2018년03월31일년 정보보안기사 필기시험 기출문제 답안

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

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

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

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

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

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 인증관리방법에 해당하는 것은?

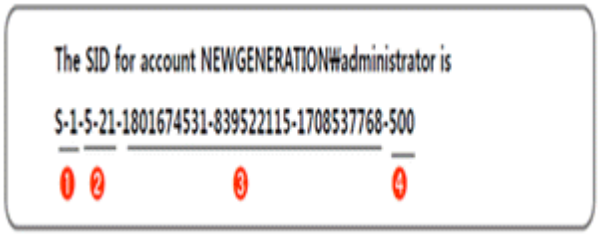
> 다수의 서버가 존재하는 업무환경에서 하나의 시스템에 인증을 성공하게 되면 다른 시스템에 대한 접근 권한을 얻게 되도록 하는 통합인증 시스템

① PAM
② OTP
③ 계정 접속관리(IAM 등)
④ SSO

2. 다음 중 리눅스에서 Process ID(PID) 1번을 가지고 있는 프 로세스는 무엇인가?

① init
② 부트로더
③ OS 커널
④ BIOS

3. 사용자의 고유한 ID에 해당되는 필드는?



① ①번 필드
② ②번 필드
③ ③번 필드
④ ④번 필드

4. SetUID와 SetGID가 설정된 모든 파일을 찾으려는 명령어가 바르게 기술된 것은?

① find / -type f \(-perm -1000 -0 perm -2000 \) -print
② find / -type f \(-perm -2000 -0 perm -4000 \) -print
③ find / -type f \(-perm -100 -0 perm -200 \) -print
④ find / -type f \(-perm -200 -0 perm -400 \) -print

5. 다음 지문에서 설명하고 있는 보안 기술은 무엇인가?

> - 동일한 패스워드를 사용하는 보안상의 취약점을 극복하여 일회성의 서로 다른 패스워드를 생성하게 함으로써 안전한 자상거래를 진행한다.
> - 온라인 뱅킹, 전자상거래, 온라인 게임, 기업 네트워크 등에서 사용한다.
> - 하드웨어적 또는 소프트웨어적으로 구현 가능하다.

① 스마트토큰
② OTP(One-Time Pad)
③ OTP(One-Time Password)
④ 보안카드

6. 다음 지문에 (㉠)에 들어갈 용어로 올바른 것은?

> (㉠)은(는) 프로그램이 실행되면서 동적 할당하여 사용되는 메모리 영역이다. 개발자가 malloc과 같은 메모리 할당 함수를 이용해 프로그램을 개발하였다면, (㉠) 영역을 오버플로우 시켜 특정 코드를 실행하도록 하는 공격이 가능하다.

① 스택(Stack)
② 힙(Heap)
③ 버퍼(Buffer)
④ 스풀(Spool)

7. 취약점 점검용으로 사용되는 도구가 아닌것은?

① SATAN
② Nessus
③ Snort
④ ISS

8. 이메일과 관련되 프로토콜이 아닌것은?

① SMTP
② SNMP
③ POP3
④ IMAP

9. 트로이목마의 특징이 아닌 것은?

① 백도어(Back Door)로 사용할 수 있다.
② 자기복제 능력이 있다.
③ 유용한 프로그램에 내장되어 배포될 수 있다.
④ 정보유출이나 자료파괴 같은 피해를 입힐 수 있다.

10. 다음 지문은 무엇을 설명한 것인가?

> 일반 프로그램에 악의적인 루틴을 추가하여 그 프로그램을 사용할 때 본래의 기능 이외에 악의적인 기능까지 은밀히 수 행하도록 하는 공격을 말한다. 예를들어 사용자 암호를 도출 하기 위해서 합법적인 로그인(login) 프로그램으로 가장하고 정상적인 로그인 순서와 대화를 모방하여 작성될 수 있다.

① 트로이목마(Netbus)

② 매크로 바이러스(Macro virus)

③ 웜(I-Worm/Hybris)

④ 악성 스크립트(mIRC)

11. xfile(파일)에 대한 접근권한을 숫자로 올바르게 표현한 것은?

```
-r-s-wsrwt 1 root root 11 11월 8 13:11 xfile
```

① 6426

② 7537

③ 1537

④ 1426

12. 다음 중 악성코드의 치료 방법이 다른 것은?

① 바이러스

② 웜

③ 트로이목마

④ 스파이웨어

13. 윈도우 시스템에서 사용자 계정과 패스워드 인증을 위해 서버나 도메인 컨트롤러에 증명하는 Challenge & Response 기반의 인증 프로토콜은?

① LSA

② SAM

③ NTLM

④ SRM

14. 다음 중 컴퓨터 바이러스에 대한 설명으로 옳지 않은 것은

① 부트 바이러스란 플로피디스크나 하드디스크의 부트섹터를 감염시키는 바이러스를 말한다.

② 파일 바이러스는 숙주 없이 독자적으로 자신을 복제해 다른 시스템을 자동으로 감염시켜 자료를 유출, 변조, 삭제하거나 시스템을 파괴한다.

③ 이메일 또는 프로그램 등의 숙주를 통해 전염되어 자료를 변조, 삭제하거나 시스템을 파괴한다.

④ 최근 들어 암호화 기법을 기반으로 구현된 코드를 감염시마다 변화시킴으로써 특징을 찾기 어렵게 하는 다형성(Polymorphic) 바이러스로 발전하고 있다.

15. 다음 중 C언어 함수 중에서 버퍼 오버플로우 취약점이 발생하지 안도록 하기 위해 권장하는 함수가 아닌 것은?

① strncat()

② strncpy()

③ snprintf( )

④ gets()

16. net 명령어에 대한 설명으로 잘못된 것은?

① net share : 서버의 모든 공유 리소스 확인 또는 제거

② net user : 서버의 사용자 계정 확인 및 관리

③ net session : 서버에 현재 원격 로그인된 사용자 확인 또는 세션종료

④ net computer : 서버에서 실행하고 있는 서비스 확인 또는 특정 서비스 실행

17. 다음 중 윈도우 운영체제에서 사용하는 파일 시스템이 아닌 것은?

① FAT16

② FAT32

③ EXT3

④ NTFS

18. 다음 중 Telnet 보안에 대한 설명 중 틀린 것은?

① TELNET 세션은 암호화 및 무결성 검사를 지원하지 않는다.

② SSH(Secure Shell)는 암호화를 하지 않는다.

③ 패스워드가 암호화되어 있지 않아 스니퍼를 이용하여 제3자에게 노출 될 수 있다.

④ UNIX 시스템에서 해커가 in.telnetd를 수정하여 클라이언트의 특정 터미널 종류에 대해 인증과정 없이 쉘을 부여할 수도 있다.

19. 유닉스 시스템 명령어는?

> 시스템의 파일 또는 레터리가 만들어질 때의허가권의 기본값을 지정하기 위해서 사용한다. 해당 설정은 모든 계정 사용자들에게 존재하는 값으로서 각 계정 사용자들이 생성하는 파일 또는 디렉터리의 허가권을 결정하기 위한 값이다.

① chmod

② umask

③ chown

④ touch

20. 분석 시 사용될 수 있는 명령어에 대하여 잘못 나열한 것은?

① secure - 사용자 원격접속 정보 - text file - grep

② utmp - 현재 로그인 사용자 정보 - binary file - who

③ pacct - 사용자별 명령 실행 정보 - text file - history

④ wtmp - 최근 로그인 및 접속 호스트 정보 - binary file- last

【2과목】 네트워크 보안 (20문제)

21. 내부 네트워크와 외부 네트워크 사이에 위치하여 외부에서의 침입을 1차로 방어해 주며 불법 사용자의 침입차단을 한 정책과 이를 지원하는 소프트웨어 및 하드웨어를 제공 는 것은?

① IDS(Intrusion Detection System)

② Firewall

③ Bridge

④ Gateway

22. VPN(Virtual Private Network)의 보안적 기술 요소와 거리가 먼 것은?

① 터널링 기술 : 공중망에서 전용선과 같은 보안 효과를 얻기 위한 기술

② 침입탐지 기술 : 서버에 대한 침입을 판단하여 서버의 접근제어를 하는 기술

③ 인증 기술 : 접속 요청자의 적합성을 판단하기 위한 인증 기술

④ 암호 기술 : 데이터에 대한 기밀성과 무결성을 제공하기 위해 사용되는 암호 알고리즘 적용 기술

23. 다음은 DOS 창에서 어떤 명령어를 실행시킨 결과인가?

```
C:WDocuments and SettingswAdministrator>( )
203,252,53,47 203,252,53,47 with 32 bytes of
data:
Reply from 203,25253,47: bytes=32 time<1ms
TTL=128
Reply from 203,252,53,47: bytes=32 time<1ms
TTL=128
Reply from 203,252,53,47: bytes=32 time<1ms
TTL=128
Reply from 203,252,53,47: bytes=32 time<1ms
TTL=128
statistics for 203,252,53,47 | Packets: Sent =
4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = Oms, Maximum = Oms, Average =
Oms
```

① ping

② traceroute

③ date

④ netstat

24. 다음 지문에서 설명하고 있는 침입차단시스템은?

> 외부 네트워크와 내부 네트워크 사이에 하나 이상의 경계 네트워크를 두어 내부 네트워크를 외부 네트워크로부터 분리하기 의 한 구조이다. 비무장지대(DMZ)라고 불리는 경계 네트워크에는 서비스를 위해 외부에서 접속이 많은 시스템을 구성하고 보호할 정보가 많은 시스템은 내부 네트워크 안에 구성한다.

① 스크리닝 라우터(Screening Router)

② 스크린된 호스트 게이트웨이(Screened Host Gateway)

③ 이중 홈 게이트웨이(Dual-homed Gateway)

④ 스크린된 서브넷 게이트웨이(Screened Subnet Gateway)

25. 다음 중 TCP 프로토콜을 사용하여 서버와 클라이언트가 통 신을 수행할 때 서버에서 클라이언트의 접속요청을 기다리는 함수명은?

① bind()

② connect()

③ listen()

④ accept()

26. 다음 설명에 해당하는 서비스거부(DoS) 공격은?

> 헤더가 조작된 일련의 IP 패킷조각(IP Fregments)들을 전송함으 로써 공격이 이루어지며 공격자는 데이터의 일부가 겹치거다. 일부 데이터를 포함하지 않는 패킷 조각들을 전송함으로써 패 킷 재조합 시 공격대상에서 부하를 발생시키는 공격 유형이다.

① Teardrop
② Land attack
③ Syn Flooding
④ Smurf attack

27. 다음지문에서 설명하는 침입 탐지 관련 판정은?

> 공격자가 실제로 시스템에 침입하였으나 침입탐지 시스템은 이를 정상적인 동작으로 인식하여 침입을 제대로 탐지 못한 경우의 판정

① True Positive
② False Positive
③ True Negative
④ False Negative

28. 다음 보기에서 설명하고 있는 공격에 대한 방식은?

> ICMP Echo Request 패킷의 크기를 정상적인 크기보다 크게 만들어 공격 대상 네트워크에 송신하고 네트워크를 통해 라우팅되어 공격 대상 네트워크에 도달하는 과정에서 작은 조각(Fragment)들로 분할된다.

① Teardrop 공격
② Ping of Death 공격
③ UDP Traffic Flooding 공격
④ Tiny Fragmentation 공격

29. 다음 중 방화벽의 기능이 아닌 것은?

① 접근제어
② 인증
③ 로깅 및 감사추적
④ 침입자의 역추적

30. 다음 중 무선랜 구축 시 보안 고려사항으로 가장 적합하지 않은 선택은 무엇인가?

① SSID를 숨김모드로 사용
② 관리자용 초기 ID/Password 변경
③ 무선 단말기의 MAC 주소 인증 수행
④ 보안성이 우수한 WEP(Wired Equivalent Privacy) 사용

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

31. 다음에서 호스트기반 침입탐지시스템(HIDS : host-based IDS)에 의해서 처리되는 이상행위의 유형이 아닌 것은?

① 프로토콜 이상행위(Protocol Anomaly)
② 버퍼오버플로우 취약점 공격(Buffer Overflow Exploits)
③ 권한 확대 취약점 공격(Privilege-escalation Exploits)
④ 디렉터리 검색(Directory Traversal)

32. 지식기반 침입탐지이 아닌 것은?

① 통계적 분석(Statistical Analysis)
② 시그너처 분석(Signature Analysis)
③ 페트리넷(Petri-net)
④ 상태전이분석(State Transition Analysis)

33. 무선랜 보안에 대한 설명으로 옳지 않은 것은?

① WEP 보안프로토콜은 RC4 암호 알고리즘을 기반으로 개발되었으나 암호 알고리즘의 구조적 취약점으로 인해 공격자에 의해 암호키가 쉽게 크래킹되는 문제를 가지고 있다.
② 소규모 네트워크에서는 PSK(PreShared Key) 방식의 사용자 인증이, 대규모 네트워크인 경우에는 별도의 인증서버를 활용한 802.1x 방식의 사용자 인증이 많이 활용된다.
③ WPA/WPA2 방식의 보안프로토콜은 키 도출과 관련된 파 라미터 값들이 암호화되지 않은 상태로 전달되므로 공격자 는 해당 피라미터 값들을 스니핑한 후 사전공격(Dictionary attack)을 시도하여 암호키를 크래킹할 수 있다.
④ 현재 가장 많이 사용 중인 암호 프로토콜은 CCMP TKIP이며 이 중 여러 개의 암호키를 사용하는 'TKIP역 보안성이 더욱 우수하며 사용이 권장되고 있다.

34. IPSec 보안 프로토콜에서 메시지 출처 인증, 메시지 무결성, 메시지 기밀성 서비스를 지원하는 프로토콜과 새로운 IP 헤 더가 추가되는 동작모드가 잘 묶여진 것은?

① ESP 프로토콜, Transport 동작모드

② ESP 프로토콜, Tunnel 동작모드

③ AH 프로토콜, Transport 동작모드

④ AH 프로토콜, Tunnel 동작모드

35. 다음 지문이 설명하고 있는 것은?

> 인터넷이나 다른 네트워크 메시지가 서버에 도착하였을 때, 전달되어야 할 특정 프로세스(응용프로그램)를 인식(구분)하기 위하여 필요하다.

① IP 주소

② 포트번호

③ LAN 주소

④ MAC 주소

36. NAC의 주요기능과 가장 거리가 먼 것은?

① 접근제어/인증 : 네트워크의 모든 IP기반 장치 접근제어

② PC 및 네트워크 장치 통제 : 백신 및 패치 관리

③ 해킹/Worm/유해 트래픽 탐지 및 차단 : 해킹행위 차단 및 완벽한 증거수집 능력

④ 컴플라이언스 : 내부직원 역할기반 접근제어

37. Enterprise Security Management의 구성요소에 대한 설명으로 옳지 않은 것은?

① 에이전트 : 보안 장비에 탑재, 수집된 데이터를 매니저 서버에 전달하고 통제를 받음.

② 매니저 : 에이전트에서 받은 이벤트를 룰에 의해 분석 저장, Console Part에 그 내용을 인공 지능적으로 통보

③ 콘솔 : 매니저에게 받은 데이터의 시각적 전달, 상황 판단 기능

④ 보안 패치 : 다른 환경을 가진 컴퓨터를 대상으로 중앙에서 자동으로 통제 및 제어함으로써 각종 소프트웨어의 취약점에 대한 보안 사고를 사전에 예방

38. 다음 중 제시된 Well Known Port 번호에 해당하는 프로토 콜을 순서대로 가장 적합하게 제시한 것은?

> (가) 22번 포트 (나) 53번 포트 (다) 161번 포트

① (가) SSH, (나) Gopher, (다) NetBIOS

② (가) SSH, (나) DNS, (다) SNMP

③ (가) FTP, (나) Gopher, (다) SNMP

④ (가) FTP, (나) DNS, (다) NetBIOS

39. 어떤 프로토콜에 대한 DoS 공격인가?

> - "목적지 도달 불가(Destination Unreachable)' 메시지가 일부 방화벽에서 상당히 많은 리소스를 소비한다는 사실을 이용한다.
> - 이 DOS 기술은 방화벽을 트래픽으로 뒤덮어버리는 것이 아니라, CPU를 high load 시키기 때문에 효율적이다.

① ICMP

② HTTP

③ TCP

④ SMTP

40. DoS 공격 중 Land 공격이 조작하는 IP 프로토콜의 필드에 해당하는 것은 무엇인가?

① 출발지 주소

② 목적지 주소

③ Time-To-Live 값

④ 헤더의 길이

【3과목】 어플리케이션 보안 (20문제)

41. 포맷스트링 취약점의 직접적인 위험이 아닌 것은?

① 프로그램의 복제

② 프로그램의 파괴

③ 프로세스 메모리 보기

④ 임의의 메모리 덮어쓰기

42. 웹 공격 기법은?

> 게시판의 글에 원본과 함께 악성코드를 삽입하여 글을 읽을 경우 악성코드가 실행되도록 하여 클라이언트의 정보를 유출하는 클라이언트에 대한 공격 기법

① SQL Injection 공격

② 부적절한 파라미터 조작 공격

③ 버퍼 오버플로우 공격

④ XSS(Cross Site Scripting) 공격

43. 아래 그림은 웹 해킹과 관련된 로그이다. 이 그림을 보고 짐작할 수 있는 웹 공격 기법은?

```
10.10.10.1 - - [10/an/2017.00:1803 10900] E
/home/login/login.php?
userid=%27%2008%201%201%20%2D
HTTP/"1.1" 200 970
"http://10.10.10.20/home/login/ogin_form.php"
"Mezia-50 (Windows NT 6.3; WOW64;
Tricent/7.0; v.11.0)
like Cecko)
```

① SQL Injection

② Cross Site Request Forgery

③ Distribute Denial of Service

④ Cross Site Script

44. FTP 전송모드에 대한 설명으로 옳은 것은?

① 디폴트는 active 모드이며, passive 모드로의 변경은 FTP 서버가 결정한다.

② 디폴트는 active 모드이며, passive 모드로의 변경은 FTP 클라이언트가 결정한다.

③ 디폴트는 passive 모드이며, active 모드로의 변경은 FTP 서버가 결정한다.

④ 디폴트는 passive 모드이며, active 모드로의 변경은 FTP 클라이언트가 결정한다.

45. 어떤 종류의 취약점에 대응하기 위한 대책인가?

> PHP의 경우 php.ini 파일에서 allow_url_fopen 옵션을 Off값으로 설정

① 부적절한 파라미터 조작

② 원격지 파일의 명령 실행

③ SQL Injection

④ 쿠키 세션 위조

46. 다음 지문의 설명은 FTP의 어떤 공격 유형에 속하는가?

> - 익명 FTP 서버를 이용하고 그 FTP 서버를 경유하여 호스트를 스캔한다.
> - FTP 포트 명령어를 이용한다.
> - FTP 서버를 통해 임의의 네트워크 접속을 릴레이하여 수행한다.
> - 네트워크 포트를 스캐닝하는데 사용한다.
> - FTP 프로토콜의 취약점을 이용한 공격이다.

① Bounce 공격

② Anonymous FTP 공격

③ TFTP 공격

④ 스니핑 공격

47. 다음에서 설명하는 전자우편의 보안요소로 옳은 것은?

> "중간에서 지나가는 메일을 잡아 놨다가 다시 보내는 공격 방 법을 방지해 주는 기능"

① 메시지 무결성(Message Integrity)

② 메시지 재생 방지(Message replay prevention)

③ 사용자 인증(User Authentication)

④ 송신자 부인 방지(Nonrepudiation of Origin)

48. 다음 중 스팸 필터 솔루션에 대한 설명 중 가장 부적절한 것은?

① 메일 서버 앞단에 위치하며 프락시 메일 서버로 동작한다.

② SMTP 프로토콜을 이용한 DoS 공격이나 폭탄 메일, 스팸메일을 차단한다.

③ 메일헤더 및 제목 필터링은 제공하지만 본문에 대한 필터링은 제공하지 못한다.

④ 첨부파일 필터링 기능을 이용하여 특정 확장자를 가진 파일만 전송되도록 설정할 수 있다.

49. 다음 중 PGP(pretty good privacy)의 기능이 아닌 것은?

① 전자서명

② 기밀성

③ 단편화와 재조립

④ 송수신 부인방지

50. 다음 중 E-mail 전송 시 보안성을 제공하기 위한 보안 전자 우편 시스템이 아닌 것은?

① PGP(Pretty Good Privacy)

② S/MIME(Secure Multipurpose Internet Mail Extension)

③ PEM(Privacy Enhanced Mail)

④ SSL(Secure Socket Layer)

51. 다음 중 FTP 보안대책과 가장 거리가 먼 것은?

① anonymous 사용자의 루트 디렉터리, bin, etc, pub 디렉터리의 소유자와 permission 관리

② root 계정의 ftp 접속 제한

③ 최신 ftp 서버 프로그램 사용 및 주기적인 패치

④ ftp 접근제어 설정 파일인 ftpusers 파일의 소유자를 root로 하고, 접근 허용할 계정을 등록

52. 다음의 지문에서 설명하고 있는 기술들은 전자상거래의 안 전성을 지원할 목적으로 이용되는 보안 프로토콜이다. 빈 칸 에 들어가야 할 적합한 단어는?

> 전자상거래의 안전성을 지원할 목적으로 IPSec(Internet Protoooo Security), SSL (Secure Socket Layer), OTP(One Time Password) 등이 사용된다. 이 중 IPSec은 (㉠) 계층에서 SS은 (㉡) 계 층에서, OTP는 (㉢) 계층에서 각각 동작된다.

① ㉠네트워크, ㉡ 전송, ㉢ 응용

② ㉠네트워크, ㉡ 응용, ㉢ 전송

③ ㉠ 응용, ㉡ 네트워크, ㉢ 전송

④ ㉠ 응용, ㉡ 응용, ㉢ 전송

53. 다음 지문이 설명한는 기술의 명칭은?

> 공공 거래 장부이며 가상 화폐로 거래할 때 발생할 수 있는 해킹을 막는 기술이다.
> - 분산 데이터베이스의 한 형태로, 지속적으로 성장하는 데이터 기록 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고한 되었다.

① 블록체인

② 라이트닝 네트워크

③ ECDSA

④ 인공지능

54. 다음 지문이 설명하고 있는것은?

> 이 솔루션은 인증을 통해 자산 및 사용자를 식별하고, 네트워크 접근권한 등을 부여하여 사용자 접속권한을 제어한다. 인가 받지 않은 단말에 대해 내부 네트워크 접근 통제가 가능하다.

① IPS

② Firewall

③ NAC

④ ESM

55. DNSSEC에 대한 설명 중 가장 적절하지 않은 것은?

① DNS 메시지에 대한 기밀성을 제공한다.

② 서비스 거부 공격에 대한 방지책은 없다.

③ DNS 데이터 위·변조 공격에 대응할 수 있다.

④ 메시지 송신자 인증과 전자서명을 제공한다.

56. SSL 프로토콜에 대한 설명이다. 적절치 못한 것은?

① SSL을 사용하기 위해서는 URL에 "http:// 대신에 "https://"을 사용한다.

② SSL 프로토콜은 Default로 TCP 443 Port를 사용한다.

③ SSL 프로토콜은 암호화 통신을 하기 때문에 침입탐지 방지시스템(IDS/ITS) 등의 보안장비에서 공격 페이로드의 탐지가 쉽다.

④ SSL은 Record Layer와 HandShake Layer로 구분한다.

57. 다음 중 OWASP TOP 10 2017에서 새로 선정된 보안취약 점은?

① 인젝션

② 인증 취약점

③ 크로스사이트 스크립트

④ XXE

58. BYOD 보안솔루션과 가장 거리가 먼 것은?

① NAC

② MDM

③ MAM

④ ESM

59. 다음 보기가 설명하고 있는 공격 방식은?

> 해커가 특정 기업, 기관 등의 HW 및 SW 개발, 공급과정 등 에 침투하여 제품의 악의적 변조 또는 제품 내부에 악성코드 등을 숨기는 행위로 최근에 국내 SW 개발사를 대상으로 SW가 제작되는 단계에서 설치파일 변조 침해사고가 여러 차례 확인된 바 있다. 이러한 사고 예방을 위해서는 개발환경은 외부 인터넷을 차단하여 운영하여야 한다.

① developer chain attack

② supply chain attack

③ stuxnet attack

④ scada attck

60. 다음의 설명 및 조치 내용에 해당하는 취약점은?

> 공격자가 사용자의 cookie 값이나 session 정보를 의 도한 사이트로 보내거나 특정한 동작을 유발하는 스크립트를 글에 삽입하여 사용자가 게시물 등을 클릭할 경우 공격자가 원하는 동작(계좌이체, 물건주문 등)이 실행되게 하는 취약점 (단, 공격 대상자가 사이트에 로그인해 있거나 유효한 cookie, session 정보를 가지고 있어야 공격이 성공할 수 있음)

① SQL injection(sql 명령어 삽입)

② CSRF(크로스사이트 요청변조)

③ RFI(원격 파일 포함)

④ Directory Listing(디렉터리 목록 노출)

【4과목】 정보 보안 일반 (20문제)

61. MAC 정책의 특징에 대한 설명으로 가장 부적절한 것은?

① 객체의 소유주가 주체와 객체간의 접근 통제 관계를 정의

② 보안관리자 주도 하에 중앙 집중적 관리가 가능

③ 접근 규칙수가 적어 통제가 용이

④ 사용자와 데이터는 보안 취급허가를 부여 받아 적용

62. 다음의 지문이 설명하고 있는 접근 통제 보안모델은?

> 이 모델은 데이터 무결성에 초점을 둔 상업용 접근 통제 보안 모델이다. 이 모델에서는 비인가자들의 데이터 변형에 대한 방 지만 취급하며, 주체는 보다 낮은 무결성의 정보를 읽을 수 없 다.(no read down policy)주체는 또한 자신보다 높은 무결성 수준의 객체를 수정할 수 없다.(no wile up policy) 이 모델은 상태 머신(state mechine) 모델에 기반을 두고 있다.

① Bell-LaPadula Model

② Biba Model

③ Clark-Wilson Model

④ Lattice Model

63. Kerberos 프로토콜을 개발함에 있어 요구사항으로 고려 지 않은 특성은?

① 보안성

② 재사용성

③ 투명성

④ 확장성

64. 다음 중 평문과 같은 길이의 키를 생성하여 평문과 키를 비 트단위로 XOR하여 암호문을 얻는 방법에 해당하는 것은?

① 스트림 암호

② 대칭키 암호

③ 공개키 암호

④ 블록 암호

65. 다음 각 지문은 공개키 암호에서 어떠한 보안기능을 제공하 기 위한 것인가?

> (㉠) : 수신자의 공개키로 암호화하여 송신한다.
> (㉡) : 발신자의 개인키로 암호화하여 송신한다.

① ㉠ 비밀성, ㉡ 부인방지

② ㉠ 무결성, ㉡ 비밀성

③ ㉠ 부인방지, ㉡ 무결성

④ ㉠ 가용성, ㉡ 비밀성

66. 다음은 CRL 개체 확장자를 구성하는 필드에 대한 설명이다. 잘못된 설명은?

① Reason Code : 인증서가 갱신된 이유를 나타내기 위해 사용되는 코드

② Hold Instruction Code : 인증서의 일시적인 유보를 지원하기 위해 사용되는 코드

③ Certificate Issuer : 인증서 발행자의 이름

④ Invalidity Date : 개인키 손상이 발생하는 등의 이유로 인증서가 유효하지 않게 된 날짜와 시간에 대한 값

67. 다음은 각 암호 알고리즘이 개발된 배경을 설명한 것이다. 틀린 것은?

① 스트림 암호는 One Time Pad를 실용적으로 구현할 목적으로 개발되었다.

② 블록 암호는 암호문의 위·변조를 막기 위해서 개발되었다.

③ 공개키 암호는 키 관리 문제를 극복하기 위해 개발되었다.

④ 해시 함수는 디지털 서명을 효과적으로 수행하기 위해 개발되었다.

68. 대칭키 암호화 알고리즘으로 묶여진 것은?

① DES, AES, MAC

② RC5, AES, OFB

③ SEED, DES, IDEA

④ Rabin, ECDSA, ARIA

69. 다음 중 대칭키 배송 문제를 해결할 수 있는 방법에 해당하 지 않는 것은?

① 키 배포 센터에 의한 해결

② Diffie-Hellman 키 교환 방법에 의한 해결

③ 전자서명에 의한 해결

④ 공개키 암호에 의한 해결

70. 해시함수의 요구사항과 가장 거리가 먼 것은?

① 계산용이성

② 역방향성

③ 약한 충돌회피성

④ 강한 충돌회피성

71. 다음 중 생체 인식의 요구사항과 가장 거리가 먼 것은?

① 획득성

② 영구성

③ 구별성

④ 유연성

72. 능동적 공격에 해당되지 않는 것은?

① 메시지 변조

② 전송되는 파일을 도청

③ 삽입공격

④ 삭제공격

73. 다음의 공개키 암호에 대한 내용 중 잘못된 것은?

① 하나의 알고리즘으로 암호와 복호를 위한 키 쌍을 이용해 암호화와 복호화를 수행한다.

② 송신자와 수신자는 대응되는 키 쌍을 모두 알고 있어야 한다.

③ 두 개의 키 중 하나는 비밀로 유지되어야 한다.

④ 암호화 알고리즘, 하나의 키와 암호문에 대한 지식이 있어도 다른 하나의 키를 결정하지 못해야 한다.

74. 블록암호에 대한 공격 방식과 가장 거리가 먼 것은?

① 선형공격

② 차분공격

③ 고정점 연쇄공격

④ 전수공격

75. 인수 분해의 어려움을 기초로 한 공개키 암호화 알고리즘은?

① AES

② RSA

③ ECC

④ DH

76. 블록 암호는 기밀성이 요구되는 정보를 정해진 블록 단위로 암호화 하는 대칭키 암호 시스템으로 알고리즘 구조는 파이 스텔(Feistel) 구조와 SPN 구조가 있다. 다음 중 파이스텔 구 조 블록암호가 아닌 것은?

① DES

② AES

③ SEED

④ RC5

77. 다음 인증 기술 중에서 종류가 다른 한 가지는?

① 개체 인증
② 사용자 인증
③ 신원 인증
④ 메시지 인증

78. 이중서명의 특징에 대한 설명으로 옳지 않은 것은?

① 분쟁에 대한 대비를 위해 두 메시지 간의 연관성이 구현되어야 함
② 구매자의 자세한 주문정보와 지불정보를 판매자와 금융기관에 필요 이상으로 전달하지 않아야 함
③ 이중 서명은 SSL에서 도입된 기술로 고객의 카드 정보를 상인에게 전달하면 상인은 그 요청에 유효성을 확인하게 됨
④ 구매자는 최종 메시지 다이제스트를 자신의 개인 서명키로 암호화 하여 이중서명을 생성함

79. 인증서 상태를 관리하고 있는 서버는 유효성 여부에 관하 이 답을 즉시 보내주는 프로토콜은?

① CRL
② OCSP
③ OCRL
④ SSL

80. 그림은 사용자 A가 사용자 B에게 암호문을 전달하는 과정 이다. Key_x와 Key_y가 동일하다면 이에 대한 설명으로 옮 지 않은 것은?



① n명의 사용자가 암호화 시스템에 참여하는 경우 n(n-1)/2)개의 키가 필요하다.
② 암호화 시스템 사용자가 1명씩 증가할 때마다 키의 개수는 기하급수적으로 증가한다.
③ 동일한 키를 사용함으로써 비밀성 및 부인방지의 기능을 제공한다.
④ Decrypt(C)의 알고리즘은 Encrypt(M) 알고리즘의 역순이다.

【5과목】 정보보안 관리 및 법규 (20문제)

81. 정보통신망법에 따라 정보통신서비스 제공자 등은 중요 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장하여야 한다. 다음중 법령에 따른 필수 암호화 저장 대상이 아닌것은?

① 주민등록번호
② 운전면허번호
③ 핸드폰번호
④ 계좌번호

82. 「개인정보 보호법 상 용어 정의로 가장 옳지 않은 것은?

① 개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
② 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
③ 처리: 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위
④ 개인정보관리자: 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인

83. 다음 중 빈 칸에 들어갈 용어의 순서가 가장 적합한 것은?

프로젝트의 범위 · 설정 · 기획 → (㉠) →(㉡) → (㉢) → 프로젝트의 수행 테스트 및 유지 보수

① ㉠ 복구계획 수립, ㉡ 복구전략 개발, ㉢ 사업영향평가
② ㉠ 복구전략 개발, ㉡ 복구계획 수립, ㉢ 사업영향평가
③ ㉠ 사업영향평가, ㉡ 복구계획 수립, ㉢ 복구전략 개발
④ ㉠ 사업영향평가, ㉡ 복구전략 개발, ㉢ 복구계획 수립

84. 정보보호 관리체계 인증제도에 대한 설명으로 가장 적절하지 않은 것은?

① 인증대상은 임의신청자와 의무대상자로 구분되며, 인공의무대상자가 인증을 받지 않으면 과태료 3천만원이 부과된다.
② 임의신청자의 경우 인증범위를 신청기관이 정하여 신청할 수 있으며, 심사기준 및 심사절차는 의무대상자 심사와 동일하다.
③ 정보통신망법 제46조에 따른 집적정보통신시설 사업자는 의무대상자이다.
④ 전년도 직전 3개월간 정보통신서비스 일일평균 이용자수가 10만명 이상인 자는 대상이다.

85. OECD 개인정보보안 8원칙에 포함되지 않는 것은 무엇인가?

① 이용제한의 원칙

② 정보 정확성의 원칙

③ 비공개의 원칙

④ 안전성 확보의 원칙

86. 다음 지문이 설명하는 정보보호 관련 제도는?

> 민간업체 등에서 개발한 정보보호시스템을 국제표준인 ISO 15408 및 ISO 18045를 이용하여 보안기능에 대한 안정성과 신뢰성을 보증함으로써 사용자들이 안심하고 정보보호시스템 을 사용할 수 있도록 지원하는 제도

① 정보보호제품 평가 · 인증 제도

② 정보보호 관리체계 인증 제도

③ 보안적합성 검증 제도

④ 암호모듈 검증 제도

87. 개인정보보호법 제3조(개인정보 보호 원칙)에 대한 내용 중 틀린 것은?

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 기밀성, 무결성 및 신뢰성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

88. 다음은 개인정보의 안전성 확보조치 기준에서의 인터넷 홈 페이지 취약점 점검과 관련한 설명이다. 옳은 것들을 모두 고른 것은?

> a. 인터넷 홈페이지를 통해 고유식별정보를 처리하는 개인정보처리자는 해당 인터넷 홈페이지에 대해 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.
> b. 인터넷 홈페이지의 취약점 점검은 개인정보처리자의 자체인력, 보안업체 등을 활용할 수 있으며, 취약점 점검은 상용도구, 공개용 도구, 자체제작 도구 등을 사용할 수 있다.
> c. 웹 취약점 점검과 함께 정기적으로 웹쉘 등을 점검하고 조치하는 경우 취급 중인 개인정보가 인터넷 홈페이지를 통 해 열람권한이 없는 자에게 공개되거나 유출되는 위험성을 더욱 줄일 수 있다.

① a, b

② b, c

③ a, c

④ a, b, c

89. 위험관리 절차를 순서대로 배열한 것은?

> ㉠ 자산식별 ㉡ 정보보호계획 수립
> ㉢ 정보보호대책 수립 ㉣ 위험 분석 및 평가
> ㉤ 주기적 재검토

① ㉠ - ㉡ - ㉢ - ㉣ - ㉤

② ㉠ - ㉣ - ㉢ - ㉡ - ㉤

③ ㉠ - ㉡ - ㉣ - ㉢ - ㉤

④ ㉠ - ㉣ - ㉡ - ㉢ - ㉤

90. 「개인정보 보호법」에서 규정하고 있는 개인정보 중 민감정보에 해당하지 않는 것은?

① 주민등록번호

② 노동조합 · 정당의 가입·탈퇴에 관한 정보

③ 건강에 관한 정보

④ 사상 · 신념에 관한 정보

91. 현재 존재하는 위험이 조직에서 수용할 수 있는 수준을 넘어 선다면, 이 위험을 어떤 방식으로든 처리해야 된다. 다음의 지문이 설명하고 있는 위험 처리 방식은?

> 보험이나 외주 등으로 위험 처리에 소요될 잠재적 비용을 제 3자에게 이전하거나 할당하는 위험처리 방식

① 위험 수용

② 위험 감소

③ 위험 회피

④ 위험 전가

92. 다음의 보기에서 정보통신기반보호법에서 규정된 주요정보 통신기반시설 지정 시 고려사항이 아닌 것은?

① 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성

② 다른 정보통신기반시설과의 상호연계성

③ 침해사고의 발생가능성 또는 그 복구의 용이성

④ 시설이 취급하고 있는 개인정보의 규모

93. 다음은 개인정보보호법에 따른 개인정보의 파기에 관하여 설명한 것이다. 옳은 것은?

① 개인정보처리자는 처리 목적의 달성여부와 관계없이 동의 기간이 경과해야만 개인정보를 파기할 수 있다.

② 개인정보처리자는 동의기간이 경과하더라도 처리목적이 달성되지 못한 경우에는 개인정보를 계속 이용할 수 있다.

③ 개인정보처리자는 개인정보를 파기해야 하는 사유가 발생했을 때에는 정당한 사유가 없는 한 5일 이내에 개인정보를 파기해야 한다.

④ 복원이 불가능한 방법이란 미래에 개발될 기술도 고려하여 파기 후 개인정보의 복구 가능성을 원천 차단한 방법을 의미한다.

94. 개인정보처리자가 개인정보의 수집 시 정보주체의 동의를 받지 않아도 되는 경우로 가장 적절한 것은?

① 개인정보취급 방침에 명시한 경우

② 경제적, 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우

③ 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

④ 요금 부과를 위해 필요한 경우

95. 다음 보기가 설명하는 위험분석 방법은?

> - 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하며 일정 조건 하에 위협에 대한 발생 가능한 결과들을 추정하는 방법
> - 적은 정보를 가지고 전반적인 가능성을 추론할 수 있고 위험분석과 관리층 간의 원활한 의사소통을 가능하게 한다. 그러나 발생 가능한 사건의 이론적인 추측에 불과하고 정확도, 완성도, 이용기술의 수준 등이 낮을 수 있음.

① 과거자료 분석법

② 확률 분포법

③ 델파이법

④ 시나리오법

96. 다음 지문은 정보통신망법상 전자문서의 정의 규정이다. ( )에 적합한 용어를 찾으시오.

> '전자문서'란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 (A)인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 (B)된 것을 말한다.

① A : 전기적, B: 정형화

② A : 전자적, B: 표준화

③ A : 전기적, B : 표준화

④ A : 전자적, B: 정형화

97. 다음은 정보보호 정책 및 조직과 관련한 설명이다. 옳지 않 은 것은?

① 조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 수립해야 하며, 이러한 정책은 조직과 관련한 것이므로 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 고려할 필요는 없다.

② 조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호 관리체계 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화하여야 한다.

③ 정보보호 관리체계 수립 및 운영 등 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립해야 한다.

④ 최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원을 확보하여야 한다.

98. 다음은 정보보호 교육과 관련한 설명이다. 옳지 않은 것은?

① 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호 교육 계획을 수립하면서, 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 내·외부 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.

99. 다음 중 ISMS(Information Security Management System) 의 각 단계에 대한 설명으로 옳은 것은?

① 계획 : ISMS 모니터링과 검토

② 조치 : ISMS 관리와 개선

③ 수행 : ISMS 수립

④ 점검 : ISMS 구현과 운영

100. 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대한 보호대책의 미흡으로 국가안전보장이나 경제사회 전반에 피해가 우려될 수 있으므로 기반시설을 지정하여야 한다. 다음 중 주요정보통신기반시설이 아닌 것은 무엇인가?

① 전력, 가스, 석유 등 에너지 · 수자원시설

② 인터넷포털, 전자상거래 등 인터넷시설

③ 도로·철도·지하철·공항·항만 등 주요 교통시설

④ 방송중계 국가지도통신망 시설