2022년03월13일년 정보보안기사 필기시험 기출문제 답안

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

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

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

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

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

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 취약점 점검 도구에 대한 설명으로 틀린 것은?(문제 오류로 확정답안 발표시 1, 3번이 정답처리 되었습니다. 여기서는 1번을 누르시면 정답 처리 됩니다.)

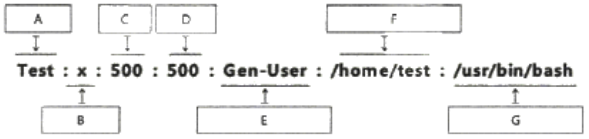
❶ COPS/COPE : 네트워크 기반의 취약점 분석도구로 컴퓨터, 서버, N/W IDS의 보안 취약점을 분석한다.

② Nessus : 네트워크 취약점 점검도구로써 클라이언트-서버 구조로 클라이언트의 취약점을 점검하는 기능이 있다.

③ nmap : 시스템 내부에 존재하는 취약성을 점검하는 도구로써 취약한 패스워드 점검 기능 등이 있다.

④ SAINT : 네트워크 취약점 분석도구로써 HTML 형식의 보고서 기능이 있으며 원격으로 취약점을 점검하는 기능을 가지고 있다.

2. 다음은 passwd 파일 구조를 나타내는 그림이다. “A”는 무엇인가?



① 패스워드

② UID 값

❸ 계정명

④ 설명

3. 버퍼오버플로우 공격을 완화할 수 있는 방법으로 스택과 힙 영역에 쉘코드 등을 실행하지 못하도록 하는 메모리 보호기법에 해당하는 것은?

① ASLR

❷ DEP/NX bit

③ Format String

④ Stack Canary

4. 도구의 기능과 도구명이 짝지어진 것 중 틀린 것은?

① 운영체제별 로그 변조 탐지도구 - Chklastlog

❷ 운영체제별 감사로그 관리도구 - Natas

③ 취약점 진단도구 - SATAN

④ 접근통제관련 로깅 도구 – Syslogd

5. 다음 윈도우(Windows)의 Administrators 그룹에 대한 설명으로 틀린 것은?

① 대표적인 관리자 그룹으로 윈도우 시스템의 모든 권한을 가지고 있다.

② 사용자 계정을 만들거나 없앨 수 있다.

③ 윈도우가 사용 가능한 모든 자원에 대한 권한을 설정할 수 있다.

❹ 해당 컴퓨터 밖의 네트워크에서도 일반 사용자보다 특별한 권한을 행사할 수 있다.

6. 사용자 PC가 언제 부팅되었는지를 확인하기 위해 입력해야 하는 명령어는?

❶ net statistics workstation

② net computer boot time

③ net reboot time

④ net time boot

7. 리눅스 proc 파일 시스템에서 ASLR(Address Space Layout Randomization) 설정값을 확인할 수 있는 파일은 무엇인가?

❶ /proc/sys/kernel/randomize_va_space

② /proc/sys/kernel/watchdog

③ /proc/sys/kernel/panic

④ /proc/sys/kernel/random

8. 다음 중 무결성(Integrity) 검사를 위한 도구가 아닌 것은?

① tripwire

② Fcheck

③ Samhain

❹ prstat

9. 다음 문장에서 설명하고 있는 내용의 괄호 안에 들어갈 올바른 항목은?

> 포렌식 관점에서 파일 시스템 영역은 매우 중요하다고 볼 수 있다. 특히, ( )는(은) 파일, 디렉터리 및 메타 정보 까지 파일 형태로 관리하여 파일과 디렉터리를 분석하여 정보를 알아내는데 유용하다.

① MBR

② BIOS

③ FAT

❹ NTFS

10. 다음 중 프로세스 스케줄링과 관계가 가장 먼 것은?

❶ 페이징(Paging)

② 스와핑(Swapping)

③ 레이스컨디션(Race condition)

④ 환형대기(Circular wait)

11. 다음 문장이 설명한 공격 위협은 무엇인가?

> 해당 취약점이 존재하는 경우 부적절하게 권한이 변경되거나 시스템 동작 및 운영에 악영향을 줄 가능성이 있으므로 "|", "&", ";", "`" 문자에 대한 필터링 구현이 필요함

❶ 운영체제 명령 실행

② XPath 인젝션

③ 디렉터리 인덱싱

④ 정보 누출

12. 웹 쿠키(Cookies)에 대한 설명 중 올바른 것은?

❶ 쿠키는 서버가 아닌 클라이언트에 저장된다.

② 쿠키는 웹 서버에 저장되므로 클라이언트에서 제어할 수 없다.

③ 쿠키는 실행가능한 파일로 바이러스로 동작할 수 있다.

④ 쿠키는 강력한 인증 기능을 제공한다.

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

13. Syslog와 같은 시스템 로그를 주기적으로 스캔하여 어떠한 행위가 발생했는지를 분석하는 시스템 로깅 도구는?

① Nikto

② X-scan

③ N-stealth

❹ Swatch(Simple WATCHer)

14. 다음 문장에서 설명한 공격 위협은 무엇인가?

> 웹 애플리케이션에서 사용자 입력 값에 대한 필터링이 제대로 이루어지지 않을 경우, 공격자는 사용자 입력 값을 받는 게시판, URL 등에 악의적인 스크립트(Javasript, VBScript, ActiveX, Flash 등)를 삽입하여 게시글이나 이메일을 읽는 사용자의 쿠키(세션)를 탈취하여 도용하거나 악성코드 유포 사이트로 Redirect 할 수 있음

① SSI 인젝션

② XPath 인젝션

❸ 크로스사이트 스크립팅

④ 악성 콘텐츠

15. 다음 중 트로이목마 프로그램인 루트킷에 대한 설명으로 가장 부적절한 것은?

① 루트킷의 목적은 자신과 다른 소프트웨어를 보이지 않게 숨기고 사용자가 공격자의 소프트웨어를 인지하고 제거할 가능성을 피한다.

② 윈도우용 루트킷에는 FU-Rootkit, Hxdef100, NTRRootkit 등이 있다.

③ 리눅스용 루트킷에는 Suckit, lrk4, lrk5, adore 등이 있다.

❹ 자기 복제를 하여 다른 컴퓨터에 루트킷을 설치함으로써 그 피해가 커질 수 있다.

16. 관리자 A는 개별그룹으로 신규 사용자 등록(kim, jang) 작업을 어느날 수행한 후 1주일 후에 아래와 같은 시스템 내용을 보고 판단하였다. 올바른 판단은?

```
#ls -al /etc/passwd
      -rw-r--r-- 1 root root 54192 Jan 20 2015 passwd
#ls -al /home/jang
      drwxr-x--- 2 jang jang 120 Jan 27 05:12 .
#ls -al /home/kim
      drwxr-xr-x 2 kim kim 120 jan 20 04:12 .
```

① 패스워드 파일(/etc/passwd)은 누구든지 직접 수정 가능하다.

② 사용자 jang은 /etc/passwd 파일의 권한을 설정할 수 있다.

❸ 사용자 kim은 사용자 계정에 jang 디렉토리에 들어가서 읽을 수도 없고 실행을 못 시킬 것이다.

④ jang은 kim의 패스워드를 바꿀 수 있다.

17. 소유권 없는 파일을 찾는 명령어 및 옵션이 아닌 것은?

❶ find / -ls 2 > /dev/null

② find / \(-nouser –o –nogroup \) -xdev –exec ls –al{}\; 2> /dev/null

③ find / -nouser -print

④ fine / -nogroup –print

18. 다음 문장의 괄호 안에 해당하는 것은 무엇인가?

> 안드로이드는 리눅스 커널을 기반으로 개발되며, 일반 사용자 계정과 루트 계정의 두가지 유형의 사용자 계정으로 나뉜다. 운영체제 변경이나, 특정 명령 실행, 도구 설치 등을 하기 위해서는 루트 권한이 필요하다. ( )은 루트 액세스 권한을 얻어 장치를 완전히 제어하는 것을 말한다. 특히, 기기의 생산지나 판매자가 걸어놓은 제약을 풀기 위해 사용한다.

① 버퍼오버플로우

❷ 루팅

③ 인젝션

④ 접근 제어

19. 다음 중 은폐형 바이러스에 대한 설명으로 가장 적합한 것은?

① 파일이 감염될 경우 그 파일의 내용을 확인할 수 없다.

❷ 감염된 파일의 길이가 증가하지 않은 것처럼 보이게 하고, 감염전의 내용을 보여주어 바이러스가 없는 것처럼 백신과 사용자를 속인다.

③ 바이러스 분석가에게 분석을 어렵게 하고 백신 개발을 지연시키도록 여러 단계의 기법을 사용한다.

④ 백신으로 진단이 어렵도록 바이러스 프로그램의 일부 또는 전체를 암호화한다.

20. 다음 문장에서 리눅스 시스템에 침해 흔적을 조사하기 위해 루트 권한을 가진 setuid를 찾는 명령어로 괄호안에 들어갈 적합한 것은?

```
find / -user root -type f ₩(     ) -exec ls -al { } ₩;
```

❶ -perm –06000 \

② -perm –00100 \

③ -perm –00400 \

④ -perm –00200 \

【2과목】 네트워크 보안 (20문제)

21. 다음 중 VPN에 대한 설명으로 가장 옳지 않은 것은?

① SSL VPN은 웹브라우저만 있으면 언제 어디서나 사용이 가능하다.

② IPsec VPN은 네트워크 계층에서 안전하게 정보를 전송하는 방법이다.

❸ IPsec VPN은 운영방식에 따라 트랜스포트 모드만 지원하고 암호화 여부에 따라 ESP, AH 프로토콜을 사용한다.

④ 기본적으로 SSL VPN과 IPsec VPN은 데이터의 기밀성과 무결성은 동일하며, 단지 데이터의 암호화 구현 방식에 차이가 있다.

22. 다음 스크린드 서브넷 구조에 대한 설명으로 가장 옳지 않은 것은?

① 외부 인터넷 환경에서 접속이 되어야 한다.

② 스크리닝 라우터 사이에 듀얼 홈드 게이트웨이가 위치하는 구조이다.

❸ 다른 방화벽에 비해 설치 및 관리가 쉽다.

④ 서비스 속도가 낮다.

23. 다음 중 Window 계열의 시스템에 대한 포트 스캐닝을 할 수 없는 것은?

① TCP SYN Scan

❷ TCP FIN Scan

③ TCP Connect Scan

④ UDP Scan

24. 바이러스 및 공격으로부터 IoT(Internet of Thing) 기기를 보호할 수 있는 접근제어, 기기 인증, 통신 암호화, 가용성 등과 같은 보안 요구 사항을 알기 쉽게 나타내도록 IoT용 SoA(Service oriented Architecture)는 4계층으로 구성된다. 다음 중 IoT용 SoA 4 계층에 포함되지 않는 것은 어떤 계층인가?

① 센싱 계층

② 네트워크 계층

❸ 트랜스포트 계층

④ 서비스 계층

25. 다음 문장의 괄호 안에 들어갈 알맞은 용어는?

> (　　)는(은) 산업제어시스템(Industrial Control System)에 대한 공정, 기반 시설, 설비를 바탕으로 한 작업공정을 감시하고 제어하는 컴퓨터 시스템으로 최근 이를 대상으로 이루어진 사이버 공격으로 인해 전력공급체계 등 사회기반시설 운영에 피해가 발생하고 있다.

① PLC
❷ SCADA
③ Stuxnet
④ Modbus

26. 네트워크에서 큰 크기의 파일을 전송할 때, 정상적인 경우에 전송가능한 최대 사이즈로 조각화 되어 전송되며, 이때 Fragment Number를 붙여 수신측에서 재조합을 하게 된다. Fragmentation Offset을 위조하여 중복하게 하거나 공간을 두어 재조합을 방해하는 공격은 OSI 7계층 중 어느 계층에서 발생하는 것인가?

① OSI 2 계층
❷ OSI 3 계층
③ OSI 4 계층
④ OSI 5 계층

27. 다음 문장은 모바일 악성코드에 관한 설명이다. 어떤 악성코드에 관한 설명인가?

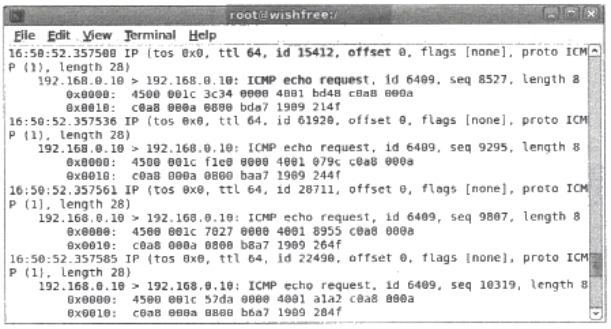
> 저장매체나 인터넷으로 전파되던 악성코드가 휴대전화 통신망으로 전파되기 시작하며, 휴대전화에 저장된 전화번호로 악성코드를 퍼트린다.

① Card trap. A
❷ CommWarrior
③ Hobbles. A
④ Brader

28. 사용자마다 계정 및 패스워드를 설정하고 원격에서 텔넷으로 라우터에 접속할 때, 계정 및 패스워드를 이용하여 로그인할 수 있도록 설정한 것은 무엇인가?

❶ Router(config)#username XXXX password XXXXRouter(config)#line vty 0 4Router(config-line)#login local
② Router#username XXXX password XXXXRouter(config)#line vty 0 4Router(config-line)#login local
③ Router(config)#line vty 0Router(config-if)#username XXXX password XXXXRouter(config-line)#login local
④ Router#username XXXXRouter(config)#password XXXXRouter(config)#line vty 0 4Router(config-line)#login local

29. 다음 화면은 DoS 공격을 실시한 TCP Dump이다. 네트워크 패킷들의 특징으로 보았을 때 무슨 공격을 한 것으로 보이는가?



① UDP 플러딩(flooding)
② SYN 플러딩(flooding)
③ Bonk 공격
❹ Land 공격

30. 다음 중 OSI 7 계층의 데이터 링크 계층과 관련성이 가장 적은 것은?

① 통신 경로상의 지점간(Link-to-Link)의 오류 없는 데이터 전송
② 멀티포인트 회선제어 기능
❸ 데이터 압축 및 암호화
④ 정지-대기 흐름제어 기법

31. Snort에서 Rule에 대한 정보제공을 위해 사용되며, 탐지에 영향이 없는 옵션의 명령어 형식은?

❶ msg

② rawbytes

③ drop

④ reject

32. 다음 문장은 무선랜 환경에서 어떠한 AP(Access Point)를 설명하고 있는가?

> 관리자의 허가없이 비인가적으로 설치되어 외부인 또는 내부인이 악의적인 목적으로 내부 네트워크에 침입 가능한 보안 위협성을 야기시킬 수 있는 AP

① Normal AP

❷ Rogue AP

③ Honeypot AP

④ Ad-hoc AP

33. 자신의 컴퓨터가 인터넷을 통해 목적지를 찾아가면서 구간의 게이트웨이 정보나 걸리는 시간 등을 표시해 줌으로써 인터넷 경로상의 네트워크 경로를 파악할 수 있게 하는 명령어는?

① Tcpdump

② Ping

❸ Traceroute(Tracert)

④ Netstat

34. N-IDS가 수집하여 처리하는 패킷들에서 다음과 같은 형태의 패킷들의 발견되었다. 이에 대한 설명으로 가장 옳은 것은?

출발지 IP	목적지 IP	출발지 포트	목적지 포트	TCP 세그먼트
S1	D1	P1	P2	SYN
S1	D1	P3	P4	SYN
D1	S1	P2	P1	SYN, ACK
S1	D1	P1	P2	RST
D1	S1	P4	P3	SYN, ACK
S1	D1	P3	P4	RST
S1	D1	P5	P6	SYN
D1	S1	P6	P5	RST, ACK

① S1 시스템이 D1 시스템에 대해 SYN flooding 공격을 시도하였다.

❷ S1 시스템이 D1 시스템에 대해 TCP SYN 스캔을 시도하였다.

③ S1 시스템이 D1 시스템에 대해 TCP CONNECT 스캔을 시도하였다.

④ S1 시스템이 D1 시스템에 대해 Stealth 스캔을 시도하였다.

35. 다음 중 세션 하이재킹(Session Hijacking)에 대한 설명으로 가장 옳지 않은 것은?

① 클라이언트와 서버 간의 통신을 관찰할 수 있을 뿐만 아니라 신뢰(trust)를 이용한 세션은 물론 Telent, FTP 등 TCP를 이용한 거의 모든 세션의 탈취가 가능하다.

② 인증에 대한 문제점을 해결하기 위해 도입된 일회용 패스워드(OTP), Token Based authentication, Kerberos(토큰 기반 인증)을 이용한 세션의 탈취도 가능하다.

③ 서버와 클라이언트가 TCP를 이용해서 통신을 하고 있을 때 RST 패킷을 보내 일시적으로 TCP 세션을 끊고, 시퀀스 넘버를 새로 생성하여 세션을 빼앗고 인증을 회피한다.

❹ 실제 DNS 서버보다도 빨리 공격 대상에게 DNS 응답(response) 패킷을 보내 공격 대상이 잘못된 IP 주소로 이름 해석을 하도록 하여 잘못된 웹 접속을 유도하는 공격이다.

36. 다음 문장에서 설명하고 있는 것은 무엇인가?

> 의심스런 트래픽을 탐지할 뿐만 아니라, 위협이 되는 트래픽을 발견하게 되는 어떻게 대응할 지를 미리 정의해 놓고 해당 패킷을 제거한다.

❶ Intrusion Prevention System

② Screened Subnet

③ Knowledge-Base IDS

④ Singature-Base IDS

37. 무선랜 보안에 대한 설명으로 가장 옳지 않은 것은?

① Open System 인증방식은 어떤 무선 단말이라도 AP를 경유하여 인터넷에 접속하도록 허용하는 방식을 의미하여, 실질적인 인증을 하지 않고 무선 단말과 AP간 전달되는 데이터가 평문 형태로 전달된다.

② Shared Key(SK) 인증방식은 무선 단말 사용자가 AP에 설정된 키와 동일한 키를 입력하는 경우 AP를 경유하여 인터넷에 접속을 허용한다.

❸ 무선 단말과 AP간 전달되는 데이터를 암호화하는 경우 WEP 암호 방식이 이용될 수 있으며, 이 방식은 AES 대칭키 암호 알고리즘을 이용하여 매우 높은 강도의 비밀성을 제공한다.

④ RSN(Robust Security Network)에서는 WPA-Personal과 WPA-Enterprise 모드가 있는데, WPA-Personal 모드에서는 미리 설정된 비밀키를 이용하는 반면 WPA-Enterprise 모드에서는 RADIUS 서버를 이용한다.

38. 클라우드 컴퓨팅 보안에 대한 설명으로 가장 옳지 않은 것은?

① 가상화 시스템의 취약점을 상속한다.

② 정보 위탁에 따른 정보 유출의 가능성이 있다.

❸ 집중화로 보안 적용이 용이하다.

④ 자원 공유 및 집중화에 따른 서비스 장애가 발생할 수 있다.

39. 다음 장비 중 네트워크 계층 장비를 바르게 설명한 것은?

① 리피터 : 불분명해진 네트워크 신호세기를 다시 증가시키기 위한 장비이다.

② 더미 허브 : 데이터를 보낼 때 모든 곳에 데이터를 똑같이 복사해서 보낸다.

③ 브리지 : 랜과 랜을 연결하는 네트워크 장치이다.

❹ 라우터 : 서로 다른 프로토콜을 사용하는 네트워크를 연결해주는 장비이다.

40. RIP(Routing Information Protocol)는 Distance Vector 라우팅 알고리즘을 사용하고 매 30초마다 모든 전체 라우팅 테이블을 Active Interface로 전송한다. 원격 네트워크에서 RIP에 의해 사용되는 최적의 경로 결정 방법은 무엇인가?

❶ HoP count

② Routed information

③ TTL(Time To Live)

④ Link length

【3과목】 어플리케이션 보안 (20문제)

41. 클라이언트(웹 브라우저)와 서버(웹 서버)간에 개인정보, 금융정보, 패스워드 등의 중요정보를 안전하게 전송하기 위해 사용되는 암호 채널은?

① S/MIME

② PGP

③ SSH

❹ SSL

42. ebXML의 구성요소가 아닌 것은?

① 비즈니스 프로세스

❷ EDI 문서

③ 핵심컴포넌트

④ 전송, 교환 및 패키징

43. 다음 중 리버스도메인에 대한 설명이 잘못된 것은?

❶ 도메인이름을 IP주소로 변환하기 위해 네임서버에 설정하는 특수 도메인이다.

② IP주소를 도메인 이름으로 변환하기 위해 네임서버에 설정하는 특수 도메인이다.

③ “역질의”라고도 한다.

④ IP주소에 해당하는 숫자와 특수 문자열 in-addr.arpa로 구성되어 있다.

44. 다음 중 SSL(Secure Socket Layter) 프로토콜에 대한 설명으로 잘못된 것은?

① 웹 서버와 브라우저간의 안전한 통신을 위해 넷스케이프사에 의해 개발되었다.

② 세션계층에서 적용되며, 응용계층의 FTP, TELNET, HTTP 등의 프로토콜의 안전성 보장을 위해 사용된다.

❸ SSL 프로토콜은 TCP/IP상의 444/tcp 포트만을 사용하여야 한다.

④ SSL을 사용하기 위해서는 우리가 흔히 사용하는 URL 표기 방식인 “http://*” 대신에 “https://*”을 사용해야 한다.

45. 다음은 보안 기술에 대해 설명한 것이다. 괄호 안에 들어갈 가장 올바른 것은?

> ( )은(는) 디지털 콘텐츠의 불법 복제와 유포를 막고 저작권 보유자의 이익과 권리를 보호해주는 기술과 서비스를 말한다. 전자책, 음악, 비디오, 게임 등등 각종 디지털 콘텐츠의 불법 유통과 복제를 방지하고, 보호된 콘텐츠로 인해 저작권 당사자에게 발생하는 이익을 관리하여 주는 기술과 서비스이다.

❶ DRM(Digital Rights Management)

② 스테가노그래피(Steganography)

③ 디지털 워터마크(Digital Watermark)

④ 보안토큰(Security Token)

46. Spam Assassin은 들어오는 메일을 미리 설정해 둔 패턴에 따라서 스팸으로 의심되면 삭제를 하거나 분리시키는 기능을 하는 스팸필터링 도구이다. 이러한 도구에서 스팸 필터링 분류기준이 아닌 것은?

① 헤더검사

② 본문내용

❸ IP 필터링

④ 첨부파일만 필터링 가능

47. 디지털 증거의 특성을 설명한 것으로 가장 적절하지 않은 것은?

① 내용 자체가 변하지 않는 한 어느 매체에 저장되어도 동일하다.

② 간단한 조작만으로 정보를 변경하거나 삭제할 수 있다.

❸ 컴퓨터 디스크에 항상 안전하게 보관할 수 있다.

④ 대량의 정보가 저장 매체에 저장되고 대량으로 유통될 수 있다.

48. 다음 암호화 구현에 대한 설명으로 잘못된 것은?

① 대칭키 알고리즘 이용시에는 키 길이를 128비트 이상으로 사용하는 것이 안전하다.

② 비대칭키 알고리즘 이용시에는 키 길이를 2,048비트 이상으로 사용하는 것이 안전하다.

❸ 입력된 메시지는 취약한 AES(Advanced Encryption Standard) 대신 안전한 DES(Data Encryption Standard) 알고리즘으로 암호화한다.

④ 해쉬함수 사용시 Salt 값을 사용한다.

49. 다음 웹 서비스 공격 유형으로 적절한 것은?

```
POST / HTTP/1.1
Host: vulnerable-website.com
Content-Length: 20
Transfer-Encoding: chunked
0
GET /home HTTP/1.1
Host: attacker-website.com
Foo: X
```

① XSS

② SSRF

❸ HTTP Smuggling

④ CSRF

50. 다음 문장에서 설명하는 데이터베이스 보안 솔루션 종류는?

> - 조직의 보안정책 구성에 따라 사용허가 및 로깅 여부를 결정한다.
> - 독립된 서버로 구축되기 때문에 이중화 구성을 필요로 한다.
> - 네트워크를 우회하여 접근하는 경우 보안 취약점이 발생한다.
> - 독립된 서버로 다중 인스턴스에 대한 통제가 가능하다.

① 데이터베이스 백업 솔루션

② 데이터베이스 감사 솔루션

③ 데이터베이스 암호화 솔루션

❹ 데이터베이스 접근 제어 솔루션

51. 다음 중 익명 FTP에 대한 보안 대책으로 틀린 것은?

❶ 익명의 사용자에게 쓰기권한을 부여하여 자유롭게 파일 업로드 및 다운로드 하여 사용할 수 있게 한다.

② 반드시 사용하지 않을 경우 서비스를 제거한다.

③ 핵심 디렉토리의 권한을 설정하여 접근하지 못하도록 설정한다.

④ 익명의 사용자가 접근하여 파일을 다운로드 할 수 있으므로 개인정보나 중요정보는 보이자 않도록 마스킹 처리한다.

52. SQL 인젝션(injection) 공격에 대한 설명으로 가장 적절하지 않은 것은?

① 클라이언트의 입력 값을 조작하여 사용자 인증 절차를 우회하는 등의 SQL 문을 생성하여 서버의 DB를 공격하는 기법이다.

② 준비된 명령문(prepared statement) 등을 이용하는 안전한 코딩 기법을 활용하여 SQL 인젝션 공격을 감소시킬 수 있다.

③ SQL 인젝션 공격에 대응하는 방법으로는 클라이언트부터 전달된 입력값을 점검없이 SQL문으로 변환하지 않고 DBMS에서 처리될 수 있는 특수문자가 포함되어 있는지 검사하는 방법이 있다.

❹ SQL 인젝션 공격에 대응하는 방법으로 허용되지 않는 입력값에 대한 블랙리스트 방식으로 차단하는 방법을 사용하는 것이 화이트리스트 방식보다 높은 보안성을 제공한다.

53. 다음 중 관리자 페이지 노출 취약점을 제거하기 위한 점검방법으로 가장 적절하지 않은 것은?

① 추측하기 쉬운 관리자 페이지 경로(/admin, /manager, /system 등) 접근을 시도하여 관리자 페이지가 노출되는지 확인한다.

② 추측하기 쉬운 포트(7001, 8080, 8443, 8888 등) 접속을 시도하여 관리자 페이지가 노출되는지 확인한다.

③ 관리자 페이지 로그인 후 식별된 하위 페이지(/admin/main.asp, /admin/menu.html 등) URL을 새 세션에서 직접 입력하여 인증과정 없이 접근 가능한지 확인한다.

❹ 관리자 페이지 로그인 후 세션이 발행된 페이지의 리퀘스트를 취득하여 일정 시간이 지난 후에 재전송 시 정상 처리가 되는지 확인한다.

54. 전자 입찰 시 필요한 보안 요구사항과 거리가 먼 것은?

① 비밀성

② 공평성

③ 무결성

❹ 동시성

55. 다음 문장에서 설명하는 것은?

> 결제자의 다양한 정보를 수집해 패턴을 만든 후 패턴과 다른 이상 결제를 잡아내고 결제 경로를 차단하는 보안 방식으로, 보안 솔루션에 의존하던 기존 보안과 달리 빅데이터를 바탕으로 적극적인 보안 갱깁을 하는 것이 특징이다.

❶ 이상행위 탐지시스템(FDS)

② 침입탐지시스템(IDS)

③ 블록체인(Blockchain)

④ SET(Secure Electronic Transaction)

56. 다음 중 FTP 서버의 Bounce Attack에 대해 바르게 설명한 것은?

① 분산 반사 서비스 거부 공격(DRDoS)으로 악용할 수 있다.

❷ 접근이 FTP의 PORT command를 악용하여 외부에서 직접 접근 불가능한 내부망 컴퓨터상의 포트에 FTP 서버를 통해 접근할 수 있다.

③ login id를 입력 후 다음 응답 코드를 줄 때까지의 반응 속도 차이를 이용하여 실제 계정이 존재하는지 여부를 추측할 수 있다.

④ active, passive 모드를 임의로 변경할 수 있다.

57. 다음 문장이 설명하는 스팸메일 대응 방안으로 가장 옳은 것은?

> 메일 헤더에 표시된 발송정보가 실제 메일을 발송한 서버와 일치하는지를 비교하여 발송자 정보의 위변조 여부를 파악할 수 있는 기술이다. 발송자의 서버를 DNS에 미리 등록하고 수신자의 서버에 메일이 도착하면 등록된 서버로부터 발신되었는지 확인 후 스팸 메일을 차단하는 기술이다.

① procmail

❷ Sender Policy Framework

③ Sanitizer

④ Spam Assassin

58. DNS 서버가 알고 있는 모든 유형의 레코드를 리턴하고 DNS 관련 DoS(서비스 거부) 공격에 많이 이용되는 질의 유형은?

① NS

❷ ANY

③ A

④ TXT

59. 다음 중 랜섬웨어(Rnasomware)에 대한 설명과 거리가 먼 것은?

① 컴퓨터나 스마트폰에 저장된 파일을 암호화한 뒤 복호화 키를 주는 대가로 돈을 요구하는 악성 프로그램이다.

② Browlock인 경우 수사 기관을 사칭한 뒤 허가받지 않은 사이트를 방문한 대가로 벌금을 지불하도록 유도하는 등의 피해가 발생한다.

❸ 암호 시스템인 RSA 서명을 위조해 암호화한 통신을 가로채는 악성 프로그램이다.

④ Cryptolocker인 경우 사용자의 파일에 강력한 암호화 알고리즘을 적용하여, 복호화 키에 대한 비용을 지불하지 않고는 파일 복구가 불가능하게 만드는 등의 피해가 발생한다.

60. 취약점 제거를 위해 보안사항을 고려하여 안전한 코드를 작성하였다. 다음 코드를 통해 차단할 수 있는 보안취약점은 무엇인가?

```
<%@ taglib prefix="c" uri="
http://java.sun.com/jsp/jstl/core"%>
<%@ taglib uri="
http://java.sun.com/jsp/jstl/functions" prefix="fn"
%>
검색결과 : <c:out value="${fn:content}"/>
```

① SQL Injection 취약점

❷ XSS(Cross Site Scripting)

③ 부적절한 에러처리를 통해 정보 노출

④ 경로 조작(Path Traversal) 취약점

【4과목】 정보 보안 일반 (20문제)

61. 다음 중 메시지 인증방식의 해시(HASH) 함수 사용 기법이 아닌 것은?

① 키 공유 해시함수 사용

② 암호화된 해시함수 사용

③ 공개키 암호체계에서 송신자 개인키 해시함수 사용

❹ 공개키 암호화된 해시함수 사용

62. 다음 문장에서 설명하고 있는 공개키 기반구조의 구성요소는?

> 자신의 도메인내의 사용자와 인증기관들이 준수해야하는 정책을 수립하고, 인증기관의 공개키를 인증하고 인증서, 인증서 취소목록 등을 관리한다.

① 정책승인기관(Policy Approving Authority)

❷ 정책인증기관(Policy Certification Authority)

③ 인증기관(Certification Authority)

④ 등록기관(Registration Authority)

63. KDC를 이용한 키 분배 방식에 대한 설명 중 옳지 않은 것은?

① 사용자들은 사전에 KDC와 마스터 키를 공유해야 한다.

② 사용자의 요청이 있는 경우, KDC는 일회용 세션키를 생성한다.

③ 사용자들 간에는 사전에 공유한 비밀정보가 필요하지 않다.

❹ KDC는 일회용 세션키를 사용자의 공개키로 암호화하여 전송한다.

64. 다음 중 해시함수의 조건이 아닌 것은?

① 압축

② 일방향

❸ 생일공격

④ 충돌회피

65. 다음 중 전자상거래에서 이중서명에 대한 설명으로 잘못된 것은?

① 카드결제에서 계좌정보나 구매물품 목록의 노출을 방지하는 효과가 있다.

❷ 이중서명의 검증은 위변조 여부 확인일 뿐 사용자 인증은 포함되지 않는다.

③ 판매자가 결제정보를 위변조하는 것을 방지한다.

④ 이중서명에 대한 검증은 판매자가 수행한다.

66. Rabin 암호시스템에서 암호문의 제곱근을 구하여 복호화하면 평문 후보가 몇 개 나오는가?

① 1

② 2

③ 3

❹ 4

67. 다음은 접근 통제 모델에 대한 설명이다. ㉠~㉢에 들어갈 말을 옳게 나열한 것은?

> - (㉠) 모델은 주체와 객체의 등급을 비교하여 접근 권한을 부여하는 방식으로서, 관리자만이 정보자원의 분류를 설정하고 변경하는 방법이다.
> - 일반적으로 ACL을 사용하는 (㉡) 모델은 주체의 신분에 근거하여 접근 통제를 적용한다.
> - (㉢) 모델은 (㉠) 모델과 (㉡) 모델의 단점을 보완한 접근 통제 모델로서, 역할에 기반을 두고 접근을 통제하는 모델이다.

① ㉠ RBAC, ㉡ MAC, ㉢ DAC
② ㉠ RBAC, ㉡ DAC, ㉢ MAC
③ ㉠ DAC, ㉡ MAC, ㉢ RBAC
❹ ㉠ MAC, ㉡ DAC, ㉢ RBAC

68. 다음 중 ACL(Acces Control List)에 대한 설명으로 옳지 않은 것은?

① 어떤 사용자들이 ACL 타켓에서 어떤 행위를 할 수 있는지 나타낸다.
② ACL은 관련된 객체에 대하여 접근 행렬에서 열의 내용을 반영한다.
③ 접근 권한의 취소가 쉽다.
❹ 개시자 또는 개시자의 그룹이 다수일 때 편리하다.

69. 다음 중 전자서명의 특징으로 볼 수 없는 것은?

① 위조불가
② 부인불가
❸ 데이터 불법유출 불가
④ 변경불가

70. 8차 기약 다항식으로 만든 LFSR(Linear Feedback Shift Register)의 출력이 가질 수 있는 주기는 어느 것인가?

① 8
② 16
❸ 17
④ 127

71. 다음 중 '커버로스(Kerberos)'의 세 가지 요소에 속하지 않는 것은?(오류 신고가 접수된 문제입니다. 반드시 정답과 해설을 확인하시기 바랍니다.)

❶ 사용자
② 클라이언트
③ SSO(Single Sign On)서버
④ 서버

72. 해시(HASH)된 패스워드를 알아내기 위한 레인보우 테이블 공격을 방어하기 위해 암호에 추가된 임의의 값은 무엇인가?

① Hash
❷ Salt
③ Extender
④ Rebar

73. 다음 중 AES-CCM 운영모드의 특징이 아닌 것은?

① 암호화 블록의 크기가 128bit 이다.
❷ 메시지 인증은 GHASH를 사용한다.
③ 패딩(Padding)이 불필요하다.
④ 인증 암호화 운영모드에 해당된다.

74. 다음 중 키 분배(Key Distriution) 프로토콜과 관련 없는 것은?

① 키 분배 센터(KDC, Key Distriution Center)는 비밀키를 만들어서 대칭키 암호화 통신을 원하는 사람들에게 키를 나누어 주는 역할을 한다.
② 키를 분배 받는 모든 사람은 키 분배 센터(KDC, Key Distriution Center)를 신뢰해야 한다.
③ 같은 키를 소유하는 관련된 사용자들은 관리기관(TA, Trusted Authority)을 제외하고는 정보가 누설되지 않도록 하여 비밀정보를 보호해야 한다.
❹ 키 관리기관은 사내 사용자가 담당하는 역할에 근거하여 자원에 대한 접근을 관리한다.

75. 다음 중 접근통제의 원칙에 대한 설명으로 올바르지 않은 것은? (문제 오류로 확정답안 발표시 모두 정답처리 되었습니다. 여기서는 1번을 누르면 정답 처리 됩니다.)

❶ 시스템 주체에게 권한을 부여할 때에는 조직의 업무효율을 떨어뜨리지 않게 주체의 업무에 필요로 하는 만큼 충분한 권한이 부여되어야 한다.

② 경영자나 관리자 한 사람이 업무의 발생, 승인, 변경, 확인, 배포 등을 처음부터 끝까지 처리할 수 없도록 해야 한다.

③ 보안정책에 따른 접근 허용된 주체와 주체의 접근 가능한 접근통제 규칙을 설정하고, 접근규칙에 해당하지 않는 모든 접근에 대해서는 위반으로 간주한다.

④ 금지된 주체와 객체의 리스트들에 대해서 미리 접근통제 규칙을 설정하고, 접근 통제 규칙에 설정되지 않은 모든 접근에 대해서는 허용한다.

76. 다음 문장은 송신자 "A"가 수신자 "B"에게 메시지를 보낼 때, 발생할 수 있는 보안 위협에 대응하는 보안기술을 설명한 것이다. 각각의 보안서비스로 알맞게 나타낸 것은?

ㄱ. "A"로부터 "B"에게 전송된 메시지가 변경 없이 전송되었는지를 확인하는 보안서비스
ㄴ. 수신자 "B"가 받은 메시지가 분명히 송신자 "A"가 보낸 것인가를 확인하는 보안서비스
ㄷ. 전송 중의 메시지가 공격자에게 노출되는 것에 대응하는 보안서비스

① ㄱ. 기밀성, ㄴ. 인증, ㄷ. 무결성

② ㄱ. 가용성, ㄴ. 무결성, ㄷ. 기밀성

③ ㄱ. 부인봉쇄, ㄴ. 가용성, ㄷ. 무결성

❹ ㄱ. 무결성, ㄴ. 인증, ㄷ. 기밀성

77. 다음 문장은 어떤 인증기법을 설명하고 있는가?

무선 네트워크에서 기기를 인증하는 IEEE표준 인증기법으로서, 사용자 ID 인증과 동적 키 관리 및 계정을 지원한다. PAP, CHAP, RADIUS, PEAP, WEP 등의 프로토콜들이 사용되며, 포트를 기반으로 네트워크 접근을 제어한다.

❶ IEEE 802.1x

② IEEE 802.11i

③ Wifi Protected Acces

④ Extensible Authentication Protocol

78. 다음 중 Kerberos V4의 단점을 개선한 Kerberos V5의 장점으로 옳지 않은 것은 무엇인가?

① Kerberos V4는 암호화 시스템으로 DES 만을 사용하였지만, Kerberos V5는 모든 종류의 암호화 시스템을 사용할 수 있다.

② Kerberos V4는 인터넷 프로토콜(IP) 주소 외에 다른 특정 네트워크 주소를 사용하지 못하였지만, Kerberos V5는 어떤 유형의 네트워크 주소로 사용될 수 있다.

❸ Kerberos V4는 인증서버로부터 클라이언트로 가는 메시지에 패스워드에 기초한 키로 암호화된 내용물을 포함하고 있어 패스워드 공격(Password attacks)에 취약하였으나, Kerberos V5는 메시지에 암호화된 내용을 포함하지 않아 패스워드 공격에 취약하지 않다.

④ Kerberos V4의 티켓 유효기간(Ticket lifetime)의 값은 최대 시간이 제한되어 있었으나, Kerberos V5는 유효기간이 따로 없다.

79. 다음은 무엇에 대한 설명인가?

전자서명과 관련한 대표적인 표준으로 1994년 미국에서 만들어진 표준이다. 이것은 DSA(Digital Signature Algorithm)를 사용하는데, DSA는 슈노어(Schnorr)와 엘가말(ElGamal)의 알고리즘을 기반으로 하여, 서명 생성이나 암호키 생성에서는 SHA-1을 이용한다. NIST가 안전성과 특허 사용료를 이유로 기존의 기업과 정보 기관에서 널리 사용하고 있는 RSA 방식을 배제하고, ElGamal 알고리즘을 사용하여 차별화하고 있다.

① 타원 곡선 전자 서명

❷ DSS

③ RSA

④ KCDSA

80. 다음에서 설명하는 블랙암호 알고리즘은 무엇인가?

입출력 크기(bit) : 128
비밀키 크기(bit) : 128/192/256
참조규격 : KATS KS X.1213-1

① SEED

② HIGHT

❸ ARIA

④ TDEA

【5과목】 정보보안 관리 및 법규 (20문제)

81. 개인정보의 가명·익명처리 시 개인정보 일부 또는 전부를 대체하는 일반화 방법으로 다음 설명에 해당되는 기술은?

① 상하단코딩(Top and bottom coding)

② 제어 라운딩(Controlled rounding)

③ 랜덤 라운딩(Random rounding)

❹ 일반 라운딩(Rounding)

82. 다음 중 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서, 정보보호 관리체계 인증을 의무적으로 받아야 할 대상이 아닌 것은?

① 집적정보통신시설 사업자

② 정보통신서비스 부문 3개월간 일일평균 이용자수 100만 명 이상인 사업자

③ 정보통신서비스 부문 100억원 이상인 사업자

❹ 연간 매출액 또는 세입 등이 1,000억원 이상인 사업자

83. 다음 정보보호 교육과 관련한 설명으로 잘못된 것은?

❶ 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호 교육 계획을 술비하면서, 대상에는 정보보호 관리체계 범위 내 임직원을 포함시켜야 하고, 외부용역 인력은 제외해도 무방하다.

② 교육에는 정보보호 및 정보보호 관리 체계 개요, 보안사고 사례, 내부 규정 및 절차, 법적 책임 등의 내용을 포함하고 일반 임직원, 책임자, IT 및 정보보호 담당자 등 각 직무별 전문성 제고에 적합한 교육내용 및 방법을 정하여야 한다.

③ 연 1회 이상 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 조직 내외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행해야 한다.

④ 교육 내용에는 구성원들이 무엇을 해야 하며, 어떻게 할 수 있는지에 대한 것을 포함해야 하며, 가장 기본적인 보안 단계의 실행에서부터 좀 더 고급의 전문화된 기술에 이르기까지 다양한 단계로 나누어 구성할 수 있다.

84. 다음 클라우드 SaaS 서비스 중 반드시 클라우드 보안인증 표준 등급으로 인증 받아야되는 서비스가 아닌 것은?

① 전자결재 서비스

② 개인정보 유통 보안 서비스

③ 소프트웨어 개발환경(개발, 배포, 운영, 관리 등)

❹ 이메일/메신저 서비스

85. 다음 정보보호 대책 구현에 관한 설명으로 올바르지 않은 것은?

① 효율적인 대책선정을 위해서는 위험분석 결과를 고려하여야 한다.

② 대책 선정에 있어 고려해야 할 중요한 요소 중 하나는 비용이다.

③ 대부분의 대책들이 복합적인 기능 즉 감지, 억제, 방어, 제한, 교정 등을 수행할 수 있기 때문에 복수의 기능을 만족시키는 대책을 선택하는 것이 비용측면에서 효율적이다.

❹ 대책이 사용될 수 있는 영역은 물리적, 기술적 환경에 한정하여야 하며, 관리적 분야 즉 인적, 행정 분야 등에는 적용하지 않는다.

86. 정보통신 서비스 제공자가 이용자의 컴퓨터나 모바일 등에 영리목적의 광고성 프로그램 등을 설치할 경우 준수해야 하는 사항으로 옳지 않은 것은?

① 정보통신서비스 제공자는 영리목적의 광고성 정보가 보이는 프로그램을 이용자의 컴퓨터나 모바일에 설치하려면 이용자의 동의를 받아야 한다.

② 정보통신서비스 제공자는 영리목적의 개인정보를 수집하는 프로그램을 이용자의 컴퓨터나 모바일에 설치하려면 이용자의 동의를 받아야 한다.

③ 정보통신서비스 제공자는 영리목적의 광고성 정보가 보이는 프로그램의 용도와 삭제 방법을 고지하여야 한다.

❹ 정보통신서비스 제공자는 영리목적의 광고성 정보를 편리하게 차단하거나 신고할 수 있는 소프트웨어나 컴퓨터 프로그램을 개발하여 보급하여야 한다.

87. 정보보호 조직 구성원의 역할과 책임에 대한 설명으로 틀린 것은?

① 최고 경영자 : 정보보호를 위한 총괄책임이 있다.

❷ 데이터 관리자 : 정보자산에 대한 책임을 보유한 현업 관리자이다.

③ 프로세스 관리자 : 해당 정보 시스템에 대한 조직의 정보보호 정책에 따라 적절한 보안을 보증할 책임이 있다.

④ 사용자 : 조직의 정보보호 정책에 따라 수립된 절차를 준수할 책임이 있다.

88. 다음 중 개인정보처리자가 내부관리계획을 수립·시행할 때 반드시 포함되어야 하는 사항이 아닌 것은?

① 개인정보보호책임자 지정에 관한 사항

❷ 개인정보취급자 상/벌에 관한 사항

③ 개인정보 암호화 조치에 관한 사항

④ 개인정보처리시스템 접근통제에 관한 사항

89. 다음 중 정보통신기반보호위원회에 대한 설명으로 틀린 것은?

① 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 구성한다.

❷ 정보통신기반보호위원회 위원장은 국무총리가 되고, 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.

③ 정보통신기반보호위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.

④ 정보통신기반보호위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

90. 다음 무장의 내용을 포함하는 지침으로 가장 적합한 것은?

- 책임과 역할
- 업무의 중요도 등급 및 업무영향분석
- 복구전략수립
- 교육 및 훈련
- 사후관리
- 비상연락망

① 문서관리 지침

② 위험평가관리 지침

③ 침해사고대응 지침

❹ 업무연속성관리 지침

91. 다음 중 개인정보 처리자가 정보주체에게 사유를 알리고 열람을 제한허가나 거절할 수 있는 경우로 옳지 않은 것은?

① 법률에 따라 열람이 금지되거나 제한되는 경우

② 다른 사람의 생명, 신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

❸ 공공기관의 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우

④ 공공기관의 학력 및 채용에 관한 시험, 자격 심사에 관한 업무를 수행할 때 중대한 지장을 초래하는 경우

92. 다음 중 정량적 분석의 장점이 아닌 것은?

① 위험평가 결과가 금전적 가치, 백분율, 확률 등으로 표현되어 이해가 쉽다.

② 위험관리 성능평가가 용이하다.

③ 정보자산의 가치가 논리적으로 평가되고 화폐로 표현되어 이해가 쉽다.

❹ 비용대비 이익을 평가할 필요가 없다.

93. 재해복구 시스템의 유형과 복구목표 시간(RTO, Recovery Time Objective)의 설명이 틀린 것은?

① 미러 사이트 : 즉시

② 핫 사이트 : 수시간 이내

③ 웜 사이트 : 수일 ~ 수주

❹ 콜드 사이트 : 수일 ~ 수주

94. 다음 중 개인정보보호 관련 법률과 그 소관 부처가 올바르게 짝지어진 것은?

① 개인정보 보호법 - 법무부

② 위치정보의 보호 및 이용 등에 관란 법률 - 국방부

③ 지방공기업법 - 국토교통부

❹ 전자서명법 – 과학기술정보통신부

95. 다음의 업무를 모두 수행하는 기관은?

- 금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 구축·운영
- 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
- 침해사고가 발생하는 경우 실시간 경보·분석체계 운영

❶ 정보공유·분석센터

② 한국인터넷진흥원

③ 관리기관

④ 지식정보보안 컨설팅업체

96. 정량적 위험분석의 방법론 중 다음 문장에서 설명한 방법으로 알맞은 것은?

이 방법은 위협의 발생빈도를 계산하는 식을 이용하여 위협을 계량하는 방법이다. 과거자료의 획득이 어려울 경우 위험 발생 빈도를 추정, 분석하는데 유용하며, 위험을 경량화 화여 매우 간결하게 나타낼 수 있다. 하지만 이는 기대 손실을 추정하는 자료의 양이 낮다는 단점이 있다.

① 연간예상손실법

② 과거자료 분석법

❸ 수학공식 접근법

④ 확률 분포법

97. 정보보호 관리체계는 정보보호를 스스로, 체계적으로, 지속적으로 하기 위해 3가지 요소가 필요하다. 관련이 적은 것은?

① 정보보호 조직과 인력

② 정보보호 사업의 추진과 예산 배정

③ 정보보호 규정에 기반한 전사적인 정보보호 활동

❹ 정보보호 운영에 필요한 보안 솔루션

98. 다음 중 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업의 내부관리계획의 내용에 포함하지 않아도 될 내용은 무엇인가?

① 개인정보 보호책임자의 지정에 관한 사항

② 개인정보 유출사고 대응 계획 수립·시행에 관한 사항

③ 개인정보의 암호화 조치에 관한 사항

❹ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

99. 인터넷에 공개된 서버를 운영하는 경우 적절하지 못한 보안 방법은?

① 공개서버를 운영하는 경우 이에 대한 보호대책을 수립·이행한다.

❷ 공개서버는 내부 네트워크의 서버팜 영역에 설치하고 침입차단 시스템 등 보안시스템을 통해 보호한다.

③ 공개서버에 개인정보 및 중요정보를 게시하거나 저장하여야 할 경우 책임자 승인 등 허가 및 게시절차를 수립·이행한다.

④ 조직의 중요정보가 웹사이트 및 웹서버를 통해 노출되고 있는지 여부를 주기적으로 확인하여 중요정보 노출을 인지한 경우 이를 즉시 차단하는 등의 적절한 조치를 취한다.

100. 다음 문장은 위험관리를 위한 위험 처리 방안 중 어떤 방안을 설명한 것인가?

> 발생할 위험을 감내할 수 없으므로 위험의 근원이 되는 자산을 제거하거나 해당 업무를 수행하지 않는 방안

① 위험 수용

② 위험 제거

③ 위험 전이

❹ 위험 회피