

정 보 보 호 론 (7 급)

(과목코드 : 141)

2025년 군무원 채용시험

응시번호 :

성명 :

1. 정적 분석에 대한 설명으로 적절하지 않은 것은?

- ① 악성코드를 실행하지 않고 실행 파일 분석만으로 악성 행위를 검증한다.
- ② 실행 프로그램 파일에서 소스를 역추출하는 방법을 디스어셈블 또는 리버싱이라고 한다.
- ③ PE 포맷 파일에서 어셈블리어를 추출하는 도구로는 GMER와 IceSword 등이 있다.
- ④ 소스 분석 및 단순 문자열 찾기를 이용한 정적 분석 방법을 회피하고자 악성코드는 보통 패킹 또는 난독화 기법을 사용한다.

2. 무선 네트워크 통신 방식과 그에 대한 예시로 가장 적절하지 않은 것은?

- ① WLAN(Wireless Local Area Network)
: 지그비(ZigBee)
- ② WPAN(Wireless Personal Area Network)
: 블루투스(Bluetooth)
- ③ WMAN(Wireless Metropolitan Area Network)
: 와이맥스(WiMax)
- ④ WWAN(Wireless Wide Area Network)
: 셀룰러 네트워크

3. 모바일 기기 보안의 블루스나프에 대한 설명으로 가장 적절한 것은?

- ① 블루투스 공격 장치의 검색 활동을 의미한다.
- ② 블루투스 장비 간의 취약한 연결 관리를 악용한 공격이다.
- ③ 블루투스의 취약점을 이용하여 스팸 메시지를 익명으로 퍼뜨리는 공격이다.
- ④ 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다.

4. 해시함수에 대한 설명으로 가장 적절하지 않은 것은?

- ① 해시함수는 메시지의 무결성과 기밀성을 위해 사용한다.
- ② 해시함수가 만들어내는 결과값에서 역으로 입력 메시지를 계산해내는 것은 불가능하다.
- ③ 서로 다른 입력 메시지에 대해서는 서로 다른 해시 결과값이 계산되어야 한다.
- ④ 해시의 종류에는 Tiger-160, RIPEMD-320, Blake3 등이 있다.

5. 침해 사고에서 위험 2등급 상황으로 가장 적절하지 않은 것은?

- ① 비인가자에 의해 관리자 명령이 실행되고 있다.
- ② 일반적이지 않은 숨김 파일 또는 디렉터리가 존재한다.
- ③ 외부 또는 내부에서 불법적인 접근 시도가 계속 발견된다.
- ④ 시스템 담당자가 알지 못하는 사용자가 추가되거나 사용자 권한이 임의로 변경된다.

6. 모바일 보안 위협 유형 중 플랫폼 공격으로 가장 적절하지 않은 것은?

- ① 바이러스/웜 ② DoS 공격
- ③ 시스템 언룩 ④ 키보드 해킹

7. 규칙기반 접근제어에 대한 설명으로 가장 적절한 것은?

- ① 기존에 네트워크 관리자에 의해 설정된 접근 제어 목록에 의해 결정된다.
- ② 기업 내 개인의 잦은 이동 및 기관의 특성에 밀접하게 적용하기에 적합하다.
- ③ 객체에 대한 소유권을 가진 주체가 객체에 대한 권한을 다른 주체에게 부여한다.
- ④ 모든 사용자와 데이터에 보안 등급을 부여하고 부여된 등급을 비교함으로써 접근의 허용 여부를 판단한다.

8. 동작에 의한 악성코드 분류에서 PUP(Potentially Unwanted Program)에 대한 설명으로 가장 적절하지 않은 것은?

- ① 프로그램 설치 시 사용자에게 직·간접적인 동의를 구하지만 용도를 파악하기 어렵게 한다.
- ② 스파이웨어나 광고가 포함된 악성코드 제거 프로그램, 웹 사이트 바로가기 생성 프로그램 등이 있다.
- ③ 불필요한 프로그램으로 사용자에게 치명적인 피해를 주지는 않지만 불편함을 주는 악성코드다.
- ④ 윈도우 또는 응용 프로그램의 취약점을 이용하거나 이메일 또는 공유 폴더를 통해 전파되며 최근에는 공유 프로그램을 통해 전파되기도 한다.

9. 다음 데이터베이스의 권한 관리에 대한 설명에서 (가), (나)에 들어갈 명령어로 가장 적절한 것은?

- (가)은(는) 사용자에게 해당 권한을 금지한다.
- (나)은(는) 데이터베이스 객체를 삭제한다.

- ① 가: DROP 나: DENY
- ② 가: DENY 나: DROP
- ③ 가: DELETE 나: REVOKE
- ④ 가: REVOKE 나: DELETE

10. 다음에서 설명하는 용어로 가장 적절한 것은?

- 파일 자체에 대해서 암호화 또는 복호화를 수행하여 적절한 인증을 받지 못한 사용자가 해당 문서를 열어보지 못하게 함
- 만약 파일이 외부로 유출된다 하더라도 암호화되어 있기 때문에 열어볼 수 없음
- 허가받지 않은 사용자가 중요 정보가 저장된 문서에 접근하여 사용하는 것을 차단하여 내부 시스템의 데이터를 보호하고 데이터 유출을 방지
- 사용자별 또는 프로세스별 권한 관리 기능을 제공하여 문서를 작성한 사람의 직책이나 직급에 따라서 문서의 열람 권한을 달리하게 만들 수 있음

- ① IPS(Intrusion Prevention System)
- ② DLP(Data Loss Prevention)
- ③ DRM(Digital Rights Management)
- ④ NAC(Network Access Control)

11. HTTP 메소드에 대한 설명으로 가장 적절하지 않은 것은?

- ① GET: 클라이언트가 보낸 요청을 그대로 반환
- ② POST: 요청 바디를 통해 클라이언트가 서버로 데이터 전송
- ③ HEAD: 서버가 헤더만 전송해줄 것을 요청
- ④ OPTIONS: 서버가 지원하는 메소드를 질의

12. 다음 설명에 해당되는 블록 암호 모드는?

- 암호화와 복호화 시 병렬 처리가 가능
- 암호문 블록의 삭제 혹은 교체에 의해 평문 변조가 가능
- 보안상 취약하여 사용을 권장하지 않음

- ① GCM 모드 ② ECB 모드
- ③ CTR 모드 ④ CBC 모드

13. 지문이나 패스워드 등을 통해 로그인이 허락된 사용자로 판명되어 업무 권한을 부여하는 것은?

- ① 허가(Permission) ② 인가(Authorization)
③ 장부(Accounting) ④ 인증(Authentication)

14. 다음 설명하는 암호화 방식으로 가장 적절한 것은?

- 전자정부 구현 등에 따라 다양한 환경에 적합한 암호화 알고리즘이 필요하여 국가보안기술연구소 주도로 학계, 국가정보원 등의 암호 전문가들이 개발하였다.
- 2004년 국가표준기본법에 의거하여 국가표준으로 지정되었다.

- ① ARIA 알고리즘 ② IDEA 알고리즘
③ SEED 알고리즘 ④ 양자 암호 알고리즘

15. 「전자정부법」에 대한 설명에서 (가), (나)에 들어갈 기간으로 가장 적절한 것은?

- 행정정보를 위조·변경·훼손하거나 말소하는 행위를 한 사람은 (가)년 이하의 징역에 처한다.
- 행정정보 공동 이용을 위한 정보 시스템을 정당한 이유 없이 위조·변경·훼손하거나 이용한 자는 (나)년 이하의 징역 또는 5천만 원 이하의 벌금에 처한다.

- ① 가: 5 나: 2 ② 가: 7 나: 3
③ 가: 10 나: 5 ④ 가: 15 나: 10

16. 다음 설명하는 용어로 가장 적절한 것은?

- 인터넷상의 최초의 웜으로 1988년 코넬 대학에서 박사 과정생이 배포하였다.
- 유닉스 운영체제가 가지고 있던 버퍼 오버플로 보안 취약점을 이용하여 전파되도록 구현하였다.
- 컴퓨터와 인터넷으로 연결된 다른 컴퓨터에 보안 취약점을 이용하여 전파시켰다.
- 당시 인터넷에 접속된 6만 대의 컴퓨터 중 약 10%의 컴퓨터를 감염시켰다.

- ① 러브레터 웜 ② 모리스 웜
③ 님다 웜 ④ 슬래머 웜

17. 디지털 포렌식에서 사실인정의 기초가 되는 사실이나 실험한 것을 진술서나 진술 기재서를 통해 보고하는 증거로 가장 적절한 것은?

- ① 물적 증거 ② 인적 증거
③ 직접 증거 ④ 간접 증거

18. 사용자 인증 유형 중 행위 기반 인증으로 가장 적절하지 않은 것은?

- ① 서명 ② 움직임
③ 패스워드 ④ 음성

19. 보안 공격 대상이 되는 IoT 환경과 예시로 가장 적절하지 않은 것은?

- ① 중계 기능: 디지털 도어락, 스마트 조명
② 센싱 기능: 스마트 온도계, 무선 감지기
③ 촬영 기능: 홈 캠, 네트워크 카메라
④ 운용 기능: 스마트 세탁기, 시스템 에어컨

20. 다음 설명하는 용어로 가장 적절한 것은?

- 인터넷 뱅킹 등 전자 금융 거래를 이용할 때 무작위로 비밀번호를 생성하는 매체이다.
- 패스워드 가로채기나 어깨너머 훑쳐보기 등에 대처가 가능하며 높은 보안성이 장점이다.
- 매체를 공유 혹은 분실했을 때 악용이 가능하며 매체 오류의 경우 인증이 실패할 수 있다.
- 시간 동기화 방식을 사용하는 경우 인증 서버와 매체의 시간이 같도록 동기화되어야 한다.

- ① 스마트카드
- ② 전자지갑
- ③ 핀(PIN)
- ④ 일회용 패스워드(One-Time Password)

21. 공개키 암호에 대한 설명으로 가장 적절하지 않은 것은?

- ① 암호화 키와 복호화 키가 동일하지 않다.
- ② 암호화 속도가 느리다.
- ③ 안전한 키 교환을 위해 사용한다.
- ④ RSA 알고리즘의 안전한 키 길이는 128 bit이다.

22. 다음 빈칸에 들어갈 용어로 가장 적절한 것은?

()은(는) 불특정 다수를 대상으로 로그인된 사용자가 자신의 의지와 무관하게 공격자가 의도한 행위를 하게 만드는 공격이다.

- ① XSS
- ② CSRF
- ③ 공격 방어 취약점
- ④ 세션 관리 취약점

23. 다음 디지털 포렌식의 원칙으로 가장 적절한 것은?

- 동일한 조건과 동일한 상황이라면 디지털 포렌식의 분석 결과는 항상 같은 결과가 나와야 함
- A분석관이 EnCase라는 포렌식 도구로 얻은 분석 결과는 B분석관이 FTK라는 포렌식 도구로 얻은 분석 결과와 같아야 함
- 현장에서는 이러한 원칙을 지키기 위해 주요 분석 결과에 대해 다른 분석관이 다른 도구로 분석하여 서로 교차분석(Cross-Analysis)을 수행하기도 함
- 만약 불법 해킹 용의자의 해킹툴이 증거 능력을 가지기 위해서는 같은 상황의 피해 시스템에 툴을 적용할 경우 피해 결과와 일치하는 결과가 나와야 함

- ① 무결성의 원칙 ② 연계보관성의 원칙
- ③ 신속성의 원칙 ④ 재현의 원칙

24. 유닉스/리눅스에서 chargen, daytime, discard, echo가 가진 보안 위협에 대한 설명으로 가장 적절한 것은?

- ① 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있음
- ② 보안공격자가 데몬에 원격 명령을 실행시킬 수 있음
- ③ 네트워크 관련 서비스로 서비스 거부 공격에 취약함
- ④ 인증 없이 관리자의 원격 접속을 가능하게 함

25. 정보보안과 관련된 국내 법률 중 공공 부문과 민간 부문 모두에 적용되는 법은?

- ① 개인정보보호법
- ② 정보통신망법
- ③ 신용정보보호법
- ④ 전자금융거래법