※ 답안지에 한 번 표기한 답을 수정테이프 등으로 정정하거나 칼 등으로 긁어 변형할 경우 그 문항은 무효로 처리함.

1. 다음 지문에서 설명하는 기술과 바르게 짝지은 것은?

(가) 디지털콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.
(나) 원본의 내용을 왜곡하지 않는 범위 내에서 사용자가 인식하지 못하도록 저작권 정보를 디지털콘텐츠에 삽입하는 기술이다.
(다) 공격자가 공격전에 공격대상에 대한 다양한 정보를 수집하는 기술이다.

① (가) 워터마킹 (나) 핑거프린팅 (다) 워터링 홀
② (가) 핑거프린팅 (나) 워터링 홀 (다) 풋프린팅
③ (가) 풋프린팅 (나) 워터마킹 (다) 핑거프린팅
④ (가) 핑거프린팅 (나) 워터마킹 (다) 풋프린팅

2. 암호학적 해시함수(Cryptographic Hash Function)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?
① 어떤 입력 x 에 대해 h(x) 를 계산하기 어려워야 한다.
② 주어진 값 y 에 대해 h(x)=y 의 x 값을 찾는 계산이 어려워야 한다.
③ 생일역설(Birthday Paradox)은 충돌 저항성 공격(Collision Resistance Attack)과 관련한 수학적 분석 결과이다.
④ 입력 길이에 상관없이 고정된 길이를 출력한다.

3. MD5(Message Digest 5)는 널리 쓰는 해시함수이며, 최종적으로 ( )비트의 해시코드를 출력한다. ( ) 안에 들어갈 적합한 숫자는 무엇인가?
① 64 ② 128 ③ 256 ④ 512

4. 공개키 암호 시스템을 이용하여 Alice가 Bob에게 암호문을 전달하고 이를 복호화하는 과정에 관한 다음 설명 중 ( ) 안에 들어갈 내용으로 바르게 짝지은 것은 무엇인가?

1. Bob은 개인키와 공개키로 이루어진 한 쌍의 키를 생성한다.
2. Bob은 (가)를 Alice에게 전송한다.
3. Alice는 (나)를 사용하여 메시지를 암호화한다.
4. Alice는 생성된 암호문을 Bob에게 전송한다.
5. Bob은 (다)를 사용하여 암호문을 복호화한다.

① (가) Bob의 공개키 (나) Alice의 공개키 (다) Alice의 개인키
② (가) Bob의 개인키 (나) Bob의 공개키 (다) Bob의 개인키
③ (가) Bob의 개인키 (나) Alice의 공개키 (다) Alice의 개인키
④ (가) Bob의 공개키 (나) Bob의 공개키 (다) Bob의 개인키

5. 임의적 접근통제(DAC : Discretionary Access Control)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?
① 객체(데이터)의 소유주에 의하여 접근권한 변경이 가능하다.
② 일반적으로 ACL(Access Control List)을 통해서 이루어진다.
③ 민감도 레이블(Sensitivity Label)에 따라 접근을 허용할 지 결정한다.
④ ID기반 접근통제이다.

6. 대칭키와 공개키 암호화 방식에 관한 다음 설명 중 옳은 것은 모두 몇 개인가?

가. 일반적으로 안전한 키 길이는 대칭키 방식의 키가 공개키 방식의 키보다 길다.
나. 대칭키 방식의 암호화키와 복호화키는 동일하며, 모두 비밀이다.
다. 공개키 방식의 암호화키와 복호화키는 모두 공개이다.
라. 일반적으로 암호화 속도는 대칭키 방식이 공개키 방식보다 빠르다.
마. 대칭키 방식의 알고리즘에는 AES, SEED, ECC 등이 있다.

① 2개 ② 3개 ③ 4개 ④ 5개

7. 다음 지문에서 설명하는 접근통제모델은 무엇인가?

접근통제모델 중 효율적인 업무처리(Well-formed transactions)와 직무분리(Separation of duties) 두 가지 원칙을 통해 좀 더 정교하게 무결성을 보장하는 모델이다.

① 벨-라파듈라(Bell-LaPadula)
② 비바(Biba)
③ 테이크 그랜트(Take Grant)
④ 클락-윌슨(Clark-Wilson)

8. 생체인증기술의 정확도는 부정거부율(FRR : False Rejection Rate)과 부정허용율(FAR : False Acceptance Rate)로 측정할 수 있다. 생체인증기술의 정확도에 관한 다음 설명 중 옳은 것끼리 짝지은 것은 무엇인가?

가. 사용자 편의성을 요구하는 경우 FAR이 높아지고 FRR은 낮아진다.
나. 사용자 편의성을 요구하는 경우 FRR이 높아지고 FAR은 낮아진다.
다. 보안성을 강화할 경우 FRR은 높아지고 FAR은 낮아진다.
라. 보안성을 강화할 경우 FAR은 높아지고 FRR은 낮아진다.

① 가, 다 ② 가, 라 ③ 나, 다 ④ 나, 라

9. 다음 중 취약점 점검 도구가 아닌 것은 무엇인가?
① SARA ② NIKTO
③ TCP WRAPPER ④ NESSUS

10. 윈도우 파일 시스템 NTFS(New Technology File System)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?
① NTFS는 기본 NTFS 보안의 공유 보안과 동일하게 Everyone 그룹에 대해서는 모든 권한이 '허용'이다.
② 기본 NTFS 보안을 변경하면 사용자마다 서로 다른 NTFS 보안을 적용시킬 수 있다.
③ 파일과 폴더에 대한 보안강화 및 접근제어가 가능하다.
④ 저용량 볼륨에 최적화되어 있다.

11. 다음 중 윈도우 레지스트리 키가 아닌 것은 무엇인가?
① HKEY_CLASSES_ROOT
② HKEY_CURRENT_USER
③ HKEY_MACHINE_SAM
④ HKEY_USERS

12. 리눅스 시스템 로그(log) 파일 중 계정들의 로그인 및 로그아웃에 대한 정보를 가진 파일은 무엇인가?

① wtmp ② dmesg ③ xferlog ④ btmp

13. 리눅스 명령어에 관한 다음 설명 중 바르게 짝지은 것은 무엇인가?

(가) 파일과 디렉터리의 퍼미션(Permission) 변경
(나) 파일과 디렉터리의 소유권(Ownership) 변경
(다) 사용자 패스워드 변경
(라) 계정 생성

	(가)	(나)	(다)	(라)
①	umask	chown	passwd	netuser
②	chmod	chgroup	passwd	useradd
③	chmod	chown	passwd	useradd
④	umask	chown	chpwd	useradd

14. 사용자가 자신의 홈디렉터리 내에서 새롭게 생성되는 서브 파일의 디폴트 퍼미션을 파일 소유자에게는 읽기(r)와 쓰기(w), group과 other에게는 읽기(r)만 가능하도록 부여하고 싶다. 로그인 쉘에 정의해야 되는 umask의 설정 값으로 옳은 것은 무엇인가?

① umask 133 ② umask 644
③ umask 022 ④ umask 330

15. 정보보호 보안평가 표준 등에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① TCSEC은 보안등급을 A,B,C,D로 구분하며 네트워크를 고려하지 않은 시스템 보안평가 표준이다.
② ITSEC은 오렌지북으로 불리는 컴퓨터시스템 평가기준으로 미 국방부에서 최초로 수용되었다.
③ CC(Common Criteria)는 단일화된 공통 평가기준을 제정하여 적용함으로써 시간의 절약, 평가비용의 절감 등의 효과가 있다.
④ ISMS는 BS7799를 기반으로 국내 환경에 적합하게 작성하였다.

16. 서비스거부 공격(DoS: Denial of Service)의 유형 중 Smurf 공격에 관한 다음 설명 중 가장 옳은 것은 무엇인가?

① 출발지 IP주소를 존재하지 않는 IP주소로 변조한 후 다량의 SYN 패킷을 전송한다.
② 출발지와 목적지의 IP주소를 동일하게 공격대상의 IP주소로 위조하여 전송한다.
③ 출발지 IP주소를 공격대상 IP주소로 위조하여 ICMP 패킷을 브로드캐스트 주소로 전송한다.
④ ICMP PING 패킷을 비정상적으로 크게 만들어 전송한다.

17. 리눅스에서 파일 접근권한 중 setuid나 setgid가 설정되어 있으면 보안상 위험해 질 수 있다. setuid나 setgid가 설정되어 있는 파일을 찾는 명령이 아닌 것은 무엇인가?

① find / -perm -1000 -print
② find / -perm -2000 -print
③ find / -perm -4000 -print
④ find / -perm -6000 -print

18. 다음 지문에서 설명하는 프로토콜은 무엇인가?

가. TCP/IP 네트워크의 시스템이 동일 네트워크나 다른 시스템의 MAC 주소를 알고자 하는 경우에 사용한다.
나. IP 주소를 물리적인 하드웨어 주소인 MAC 주소로 변환하여 주는 프로토콜이다.

① TCP/IP ② ARP ③ RARP ④ SMTP

19. 방화벽(firewall)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 패킷 필터링(Packet Filtering) 방화벽은 특정 IP, 프로토콜, 포트의 차단 및 허용을 할 수 있다.
② 패킷 필터링(Packet Filtering) 방화벽은 바이러스에 감염된 파일 전송시 분석이 불가능하다.
③ 어플리케이션 게이트웨이(Application Gateway) 방화벽은 응용계층에서 동작하기 때문에 다른 방식의 방화벽에 비해 처리속도가 가장 빠르다.
④ 어플리케이션 게이트웨이(Application Gateway) 방화벽은 각 서비스별로 프록시 데몬이 존재한다.

20. 침입탐지방법에 관한 다음 설명 중 ( ) 안에 들어갈 내용으로 바르게 짝지은 것은 무엇인가?

오용탐지(Misuse)는 침입패턴 정보를 데이터베이스화하고, 사용자 혹은 침입자가 네트워크 및 호스트를 사용하는 활동 기록과 비교하여 동일하면 침입으로 식별하는 것이다. 이 방법은 False Positive가 (가)는 장점이 있지만 반대로 False Negative가 (나)는 단점이 있다.

① (가) 높다 (나) 낮다 ② (가) 낮다 (나) 높다
③ (가) 높다 (나) 높다 ④ (가) 낮다 (나) 낮다

21. 보안 취약점 점검 도구에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① netstat은 대부분의 운영체제에 기본으로 탑재된 도구이며 네트워크 상태를 확인하기 위해 사용한다.
② tcpdump는 네트워크 패킷 출력 도구로 특정 구간의 장비 사이에서 네트워크 통신이 되는지 확인하기 위해 사용한다.
③ nmap은 포트 스캔뿐만 아니라 대상 시스템의 운영체제나 네트워크 장치 정보 등을 수집할 수 있는 보안 스캐너이다.
④ WireShark는 네트워크 패킷 생성 및 재전송 도구로 네트워크 침해사고 분석 중 확보한 패킷 파일을 시뮬레이션하기 위해 사용한다.

22. 스위치 환경 하에서 나타나는 스니핑(Sniffing) 기법이 아닌 것은 무엇인가?

① Switch Jamming ② ARP Spoofing
③ ICMP Redirect ④ Session Hijacking

23. 다음 지문은 무엇에 관한 설명인가?

무선랜을 통하여 전송되는 패킷의 각 헤더에 덧붙여지는 32 바이트 길이의 고유 식별자로서, 무선장비가 BSS(Basic Service Set)에 접속할 때 암호처럼 사용한다.

① SSID(Service Set Identifier)
② WEP(Wired Equivalent Privacy)
③ MAC(Message Authentication Code)
④ RFID(Radio Frequency Identification)

24. IPSec 프로토콜에서 AH(Authentication Header) 프로토콜이 제공하는 보안 기능이 아닌 것은 무엇인가?

① 무결성 ② 인증
③ 기밀성 ④ 재전송 공격방지

25. 무선랜에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 일반적으로 유선랜에 비해 품질이 낮다.
② 인증 암호의 취약성이 있다.
③ 무선 네트워크는 외부 전자기기와의 전파간섭이 없다.
④ 물리적 특성으로 인한 도난, 불법설치, 불법도청 등의 취약성이 있다.

26. 다음 지문은 무엇에 관한 설명인가?

> 가. Phil Zimmermann이 개발한 대표적인 이메일 보안프로토콜이다.
> 나. RSA와 Diffie-Hellman 등으로 공개키 생성이 가능하다.
> 다. 암호 알고리즘을 이용하여 기밀성, 인증, 무결성, 부인방지 등의 기능 지원이 가능하다.

① POP3 ② S/MIME
③ PEM ④ PGP

27. FTP(File Transfer Protocol)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 네트워크에서 컴퓨터 간 파일 송·수신을 위한 프로토콜이다.
② FTP는 두 개의 잘 알려진(well-known) TCP 포트를 사용한다.
③ 포트 20번은 제어 연결을 위해 사용되고, 포트 21번은 데이터 연결을 위해 사용된다.
④ FTP는 기본적으로 Active Mode와 Passive Mode를 지원한다.

28. DNSSEC는 DNS(Domain Name System)가 갖고 있는 보안 취약점을 극복하기 위한 DNS 확장 표준프로토콜이다. DNSSEC이 예방할 수 있는 공격기법은 무엇인가?

① 파밍(Pharming) ② 피싱(Phishing)
③ 스미싱(Smishing) ④ 랜섬웨어(Ransomware)

29. 웹 서비스 공격기법에 관한 다음 설명 중 공격기법을 바르게 짝지은 것은 무엇인가?

> (가) 게시판의 글에 원본과 함께 악성코드를 삽입하여 글을 읽을 경우 악성코드가 실행되도록 함으로써 클라이언트의 정보를 유출하는 공격기법
> (나) 공격자의 악의적인 데이터로 예상하지 못한 명령을 실행하거나 적절한 권한없이 데이터에 접근하도록 인터프리터를 속이는 공격기법
> (다) 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격기법

① (가) CSRF (나) Injection (다) XSS
② (가) XSS (나) Injection (다) CSRF
③ (가) CSRF (나) XSS (다) File Upload
④ (가) XSS (나) File Upload (다) Injection

30. 데이터베이스 보안 요구사항에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 부적절한 접근방지 - 인가된 사용자의 접근만이 허락되고 모든 접근요청은 DBMS가 검사한다.
② 추론방지 - 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 해야 하는 것을 의미한다.
③ 사용자 인증 - 별도의 엄격한 사용자 인증방식이 필요하다.
④ 다단계 보호 - 데이터에 대한 등급분류를 통하여 책임추적성을 보장한다.

31. 다음 지문은 무엇에 관한 설명인가?

> 가. 기기 내부에 암호화 및 복호화 그리고 전자서명을 위한 프로세스 및 연산장치가 내장되어 있어 암호화와 관련된 키의 생성 및 검증 등이 가능하다.
> 나. 보안토큰을 말하는 것으로 USB토큰 형태 이외에도 칩 형태, PCMCIA토큰 형태 등을 갖는다.

① OTP(One Time Password)
② TPM(Trusted Platform Module)
③ PKI(Public Key Infrastructure)
④ HSM(Hardware Security Module)

32. 다음 지문은 무엇에 관한 설명인가?

> 신용카드 기반 지불시스템인 SET(Secure Electronic Transaction)에서는 상점이 카드 사용자의 계좌번호와 같은 정보를 모르게 하는 동시에, 상점에 대금을 지불하는 은행은 카드 사용자가 구매한 물건을 알지 못하지만 상점이 요구한 결제 대금이 정확한지 확인할 수 있게 하기 위해 사용하는 방식이다.

① 인증서(Certificate)
② 전자봉투(Digital Envelop)
③ 이중서명(Dual Signature)
④ 지불게이트웨이(Payment Gateway)

33. 다음 중 전자화폐의 요구사항에 포함되지 않는 것은 무엇인가?

① 이중 사용방지(Double-Spending)
② 양도성(Transferability)
③ 온라인성(On-Line)
④ 분할성(Divisibility)

34. 다음 지문은 무엇에 관한 설명인가?

> 일반적인 정보검색엔진에서는 검색되지 않지만 특정한 환경의 웹 브라우저에서만 접속되어 검색되는 사이트를 가리킨다. 주로 사이버 범죄가 이루어지는 공간이다.

① 웹 쉘(Web Shell)
② 다크 웹(Dark Web)
③ 스턱스넷(StuxNet)
④ 고스트넷(GhostNet)

35. OECD 개인정보보안 8원칙에 포함되지 않는 것은 무엇인가?

① 이용제한의 원칙
② 정보 정확성의 원칙
③ 비공개의 원칙
④ 안전성 확보의 원칙

36. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제70조 (벌칙) 내용이 아닌 것은 모두 몇 개인가?

가. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
나. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.
다. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 다른 사람을 모욕한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.
라. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 사자의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 3천만원 이하의 벌금에 처한다.

① 1개 ② 2개 ③ 3개 ④ 4개

37. 「전자서명법」 제21조(전자서명생성정보의 관리) 제4항의 내용 중 ( ) 안에 들어갈 단어로 바르게 짝지은 것은 무엇인가?

공인인증기관은 자신이 이용하는 전자서명(가)정보를 안전하게 보관·관리하여야 한다. 이 경우 당해 전자서명(나)정보가 분실·훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 지체없이 그 사실을 (다)에(게) 통보하고 인증업무의 안전성과 신뢰성을 확보할 수 있는 대책을 마련하여야 한다.

① (가) 생성 (나) 생성 (다) 인터넷진흥원
② (가) 검증 (나) 생성 (다) 인터넷진흥원
③ (가) 생성 (나) 생성 (다) 이용자
④ (가) 생성 (나) 검증 (다) 이용자

38. 다음 지문은 무엇에 관한 설명인가?

가. 자신에게 불리한 증거자료를 사전에 차단하려는 활동이나 기술 나. 데이터 복구 회피기법 다. 데이터 은닉(Steganography)

① Anti Forensic ② Digital Forensic
③ Root Kit ④ Stealth Scan

39. 1998년 Guidance Software Inc.가 사법기관 요구사항에 바탕을 두고 개발한 컴퓨터 증거분석용 소프트웨어인 엔케이스(EnCase) 고유의 포렌식 디스크 이미지 파일형식은 무엇인가?

① FTK ② dd ③ SHA ④ E01

40. 다음 지문에서 설명하는 디지털포렌식의 원칙은 무엇인가?

증거는 획득하고 난 뒤 이송, 분석, 보관, 법정 제출이라는 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다.

① 정당성의 원칙
② 재현의 원칙
③ 연계 보관성의 원칙
④ 무결성의 원칙