

정보보호론(7급)

(과목코드 : 141)

2026년 군무원 채용시험

응시번호 :

성명 :

- | | |
|--|---|
| <p>1. 대역폭 공격보다 적은 트래픽으로 서버의 과부하를 유발할 수 있는 자원 소진 공격에 해당하는 분산 서비스 거부 공격(DDoS)의 유형으로 가장 적절한 것은?</p> <p>① UDP 플러딩
② ICMP 플러딩
③ GET 플러딩
④ TCP SYN 플러딩</p> <p>2. 제로 트러스트 아키텍처(Zero Trust Architecture) 보안 모델의 논리적인 구성요소와 그 역할에 대한 설명으로 가장 적절한 것은?</p> <p>① 정책 엔진(PE)은 접근 주체가 자원에 접근할 수 있도록 세션의 인증 및 인가 토큰을 생성한다.
② 정책정보지점(PIP)은 접근 결정을 위한 정책 규칙으로 활용할 수 있는 정보를 생성하여 전달한다.
③ 정책시행지점(PEP)은 다양한 입력 요소를 검토하여 접근 주체의 자원 접근 허용을 최종적으로 결정한다.
④ 정책 관리자(PA)는 접근 주체와 자원의 연결을 활성화하고 모니터링하며 최종적으로 연결을 종료한다.</p> <p>3. S/W 공급망 위험관리를 위한 SBOM(S/W Bill Of Materials) 데이터 필드의 기본항목 중에서 구성요소를 생성하고 정의 및 식별한 주체의 이름을 나타내는 것은?</p> <p>① 공급자명(Supplier Name)
② 저작권자(Author Name)
③ 구성요소명(Component Name)
④ 고유식별자(Unique Identifier)</p> | <p>4. 통계작성, 과학적 연구, 공익적 기록보존 등 목적으로 가명정보 제도를 통해 처리되는 가명정보라고 해도 일반적인 개인정보와 동일하게 적용되는 「개인정보보호법」 상의 조항에 해당하는 것은?</p> <p>① 제26조(업무위탁에 따른 개인정보의 처리 제한)
② 제27조(영업양도 등에 따른 개인정보의 이전 제한)
③ 제36조(개인정보의 정정·삭제)
④ 제37조(개인정보의 처리정지 등)</p> <p>5. 조직의 내부 중요정보의 유출에 대한 대책으로 사용되는 정보보호시스템에 대한 기능의 설명이 가장 적절한 것은?</p> <p>① DRM은 PC 메신저나 웹 메일 등의 정보유출 수단으로 쓰이는 프로그램을 도메인 기준으로 차단한다.
② VDI는 PC에 저장되는 파일을 암호화하고 승인 절차를 거쳐 복호화하여 중요문서의 유출을 방지한다.
③ DLP는 메일, 메신저, 웹 등을 통해 발생할 수 있는 중요정보의 유출을 탐지하고 차단한다.
④ VPN은 가상머신을 실행하여 서버에 로그인한 후 문서를 작업하여 결과가 PC에 남지 않도록 한다.</p> <p>6. 소프트웨어 개발의 보안 약점인 크로스사이트 요청 위조(CSRF)에 대한 설명으로 가장 적절하지 않은 것은?</p> <p>① 사용자의 의도와 무관하게 공격자가 의도한 수정, 삭제, 등록 등을 요청할 수 있다.
② 사용자가 인증한 세션이 계속 유지되어 비정상적인 요청을 구분하지 못하는 점을 악용한다.
③ 입력 화면의 양식은 POST 방식보다 GET 방식을 사용하여 처리하는 대책을 마련한다.
④ 입력을 처리하는 토큰을 사용하여 공격자의 직접적인 URL 사용이 동작하지 않도록 대응한다.</p> |
|--|---|

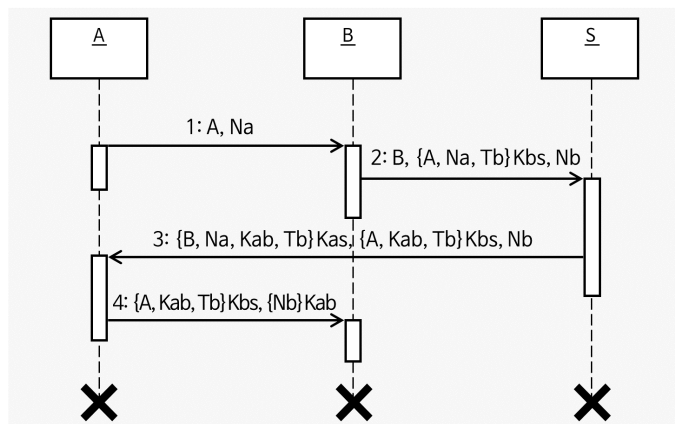
7. 시스템에 등록된 모든 계정의 비밀번호를 암호화된 형태로 저장 및 관리하는 파일을 (# chown root 수행 후) 관리자만 접근할 수 있게 하여 비인가자들의 임의적인 파일 변조를 방지하기 위한 LINUX 명령어로 가장 적절한 것은?

- ① # chmod 400 /etc/shadow
- ② # chmod 400 /etc/hosts
- ③ # chmod 644 /etc/shadow
- ④ # chmod 644 /etc/hosts

8. 국내에서 개발된 대칭키 암호화 알고리즘에 해당하는 것으로 묶인 것은?

- ① AES, HIGHT
- ② ARIA, HIGHT
- ③ AES, KCDSA
- ④ ARIA, KCDSA

9. 다음은 키 분배 서버 S를 이용하여 A와 B가 키 공유를 수행하는 프로토콜에 대한 그림이다. 이 프로토콜에 대한 설명으로 가장 적절한 것은? (K는 비밀키, N은 난수값, T는 타임스탬프)



- ① A와 B는 S가 알 수 없는 비밀키 Kas와 Kbs를 사전에 공유하고 있어야 한다.
- ② B는 A와 공유할 세션키 Kab를 생성하여 S를 통해 A에게 전달하게 된다.
- ③ A와 B의 시스템 시간을 동기화하지 않아도 세션키 Kab의 최신성을 확인할 수 있다.
- ④ 세션키 Kas를 보유하는 순간 추가적인 절차 없이 A와 B의 쌍방향 인증이 이루어진다.

10. 국내 “개인정보 및 개인정보보호 관리체계 (ISMS-P)” 인증제도의 인증기준 중에서 보호 대책 요구사항 영역의 ‘사고 예방 및 대응’에 해당하는 항목은?

- ① 성능 및 장애관리
- ② 운영환경 이관
- ③ 취약점 점검 및 조치
- ④ 재난 복구 시험 및 개선

11. 보안 관제 플랫폼 기술인 SIEM에 비해서 SOAR가 추가적으로 지원하는 기능으로 가장 적절한 것은?

- ① 로그 수집
- ② 자동화 대응
- ③ 중앙 집중화
- ④ 분석과 보고

12. 5G 코어망의 네트워크 기능(Network Function)과 그 설명의 연결로 가장 적절한 것은?

- ① AMF(Access and Mobility Management Function) - 단말 사용자가 정식 가입자인지 인증하고 검증하는 기능
- ② AUSF(Authentication Server Function) - 단말 기기의 접속, 등록, 위치추적, 이동성 제어 신호를 관리하는 기능
- ③ UDM(Unified Data Management) - 인증키, 가입자 은닉 ID 등의 가입자 정보를 안전하게 보관하고 제공하는 기능
- ④ PCF(Policy Control Function) - 실제 사용자 데이터를 목적지까지 전달하여 처리하고 트래픽 경로를 제어하는 기능

13. 정보보호 관리체계(ISMS) 국제표준인 ISO/IEC 27001 시리즈에서 클라우드 서비스의 정보보호 통제와 개인정보보호 지침을 다루는 문서로 묶어진 것은?
- ① ISO/IEC 27003, ISO/IEC 27004
 - ② ISO/IEC 27005, ISO/IEC 27007
 - ③ ISO/IEC 27011, ISO/IEC 27013
 - ④ ISO/IEC 27017, ISO/IEC 27018
14. 국내 사이버 위기 경보단계 중에서 경계(Orange)에 해당하는 판단 기준으로 가장 적절한 것은?
- ① 국가 차원의 주요 정보통신망 및 정보시스템 장애 또는 마비
 - ② 다수의 기관에서 사고 발생했거나 대규모 피해로 확대될 가능성 증가
 - ③ 국내외 정치적 또는 군사적 위기발생 등 사이버안보 위해 가능성 고조
 - ④ 위험도가 높은 컴퓨터 바이러스 취약점의 출현으로 피해 발생 가능성 증가
15. 일반적으로 유사한 수준의 보안강도를 보장하기 위해 가장 작은 크기(비트수)의 공개키가 필요한 암호 알고리즘은?
- ① RSA
 - ② ECDSA
 - ③ ElGamal
 - ④ Diffie-Hellman
16. 악의적인 의도에 맞게 학습 결과를 유도하기 위해 인공지능 모델의 학습에 사용했던 데이터 자체를 추출하는 공격으로 가장 적절한 것은?
- ① 전도 공격(Inversion Attack)
 - ② 회피 공격(Evasion Attack)
 - ③ 오염 공격(Poisoning Attack)
 - ④ 프롬프트 공격(Prompt Attack)
17. 드론에 대한 GPS 재밍(Jamming) 공격의 대책으로 가장 적절한 것은?
- ① 무선통신 방해 신호를 탐지하고 우회 통신 채널을 확보한다.
 - ② 중요한 정보가 노출되지 않도록 데이터를 암호화하여 전송한다.
 - ③ 위치정보를 기반으로 비행 금지구역에 대한 접근을 방지한다.
 - ④ 온보드 펌웨어와 소프트웨어가 변조되지 않도록 보호한다.
18. 침입탐지시스템(IDS)에 대한 설명으로 가장 적절하지 않은 것은?
- ① Signature 기반 탐지 방법은 상대적으로 False Positive 비율이 낮다.
 - ② 호스트 기반 IDS와 네트워크 기반 IDS가 있다.
 - ③ 이상(Anomaly) 탐지 방법은 상대적으로 False Positive 비율이 높다.
 - ④ False Negative 비율은 공격으로 탐지되었는데 공격이 아닌 비율을 말한다.
19. 현재 TLS 1.3에서 안전하게 제공되는 암호기 조합(Cipher Suite)에 포함되는 알고리즘은?
- ① RC4
 - ② 3DES
 - ③ SHA-1
 - ④ AES
20. ARP 프로토콜에 대한 설명으로 가장 적절하지 않은 것은?
- ① ARP 프로토콜은 IP 주소를 MAC 주소로 맵핑하는 서비스이다.
 - ② 공격자가 거짓 ARP 응답을 보내서 ARP 테이블을 갱신하게 만들어 공격할 수 있다.
 - ③ 공격자가 ARP 테이블을 변경시켜 통신을 가로챌 수 있다.
 - ④ ARP Spoofing 공격을 통하여 서비스거부(DoS) 공격은 불가능하다.

21. 비밀번호 Salt를 사용하는 가장 중요한 이유로 가장 적절한 것은?
- ① 비밀번호를 축약해서 저장하기 위해서
 - ② 해시 속도를 높이기 위하여
 - ③ Rainbow Table 공격에 대응하기 위하여
 - ④ 암호화하지 않기 위해서
22. 컴퓨터 보안의 목표인 CIA Triad의 3요소에 해당하지 않는 것은?
- ① Authentication (인증)
 - ② Availability (가용)
 - ③ Confidentiality (기밀)
 - ④ Integrity (무결)
23. 전자 서명(Digital Signature)에 대한 설명으로 가장 적절하지 않은 것은?
- ① 일반적으로 계산량을 감소시키기 위하여 해시 함수를 사용하여 해시 값을 생성하여 서명한다.
 - ② 전자 서명하려고 하는 사용자의 Public Key로 암호화한다.
 - ③ 전자 서명을 통하여 문서의 무결성을 보장할 수 있다.
 - ④ RSA 알고리즘을 사용할 수 있다.
24. 일반적인 개인정보 영향평가의 수행 단계에서 개인정보 흐름 분석의 세부 절차에 따른 산출물의 작성 순서로 가장 적절한 것은?
- ① 개인정보 처리업무표 및 업무흐름도 → 개인정보 흐름도 → 개인정보 흐름표 → 정보시스템 구조도 및 정보보호 현황표
 - ② 정보시스템 구조도 및 정보보호 현황표 → 개인정보 흐름도 → 개인정보 흐름표 → 개인정보 처리업무표 및 업무흐름도
 - ③ 개인정보 처리업무표 및 업무흐름도 → 개인정보 흐름표 → 개인정보 흐름도 → 정보시스템 구조도 및 정보보호 현황표
 - ④ 정보시스템 구조도 및 정보보호 현황표 → 개인정보 흐름표 → 개인정보 흐름도 → 개인정보 처리업무표 및 업무흐름도
25. ASLR 기법에 대한 설명으로 가장 적절하지 않은 것은?
- ① Linux, Windows 10 등의 최신 운영체제에서 지원하고 있다.
 - ② 스택 영역의 시작 위치가 프로세스마다 달라진다.
 - ③ 버퍼오버플로우 공격에 대응할 수 있다.
 - ④ 프로세스 스케줄링 기법 중의 하나이다.