2015년03월28일년 정보보안기사 필기시험 기출문제 답안

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

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

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

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

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

CBT기출문제

전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!

Download on the App Store

GET IT ON Google Play

【1과목】 시스템 보안 (20문제)

1. 다음은 스캔 도구로 유명한 Nmap의 스캔 타입을 설명한 내용이다. 보기에서 설명하는 스캔 타입은 무엇인가?

> 정상적인 3Way 핸드쉐이킹을 하지 않고 끊기 때문에 Half-Open 스캐닝이라고도 한다. 접속이 이루어 지지않는 상태에서 접속을 끊었기 때문에 로그가 남지 않는 경우가 많다.

① -sX
② -sS
③ -sU
④ -sP

2. 다음 중 원격 서버의 /etc/hosts/equiv 파일에 정확한 설정이 있어야만 정상적으로 실행이 되어 신뢰받는 로그인을 할 수 있는 명령어는 무엇인가?

① telnet
② login
③ rlogin
④ talkd

3. 다음 중 비밀번호 앞 또는 뒤에 문자열을 추가하여 동일 비밀번호에 대하여 동일 다이제스트를 생성하는 해시 함수의 문제점을 보완해 주는 기술은 무엇인가?

① 0TP
② 솔트
③ HMAC
④ 스트레칭

4. 다음 중 응용 프로그램 로그에 해당되지 않는 것은?

① UNIX Syslog
② DB 로그
③ 웹 로그
④ FTP 로그

5. 다음의 취약성 점검 도구 중 NESSUS 도구로 탐지할 수 없는 것은?

① 사용할 때만 열리는 닫힌 포트
② 쿠키값
③ 운영 체제 종류
④ 웹 서버 취약점

6. 다음에서 설명하고 있는 접근 제어 정책으로 올바른 것은?

> - 자원에 대한 접근은 사용자에게 할당된 역할에 기반한다.
> - 관리자는 사용자에게 특정한 권리와 권한이 정의된 역할을 할당한다.
> - 사용자와 할당된 역할의 연관성으로 인하여 자원들에 접근할 수 있고, 특정한 작업들을 수행할 수 있다.

① MAC
② DAC
③ RBAC
④ HMAC

7. UNIX 시스템에서는 일반 계정의 비밀번호를 저장할 때 암호화하여 저장한다. 다음 중 어떤 알고리즘을 이용하여 저장하는가?

① DES
② RSA
③ MD5
④ SHA

8. 다음의 일반적인 보안 원칙 중 보기에 알맞은 것은?

> 사용자나 관리자에게 작업을 수행하는데 필요한 권한을 최소화하는 원칙

① 소프트웨어 최신 유지
② 중요 서비스에 대한 액세스 제한
③ 시스템 작업 모니터링
④ 최소 권한 원칙 준수

9. 다음 중 PAM(Pluggable Authentication Module) 에 대한 설명으로 옳지 않은 것은?

① 사용자를 인증하고 그 사용자 서비스에 대한 액세스를 제어하는 모듈화 방법이다.
② 응용 프로그램의 재컴파일이 필요하다.
③ 관리자가 응용 프로그램들의 사용자 인증 방법을 선택하도록 해 준다.
④ 권한을 부여하는 소프트웨어의 개발과 안전하고, 적정한 인증의 개발을 분리하려는데 있다.

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

10. 다음 중 7.7 DDoS 공격과 3.20 DDoS 공격의 공통점은 무엇인가?

① 대역폭 과부하

② 리소스 고갈

③ MBR 파괴

④ 금융 정보 유출

11. 다음의 리눅스 파일 시스템에서 SetUID, SetGID, Sticky bit 설명으로 옳은 것은?

① 파일에 SetUID가 걸려 있어도 겉으로는 알 수 없다.

② 파일에 대한 접근 권한이 7777'이면 문자로는 'rwsrwgrwt'로 표시된다.

③ SetUID 비트가 세트된 파일을 실행하면 파일 소유자 권한으로 수행된다.

④ SetUID 비트가 세트되어 있어도 루트 권한으로 실행되는 경우는 없다.

12. 다음 중 HTTP 프로토콜의 상태 코드로 올바르지 못한 것은?

① 200 : HTTP 요청에 대해 에러 없이 성공

② 300 : 클라이언트가 선택할 수 있는 리소스에 대한 다중 옵션 표시

③ 403 : 유효한 요청에 대한 클라이 언트가 응답 거부

④ 404 : 현재 요청한 리소스를 찾을 수 없으나 향후 요청에 대해서는 유효할 수 있음

13. 다음 중 루트킷에 대한 특징으로 올바르지 못한 것은?

① 트래픽이나 키스트로크 감시

② 커널 패치

③ 로그 파일 수정

④ 시스템 흔적 제거

14. 다음 시나리오의 빈칸 (가)에 알맞은 명령어는?

중국발 해킹을 통하여 웹 서버를 공격하고 있다는 사실을 알았다. 찾아낸 IP는 10.10.11 ~ 10.10.1.255, 10.10.2.3, 10.10.3.5와 같으며 접근 통제 정책을 통하여 위의 IP에 대하여 web 접속을 거부하라. 단, 10.10.1.11 IP는 web 접속을 허락하여야 한다.
/sbin/iptables -A INPUT -s 10.10.1.33 -p tcpl -dporl 80 -j ACCEPT
/sbin/iptables -A INPUT -s 10.10.1.1/10.10.1.255 -p tcp -dport 80 -j DROP
(가)
/sbin/iptables -A INPUT -s 10.10.3.5 -p tcp j -dport 80 -j DROP

① /sbin/iptables -A INPUT -s 10.10.2.1 -p tcp -dport 80 -j DROP

② /sbin/iptables -A INPUT -s 10.10.2.2 -p tcp -dport 80 -j ACCEPT

③ /sbin/iptables -A INPUT -s 10.10.2.3 -p tcp -dport 80 -j DROP

④ /sbin/iptables -A INPUT -s 10.10.3.5 -p tcp -dport 80 -j ACCEPT

15. 다음 중 시스템에서 FTP로 어떤 파일을 주고 받았는지를 기록하는 로그는 무엇인가?

① xferlog

② last

③ lastlog

④ secure

16. 다음 중 윈도우의 패스워드 복구 시 관련이 있는 파일명은?

① Password

② SAM

③ PAM

④ Kernel

17. 다음의 보기에서 빈칸에 알맞은 용어는 무엇인가?

( )는 /etc/hosts.deny와 /etc/hosts.allow 파일을 통하여 접근 통제를 강력히 구현할 수 있다.

① tcp_wrapper
② tripwire
③ SARA
④ NESSUS

18. 다음 중 윈도우의 암호 정책에 포함되지 않는 것은?

① 최근 암호 기억
② 최소 암호 사용 기간
③ 암호의 복잡성
④ 암호 알고리즘 종류

19. 다음 중 취약성 점검 도구가 아닌 것은?

① nikto2
② SARA
③ NESSUS
④ Tripwire

20. 다음 중 포트 스캐닝에 대한 설명으로 올바르지 못한 것은?

① UDP 패킷을 보내어 포트가 열려 있으면 아무런 응답이 없다.
② 포트가 열려 있지 않으면 아무런 응답이 없다.
③ 인가되지 않는 포트 스캐닝은 하지 말아야한다.
④ 포트 정보를 수집함으로 인하여 취약점 서비스를 찾아낸다

【2과목】 네트워크 보안 (20문제)

21. 다음 중 리눅스 운영 체제에서 원격 접속 방법의 하나로 평문이 아닌 암호화된 접속을 통한 안전한 접속방법을 무엇이라 하는가?

① 원격 터미널 서비스
② telnet
③ rlogin
④ ssh

22. 다음 중 가상 사설망(VPN) 프로토콜로 올바른 것은?

가. PPTP	나. L2F
다. IPSEC	라. SSH

① 가
② 가, 나
③ 가, 나, 다
④ 가, 나, 다, 라

23. 다음 중 패킷 전송 시 출발지 IP 주소와 목적지 IP 주소값을 공격 대상의 IP 주소로 동일하게 만들어 공격 대상에게 보내는 것은?

① DDoS
② 세션 하이젝킹
③ 스푸핑 (Spoofing)
④ 랜드 (Land) 공격

24. 다음 중 사용자로부터 파라미터를 입력받아 동적으로 SQL Query를 만드는 웹페이지에서 임의의 SQL Ojery와 Command를 삽입하여 웹 사이트를 해킹하는 기법은?

① SQL Spoofing
② Smurf
③ SQL Injection
④ SQL Redirect

25. 다음 지문의 빈칸에 알맞은 단어는 무엇인가?

(ⓐ)은/는 printf 등의 함수에서 문자열 입력 포맷을 잘못된 형태로 입력하는 경우 나타나는 버그이다. (ⓑ) 특정 프로그램을 이용하여 네트워크상의 데이 터를 몰래 캡처하는 행위를 말한다.

① ⓐ 포맷 스트링, ⓑ 스니핑
② ⓐ 버퍼 오버플로우, ⓑ 하이젝킹
③ ⓐ 스니핑, ⓑ 버퍼 오버플로우
④ ⓐ 스니핑, ⓑ 스푸핑

26. 다음 중 DMZ(Demilitarized Zone) 구간에 위치하고 있으면 안되는 시스템은?

① 웹서버
② 디비 서버
③ 네임 서버
④ FTP 서버

27. 다음 중 DNS Lookup 정보로 알 수 없는 것은?

① 디비 서버

② 네임 서버

③ 이메일 서버

④ 이메일 서버 IP

28. 다음 중 파일 업로드 공격의 취약점에 대한 설명으로 틀린 것은?

① 게시판 글쓰기 권한이 있는지 확인한다.

② 쉘 획득이 가능한 공격이다.

③ 업로드 외에는 파일 확장자 필터가 적용되어야 한다.

④ 업로드 폴더를 제거한다.

29. 다음 중 해킹 시 서버 수집 단계에서 하는 행동과 다른 것은?

① 서버 IP

② Smurf

③ 운영 체제

④ 서비스 데몬

30. 다음 중 괄호 안에 알맞은 용어는 무엇인가?

> 라우터에서 패킷 필터링하는데 바깥에서 들어오는 패킷의 출발지가 내부 IP 대역이면 필터링한다. (A)을 막고, 이러한 필터링 방법을 (B)라고 한다.

① A : ARP, B : 스푸핑

② A : IP 스푸핑, B : INGRESS

③ A : 스니핑, B : INGRES

④ A : 스푸핑, B : EGRESS

31. Ping을 이용한 공격으로 ICMP_ECHO_RE- QUEST를 보내면 서버에서 다시 클라이언트로 ICMP_ECHO_REPLY를 보낸다. 이때, 출발지 주소를 속여서(공격하고자 하는) 네트워크 브로드캐스팅 주소로 ICMP_ECHO_REQUEST를 전달 할 경우 많은 트래픽을 유발시켜 공격하는 것을 무엇이라 하는가?

① 세션 하이젝킹 공격

② 브로드캐스팅 공격

③ Tear Drop 공격

④ Smurf 공격

32. 다음 중 포트 스캐닝 기술이 다른 하나는 무엇인가?

① NULL Scanning

② X-MAS Scanning

③ FIN Scanning

④ TCP Connect Scanning

33. 다음 중 NIDS에서 탐지할 수 없는 것은?

① 악성 코드가 담긴 파일

② 악성 코드가 담긴 메일

③ Fragmentation

④ 포트 스캔

34. 다음의 보기에서 설명하고 있는 웹 취약점 공격 기술은?

> SQL 삽입 후 결과 화면의 차이 즉, 참과 거짓이라는 결과만으로데이터베이스 내의 정보를빼내는 방법

① 세션 하이잭킹

② 파일 업로드 공격

③ Blind SQL Injection 공격

④ XSS 공격

35. 다음의 보기에서 설명하고 있는 공격은?

> - 헤더 옵션 값을 사용함으로써 웹 서버에 더 많은 부하를 유발시키는 지능화된 DDoS 공격 기법이다.
> - 웹 트랜잭션의 효율히를 이용하여 사용하게 되는 Cache 기능을 사용하지 않고, 자주 변경되는 데이터에 대해 새롭게 HUP 요청 및 응답을 요구하기 위하여 사용되는 옵션이다.

① CSRF 공격

② HTTP CC Attack

③ Blind SQL Injection 공격

④ XSS 공격

36. 다음 중 네트워크의 공격 대응 방법으로 올바르지 못한 것은?

① Ping of Death 공격은 UDP를 차단한다.

② Syn Flooding 공격은 최신 패치를 한다.

③ 스니핑 공격을 SSL 암호화 프로토콜 사용으로 패킷을 보호한다.

④ DDoS 공격은 적절한 라우팅 설정 및 Null 처리를 한다.

37. 다음 중 네트워크 접속 사용자 또는 단말기를 등록하거나 인증하고, 미인가 사용자 및 단말기 네트워크를 차단하는 솔루션은 무엇인가?

① NAC
② ESM
③ SSO
④ EAM

38. 공격자는 공격 대상 서버에 파일을 업로드한 후에 웹을 이용하여 시스템 명령어를 수행하므로 네트워크 방화벽 등의 영향력을 받지 않고 서버를 제어할 수 있는 공격 기술을 무엇이라 하는가?

① SQL 인젝션
② 파일 업로드
③ XSS
④ 웹 쉘

39. 다음의 보기에서 설명하고 있는 기술은?

- 물리적으로 하나인 단말기를 개인 영역과 업무 영역을 완벽히 분리해 마치 2개의 독자적인 단말기를 사용하는 것처럼 해준다.
- 개인 영역이 악성 코드에 감염되어도 업무 영역의 모바일 메신저 대화나 문자, 통화 내역에 접근하는 것이 불가능하다.

① MAM
② MDM
③ 모바일 가상화
④ WIPS

40. 다음의 TCP Flag 중에서 연결 시작을 나타내기 위해 사용하는 Flag는 무엇인가?

① FIN
② SYN
③ ACK
④ RST

【3과목】 어플리케이션 보안 (20문제)

41. 다음 중 DNSSEC로 방어가 가능한 최신 보안 이슈는 무엇인가?

① 피싱
② 파밍
③ 스미싱
④ 큐싱

42. 다음 중 인간의 감지 능력으로는 검출할 수 없도록 사용자 정보를 멀티미디어 콘텐츠에 삽입하는 기술을 무엇이라 하는가?

① 핑거 프린팅(Digital Fingerprinting)
② 워터 마킹(Water Marking)
③ 포렌식 마킹(Forensic Marking)
④ 태그 마킹(Tag Marking)

43. 다음의 보기에서 설명하고 있는 프로토콜은?

- 1994년 네스케이프사의 웹 브라우저를 위한 보안 프로토콜이다.
- 1999년 TLS(Transparent Layer fecurity) 라는 이름으로 표준화되었다.
- TCP 계층과 응용 계층 사이에서 동작한다.

① HTTP
② SSL
③ HTTPS
④ SET

44. 다음 중 디비(DB) 보안에 해당하지 않는 것은?

① 흐름 통제
② 추론 통제
③ 접근 통제
④ Aggregation

45. 다음 중 SCT 프로토콜에 대한 특징으로 올바르지 못한 것은?

① 전자상거래 사기를 방지한다.
② 구현이 용이하다.
③ 기존 신용 카드 기반 그대로 활용이 가능하다.
④ 상점에 대한 인증을 할 수 있다.

46. 다음의 보기에서 설명하고 있는 프로토콜은?

구매 요구 거래에서 상인은 주문 정보만 알아야 하고 매입사는 지불 정보만 알아야 한다. 즉, 지불 정보와 주문 정보를 해쉬한 후에 이것을 다시 고객의 서명용 개인키로 암호화하는 기술을 말한다.

① 블라인드 서명
② 이중 서명
③ 은닉 서명
④ 전자 봉투

47. 다음의 SSL 핸드쉐이킹 과정 중 보기에서 설명 하고 있는 과정은 어느 단계인가?

> 서버는 기본적으로 클라이언트에서 서버 자신을 인증할 수 있도록한다.

① Hello Request
② Client Hello
③ Certificate Request
④ Client Certificate

48. 다음의 보기에서 설명하고 있는 전자 투표 방식은?

> - 지정된 투표소에서 전자 투표를 한다.
> - 전자 투표 기기를 선거인단이 관리한다.
> - 국민 투표의 활용 가능성이 크다.

① PSEV
② 키오스크
③ LKR
④ REV

49. 다음 중 전자 서명의 특징에 포함되지 않는 것은?

① 위조 불가
② 부인 불가
③ 서명자 인증
④ 재사용 가능

50. 다음 중 파일 업로드 공격 취약점의 대응 방법으로 올바르지 못한 것은?

① 첨부 파일에 대한 검사는 반드시 클라이언트 측에서 스크립트로 구현한다.
② 첨부 파일을 체크하여 특정 종류의 파일만 첨부한다.
③ 파일 업로드 시에 실행 파일은 파일 첨부를 불가능하게 한다.
④ 임시 디렉토리에서 업로드된 파일을 지우거나 다른 곳으로 이동한다

51. 다음 중 PGP에 대한 설명으로 올바르지 못한 것은?

① 이메일 어플리케이션에 플러그인으로 사용이 가능하다.
② 공개키 서버와 연결되어 공개키 분배 및 취득이 어렵다.
③ 메뉴 방식을 통한 기능 등에 쉽게 접근이 가능하다.
④ 필 짐버만이 독자적으로 개발하였다.

52. 검증되지 않는 외부 입력값에 의해 웹 브라우저에서 악의적인 코드가 실행되는 보안 취약점을 무엇이라 하는가?

① SQL 삽입
② XSS
③ 부적절한 인가
④ LDAP 삽입

53. 다음 중 네트워크형 전자 화폐에 포함되지 않는 것은?

① Mondex
② Ecash
③ Netcash
④ Payme

54. 다음 중 전자 입찰 시 요구되는 보안 사항에 포함되지 않는 것은?

① 비밀성
② 무결성
③ 공개성
④ 독립성

55. 다음 중 전자상거래 프로토콜인 SET의 구성 요소에 포함되지 않는 것은?

① 상점
② 고객
③ 매입사
④ 등록기관

56. DRM의 세부 기술 중에서 다음 보기에 해당하는 것은?

> 보호 대상인콘텐츠를메타 데이터와 함께 시큐어 콘테이너 포맷 구조로 패키징하는 모듈이다.

① 식별자
② 메타데이터
③ 패키져
④ 콘텐츠

57. 다음은 에러 로그 위험도를 8가지로 분류하여 높은 에러에서 낮은 에러로 표시한 것이다. 빈 곳에 알맞은 용어는?

```
emeg → (    ) → crit → error → (    ) →
notice → (    ) → debug
```

① alert, warn, info

② info, alert, warn

③ warn, info, alert

④ alert, info, warn

58. 다음 중 전자 우편 프로토콜과 관련성이 적은 것은?

① MDM

② MUA

③ MDA

④ MRA

59. 다음 중 전자 입찰의 문제점으로 올바르지 못한 것은?

① 입찰자와 입찰 공고자의 정보는 공개 네트 워크를 통하여 서버로 전송, 수신된다.

② 입찰자와 서버 사이에 서로 공모할 가능성이 있다.

③ 서버가 입찰자의 정보 또는 입찰 공고자 정보를 단독으로 처리하여 신뢰성이 높다.

④ 입찰자들이 입찰가에 대한담합을통하여 서로 공모할 가능성이 있다.

60. 다음 중 전자 화폐의 요구 조건이 아닌 것은?

① 교환성

② 익명성

③ 추적성

④ 인식 가능성

【4과목】 정보 보안 일반 (20문제)

61. 다음의 블록 암호 알고리즘 운영 방식 중에서 가장 단순하면서 권장하지 않는 방식은 무엇인가?

① ECC

② CBC

③ OFB

④ ECB

62. 다음 중 공인인증서 내용에 포함되지 않는 것은?

① 발행자

② 유효 기간

③ 비밀번호

④ 공개키정보

63. 다음 중 블록 암호 알고리즘의 하나인 DES 공격 방법으로 알맞은 것은?

① 선형 공격

② 블록 공격

③ 전수공격

④ 비선형공격

64. 다음 중 암호문으로부터 평문의 어떤 부분 정보도 노출되지 않는 암호 방식이며, 인수 분해 문제와 제곱 잉여의 원리를 이용하여 확률 암호를 정의한 것은?

① Elgamal

② Goldwasser-Micali

③ Diffi-Hellman

④ Massey-Omura

65. 다음 중 능동적 공격에 포함되지 않는 것은?

① 도청

② 삽입

③ 삭제

④ 재생

66. 다음에서 설명하고 있는 프로토콜은 무엇인가?

- MIT에서 개발한 분산 환경에서 개체 인증 서비스를 제공하는 네트워크 인증 시스템이다.
- 4개의 개체로 구성되어 있다.
- "지옥에서 온 머리가 3개 달린 경비견"이라는 유래가있다.

① KDC

② Kerberos

③ PPP

④ ECC

67. 다음 중 디바이스 인증 기술에 포함되지 않는 것은?

① 아이디 패스워드 인증

② 암호 프로토콜 인증

③ 시도 응답 인증

④ 커버로스

68. 다음 중 싱글사인온(SSO)은 한 번의 인증 과정으로 여러 컴퓨터상의 자원을 이용 가능하게 하는 인증 기능이다. 대표적인 인증 프로토콜은 무 엇인가?

① BYOD

② KDC

③ Kerberos

④ PAP

69. 다음 중 알고 있는 것에 기반한 사용자 인증 기술은 무엇인가?

① 핀 번호

② 스마트 카드

③ 홍채

④ 목소리

70. 다음 중 메시지 출처 인증 기술 중에 ( ) 안에 들 어갈 기술은 무엇인가?

메시지와 비밀키를 입력하여 인증값으로 사용될 고정된 길이의 어떤 값을 생성한다. 그 값을 ( ) 이라 한다.

① 디지털서명

② 해시 함수

③ 메시지 인증 코드(MAC)

④ 메시지 암호화

71. 다음 중 메시지 인증 코드(MAC)에 대한 설명으로 올바르지 못한 것은?

① 송신자와 수신자가 서로 동일한 공개키를 가지고 메시지를 대조한다.

② 송신자를 보증하는 디지털 서명을 지원하지 않는다.

③ 송신자와 수신자 사이에 메시지 무결성을 보장한다.

④ 송신자 인증에 사용된다.

72. 다음 중 X509v2의 설명으로 올바르지 못한 것은?

① 인증서 취소 목록을 도입하였다.

② 주체 고유 식별자를 사용하였다.

③ 인증기관 고유 ID를 도입하였다.

④ 확장자 개념이 도입되었다.

73. 다음의 보기에서 설명하고 있는 블록 암호 공격은 무엇인가?

선택된 평문 공격으로 두 개의 평문 블록들의 비트 차이에 대하여 대응되는 암호분 블록의 비트 차이를 이용하여 사용된 암호 키를 찾아내는 방법

① 선형 공격

② 차분공격

③ 전수공격

④ 수학적 분석

74. 다음의 보기에서 설명하고 있는 암호 알고리즘은 무엇인가?

- 이산 대수의 어려움에 근거를 두고 있다. - 암호화 과정에서 암호화 속도를 높이기 위하여 지수승 연산 시 Hammhg Weight가 작은 무작위 지수 k를 사용한다. - Baby-Step Giant-Step 공격을 고려하여 지수의 크기는 충분히커야한다. - 80비트 비밀키 암호의 안전성이 필요할 때 지수의 크기는 160 비트 이상이어야 한다.

① DES

② RSA

③ El Gamal

④ ECC

75. 사용자는 특정 작업 또는 세션 동안 한번 사용하기 위해 키를 생성할 수 있다. 이를 무엇이라 하는가?

① 공개키

② 비밀키

③ 세션키

④ 암호키

76. 다음 중 2 Factor 요소로 올바르게 짝지은 것은?

① 홍채-지문

② PIN-USB 토큰

③ 패스워드-PIN

④ 스마트 카드-토큰

77. 다음 중 비대칭키에 대한 설명으로 올바르지 못한 것은?

① 키 분배가 용이하다.

② 확장 가능성이 높다.

③ 암/복호화 처리 시간이 빠르다.

④ 복잡한 키 관리 구조를 가지고 있다.

78. 다음 보기의 역할을 하는 PKI 구성 요소는 무 엇인가?

- 인증서 발급
- 인증서 상태 관리, 인증서 철회를 위한 CRL 발급
- 유효한 인증서와 CRL의 리스트 발행

① CA

② RA

③ CRL

④ PCA

79. 다음 중 보기에서 설명하고 있는 접근 통제 모델은 무엇인가?

- 미국방부 다수준 보안 정책으로부터 개발되었다.
- 기밀성을 유지하는데 중점을 둔다.

① 비바 모델

② 클락 - 윌슨 모델

③ 벨 - 라파듈라 모델

④ 제한 인터페이스 모델

80. 다음 중 이산 대수에 기반한 암호 알고리즘이 아닌 것은?

① KCDSA

② Diffie-Hellman

③ El Gamal

④ RSA

【5과목】 정보보안 관리 및 법규 (20문제)

81. 다음 중 국제 공통 보안 평가 기준을 나타내는 것은?

① TCSEC

② ITSEC

③ CC

④ 오렌지북

82. 다음 중 정성적 위험 분석에 포함되지 않는 것은?

① 객관적인 평가 기준이 적용된다.

② 위험 분석 과정이 지극히 주관적이다.

③ 계산에 대한 노력이 적게 든다.

④ 측정 결과를 화폐로 표현하기 어렵다.

83. 다음 중 기업(조직)이 각종 위협으로부터 주요 정보 자산을 보호하기 위해 수립, 관리, 운영하는 종합적인 체계의 적합성에 대해 인증을 부여하는 제도를 무엇이라 하는가?

① TCSEC

② ITSEC

③ CC

④ ISMS

84. 다음 재난 복구 계획 중 서버와 단말기까지 모든 컴퓨터 설비를 완전히 갖추고, 실제로 운영되 는 환경과 동일한 상태로 지속 관리되는 사이트는 무엇인가?

① 웜사이트

② 핫사이트

③ 콜드사이트

④ 상호 지원계약

85. 다음 중 '정보통신망 이용 촉진 및 정보보호 등에 관한 법률'에서 정의하는 용어 설명으로 올바르지 못한 것은?

① 사용자 : 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.

② 정보통신서비스 : '전기통신사업법' 제2조 6호에 따른 전기 통신 역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.

③ 정보통신서비스 제공자 : '전기통신사업법' 제2조 8호에 따른 전기통신사업자와 비영리를 목적으로 전기통신사업자의 전기통신 역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

④ 개인정보 : 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보를 말한다.

86. 다음 중 개인정보 유출로 인하여 과태료를 지불해야 할 상황에 맞는 위험 대응 전략은 무엇인가?

① 위험회피

② 위험 전가

③ 위험 수용

④ 위험 감소

87. 다음 중 정보보호 관리 체계(ISMS) 의무 인증 대상에 포함되지 않는 것은?

① 서울 및 모든 광역시에서 정보통신망 서비스 제공
② 정보통신 서비스 부문 전년도 매출액 100억 이상
③ 전년도말 기준 직전 3개월간 일일 평균 이용 자 수 100만 명 이상 사업자
④ 매출액 100억 이하인 영세 VIDC

88. 다음 중 개인정보 이용 및 수집에서 정보 주체의 별도 동의를 받지 않아도 되는 것은?

① 외국인등록번호
② 병력
③ 운전자면허번호
④ 휴대폰 번호

89. 다음 중 주요 정보통신 기반 시설 보호 계획의 수립에 포함되지 않는 것은?

① 주요 정보통신 기반 시설의 침해 사고에 대한 예방 및 복구 대책에 관한 사항
② 주요 정보통신 기반 시설의 취약점 분석, 평가에 관한 사항
③ 그 밖에 주요 정보통신 기반 시설의 보호에 관하여 필요한 사항
④ 주요 정보통신 기반 시설 보호 대책 이행 여부의 확인 절차

90. 다음 중 주요 정보통신 기반 시설 보호 지원에 포함되지 않는 것은?

① 도로, 철도
② 인터넷 포털
③ 교통 정보
④ 도시, 가스

91. 금융 업무를 보지 못하여 물건 결제를 하지 못하였다면 보안의 목적 중 무엇을 충족하지 못하였는가?

① 기밀성
② 가용성
③ 무결성
④ 부인 방지

92. 다음 중 개인정보보호, 정보보호 교육에 대한 설명으로 올바르지 못한 것은?

① 개인정보보호법에 따라 연 정기적으로 개인 정보보호 교육을 의무적으로 한다.
② 정보보호 교육 시 자회사 직원만 교육하고 협력사는 제외한다.
③ 정보통신망법에 따라 연 2회 이상 개인정보 교육을 의무적으로 한다.
④ 개인정보보호, 정보보호에 대한 교육은 수준별, 대상별로 나누어 교육한다.

93. 다음 중 개인정보 이용 및 수집 시 동의 없이 처리할 수 있는 개인정보라는 입증 책임은 누구에게 있는가?

① 개인정보 처리자
② 개인정보보호 책임자
③ 개인정보 담당자
④ 개인정보 취급자

94. 다음 중 전자서명법상 용어의 설명으로 올바르지 못한 것은?

① “전자서명”이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
② “전자문서”라 함은 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.
③ “인증”이라 함은 전자서명 생성 정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말한다.
④ “인증서”라 함은 전자서명 검증 정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.

95. 개인정보 수집 시 정보 주체의 동의를 얻어야 한다. 다음 중 포함되지 않는 사항은?

① 개인정보 수집 목적
② 개인정보 수집 항목
③ 개인정보 보유 기간
④ 개인정보 파기 방법

96. 업무 연속성 관리 단계 중 다음의 보기와 같은 내용을 수행하는 단계는?

> - 업무가 지속적으로 운영되기 위한 프로그램을 수립하는 단계
> - 위험 감소 조치 및 재해 복구를 위한 설비 구현
> - 초기시험을 수행하는 단계

① 전략 수립 단계

② 운영 단계

③ 계획 단계

④ 구현 단계

97. 다음 중 정보보호 예방 대책을 관리적 예방 대책과 기술적 예방 대책으로 나누어 볼 때 관리적 예방 대책에 속하는 것은?

① 고유 식별 정보의 암호화

② 로그 기록 보관

③ 운영 체제 패치

④ 문서 처리 순서의 표준화

98. 다음 중 정보통신망법에 의하여 개인정보를 제3자에게 제공하기 위하여 동의를 받는 경우에 이용자에게 알려야 하는 사항이 아닌 것은?

① 개인정보의 제공 계약의 내용

② 개인정보를 제공 받는 자

③ 제공하는 개인정보의 항목

④ 개인정보를 제공 받는 자의 개인정보 이용 목적

99. 다음 중 OECD의 개인정보 8원칙에 포함되지 않는 것은?

① 정보 정확성의 원칙

② 안전 보호의 원칙

③ 이용 제한의 원칙

④ 비밀의 원칙

100. 다음 중 정보보호 정책에 포함되지 않아도 되는 것은?

① 자산의 분류

② 비인가자의 접근 원칙

③ 법 준거성

④ 기업 보안 문화