정보보호론

1. 검증을 마친 시스템 사용자가 시스템 자원에 접근할 수 있도록 허락하는 과정은?
   ① Authentication
   ② Authorization
   ③ Audit
   ④ Accounting

2. 도출된 위험에 대하여 보안 대책 마련을 위한 추가적인 비용의 투입이나 외부와의 연계·협력을 고려하지 않고, 잠재적 위험을 자체적으로 감수하거나 일부 시스템 기능의 사용 포기에 따른 불편함을 감수하는 방식의 위험 대처에 해당하는 것만을 모두 고르면?

ㄱ. 위험 수용	ㄴ. 위험 회피
ㄷ. 위험 감소	ㄹ. 위험 전가

   ① ㄱ, ㄴ
   ② ㄱ, ㄹ
   ③ ㄴ, ㄷ
   ④ ㄷ, ㄹ

3. 해시 충돌을 바르게 나타낸 것은? (단, 해시 함수 $h_1 \neq h_2$, 해시 입력값 $k_1 \neq k_2$)
   ① $h_1(k_1) = h_2(k_1)$
   ② $h_1(k_1) = h_1(k_2)$
   ③ $h_1(k_1) \neq h_1(k_2)$
   ④ $h_1(k_1) \neq h_2(k_2)$

4. 메시지 인증 코드(MAC)에 대한 설명으로 옳지 않은 것은?
   ① MAC을 사용하기 위해서는 송·수신자만의 공유 비밀키가 필요하다.
   ② MAC의 길이는 메시지의 길이와 같다.
   ③ 메시지와 함께 전달되어 메시지 무결성 검증에 이용된다.
   ④ 수신자는 검증을 통해 메시지가 송신자로부터 전송된 것을 확인할 수 있다.

5. 리눅스 파일의 접근 권한을 설정하기 위하여 다음과 같은 명령을 실행한 경우, 해당 파일에 부여된 권한을 바르게 나타낸 것은?

```
chmod 2755 file1
```

   ① -rwxr-xr-x
   ② -rwsr-xr-x
   ③ -rwxr-sr-x
   ④ -rwsr-sr-x

6. 「정보통신기반 보호법」상 주요정보통신기반시설을 관리하는 관리기관의 장이 국가정보원장에게 우선적으로 기술적 지원을 요청하여야 하는 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설이 아닌 것은?
   ① 도로·철도·지하철·공항·항만 등 주요 교통시설
   ② 전력, 가스, 석유 등 에너지·수자원 시설
   ③ 금융 정보통신기반시설 등 개인정보가 저장된 정보통신기반시설
   ④ 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

7. AES 알고리즘의 복호화 과정에서 한 암호 블록에 대해 실행되는 처음 4개의 오퍼레이션을 첫 번째부터 네 번째까지 순서대로 바르게 나열한 것은? (단, ARK: Add Round Key, IMC: Inverse Mix Columns, ISR: Inverse Shift Rows, ISB: Inverse Substitute Bytes)
   ① ARK − IMC − ISR − ISB
   ② ARK − ISB − ISR − IMC
   ③ ARK − ISR − ISB − ARK
   ④ IMC − ISR − ISB − ARK

8. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3의 일부이다. (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

> (가)는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 (나)로 지정하고 과학기술정보통신부장관에게 신고하여야 한다.

	(가)	(나)
①	정보통신서비스 제공자	정보보호 최고책임자
②	정보통신서비스 제공자	개인정보 보호책임자
③	개인정보처리자	정보보호 최고책임자
④	개인정보처리자	개인정보 보호책임자

9. 리눅스에서 사용자 계정의 패스워드를 변경한 후 그 패스워드를 그대로 사용해야 할 최소 기간과 사용할 수 있는 최대 기간을 지정하기 위한 명령어와 그 명령의 실행 결과가 저장되는 파일을 바르게 연결한 것은?

	명령어	파일
①	usermod	/etc/passwd
②	chage	/etc/passwd
③	usermod	/etc/shadow
④	chage	/etc/shadow

10. 서비스 거부(DoS) 공격에 대한 대응 방법으로 옳지 않은 것은?
   ① Smurf 공격에 대응하기 위해 브로드캐스트 IP 주소로 전송되는 ICMP 패킷을 차단한다.
   ② Land 공격에 대응하기 위해 출발지와 목적지의 IP 주소가 동일한 패킷을 차단한다.
   ③ TCP SYN Flooding 공격에 대응하기 위해 서버의 TCP 연결 테이블의 크기를 감소시킨다.
   ④ Slowloris 공격에 대응하기 위해 특정 클라이언트로부터 전송된 일정 시간 동안의 불완전한 HTTP 요청 개수와 연결 유지 시간을 제한한다.

11. 다음 설명에 해당하는 RAID 레벨은?

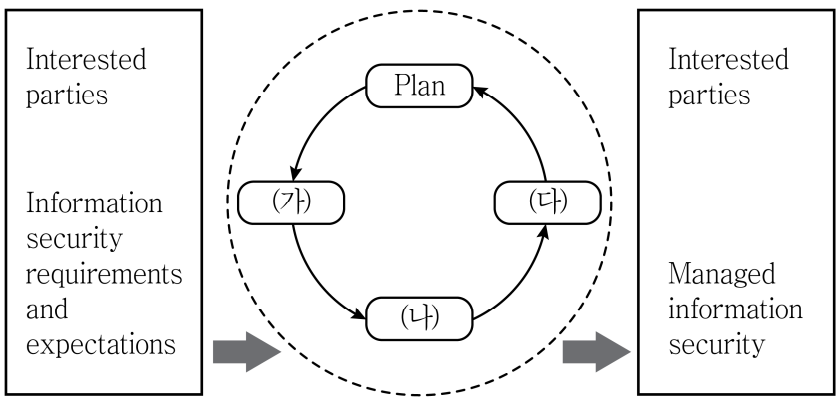
> ○ 패리티를 생성하기 위해 XOR 연산자를 이용한 오류 정정 코드를 사용한다.
> ○ 패리티 블록들은 전체 디스크 배열에 분산되어 저장된다.

① RAID 레벨 1
② RAID 레벨 3
③ RAID 레벨 4
④ RAID 레벨 5

12. 객체 소유자가 자율적 판단에 따라 객체에 대한 접근 권한을 제어하는 것은?

① 임의적 접근 제어(DAC)
② 강제적 접근 제어(MAC)
③ 역할 기반 접근 제어(RBAC)
④ 래티스 기반 접근 제어(Lattice Based Access Control)

13. ISO 27001 표준의 관리 체계 모델을 나타낸 다음 그림의 (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?



(가)	(나)	(다)
① Check	Act	Do
② Check	Do	Act
③ Do	Act	Check
④ Do	Check	Act

14. 네트워크 환경에서의 재전송(replay) 공격을 방지하기 위한 수단이 아닌 것은?

① 시퀀스 번호
② 타임 스탬프
③ 비표(nonce)
④ 샌드박스

15. 송신자 측에서 SSL Record 프로토콜이 수행되는 순서를 바르게 나열한 것은?

① 단편화 – 암호화 – MAC 추가 – 압축
② 단편화 – 압축 – MAC 추가 – 암호화
③ 단편화 – MAC 추가 – 암호화 – 압축
④ 압축 – MAC 추가 – 암호화 – 단편화

16. 「개인정보 보호법」상의 개인정보 보호 인증과 관련한 다음 설명의 (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

> 개인정보 보호위원회는 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 「개인정보 보호법」에 부합하는지 등에 관하여 인증할 수 있다. 인증의 유효기간은 [(가)]으로 하며, 인증의 실효성 유지를 위하여 [(나)] 사후관리를 실시하여야 한다.

(가)	(나)
① 2년	연 1회 이상
② 2년	연 2회 이상
③ 3년	연 1회 이상
④ 3년	연 2회 이상

17. Snort에 대한 설명으로 옳지 않은 것은?

① 오픈 소스 네트워크 기반 침입 탐지 시스템으로 개발되었다.
② 수집된 트래픽을 정상행위 프로파일과 비교하여 침입을 탐지한다.
③ 패킷의 삭제, 기록 그리고 침입 경고 생성 등의 기능을 제공한다.
④ 관리자가 정의한 침입탐지 규칙을 적용할 수 있다.

18. 다음 설명에 해당하는 웹 보안 공격은?

> 사용자가 인지하지 못한 사이에 웹 서버가 신뢰하는 사용자의 웹 브라우저로부터 공격자가 의도한 명령이 웹 서버에 전달되어 사용자의 권한으로 실행되도록 한다.

① 저장형 XSS
② 반사형 XSS
③ XXE(XML eXternal Entity)
④ CSRF

19. TCP 세션 하이재킹 공격에 대한 다음 설명의 (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

> ○ 공격자는 클라이언트와 서버의 TCP 연결 상태를 스니핑한다.
> ○ 공격자는 세션이 완전히 끊어지지 않는 범위에서 서버에게 [(가)] 세그먼트를 보내어 서버를 잠시 Closed 상태로 만든다.
> ○ 공격자는 조작된 [(나)] 번호로 서버와 새로운 TCP 연결을 설정한다.
> ○ 결과적으로 공격자는 세션을 탈취하고 인증을 회피할 수 있게 된다.

(가)	(나)
① FIN	Sequence
② FIN	Acknowledgment
③ RST	Sequence
④ RST	Acknowledgment

20. 다음은 사용자 A와 B가 Diffie-Hellman 키 교환 프로토콜을 이용하여 비밀키를 공유하려고 하는데 D에 의한 중간자 공격이 발생한 과정을 순서대로 나타낸 것이다. 이 결과로 A가 얻은 비밀키와 B가 얻은 비밀키를 바르게 연결한 것은? (단, 사전에 A와 B는 공개된 소수 q와 원시근 α를 이용하여 각자 자신의 개인키로 X_A와 X_B를 생성하고 자신의 공개키로 Y_A와 Y_B를 각각 산출한다)

○ D는 임의 개인키 X_{D1}과 X_{D2}를 생성하고 이에 대응하는 공개키 Y_{D1}과 Y_{D2}를 계산한다.
○ A가 Y_A를 B에게 전송한다.
○ D는 Y_A를 가로채고 대신에 Y_{D1}을 B에게 전송한다.
○ B는 Y_{D1}을 받고 A에게 Y_B를 전송한다.
○ D는 Y_B를 가로채고 대신에 Y_{D2}를 A에게 전송한다.
○ A가 Y_{D2}를 받는다.

	A의 비밀키	B의 비밀키
①	$(Y_A)^{X_{D1}} \bmod q$	$(Y_B)^{X_{D2}} \bmod q$
②	$(Y_B)^{X_{D2}} \bmod q$	$(Y_A)^{X_{D1}} \bmod q$
③	$(Y_A)^{X_{D2}} \bmod q$	$(Y_B)^{X_{D1}} \bmod q$
④	$(Y_B)^{X_{D1}} \bmod q$	$(Y_A)^{X_{D2}} \bmod q$

21. IEEE 802.11i에서 사용하는 CCMP에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. 무선 단말과 AP 사이 구간에서의 데이터 기밀성과 무결성을 위해 동일한 128비트 키가 사용된다.
ㄴ. Michael 알고리즘에 의한 MIC(Message Integrity Code)를 추가하여 무결성을 제공한다.
ㄷ. 데이터 암호화를 위해 AES 암호 알고리즘과 CBC 블록 암호 운용 모드를 사용한다.
ㄹ. CBC 블록 암호 운용 모드를 이용한 암호 기반의 MAC을 이용한다.

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

22. TCP 프로토콜의 보안 관련 특징에 대한 설명으로 옳지 않은 것은?

① 포트 번호를 활용하여 응용에 대한 접근통제 정책을 설정할 수 있다.
② SYN Flooding은 3-way handshaking 동작 절차를 악용한 공격이다.
③ TCP 포트 스캐닝을 통해 동작 중인 서비스를 확인할 수 있다.
④ TCP 헤더의 체크섬을 이용하여 전송 중에 발생한 데이터의 위·변조를 탐지할 수 있다.

23. SEED 128 알고리즘에 대한 설명으로 옳지 않은 것은?

① 1999년 2월 한국인터넷진흥원과 국내 암호 전문가들이 순수 국내 기술로 개발한 128비트 블록 암호 알고리즘이다.
② 전체 구조는 SPN 구조로 이루어져 있으며, 128비트의 평문 블록과 128비트 키를 입력으로 사용하여 총 16라운드를 거쳐 128비트의 암호문을 출력한다.
③ 128비트 암호키를 64비트씩 좌우로 나누어 처리해서 얻어진 4개의 워드에 대해 간단한 산술연산과 G 함수를 적용하여 라운드 키를 생성한다.
④ 1999년 9월 정보통신단체표준(TTA)으로 제정되었으며, 2005년에는 국제 표준화 기구인 ISO/IEC와 IETF로부터 암호화 표준 알고리즘으로 인정받았다.

24. ISMS-P 인증기준의 개인정보 처리 단계별 요구사항으로 옳지 않은 것은?

① 인증 및 권한관리
② 개인정보 수집 시 보호조치
③ 개인정보 보유 및 이용 시 보호조치
④ 정보주체 권리보호

25. 다음은 쿠키(Cookie)의 일반적인 생성 및 저장 과정을 순서대로 나타낸 것이다. 이 과정 이후에 클라이언트가 다시 서버에 요청을 보낼 때, HTTP 메시지에 포함되는 것은?

○ 서버가 클라이언트로부터 요청을 받으면 서버는 클라이언트에 관한 정보를 파일이나 문자열로 저장한다.
○ 서버는 클라이언트에게 보내는 응답에 쿠키를 포함한다.
○ 클라이언트가 응답을 받으면 브라우저는 쿠키를 도메인 서버 이름으로 정렬되는 쿠키 디렉터리에 저장한다.

① 요청 라인의 Set-Cookie
② 헤더 라인의 Set-Cookie
③ 요청 라인의 Cookie
④ 헤더 라인의 Cookie