

【문 1】 다음 중 커버로스(Kerberos) 프로토콜에서 티켓-승인 티켓과 서비스 티켓을 구분하여 발급하는 이유로 가장 옳지 않은 것은?

- ① 사용자가 처음에 한 번 비밀번호로 로그인하면, 그 이후부터는 티켓-승인 티켓만을 가지고 추가 인증이 진행되도록 함으로써, 비밀번호 재사용을 막아 안전성을 높인다.
- ② 티켓-승인 티켓은 해당 사용자가 신원 확인을 마쳤다는 증거로, 서비스 티켓은 특정 서비스에 대해 접근 권한이 있다는 증거로 사용되어 안전성 및 유연성이 증가한다.
- ③ 사용자가 한 번 로그인하면, 티켓-승인 티켓으로 다양한 서비스에 추가 로그인 없이 접근할 수 있으므로 사용자 편의성이 증가한다.
- ④ 티켓-승인 티켓과 서비스 티켓은 각각 유효기간이 따로 설정되어 있어, 만약 서비스 티켓이 탈취되는 경우 보안 사고 대응력을 약화한다.

【문 2】 보안 시스템 설계 시 참고하는 접근 제어 원칙 중 다음 <보기>에 해당하는 원칙은?

< 보 기 >

어떤 주체가 객체에 대해서 명시적으로 접근 권한을 부여받지 않았다면, 그 주체는 객체에 대한 접근이 금지되어야 한다. 이 원칙은 또한 주체가 주어진 일을 완료하지 못하고 실패했을 때, 그 주체가 행한 변화를 초기 상태로 되돌림으로써 시스템을 안전한 상태로 유지해야 한다는 것을 의미한다.

- ① 직무 분리(Separation of Duties)
- ② 고장시 안전 초기화(Fail-Safe Default)
- ③ 최소 권한(Least Privilege)
- ④ 알 필요성(Need to Know)

【문 3】 네트워크 보안 공격의 하나인 스니핑에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 스니핑은 대표적인 수동적 공격의 하나로, 송신자와 수신자가 주고받는 데이터를 중간에 도청하여 실행한다.
- ② 스니핑을 막기 위한 방법으로는 주고받는 데이터를 암호화하는 방법이 있으며, 웹에서는 HTTPS, 이메일에서는 PGP와 S/MIME, 원격 접속에서는 SSH와 VPN을 활용할 수 있다.
- ③ 스니핑을 막기 위해서는 허브 대신 스위치를 사용하고 스위치의 매핑 테이블을 정적으로 설정하는 방법이 있다.
- ④ 스니핑을 탐지하는 방법으로 호스트 기반 탐지 도구인 ARP watch나 네트워크 기반 탐지 도구인 ifconfig를 활용하는 방법이 있다.

【문 4】 다음 중 버퍼 오버플로 공격에 대한 대응 방법 중 스택 가드에 대한 설명에 해당하는 것은?

- ① 스택에서 execution 권한을 제거함으로써 스택에 로드된 공격자의 공격 코드를 실행할 수 없도록 하는 기법이다.
- ② 스택에 있는 ret 주소를 실행 가능한 임의의 주소로 돌려원하는 함수를 수행하게 하는 기법이다.
- ③ 메모리 공격을 방어하기 위하여 주소 공간 배치를 난수화하는 기법으로, 스택, 힙, 라이브러리 등 데이터 영역의 주소등을 난수화한다.
- ④ 컴파일러가 프로그램의 함수를 호출할 때, ret 앞에 canary 값을 주입하고, 함수를 종료할 때 canary 값을 변조했는지 확인하는 기법이다.

【문 5】 CC(Common Criteria) 인증에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① CC 인증은 정보보호 시스템의 보안 기능 요구사항과 보증 요구사항 평가를 위해 공통으로 제공되는 국제 평가 기준이다.
- ② CC 인증은 사용자의 보안 요구를 표현하기 위한 공통 평가 기준 PP(Protection Profile), 특정 제품의 보안 기능을 표현한 평가 기준 자료 ST(Security Target), 인증 및 평가의 직접적인 대상 TOE(Target Of Evaluation)으로 구성된다.
- ③ 각 시스템은 EAL(Evaluation Assurance Level)로 보안 수준을 평가 받는데, 이는 5단계로 구성되어 있다.
- ④ CC 인증 상호인정협정 회원국은 인증서 발행국과 인증서 수용국으로 나눌 수 있는데, 대한민국은 다른 국가에서 발행된 인증서를 자국에서 인정해 주는 동시에 자국 내 국제 상호인정협정에 의해 공인된 평가 및 인증기관을 보유하고 있는 인증서 발행국에 속해 있다.

【문 6】 메시지 인증 코드(Message Authentication Code)에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 메시지 인증 코드는 전자서명과 함께 데이터의 무결성을 보장하기 위한 기법의 하나이다.
- ② 메시지 인증 코드를 설계하는 대표적인 방법으로는 해시 함수를 이용하는 HMAC과 블록암호 운용방식의 하나인 CBC 모드를 이용하는 CBC-MAC이 있다.
- ③ 메시지 인증 코드를 사용하기 위해서는 별도의 다른 안전한 방법으로 키를 공유해야 한다.
- ④ 메시지 인증 코드는 비밀키를 소유한 사람이 메시지에 대한 MAC 값을 계산하여 공개한다면, 누구나 검증이 가능하다.

【문 7】 RSA 암호의 모듈러스를 두 소수 7과 11을 곱하여 $N=7 \times 11=77$ 로 생성하였다고 할 때, 공개키 e로 선택할 수 있는 값은?

- ① 6 ② 15 ③ 23 ④ 30

【문 8】 KDC(Key Distribution Center)는 교환 키의 위험을 줄이기 위해 계획된 암호체계의 부분이다. 세션 키를 포함한 Ticket을 만드는 순서로 올바르게 나열한 것은?

- (A) 사용자는 파일서버에 대한 접근을 요청한다.
- (B) 티켓 부여 서비스는 세션 키에 포함된 새로운 티켓을 만든다.
- (C) 인증 서비스는 사용자에게 시작 티켓(Initial Ticket)을 전송한다.
- (D) 사용자는 하나의 세션 키를 추출하고 티켓을 파일 서버로 전송한다.
- (E) 사용자는 인증 서비스에 인증한다.

- ① (A) - (B) - (C) - (D) - (E)
- ② (C) - (A) - (B) - (D) - (E)
- ③ (B) - (C) - (E) - (A) - (D)
- ④ (E) - (C) - (A) - (B) - (D)

【문 9】 다음 중 utmp 로그와 관련 있는 명령어가 아닌 것은?

- ① w
- ② history
- ③ whodo
- ④ users

【문10】 CVE(Common Vulnerabilities and Exposures)에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① CVE는 미국의 비영리기관인 MITRE에서 만든 소프트웨어에서 공통으로 발생하는 잠재적인 보안 약점을 분류한 체계이다.
- ② 취약점 번호의 체계는 CVE-(발견년도)-(취약점 번호)의 형태로 이루어져 있다.
- ③ CVE에 정리된 대표적인 취약점으로는 인터넷 익스플로러의 0-Day 취약점, Apache Struts2의 RCE(Remote Code Execution) 취약점 등이 있다.
- ④ CVE로 체계화된 취약점들은 일반적으로 설계상의 문제이므로, 운영하는 쪽에서 자체 개선하기는 힘들며, 제조사의 공식 패치에 따라 개선할 수 있다.

【문11】 정보보호관리체계(ISMS)에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① ISMS의 위험 관리 절차는 일반적으로 식별 → 분석 → 평가 → 대응의 순서로 진행된다.
- ② 위험 분석 단계에서는 자산, 위협, 취약점 등을 기반으로 사건이 발생할 가능성과 사건이 미치는 영향을 평가한다.
- ③ ISMS-P는 정보보호와 개인정보보호를 통합적으로 평가하는 국제 인증 제도이다.
- ④ ISO/IEC 27001은 조직의 정보보호관리체계 수립, 실행, 유지, 개선을 위한 국제 표준으로서 일반적인 정보보호를 다룬다.

【문12】 리눅스의 권한 설정에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 파일의 접근 권한을 파일을 만든 소유자 권한, 소유자가 속한 소유 그룹 권한, 그 외 사용자 권한으로 나눠서 관리한다.
- ② 기본적으로 명령어를 실행시킨 사용자 ID를 체크하여 실행 권한이 있으면 명령어를 수행한다.
- ③ 명령어를 실행시킨 사용자 ID에게 실행 권한이 없으면 SetUID, SetGID, Sticky bit가 설정되어 있는지를 확인한다.
- ④ Sticky bit가 설정된 디렉터리 내에서는 타인이 생성한 파일도 일반 사용자가 삭제할 수 있다.

【문13】 블록암호 AES(Advanced Encryption Standard)에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① AES는 128비트의 평문을 128비트의 암호문으로 암호화한다.
- ② AES의 키의 크기는 128, 192, 256비트 3가지로 설정이 가능하다.
- ③ AES는 키의 크기에 따라 12, 14, 16라운드를 갖는다.
- ④ 암호화 과정에서 AES의 각 라운드는 SubBytes, ShiftRows, MixColumns, AddRoundKey의 순서로 수행되지만, 마지막 라운드에서는 MixColumns를 수행하지 않는다.

【문14】 DES에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 64비트 평문을 64비트의 암호문으로 변환시키고, 16라운드 구조로 이루어져 있다.
- ② 라운드함수에서 특히 S-Box는 confusion을 구현하는 기능을 갖고 있다.
- ③ 키는 보통 패리티비트들을 포함하여 48비트로 표현하지만 실제 키길이는 56비트이다.
- ④ Double DES는 중간가로채기공격으로 인해 쓰이지 않는 메커니즘이다.

【문15】 스푸핑 공격에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① ARP 스푸핑 공격은 MAC 주소를 속이는 것이다.
- ② IP 스푸핑 공격을 막기 위해 중요 접속 서버의 URL에 대한 IP를 hosts 파일에 등록하면 된다.
- ③ ICMP 리다이렉트 공격은 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격이다.
- ④ DNS 스푸핑 공격은 실제 DNS 서버보다 빠르게 공격 대상에게 DNS Response 패킷을 보내어 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다.

【문16】 무선 랜 프로토콜에 관한 다음 설명 중 가장 옳은 것은?

- ① 802.11b는 와이파이(Wi-Fi)라고 하며, WEP 방식의 보안을 구현한다.
- ② 802.11a는 802.11b의 속도를 개선한 프로토콜로, 802.11b와 호환되지만 네트워크 공유 시 데이터 처리의 효율이 현격히 떨어진다.
- ③ 802.11i는 여러 안테나를 사용하는 다중입력/다중출력(MIMO) 기술로 대역폭을 최소화하고 최대 속도는 600Mbps이다.
- ④ 802.11ac는 최대속도 7Gbps이고, 기존 2.5GHz/5GHz 대신 60GHz 대역을 사용하여 전송하는 방식이며, 대용량 데이터나 높은 비트레이트 동영상 스트리밍에 적합하다.

【문17】 다음 중 주로 시스템 자원(예: 메모리, CPU, 디스크 등)이나 네트워크 대역폭을 빠르게 소모시켜 과부하를 일으키는 것을 목표로 하지 않고, 서버의 동시 연결 수를 소진시켜 정상 사용자가 접속하지 못하게 만드는 것을 목표로 하는 공격은?

- ① HTTP Get Flooding 공격
- ② Slowloris 공격
- ③ Ping of Death 공격
- ④ Smurf 공격

【문18】 포맷 스트링 공격에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 포맷 지정자를 악용하여 메모리 내용을 유출하거나 조작하는 공격 방법이다.
- ② C언어 계열에서 printf()와 같은 출력 함수에 사용자 입력을 포맷 문자열로 직접 전달할 때 발생할 수 있다.
- ③ 컴파일 시점에 발생하며, 실행 시에는 영향을 미치지 않는다.
- ④ 공격을 방지하기 위해서는 사용자 입력을 포맷 문자열로 받지 않고, 명시적인 서식 지정자를 사용하도록 한다.

【문19】 다음 LLM(Large Language Model, 대형언어모델)에 대한 공격 중 기존 LLM의 콘텐츠 제한 정책을 우회하는 프롬프트를 생성하여 LLM이 의도하지 않은 작업을 실행하도록 유도하는 공격은?

- ① 프롬프트 인젝션(Prompt Injection)
- ② 부적절한 출력 처리(Improper Output Handling)
- ③ 시스템 프롬프트 노출(System Prompt Leakage)
- ④ 허위 정보(Misinformation)

【문20】 호스트 기반 침입탐지 시스템(HIDS, Host-based Intrusion Detection System)에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 특정 호스트의 로그, 파일 무결성, 시스템 콜 등을 분석하여 침입 여부를 탐지한다.
- ② 개별 시스템에 설치하므로, 네트워크 전체의 트래픽 흐름을 중앙에서 분석하는 데 효과적이다.
- ③ 루트킷 탐지, 파일 변경 감시, 비정상 프로세스 탐지 등에 효과적이다.
- ④ 운영체제에 가까운 수준에서 동작하며, 내부자의 이상 행위 탐지에 유리하다.

【문21】 서비스거부공격(DoS)에 관한 다음 설명 중 가장 옳지 않은 것은?

- ① 분산서비스공격(DDoS)도 DoS공격의 일종이다.
- ② Boink, Bonk 공격은 프로토콜의 오류 제어 로직을 악용하여 시스템자원을 고갈시키는 방식이다.
- ③ TearDrop 공격은 패킷 전송 시 출발지 IP 주소와 목적지 IP 주소를 동일하게 만들어 공격 대상에게 보내는 공격이다.
- ④ 라우터에서 다이렉트 브로드캐스트를 막는 형태로 Smurf 공격에 대응할 수 있다.

【문22】 위험관리에 관한 다음 설명 중 가장 옳은 것은?

- ① 위험에는 인위적 위험과 자연적 위험이 존재하며, 인위적 위험에는 고의적 위험과 우발적 위험이 있다.
- ② 위험분석에서 연간손실예상액(ALE)는 어떤 위험이 한 번 발생했을 때 예상되는 손실을 의미하며, 1회손실예상액(SLE)과 연간발생빈도(ARO)의 합으로 구할 수 있다.
- ③ 영향이란 보안사고가 자산에 미치는 원인을 말한다.
- ④ 취약성 분석은 환경과 기존의 보안대책을 고려하여 현존하는 위험의 공격대상이 될 수 있는 자산의 강점을 검사하는 것이다.

【문23】 SYN Flood에 관한 다음 설명 중 가장 옳은 것은?

- ① 네트워크를 통해 데이터를 주고받기 위해 세워진 프로토콜의 허점을 이용한 DoS 공격방식 중 하나이다.
- ② TCP/IP의 취약성을 이용한 서비스 거부 공격 방식 중 하나로 SYN 공격은 대상시스템에 간헐적인 SYN 패킷을 보내는 공격이다.
- ③ 공격을 막는 근본적인 방법은 존재하지 않으나, 백 로그 큐를 줄이고 대기 상태를 늘리는 방법으로 해결할 수 있다.
- ④ 해당 공격이 외부의 정당한 접속을 방해하는 것은 아니다.

【문24】 다음 대칭키 알고리즘 운영 모드 중에서 평문을 블록 단위로 나누고, 각 블록이 독립적으로 암호화되기 때문에 패턴 노출 등 보안성이 약한 운영 모드에 해당하는 것은?

- ① ECB ② CTR ③ CFB ④ OFB

【문25】 다음 중 IPSec의 구성 요소가 아닌 것은?

- ① 키 교환 및 관리(Key Exchange & Management)
- ② 보안 연계(Security Association)
- ③ 에이전트 보안(Agent Security)
- ④ 보안 프로토콜(Security Protocol)