2016년09월24일년 정보보안기사 필기시험 기출문제 답안

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

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

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

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

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

CBT 기출문제

전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!

Download on the App Store

GET IT ON Google Play

【1과목】 시스템 보안 (20문제)

1. 다음의 공격도구들이 공통적으로 제공 기능은?

- John the Ripper
- Wfuzz
- Cain and Abel
- THC Hydra

① Brute Force 공격

② Web 공격

③ 스니핑 공격

④ 사회 공학 공격

2. 괄호 안에 들어갈 말로 옳은 것은?

운영체제의 구조는 이중 모드(dual mode)로 되어 있는데, 이는 사용자 모드(user mode)와 커널 모드(kernel mode, 또는 운영체제 실행 모드)이다. 이 중 사용자 모드는 특권 명령어를 사용할 수 없으며, 이러한 경우에 사용자 프로세스는 운영체제에게 도움을 요청하게 되는데, 이를 ( )(이)라 한다. 즉 ( )는(은) 실행 중인 프로그램과 운영체제 사이에 인터페이스를 제공하는 것이다.

① 시스템 관리(system management)

② 시스템 호출(system call)

③ 프로세스 관리(process management)

④ 스케줄링(scheduling)

3. 다음을 운영체제의 5계층에 따라 계층별로 올바르게 나열한 것은?

① 동기화 및 프로세서 스케줄링 담당
② 파일의 생성과 소멸, 파일의 열기와 닫기, 파일의 유지 및 관리 담당
③ 메모리의 할당 및 회수 기능 담당
④ 주변장치의 상태파악과 입출력 장치의 스케줄링
⑤ 프로세스의 생성, 제거, 메시지 전달, 시작과 정지 등의 작업

① 1계층(①)-2계층(③)-3계층(⑤)-4계층(④)-5계층(②)

② 1계층(④)-2계층(③)-3계층(⑤)-4계층(①)-5계층(②)

③ 1계층(②)-2계층(④)-3계층(⑤)-4계층(③)-5계층(①)

④ 1계층(③)-2계층(①)-3계층(②)-4계층(④)-5계층(⑤)

4. 휘발성 증거들의 수집 순서를 우선순위가 높은 것부터 올바르게 배열한 것은?

① 레지스터와 캐시, 시스템 메모리의 내용, 임시파일시스템, 디스크의 데이터

② 시스템 메모리의 내용, 레지스터와 캐시, 임시파일시스템, 디스크의 데이터

③ 레지스터와 캐시, 임시파일시스템, 시스템 메모리의 내용, 디스크의 데이터

④ 레지스터와 캐시, 디스크의 데이터, 시스템 메모리의 내용, 임시파일시스템

5. UNIX 또는 리눅스 시스템에서 똑같은 작업을 사용자가 지정된 시간에 반복 작업하기 위해서 cron 테이블을 작성한다. 만약 사용자가 매주 토요일 오전 10시 정각에 'mytest'라는 프로그램을 주기적으로 수행시키기 위해 작성한 cron 테이블 내용 중 맞는 것은?

① 0 10 6 * * mytest

② 0 10 * * 6 mytest

③ 0 10 * 6 * mytest

④ 0 10 6 * * mytest

6. 사용자가 자신의 홈 디렉터리 내에서 새롭게 생성되는 서브파일에 디폴트 파일 허가권을 파일 소유자에게는 읽기와 쓰기, 그룹과 other에게는 읽기만 가능하도록 부여하고 싶다. 로그인 셸에 정의해야 하는 umask의 설정값은 어느 것인가?

① umask 644

② umask 022

③ umask 330

④ umask 033

7. Cron에 대한 설명으로 옳지 않은 것은?

① 정기적인 작업을 지정시간에 처리하기 위해 사용한다.

② Cron에 의해 수행된 작업에 관한 로그는 기본적으로 /etc/default/cron 파일에 저장된다.

③ 시간별, 일별, 주별, 월별로 작업을 정의할 수 있다.

④ /etc/crontab 파일에 처리할 작업 목록이 정의되고 저장되어 있다.

8. 개인 PC 보안에 관한 점검 사항으로 적절하지 않은 것은?

① 디렉터리(데이터 공유), 패스워드 미설치 점검

② 바이러스 백신을 활용한 바이러스 웜 점검

③ 화면 보호기 암호 설정

④ 라우팅 테이블 점검

9. 하드웨어와 소프트웨어 설치 드라이버 설정에 대한 정보를 포함하고 있는 윈도우 레지스트리 키(Registry Key)는?

① HKEY_LOCAL_MACHINE

② HKEY_CLASS_ROOT

③ HKEY_CURRENT_USER

④ HKEY_USERS

10. 다음 xinetd에 대한 설정으로 틀린 설명은?

```
[root@forensics xinetd.d]# cat telnet
service telnet
{
disable = no
flags = REUSE
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.telnetd
log_on_failure += USERID
}
```

① 현재 telnet 서비스는 동작 중에 있다.

② wait 값이 no인 것으로 보아 single thread로 실행됨을 의미한다.

③ 소켓 형태는 스트림 기반의 서비스이다.

④ 해당 서비스를 실행할 데몬 프로그램은 /user/sbin/in.telnetd 이다.

11. 버퍼 오버플로우 공격의 대응수단으로 적절하지 않은 것은?

① 스택상에 있는 공격자의 코드가 실행되지 못하도록 한다.

② 프로세스 주소 공간에 있는 중요 데이터 구조의 위치가 변경되지 않도록 적재 주소를 고정시킨다.

③ 함수의 진입(entry)과 종료(exit) 코드를 조사하고 함수의 스택 프레임에 대해 손상이 있는지를 검사한다.

④ 변수 타입과 그 타입에 허용되는 연산들에 대해 강력한 표 기법을 제공하는 고급수준의 프로그래밍 언어를 사용한다.

12. 다음 중 가장 바르지 않은 것은?

① wtmp: 사용자들이 로그인, 로그아웃한 정보를 가지고 있다.

② pacct: 사용자가 로그인한 후부터 로그아웃할 때까지의 입력한 명령과 시간, 작동된 tty 등에 대한 정보를 가지고 있다.

③ utmp: 시스템에 현재 로그인한 사용자들에 대한 상태 정보를 가지고 있다.

④ btmp: 사용자별로 가장 마지막에 로그인한 시간과 접속 IP, tty 등에 대한 정보를 가지고 있다.

13. 악성코드의 종류는 무엇인가?

> 이 악성코드는 컴퓨터 시스템에 저장된 사용자 문서 파일을 암호화하거나 컴퓨터 시스템을 잠그고 돈을 요구하는 악성 프로그램으로 전자메일이나 웹사이트 등 다양한 경로를 통해 감염된다. 이러한 악성코드로는 크립토월, 크립토락커, CoinVault 등이 대표적으로 알려져 있다.

① 바이러스

② 루트킷

③ 웜

④ 랜섬웨어

14. 스택 버퍼 오버플로우 공격의 수행절차를 순서대로 바르게 나열한 것은?

> ㄱ. 특정 함수의 호출이 완료되면 조작된 반환 주소인 공격셸 코드의 주소가 반환된다.
> ㄴ. 루트 권한으로 실행되는 프로그램 상에서 특정 함수의 스택 버퍼를 오버플로우시켜서 공격 셸 코드가 저장되어 있는 버퍼의 주소로 반환 주소를 변경한다.
> ㄷ. 공격 셸 코드를 버퍼에 저장한다.
> ㄹ. 공격 셸 코드가 실행되어 루트 권한을 획득하게 된다.

① ㄱ→ㄴ→ㄷ→ㄹ

② ㄱ→ㄷ→ㄴ→ㄹ

③ ㄷ→ㄴ→ㄱ→ㄹ

④ ㄷ→ㄱ→ㄴ→ㄹ

15. Process ID(PID) 1번을 가지고 있는 프로세스는 무엇인가?

① init

② 부트로더

③ OS 커널

④ BIOS

16. 백도어를 사용하여 접근하는 경우 정상적인 인증을 거치지 않고 관리자의 권한을 얻을 수 있다. 이에 대한 대응책으로 옳지 않은 것은?

① 주기적으로 파일의 해쉬값을 생성하여 무결성 검사를 수행한다.

② 불필요한 서비스 포트가 열려있는지 확인한다.

③ 윈도우의 작업관리자나 리눅스 시스템의 ps 명령어를 통해 비정상적인 프로세스가 있는지 확인한다.

④ promiscuous로 변경되어 있는지를 주기적으로 검사한다.

17. 해킹기법과 그 대응책에 대한 설명으로 옳지 않은 것은?

① Buffer Overflow 공격: 프로그램밍 시 경계값 검사를 적용하고 최신 운영체제로 패치

② Format String Bug 공격: 데이터 형태(포맷 스트링)에 대한 명확한 정의

③ Denail of Service 공격: MAC 주소값을 고정으로 설정

④ SYN Flooding 공격: SYN Received의 대기시간을 축소

18. 다음 설명에 해당되는 공격 유형은?

> 버그가 가고 있는 System Program과 침입자의 Exploit Program이 거의 같은 시간대에 실행되어 System Program이 갖는 권한으로(Set-User ID가 붙은 경우 Root, Bin 등…) File에 대한 Access를 가능하게 하는 방법을 말한다.

① Stack Based Buffer Overflow

② Format String

③ Race Condition

④ Synchronization

19. 리눅스 서버에서 외부의 모든 Ping of Death 공격을 방어하기 위하여 리눅스의 기본 커널 옵션을 조정하려고 한다. 적절한 명령어는?

① sysctl -w net.ipv4.icmp_echo_ignore_all=0

② sysctl -w net.ipv4.icmp_echo_ignore_all=1

③ sysctl -n net.ipv4.icmp_echo_ignore_broadcasts=1

④ sysctl -n net.ipv4.icmp_echo_ignore_broadcasts=0

20. 다음은 크래커 A가 남긴 C소스 코드와 바이너리 파일이다. 이에 대한 설명으로 적합한 것은?

```
[user@localhost test]$ ls -l
total 20
-rwsr-xr-x 1 root 13923 Oct 7 21:13 test
-rw-rw-r- 1 root root 88 Oct 7 21:12 test. C
[user@localhost test]$ cat test.c
#include
void main()
{
setuid(0);
setgid(0);
system("/bin/bash");
}
```

① setgid 시스템 콜의 인자를 0으로 준 것으로 보아 Race Condition 기법의 공격이다.

② /bin/sh를 실행시키는 것으로 보아 Sniffing 기법이다.

③ setuid 시스템 콜의 인자가 0이고 컴파일된 바이너리 파일의 퍼미션이 4755인 것으로 보아 루트 권한을 탈취하는 백도어이다.

④ main 함수의 리턴형태가 void 이므로 Format String Attack으로 보인다.

【2과목】네트워크 보안 (20문제)

21. 다음 지문에 해당하는 ICMP 오류 메시지는?

> 데이터그램(Datagram)dl 라우터를 방문할 때, 이 필드의 값은 1씩 감소되며, 이 필드 값이 0이 되면 라우터는 데이터그램을 폐기한다. 그러나 데이터그램이 폐기될 때 라우터는 오류 메시지를 원 발신지에 송신한다.

① 목적지 도달 불가능

② 시간 경과

③ 매개변수 문제

④ 발신지억제

22. 네트워크에 존재하는 많은 종류의 장비 중 리피터(Repeater)에 대한 설명으로 잘못된 것은?

① 물리계층에서 동작하는 장비이다.

② 감쇄되는 신호를 증폭하고 재생하여 전송한다.

③ 연속적으로 2개 이상의 케이블을 연결함으로써 케이블의 거리 제한을 극복한다.

④ 이더넷 멀티포트 리피터(Ethernet Multi-port Repeater) 또는 연결 집중 장치라고도 불린다.

23. 다음 중 전문가 시스템(Expert System)을 이용한 IDS에서 사용되는 침입 탐지기법은?

① Behavior Detection

② State Transition Detection

③ Knowledge Based Detection

④ Statistical Detection

24. 다음 중 프로토콜과 포트번호의 연결이 옳지 않은 것은 무엇인가?

① HTTP - 80

② SMTP - 25

③ DNS - 53

④ TELNET - 20

25. 다음 지문이 설명하는 것은?

- 엔드포인트(단말, 내부사용자) 보안 문제를 해결하기 위해 고려된 방식이다.
- 접근제어를 위한 사용자 인증과 백신 관리, 패치 관리 등 무결성 체크와 같은 핵심 기능이 존재한다.

① Network Access Control

② Network Management System

③ Enterprise Security Management

④ Unigied Threat Manager

26. 다음 지문에서 설명하는 것은?

침입탐지시스템은 Telnet 접속 시 사용되는 계정이나, 메일의 첨부파일의 형태, 웹서버에 전송되는 패킷의 내용 등에서 미리 정의된 공격자 패턴과 일치하는지의 여부에 따라 침입여부를 결정하는 이 탐지방법을 사용하고 있다.

① Signatur-based detection

② Anomaly-based detection

③ Network Behavior detection

④ Stateful Protocol detection

27. 서브넷팅에 대한 설명 중 틀린 것은?

① 네트워크 세그먼트로 나눈 개별 네트워크를 말한다.

② 서브넷 마스크는 네트워크 ID와 호스트 ID를 구분 짓는 역할을 한다.

③ 서브넷 마스크는 32비트의 값을 가진다.

④ 각각의 서브넷들이 모여 물리적인 네티워크를 이루어 상호 접속을 수행한다.

28. 다음 중 무결성 점검을 위해 사용하는 프로그램은?

① tripwire

② tcpdump

③ hunt

④ dsniff

29. 다음 중 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고오류를 알려주는 프로토콜은 어느 것인가?

① SMTP

② SSH

③ ICMP

④ IGMP

30. 다음 중 SIEM에 사용되는 프로그램과 가장 거리가 먼 것은?

① SPLUNK

② QRadar

③ Arcsight

④ EnCase

31. VPN 터널을 위해 사용할 수 없는 것은?

① IPSec

② PPTP

③ SSL

④ RTP

32. 다음 지문은 어떤 종류의 ICMP 메시지를 설명하는 것인가?

데이터를 보내는 호스트에게 IP 데이터그램의 라우터 집중 현상에 의해 패킷이 손실되고 있음을 알리기 위해 라우터가 보내는 메시지

① Source Quench.

② Echo Request

③ Echo Reply

④ Destination Unreachable

33. 네트워크를 통해 무선 LAN을 공격하기 위한 기술적 공격 방 식이 아닌 것은?

① 구성 설정 초기화

② 무선 전파 전송 방해

③ 불법 AP를 통한 전송 데이터 수집

④ 암호화 되지 않은 통신 데이터 도청

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

34. 다음은 IPSec의 AH 프로토콜이 하는 역할에 대한 설명이다. 맞는 것은?

① 라우터와 라우터 간의 IP 패킷을 암호화한다.

② 단말과 단말 간의 IP 패킷을 암호화한다.

③ 단말과 라우터 간의 IP 패킷에 대한 송신 인증 및 무결성 서비스를 계공한다.

④ 단말과 라우터 간의 IP 패킷에 대한 송신 인증, 무결성 그리고 암호화 서비스를 제공한다.

35. 다음은 IPSec 터널모드에서 IP 패킷을 암호화하고 인증 기 능을 수행하는 그림이다. ㉠과 ㉡에 추가되는 헤더 정보를 바르게 연결한 것은?

		IP Header	data
		↓	↓
ㄱ	ㄴ	IP Header	data

① new IP header ESP/AH

② ESP/AH new IP header

③ IKE header new IP header

④ new IP header IKE header

36. DDoS 긴급 대응 절차 순서를 올바르게 나열한 것은?

가. 모니터링	나. 상세분석	다. 공격탐지
라. 초동조치	마. 차단조치	

① 라, 다, 가, 나, 마

② 라, 가, 마, 다, 나

③ 가, 다, 라, 나, 마

④ 가, 다 나, 라, 마

37. 전통적인 응용 게이트웨이 방식의 방화벽에 대한 설명 중 옳지 않은 것은?

① 외부 네트워크에 연결된 컴퓨터는 내부 네트워크에 연결된 컴퓨터에 직접 연결되지 않고 프락시를 통해서만 연결된다.

② 외부 네트워크와 내부 네트워크 간에 전달되는 모든 데이터는 하나의 프락시를 통해 처리된다.

③ 프락시를 통해 2개의 서로 다른 연결이 설정되므로 외부 네트워크에 연결된 사용자들에게 내부 네트워크 정보를 숨기는 효과가 있다.

④ 응용 계층에서 처리하는 데이터에 대한 점검 기능을 수행하므로 패킷 필터링 수준의 방화벽보다 우수한 보안 서비스를 제공한다.

38. 다음 중 패킷 필터링 시에 패킷 헤더에서 검출할 수 있는 정보가 아닌 것은?

① 목적지 IP 주소

② TCP/UDP 소스 포트

③ ICMP 메시지 타입

④ 패킷의 생성 시간

39. 지문의 특성을 갖는 공격 방법은 무엇인가?

> 에이전트 설치의 어려움을 보완한 공격 기법으로 TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용한 공격으로 정상적인 서비스를 제공 중인 서버를 Agent로 활용하는 공격 기법이다.

① Botnet
② DRDoS
③ APT
④ Sniffing

40. 다음의 공격 방법을 방어하기 위한 침입차단시스템 유형으로 가장 적절한 것은?

> 침입차단시스템을 우회하기 위하여 침입차단시스템 내부망에 있는 시스템의 서비스 요청을 받은 것으로 가장하여 패킷을 전송한다.

① 응용레벨 게이트웨이(Application level Gateway)
② 회로레벨 게이트웨이(Circuit level gateway)
③ 패킷 필터링 라우터(Packet giltering router)
④ 상태검사 패킷 필터(State inspection packet filter)

【3과목】 어플리케이션 보안 (20문제)

41. 다음 중 이메일(E-mail) 송수신을 위해서 사용되는 프로토콜로 가장 적절하지 않은 것은?

① SMTP
② POP3
③ IMAP
④ SBMP

42. 전자 상거래에 활용되는 암호화에 대한 설명이 적당하지 않은 것은?

① 전자상거래에 사용되는 암호시스템은 공개키보다 대칭키를 사용하는 시스템이다.
② 전통적으로 정보의 보안을 유지하는 가장 효과적인 방법은 암호화를 도입하는 것이다.
③ 암호화(Encryption)는 데이터를 읽을 수 없는 형태로 만드는 것을 의미한다.
④ 암호를 이용한 암호 방법은 자격이 없는 임의의 방문자로부터 정보를 숨김으로써 개인의 프라이버시를 보장한다는데 의의가 있다.

43. 파일 업로드 취약점을 이용한 공격으로 가장 많이 사용되는 유형은 무엇인가?

① SQL 삽입 공격
② 웹셸 공격
③ CRSF 공격
④ 쿠키 하이재킹 공격

44. 다음 OTP 생성 방식은 무엇인가?

> OTP 토큰과 OTP 인증서버의 동기화된 인증 횟수(Counter)를 기준으로 사용자가 인증을 요청할 때마다 OTP 값을 생성한다.

① 질의·응답 방식
② 이벤트 동기화 방식
③ 시간 동기화 방식
④ S/KEY 방식

45. 다음 중 웹 브라우저와 웹 서버 간에 안전한 정보 전송을 위해 사용되는 암호화 방법으로 가장 적절한 것은?

① SSH(Secure Shell)
② PGP(Pretty Good Privacy)
③ SSL(Secure Socket Layer)
④ S/MIME(Secure Multipurpose Internet Mail Extension)

46. 다음 전자메일 프로토콜은 무엇인가?

> - 메일을 안전하게 전송하기 위한 프로토콜로서 디지털 서명과 메시지 암호화 기능을 제공한다.
> - 공개키 인증서는 반드시 X.509 형식을 사용한다.

① IMAP
② SMTP
③ S/MIME
④ PGP

47. 다음 지문이 설명하는 공격기법은 무엇인가?

> 게시판이나 웹 메일 등에 악의적인 스크립트를 삽입함으로써 사용자의 쿠키 및 기타 개인정보를 특정 사이트로 전송하게하거나 악성파일을 다운로드하여 실행하도록 하는 공격

① 파라미터 변조 공격

② 쿠키/세션 위조

③ XSS(Cross Site Scripting)

④ SQL Injection

48. 다음 중 FTP 명령의 수행 기능을 올바르게 설명한 것은?

① RMD: 파일 다운로드

② STOR: 원격지 파일 저장

③ CWD: 디렉터리 생성

④ MKD: 디렉터리 목록 보기

49. 입력 값에 대한 검증을 누락하거나 부적절한 검증, 데이터의 잘못된 형식지정 등으로 인해 발생할 수 있는 보안 취약점과 가장 거리가 먼 것은?

① SQL 삽입

② 크로스사이트 스크립트

③ CMD 삽입

④ 경쟁 조건

50. 다음 중 커버로스(Kerberos)의 특징이 아닌 것은?

① 재생공격을 예방할 수 있다.

② 데이터의 무결성을 제공한다.

③ 타임스템프는 필요하지 않다.

④ 대칭키를 이용한 기밀성 제공이 가능하다,

51. 메일 서버 서비스에 대해서 할 수 있는 서버 공격 기법은 무엇인가?

① Active Contents 공격

② 트로이목마 공격

③ 서비스 거부(DoS, DDoS) 공격

④ Mail Bomb

52. 컴퓨터 메모리는 사용되는 방식에 따라 여러 개의 영역으로 나누어 생각할 수 있는데 프로그램 실행 중 함수 호출시 생성되는 지역변수와 매개변수가 저장되었다가 함수가 종료되 면 시스템에 반환되는 영역은 무엇인가?

① Text 영역

② Data 영역

③ Stack 영역

④ Heap 영역

53. 다음 설명에 해당하는 것은?

> - 송신자 측에서는 전송할 이메일femaiO에 대한 전자서명 생성에 사용되며, 수신자 측에서는 이메일에 포함된 전자서명의 확인 작업에 사용된다.
> - 비대칭 암호 기술을 사용한다.
> - 이메일 애플리케이션에 플러그인(plug-in) 방식으로 확장이 가능하다.
> - 최초 개발자는 '필 짐머만(Phil 2mmermann)'이다.

① PGP(Pretty Good Privacy)

② PKI(Public-Key Infrastructure)

③ MIME(Multipurpose Internet Mail Extensions)

④ IKE(Internet Key Exchange)

54. S/MIME이 수행하는 기능이 아닌 것은?

① 메시지 기밀성 보호

② 메시지 무결성 보호

③ 송신자 인증

④ 악성 메일 차단

55. 다음 중 포맷 스트링 취약점 점검 툴이 아닌 것은?

① gdb

② objdump

③ ltrace

④ tcpdump

56. 다음은 웹서버 로그에서 볼 수 있는 상태코드로 HTTP/1.1 에서 정의한 것이다, 이 중 잘못된 것은?

① 304 : Not Modified

② 403 : Forbidden

③ 404 : Method Not Allowed

④ 504 : Gateway Timeout

57. 다음 중 SSO(Single Sign On)의 장점이 아닌 것은?

① 운영 비용 감소

② 관리자 서버의 업무 부담이 상대적으로 적다,

③ 사용자 편의성 증가

④ 중앙 집중 관리를 통한 효율성 증대

58. 아래 지문은 크로스사이트 요청 우위조(CSRF)의 보안대책을 설명한 것이다. 다음 중 ( ) 안에 들어갈 내용이 맞게 구성 된 것은?

> 입력화면 폼 작성 시 (A) 방식보다는 (B) 방식을 사용하고 입력화면 폼과 해당 입력을 처리하는 프로그램 사이에 (C)을(를) 사용하여, 공격자의 직접적인 URL 사용이 동작하지 않도록 한다. 특히, 중요한 기능에 대해서는 (D)과(와) 더불어 (E)를(을) 유도한다.

① (A) : GET, (B) : POST, (C) : 세션, (D) : 사용자 세션검증, (E) : 재사용

② (A) : POST, (B) : GET, (C) : 세션, (D) : 쿠키 식별, (E) : 재사용

③ (A) : POST, (B) : GET, (C) : 토큰, (D) : 쿠키 식별, (E) : 재인증

④ (A) : GET, (B) : POST, (C) : 토큰, (D) : 사용자 세션 검증, (E) : 재인증

59. S/MIME(Secure/Multipurpose internet Mail Extension)은 기존 전자우편 보안시스템의 문제점인 PEM 구현의 복잡성, PGP의 낮은 보안성과 기존 시스템과의 통합이 용이하지 않 다는 점을 보완하기 위해 IETF의 작업그룹에서 RSADSI(RSA Data Security Incorporation)의 기술을 기반 으로 개발된 전자우편 보안이다. S/MIME이 달성하고자 하는 목표가 아닌 것은?

① 강력한 암호화

② 디지털 서명

③ 상호 운영성

④ 키 관리의 간소화

60. 소프트웨어 수명주기(Life-Cycle) 모형 중 프로토타이핑(Prototyping) 모형의 가장 큰 장점이라고 볼 수 있는 것은?

① 개발비용의 절감

② 4세대 언어의 적용

③ 개발단계의 명확성

④ 사용자 요구사항의 정확한 파악

【4과목】 정보 보안 일반 (20문제)

61. 다음 중 DES 및 3-DES에 관한 설명으로 잘못된 것은?

① DES의1 F-함수는 8개의 S-box로 구성되어 있으며, 각 S-box는 6비트 입하 4비트 출력을 갖는다.

② DES의 S-box는 모두 선형(Linear) 구조이며 DES의 안전성의 핵심 모듈이다.

③ DES의 F-함수의 확장(Expansion)은 입력 32비트를 출력 48비트로 확장하는 과정이다.

④ 3-DES는 2개 또는 3개의 서로 다른 키를 이용하여 DES를 반복 적용하는 것이다.

62. 사용자 인증을 위해 사용되는 생체인식 기술의 요구조건이 아닌 것은 무엇인가?

① 보편성

② 구별성

③ 영구성

④ 시간 의존성

63. 스트림 암호에 관한 설명으로 잘못된 것은?

① 이진 수열(비트)로 된 평문과 키 이진 수열 비트 단위로 XOR하여 암호화 한다.

② 암호화 알고리즘에 치환변환과 전치변환이 주로 쓰인다,

③ 주로 유럽을 중심으로 발전하였으며 군사용으로 쓰인다.

④ 일회용 패드(One-Time Pad)는 스트림 암호의 한 예이다.

64. 전자서명에서 사용되는 해시 함수(H)와 관련한 설명으로 옳지 않은 것은?

① 해시 값 h가 주어져 있을 때 h=H(M) 인 메시지 M 을 찾는 일은 시간이 아주 많이 걸리는 일이어야 한다.

② 메시지 M이 주어져 있을 때, H(M)-H(M')인 다른 메시지 M' 을 찾는 일은 시간이 아주 많이 걸리는 일이어야 한다.

③ H(M)=H(M')인 서로 다른 두 메시지 M과 M'을 찾는 일은 시간이 아주 많이 걸리는 일이어야 한다.

④ 해시 힘수의 출력의 크기는 해시 함수의 안전성과는 무관하지만, 해시 함수 계산 시간에는 많은 영향을 미친다.

65. 다음 중 무결성(Integrity) 점검을 위한 해시 함수가 아닌 것은?

① tripwire

② MD5

③ SHA-256

④ RIPEMD-160

66. 최근 입사하여 소속 부서의 프린터 관리를 담당하게 된 홍길동은 이전 담당자의 자원 접근 권한을 그대로 인계 받아 업무를 수행하게 되었다. 이러한 상황과 가장 관련성이 높은 접근 통제 기술은 무엇인가?

① 강제적 접근통제(MAC)

② 임의적 접근통제(DAC)

③ 역할기반 접근통제(RBAC)

④ 다단계 보안정책(MLS)

67. 일방향 해시(hash) 함수 MD5의 출력 해시의 크기는?

① 128비트

② 256비트

③ 512비트

④ 1024비트

68. 아래 지문에 가장 적합한 세션키(Session key) 키 분배 방 법은?

"A"가 생성한 세션키를 "B"에게 분배하고자 할 때는 자신이 생성한 세션키를 "B"의 공개키로 암호화하여 "B"에게 보낸다. 이를 받은 "B"는 자신의 개인키로 복호화하여 세션키를 얻는다.
→ "A"와 "B"는 동일한 세션키를 갖게 된다.

① Diffie - Heilman 키 분배

② KDC 기반 키 분배

③ RSA 알고리즘을 이용한 키 분배

④ Needham-Schroeder 키 분배

69. 메시지의 무결성 보장과 송신자에 대한 인증을 목적으로 공유 비밀키와 메시지로부터 만들어지는 것은?

① 의사

② 메시지 인증 코드

③ 해시

④ 인증서

70. 다음 중 아래 괄호 부분에 들어갈 내용으로 적합한 것은?

(가) 기술은 암호화와 복호화에 서로 다른 키를 이용하는 암호 기법으로 메시지의 기밀성을 제공하기 위해 사용되며, 이는 (나) 기술에 비해 속도가 매우 느리기 때문에 하이브리드 암호 방식으로 사용된다. (가) 기술은 (나)의 키 배송 문제를 해결할 수 있지만, 중간자 공격에 의해 위장 공격이 가능하기 때문에 (다)을/를 이용한 공개키 인증이 필요하다.

① (가) 일방향 해시함수, (나) 대칭키 암호, (다) 공개키 암호 기술

② (가) 일방향 해시함수, (나) 메시지 인증 코드, (다) 전자 서명

③ (가) 공개키 암호 (나) 메시지 인증 코드, (다) 대칭키 암호 기술

④ (가) 공개키 암호, (나) 대칭키 암호, (다) 전자 서명

71. 컴퓨터 보안에서 사용되는 암호에 관한 설명 중 옳은 것은?

① 암호는 정당한 권한이 부여된 사용자만이 데이터의 내용을 파악할 수 있는 데이터의 가용성을 보장해 준다.

② 암호는 수신된 메시지가 불법적으로 재생된 것인지 또는 전송과정에서 변조, 재구성되었는지 등을 확인할 수 있는 무결성을 보장한다.

③ 암호는 수신된 메시지가 정당한 송신자로부터 전송된 것인지를 확인할 수 있는 기밀성을 보장한다.

④ 암호는 메시지를 특정 수신자에게 전송할 때 송신자는 그 메시지의 발송을 나중에 부인할 수가 없고 또한 송신자에 의해서 발송되지 않은 메시지를 받았다고 수신자가 주장할 수 없도록 하는 인증을 보장한다,

72. 전자입찰시스템의 요구조건을 기술한 다음 지문의 ( )안에 들어갈 단어를 순서대로 나열한 것은?

- ( ) : 전자입찰 시스템의 각 구성요소들은 자신들의 독자적인 자율성을 보장받아야 한다.
- ( ) : 입찰이 수행될 때 모든 정보는 공개되어야 한다.
- ( ) : 네트워크상에서 각 구성요소 간에 개별 정보는 누구에게도 노출되어서는 안 된다.
- ( ) : 입찰시 입찰자 자신의 정보를 확인 가능하게 함으로써 누락 및 변조 여부를 확인할 수 있어야 한다.
- ( ) : 각 입찰 참여자 간의 공모는 방지되어야 하고 입찰 공고자와 서버의 독단이 발생하면 안 된다.

① 비밀성, 안정성, 독립성, 무결성, 공평성
② 비밀성, 공평성, 독립성, 무결성, 안정성
③ 독립성, 안전성, 비밀성, 무결성, 공평성
④ 독립성, 공평성, 비밀성, 무결성, 안정성

73. 암호 해독자가 일정량의 평문에 해당하는 암호문을 알고 있을 경우 암호 키를 찾아내는 암호 공격 방식은?

① 암호문 단독 공격
② 기지 평문 공격
③ 선택 평문 공격
④ 선택 암호문 공격

74. 접근통제 모델 중 기밀성을 강조한 최초의 수학적 모델로 시스템 보안을 위한 규칙 준수 규정과 주체의 객체 접근 허용 범위를 규정한 것으로 옳은 것은?

① 벨-라파듈라 모델
② 비바 모델
③ 클락-윌슨(Clark-Wilson) 모델
④ 만리장성 모델

75. 접근통제 모델 중 정보의 소유자가 정보의 보안 수준을 결정하고 이에 대한 정보의 접근 통제까지 설정하는 모델은 무엇 인가?

① DAC(Discretionary Access Control)
② MAC((Mandatory Access Control)
③ RBAC(Role-Based Access Control)
④ HAC(Horizon Access Control)

76. 다음 중 블록 암호 알고리즘의 종류가 아닌 것은?

① RC5
② MD5
③ DES
④ IDEA

77. SET에서 도입된 기술로 고객의 구매 정보는 은행이 모르게 하고 지불 정보는 상점이 모르게 하기 위해 사용하는 서명 방식은?

① 은닉 서명
② 그룹 서명
③ 수신자 지정 서명
④ 이중 서명

78. 다음은 어떤 전자서명 방식에 대한 설명인가?

(1) 미국의 NBT에서 발표한 표준 전자서명 방식이다.
(2) DSA 알고리즘을 사용한다.
(3) 트랩도어가 존재할 가능성이 있다.
(4) Schnorr 방식과 비슷한 구조를 가지고 있다.

① KCDSA
② DSS
③ FFS
④ ElGameil

79. 다음에서 설명하는 블록 암호 공격 기법은?

선택 평문 공격으로서 두 개의 평문 블록들의 비트 차이에 대응되는 암호문 블록의 비트 차이를 이용하여 사용된 암호키를 찾아내는 방법이다.

① 차분 공격
② 선형 공격
③ 통계적 분석
④ 치환 공격

80. 우리나라 표준 서명 알고리즘으로 가장 적절한 것은?

① RSA
② KCDSA
③ ECC
④ ECDSA

【5과목】정보보안 관리 및 법규 (20문제)

81. 지문에서 설명하는 위험분석 방법은 무엇인가?

> 이 방법은 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고, 위험을 분석 및 평가하여, 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 정성적 위험분석 방법의 일종이다. 이 방법은 위험 분석을 짧은 기간에 도출할 수 있어 시간과 비용을 절약할 수 있는 장점이 있는 반면에, 위험분석결과에 대한 신뢰도가 낮다는 단점이 존재한다.

① 연간예상손실 계산법

② 과거 통계자료 분석법

③ 델파이법

④ 시나리오 기반 분석법

82. 인터넷 보안 프로토콜에 해당하지 않는 것은?

① SSL

② HTTPS

③ S/MIME

④ TCSEC

83. 다음 설명은 정보의 속성 중에서 무엇을 설명한 것인가?

> 송신자와 수신자간에 전송된 메시지를 놓고 전송치 않았음을 또는 발송되지 않은 메시지를 받았다고 주장할 수 없게 한다.

① 비밀성

② 인증

③ 부인방지

④ 액세스제어

84. 다음은 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"의 목적규정 내용 중 ( ) 에 적합한 내용은?

> 이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 (가)을(를) 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성함으로써 (나)의 향상과 (다)의 증진에 이바지함을 목적으로 한다.

① 가: 권익보호, 나: 서비스의 품질, 다: 공공복리

② 가: 인격보호, 나: 보안의식, 다: 표준화

③ 가: 이용권, 나: 정보통신기술, 다: 정보화

④ 가: 개인정보, 나: 국민생활, 다: 공공복리

85. 다음의 지문은 무엇에 대한 설명인가?

> 이것은 각종 재해 시 재난의 발생을 대비하기 위하여 핵심 시스템의 가용성과 신뢰성을 회복하고 사업의 연속성을 유지하기 위한 일련의 사업지속성 계획과 절차를 말한다. 단순한 데이터의 복구나 신뢰도를 유지하며 나아가 기업의 전체적인 신뢰성 유지와 가치를 최대화 하는 방법과 절차이다.

① 위험관리

② 업무 연속성 계획

③ 재난 대비 가용성 확보 대책

④ 피해 복구 대책

86. 다음과 같은 개인정보보호에 대한 시책 마련은 어느 법률에서 규정하고 있는가?

> 미래창조과학부장관 또는 방송통신위원회는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자의 개인정보보호 등을 통해 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다.

① 국가정보화 기본법

② 개인정보보호법

③ 정보통신기반 보호법

④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

87. 정량적 위험분석과 정성적 위험분석에 대한 다음의 설명 중 틀린 것은?

① 정량적 분석은 객관적인 평가기준이 적용된다.

② 정량적 분석은 위험관리 성능평가가 용이하다.

③ 정성적 분석은 계산에 대한 노력이 적게 소요된다.

④ 정성적 분석은 비용과 이익에 대한 평가가 필수적으로 요구된다.

88. 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 에서 규정하고 있는 내용이 아닌 것은?

① 주요정보통신기반시설의 보호체계

② 정보통신망에서의 이용자 보호 등

③ 정보통신망의 안정성 확보 등

④ 개인정보의 보호

89. 다음의 ISMS 인증 의무 대상자에 대한 설명으로 잘못 기술된 것은?

① 전기통신사업법의 전기통신사업자로 전국적으로 정보통신망 서비스를 제공히는 사업자

② 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시 설을 운영 • 관리하는 사업자

③ 정보통신서비스 부문 전년도 매출액 100억 이상 사업자

④ 전년도말 기준 직전 6월간 일일 평균 이용자 수 100만명 이상 사업자

90. 다음 중「정보통신기반보호법」상 국가안전보장에 중대한 영향을 미치는 것으로서 관리기관의 장이 기술적 지원을 요청 하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 하는 주요정보통신기반기설에 해당하지 아니하는 것은?

① 도로·철도·지하철·공항·항만 등 주요 교통시설

② 전력, 가스, 석유 등 에너지 수자원 시설

③ 방송중계·금융정보통신기반시설

④ 원자력·국방과학·첨단방위산업관련 정부출연 연구기관의 연구시설

91. 다음의 보기 중에서 일반직원 대상의 통상적인 정보보호 교육 및 훈련의 내용에 해당되지 않는 것은?

① 정보보호 요구사항

② 정보보호 사고 발생 시의 사용자의 법적인 책임

③ 조직의 정보보호 관리통제 방법

④ 조직의 정보보호 시스템 구성도 및 운영방법

92. 다음 중 정보통신서비스 제공자 등이 개인정보의 분실, 도난, 누출 사실을 안 때에는 지체 없이 수행해야 할 행동으로 잘못 기술된 것은?

① 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.

② 정당한 사유 없이 그 사실을 안 때부터 5일을 경과하여 통지 신고해서는 아니 된다.

③ 이용자에게 알릴 때에는 누출 등이 된 개인정보 항목이 포함된다,

④ 한국인터넷진흥원이 신고를 받았다면 그 사실을 방송통신 위원회에 알려야 한다.

93. 다음은 정보통신서비스 제공자가 정보통신망법의 규정을 위반하여 부당하게 되는 손해배상책임에 관한 규정이다. ( )에 적합한 용어는?

> 이용자는 정보통신서비스 제공자 등이 이 장의 규정을 위반 한 행위로 (A)를 입으면 그 정보통신서비스 제공자 등에게 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자 등은 고의 또는 (B)이 없음을 입증하지 아니하면 책임을 면할 수 없다.

① A : 불명예, B : 과실

② A : 손해, B : 부주의

③ A : 이익, B : 손해

④ A : 손해, B : 과실

94. 위험관리의 개념에서 위험 완화 방법에 대한 설명으로 옳지 않은 것은?

① 회피(avoidance)는 특정 위험으로부터의 손실 부담 또는 위험 획득을 수용하는 것이다.

② 이전(transfer)은 잠재적 비용을 제3자에게 전가하거나 할당하는 것이다.

③ 감소(reduction)는 위힘을 감소시킬 수 있는 대책을 채택하여 구현하는 것이다.

④ 수용(acceptance)은 위험을 받아들이고 비용을 감수하는 것이다.

95. 아래는 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 한 규정의 내용이다. ( )안에 들어갈 말로서 바르게 나열된 것은?

> 정보통신서비스제공자는 이용자의 개인정보를 ( ) 하려고 ( ) 하는 때에는 다음 각 호의 ( ) 사항에 대하여 이용자에게 알리고 ( )를 얻어야 한다. 다음 각 호의 어느 하나의 사항을 ( )하려는 때에도 또한 같다.
> 1. 개인정보의 수집·이용 목적
> 2. 수집하는 개인정보의 항목
> 3. 개인정보의 보유 및 이용 기간

① 이용 - 수집 - 모든 - 동의 - 변경

② 이용 - 보유 - 개별 - 양해 - 수정

③ 사용 - 보유 - 개별 - 양해 - 수정

④ 이용 - 수집 - 모든 - 양해 - 변경

96. 다음 중「전자서명법」에 의거하여 공인인증기관이 발급하는 공인인증서에 포함되는 사항이 아닌 것은?

① 가입자와 공인인증기관이 이용하는 전자인증 방식

② 공인인증서의 일련번호

③ 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보

④ 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항

97. 다음의 지문은 무엇에 대한 설명인가?

이것은 부분적으로 설비를 가지고 있는 백업 사이트로서, 대개 디스크 드라이브, 테이프 드라이브와 같이 가격이 저렴한 주변기기를 가지고 있으나, 주 컴퓨터는 가지고 있지 않는 재난복구 서비스의 일종이다.

① 중복 시스템

② 핫 사이트(Hot site)

③ 웜 사이트(Warm site)

④ 콜드 사이트(Cold site)

98. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보처리방침에 포함되어야 할 사항이 아닌 것은?

① 이용자 및 법정대리인의 권리와 그 행사 방법

② 개인정보에 대한 내부 관리 계획

③ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항

④ 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집 방법

99. 정보통신망 이용촉진 및 정보보호 등에 관한 법률상 정보통신서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있도록 정하고 있다. 정보통신서비스 제공자의 정보보호 최고책임자가 총괄라는 업무에 해당하지 않는 것은? (단, 이 법에 명시된 것으로 한정함)

① 정보보호관리체계 수립 및 관리·운영

② 주요 정보통신기반시설의 지정

③ 정보보호 취약점 분석·평가 및 개선

④ 정보보호 사전 보안성 검토

100. 다음 보기 중에서 통상적으로 정보보호 정책서에 기술하지 않는 항목은?

① 정보보호 목적과 구성

② 정보보호 실행 계획 수립

③ 보안에 대한 역할과 책임

④ 정보보호 선언