

# 네트워크보안(9급)

(과목코드 : 142)

2025년 군무원 채용시험

응시번호 :

성명 :

1. 최근 사이버 공격자들이 서비스형 랜섬웨어를 활용하는 주된 이유에 대한 설명으로 가장 적절한 것은?

- ① 자체적인 랜섬웨어 개발 능력이 부족해도 쉽게 공격을 실행할 수 있기 때문이다.
- ② 암호화된 데이터의 복호화 키를 안전하게 관리하기 위해서이다.
- ③ 공격 대상 시스템의 취약점을 분석하는 시간을 단축하기 위해서이다.
- ④ 법적 추적을 피하기 위해 익명성을 강화하는 효과가 있기 때문이다.

2. CIDR에 대한 설명으로 가장 적절하지 않은 것은?

- ① IPv4의 주소 클래스를 사용하지 않는다.
- ② ‘/’ 문자를 통해 네트워크 ID의 길이를 표시한다.
- ③ 접두어 합침을 통해 라우팅 테이블이 유지해야 하는 정보의 수를 클래스 기반 주소 지정에 비해 감소시킨다.
- ④ IPv6 주소 클래스 단위로 주소를 할당한다.

3. 다음 설명으로 가장 적절한 것은?

- 개별 시스템에 설치되어 해당 장비에 대한 직접적인 접근제어를 제공한다.
- OS 레벨에서 동작하며 일반적으로 SW 기반으로 구현된다.
- Windows Defender, iptables 등이 대표적이다.

- ① 경계형 방화벽      ② 내부 방화벽
- ③ 이중 방화벽      ④ 호스트 기반 방화벽

4. 다음 설명의 보안 공격 기법으로 가장 적절한 것은?

한 사용자는 어느 블로그 댓글 입력창에 글을 작성했다. 그런데 해당 입력창에 숨겨진 악성 스크립트가 삽입되어 있었고, 사용자가 댓글을 등록하자마자 그의 브라우저에서 스크립트가 실행되어 쿠키 정보가 공격자에게 전송되었다.

- ① SQL 인젝션(SQL Injection)
- ② 사이트 간 스크립팅(Cross Site Scripting)
- ③ 무차별 대입 공격(Brute Force Attack)
- ④ 사이트 간 요청 위조(Cross Site Request Forgery)

5. ARP를 악용한 해킹처럼 동일한 네트워크에서 메시지를 몰래 가로채는 중간자 공격이 주로 발생하는 OSI 참조 모델의 계층은?

- ① 데이터 링크 계층    ② 네트워크 계층
- ③ 전송 계층            ④ 세션 계층

6. DNS 프로토콜의 보안 취약점을 해결하기 위해 도입된 DNSSEC이 제공하는 주요 보안 기능에 대한 설명으로 가장 적절한 것은?

- ① DNS 질의 및 응답 메시지 암호화
- ② DNS 서버 간 영역 전송 암호화
- ③ DNS 데이터의 무결성 및 출처 인증 보장
- ④ DNS 서버 자체의 가용성 보장

7. Advanced, Persistent, Threats는 APT를 정의하는 세 가지 핵심 요소다. 'Persistent'가 의미하는 바에 대한 설명으로 가장 적절한 것은?

- ① 공격자가 최신 기술을 사용하여 공격한다.
- ② 공격 배후에 숙련되고 목적의식이 뚜렷한 주체가 있다.
- ③ 공격자가 탐지를 회피하며 장기간에 걸쳐 시스템에 침입 상태를 유지한다.
- ④ 공격이 일회성으로 끝나지만 피해 규모가 크다.

8. 애플리케이션 게이트웨이에 대한 설명으로 적절하지 않은 것은?

- ① 응용 계층에서 동작한다.
- ② 프로토콜별로 Proxy Daemon이 필요하다.
- ③ 응용 프로그램 사용을 기록하여 사용자 및 응용 서비스 접근제어를 제공한다.
- ④ 처리 속도가 빠르고, 다양한 서비스에 대한 유연성을 제공한다.

9. 보안사고 대응 절차 중 사고 상황을 문서화하고 전문 인력에게 보고한 후 신속히 조치 조치를 가동하며 관계 부서에도 공식적으로 통보하는 단계로 가장 적절한 것은?

- ① 사고 탐지                      ② 초기 대응
- ③ 사고 조사                    ④ 해결

10. SSH의 전송 계층 프로토콜 동작 과정으로 적절하지 않은 것은?

- ① 서버가 클라이언트에게 개인키를 전송하여 서버 인증
- ② 클라이언트와 서버 간 키 교환
- ③ 클라이언트와 서버가 SSH 버전 정보 교환
- ④ 암호화, MAC, 압축 방식 협의

11. 침입 탐지 시스템(IDS) 중 알려진 공격 패턴을 수집하고 분류한 후 네트워크 트래픽을 검사하여 일치하는 패턴의 위협 수준을 평가하는 방식으로 가장 적절한 것은?

- ① 이상 탐지 기반 IDS
- ② 하이브리드 IDS
- ③ 시그니처 기반 IDS
- ④ 행동 분석 기반 IDS

12. CSMA/CD 방식에서 데이터 전송 중 충돌이 감지되었을 때 송신 장치가 잼 신호(Jam Signal)를 전송하는 이유로 가장 적절한 것은?

- ① 데이터 전송 속도를 일시적으로 높이기 위해
- ② 충돌에 관여된 다른 모든 장치에 충돌 발생을 확실히 알리기 위해
- ③ 특정 시간 동안 매체를 독점적으로 쓰기 위한 예약 신호로 사용하기 위해
- ④ 손상된 프레임을 즉시 복구하기 위한 정보를 포함하기 위해

13. 포트 미러링에 대한 설명으로 가장 적절한 것은?

- ① 네트워크 속도를 증가시킨다.
- ② 특정 포트의 트래픽을 복사하여 다른 포트로 전달한다.
- ③ 트래픽 모니터링과 암호화를 통해 기밀성을 제공한다.
- ④ 여러 포트에서 유입되는 트래픽을 모아 보관하는 것이 목적이다.

14. 패스워드 크래킹에 대한 설명으로 가장 적절하지 않은 것은?
- ① 사전 공격은 패스워드 크래킹의 소요 시간을 감소시킬 수 있다.
  - ② 패스워드 입력 실패 횟수에 제한이 없고 충분한 시간이 주어지면 무작위 대입 공격으로 패스워드를 알아낼 수 있다.
  - ③ 충분한 길이의 패스워드는 이론적으로 패스워드 크래킹이 불가능하다.
  - ④ John the Ripper는 패스워드 크래킹 도구이다.
15. 시스템 및 네트워크 모니터링에 대한 설명으로 가장 적절하지 않은 것은?
- ① 서버나 네트워크 장비의 성능에 영향을 줄 수 있는 시스템 상태를 사전에 감지하기 위해 수행하는 것을 리소스 모니터링이라고 한다.
  - ② 서버나 네트워크 장비가 정상적으로 작동하는지 확인하기 위해 네트워크 트래픽 흐름과 병목 발생 여부를 감시하는 것을 트래픽 모니터링이라고 한다.
  - ③ 웹 서버나 애플리케이션 서버의 상태를 주기적으로 점검하여 정상 동작 여부를 확인하는 것을 헬스 체크라고 한다.
  - ④ ping이나 HTTP 요청을 외부에서 보내 응답 상태를 확인하는 방식은 일반적으로 내부 모니터링이라고 한다.
16. 이더넷을 통해 데이터를 전송할 때 이더넷 프레임의 헤더에 포함되지 않는 항목으로 가장 적절한 것은?
- ① 목적지(Destination) 이더넷 주소
  - ② 발신지(Source) 이더넷 주소
  - ③ 이더넷 유형(Type)
  - ④ 체크섬(Checksum)
17. 클라우드 환경에서 발생할 수 있는 여러 보안 위협 중 가장 적절하지 않은 것은?
- ① 시스템 취약점(System Vulnerabilities)
  - ② 잘못된 설정(Misconfiguration)
  - ③ 서버과열로 인한 성능저하(Server Overheating)
  - ④ APT(Advanced Persistent Threats)
18. 방화벽에서 정책이 적용될 때 네트워크 트래픽이 특정 규칙에 따라 허용되거나 차단되는 과정에 대한 설명으로 가장 적절한 것은?
- ① 가장 마지막에 설정된 규칙이 우선 적용된다.
  - ② 트래픽 정보와 가장 많이 일치하는 규칙이 적용된다.
  - ③ 룰셋의 위에서부터 순서대로 규칙을 평가하며 가장 먼저 일치하는 규칙의 액션이 적용된다.
  - ④ 설정된 모든 규칙을 동시에 평가하여 최종 액션을 결정한다.
19. 네트워크 보안 위협에 대한 설명으로 가장 적절하지 않은 것은?
- ① 악성코드: 바이러스, 웜 등 시스템에 피해를 주거나 정보를 탈취하는 해로운 소프트웨어
  - ② 제로데이 공격: 아직 공개되지 않은 보안 취약점을 악용해 공격하는 것으로 기존 보안 시스템이 탐지하기 어려움
  - ③ 권한 상승: 공격자가 일반 사용자 권한을 탈취한 후 관리자 수준의 권한으로 상승시켜 시스템을 제어함
  - ④ DDoS: 조직 내부자가 시스템에 접근해 데이터를 탈취하거나 오용하는 내부자 위협

20. VPN의 구성에 필요한 기능으로 가장 적절하지 않은 것은?

- ① 인증: 사용자나 장치의 신원을 검증하여 안전한 접근을 보장하는 기능
- ② 백업: 시스템 장애나 데이터 손실을 대비해 데이터를 복사해두는 기능
- ③ 터널링: 공용 네트워크상에서 사설 네트워크 처럼 데이터를 주고받기 위한 가상 연결 생성 기능
- ④ 암호화: 전송 중인 데이터를 보호하기 위해 내용을 암호화하는 보안 기능

21. TLS와 프로토콜의 연동 목적으로 적절하지 않은 것은?

- ① HTTPS는 HTTP에 TLS를 적용하여 웹사이트 상의 보안 통신을 지원한다.
- ② FTPS는 FTP에 TLS를 적용하여 보안 파일 전송을 지원한다.
- ③ SMTPS는 SMTP에 TLS를 적용하여 이메일 보안을 지원한다.
- ④ IMAPS는 IMAP에 TLS를 적용하여 인증서 기반의 부인 방지를 지원한다.

22. A와 B가 비대칭키 암호화를 이용하여 통신하는 과정에서 발생할 수 있는 문제점으로 가장 적절한 것은?

- 1. A는 통신을 시작하기 전에 자신의 공개키와 개인키로 구성된 쌍을 생성한다.
- 2. A는 자신의 공개키를 사용하여 메시지를 암호화한다.
- 3. A는 암호화된 메시지를 B에게 전송한다.
- 4. B는 해당 메시지를 복호화하기 위해 A의 개인키를 요청한다.

- ① B는 A의 개인키를 받을 수 없기 때문에 A의 공개키로 암호화된 메시지를 복호화할 수 없다.
- ② B뿐만 아니라 공격자 C 또한 A의 개인키를 입수하여 암호화된 메시지를 복호화할 수 있다.
- ③ 공격자 C가 자신의 개인키를 생성하여 A의 공개키로 암호화된 메시지를 복호화할 수 있다.
- ④ 공격자 C가 B의 공개키를 확보하여 A의 공개키로 암호화된 메시지를 복호화할 수 있다.

23. 공개키 기반 구조(PKI)의 구성요소로 가장 적절하지 않은 것은?

- ① 인증기관(Certificate Authority)
- ② TGS(Ticket Granting Server)
- ③ 디지털 인증서(Digital Certificate)
- ④ 등록기관(Registration Authority)

24. RIPEMD-160, TIGER와 같이 데이터의 변조 여부를 확인하기 위한 무결성 검증 방식으로 가장 적절한 것은?

- ① 해시함수(Hash Function) 방식
- ② 비대칭키(Asymmetric Key) 방식
- ③ 대칭키(Symmetric Key) 방식
- ④ 공개키(Public Key Encryption) 방식

25. traceroute 명령이 경로를 단계별로 파악하기 위해 사용하는 IP 헤더 필드와 ICMP 메시지로 가장 적절한 것은?

- ① IP 헤더 필드: Fragment Offset,  
ICMP 메시지: Destination Unreachable
- ② IP 헤더 필드: Differentiated Services Field,  
ICMP 메시지: Echo Reply
- ③ IP 헤더 필드: Time To Live(TTL),  
ICMP 메시지: Time Exceeded
- ④ IP 헤더 필드: Protocol,  
ICMP 메시지: Redirect