정 보 보 호 론 (9급)

(과목코드 : 141)

2026년 군무원 채용시험　　응시번호 :　　성명 :

1. PKI(Public Key Infrastructure)의 구성 요소가 아닌 것은?
① 인증기관(CA)
② 등록기관(RA)
③ 디렉터리 서비스
④ 침입탐지 시스템(IDS)

2. 스팸 메일 필터링 방식 중 이메일 발신 도메인의 DNS에 등록된 IP를 검증하는 방식은?
① 베이지안 필터
② SPF(Sender Policy Framework)
③ 블랙리스트 필터
④ 콘텐츠 필터

3. VPN(Virtual Private Network)의 주된 목적으로 가장 적절한 것은?
① 공중망에서 안전한 사설 통신 채널 구성
② 인터넷 속도 향상
③ 악성코드 차단
④ 이메일 필터링

4. XSS(Cross-Site Scripting) 공격에서 주로 이용하는 취약점으로 가장 적절한 것은?
① SQL 데이터베이스 취약점
② 웹 애플리케이션의 입력값 검증 미흡
③ 운영체제 커널 취약점
④ 네트워크 라우팅 취약점

5. 사물인터넷(IoT) 장비를 주로 감염시키고 P2P(Peer-To-Peer) 기반의 봇넷을 구성하며, 2020년대 들어 지속해서 대량으로 탐지되고 있는 악성코드는?
① Emotet
② LokiBot
③ Mozi
④ FormBook

6. TLS Handshake 과정에서 서버가 클라이언트에게 전송하는 것으로 가장 적절하지 않은 것은?
① 서버 인증서
② 지원하는 암호화 알고리즘 목록
③ 서버 랜덤값
④ 서버의 개인키

7. 과학기술정보통신부가 주무 부처로 관장하는 법률이 아닌 것은?
①「정보통신기반 보호법」
②「산업기술의 유출방지 및 보호에 관한 법률」
③「전자서명법」
④「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」

8. 커버로스(Kerberos) 인증 프로토콜에 대한 설명으로 가장 적절하지 않은 것은?
① 티켓 기반 인증 방식을 사용한다.
② 대칭키 암호화를 기반으로 한다.
③ 공개키 인프라(PKI)만을 사용한다.
④ 단일 로그온(SSO)을 지원한다.

9. 디지털 포렌식(Digital Forensics) 원칙에 대한 설명으로 옳은 것을 모두 고르면?

ㄱ. 원본 증거의 무결성을 보존하기 위해 이미지 복사본으로 분석을 수행한다.
ㄴ. 해시값을 통해 수집된 증거의 변조 여부를 검증할 수 있다.
ㄷ. 증거의 연속성(Chain Of Custody)은 증거의 취급 이력을 문서화한다.
ㄹ. 포렌식 도구로 수집한 모든 데이터는 법적 효력을 자동으로 가진다.

① ㄱ, ㄴ
② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ, ㄹ

10. 침입탐지 시스템(IDS)에 대한 설명으로 틀린 것을 모두 고르면?

ㄱ. 시그니처 기반 탐지는 알려진 공격 패턴과 비교하여 탐지하므로 알려지지 않은 공격(Zero-day)에 취약하다.
ㄴ. 이상 탐지(Anomaly Detection)는 정상 행위 기준을 설정하고 벗어나는 행위를 탐지하므로 오탐(False Positive)이 발생할 수 있다.
ㄷ. NIDS는 암호화된 트래픽도 복호화하여 내용 기반으로 탐지할 수 있다.
ㄹ. IDS는 탐지만 수행하며, 능동적 차단은 IPS의 역할이다.

① ㄷ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

11. IPSec 프로토콜에 대한 설명으로 틀린 것을 모두 고르면?

ㄱ. AH(Authentication Header)는 데이터 무결성과 인증을 제공하지만 기밀성은 제공하지 않는다.
ㄴ. ESP(Encapsulating Security Payload)는 데이터 암호화와 인증을 모두 제공한다.
ㄷ. 전송 모드(Transport Mode)는 원본 IP 헤더를 포함한 전체 패킷을 새 패킷으로 캡슐화한다.
ㄹ. IKE(Internet Key Exchange)는 IPSec에서 보안 연결(SA) 협상에 사용된다.

① ㄷ
② ㄷ, ㄹ
③ ㄴ, ㄷ
④ ㄱ, ㄷ

12. 방화벽(Firewall)에 대한 설명으로 틀린 것을 모두 고르면?

ㄱ. 상태 기반 검사(Stateful Inspection) 방화벽은 TCP 연결 상태를 추적한다.
ㄴ. 방화벽은 암호화된 악성코드 내부 내용을 자동으로 탐지하고 차단한다.
ㄷ. 패킷 필터링 방화벽은 IP 주소와 포트 번호를 기반으로 트래픽을 제어한다.
ㄹ. 방화벽은 내부 사용자에 의한 모든 내부 위협을 완벽하게 차단한다.

① ㄱ, ㄷ
② ㄴ, ㄹ
③ ㄴ, ㄷ, ㄹ
④ ㄱ, ㄴ, ㄷ, ㄹ

13. 공개키 기반구조(PKI)에 대한 설명으로 옳은 것을 모두 고르면?

ㄱ. 인증기관(CA)은 공개키 인증서를 발급·관리한다.
ㄴ. 인증서 폐지 목록(CRL)은 유효기간이 만료된 인증서 목록이다.
ㄷ. 등록기관(RA)은 사용자 신원을 확인하고 인증서 발급을 요청한다.
ㄹ. OCSP는 인증서의 실시간 유효성 검증을 위한 프로토콜이다.

① ㄱ, ㄷ
② ㄱ, ㄴ, ㄹ
③ ㄱ, ㄷ, ㄹ
④ ㄱ, ㄴ, ㄷ, ㄹ

14. 해시함수 H에 대한 성질을 설명한 것으로 가장 적절한 것은?

A. 서로 다른 입력 값 x, y에 대해 H(x) = H(y)가 되는 경우를 찾기 어렵다.
B. 주어진 출력 값 y에 대해 H(x) = y를 만족하는 x를 찾기 어렵다.

① A - 제2역상저항성 B - 충돌저항성
② A - 충돌저항성 B - 일방향성
③ A - 일방향성 B - 제2역상저항성
④ A - 충돌저항성 B - 제2역상저항성

15. 다음은 MAC(Message Authentication Code)을 사용하는 환경을 설명한다. 이에 대한 설명으로 가장 적절하지 않은 것은?

어떤 시스템에서 송신자 A와 수신자 B는 비밀키 K를 공유하고 있으며, 메시지 M과 MAC 값을 함께 전송하고 있다.

① MAC 값은 보안을 위해 반드시 96비트 길이로 절단(Truncation)해야 한다.
② MAC은 메시지의 무결성과 송신자 인증을 제공할 수 있다.
③ 재전송 공격을 방지하기 위해 Nonce나 타임스탬프를 함께 사용할 수 있다.
④ 안전한 MAC 알고리즘은 K를 알지 못하면 새로운 유효한 MAC 값을 생성하기 어렵다.

16. TLS 1.3에 대한 설명으로 가장 적절하지 않은 것은?

① TLS 1.3에서는 Handshake 과정에서 디피-헬만 키 교환을 사용하여 전방향 안전성(Forward Secrecy)을 기본적으로 제공한다.
② TLS 1.3에서는 서버 인증 시 X.509 인증서를 사용하며, 클라이언트는 이를 검증하여 서버의 신원을 확인한다.
③ TLS 1.3에서는 RSA 키 교환 방식이 제거되었으나, RSA 기반 전자서명은 여전히 사용될 수 있다.
④ TLS 1.3에서는 Handshake 과정에서 암호화되지 않은 서버의 X.509 인증서를 클라이언트에게 전송한다.

17. DNSSEC(Domain Name System Security Extensions)에 대한 설명으로 가장 적절한 것은?

① DNSSEC은 전자서명을 이용하여 DNS 데이터의 무결성과 출처 인증을 제공한다.
② DNSSEC은 DNS 응답 데이터를 암호화하여 기밀성을 제공한다.
③ DNSSEC은 공유 비밀키를 이용하여 DNS 서버 간 인증을 수행한다.
④ DNSSEC은 DNS 질의 자체를 보호하여 스니핑을 방지한다.

18. 웹 보안에서 사용하는 쿠키(Cookie)의 보안 속성에 대한 설명으로 가장 적절한 것은?

① HttpOnly 속성이 설정된 쿠키는 HTTPS 연결에서만 전송된다.
② Secure 속성이 설정된 쿠키는 클라이언트 측 스크립트에서 접근할 수 없다.
③ SameSite 속성은 교차 사이트 요청에서 쿠키 전송 여부를 제어할 수 있다.
④ 쿠키는 기본적으로 암호화되어 저장되므로 별도의 보호가 필요 없다.

19. 웹 애플리케이션에서 CSRF(Cross-Site Request Forgery) 공격에 대한 설명으로 가장 적절한 것은?
① CSRF 공격은 주로 서버 측 데이터베이스 취약점을 이용한다.
② CSRF 토큰은 예측 불가능한 값으로 생성되어야 한다.
③ CSRF 공격은 암호화된 통신(HTTPS)을 사용하면 완전히 방지된다.
④ CSRF는 사용자의 비밀번호를 직접 탈취하는 공격이다.

20. 시스템 관리자가 특정 파일에 대해 소유자만 읽기와 쓰기가 가능하도록 설정하려고 한다. 이때 사용할 수 있는 명령어로 가장 적절한 것은?
① chmod 777 file.txt
② chmod 644 file.txt
③ chmod 755 file.txt
④ chmod 600 file.txt

21. 아래의 공격 시나리오에 대한 설명으로 가장 적절한 것은?

> 공격자는 특정 웹사이트에 악성 스크립트를 삽입하여 사용자 브라우저에서 실행되도록 하였고, 이를 통해 사용자의 세션 쿠키를 탈취하였다. 이후 탈취한 쿠키를 이용하여 정상 사용자로 가장하여 시스템에 접근하였다.

① Session Hijacking 공격으로, XSS를 통해 세션 정보를 탈취한 후 수행한 것이다.
② SQL Injection 공격으로, 데이터베이스를 조작한 것이다.
③ CSRF 공격으로, 사용자의 요청을 위조한 것이다.
④ DoS 공격으로, 시스템 자원을 고갈시킨 것이다.

22. 현재 디렉터리에 있는 파일과 하위 디렉터리 목록을 확인하는 명령어로 가장 적절한 것은?
① ls
② cd
③ pwd
④ mkdir

23. 공급망 공격(Supply Chain Attack)에 대한 설명으로 가장 적절한 것은?
① 공격자가 직접 사용자 컴퓨터를 해킹하여 데이터를 탈취하는 공격이다.
② 신뢰된 소프트웨어나 업데이트 경로를 악용하여 악성코드를 배포하는 공격이다.
③ 네트워크 트래픽을 가로채어 정보를 수집하는 공격이다.
④ 사용자에게 이메일을 보내 비밀번호를 입력하게 하는 공격이다.

24. 「개인정보 보호법 시행령」에 따라 개인정보처리자가 정보주체의 동의 없이 개인정보를 이용 또는 제공하려는 경우 고려해야 하는 사항으로 가장 적절하지 않은 것은?
① 당초 수집 목적과 관련성이 있는지 여부
② 정보주체의 이익을 부당하게 침해하는지 여부
③ 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부
④ 익명정보가 다른 정보와 결합하여 개인을 식별할 수 있는지 여부

25. 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 분야에 대한 설명으로 가장 적절하지 않은 것은?

① 위험관리는 조직이 자산, 위협, 취약점을 식별하고 위험을 평가·처리하는 과정을 포함한다.

② 접근통제는 사용자 인증, 권한 관리, 접근 기록 등을 통해 시스템 접근을 통제하는 것을 포함한다.

③ 암호화 적용은 모든 정보 자산에 대해 반드시 동일한 암호 알고리즘을 적용하도록 요구한다.

④ 시스템 및 서비스 운영관리는 이상 행위를 탐지하고 대응하기 위한 기록 및 분석 활동을 포함한다.