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

1. 다음 중 정보보호의 목표에 대한 설명으로 가장 옳은 것은?
① 가용성(Availability)은 정보에 접근할 수 있는 객체의 자격이나 내용을 검증하는 데 사용되는 성질이다.
② 기밀성(Confidentiality)은 정당한 사용자가 정보 시스템의 데이터 또는 자원을 필요로 할 때 지체 없이 접근하여 사용할 수 있게 하는 성질이다.
③ 무결성(Integrity)은 정보의 내용이 불법적으로 생성, 변경 또는 삭제되지 않도록 하는 성질이다.
④ 인증성(Authentication)은 행위나 사건이 발생하였을 때 그것을 증명하여 나중에 그런 행위나 사건을 부인할 수 없도록 하는 성질이다.

2. 다음 지문은 OECD의 개인정보보호 8원칙 중 무엇에 관한 설명인가?

> ○ 정보주체의 개인정보 열람·정정·삭제 청구권 보장
> ○ 정보주체가 합리적 시간과 방법에 의해 개인정보에 접근할 수 있도록 보장

① 수집 제한의 원칙(Collection Limitation Principle)
② 공개의 원칙(Openness Principle)
③ 안전성 확보의 원칙(Security Safeguard Principle)
④ 개인 참가의 원칙(Individual Participation Principle)

3. 다음 지문에 주어진 암호문을 Caesar Cipher를 사용하여 복호화할 때 결과는?

> 다음은 SHIFT +3을 적용한 암호문이다.
> SROLFHORYH

① VULNERABLE ② VUROIKRUBK
③ POLICEBEST ④ POLICELOVE

4. 다음 지문에서 대칭키 방식의 암호화 알고리즘은 모두 몇 개인가?

> 가. ARIA 나. DES 다. DSA 라. ElGamal
> 마. ECC 바. RSA 사. SEED

① 2 개 ② 3 개 ③ 4 개 ④ 5 개

5. 송신자 A와 수신자 B가 Diffie-Hellman 키 분배 알고리즘을 이용하여 동일한 비밀키를 분배받고자 한다. 다음과 같은 조건이 주어졌을 때 분배받은 비밀키 값으로 옳은 것은?

> $g^x \bmod p$ (p, g는 값은 공개되어 있고, x는 개인키)
> 송신자 A: $p = 7$, $g = 3$, $x = 3$
> 수신자 B: $p = 7$, $g = 3$, $x = 2$

① 1 ② 3 ③ 5 ④ 7

6. 다음 중 암호학적 해시 함수(hash function)가 갖추어야 할 특성에 대한 설명으로 가장 옳지 <u>않은</u> 것은?
① 임의 길이의 메시지를 고정 길이의 해시값 출력으로 변환하여야 한다.
② 해시값 출력의 충돌을 방지하기 위해 입력 공간이 출력 공간보다 커야 한다.
③ 임의의 해시값 출력에 대한 입력 메시지를 구하는 것이 계산상 불가능해야 한다.
④ 같은 해시값 출력을 생성하는 임의의 2개의 입력값을 찾는 것이 계산상 불가능해야 한다.

7. 다음 중 국산 해시 암호 알고리즘으로 올바르게 묶인 것은?
① SEED, HIGHT ② HAS-160, LSH
③ SHA-1, HAS-160 ④ LSH, LEA

8. 다음 중 전자 서명에 대한 설명으로 가장 옳지 <u>않은</u> 것은?
① 은닉 서명은 문서의 내용을 공개하지 않고, 문서에 대한 서명을 받는다.
② 부가형 서명은 서명 검증 과정에서 메시지를 추출할 수 없다.
③ 부인 방지 서명은 대칭키 암호 알고리즘을 이용하여 구현된다.
④ 다중 서명 방식은 하나의 문서에 여러 명이 서명할 수 있다.

9. 정부가 추진하는 '5G+전략' 10대 핵심 산업과 가장 관련성이 <u>없는</u> 것은?
① 지능형 CCTV ② 미래형 드론
③ 정보보안 ④ 나노 복제

10. 다음 지문에서 설명하고 있는 보안 통제 기법은?

> 임의의 객체에 포함되어 있는 정보가 명시적으로 혹은 암시적으로 보다 보호수준이 낮은 객체로 이동하는 것을 검사하여 부당한 데이터 전달을 제어하는 기술

① 접근 제어 ② 흐름 제어
③ 추론 제어 ④ 사후 추적

11. 다음 지문에서 설명하고 있는 접근통제 모델은?

> 이 모델은 데이터의 기밀성을 희생하더라도 무결성을 보호하는 것에 초점을 둔 최초의 수학적 모델이며, 무결성 레벨을 계층적으로 정의한다. 이 레벨은 조직에 따라, 다루는 업무에 따라 달라질 수 있다. 이 모델에서 주체는 자신보다 낮은 무결성 수준의 데이터를 읽을 수 없다(단순 무결성 원칙). 주체는 자신보다 높은 무결성 수준에 있는 객체를 수정할 수 없다(스타 무결성 원칙).

① 벨 라파듈라 모델 (Bell Lapadula Model)
② 비바 모델 (Biba Model)
③ 래티스 모델 (Lattice Model)
④ 클라크 윌슨 모델 (Clark-Wilson Model)

12. 다음 지문은 사회공학을 기반으로 한 공격 중 무엇에 관한 설명인가?

> 사람들은 바빠서 사무실에 들어갈 때 누가 바짝 따라와 같이 들어가더라도 그 사실을 인지하지 못한다. 핸드폰으로 통화시늉을 하고, 미소를 지으며 문을 잡아 준다. 사무실에 들어가 빈자리를 찾아 AP를 연결하고 외부에 있는 (차량에 탄) 동료의 무선네트워크가 연결되면, 이를 통해 내부네트워크를 해킹할 수 있다.

① Phishing ② Pretexting ③ Tailgating ④ Vishing

13. 다음 중 리눅스에서 루트(root)가 자신이 소유한 /etc/inetd.conf 파일의 권한을 설정할 때 가장 옳은 것은?
① #chmod 400 /etc/inetd.conf ② #chmod 555 /etc/inetd.conf
③ #chmod 600 /etc/inetd.conf ④ #chmod 777 /etc/inetd.conf

14. 다음은 /etc/shadow 파일의 일부이다. 설명한 내용 중 가장 옳지 않은 것은?

```
pol_admin:!:15964:0:99999:7:0:11323:
police:$5$C7n1nPnI$a6nCwOTqrNR2oDulKirRZ:14684:0:99999:7:::
```

① pol_admin 계정은 패스워드 미설정 상태이다.
② police 계정은 SHA-256 해시 암호 알고리즘을 사용하였다.
③ police 계정은 salt와 패스워드로 암호화된 필드가 있다.
④ /etc/shadow 파일에 사용자 패스워드 최소 길이 필드가 있다.

15. 다음 지문에서 설명하고 있는 메모리 보호 기법은?

> 함수 진입 시 스택에 리턴 주소와 프레임포인터 정보를 저장할 때 정보를 보호하기 위해 특정한 값(Canary)을 기록한다.

① ASLR (Address Space Layout Randomization)
② NX (No-eXecute)
③ SSP (Stack Smashing Protector)
④ Format String

16. 다음 지문에서 설명하고 있는 보안 공격 기법은?

> 알고리즘의 약점을 찾기보다 연산시간 분석, 소비전력, 방출 전자기파, 소리 등을 통해 정보를 추출하는 공격이다.

① 부 채널 공격 (Side Channel Attack)
② 스펙터 (Spectre)
③ 멜트다운 (Meltdown)
④ 고스트다운 (Ghostdown)

17. 다음 중 클라우드에서 제공하는 정보보호 서비스인 SecaaS(Security as a Service)에 대한 설명으로 가장 옳지 않은 것은?

① 보안의 책임을 기업으로부터 보안 서비스 제공자로 이관하게 된다.
② 보안 서비스를 사용한 만큼 비용을 지불하는 방식이다.
③ 클라우드 컴퓨팅의 서비스 모델 중에서 IaaS에 해당된다.
④ 접근 관리, 웹보안, 이메일 보안 등의 서비스를 제공한다.

18. 비트코인과 이더리움 등 가상화폐의 시세가 급등할수록 보안 위협은 증가한다. 이때 해킹으로 블록체인 플랫폼에 커다란 손상이 발생하거나 소프트웨어에 심각한 결함이 발견된다. 이에 신규 기능이 추가된 최신 블록체인 노드를 이전 버전의 블록체인과 호환되지 않도록 업데이트시키는 기술은?

① Hard Fork　② Secure Fork
③ Smart Fork　④ Soft Fork

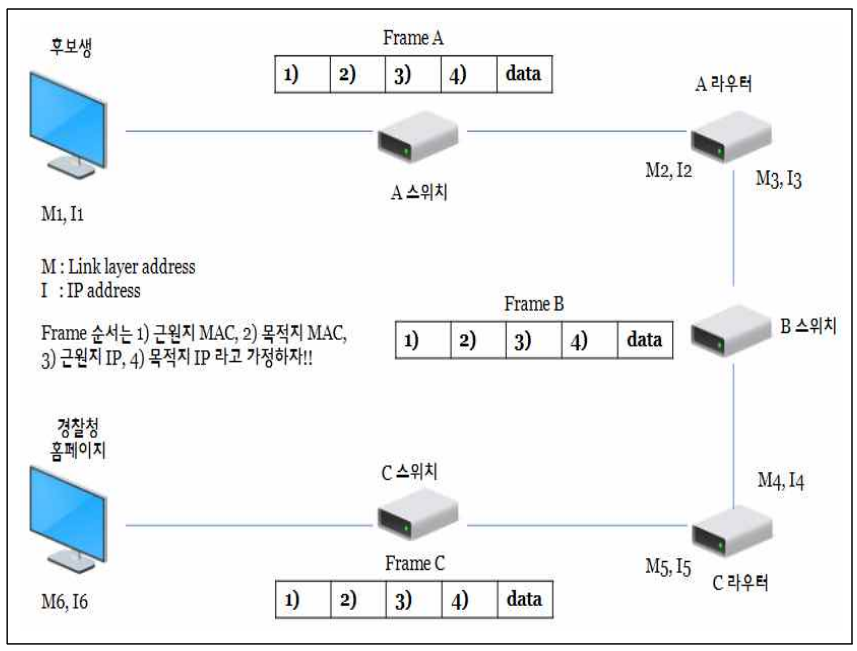
19. 다음 중 TCP와 UDP에 대한 설명으로 가장 옳지 않은 것은?

① TCP와 UDP는 전송 계층(Transport layer)에 해당하는 프로토콜이다.
② TCP는 가상 회선 방식이며, UDP는 데이터그램 방식으로 동작한다.
③ TCP는 전송 순서를 보장하며, UDP에 비해 높은 신뢰성을 갖고 있다.
④ TCP는 연결 지향적이며, UDP에 비해 상대적으로 전송 속도가 빠르다.

20. 다음 중 OSI 7계층에 대한 설명으로 가장 옳지 않은 것은?

① 물리 계층은 장치들 간의 물리적인 접속과 비트 정보를 다른 시스템에 전송하는 데 필요한 규칙을 정의하며, 이 계층에서 다루는 데이터를 비트스트림(Bit Stream)이라고 한다.
② 데이터 링크 계층은 통신 경로상의 지점간(link-to-link) 회선 제어, 흐름 제어, 오류 제어를 담당하며, 이 계층에서 다루는 데이터를 프레임(Frame)라고 한다.
③ 네트워크 계층은 두 사용자 사이의 신뢰성 있는 데이터 전송을 위한 종단간(end-to-end) 제어를 담당하며, 이 계층에서 다루는 데이터를 세그먼트(Segment)라고 한다.
④ 세션 계층은 두 응용프로그램 간의 연결설정, 이용 및 연결 해제 등 대화를 유지하기 위한 구조를 제공하며, 이 계층에서 다루는 데이터를 메시지(Message)라고 한다.

21. 간부후보생이 경찰청 홈페이지에 접속하여 정보를 검색할 때, 후보생의 요청정보가 홈페이지 서버에 전달된다. 이때 각 스위치 구간(A, B, C 스위치)에서 해커가 볼 수 있는 프레임의 네트워크 정보를 맞게 설명한 것은? (단, 후보생이 경찰청 홈페이지로 요청하는 정보만을 가정한다.)



① A스위치: M1,M2,I1,I6 B스위치: M3,M4,I1,I6 C스위치:M5,M6,I1,I6
② A스위치: M1,M2,I1,I2 B스위치: M3,M4,I3,I4 C스위치:M5,M6,I5,I6
③ A스위치: M1,M3,I1,I6 B스위치: M3,M5,I1,I6 C스위치:M5,M6,I1,I6
④ A스위치: M1,M3,I1,I2 B스위치: M3,M5,I3,I4 C스위치:M5,M6,I5,I6

22. 다음 중 인터넷 프로토콜과 그 용도가 올바르게 짝지어진 것은?

① CIDR : 혼잡 제어를 통해 신뢰성 있는 순차적 메시지 전송에 사용
② FTP : IP 주소를 물리적 네트워크 주소로 대응시키는 데 사용
③ ICMP : 호스트와 인접 라우터가 멀티캐스트 멤버십을 구성하는 데 사용
④ SNMP : IP 네트워크 상의 장치 정보를 수집하고 관리하는 데 사용

23. 다음 중 ARP 스푸핑(Spoofing)을 이용한 스니핑(sniffing) 공격에 대한 대응책으로 가장 옳지 않은 것은?

① 공격자가 내용을 알 수 없도록 데이터를 암호화하여 전송한다.
② ARP테이블을 동적으로 설정하여 융통성 있게 관리한다.
③ 주기적으로 무차별(promiscuous) 모드로 동작하는 기기가 있는지 검사한다.
④ 스위치 각 포트에 대해 접근 제한(Port Security)을 설정한다.

24. 다음 중 세션 하이재킹(Session Hijacking) 공격을 방어하는 수단으로 가장 옳지 않은 것은?

① 동기화 상태 탐지　② ACK Storm 탐지
③ 데이터 암호화　④ MAC 주소 고정

25. 다음 중 취약점 분석을 위해 사용하는 nmap의 사용법과 그에 대한 설명으로 가장 옳지 <u>않은</u> 것은?
① nmap -sU -p 53 192.168.xxx.xxx : 192.168.xxx.xxx의 53번 포트에 대한 UDP 스캔을 수행한다.
② nmap -sP 192.168.xxx.xxx : 192.168.xxx.xxx의 활성화 여부를 ping을 통해 검사한다.
③ nmap -sR -p 1-4000 192.168.xxx.xxx : 192.168.xxx.xxx의 1번 포트부터 4000번 포트까지 RPC 포트를 검색하여 보여준다.
④ nmap -sT -p 4000- 192.168.xxx.xxx : 192.168.xxx.xxx의 4000번 이하의 포트들에 대해 TCP Connect 스캔을 수행한다.

26. 다음 중 IPSec에 대한 설명으로 가장 옳지 <u>않은</u> 것은?
① IPSec 운영 모드 중 터널 모드는 종단 노드(end point) 구간에서 사용되며 전체 IP패킷을 보호하지 않는다.
② AH(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP패킷으로 전달되는 페이로드의 무결성을 보장하기 위해 설계되었다.
③ ESP(Encapsulating Security Payload)는 발신지 인증, 무결성, 프라이버시를 제공하는 프로토콜이다.
④ IPSec은 IP 계층의 보안을 위해 IETF에 의해 제안되었으며, VPN 구현에 사용되고 있다.

27. 다음 중 PGP(Pretty Good Privacy) 프로토콜에 대한 설명으로 가장 옳지 <u>않은</u> 것은?
① 안전한 전자 우편 송수신을 위해 Phil Zimmermann에 의해 제안되었다.
② 제3자의 개입 없이 수신자에 대한 인증과 부인방지 기능을 제공한다.
③ 하나의 파일을 여러 개의 파일로 분할하는 기능을 제공한다.
④ 별도의 인증기관은 필요 없으며, 키 링(Key ring)을 이용하여 공개키를 인증한다.

28. 다음 중 HTTP 프로토콜에서 요청 메시지에 적합한 인증 부족(Unauthorized)이라는 클라이언트 오류를 의미하는 상태 코드는?
① 200 ② 301 ③ 401 ④ 503

29. 다음 중 SSL/TLS 설명으로 가장 옳지 <u>않은</u> 것은?
① SSL은 TLS 이전 버전이며, 현재 릴리즈 버전은 TLS 1.4이다.
② HTTPS, SMTPS, FTPS는 TLS를 지원한다.
③ TLS 통신은 대칭키와 비대칭키 암호를 사용한다.
④ 브라우저 벤더들의 경우, 2020년까지 TLS 1.0/1.1 지원을 중단할 예정이다.

30. 소프트웨어 보안 취약점 유형 중, 입력값 검증 누락, 잘못된 검증으로 인해 발생할 수 있는 취약점으로 가장 옳지 <u>않은</u> 것은?
① 레이스 컨디션(Race Condition)
② 크로스 사이트 스크립팅(Cross Site Scripting)
③ SQL 삽입(SQL Injection)
④ 크로스 사이트 요청 위조(Cross Site Request Forgery)

31. 다음 중 전자 상거래를 위한 SET(Secure Electronic Transaction)에 대한 설명으로 가장 옳지 <u>않은</u> 것은?
① SET은 전자 지갑이라는 개념없이 간편한 전자 상거래를 지원한다.
② 인증기관(CA)은 참여자들의 신원을 확인하고 인증서를 발급한다.
③ SET은 이중 서명(dual signature) 방식으로 은닉 서명을 지원한다.
④ SET은 대칭키 및 공개키 방식의 암호화 알고리즘을 모두 사용한다.

32. 다음 지문에서 설명하고 있는 전자 입찰 시스템의 요구사항은?

> 각 입찰 참여자 간의 공모를 방지하여야 하며, 입찰 공고자와 서버의 독단이 발생하지 않도록 한다.

① 비밀성 ② 무결성 ③ 공평성 ④ 안전성

33. 저장매체의 물리적인 공간과 실제 사용되는 논리적 공간의 차이로 발생하는 낭비 공간을 의미한다. 디지털포렌식 관점에서는 공격자가 의도적으로 이 공간에 정보를 은닉할 수 있어 검사가 필요하다. 이 공간을 무엇이라고 하는가?
① 히든 공간 (Hidden Space) ② 슬랙공간 (Slack Space)
③ 짓 공간 (Git Space) ④ 그레이 공간 (Gray Space)

34. 다음 지문에서 설명하고 있는 디지털포렌식의 원칙은?

> 디지털포렌식 과정을 통해 수집된 증거는 획득되고 난 뒤, 이송, 분석, 보관, 법정제출이라는 일련의 과정이 명확해야 한다. 그리고 증거를 전달하고 전달받은 담당자 및 책임자에 대한 추적성이 명확하여 증거물의 진정성을 유지해야 한다.

① 전문배제성 ② 독수독과성
③ 연계보관성 ④ 수집신속성

35. 다음 중 정보보호 시스템 평가기준인 국제공통평가기준(Common Criteria)에 대한 설명으로 가장 옳지 <u>않은</u> 것은?
① EAL1에서 EAL7까지 7단계로 구성되어 있다.
② 우리나라는 CCP(Certificate Consuming Participants)로 분류된다.
③ 정보보호 측면에서 정보보호 기능이 있는 IT 제품의 안전성을 보증·평가한다.
④ 보안기능 요구사항과 보증 요구사항으로 구성된다.

36. 다음은 「개인정보보호법」 제34조(개인정보 유출 통지 등) 및 관련 시행령 제39조, 제40조에 따른 개인정보 유출통지 및 신고에 대한 내용이다. 빈칸에 순서대로 들어갈 내용으로 옳은 것은?

> <개인정보 유출 시 신고 방법>
> - 대상: (㉠) 이상의 정보주체의 개인정보 유출 시
> - 기관: 행정안전부, 전문기관 (㉡)
> - 시기: 지체없이
> - 방법: 전화, 전자우편, 팩스
> - 내용: 정보주체의 통지여부, 유출항목 및 규모, 유출시점과 경위, 유출피해 최소화 대책, 조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서, 담당자 및 연락처
> - 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 법 제34조제1항 각 호의 사항을 (㉢)일 이상 게재

① ㉠ 1천명 ㉡ 한국인터넷진흥원 ㉢ 7
② ㉠ 1천명 ㉡ 경찰청 사이버수사대 ㉢ 7
③ ㉠ 1만명 ㉡ 한국인터넷진흥원 ㉢ 10
④ ㉠ 1만명 ㉡ 경찰청 사이버수사대 ㉢ 10

37. 다음 중 「개인정보 보호법 시행령」으로 규정되어 있는 사항이 아닌 것은?

① 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항
② 개인정보의 파기방법 및 절차 등에 필요한 사항
③ 개인정보 보호책임자의 지정요건, 업무, 자격요건, 그 밖에 필요한 사항
④ 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항

38. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 (제44조의8 대화형정보통신서비스에서의 아동 보호)에 관한 사항 중 괄호 안에 들어갈 내용은?

> 정보통신서비스 제공자는 (　　)의 아동에게 문자·음성을 이용하여 사람과 대화하는 방식으로 정보를 처리하는 시스템을 기반으로 하는 정보통신서비스를 제공하는 경우에는 그 아동에게 부적절한 내용의 정보가 제공되지 아니하도록 노력하여야 한다.

① 만 12세 미만　　② 만 13세 미만
③ 만 14세 미만　　④ 만 15세 미만

39. 다음 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 명시된 정보보호 최고책임자의 업무에 해당하지 않는 것은?

① 사전 정보보호대책 마련 및 보안조치 설계·구현
② 정보보호 인증·평가 등의 실시 및 지원
③ 정보보호관리체계의 수립 및 관리·운영
④ 중요 정보의 암호화 및 보안서버 적합성 검토

40. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 정보보호 관리체계의 인증에 대한 내용이다. 빈칸에 순서대로 들어갈 내용으로 옳은 것은?

> 다음 각 호의 어느 하나에 해당하는 자는 인증을 받아야 한다.
> 1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
> 2. 집적정보통신시설 사업자
> 3. 연간 매출액 또는 세입 등이 (㉠) 이상이거나 정보통신서비스 부문 전년도 매출액 100억원 이상 또는 3개월간의 일일평균 이용자수 (㉡) 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

① ㉠ 1000억원　　㉡ 50만명
② ㉠ 1000억원　　㉡ 100만명
③ ㉠ 1500억원　　㉡ 50만명
④ ㉠ 1500억원　　㉡ 100만명