**157. 소프트웨어 개발 방법론**

소프트웨어 개발, 유지보스 등에 필요한 일등의 수행 방법과 효율적으로 수행하려는 과정에서 필요한 각종 기법 및 도구를 체계적으로 정리하여 표준화한 것, 생산성과 품질 향상

2. 구조적 방법론 – 정형화된 분석절차, 사용자 요구사항을 파악하여 문서화, 처리 중심의 방법론

타당성 검토 단계 → 계획 → 요구사항 → 설계 → 구현 → 시험 → 운용/유지보수 단계

3. 정보공학 방법론 – 정보 시스템의 개발을 위해 계획, 분석, 설계, 구축에 정형화된 기법들을 상호 연관성 있게 통합 및 적용하는 자료 중심의 방법론

정보 전략 계획 수립 단계 → 업무 영역 분석 → 업무 시스템 설계 → 업무 시스템 구축

4. 객체지향 방법론

**158. 비용 산정 기법**

**159. 비용 산정 기법 – 하향식**

**160. 비용 산정 기법 – 상향식**

**161. 수학적 산정 기법**

**162. 소프트웨어 개발 방법론 결정**

**163. 소프트웨어 개발 표준**

**164. 소프트웨어 개발 방법론 테일러링**

**165. 소프트웨어 개발 프레임워크**

**166. 네트워크 관련 신기술**

**167. 네트워크 구축**

**168. 스위치**

**169. 경로 제어 / 트래픽 제어**

**170. SW 관련 신기술**

**171. 소프트웨어 개발 보안**

**172. 소프트웨어 개발 직무별 보안** **활동**

**173. 소프트웨어 개발 보안 활동 관련 법령 및 규정**

**174. HW 관련 신기술**

**175. Secure OS**

**176. DB 관련 신기술**

**177. 회복 / 병행 제어**

**178. 데이터 표준화**

**179. Secure SDLC**

**180. 세션 통제**

**181. 입력 데이터 검증 및 표현**

**182. 보안 기능**

**183. 시간 및 상태**

**184. 에러처리**

**185. 코드 오류**

**186. 캡슐화**

**187. API 오용**

**188. 암호 알고리즘**

**189. 서비스 공격 유형**

1. 서비스 거부(DoS; Denial of Service) 공격의 개념

서버의 자원 고갈을 목적으로 다수의 시스템에서 대량의 데이터를 한 서버에 집중, 기능 방해

2. Ping of Death(죽음의 핑)

Ping 명령을 전송할 때 패킷의 크기를 인터넷 프로토콜 허용 범위 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격 방법, ICMP Ping 응답 처리로 인해 시스템 다운

3. SMURFING(스머핑)

IP, ICMP의 특성을 악용해 엄청난 양의 데이터를 한 사이트에 집중, 네트워크를 불능 상태로 만듬

송신 주소를 공격 대상지의 IP 주소로 위장해 해당 네트워크 라우터의 브로드캐스트 주소를 수신지로 하여 패킷 전송 시 수신 패킷은 해당 네트워크 내의 모든 컴퓨터로 전송, 이후 해당 네트워크 내의 컴퓨터들은 수신 패킷에 대한 응답 메시지를 송신 주소로 집중 전송, 네트워크 과부화

무력화 하기 위해 각 네트워크 라우터에서 브로드 캐스트 주소를 사용할 수 없게 미리 설정

4. SYN Flooding

공격자가 가상의 클라이언트로 위장해 3-way-handshake 과정을 의도적으로 중단시켜 공격 대상지인 서버가 대기 상태에 놓여 정상적인 서비스를 수행하지 못하게 하는 공격 방법

과정 : 공격자는 1단계 수행→공격 대상 서버는 2단계 수행 → ACK 신호가 전송되지 않아 서버는 메모리 공간 확보 상태에서 대기 → 반복 시 동시 사용자 수가 꽉 차 정상 서비스 수행 불가능

대비 방법 : 수신지의 SYN 수신 대기 시간을 줄이거나 침입 차단 시스템을 활용

※ 3-way-handshake : 송신지와 수신지 간의 통신에 앞서 3단계의 확인 작업 수행 후 통신

송신지에서 수신지로 (1단계)‘SYN’ 패킷을 전송 → (2단계)수신지에서 송신지로 ‘SYN + ACK’ 패킷을 전송 → (3단계)송신지에서 수신지로 ‘ACK’ 패킷을 전송

5. TearDrop – 패킷이 여러 개로 분할되어 전송될 때 분할순서를 알 수 있도록 Fragment Offset 값을 함께 전송, Offset 값을 변경시켜 패킷 재조립 시 오류로 인한 과부화를 발생해 시스템 다운

대비 방법 : Fragment Offset이 잘못된 경우 해당 패킷을 폐기하도록 설정

6. Land – 패킷을 전송할 때 수신 IP 주소를 모두 공격 대상의 IP주소로 해 공격 대상에게 전송

대비 방법 : 송, 수신 IP 주소의 적절성을 검사해 자신에 대한 무한 응답을 방지

7. DDoS(Distributed Denial of Service, 분산 서비스 거부) 공격

여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 분산 서비스 공격을 수행하는 것

네트워크 취약점을 가진 호스트를 탐색, 분산 서비스 공격용 툴을 설치해 DDoS 공격에 이용

**190. 서버 인증**

1. 보안 서버 – 인터넷을 통해 개인정보를 암호화하여 송, 수신할 수 있는 기능을 갖춘 서버

2. 인증(Authentication)의 개념 – 사용자의 정보를 확인, 접근 권한을 검증하는 보안 절차

전송 메시지의 위/변조 여부를 확인, 네트워크를 통해 사용자의 등록 여부 확인

3. 지식 기반 인증(Something You Know) – 사용자가 기억하고 있는 정보를 기반으로 인증

관리 비용 저렴, 고정된패스워드, Passpharse(기억하기 쉬운 문장 활용), 아이핀(사이버 주민번호)

4. 소유 기반 인증(Something You Have) – 사용자가 소유하고 있는 것을 기반으로 인증 수행

신분증, 메모리 카드(토큰, 마그네틱), 스마트 카드(IC칩), OTP(One Time Password)

5. 생체 기반 인증 – 고유 생체 정보 기반, 사용 쉬움, 위조 어렵, 지문/홍채/망막/얼굴/음성 등

6. 기타 인증 기법 – 행위 기반 인증, 위치 기반 인증(위치의 적절성 확인)

**191. 보안 아키텍처 / 보안 프레임워크**

1. 보안 아키텍처(Security Architecture)

무결성, 가용성, 기밀성 확보를 위해 보안 요소, 보안 체계 식별, 이들 간의 관계를 정의한 구조

관리적, 물리적, 기술적 보안 개념의 수립, 보안 관리 능력의 향상, 일관된 보안 수준의 유지 기대

2. 보안 프레임워크 – 안전한 정보 시스템 환경을 유지하고 보안 수준을 향상시키기 위한 체계

ISO27001 : 정보보안 관리를 위한 국제 표준, 일종의 보안 인증이자 대표적인 보안 프레임워크

영국의 BSI가 제정한 BS799이 기반, 실제 심자/인증용으로 사용

**192. 로그 분석**

1. 로그의 개념 – 시스템 사용에 대한 모든 내역을 기록해 놓은 것

로그 정보를 정지적으로 분석 시 시스템에 대한 침입 흔적이나 취약점을 확인할 수 있다.

2. 리눅스 로그 – 모든 로그를 var/log 디렉터리에서 기록 및 관리

syslogd 데몬은 etc/syslog.conf 파일을 읽어 로그 관련 파일 위치 파악 후 로그 작업 시작

stslog.conf 파일을 수정하여 로그 관련 파일들의 저장 위치와 파일명을 변경할 수 있다.

3. 리눅스의 주요 로그 파일 – 커널/부팅/크론/시스템/보안/FTP/메일 로그

4. 윈도우 로그 – 이벤트 로그 형식으로 시스템 로그 관리, 이벤트 뷰어에서 확인 가능

5. Windows 이벤트 뷰어의 로그 – 응용 프로그램/보안/시스템/Set up/Forwarded Events 로그

**193. 보안 솔루션**

접근 통제, 침입 차단 및 탐지 등을 수행하여 외부로부터의 불법적인 침입을 막는 기술, 시스템

2. 방화벽(Firewall) – 기업, 조직 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용, 거부, 수정하는 기능을 가진 침입 차단 시스템, 내→외부 통과, 외→내부 패킷 엄밀히 체크

3. 침입 탐지 시스템(IDS; Intrusion Detection System)

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

오용 탐지(Misuse Detection) : 미리 입력해 둔 공격 패턴이 감지되면 이를 알려준다.

이상 탐지(Anomaly Detection) : 평균적인 시스템의 상태를 기준으로 비정상적인 행위나 자원의 사용이 감지되면 이를 알려준다.

4. 침입 방지 시스템(IPS; Intrusion DPrevention System)

5. 데이터 유출 방지(DLP; Data Leakage/Loss Prevention) – 내부 정보의 외부 유출 방지

6. 웹 방화벽(Web Firewall) – SQL 삽입 공격, XSS등의 웹 기반 공격 감지 및 차단

7. VPN(Virtual Private Network, 가상 사설 통신망) – 인터넷 등 통신 사업자의 공중 네트워크와 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안 솔루션

8. NAC(Network Access Control) – 내부 PC MAC IP 관리 시스템 등록, 일관된 보안 기능 제공

9. ESM(Enterprise Security Management) – 다양한 장비에서 발생하는 로그, 보안 Event 통합 관리

**194. 취약점 분석 ∙ 평가**

사이버 위협으로부터 정보 시스템의 취약점을 분석 및 평가한 후 개선하는 일련의 과정

2. 취약점 분석, 평가 범위 및 항목 – 상(필수 점검), 중, 하(선택적)로 중요도 분리

정보 시스템과 정보 시스템 자산에 직, 간접적으로 관여된 물리/관리/기술적 분야를 보함

3. 수행 절차 및 방법

취약점 분석, 평가 계획 수립 → 취약점 분석, 평가 대상 선별 → 취약점 분석 수행 →평가 수행