- SQL injection
  - 코드 인젝션의 한 기법으로 클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격할 수 있는 공격
- XSS(Cross-Site Scripting)
  - 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법
- CSRF(Cross-Site Requset Forgery)
  - 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 해킹 공격
- Backdoor
  - 정상적인 인증 절차를 거치지 않고, 응용프로그램 및 시스템에 접근할 수 있도록 만든 프로그램
- Password Cracking
  - 시스템의 비밀번호를 각종 툴(프로그램)을 통해 알아내는 공격 기법
- Rainbow Table
  - 해시함수(MD-5, SHA-1, SHA-2 등)를 사용하여 만들어낼 수 있는 값들을 대량으로 저장한 테이블
- APT(Advanced Persistent Threat)
  - 지속적이고 지능적인 해킹 공격의 통칭
- Nucking
  - 특정 아이피에 대량의 패킷을 보내 인터넷 접속을 끊는 크래킹의 일종
- 부채널 공격(Side Channel Attack)
  - 암호 알고리즘을 대상으로 한 물리적 공격 기법
- Brute Force
  - 무차별 대입 공격
- Dictionary Attack
  - 많이 사용되는 날짜, 전화번호 등과 같은 패턴들을 사전(Dictionary) 형태로 만들고 이들을 조합하는 방식으로 공격
- Key Logger Attack
  - 컴퓨터 사용자의 키보드 움직임을 탐지해 ID, 패스워드 등 개인의 중요한 정보를 몰래 빼가는 해킹 공격
- 스파이웨어(Spyware)
  - 사용자 동의 없이 사용자 정보를 수집하는 프로그램
- 애드웨어(Adware)
  - 프로그램 실행 중 광고를 보여주고, 이를 봄으로써 비용 납부를 대신하는 형태의 프로그램
- 트랙웨어(Trackware)
  - 시스템 작업을 추적하고 시스템 정보를 수집하거나 사용자 습관을 추척하여 이 정보를 다른 조직에 전달하는 소프트웨어 패키지
- 그레이웨어(Grayware)
  - 사용자의 동의를 얻어서 설치가 되기 때문에 일반 소프트웨어라고 할 수 있지만 설치되면 사용자에게 불편을 주는 소프트웨어
- 크라임웨어(Crimeware)
  - 불법 온라인 활동을 용이하게 하기 위해 고안된 소프트웨어
- 랜섬웨어(Ransomware)
  - 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다.
- 제로데이 공격(Zero-Day Attack)
  - 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격

- 사회공학(Social Engineering)
  - 사람들 간의 기본적인 신뢰를 기반으로 사람을 속여 비밀정보를 획득하는 기법
- Evil Twin Attack
  - 와이파이(WiFi) 무선 네트워크에서 공격자가 가짜 AP(Access Point)를 구축하고 강한 신호를 보내어 사용자가 가짜 AP에 접속하게 함으로써 사용자 정보를 중간에서 가로채는 기법
- Bluebug
  - 한 번 연결되면 이후에는 다시 연결해주지 않아도 자동으로 연결되는 인증 취약점 이용
- BlueSnarf
  - 블루투스 취약점을 이용하여 장비의 파일에 접근하는 공격
  - 인증 없이 정보를 교환하는 OPP 기능을 사용하여 파일에 접근
- BluePrinting
  - 블루투스 공격 장치의 검색 활동
- BlueJacking
  - 개인이 특정 반경 내에서 Bluetooth 지원 장치로 익명 메시지를 보낼 수 있는 해킹 방법
- Switch Jamming
  - 스위치 MAC 주소 테이블의 저장 기능을 혼란시켜 더미 허브(Dummy Hub)처럼 작동하게 하는 공격
- Honeypot
  - 침입자를 속여 실제 공격을 당하는 것처럼 보여줌으로써 크래커 추적 및 공격기법의 정보를 수집하는 역할
- 블루킵(Bluekeep)
  - 원격 데스크톱 서비스를 인증 없이 조작할 수 있는 취약점
- 인포데믹스(Infodemics)
  - 잘못된 정보나 소문이 지나치게 빨리 확산되면서 대중의 두려움이 필요 이상으로 증폭되는 현상
- 살라미(Salami)
  - 금융기관이나 인터넷상에서 많은 사람들로부터 적은 금액을 조금씩 빼내는 기법
- 다크 데이터(Dark Data)
  - 기업이 정보를 수집한 후, 저장만 하고 분석에 활용하고 있지 않은 다량의 데이터
- 킬 스위치(Kill Switch)
  - 분실한 정보기기를 원격으로 조작해 개인 데이터를 삭제하고 사용을 막는 일종의 자폭 기능
- 트러스트존(TrustZone)
  - 독립적인 보안 구역을 따로 두어 중요한 정보를 보호하는 하드웨어 기반의 보안 기술