정 보 보 호 론 (9급)

(과목코드 : 141)

2024년 군무원 채용시험　　응시번호 :　　성명 :

1. 멀티 팩터 인증(Multi-Factor Authentication)에서 사용되는 인증 수단과 가장 거리가 먼 것은?
   ① 무엇을 알고 있나(지식)
   ② 어디에 있나(지리적 위치)
   ③ 무엇을 갖고 있나(소유)
   ④ 누구인가(생체 인식)

2. 다음 중 정보 보안의 중요한 3대 요소와 가장 거리가 먼 것은?
   ① 가용성(Availability)
   ② 무결성(Integrity)
   ③ 기밀성(Confidentiality)
   ④ 중복성(Redundancy)

3. 안티바이러스 프로그램에서 시그니처 기반 검출은 무엇을 기반으로 하는 것인가?
   ① 사용자 행동
   ② 알려진 바이러스 코드 패턴
   ③ 네트워크 트래픽
   ④ 시스템 성능 지표

4. 정보 기술 분야에서 클라우드 서비스 모델에 포함되지 않는 것은?
   ① PaaS(Platform as a Service)
   ② SaaS(Software as a Service)
   ③ RaaS(Role as a Service)
   ④ IaaS(Infrastructure as a Service)

5. BYOD(Bring Your Own Device) 업무 환경에서 필요한 사항으로 가장 적절하지 않은 것은?
   ① 다양한 애플리케이션의 지원
   ② 디바이스 암호화
   ③ 네트워크 접속에 대한 보안
   ④ 역할기반 인증

6. 다음 중 정보보호 기본목표에 대한 설명으로 가장 적절한 것은?

> ○ 최근 사회적 혼란을 야기하기 위해 국내 정부부처 웹사이트를 대상으로 (가) 공격이 증가하고 있다.
> ○ (가) 공격은 대상 웹서비스 중단을 목적으로 서버, 서비스 또는 네트워크에 인터넷 트래픽을 대량으로 보내는 악의적인 사이버 공격으로 정보보호의 기본목표인 (나) 을/를 훼손하기 위한 목적으로 시도되는 공격이다.

   ① (가): 세션 하이재킹(Session Hijacking)
   (나): 기밀성
   ② (가): SQL 인젝션(SQL injection)
   (나): 무결성
   ③ (가): 분산서비스 공격(Distributed Denial of Service)
   (나): 가용성
   ④ (가): 제로데이 공격(ZeroDay Attack)
   (나): 책임추적성

7. HTTP Request Methods 중 GET 방식에 대한 설명으로 가장 적절한 것은?
   ① GET 방식은 각 이름과 값을 '&'로 결합하고 URL의 글자수를 제한하고 있지 않다.
   ② GET 방식은 데이터가 주소 입력란에 표시되기 때문에 보안에 매우 취약한 방식이다.
   ③ GET 방식은 URL에 요청 데이터를 기록하지 않고 HTTP 헤더에 데이터를 전송하는 방식이다.
   ④ GET 방식의 요청은 브라우저 히스토리에 남지 않는다.

8. 다음 중 해시(Hash)에 대한 설명으로 가장 적절하지 않은 것은?
   ① 해시는 양방향 암호화 기법을 사용하고, 암호화(Encryption)는 단방향 암호화 기법을 사용한다.
   ② 해시 함수는 임의 길이의 입력값을 받아 고정된 길이의 출력값을 내는 함수이다.
   ③ 해시 알고리즘은 MD5, SHA-256 등이 존재하며 MD5는 보안상 매우 취약한 알고리즘으로 사용하는 것을 권고하고 있지 않다.
   ④ 해시는 입력값이 일부만 변경되어도 전혀 다른 결과값을 출력하는 특징을 가지고 있다.

9. 다음 중 주요정보통신기반시설에 대한 설명으로 가장 적절한 것은?
   ① 주요정보통신기반시설은 「국가정보원법」에서 관련 근거 조항을 찾을 수 있다.
   ② 주요정보통신기반시설에 대한 취약점 분석·평가는 주요정보통신기반시설의 관리기관이 직접 수행하는 방법이 유일하다고 할 수 있다.
   ③ 주요정보통신기반시설로 신규 지정이 된 경우, 지정 후 10개월 이내에 취약점 분석·평가를 실시하여야 한다.
   ④ 주요정보통신기반시설에 대한 최초의 취약점 분석·평가를 한 후에는 매년 정기적으로 취약점 분석·평가를 실시하여야 한다.

10. 블록체인(Blockchain) 기술에 대한 설명으로 가장 적절한 것은?
   ① 처리 노드의 다중화
   ② 중앙 집중식 데이터 관리
   ③ 데이터 무결성 및 분산 합의
   ④ 단일 실패 지점(SPOF) 방지

11. 다음 중 공격과 이에 대한 대응 방안의 연결 중 가장 적절하지 않은 것은?
   ① sniffing - encryption
   ② spoofing - authentication
   ③ insecure defaults - reconfiguration
   ④ code injection - masquerading

12. 다음 중 SSO(Single Sign-On) 인증에 대한 설명으로 가장 적절하지 않은 것은?
   ① 1회 사용자 인증으로 다수의 애플리케이션 및 웹사이트에 대한 사용자 로그인을 허용하는 인증방식이다.
   ② ID와 패스워드를 개별적으로 관리하는 위험성을 해소하고, 중앙 집중 관리를 통해 보안을 강화하는 것을 목적으로 한다.
   ③ 관리자에게는 관리의 편의성을 제공하지만, 사용자에게는 사용의 편의성을 충분히 제공하지 못하는 단점이 있다.
   ④ SSO 서버가 단일 실패 지점(Single Point of Failure)이므로, 해당 서버가 침해되면 모든 서버의 보안이 위협받을 수 있는 위험이 있다.

13. 다음 중 리눅스(LINUX)의 특징에 대한 설명으로 가장 적절한 것은?
   ① 리눅스는 싱글유저 환경을 지원하는 시스템이다.
   ② 리눅스는 사용자가 쉘(Shell) 없이 직접 커널에 접속하여 명령을 수행하는 구조이다.
   ③ 리눅스는 다양한 쉘(Shell)을 제공하며, 쉘은 리눅스에서 명령어와 프로그래밍을 실행할 때 사용되는 인터페이스 역할을 한다.
   ④ 리눅스는 보안성을 강화하기 위해 프로그램 소스코드를 외부에 공개하지 않고 있다.

14. 정보보호의 설명 중 가장 적절하지 않은 것은?
   ① 위험 평가(Risk Assessment)의 목적은 조직에 잠재적인 위험 요인을 식별하고 분석하는 것이다.
   ② 가상 사설망(VPN, Virtual Private Network)은 안전한 원격 접속 및 데이터 전송을 목적으로 한다.
   ③ 키로거(Keylogger)의 위협은 암호화된 키 입력 사용으로 대응할 수 있다.
   ④ 블랙햇 해커(Black Hat Hacker)는 공인된 보안 전문가를 지칭한다.

15. 운영체제/보안에서 레이스 컨디션(race condition)에 대한 설명으로 가장 적절한 것은?
① 경쟁 상대를 물리치기 위한 공격
② 네트워크 경쟁자의 성능을 측정하는 과정
③ 컴퓨터의 처리 속도를 최적화하기 위한 테크닉
④ 비동기적으로 실행되는 프로세스들 사이의 동기화에서 문제 발생

16. PKI에서 발급하는 전자 인증서를 보유한 주체로 가장 적절한 것은?
① 사용자 또는 장치
② 인증 기관(CA)
③ 등록 기관(RA)
④ 키 분배 센터

17. 다음 중 생체인증(바이오) 시스템의 정확도(또는 성능측정)에 대한 설명으로 가장 적절하지 않은 것은?
① FRR(False Rejection Rate)은 시스템에 등록된 사용자가 사용 시 본인임을 확인하지 못하고 인증을 거부하는 오류로 Type 1 Error로 불리기도 한다.
② FAR(False Acceptance Rate)은 인증 권한이 없는 사용자가 인증을 시도했을 때 성공하는 경우를 의미하며 FAR에 비해 FRR이 높은 것은 정보보호 측면에서 더 심각한 문제가 될 수 있다.
③ CER(Crossover Error Rate)은 FAR과 FRR이 그리는 곡선의 교차점을 말한다.
④ 생체인증(바이오) 시스템은 CER이 낮을수록 정확한 시스템이다.

18. 하드웨어 보안 모듈(HSM)의 사용 목적과 가장 가까운 것은?
① 고속 연산 처리
② 공개키 인프라(PKI) 내의 암호화키 관리
③ 하드웨어 구성 업데이트
④ 바이러스 실시간 탐지

19. 유닉스의 특수권한인 setuid, setgid, sticky bit에 대한 설명으로 가장 적절한 것은?
① setgid가 붙은 프로그램은 실행 시 소유자의 권한으로 전환된다.
② setuid를 설정하려면 root 권한으로 'chmod 2755 filename'와 같이 설정하면 된다.
③ sticky bit가 설정된 디렉터리는, 누구나 파일을 만들 수 있지만 자신의 소유가 아닌 파일은 삭제할 수 없다.
④ sticky bit는 파일과 디렉터리에 모두 설정할 수 있다.

20. 다음에서 설명하는 네트워크 공격방식으로 가장 적절한 것은?

> ○ 네트워크 공격방식의 일종으로 source ip와 destination ip를 똑같게 해서, 공격 대상이 자기 자신에게 응답하도록 하는 공격방식이다.
> ○ 대응방법으로 출발지와 목적지 IP가 동일한 패킷을 방화벽 등에서 차단한다.

① Land Attack
② SMURF Attack
③ PING OF DEATH
④ SYN Flooding

21. 블록 암호화 운영모드 중 ECB(Electronic CodeBook) 모드에 대한 설명으로 가장 적절한 것은?
① 가장 단순한 모드로 블록단위로 나누어 순차적으로 암호화하는 구조이다.
② 블록 암호화 모드 중 보안이 가장 강력한 암호화 모드로 평가된다.
③ 동일한 평문 블록이라도 서로 다른 암호문 블록으로 암호화된다.
④ 암호화, 복호화에 쓰이는 키는 서로 다르다는 특징이 있다.

22. 다음 중 정보보호 및 개인정보보호 관리체계 인증체계(ISMS-P)에 대한 설명으로 가장 적절하지 않은 것은?

① 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)가 통합된 관리체계이다.

② 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합한지에 대해 한국인터넷진흥원 또는 인증기관이 증명하는 제도이다.

③ 개인정보보호법에 따라 일정 규모의 개인정보처리자는 정보보호 및 개인정보보호 관리체계 인증을 의무적으로 신청해야 한다.

④ 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항 등으로 구분된다.

23. 패스워드 크래킹(Password Cracking) 방법 중 레인보우 테이블(Rainbow Table)을 이용한 공격 방법에 대한 설명으로 가장 적절한 것은?

① 윈도우 LM(Lan Manager) 패스워드를 몇 분 만에 크래킹하면서 유명해진 해킹방법으로 패스워드와 해시로 이루어진 테이블을 무수히 만들어 놓은 체인을 이용한다.

② 패스워드를 모아서 하나의 사전파일로 만든 후 하나씩 대입하여 패스워드 일치 여부를 확인하는 방법이다.

③ 비밀번호로 사용될 수 있는 모든 문자를 대입하여 패스워드 일치 여부를 확인하는 방법이다.

④ 사전 공격(Dictionary Attack) 기법과 무차별 대입 공격(Brute Force Attack)을 혼합하여 사용하는 방법이다.

24. 다음 중「개인정보의 안전성 확보조치 기준」에 대한 설명으로 가장 적절한 것은?

① 개인정보 암호화 대상은 주민등록번호, 여권번호, 비밀번호 등이 있으며 모두 복호화가 가능한 암호화 알고리즘을 사용하여 암호화하여야 한다.

② 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.

③ 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 6개월 이상 보관·관리하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 개인정보취급자의 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 1년간 보관하여야 한다.

25. 다음 중 윈도우(Windows) 인증에 대한 설명으로 가장 적절하지 않은 것은?

① LSA(Local Security Authority)는 모든 계정의 로그인을 검증하고 시스템 자원(파일 등)에 대한 접근 권한을 검사한다.

② SAM(Security Account Manager)은 인증된 사용자에게 SID(Security ID)를 부여한다.

③ SRM(Security Reference Monitor)은 SID를 기반으로 파일이나 디렉터리에 접근을 허용할지 결정하고 이에 대한 감사 메시지를 생성하는 역할을 수행한다.

④ 윈도우 인증과정에서 사용되는 주요 서비스로 LSA, SAM, SRM이 있다.