1과목 : 시스템 보안

1. rlogin 시에 아이디와 패스워드 없이 시스템에 인증할 수 있다. 다음 중 관련된 파일은?
① /etc/hosts.deny ❷ /etc/hosts.equiv
③ /etc/hosts.allow ④ /etc/host.login

2. 다음 중 비선점 스케줄링에 해당되는 것은?
❶ 최단 작업 우선 처리 ② 다단계 큐
③ 순환 할당스케줄링 ④ 최단 잔여 시간

3. 다음 중 ing을 이용한 공격으로 ICMP_ECH0_REQUEST를 보내면 서버에서 다시 클라이언트로 ICMP_ECHO_REPLY를 보낸다. 이때, 출발지 주소를 속여서(공격하고자 하는) 네트워크 브로드캐스팅 주소로 ICMP_ECHO_RE_QUEST를 전달할 경우 많은 트래픽을 유발시켜 공격하는 기술은?
① 세션 하이젝킹 공격 ② 브로드캐스팅 공격
③ Tear Drop 공격 ❹ Smurf 공격

4. 다음 중 아이 노드(i-node)에 포함하고 있는 정보가 아닌 것은?
① 파일 유형 ❷ 파일 이름
③ 링크 수 ④ 수정시각

5. 다음의 메모리 관리 기법 중 블록 사이즈 고정된 방식과 가변된 방식은 무엇인가?
❶ 페이징, 세그먼테이션 ② 힙, 쓰레드
③ 논리 주소 공간, 물리 메모리 ④ 할당 영역, 자유 영역

6. 다음 중 무결성 점검 도구로 그 성격이 다른 것은?
① tripwire ② fcheck
③ md5 ❹ nessus

7. 다음 중 포트와 서비스가 올바르게 연결된 것이 아닌 것은?
① WEB - 80 ❷ IMAP - 110
③ SSH - 22 ④ TELNET - 23

8. 다음 중 백그라운드 프로세스로 운영되면서 로그메시지를 받아 하나 이상의 개별 파일에 기록하는 데몬은 무엇인가?
① crond ② logd
③ xinetd ❹ syslogd

9. 다음 중 레이스 컨디셔닝 공격에 대한 설명으로 올바르지 않은 것은?
① Setuid가 설정되어 있어야 한다.
② 임시 파일을 생성해야 한다.
③ 임시 파일을생성할 때 레이스 컨디셔닝에 대응하지 않아야 한다.
❹ 임시 파일 이름을 공격자가 몰라도 된다.

10. 다음 중 루트킷에 대한 설명으로 올바르지 못한 것은?
① 로그 파일을 수정한다.
❷ 루트킷은 자기 복제가 가능해 다른 PC에도 설치된다.
③ 시스템 흔적을 제거한다.
④ 기존 시스템 도구들을 수정한다.

11. 다음 중 안티 루트킷의 주요 기능이 아닌 것은?
① 숨김 파일 찾기 ② 수정된 레지스트리 찾기
③ 프로세스 보호 해제 ❹ 로그 파일 흔적 제거

12. 메모리 오류를 이용해 타깃 프로그램의 실행 흐름을 제어하고, 최종적으로는 공격자가 원하는 임의의 코드를 실행하는 것을 무엇이라 하는가?
① 포맷 스트링 ❷ 버퍼 오버플로우
③ 레이스 컨디셔닝 ④ 메모리 단편화

13. 다음 중 'lastb'라는 명령을 통하여 로그를 살펴볼 수 있는 로그 파일명은?
① utmp ❷ btmp
③ dmGsg ④ secure

14. 다음 중 윈도우의 암호 정책으로 포함되지 않는 항목은?
① 최소 암호 사용 기간 ② 암호의 복잡성
③ 최근 암호 기억 ❹ 암호 알고리즘 종류

15. 다음 윈도우의 계정 잠금 정책 중 포함되지 않는 것은?
① 계정 잠금 기간
② 계정 잠금 임계값
❸ 계정 잠금 횟수
④ 다음 시간 후 계정 잠금 수를 원래대로 설정

16. 다음 중 iptables에서 체인 형식으로 사용하지 않는 것은?
① OUTPUT ② INPUT
❸ DROP ④ FORWORD

17. 리눅스 시스템에서 사용자가 최초 로그인 후에 생성되며, 사용자가 쉘에서 입력한 명령어를 기록하는 파일은 무엇인가?
① .bashrc ② .bash_profile
❸ .bashjiistoiy ④ .cshrc

18. 다음 중 레지스트리 트리에 해당되지 않는 것은?
① HKEY—CLASS_ROOT ② HKEY—USERS
③ HKEY_LOCAL__MACHINE ❹ HKEY—PROGRAMS

19. 다음의 운영 체제 구조에서 2계층부터 5계층까지 올바르게 나열한 것은?
① 프로세스 관리 → 메모리 관리 → 주변 장치관리 → 파일 관리
❷ 메모리 관리→ 프로세스 관리→ 주변 장치관리 → 파일 관리
③ 파일 관리 → 프로세스 관리 → 메모리 관리 → 주변 장치 관리
④ 주변 장치 관리 →프로세스 관리 → 파일 관리 → 메모리 관리

20. 다음 중 프로세스 교착 상태의 발생 조건아 아닌 것은?
① 상호 배제 ② 점유와 대기
❸ 중단 조건 ④ 환형 대기 조건

2과목 : 네트워크 보안

21. 다음 중 무선 암호 프로토콜 WPA, WPA2에서 공통으로 사용하는 프로토콜은?

❶ EAP ② IEEE802.1
③ IEEE802.H ④ WEP

22. 다음의 보기에서 설명하고 있는 기술은 무엇인가?

> - 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
❸ 모바일 가상화 ④ MPS

23. 다음 중 베스천 호스트에 대한 설명으로 올바른 것은?

① 두 개의 스크린 호스트를 이용한다.
② 라우터 기능 외에 패킷 통과 여부를 결정할 수 있는 스크린 기능을 가지고 있다.
③ 두 개의 랜 카드를 가진 호스트를 말한다.
❹ 보호된 네트워크에 유일하게 외부에 노출되는 내외부 네트워크 연결점으로 사용되는 호스트이다.

24. 다음 중 악의적인 의도를 가진 소프트웨어로 이에 감염된 봇들 다수가 연결되어 네트워크를 만드는 것을 무엇이라 하는가?

① C&C ② 봇 마스터
❸ 봇넷 ④ 봇클라이언트

25. 다음의 보기에서 VPN 프로토콜로 사용되는 것을 모두 고르시오.

> 가. PPTP 나. L2TP
> 다. IPSEC 라. SSH 마. Sock V5

① 가, 나 ② 가, 나, 다
③ 가, 나, 다, 라 ❹ 가, 나, 다, 마

26. 다음의 보기내용에 대한 설명으로 올바르지 못한 것은?

```
Switch#conf t
Enter configuration commands, one per line.?
End with CNTL/Z.
Switch(config)#ip access-list extended UDP—
DENY j
Switch(config)#ip access—list extended TCP—
DENY
Switch(config-ext-nacl)#deny udp any host
192.168.1.100 eq 80
Switch(config-ext-nacl)#deny tcp any host
192.168.1.100 eq 21
Switch(config-ext-nacl)#deny tcp any host
192.168.1.100 eq 22
Switch(config-ext-nacl)#permit ip any any
Switch(config)#intertace vlan 300
Switch(config)#ip access-group UDP-DENY out
Switch(config)#ip access—group TCP-DENY in
```

① 소스에서 타깃으로 ssh 차단된다.
❷ 소스에서 타깃으로 web이 차단된다.
③ 소스에서 타깃으로 ftp가 차단된다.
④ 소스에서 타깃으로 telnet이 차단된다.

27. 다음 중 스니핑 기법이 아닌 것은?

① Switch Jamming ② ICMP Redirect
③ ARP Redirect ❹ Syn Flooding

28. 다음의 보기에서 허니팟에 대한 특징을 모두 고르시오.

> 가. 비정상적인 접근을 탐지하게 위해 의도적으로 설치해 둔 시스템을 의미한다.
> 나. 공격자가 최대한 오래 머물게 해야 한다.
> 다. 실제 사용 중인 네트워크로부터 공격자를 떼어 놓을 수 있기 때문에 공격자의 주의를 딴 데로 뺏으려는 목적도 있다.
> 라. 회사의 규모가 커지고 허니팟을 이용하여 침입자를 잡는데 익숙해지면 허니팟 네트워크 즉, 허니넷을 만들 수 있다.
> 마. 공격자 성향(패턴)을 분석할 수 있다.

① 가 ② 가, 나
③ 가, 나, 다 ❹ 가, 나, 다, 라, 마

29. 다음 중 세션에 대한 특징으로 올바르지 못한 것은?

① 세션은 일정한 시간동안 웹 브라우저를 통해 종료하기까지의 시간을 말한다.
② 세션은 클라이언트가 아닌 서버에 세션 아이디를 저장한다.
③ 클라이언트 세션 아이디가 없으면 서버에서 발행해 생성한다.
❹ 세션은 서버나 클라이 언트 위치가 바뀌어도 계속 유지되어야 한다.

30. 다음 중 각 OSI 7 모델 중 계층과 프로토콜이 올바르게 연결된 것은?

❶ L2TP - 데이터 링크 계층
② IP - 전송 계층
③ PPP - 물리 계층
④ IEEE 802.11 - 데이터 링크 계층

31. 다음 중 MDM(Mobile Device Management)에 대한 설명으로 올바르지 못한 것은?
① 루팅을 하지 못하도록 제어가 가능하다.
② 하드웨어적 API를 이용하여 카메라 등을 제어한다.
③ 분실된 단말기의 위치 조회 및 원격 제어가 가능하다.
❹ 보안상 특정 앱만 통제하는 방식을 말한다.

32. 다음 중 APT(Advanced Persistent Threat) 공격 시 진행 형태가 아닌 것은?
① 침투(Incursion) ② 탐색 (Discovery)
③ 수집/공격(Capture/Attack) ❹ 방어 (Defence)

33. 침입 탐지 시스템에서 탐지 방법 중 악의적인 트래픽을 정상으로 판단하는 것을 무엇이라 하는가?
① False Positive ❷ False Negative
③ FAR ④ FRR

34. 다음 중 IP 프로토콜에 대한 설명으로 올바르지 못한 것은?
① 패킷 목적지 주소를 보고 최적의 경로를 찾아 패킷을 전송한다.
② 신뢰성보다는 효율성 에 중점을 두고 있다.
③ 헤더에 VERS는 버전을 나타낸다.
❹ TTL은 데이터 그램이 라우터를 지날 때마다 값이 +1씩 증가한다.

35. 다음 중 ARP 프로토콜에 대한 설명으로 올바르지 못한 것은?
① IP 주소를 알고 있을 때 MAC 주소를 알고자 할 경우 사용된다.
❷ AEP 테 이블에 매칭 되는 주소가 있을 때 AEP 브로드캐스팅 한다.
③ MAC 주소는 48비트 주소 체계로 되어 있다.
④ Opcode 필드가 2일 경우는 ARP Reply 이다.

36. 다음 중 서비스 거부(DoS) 공격에 대한 대응 방안으로 올바르지 못한 것은?
① 입력 소스 필터링 ② 블랙 홀 널(NULL) 처리
③ 위장한 IP 주소 필터링 ❹ 대역폭 증대

37. 다음 중 ARP 스푸핑 공격에 대한 설명으로 올바르지 못한 것은?
① 공격 대상은 같은 네트워크에 있어야 한다.
❷ 랜 카드는 정상 모드로 동작해야 한다.
③ 정상적인 상황에서 2개 이상 IP 주소를 가진 MAC이 보인다.
④ 공격자는 신뢰된 MAC 주소로 위장을 하고, 악의적인 공격을 한다.

38. 다음 중 스니핑 방지 대책으로 올바르지 못한 것은?
① SSL 암호화 프로토콜을 사용한다.
② 원격 접속 시 SSH를 통해 접속한다.
❸ MAC 주소 테이블을 동적으로 지정해 놓는다.
④ 스니핑 탐지 도구를 이용하여 정기적으로 점검한다.

39. 다음의 보기에서 설명하고 있는 네트워크 활용 공격 방법은 무엇인가?

> 헤더가 조작된 일련의 IP 패킷 조각들을 전송함으로써 공격이 이루어진다.

① DDoS ② Smurf
③ Land 공격 ❹ Teardrop 공격

40. 다음 중 침입 차단 시스템의 주요 기능으로 올바르지 못한 것은?
① 접근 통제 ② 감사 및 로깅 기능
❸ 침입 분석 및 탐지 ④ 프록시 기능

3과목 : 어플리케이션 보안

41. 다음 중 인터넷 표준 XML을 활용한 웹 표준 기술이 아닌 것은?
① UDDI ❷ OCSP
③ SOAP ④ WS0I

42. 다음의 보기에서 설명하고 있는 프로토콜은 무엇인가?

> 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 ❷ 이중 서명
③ 은닉 서명 ④ 전자봉투

43. 다음 중 신용 카드의 보안 코드 세 자리 번호와 관계가 없는 것은?
❶ CSS ② CID
③ CW ④ CVC

44. 다음 중 SSL 통신에서 한동안 통신을 하지 않다가 재통신할 때 보내는 메시지는?
① Server_Hello ② Client_Hello
③ Certificate ❹ Abbreviated Handshake

45. 다음 중 돈을 맡기고 나중에 물건을 받으면 입금하는 시스템을 무엇이라 하는가?
① Payment Gateway ② 에스크로
❸ E-Cash ④ Mondex

46. 다음 중 SSL 프로토콜에 대한 설명으로 올바르지 못한 것은?
① 보안성과 무결성을 유지하기 위해 마지막에는 HMAC을 붙인다.
② SSL/TLS의 가장 하위 단은 Record Protocol 이다.
❸ Record 프로토콜은 어떤 암호 방식을 사용할지 선택하는 역할을 한다.
④ SSL/TLS를 시작하기 위한 최초의 교신은 암호화와 MAC 없이 시작한다.

47. 다음 중 전자 투표 시스템의 요구 사항으로 올바르지 못한 것은?
① 완전성 ② 확인성
❸ 독립성 ④ 비밀성

48. 다음 중 FTP 서비스 공격 유형으로 올바르지 못한 것은?
① 무작위 대입 공격
② 스니핑에 의한 계정 정보 노출
❸ 인증된 사용자 FTP 서비스 공격
④ FTP 서버 자체의 취약점

49. 다음 중 전자 화폐의 성질이 다른 하나는 무엇인가?
① Mondex ❷ E-Cash
③ ChipKnip ④ Proton

50. 다음 중 OTP(One Time Password) 방식에 대한 설명으로 올바르지 못한 것은?
① 동기화 방식은 OTP 토큰과 서버간에 미리 공유된 비밀 정보와 동기화 정보에 의해 생성되는 방식이다.
❷ 동기화 방식은 OTP 토큰과 서버간에 동기화가 없어도 인증이 처리된다.
③ 이벤트 동기화 방식은 서버와 OTP 토큰이 동일한 카운트 값을 기준으로 비밀번호를 생성한다.
④ 조합 방식은 시간 동기화 방식과 이벤트 동기화 방식의 장점을 조합하여 구성한 방식이다.

51. FTP 서버가 데이터를 전송할 때 목적지가 어디인지를 검사하지 않는 설계상의 문제점을 이용한 공격을 무엇이라 하는가?
① 어나니머스 공격 ❷ 바운스 공격
③ 무작위 대입 공격 ④ 스니핑 공격

52. 다음 중 메일 서비스 관련 프로토콜이 아닌 것은?
① MUA ② MDA
③ MTA ❹ MDM

53. 다음 중 스팸 어세신의 분류 기준으로 올바르지 못한 것은?
❶ 첨부 파일 검색 ② 헤더 검사
③ 본문 내용 검사 ④ 주요 스팸 근원지와 자동 생성

54. 다음 중 S/MIME이 제공하는 보안 서비스가 아닌 것은?
① 메시지 무결성 ② 메시지 기밀성
③ 부인 방지 ❹ 메시지 가용성

55. 다음의 보기에서 설명하고 있는 보안 전자 우편 프로토콜은?

- IETF 인터넷 보안 표준안 - 중앙에 집중화 된 키 인증 - 구현이 어려움 - 군사용, 은행용 시스템에 주로 사용

❶ PEM ② S/MIME
③ PGP ④ MIME

56. 다음의 보기에서 설명하고 있는 웹 보안 취약점은 무엇인가?

어플리케이션이 신뢰할 수 없는 데이터를 가져와 적절한 검증이나 제한 없이 웹 브라우저로 보낼 때 발생한다. 공격자가 피해자의 브라우저에 스크립트를 실행하여 사용자 세션 탈취, 웹 변조, 악의적인 사이트로 이동할 수 있다.

① SQL Injection ❷ XSS
③ CSRF ④ Webshell

57. 웹 취약점 공격 방지 방법 중 올바르지 못한 것은?
① 임시 디렉터리에 업로드 된 파일을 삭제하거나 이동한다.
② 첨부 파일에 대한 검사는 반드시 서버 측면스크립트에서 구현한다.
❸ 쿠키 저장 시 원활한 사이트 접속을 위해 타인이 읽을 수 있도록 한다.
④ 사용 중인 SQL 구문을 변경시킬 수 있는 특수 문자가 있는지 체크한다.

58. 다음 중 Mod_Security 기능에 포함되지 않는 것은?
① Request Filtering
② Audit Logging
❸ No Understanding of the HTTP Protocol
④ HTTPS Filtering

59. 다음 중 대표적인 윈도우 공개용 웹 방화벽은 무엇인가?
① Inflex ❷ WebKnight
③ Mod_Security ④ Public Web

60. 다음 중 DNS가 가지고 있는 보안 취약점을 극복하기 위한 DNS 확장 표준 프로토콜은?
① DNS Protection ② DNS Defence
❸ DNSSEC ④ DNS Poisoning

4과목 : 정보 보안 일반

61. 다음 중 올바르지 못한 것은?
① CRL은 갱신되어야만 폐기로 판단한다.
② CA가 인증서 폐기 시 폐기 목록을 일정한 주기마다 생성한다.
❸ OCSP는 무료로 사용이 가능하다.
④ CRL은 비용 지불 없이 사용이 가능하다.

62. 다음 중 주체가 속해 있는 그룹의 신원에 근거해 객체에 대한 접근을 제한하는 방법은?
① 역할기반 접근통제 ② 강제적 접근통제
❸ 임의적 접근 통제 ④ 상호적 접근 통제

63. 다음 중 커버로스에 대한 설명으로 올바르지 못한 것은?
① 패스워드 추측 공격에 취약하다.
❷ 커버로스는 공개키 방식을 이용하여 티켓을 발급한다.
③ MIT에서 개발한 분산환경 하에서 개체 인증서비스를 제공한다.

④ 커버로스는 4개의 개체로 구성된다.

64. 다음의 접근 통제 모델 중 보기에 알맞은 모델은 무엇인가?

> 비군사적 조직에 있어서 무결성을 더 중요시 하였다. 주어진 무결성보다 낮은 무결성 등급에서는 읽을 수 없다. (No Read Down)

① 벨-라파둘라 모델 ❷ 비바 모델
③ 클락-윌슨 모델 ④ 접근 통제 매트릭스

65. 다음 중 암호화 알고리즘에 대한 설명으로 올바르지 못한 것은?

① 평문을 암호학적 방법으로 변환한 것을 암호문 (Ciphertext) 이라 한다.
② 암호학을 이용하여 보호해야 할 메시지를 평문 (Plaintext) 이라 한다.
❸ 암호화 알고리즘은 공개로 하기 보다는 개별적으로 해야 한다.
④ 암호문을 다시 평문으로 변환하는 과정을 복호화 (Decryption) 라 한다.

66. 다음 중 SPN 구조와 Feistel 구조에 대한 설명으로 틀린 것은?

① Feistel 구조는 평문 두 개의 블록으로 나누어 배타적 논리합과 라운드를 가진다.
② Feistel 구조는 전형 적 인 라운드 함수로 16라운드를 거친다.
❸ SPN 구조는 역 변환 함수에 제약이 없다.
④ SPN 구조는 S-BOX와 P-BOX를 사용한다.

67. 다음 중 전자 서명과 공개키 암호화 방식에서 사용되는 키로 알맞게 연결된 것은?

① 공개키 - 공개키 ❷ 개 인키 _ 공개키
③ 개인키 ㅡ 개인키 ④ 공개키 - 개 인키

68. 다음 중 RSA 암호 알고리즘에 대한 설명으로 올바르지 못한 것은?

❶ 이산 대수 어려움에 기반한 암호 알고리즘이다.
② 1978년 Rivest, Shamir, Adleman에 의해 만들어 졌다.
③ 공개키 암호 시스템은 키 사전 분배를 해결하였다.
④ 디지털 서명과 같은 새로운 개념을 출현시켰다.

69. 다음의 보기에서 성질이 같은 것으로 연결된 것은?

> 가. DES 나. AES 다. RSA
> 라. Elgamal 마. Rabin

① 가, 나 ② 가, 다, 라
❸ 다, 라, 마 ④ 나, 다, 라

70. 다음 중 인증 기관(Certification Authority)에 대한 설명으로 올바르지 못한 것은?

① 인증서를 발급한다.
② 유효한 인증서와 CRL의 리스트를 발행한다.
③ 인증서 상태 관리를 한다.
❹ 인증서와 CRL을 사용자에게 분배하는 역할을 한다.

71. 다음 중 WPKI의 구성 요소가 아닌 것은?

❶ RA ② WPKI CA
③ CP 서버 ④ OCSP 서버

72. 다음 중 키 사전 분배 방식에 대한 설명으로 올바르지 못한 것은?

① 중앙 집중식 방식은 가입자가 비밀 통신을 할 때마다 KDC로부터 세션키를 분배 받는다.
② Blom 방식은 두 노드에게 임의 함수 값을 전송하면 두 노드는 전송 받은 정보로부터 두 노드 사이의 통신에 필요한 세션키를 생성한다.
③ 중앙 집중식 방식의 대표적 인 분배 방식은 커버로스 방식이다.
❹ 중앙 집중식 방식 일 경우 암호 통신을 할 때마다 세션키를 변경할 필요는 없다.

73. 다음의 보기에서 설명하고 있는 서명 방식은 무엇인가?

> 사용자 A가 서명자 B에게 자신의 메시지를 보여주지 않고, 서명을 얻는 방법을 말한다. 메시지의 비밀성을 지키면서 타인에게 인증을 받고자 하는 경우에 주로 사용산다.

① 이중 서명 ❷ 은닉 서명
③ 전자 서명 ④ 영지식증명

74. 다음 중 Diffie-Hellman 키 교환 프로토콜에 대한 설명으로 올바르지 못한 것은?

① 1976년에 발표 되었으며, 공개키 암호에 대한 시초가 되었다.
❷ 신분 위장이나 재전송 공격에 강하다.
③ DH 알고리즘은 이산 대수 계산의 어려움에 의존한다.
④ 네트워크상에서 A와 B가 비밀키를 서로 만나지 않고도 공유할 수 있는 방법을 제시하였다.

75. 다음 중 ITU에 의해 제안된 인증서에 대한 기본형식을 정의한 규격을 무엇이라 하는가?

① SOA ② CRL
❸ X.509 ④ OGSP

76. 다음 중 x.509 v3에서 확장 영역을 구분하는 것에 포함되지 않는 것은?

① 인증서 경로 및 규제 정보 ② CRL을 위한 확장자
③ 키 및 정책 확장자 ❹ 공개키 정보

77. 다음 중 전자 서명의 특징으로 올바르지 않는 것은?

❶ 재사용 가능 ② 위조 불가
③ 부인 불가 ④ 서명자 인증

78. 다음 중 공개키 인증서의 구성 요소에 포함되지 않는 것은?

① 인증서 정책 ② 인증서 경로
❸ 비밀키 인증서 ④ 인증서 철회 리스트

79. 다음 중 인증 기관의 역할별로 올바르게 연결되지 못한 것은?

① PAA - 정책 승인 기관 ❷ PCA - 정책 승인 기관

③ CA _ 인증 기관 ④ RA - 등록 기관

80. 다음 중 인증서 폐기의 사유가 아닌 것은?

① 비밀키 손상 ② 기간 만료
③ 공개키 손상 ❹ 공개키 노출

5과목 : 정보보안 관리 및 법규

81. 다음 중 정보보호 관리 체계(ISMS)의 관리 과정순서로 올바른 것은?

가. 정보보호 정책 수립 및 범위 설정
나. 위험관리
다. 사후 관리
라. 경영진 책임 및 조직 구성
마. 정보보호 대책 구현

① 마-라-다-나-가 ② 가-나-다-라-마
❸ 가-라-나-마-다 ④ 나-가-다-라-마

82. 다음 중 개인정보 유출 시 신고해야 하는 기관과 가장 관련이 깊은 곳은?

① 한국산업기술진흥원 ② 한국콘텐츠진흥원
❸ 한국인터넷진흥원 ④ 한국정보통신진흥원

83. 다음 중 물리적 보안의 예방책으로 올바르지 못한 것은?

① 화재 시 적절한 대처 방법을 철저히 교육한다.
② 적합한 장비 구비 및 동작을 확인한다.
❸ 물 공급원(소화전)을 멀리 떨어진 곳에 구비한다.
④ 가연성 물질을 올바르게 저장한다.

84. 다음 중 개인정보 수집 및 이용 시 정보 주체의 동의를 받지 않아도 되는 것은?

❶ 제한구역에 신분증을 받고 다시 반납할 경우
② 교사가 학생 상담을 위하여 수첩에 이름, 주소 등을 기록할 경우
③ 치과에서 스켈링 후 의료 보험을 적용할 경우
④ 경품 제공을 위한 개인정보를 수집할 경우

85. 다음의 보기에서 정성적 위험 분석 방법으로연결된 것은?

가. 과거 자료 분석법	나. 수학 공식 접근법
다. 확률 분포법	라. 델파이법
마. 시나리오법	

① 나, 다, 라 ② 가, 나, 다
❸ 라, 마 ④ 가, 나, 마

86. 다음은 위험 분석 방법론에 대한 설명이다. 올바르지 못한 것은?

① 과거 자료 분석법 : 과거 자료를 통하여 위험 발생 가능성을 예측
② 수학 공식 접근법 : 위험 발생 빈도를 계산하는 식을 이용하여 계량화
❸ 우선 순위법 : 전문가 집단을 이용한 설문 조사를 통한 조사 방법
④ 시나리오법 : 특정 시나리오를 통해 발생 가능한 위협에 대해 결과를 도출해 내는 방법

87. 다음 중 외주 업체 정보보호 원칙으로 올바르지 못한 것은?

① 외주 업체는 수탁사로 위탁사 관리/감독을 받는다.
② 외주 업체가 내부와 동일한 정보보호 정책을 적용한다.
❸ 외주 업체도 내부와 동등한 권한을 부여한다.
④ 외주 업체가 내부 서버 접속 시 외주 업체 책임자에게 확인을 받는다.

88. 다음 중 전자서명법에 대한 설명으로 올바르지 못한 것은?

① 전자서명 생성 정보는 전자서명을 생성하기 위해 이용하는 전자적 정보를 말한다.
② 전자서명 검증 정보는 전자서명을 검증하기 위해 이용하는 전자적 정보를 말한다.
❸ 인증은 전자서명 검증 정보가 가입자에게 유일하게 속한다는 사실을 확인하고, 증명 하는 행위를 말한다.
④ 인증서는 전자서명 생성 정보가 가입자에게 유일하게 속한다는 사실을 확인하고, 이를 증명하는 전자적 정보를 말한다.

89. 다음의 ( ) 안에 알맞은 용어는 무엇인가?

전자문서는 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 (가)인 형태로 작성되어 송수신되거나 저장된 문서 형식의 자료로서 (나)된 것을 말한다.

① 가 - 전기적, 나 _ 정형화
❷ 가 - 전자적, 나 - 표준화
③ 가 - 전기적, 나 - 표준화
④ 가 - 전자적, 나 - 정형화

90. 다음 중 대통령 직속 기구에 속하는 기관은?

① 정보통신기반보호위원회 ❷ 개인정보보호위원회
③ 공정거래위원회 ④ 국가권익위원회

91. 다음의 보기에서 설명하는 위험 분석 접근법은 무엇인가?

자산 분석, 위협 분석, 취약성 분석의 각 단계를 수행하여 위험을 분석하는 것을 말한다.

① 베이스 라인 접근법 ② 비정형 접근법
❸ 상세 위험 분석 ④ 혼합 접근법

92. 다음 중 위험 통제 시점에 따라 통제 구분에 포함되지 않는 것은?

① 예방통제 ② 탐지통제
❸ 교정 통제 ④ 잔류 위험

93. 다음 중 업무 연속성에서 사업 영향 평가의 주요 목적에 포함되지 않는 것은?

① 핵심 우선 순위 결정 ❷ 복구 계획 수립
③ 중단시간산정 ④ 자원 요구 사항

94. 다음 중 사례 연구 또는 시나리오 기반으로 복구, 운영 계획 집행 및 절차에 대한 제반 사항에 대해 1차 사이트에서 가상으로 수행하는 복구 테스트 방법은?

① 체크 리스트 ② 구조적 점검

❸ 시뮬레이션 ④ 병렬테스트

95. 다음 중 OECD 정보보호 가이드라인에 포함되지 않는 것은?
❶ 대책 ② 대응
③ 책임 ④ 인식

96. 다음 중 유럽의 보안성 평가 기준은 무엇인가?
❶ ITSEC ② TCSEC
③ CTCPEG ④ DTIEC

97. 다음 중 정보보호 관리 체계의 정보보호 관리 과정에 포함되지 않는 것은?
① 정보보호 정책 수립 및 범위 설정 ② 사후 관리
③ 정보보호 대책 구현 ❹ 구현

98. 다음 중 정보보호 관리 체계에서 접근 통제 분야에 포함되지 않는 것은?
① 사용자 인증 및 식별 ② 접근 권한 관리
③ 데이터베이스 접근 ❹ 침해 시도 모니터링

99. 다음 중 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에서 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우 알려야 하는 사항에 포함되지 않는 것은?
① 개인정보수집 목적 ② 수집하려는 개인정보의 항목
③ 개인정보 보유 기간 ❹ 동의하지 않을 시 불이익

100. 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에서 개인정보 유효 기간제로 인하여 로그인하지 않는 개인정보는 별도 보관이나 파기해야 한다. 다음 중 개인정보 유효 기간은 얼마인가?
❶ 1년 ② 3년
③ 5년 ④ 7년

1	2	3	4	5	6	7	8	9	10
②	①	④	②	①	④	②	④	④	②
11	12	13	14	15	16	17	18	19	20
④	②	②	④	③	③	③	④	②	③
21	22	23	24	25	26	27	28	29	30
①	③	④	③	④	②	④	④	④	①
31	32	33	34	35	36	37	38	39	40
④	④	②	④	②	④	②	③	④	③
41	42	43	44	45	46	47	48	49	50
②	②	①	④	③	③	③	③	②	②
51	52	53	54	55	56	57	58	59	60
②	④	①	④	①	②	③	③	②	③
61	62	63	64	65	66	67	68	69	70
③	③	②	②	③	③	②	①	③	④
71	72	73	74	75	76	77	78	79	80
①	④	②	②	③	④	①	③	②	④
81	82	83	84	85	86	87	88	89	90
③	③	③	①	③	③	③	③	②	②
91	92	93	94	95	96	97	98	99	100
③	③	②	③	①	①	④	④	④	①