네 트 워 크 보 안 (7 급)

(과목코드 : 142)

2026년 군무원 채용시험　　　　응시번호 :　　　　　　　성명 :

1. 다음에서 설명하는 공격 기법을 이용하는 공격으로 가장 적절하지 않은 것은?

공격 대상이 되는 서버, 시스템, 네트워크의 자원을 고갈시켜 정상적인 사용자가 서비스를 이용하지 못하도록 방해하는 공격 기법

① SYN Flooding
② UDP Flooding
③ ARP Spoofing
④ Ping of Death

2. 디지털 서명이 제공하는 보안 속성으로 가장 적절하지 않은 것은?
① 메시지 무결성
② 송신자 인증
③ 부인 방지
④ 메시지 기밀성

3. TCP 세션 하이재킹 탐지 사항에 대한 설명으로 가장 적절하지 않은 것은?
① 예상치 못한 접속의 리셋은 TCP 세션 하이재킹의 징후이다.
② 동기화 상태 탐지는 TCP 세션 하이재킹의 징후이다.
③ ACK Storm은 TCP 세션 하이재킹의 징후이다.
④ 패킷의 유실과 재전송 증가는 TCP 세션 하이재킹의 징후이다.

4. X.509 인증서에 대한 설명으로 가장 적절하지 않은 것은?
① 주체 유일 식별자(Subject Unique Identifier)는 비트열 필드로 필수적이며 주체를 유일하게 구별하는데 사용한다.
② 일련번호(Serial Number)는 다른 인증서와 혼동되지 않도록 인증서와 연관된 정수값으로 한 CA가 발행한 인증서 일련번호는 유일하다.
③ 각 CA 디렉토리에 존재하는 인증서는 순방향 인증서와 역방향 인증서로 구성된다.
④ CA가 발행한 사용자 인증서는 어느 사용자도 들키지 않게 인증서를 변경할 수 없다.

5. DOS 공격 및 DRDOS 공격에 대한 설명으로 가장 적절하지 않은 것은?
① 7계층(애플리케이션 계층) DOS 공격에는 대역폭 고갈 공격, 세션 고갈 공격, 서버의 자원 고갈 공격 등이 있다.
② 라우터나 방화벽에서 출발 IP, 목적 IP가 동일시되면 탐지하여 차단되는 공격은 Land Attack이다.
③ Smurf 공격은 ICMP 패킷을 사용하여 출발지 IP를 피해자 주소로 위조하여 브로드캐스트 주소로 전송하여 과부하를 일으키는 공격이다.
④ Fraggle 공격은 UDP를 이용하여 출발지 IP를 위조하고 브로드캐스트 주소로 전송하는 공격이다.

6. TCP 연결에서 RST 플래그가 비정상적으로 다량 관측될 경우, 합리적인 해석으로 가장 적절한 것은?
① 스니핑 공격 시도
② 버퍼 오버플로우 공격 시도
③ 혼잡 제어 실패로 인한 DDOS 공격
④ 포트 스캔 또는 세션 하이재킹 시도

7. 바이러스 및 악성 소프트웨어에 대한 설명으로 가장 적절하지 않은 것은?
① 은닉 전략을 활용하는 바이러스 유형 중 폴리모픽 바이러스(Polymorpic Virus)는 감염시킬 때마다 변형하는 바이러스이기 때문에 특징(Signature)을 이용한 탐지를 해야한다.
② 일반적으로 바이러스 활동기간은 잠복 단계, 확산 단계, 트리거 단계, 실행 단계로 구분할 수 있다.
③ 컴퓨터 바이러스는 감염 메커니즘, 트리거, 페이로드 등으로 구성된다.
④ 악성 소프트웨어 중 플러더(Flooders)는 네트워크 컴퓨터 시스템에 대량의 자료를 보내어 서비스 거부 공격을 하는데 사용한다.

8. NAC(Network Access Control)의 주요 기능으로 가장 적절한 것은?
① 네트워크에 접속하는 단말의 인증 및 보안 정책 준수 여부를 점검한 후 접근 권한을 동적으로 부여한다.
② 네트워크 구간에서 공개키 기반 암호화를 수행하여 종단 간 데이터 기밀성을 보장한다.
③ 네트워크 트래픽을 실시간으로 모니터링하여 알려진 공격 패턴이나 비정상 행위를 탐지한다.
④ 네트워크 내부의 브로드캐스트 도메인을 논리적으로 분리하여 트래픽 충돌을 감소시킨다.

9. 네트워크 보안 장비 로그와 Wireshark 트래픽을 함께 분석하던 중, 패킷은 정상적으로 캡처되었으나 비정상 행위 경고(Alert)만 발생했다. 이 장비의 역할로 가장 적절한 것은?
① 패킷 필터링 방화벽
② 침입 탐지 시스템
③ NAT 라우터
④ 프록시 서버

10. PBE(Password Based Encryption)에 대한 설명으로 가장 적절하지 않은 것은?
① 세션키는 각 통신마다 새로 생성한다.
② 암호화 3단계는 KEK 생성 → 세션키 생성과 암호화 → 메시지 → 암호화로 이루어진다.
③ 패스워드를 기초로 해서 만든 키로 암호화를 수행하는 방법으로 암호화와 복호화 양쪽에서 서로 다른 패스워드가 필요하다.
④ Salt는 의사난수 생성기로 만들어지는 랜덤한 값으로 KEK를 만들때에 패스워드와 함께 일방향 해시 함수에 입력된다.

11. 3계층(네트워크 계층)에서 동작하는 보안 장비 또는 기술들로 가장 적절한 것은?
① NAT, TLS, WAF
② 패킷 필터링 방화벽, IPSec, NAT
③ WAF, TLS, 패킷 필터링 방화벽
④ 프록시 방화벽, HTTP 필터링, NAT

12. TLS에 대한 설명으로 가장 적절한 것은?
① 2계층에서 동작하는 보안 프로토콜이다.
② UDP 연결에서만 사용된다.
③ TCP 연결 위에서 종단 간 보안을 제공한다.
④ 방화벽의 내부 정책을 정의한다.

13. XSS 공격의 주된 위험성으로 가장 적절한 것은?
① 서버 메모리를 초과 사용하게 만든다.
② 서버의 파일 권한을 직접 변경한다.
③ 네트워크 라우팅 정보를 변경한다.
④ 사용자의 브라우저에서 악성 스크립트를 실행한다.

14. 한 기업의 내부 네트워크에서 다음과 같은 이상 징후가 발견되었다. 이 상황에서 발생한 ARP Spoofing 공격의 결과로 가장 적절한 것은?

- 직원 PC와 서버 간 통신이 정상적으로 이루어지는 것처럼 보임
- 동시에, 특정 내부 PC에서 ARP 테이블이 비정상적으로 변경됨
- 이후 사내 웹 시스템 로그인 계정이 외부에서 악용된 정황이 확인됨

① 인증 정보 탈취
② 패킷 분실
③ 암호화 키 생성
④ 포트 스캔

15. 다수의 사용자 계정에서 몇 가지 흔한 비밀번호를 사용하여 공격하는 방식으로 가장 적절한 것은?
① Brute Force Attack
② Rainbow Table Attack
③ Password Spraying
④ Shoulder Surfing

16. 스니핑 공격에 대한 설명으로 가장 적절하지 않은 것은?

① ARP 리다이렉트는 2계층에서 MAC 주소를 속여 패킷의 흐름을 바꾸는 공격 방법이다.

② 포트미러링은 데이터를 해당 포트에 똑같이 보내는 방법으로 브로드캐스트와 같은 방식으로 전송한다.

③ ICMP 리다이렉트는 네트워크 계층에서 스니핑 시스템이 네트워크에 존재하는 또 다른 라우터라고 알려 패킷의 흐름을 바꾸는 공격이다.

④ 스위치 재밍은 MAC 테이블을 위한 캐시 공간에 버퍼 오버플로우 공격으로 시스템이 오작동하는 것을 의미한다.

17. IP 주소 체계에 대한 설명으로 가장 적절하지 않은 것은?

① IPv4의 사설 주소 대역은 공인 네트워크에서 직접 라우팅되지 않으며 일반적으로 NAT와 함께 사용된다.

② IPv6의 루프백(Loopback) 주소는 ::1이다.

③ IPv6는 주소 공간 확장과 헤더 구조 단순화를 통해 라우터의 패킷 처리 효율 향상을 고려하여 설계되었다.

④ IPv4와 IPv6 모두 네트워크 계층에서 브로드캐스트 주소를 이용하여 모든 호스트에 패킷을 전달한다.

18. SSH(Secure Shell)에 대한 설명으로 가장 적절하지 않은 것은?

① TCP 상에서 수행되는 사용자 인증 프로토콜, 연결 프로토콜 등으로 구성한다.

② 패킷 교환 형식 중 메시지 인증 코드는 메시지 인증 협상이 완료되면 각 패킷마다 MAC 값이 생성되어 포함된다.

③ 호스트 키 관리는 2가지 신뢰 모델을 제시하고 있는데 그중 하나는 클라이언트가 각 호스트 이름과 대응되는 호스트 공개키를 짝지어 주는 로컬 데이터베이스를 갖는 것이다.

④ SSH 연결 프로토콜은 기밀성, 무결성을 제공하고 옵션으로 압축을 제공한다.

19. 디지털 포렌식의 수행 절차와 그에 대한 설명으로 가장 적절하지 않은 것은?

① 수사 준비 : 장비와 툴을 확보하고 적정한 법적 절차를 걸쳐 피의자 또는 수사 대상에 접근한다.

② 증거 수집 : 증거물을 획득할 때는 증거물을 획득한 사람, 감독한 사람, 그리고 이를 인증해 주는 사람이 필요하다.

③ 분석 및 조사 : 증거를 분석할 때는 항상 원본을 이용하여 분석하고 변형되었다면 해당 내용을 기록하고 다시 보관한다.

④ 보고서 작성 : 증거 데이터, 분석 및 조사 과정에 관련된 정보, 수행 결과 등을 보고서로 작성하여 제출한다.

20. 다음 C 코드에서 발생 가능한 보안 취약점으로 가장 적절한 것은?

```
#include <stdio.h>

int main(int argc, char *argv[]) {
printf(argv[1]);
return 0;
}
```

① 버퍼 오버플로우 공격

② 포맷 스트링 공격

③ 레이스 컨디션

④ 스택 언더플로우

21. IDS에 대한 설명으로 가장 적절하지 않은 것은?

① 침입자의 행동을 좁게 잡으면 침입자를 합법적 사용자로 판단하게 되는 긍정 오류(False Positive)를 유발하게 된다.

② 규칙 기반 탐지(Rule Based Detection) 중 침투 식별(Penetration Identification)은 의심스러운 행동을 찾아내는 규칙으로 전문가 시스템을 활용한다.

③ 침입 탐지를 위한 감사 기록(Audit Record)에는 기본(Native) 감사 기록과 탐지 전용(Detection-specific) 감사 기록으로 구분할 수 있다.

④ 침입 탐지의 통계적 변형 탐지(Statistical Anomaly Detection) 중 임계값 탐지(Threshold Detection)는 사용자와 무관하게 다양한 사건의 발생 빈도에 대한 임계값을 정의한다.

22. 다음 보안관제 시스템 현상에 대한 분석으로 가장 적절한 것은?

- 사내 여러 PC가 주기적으로 특정 외부 서버와 암호화된 세션을 유지하고 있다.
- 해당 PC들은 평상시 정상 동작을 수행하지만 특정 시점에 동시에 대량의 외부 트래픽을 발생시킨다.
- 일부 시스템에서는 사용자 모르게 스팸 메일 발송 및 비정상 DNS 질의가 확인되었다.
- 감염된 시스템을 포맷하더라도 동일 네트워크 내 다른 호스트를 통해 재감염되는 사례가 반복되었다.

① 감염된 시스템들은 스파이웨어에 감염된 상태이며 개인정보를 수집하는 것으로 볼 수 있다.
② 공격자는 감염된 호스트들을 봇으로 구성하여 C&C 기반의 봇넷 형태로 제어하고 있을 가능성이 높다.
③ 해당 공격은 운영체제 취약점을 악용하여 관리자 권한 획득 및 지속성 확보를 목적으로 하는 루트킷 유형으로 판단할 수 있다.
④ DNS 질의가 발생하였으므로 DNS 캐시 포이즈닝 공격으로 판단하는 것이 가장 타당하다.

23. IEEE 802.11i 표준버전을 RSN(Robust Security Network)이라고 한다. 이에 대한 설명으로 가장 적절하지 않은 것은?
① 인증 및 키생성 서비스에는 확장 가능 인증프로토콜 (Extensible Authentication Protocol, EAP)을 활용한다.
② 동작 단계는 탐색 → 키관리 → 인증 → 안전 데이터 전송 → 연결 중단 순으로 진행된다.
③ MAC 계층의 데이터와 데이터가 바뀌지 않음을 확인할 수 있는 메시지 무결성 코드를 함께 암호화한다.
④ 기밀성을 지원하기 위해 TKIP, AES-CCMP 알고리즘을 활용한다.

24. Side-channel Attack에 대한 설명으로 가장 적절한 것은?
① 암호화 알고리즘의 수학적 취약점을 이용하여 키를 복원한다.
② 버퍼 오버플로우와 같은 소프트웨어 버그를 이용하여 실행 흐름을 변조한다.
③ 암호화 모듈이 동작할 때 발생하는 전력 소비, 전자기파, 처리 시간 등 물리적 정보를 분석하여 비밀 정보를 추출한다.
④ 네트워크 패킷의 메타데이터를 분석하여 암호화 키를 복원한다.

25. 암호화 알고리즘의 안전성 평가 기준인 키 길이(Key Length)와 보안 강도(Security Strength) 관계에 대한 설명으로 가장 적절한 것은?
① 해시 함수 SHA-256의 충돌 저항성 보안 강도는 256비트이다.
② 2중 DES는 키의 길이가 2배 확장된 효과를 얻을 수 있다.
③ 대칭키 128비트의 보안 강도는 RSA 3072비트와 유사한 수준이다.
④ ECC 256비트의 보안 강도는 RSA 256비트보다 낮다.