2014년09월27일년 정보보안기사 필기시험 기출문제 답안

【1과목 : 20문제】 시스템 보안	1	2	3	4	5	6	7	8	9	10
	③	④	①	④	④	②	③	①	④	④
	11	12	13	14	15	16	17	18	19	20
	①	④	④	③	④	④	②	①	③	④

【2과목 : 20문제】 네트워크 보안	21	22	23	24	25	26	27	28	29	30
	②	①	④	④	④	②	①	②	①	③
	31	32	33	34	35	36	37	38	39	40
	④	②	④	③	②	③	③	④	②	③

【3과목 : 20문제】 어플리케이션 보안	41	42	43	44	45	46	47	48	49	50
	③	④	①	③	③	①	③	④	③	③
	51	52	53	54	55	56	57	58	59	60
	①	④	③	④	②	④	②	①	③	②

【4과목 : 20문제】 정보 보안 일반	61	62	63	64	65	66	67	68	69	70
	③	③	①	④	②	①	④	③	④	①
	71	72	73	74	75	76	77	78	79	80
	③	①	②	④	④	④	④	②	③	③

【5과목 : 20문제】 정보보안 관리 및 법규	81	82	83	84	85	86	87	88	89	90
	④	③	④	③	③	③	①	①	④	④
	91	92	93	94	95	96	97	98	99	100
	③	②	②	①	④	③	④	③	④	③

전자문제집 CBT 홈페이지 : https://www.cbtestpro.kr

최신 수정 자료와 해설(오타・오답・규정변경)은 cbtestpro.kr 웹 및 앱에서 확인하세요.

기출문제의 저작권은 출제기관에 있습니다. cbtestpro.kr 및 관련 앱에서는 편집 및 재구성 작업만 하였음을 밝힙니다.



전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!

Download on the App Store

GET IT ON Google Play

【1과목】 시스템 보안 (20문제)

1. 다음 중 운영체계 5계층이 순서대로 나열된 것은?

① 메모리관리-프로세스관리-프로세서관리-주변장치관리-파일관리

② 프로세스관리-주변장치관리-파일관리-프로세서관리-메모리관리

❸ 프로세서관리-메모리관리-프로세스관리-주변장치관리-파일관리

④ 파일관리-메모리관리-프로세스관리-프로세서관리-주변장치관리

2. 사용자가 작성한 프로그램을 운영체계에 실행하도록 제출하면 운영체제는 이를 제출받아 프로세스를 만든다. 이때 생성된 프로세스의 주소영역을 구성하는 요소를 올바르게 나열한 것은?

① 데이터영역-스택영역-텍스트영역

② 텍스트영역-스택영역-데이터영역

③ 데이터영역-텍스트영역-스택영역

❹ 텍스트영역-데이터영역-스택영역

3. 다음 중 운영체제 발전 흐름에 대한 설명으로 올바르지 못한 것은?

❶ 다중처리시스템 : 여러 개의 CPU와 여러 개의 주기억장치를 이용하여 여러 개의 프로그램을 처리하는 방식이다.

② 시분할시스템 : 여러 명의 사용하는 시스템에서 각 사용자는 독립된 컴퓨터를 사용하는 느낌으로 사용한다.

③ 다중프로그램 : 하나의 CPU와 주기억장치를 이용하여 여러개의 프로그램을 동시에 처리하는 방식이다.

④ 분산처리시스템 : 여러 개의 컴퓨터를 통신회선으로 연결하여 하나의 작업을 처리하는 방식을 말한다.

4. 다음 중 윈도우 NTFS 파일 시스템에 대한 설명으로 올바르지 않는것은?

① NTFS 구조는 크게 VBR영역, MFT영역, 데이터영역으로 나눈다.

② 이론적인 최대 NTFS 파일 크기는 16EB이다.

③ 실제 최대 NTFS파일 크기는 16TB이다.

❹ 기본 NTFS보안을 변경하면 사용자마다 각기 다른 NTFS 보안을 설정할 수 있다.

5. 다음 올바르게 설명하고 있는 것은 무엇인가?

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonShutdownWithoutLogon 값이 '0' 일때

① 시스템 정상적인 종료로 인하여 대화상자에 종료버튼을 삭제 처리한다.

② 시스템 비정상적인 종료로 인하여 대화상자에 종료버튼을 비활성화 처리한다.

③ 시스템 정상적인 부팅하여 대화상자에 종료버튼을 삭제 처리한다.

❹ 시스템 정상적인 부팅하여 대화상자에 종료버튼을 비활성화 처리한다.

6. 윈도우즈 운영체제에서 네트워크상 관리목적으로 기본 공유폴더를 삭제하는 알맞은 명령어는 무엇인가?

① net Share_Dir / delete

❷ net share Share_Dir /delete

③ net delete

④ net share delete

7. 다음 중 레지스트리 편집기 종류에 대한 설명으로 올바르지 못한 것은?

① HKEY_CLASSES_ROOT : OLE데이터 확장자에 대한 정보 및 파일과 프로그램간 연결 정보가 포함되어 있다.

② HKEY_CURRENT_USER : 컴퓨터 환경정보가 저장되어 있으며, 다수 사용자가 사용할 경우 각 사용자별 프로파일이 저장되어 있다.

❸ HKEY_USERS : 각 사용자 정보들이 저장되어 있다.

④ HKEY_CURRENT_CONFIG : HKEY_LOCAL_MACHINE에 서브로 존재하는 Config 내용이 담겨져 있다.

8. 다음 중 인터넷 익스플로러 브라우저의 보안에 대한 설명으로 올바르지 못한 것은?

❶ 임시 인터넷파일 저장위치를 변경 할 수 있다.

② 방문한 웹사이트 저장 목록 일자를 변경할 수 있다.

③ 고급 탭에서 HTTP1.1 사용을 설정 할 수 있다.

④ 압축된 개인정보 취급방침 없는 타사의 쿠키를 차단하는 설정은 '보통'으로 하면 된다.

9. 다음 중 HTTP상태 프로토콜 값으로 연결이 올바른 것은?

① 200 : OK

② 204 : No Content

③ 400 : Bad Request

❹ 500 : Server Busy

10. 다음 스캐닝 방법 중에서 그 성격이 다른 하나는?

① FIN 스캐닝

② X-MAS 스캐닝

③ NULL 스캐닝

❹ SYN 스캐닝

11. 다음 보기를 보고 올바르게 설명하고 있는 것을 고르시오.

```
# iptables -A INPUT -s 172.10.10.10 -p tcp
-j drop
```

❶ 외부 ip 172.10.10.10에서 들어오는 패킷을 차단한다.

② 내부 ip 172.10.10.10에서 나가는 패킷을 차단한다.

③ 외부 ip 172.10.10.10에서 나가는 패킷을 차단한다.

④ 내부 ip 172.10.10.10에서 들어오는 패킷을 차단한다.

12. 다음 중 HTTP/1.1 요청방식이 아닌 것은?

① GET

② DELETE

③ TRACE

❹ PUSH

13. 다음 중 운영체제 5단계에 포함되지 않는 것은?

① 메모리관리

② 주변장치 관리

③ 파일관리

❹ 사용자관리

14. 다음 중 버퍼링과 스풀링에 대한 설명으로 올바르지 못한 것은?

① 버퍼링과 스풀링은 CPU 연산과 I/O 연산을 중첩시켜 CPU의 효율을 높이기 위하여 사용한다.

② 버퍼링은 단일사용자 시스템에 사용되고, 스풀링은 다중 사용자 시스템에 사용된다.

❸ 버퍼링은 디스크를 큰 버퍼처럼 사용하고 스풀링은 주기억 장치를 사용한다.

④ 버퍼링과 스풀링은 큐 방식의 입출력을 수행한다.

15. 다음 중 커널에 대한 설명으로 올바르지 못한 것은?

① 커널에는 커널모드와 사용자모드가 있다.

② 운영체제의 핵심을 커널이라 부른다.

③ 응용프로그램에 커널 서비스를 제공하는 인터페이스를 '시스템 콜 인터페이스'라 한다.

❹ 하드웨어 장치를 사용할 경우 사용자모드에서 사용된다.

16. 다음 중 취약성 점검도구가 아닌 것은 무엇인가?

① NESSUS

② SARA

③ NIKTO2

❹ TRIPWIRE

17. 다음 보기에 해당하는 로그 파일은 무엇인가?

```
- 시스템 로그인에 실패할 경우 이 파일에 저장
  된다.
- lastb 명령어를 통해 확인이 가능하다.
```

① wtmp

❷ btmp

③ utmp

④ pact

18. 다음 중 버퍼오버플로우 대한 설명으로 올바르지 못한 것은?

❶ 버퍼에 저장된 프로세스 간의 자원 경쟁을 야기해 권한을 획득하는 기법으로 공격하는 방법이다.

② 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소를 조작하는 기법을 사용하여 해킹을 한다.

③ 스택 버퍼오버플로우와 힙 오버플로우 공격이 있다.

④ 버퍼오버플로우가 발생하면 저장된 데이터는 인접한 변수영역까지침범하여 포인터 영역까지 침범하므로 해커가 특정코드를 실행하도록 하는 공격기법이다.

19. 다음 공격기법을 무엇이라 하는가?

> printf 함수의 취약점을 이용한 공격으로, 리턴 위치에 쉘코드 주소를 할당시켜 쉘을 획득하는 공격

① 버퍼오버플로우공격
② 스니핑 공격
❸ 포맷스트링공격
④ 세션하이젝킹 공격

20. 다음 리눅스 iptables에서 chain 형식으로 사용이 옳지 않은 것은?

① INPUT
② FORWORD
③ OUTPUT
❹ DROP

【2과목】 네트워크 보안 (20문제)

21. VPN 프로토콜 중 IPSEC에서 암호화 기능을 담당하는 프로토콜은?

① AH
❷ ESP
③ IKE
④ PPTP

22. 다음 중 CIDR 기법을 사용하지 않는 라우팅 프로토콜은?

❶ RIP v1
② RIP v2
③ EIGRP
④ OSPF

23. 다음 중 DDOS공격 프로그램이 아닌 것은 무엇인가?

① TRINOO
② TFN
③ Stacheldraht
❹ Teardrop

24. 다음에서 설명하고 있는 네트워크 공격방법은 무엇인가?

> 스위치에 주소테이블이 가득차게 되면 모든 네트워크 세그먼트로 브로드 캐스팅하게 된다. 공격자는 위조된 MAC주소를 지속적으로 네트워크에 보냄으로써 스위칭 허브의 주소 테이블을 오버플로우시켜 다른 네트워크 세그먼트의 데이터를 스니핑할수 있게 된다.

① ARP스니핑
② ICMP Redirect
③ ARP스푸핑
❹ 스위치재밍

25. 다음 중 TCP신호를 보내는 Flag 종류 연결로 올바르지 못한 것은?

① SYN – 요청 Flag로써 초기에 세션을 설정하는데 사용된다.
② ACK – 요청에 대한 응답을 하는 Flag이다.
③ FIN – 세션을 종료시키기 위한 Flag이다.
❹ RST – 패킷을 보내면 3way핸드쉐이킹 후 Closed모드에 들어간다.

26. 다음 그림에서 IDS 위치로 올바른 것은?

> PC -1- 방화벽 -2- 스위치 -3- 라우터 -4- 서버

① (1)
❷ (2)
③ (3)
④ (4)

27. 다음 중 세션하이젝킹에 이용되는 툴(도구)은 무엇인가?

❶ HUNT
② TRINOO
③ NIKTO2
④ TRIPWIRE

28. IDS에서 오용탐지를 위해 쓰이는 기술이 아닌 것은?

① 전문가시스템(expert System)
❷ 신경망(neural networks)
③ 서명분석(signature analysis)
④ 상태전이분석(State transition analysis)

29. 다음에서 설명하고 있는 VPN 키 관리 기법은 무엇인가?

- Diffie-Hellman 프로토콜에 기반한다.
- 네트워크 공격방지를 위한 메커니즘을 첨가하여 설계하였다.
- IETF제안으로 ISAKML와 Oakley결합한 키교환 프로토콜이다.

❶ ISAKMP
② OAKLEY
③ IKE
④ OCSP

30. 다음 IPS종류 중 어플리케이션게이트웨이 방식 설명으로 옳지 않은것은?

① 내부와 외부 네트워크가 프록시 서버를 통해서만 연결이 된다.
② 각 서비스별 프록시 데몬이 존재한다.
❸ 1세대 방화벽에 속 한다
④ 일부 서비스에 대해 투명성을 제공하기 어렵다.

31. 다음 중 IPTABLES에서 새로운 규칙을 출력하는 옵션은?

① -p
② -D
③ -A
❹ -L

32. ICMP메시지 종류중에서 TYPE 5인 메시지는 무엇인가?

① Echo Reply
❷ Redirect
③ Echo Request
④ Time Exceed

33. 다음 보기에서 설명하고 있는 네트워크 공격기법은 무엇인가?

- 공격자는 출발지 IP로 스푸핑하여 SYN패킷을 공격 경유지 서버로 전송한다.
- SYN패킷을 받은 경유지 서버는 스푸핑된 IP로 타겟 서버에 SYN/ACK을 전송한다.
- 타겟 서버는 수많은 SYN/ACK를 받아 이용 불능이 된다.

① dos
② ddos
③ drdos
❹ syn flooding

34. 다음 중 VPN에 대한 설명으로 올바르지 못한 것은?

① SSL VPN은 웹 어플리케이션 기반으로 구성된다.
② SSL VPN이 설치가 더 용이하다.
❸ IPSEC VPN은 시간과 장소에 제약이 없다.
④ IPSEC VPN은 규정된 사용자, 제한된 사용자만 수용한다.

35. 다음에 나열된 공격이 사용되는 융복합 서비스는 무엇인가?

bye attack, cancel attack, RTP Flooding, ARP cache poisoning, ddos

① IPTV
❷ VoIP
③ Smart TV
④ CCTV

36. VPN프로토콜 중 IPSEC에서 암호화 기능을 담당하는 프로토콜은?

① AH
② IKE
❸ ESP
④ OCSP

37. 다음 보기는 어떤 공격에 대한 설명인가?

> 웹사이트에서 입력을 엄밀하게 검증하지 않는 취약점을 이용하는 공격으로, 사용자로 위장한 공격자가 웹사이트에 프로그램 코드를 삽입하여 나중에 다시 이 사이트를 방문하는 다른 사용자의 웹 브라우저에서 해당 코드가 실행되도록 한다.

① 세션하이재킹
② 소스코드 삽입공격
❸ 사이트간 스크립팅(xss)
④ 게시판 업로드공격

38. 다음 중 IPSec에 대한 설명으로 올바르지 못한 것은?

① ESP는 헤더의 기밀성을 제공하기위해 사용된다.
② AH프로토콜은 메시지의 인증과 무결성을 위해 사용된다.
③ IKE프로토콜은 SA를 협의하기위해 사용된다.
❹ IPSec은 전송계층 레이어에서 작동된다.

39. 다음에서 설명하고 있는 기술은 무엇인가?

> 디지털 콘텐츠 저작권을 보호하기 위한 기술로 주로 콘텐츠의 불법적인 복제를 방지하고 허가받지 않은 기기에서 콘텐츠 소비를 방지한다.

① DLP
❷ DRM
③ IDS
④ VPN

Download on the App Store 전자문제집 CBT(App Store) :[다운로드]
GET IT ON Google Play 전자문제집 CBT(Google Play) :[다운로드]

40. 공격자가 자신이 전송하는 패킷에 다른 호스트 IP주소를 담아서 전송하는 공격은?

① 패킷스니핑
② 포맷스트링
❸ 스푸핑
④ 버퍼오버플로우

【3과목】 어플리케이션 보안 (20문제)

41. 다음에서 설명하고 있는 FTP공격 형태는 무엇인가?

> FTP서버가 데이터를 전송할 목적지가 어디인지 검사하지 않는 설계상의 문제점을 이용한 공격이다.

① 익명FTP공격
② FTP서버 자체 취약점
❸ 바운스공격
④ 무작위 전송 공격

42. 메일 필터링 스팸어쌔신에서 스팸 분류기준이 아닌 것은?

① 헤더검사
② 본문 내용검사
③ 주요 스팸 근원지와 비근원지 자동생성
❹ 첨부파일 검사

43. 다음 그림에 대한 ftp설명으로 올바르지 못한 것은?

> 1. 클라이언트 → 서버 (제어 연결)
> 2. 클라이언트 ← 서버 (데이터전송 연결)
> 3. 클라이언트 ↔ 서버 (데이터 전송)

❶ 두 번째 접속은 서버에서 클라이언트로 한다.
② 서버는 21번 포트와 1024이후의 포트를 연다
③ 첫 번째 접속은 21번 포트인 명령어 포트이다
④ 서버는 1024이후의 포트를 모두 연다.

44. 다음 보기에서 설명하고 있는 전자투표 방식은?

> - 지정된 투표소에서 하는 방식이다.
> - 선거인단이 관리하고 국민투표 활용성이 가장 크다.
> - 확인키 발급시 투표매매 가능성도 존재한다.

① 키오스크방식
② REV방식
❸ PSEV방식
④ LKR방식

45. 다음 보기의 SMTP 송신자 인증 방식은 무엇인가?

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
s: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob-example.org>
S: 250 OK
C: RCPT TO:<alice-example.com>
S: 250 OK
C: TCPT TO:<theboss-example.com>
S: 250 OK
C: DATA
S: 354 End data with<CR><LF>.<CR><LF>
C: FROM: "Bob Example" <bob-example.org>
C: To: "Alice Example"<alice-example.com>
C: Cc: theboss-example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
```

① HELO

② RCPT

❸ AUTH

④ DATA

46. 데이터베이스 보안요구사항 중 비기밀 데이터에서 기밀 데이터를 얻어내는 것을 방지하는 요구사항은?

❶ 추론방지

② 접근통제

③ 흐름제어

④ 암호화

47. 웹 브라우저와 웹 서버 간에 안전한 정보 전송을 위해 사용되는 암호화 방법은?

① PGP

② SSH

❸ SSL

④ S/MIME

48. 다음 중 PGP에 대한 설명으로 올바르지 못한 것은?

① PGP는 메시지인증 기능도 지원한다.

② IDEA암호알고리즘을 이용하여 암호화 한다.

③ 세션 키 로서 128비트 랜덤 키를 사용한다.

❹ 수신자는 세션 키를 자신이 생성한다.

49. 다음은 SET에서 사용하는 보안 메커니즘을 설명한 것이다. 다음의 내용에 해당하는 것은 무엇인가?

> 고객의 지불정보(신용카드번호 등)는 상점이 알지 못하게 하고, 주문정보(상품 등)는 은행이 알지 못하게 함으로써 프라이버시를 보호한다.

① 은닉서명

② 전자서명

❸ 이중서명

④ 영지식증명

50. 전자화폐 지불방식이 아닌 것은?

① 온라인 지불

② 오프라인 지불

❸ 고액 지불

④ 선불방식

51. PKI구조에 대한 설명 중 올바르지 못한 것은?

❶ 계층적 구조는 네트워크 구조에 비해 인증 경로 탐색이 어렵다.

② 네트워크 구조는 인증기관의 비밀 키 노출 시 해당 인증 도메인에만 영향을 미친다.

③ 계층적 구조는 단일화된 인증 정책과 중앙 집중적인 조직 체계에적절하다.

④ 네트워크 구조는 계층적 구조에 비해 구조가 유연하여 기존 구축된 서로 다른 도메인 간 연결할 때 유리하다.

52. 다음 중 전자화폐시스템에 대한 일반적 모델로 프로토콜 구성이 올바르지 않은 것은?

① 예치 : 상점서버 - 금융기관

② 지불 : 상점서버 - 사용자

③ 인출 : 사용자 - 금융기관

❹ 인증 : 지불서버 – 인증기관

53. 다음 중 SSL최하위 계층에 위치하고 있는 프로토콜은 무엇인가?

① Handshake

② Alert

❸ Record layer

④ Change CipherSpec

54. 전자투표 요구사항에 포함되지 않는 것은?

① 정확성
② 단일성
③ 합법성
❹ 독립성

55. 다운로드를 위한 게시판 파일을 이용하여 임의의 문자나 주요 파일명의 입력을 통해 웹 서버 홈 디렉토리를 벗어나 시스템 내부의 다른 파일로 접근하여 다운로드하는 공격은?

① CSS
❷ 파일다운로드
③ 인젝션
④ 쿠키/세션위조

56. 다음 중에서 SQL인젝션 공격에 대한 보호대책으로 거리가 먼 것은?

① 사용자 입력이 SQL 문장으로 사용되지 않도록 한다.
② 사용자 입력으로 특수문자의 사용은 제한하도록 한다.
③ 원시 ODBC오류를 사용자가 볼 수 없도록 코딩해야한다.
❹ 테이블 이름, SQL구조 등이 외부 HTML에 포함되어 나타나도록한다.

57. IETF에서 표준화하고 개발한 것으로 중앙 집중적으로 키 관리를 수행하는 이메일 보안 시스템은?

① PGP
❷ PEM
③ TSL
④ SET

58. XML기반 보안 기술이 아닌 것은?

❶ XPKI
② SAML
③ XKMS
④ XACML

59. 전자화폐의 안전성을 제공하기 위해 요구되는 기능 중에서 이중지불을 방지 할 수 있는 기능에 해당하는 것은?

① 익명성
② 양도성
❸ 분할성
④ 오프라인성

60. 전자 입찰시스템에서 필요한 5가지 보안 요구사항과 가장 거리가 먼 것은?

① 독립성
❷ 효과성
③ 비밀성
④ 무결성

【4과목】 정보 보안 일반 (20문제)

61. 적극적 공격에 해당되지 않는 것은?

① 변조
② 삽입
❸ 트래픽분석
④ 재생

62. 커버로스에 대한 설명으로 올바르지 못한 것은 무엇인가?

① mit에서 개발한 분산환경하에서 개체인증 서비스를 제공한다.
② 클라이언트, 인증서버, 티켓서버, 서버로 구성된다.
❸ 커버로스는 공개키 기반으로 만들어졌다.
④ 커버로스의 가장 큰 단점은 재전송공격에 취약하다는 것이다.

63. 다음 보기에서 설명하고 있는 블록 암호 모드는 무엇인가?

- 패딩 작업이 필요하다.
- 블록크기보다 작은 데이터에도 적용 가능하다.
- 재전송공격에 취약하다.

❶ ECB
② CBC
③ CTR
④ CFB

64. 다음은 어떤 접근제어 정책을 설명하고 있는가?

> 주제나 소속되어 있는 그룹들에 근거하여 객체에 대한 접근을 제한한다. 즉 접근 통제는 객체의 소유자에 의하여 임의적으로 이루어진다. 그러므로 어떠한 접근 허가를 가지고 있는한 주체는 임의의 다른 주체에게 자신의 접근권한을 넘겨줄 수 있다.

① MAC
② RBAC
③ CBAC
❹ DAC

65. 다음 보기에서 설명하고 있는 보안 기술은 무엇인가?

> - 기본 채널에 기생하는 통신 채널이다.
> - 기본 채널에서 신호대 잡음비를 축소해서 기본 채널의 대역폭을 축소시킨 것으로 은닉 메세지는 다른 사람 눈으로는 볼 수 없으며, 송신자와 수신자만 볼 수 있다.

① SSH터널링
❷ 은닉채널
③ 전송터널
④ 이중터널

66. 다음 중 Kerberos 인증 프로토콜에 대한 설명으로 옳지 않은 것은?

❶ 중앙서버 개입 없이 분산형태로 인증을 수행한다.
② 티켓 안에는 자원 활용을 위한키와 정보가 포함되어 있다.
③ 대칭키 알고리즘을 사용한다.
④ TGT를 이용해 자원사용을 위한 티켓을 획득한다.

67. DES에 대한 설명으로 옳지 않은 것은?

① Feistel암호방식을 따른다.
② 1970년대 블록암호 알고리즘이다.
③ 한 블록의 크기는 64비트이다.
❹ 한 번의 암호화를 거치기 위하여 10라운드를 거친다.

68. 국내기관에서 개발한 암호알고리즘은 무엇인가?

① AES
② DES
❸ ARIA
④ IDEA

69. 소인수 분해 어려움에 기반 한 큰 안정성을 가지는 전자서명알고리즘은?

① ECC
② KCDSA
③ Elgamal
❹ RSA

70. 다음 접근제어 모델 중에서 대상기반 접근제어가 아니라 특정한 역할들을 정의하고 각 역할에 따라 접근원한을 지정하고 제어하는 방식은?

❶ RBAC
② MAC
③ DAC
④ ACL

71. 다음 중 공개키 암호에 대한 설명으로 옳은 것은?

① 일반적으로 같은 양 데이터를 암호화한 암호문이 대칭키 암호보다 현저히 짧다.
② 대표적인 암호로 DES, AES가 있다.
❸ 대표적인 암호로 RSA가 있다.
④ 대칭키 암호보다 수년전 고안된 개념이다.

72. 다음의 내용이 설명하고 있는 것은?

> - 일종의 비밀 채널로 지적 재산권을 보호하기 위한 수단으로 사용함
> - 파일 내부에 비밀 정보를 삽입시켜 합법적인 소유자를 확인 할 수 있게 함
> - 그래픽, 오디오, 컴퓨터 프로그램 등 다양한 분야에 응용함

❶ 워터마크
② 암호화
③ 전자서명
④ 저작권

73. 다음 중 공인 인증서 구성요소 내용으로 올바르지 않은 것은?

① 공인 인증서 일련번호

❷ 소유자 개인키

③ 발행기관 식별명칭

④ 유효기간

74. 다음 중 Diffi-Hallman 알고리즘 특징이 아닌 것은?

① 단순하고 효율적이다.

② 인증 메시지에 비밀 세션 키를 포함하여 전달할 필요가 없다.

③ 세션 키를 암호화한 전달이 필요하지 않다.

❹ 사용자 A와 B만이 키를 계산할 수 있기 때문에 무결성이 제공된다.

75. 공개키 기반구조(PKI)에 대한 설명으로 올바르지 못한 것은?

① 인증서버 버전, 일련번호, 서명, 발급자, 유효기간 등의 데이터 구조를 포함하고 있다.

② 공개키 암호시스템을 안전하게 사용하고 관리하기 위한 정보보호방식이다.

③ 인증서 폐지 여부는 인증서폐지목록(CRL)과 온라인 인증서 상태 프로토콜(OCSP)확인을 통해서 이루어진다.

❹ 인증서는 등록기관(RA)에 의해 발행된다.

76. 다음 중 전자서명의 특징이 아닌 것은?

① 위조불가

② 서명자 인증

③ 부인불가

❹ 재사용가능

77. 대칭키 암호 알고리즘이 아닌 것은?

① DES

② SEED

③ 3DES

❹ DSA

78. 다음 중 스트림 암호 기술에 포함되지 않는 것은?

① OTP

❷ Peistel

③ LFSR

④ FSR

79. 다음 중 공개키 암호알고리즘 중에서 이산대수 문제에 기반 한 알고리즘이 아닌 것은?

① Schnorr

② DSA

❸ Rabin

④ KCDSA

80. 다음은 암호메시지 공격 중에 어떤 공격인가?

> 평문을 선택하면 대응되는 암호문을 얻을 수 있는 상황에서 공격하는 것을 말한다.

① 암호문 단독공격

② 알려진 평문공격

❸ 선택 평문공격

④ 선택 암호문공격

【5과목】 정보보안 관리 및 법규 (20문제)

81. 다음 중 정량적 위험분석 방법이 아닌 것은?

① 과거자료분석방법

② 확률분포법

③ 수학공식법

❹ 시나리오법

82. 통제수행시점에 따른 분류 중 설명이 올바르지 않은 것은?

① 예방통제 : 발생 가능한 잠재적인 문제들을 식별하여 사전에 대처하는 통제방법

② 탐지통제 : 예방통제를 우회하는 문제점을 찾아내는 통제방법

❸ 교정통제 : 교정통제에 대표적인 방법은 로깅기능을 통한 감사증적이 있다.

④ 잔류위험 : 사건발생가능성과 손실관점에서 위험을 허용하는 부분에 남아 있는 위험

83. OECD 정보보호 가이드라인에 포함되지 않는 내용은?

① 인식

② 책임

③ 윤리

❹ 교육

84. 다음에서 설명하고 있는 인증 제도는 무엇인가?

> 기업이 정보보호 활동을 지속적, 체계적으로 수행하기 위해 필요한 보호조치를 체계적으로 구축하였는지를 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도로 한국인터넷진흥원에서 시행중인 제도

① PIMS
② PIPL
❸ ISMS
④ PIA

85. 다음에 설명하고 있는 재난복구 대체처리 사이트는 무엇인가?

> - 하드웨어가 있고 연결이 이미 확립되어 있지만 애플리케이션이 설치되어 있지 않다.
> - 전체 워크스테이션은 설치되어 있지 않다.

① 쿨사이트
② 핫사이트
❸ 웜사이트
④ 콜드사이트

86. 다음 중 나라별, 지역별로 서로 다른 평가기준을 가짐에 따라 동일한 제품에 대한 중폭평가를 피하고 해결하기위한 정보보호시스템 공통평가기준을 무엇이라 하는가?

① ITSEC
② TCSEC
❸ CC
④ OCRA

87. 다음 중 개인정보보호법에 대한 설명으로 올바른 것은?

❶ 개인정보보호 위원회 위원은 대통령이 임명한다.
② 정보주체란 개인정보를 생성, 처리하는 자를 의미한다.
③ 개인정보는 어떤 경우에도 위탁이나 제 3자제공이 돼서는 안된다.
④ 개인정보 목적 달성 후 1년간 보관한다.

88. ISMS인증에서 정보보호관리 과정에 포함되지 않는 것은?

❶ 정보보호 교육 및 훈련
② 경영진 책임 및 조직구성
③ 위험관리
④ 사후관리

89. 공인인증서 소멸사유에 포함되지 않는 것은?

① 공인인증서 효력이 정지된 경우
② 공인인증서 기관이 취소된 경우
③ 공인인증서 유효기간이 경과한 경우
❹ 공인인증서 분실된 경우

90. 전자서명법상 전자서명의 효력으로 옳지 않은 것은?

① 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한것으로 본다.
② 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명 된 후 그 내용이 변경되지 아니하였다고 추정한다.
③ 공인전사저명외의 전자서명은 당사자 간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.
❹ 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명 된 후 그 내용이 변경되지 아니한 것으로 본다.

91. 다음은 정보관리 측면에서 무엇에 대한 설명인가?

> 비정상적인 일이 발생할 수 있는 가능성을 말한다.

① 위협
② 결함
❸ 위험
④ 취약성

92. 개인정보보호, 정보보호 교육에 대한 설명으로 옳지 않은 것은?

① 개인정보보호법에 따라 연1회이상 개인정보 교육을 의무적으로 한다.
❷ 정보보호 교육 시 자회사 직원만 교육하고 협력사는 제외한다.
③ 정보통신망법에 따라 연2회 이상 개인정보 교육을 의무적으로 한다.
④ 개인정보보호, 정보보안에 대한 교육은 수준별, 대상별로 나누어 교육한다.

93. 업무연속성(BCP) 5단계 순서를 올바르게 나열한 것은?

① 사업영향평가-복구전략개발-수행및테스트-범위설정 및 기획-복구수립계획

❷ 범위설정및기획-사업영향평가-복구전략개발-복구수립계획-수행및테스트

③ 복구수립계획-범위설정및기획-사업영향평가-복구전략개발-수행및테스트

④ 복구전략개발-복구수립계획-사업영향평가-범위설정및기획-수행및테스트

94. 개인정보보호법상 개인정보처리와 정보주체의 권리에 대한 설명으로 올바르지 않은 것은?

❶ 개인정보에 대한 열람은 가능하나 사본 발급은 요구할 수 없다.

② 개인정보처리로 인해 피해 발생이 될 경우 적법한 절차에 따라 구제 받을 수 있다.

③ 개인정보처리에 대한 정보를 제공받을 수 있다.

④ 개인정보처리 동의 여부, 범위 등을 선택하고 결정할 수 있다.

95. '정보통신망 이용촉진 및 정보보호등에 관한법률' 에 따라 정보보호책임자를 지정해야 한다. 정보보호 최고책임자가 해야 할 업무가 아닌 것은?

① 정보보호관리체계의 수립 및 관리/운영

② 정보보호 취약점 분석/평가 및 개선

③ 정보보호 사전 보안성 검토

❹ 주요 정보통신 기반시설 지정

96. '개인정보보호법'에 따라 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 정보주체에게 알려야 한다. 해당되지 않는 내용은?

① 유출된 시점과 그 경위

② 유출된 개인정보 항목

❸ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당자 및 연락처

④ 개인정보처리자의 대응조치 및 피해구제절차

97. 개인정보영향평가 대상 범위에 포함되지 않는 것은?

① 구축 또는 변경하려는 개인정보파일 중 민감 정보, 고유식별정보 5만 명 처리

② 구축 또는 운영하려는 개인정보파일이 내•외적으로 50만 명 이상연계

③ 구축 또는 변경하려는 개인정보 파일 중 정보추체가 100만 명 이상

❹ 구축 또는 변경하려는 개인정보 파일 중 주민등록번호가 포함시

98. 다음 중 개인정보보호법상 개인정보 영향평가 시 고려 사항이 아닌것은?

① 처리하는 개인정보의 수

② 개인정보 제3자 제공여부

❸ 개인정보영향평가기관 능력

④ 민감 정보 또는 고유 식별정보 처리여부

99. 개인정보보호법에서 개인정보처리자는 개인정보 열람요구서를 받은날부터 며칠 이내에 정보주체에게 해당 개인정보를 열람 할수 있도록 알려주어야 하는가?

① 3일

② 5일

③ 7일

❹ 10일

100. 최근 개인정보보호법이 개정이 되었다. 개인정보보호법상 주민번호 수집 후 유출시 얼마의 과징금이 부과되는가?

① 1억

② 3억

❸ 5억

④ 7억