네 트 워 크 보 안 (9급)

(과목코드 : 142)

2026년 군무원 채용시험　　응시번호 :　　성명 :

1. TLS를 올바르게 구성했을 때 기대할 수 있는 보안 효과로 가장 적절한 것은?
   ① IP 주소 위조를 물리적으로 불가능하게 한다.
   ② 클라이언트와 서버 사이 통신의 도청, 변조, 메시지 위조 위험을 줄인다.
   ③ 모든 웹 애플리케이션 취약점을 자동 제거한다.
   ④ 서버 운영체제의 권한 상승 취약점을 자동 패치한다.

2. S/MIME에 대한 설명으로 가장 적절하지 않은 것은?
   ① S/MIME은 RSA를 이용해 MIME 인터넷 전자메일 형식 표준을 보안적으로 강화시킨 것이다.
   ② MIME은 SMTP가 실행파일이나 2진 데이터를 전송하지 못하는 것을 개선하였다.
   ③ MIME 전송 부호화 방법 중 Base64 전송 부호화는 일반적으로 임의의 2진 데이터를 부호화하는데 사용한다.
   ④ 기능면에서 S/MIME은 PGP와 유사하지만 PGP는 메시지를 서명하고 암호화하는 기능을 제공하지 않는다.

3. 방화벽 로그에서 외부 IP 하나가 짧은 시간동안 22, 23, 80, 443, 445, 3389 포트로 순차 접속을 시도했다. 이에 대한 판단으로 가장 적절한 것은?
   ① 포트 스캔 또는 서비스 탐색 가능성이 있으므로 출발지, 빈도, 대상 포트, 성공 여부를 분석한다.
   ② 정상적인 웹 브라우징이다.
   ③ TCP 포트이므로 보안 이벤트가 아니다.
   ④ 443 포트가 포함되어 있으므로 모두 정상이다.

4. OSI 7계층에서 2계층(데이터링크계층)의 데이터 단위(Protocol Data Unit)로 가장 적절한 것은?
   ① 비트(Bits)
   ② 세그먼트(Segment)
   ③ 패킷(Packet)
   ④ 프레임(Frame)

5. 다음에 대한 설명으로 가장 적절한 것은?

> - 이것은 메시지의 암호화 및 전자서명을 제공하고 인터넷상에서 안전한 신원 확인과 데이터 보호를 가능하게 하는 보안 프레임워크이다.
> - 이것이 되려면 인증 정보를 일원화하여 호환성을 갖춤으로써 개인이 쉽게 접근할 수 있어야 한다.
> - 신뢰를 구축하기 위해 여러 주체(PAA, PCA, CA, RA)가 트리형으로 구성하고 있다.

   ① 전자봉투
   ② DRM
   ③ 공개키 기반 구조
   ④ 커버로스

6. 다음 Snort/Suricata 형식의 규칙이 있다. 가장 적절한 것은?

> - alert tcp any any -> 192.168.10.0/24 80 (msg:"Suspicious URI"; content:"/admin.php"; http_uri; sid:100001;)

   ① 출발지가 내부망이고 목적지가 외부망인 패킷만 탐지한다.
   ② 목적지가 192.168.10.0/24의 TCP 80번이며 HTTP URI에 /admin.php가 포함된 트래픽을 경고한다.
   ③ 모든 UDP 패킷을 차단한다.
   ④ 이 규칙은 방화벽 NAT 규칙이다.

7. 랜섬웨어의 감염 경로로 가장 적절하지 않은 것은?
   ① 스팸 메일
   ② SNS로 유포된 URL
   ③ 허용된 프로그램만 실행 가능한 USB
   ④ 파일 공유 사이트에서 다운로드한 파일

8. TLS와 같은 공개 인터넷 환경의 보안 통신에서 공개키 기반 절차와 대칭키 암호를 함께 사용하는 주된 이유로 가장 적절한 것은?
① 공개키 암호는 대칭키 암호보다 항상 빠르므로 대용량 데이터 암호화에만 사용한다
② 통신 전에 안전한 비밀키를 공유하기 어려운 환경에서 공개키 기반 인증과 키 합의 절차로 세션키를 설정하고, 이후 대칭키 암호로 데이터를 효율적으로 보호할 수 있기 때문이다.
③ 공개키 암호와 대칭키 암호는 항상 같은 키를 사용한다.
④ 대칭키 암호는 기밀성을 제공할 수 없으므로 사용하지 않는다.

9. 기관 로그인 시스템에서 5회 실패 시 계정을 24시간 동안 잠그도록 설정했다. 이후 공격자가 여러 사용자 ID에 대해 일부러 5회씩 실패 로그인을 발생시켜 업무가 중단되었다. 이에 대한 개선책으로 가장 적절한 것은?
① 계정 잠금 정책을 완전히 제거한다.
② 비밀번호 길이를 4자리로 줄인다.
③ 위험 기반 지연, 단계적 제한, CAPTCHA 또는 추가 인증, 출발지 평판, 관리자 알림을 조합한다.
④ 실패 로그를 남기지 않는다.

10. NAT에 대한 설명으로 가장 적절한 것은?
① NAT는 주소 변환 기능이며, 접근 제어, 침입 탐지, 인증을 대체하지 못한다.
② NAT만 적용하면 내부망의 모든 보안 위협이 제거된다.
③ NAT는 암호화 프로토콜이다.
④ NAT를 사용하면 악성코드의 외부 통신이 원천적으로 불가능하다.

11. DES/3DES에 대한 설명으로 가장 적절하지 않은 것은?
① 3DES는 DES의 동일한 암호키를 3번 반복(암호키-암호키-암호키)한다.
② 라운드(Round)라는 암호화의 한 단계를 16회 반복한다.
③ 기본구조는 페이스텔 네트워크(Feistel Network) 또는 페이스텔 암호(Feistel Cipher)라고 한다.
④ 규격상으로 DES의 키는 총 64비트이지만 각 바이트의 마지막 1비트씩 총 8비트가 패리티비트로 사용되어 실제 암호화에 쓰이는 키 길이는 56비트이다.

12. 원격 근무자가 기관 내부 시스템에 접속하기 위해 VPN을 사용한다. 이에 대한 설명으로 가장 적절한 것은?
① VPN은 원격 단말의 악성코드 감염 여부와 무관하게 모든 접근을 신뢰하게 만든다.
② VPN은 방화벽 정책과 동시에 사용할 수 없다.
③ VPN을 쓰면 계정 탈취 위험은 사라진다.
④ VPN은 통신 구간 보호와 내부 접근 경로 제공에 도움을 주지만, 사용자 인증·단말 상태 점검, 접근 권한 통제와 함께 운영해야 한다.

13. 침해 사고 조사에서 서버 로컬 로그가 삭제되어 원인 분석이 어렵다. 향후 재발 방지를 위한 방안으로 가장 적절한 것은?
① 로그를 남기지 않도록 설정한다.
② 중앙 로그 서버 또는 SIEM으로 전송하고, 시간 동기화와 접근 통제를 적용한다.
③ 관리자 계정으로 누구나 로그를 수정할 수 있게 한다.
④ 로그 저장 기간을 1시간으로 줄인다.

14. IPv4 주소를 CIDR 방식으로 211.222.100.150/26인 단말기가 속한 서브 네트워크의 브로드캐스트 IP로 가장 적절한 것은?
① 211.222.100.128
② 211.222.100.223
③ 211.222.100.191
④ 211.222.100.255

15. IPv6에서 지원하는 주소 종류로 가장 적절하지 않은 것은?
① Unicast
② Anycast
③ Broadcast
④ Multicast

16. 침입차단 시스템에 대한 설명으로 가장 적절하지 않은 것은?
① DMZ 네트워크 구성에서 외부 침입차단 시스템은 인터넷이나 다른 WAN으로 연결되는 경계 라우터의 바로 안쪽 로컬 네트워크나 엔터프라이즈 네트워크 끝에 위치한다.
② IPSec을 침입차단 시스템 내부에서 구현할 때 침입차단 시스템은 양방향에서 암호화된 VPN 트래픽에 대해서 필터링 기능이나 접근통제, 로깅, 바이러스 스캐닝과 같은 보안기능을 수행할 수 있다.
③ VPN에서는 안전하지 않는 다른 네크워크인 인터넷을 통한 안전한 연결을 위해 하위 프로토콜 계층에서 암호와 인증을 사용한다.
④ 외부 공격으로부터 서버등을 보호해야 하기 때문에 DMZ 네트워크 구성에서 내부 침입차단 시스템은 외부 차단 시스템보다 더 엄격한 필터링 능력을 갖고 있다.

17. 다음은 Ping 명령의 실행 결과이다. 이에 대한 설명으로 가장 적절하지 않은 것은?

```
Ping www.google.com [142.251.157.119] 32바이트 데이터 사용:
142.251.157.119의 응답: 바이트=32 시간=39ms TTL=114
142.251.157.119의 응답: 바이트=32 시간=39ms TTL=114
142.251.157.119의 응답: 바이트=32 시간=42ms TTL=114
142.251.157.119의 응답: 바이트=32 시간=39ms TTL=114
142.251.157.119의 응답: 바이트=32 시간=40ms TTL=114

142.251.157.119에 대한 Ping 통계:
    패킷: 보냄 = 5, 받음 = 5, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 39ms, 최대 = 42ms, 평균 = 39ms
```

① 명령 프롬프트에서 'ping - t 5 www.google.com' 실행하면 된다.
② IP 패킷의 유효기간이 114이며 메시지가 5개 반복된 것은 테스트를 5회 했음을 나타낸다.
③ 서버의 FQDN(Fully Qualified Domain Name)인 www.google.com과의 사이에서 응답 테스트용 메시지를 송수신했음을 나타낸다.
④ IPv4주소 142.251.157.119로부터 응답이 있고 데이터의 크기는 32바이트, ping 테스트의 송신부터 수신까지 패킷 손실은 없음을 나타낸다.

18. 2.4GHz 대역과 5GHz 대역 2개의 채널을 지원하며, 최대 600Mbps까지의 속도까지 지원하는 무선랜 표준에 대한 설명으로 가장 적절한 것은?
① 802.11a
② 802.11b
③ 802.11g
④ 802.11n

19. 기관 내부 사용자가 정상 도메인을 입력했는데 악성 사이트로 이동했다. 내부 DNS 캐시가 오염되었을 가능성이 있다. 이에 대한 대응으로 가장 적절한 것은?
① DNS는 UDP를 사용하므로 보안 검토 대상이 아니다.
② DNSSEC 검증, 신뢰 가능한 재귀 DNS 사용, 캐시 무결성 점검, 의심 레코드 삭제 및 로그 분석을 수행한다.
③ 사용자 브라우저 캐시만 삭제하면 충분하다.
④ TLS 인증서 검증은 DNS와 무관하므로 확인할 필요가 없다.

20. 사용자가 공공기관 사이트 접속 중 브라우저에서 "인증서 이름이 사이트 주소와 일치하지 않음" 경고를 보았다. 이에 대한 보안 판단으로 가장 적절한 것은?
① 암호화는 적용되므로 경고를 무시해도 된다.
② 서버 인증서의 주체 이름 또는 SAN(Subject Alternative Name)과 접속 도메인이 맞지 않아 서버 인증이 실패한 상황일 수 있으며, 중간자 공격 가능성도 고려해야 한다.
③ HTTPS는 인증서 검증을 수행하지 않는다.
④ 인증서 경고는 네트워크 속도 문제만 의미한다.

21. 내부 업무 시스템에서 일반 사용자가 다음 URL의 숫자만 바꾸어 다른 부서 문서를 조회할 수 있었다. 개발팀은 “로그인한 사용자만 접근 가능하므로 인증 문제는 없다”고 주장한다. 판단으로 가장 적절한 것은?

- https://intra.example/doc/1001 - https://intra.example/doc/1002

① 인증이 성공했으므로 보안 취약점이 아니다.
② TLS가 적용되어 있으면 문서 번호 변경 공격은 방지된다.
③ 인증과 인가는 다르며, 객체 단위 권한 검증이 서버 측에서 수행되지 않은 접근제어 실패로 보아야 한다.
④ URL을 복잡하게 만들면 서버 측 권한 검사는 생략할 수 있다.

22. 악성코드와 그에 대한 설명으로 가장 적절하지 않은 것은?
① 웜 : 사용자 컴퓨터에 침입하여 파일을 암호화하고 해제를 위해 대가를 요구하는 프로그램
② 바이러스 : 사용자 컴퓨터에 몰래 실행 가능한 부분을 변형하고 복제하는 프로그램
③ 트로이 목마 : 트로이 목마가 직접 컴퓨터에 영향을 주기보다는 악의적인 공격자가 해당 프로그램을 이용하여 사용자의 컴퓨터를 조종할 수 있는 방식
④ 악성 자바 코드 : 웹 사이트의 동적 구현을 위한 자바 애플릿이 악의적인 기능으로 동작하도록 만든 코드

23. Ping Of Death 공격에 대한 설명으로 가장 적절하지 않은 것은?
① 네트워크 연결 상태를 점검하기 위한 Ping 명령을 이용한 공격방법이다.
② 수신자는 대량의 패킷을 한꺼번에 받게 되어 네트워크가 마비된다.
③ Ping 명령과 함께 가능한 긴 패킷을 같이 보내는 방법이다.
④ 누락된 패킷에 대해서는 계속적으로 재전송을 요구한다.

24. AES의 운영 모드에 대한 설명으로 가장 적절하지 않은 것은?
① OFB 모드는 블록을 암호화할 때마다 1씩 증가하는 카운터를 암호화 한 후에 XOR 연산으로 암호문을 만들며 암호화와 복호화가 동일하며 병렬로 처리할 수 있다.
② CBC 모드는 블록 운영 모드 중 보안성이 우수하며 블록 단위로 동작하므로 평문과 암호문의 길이가 다르다. 각 블록은 이전 암호문과 XOR 연산 후 암호화되며 첫 번째 암호문을 위해 IV가 필요하다.
③ CFB 모드는 스트림 암호처럼 동작하며 평문과 암호문의 길이가 같고 최초의 키 생성 버퍼로 IV가 필요하다. 암호화는 순차적으로 처리하지만 복호화는 병렬로 처리할 수 있다.
④ ECB 모드는 블록 단위로 순차적으로 암호화하는 가장 단순한 모드이며 블록 단위로 동작하기 때문에 평문과 암호문의 길이가 다르다. 각 블록이 독립적으로 동작하므로 한 블록에서 에러가 발생해도 다른 블록에 영향을 주지 않는다. 다만, 하나의 블록만 해독하면 나머지 블록도 해독되는 단점이 있다.

25. 관리자가 다음 순서로 방화벽 규칙을 적용했다. 장비는 위에서 아래로 첫 번째 일치 규칙을 적용한다. 203.0.113.5에서 서버 SSH 접속을 시도할 때 결과와 개선책으로 가장 적절한 것은?

- allow tcp any any -> server 22 - deny tcp 203.0.113.0/24 any -> server 22 - allow tcp 10.10.0.0/16 any -> server 22 - 기본 정책 deny

① 1번 규칙에 먼저 일치하여 허용되므로, 차단 또는 세부 허용 규칙을 더 위에 두고 광범위 허용 규칙을 제거해야 한다.
② 2번 규칙에 의해 차단되며 개선이 필요없다.
③ 기본 정책 deny에 의해 차단된다.
④ 3번 규칙 때문에 허용된다.