

네트워크보안(7급)

(과목코드 : 142)

2025년 군무원 채용시험

응시번호 :

성명 :

- | | |
|--|--|
| <p>1. TCP CUBIC의 혼잡 제어 메커니즘을 직접적으로 타깃으로 하여 공격자가 의도적으로 대역폭을 축소시키거나 패킷 손실을 유도할 수 있는 공격 예시로 가장 적절한 것은?</p> <p>① 암호화되지 않은 패킷 스니핑을 통한 데이터 유출 공격</p> <p>② 위조된 중복 ACK 패킷을 이용한 cwnd 강제 감소 공격</p> <p>③ TCP 연결 테이블 고갈을 위한 TCP SYN Flooding 공격</p> <p>④ 스텔스 포트 스캔을 통한 취약점 탐지 공격</p> | <p>4. 메시지 M을 인증하기 위해서 송신자는 M의 해시값 H(M)을 구한 후 H(M)을 RSA 암호 방식으로 암호화한다. 이때 송신자가 H(M)을 암호화하기 위해서 사용하는 키로 가장 적절한 것은?</p> <p>① 송신자의 공개키</p> <p>② 송신자의 개인키</p> <p>③ 수신자의 공개키</p> <p>④ 수신자의 개인키</p> |
| <p>2. 「개인정보 보호법」에서 네트워크 전송구간 암호화 대상이 아닌 것은?</p> <p>① 여권번호</p> <p>② 운전면허번호</p> <p>③ 계좌번호</p> <p>④ 외국인등록번호</p> | <p>5. TCP의 신뢰적 데이터 전송에서 패킷 손실을 감지하고 이를 복구하기 위해 사용하는 가장 핵심적인 기본 방식으로 적절한 것은?</p> <p>① Positive ACK 전송 후 재전송</p> <p>② Negative ACK(NAK) 전송 후 재전송</p> <p>③ 패킷 순서 재조정</p> <p>④ 타임아웃 기반 재전송</p> |
| <p>3. Split Horizon 규칙을 비활성화할 경우 거리 벡터 기반 라우팅 프로토콜에서 네트워크 안정성에 가장 심각한 영향을 미칠 수 있는 현상은?</p> <p>① 라우팅 테이블 크기 증가</p> <p>② 네트워크 대역폭 감소</p> <p>③ 패킷 손실 증가</p> <p>④ 라우팅 루프 발생</p> | <p>6. 재귀적 DNS 질의의 특징으로 가장 적절한 것은?</p> <p>① 클라이언트가 직접 모든 DNS 서버에 질의한다.</p> <p>② DNS 서버가 최종 IP 주소를 찾아 클라이언트에게 반환한다.</p> <p>③ DNS 서버가 중간 결과만 반환하고 클라이언트가 재질의한다.</p> <p>④ TTL 값이 무제한으로 유지된다.</p> |
| | <p>7. 해시함수 H에 대한 설명으로 가장 적절하지 않은 것은?</p> <p>① H의 결과값은 고정 비트 개수 이내의 값이다.</p> <p>② H의 입력값은 고정 비트 개수 이내의 값이다.</p> <p>③ H의 결과값에서 입력값을 계산적으로 찾아내기 어려워야 한다.</p> <p>④ H의 같은 결과값을 만드는 서로 다른 입력값을 계산적으로 찾아내기 어려워야 한다.</p> |

8. 바이러스 또는 웜의 특징으로 가장 적절하지 않은 것은?
- ① 웜은 네트워크 연결을 통해 시스템 간에 전파된다.
 - ② 웜은 바이러스보다 확산 속도가 빠르다.
 - ③ 바이러스는 프로그램의 취약점을 찾아 시스템에 침투한다.
 - ④ 바이러스는 다른 프로그램을 감염시키고 수정 또는 삭제할 수 있다.
9. Whois 서버에서 얻을 수 있는 정보로 가장 적절하지 않은 것은?
- ① DNS 레코드의 조회 결과
 - ② 도메인 등록 및 관리 기관 정보
 - ③ 레코드의 생성 시기와 갱신 시기
 - ④ 관리자 개인정보
10. IEEE 802.11i의 동작 과정에 대한 설명으로 가장 적절한 것은?
- ① 키 관리 단계에 유니캐스트 트래픽을 위한 쌍별(Pairwise) 키만 생성된다.
 - ② AP와 스테이션은 멀티캐스트 트래픽에 대한 암호 기술을 결정한다.
 - ③ AP는 인증에 참여하지 않고 AS와 스테이션 사이에서 전달(Relay) 역할만 한다.
 - ④ 종단 스테이션 간의 데이터 전송을 암호화한다.
11. 메시지 블록 M에 modulo k 연산이 사용되는 RSA 암호화 방식으로 암호화한 결과의 최댓값은?
- ① $k-1$
 - ② k
 - ③ $k+1$
 - ④ $2k$
12. IPv4 패킷의 단편화 없이 단일 패킷으로 전송 가능한 이론적 최대치로 허용되는 값은?
- ① 1,024 바이트
 - ② 1,500 바이트
 - ③ 32,768 바이트
 - ④ 65,535 바이트
13. SDN 환경에서 공격 표적이 크게 증가하는 주된 원인으로 가장 적절한 것은?
- ① 암호화 통신 미사용
 - ② 네트워크 내 물리적 장비 수의 증가
 - ③ 모든 네트워크 기능의 가상화
 - ④ 라우팅 프로토콜의 복잡성으로 인한 네트워크 관리의 어려움
14. 두 개의 클라우드 환경에서 BGP 라우터 피어 간의 세션 무결성과 인증을 보장하기 위해 실제로 가장 널리 사용되는 인증 방식은?
- ① MD5 해시
 - ② SHA-256 해시
 - ③ 공개키 인증서
 - ④ DES 암호화
15. 가명 정보의 기술적 보호조치에 대한 설명으로 가장 적절하지 않은 것은?
- ① 추가정보의 분리 보관
 - ② 접근권한의 분리
 - ③ 가명 정보 처리 관련 기록 작성·보관
 - ④ 가명 정보보호 교육 시행

16. 패킷 필터링 방화벽에 대한 설명으로 가장 적절하지 않은 것은?
- ① 디폴트 정책이 전달(Forward)인 것이 제거(Discard)보다 안전하다.
 - ② TCP 세그먼트의 페이로드를 조사하지 않는다.
 - ③ 상태(Stateful) 방화벽보다 처리 속도가 빠르다.
 - ④ 상태 방화벽보다 스푸핑 공격을 받을 가능성이 크다.
17. TLS 1.3에서 보안 결함으로 인해 제거된 암호화 알고리즘은?
- ① AES-GCM
 - ② ChaCha20-Poly1305
 - ③ RC4
 - ④ SHA-256
18. 운영체제 탐지(식별) 방법으로 가장 적절하지 않은 것은?
- ① Banner Grabbing
 - ② SYN Scan
 - ③ Netcraft
 - ④ Traceroute
19. 바이러스 방어 방법에 대한 설명으로 가장 적절하지 않은 것은?
- ① 복구(Recovery) - 시스템 복구를 통해 감염을 사전에 차단한다.
 - ② 탐지(Detection) - 감염되면 바이러스를 탐지하고 위치를 파악한다.
 - ③ 식별(Identification) - 프로그램을 감염시킨 특정 바이러스를 식별한다.
 - ④ 제거(Removal) - 바이러스를 모든 감염된 시스템으로부터 제거한다.
20. traceroute 결과에서 특정 홉(Hop)의 응답 시간이 불규칙하게 크게 증가하는 주요 원인으로 가장 적절한 것은?
- ① 해당 라우터의 큐잉 지연 증가
 - ② 전송되는 패킷의 크기 증가
 - ③ DNS 이름 해석에 대한 실패
 - ④ Time To Live(TTL) 필드 값 감소
21. Web Cache Deception 공격을 예방하기 위한 URL 설계 방법으로 가장 적절한 것은?
- ① 모든 자원(Resource)에 동일한 캐시 정책을 적용
 - ② 정적 파일과 동적 파일의 URL 패턴을 명확히 구분
 - ③ URL에 랜덤(Random) 쿼리 스트링을 추가
 - ④ 캐시 만료 시간을 무제한으로 설정
22. 보안 통신을 기본적으로 제공하지 않는 서비스 포트 번호로 가장 적절한 것은?
- ① 22
 - ② 23
 - ③ 443
 - ④ 465
23. TLS Handshake 프로토콜에서 클라이언트의 Public Diffie-Hellman 파라미터들이 포함되어 전송되는 메시지는?
- ① Certificate_Verify 메시지
 - ② Change_Cipher_Spec 메시지
 - ③ Client_Hello 메시지
 - ④ Client_Key_Exchange 메시지

24. IPsec Transport Mode ESP에 대한 설명으로 가장 적절하지 않은 것은?

- ① IPv4 패킷의 헤더를 인증한다.
- ② IPv4 패킷의 페이로드를 암호화한다.
- ③ ESP 헤더를 인증한다.
- ④ ESP 트레일러를 암호화한다.

25. 디피-헬만 키교환 방식은 중간자 공격에 취약하다. 그 원인으로 가장 적절한 것은?

- ① 기밀성을 제공하지 않는다.
- ② 무결성을 제공하지 않는다.
- ③ 메시지 인증을 제공하지 않는다.
- ④ 송신자 인증을 제공하지 않는다.