1과목 : 시스템 보안

1. 다음 중 주로 카메라, DVR 등 인터넷에 연결된 기기들을 감염시켜 봇넷을 만든 후 디도스(DDoS) 공격을 수행하는 악성코드는?
   ① 백오리피스(BackOrifice) 악성코드
   ② 다이어(Dyre) 악성코드
   ③ 미라이(Mirai) 악성코드
   ④ 워너크라이(Wannacry) 악성코드

2. 계정의 패스워드를 암호화된 형태로 저장하고 있는 파일은?
   ① /etc/security ② /etc/shadow
   ③ /etc/profile ④ /etc/login.defs

3. Internet Explorer의 검색 히스토리는 어느에 저장되는가?
   ① config.sys ② command.com
   ③ index.dat ④ sys.bak

4. ftp 접근 여부를 검토할 수 있는 로그는?
   ① utmp ② sulog
   ③ wtmp ④ xferlog

5. Null Session 공유 취약점을 가지고 있는 것은?
   ① C$ ② Print$
   ③ IPC$ ④ ADMIN$

6. root 계정과 동일한 권한을 가진 계정은?
   ① chalie 계정 uid: 0 gid: 200
   ② sally 계정 uid: 100 gid: 0
   ③ johny 계정 uid: 10 gid: 10
   ④ sara 계정 uid: 10 gid: 200

7. 다음 지문에서 설명하는 크래킹 방법은?

> 패스워드에 사용될 수 있는 문자열의 범위를 정하고, 그 범위 내에서 생성 가능한 모든 패스워드를 생성하여 이를 하나씩 대입, 패스워드 일치 여부를 확인한다.

   ① Rainbow Table Attack ② Dictionary Attack
   ③ Brute Force Attack ④ Hash Attack

8. 리눅스 서버 관리자 A씨는 피해 시스템을 점검하던 중 다음과 같은 시스템 바이너리 파일들이 변조된 것을 확인하였다. 공격자의 입장에서 파일을 변조한 이유가 잘못 연결된 것은?
   ① ps, top: 특정 프로세스 정보를 숨김
   ② ls, du: 특정 파일이나 디렉터리를 숨김
   ③ w, who: 특정 사용자의 정보를 숨김
   ④ ifconfig: 특정 IP에서의 접속을 숨김

9. 소유자에게만 읽기와 쓰기 권한이 있는 경우는?
   ① rwxr--r-- 1 root root 312 Nov 30 13:05 listner.ora
   ② r-xrw-r-- 1 root root 312 Nov 30 13:05 listner.ora
   ③ rwxrw-rw- 1 root root 312 Nov 30 13:05 listner.ora
   ④ rwxr—rw- 1 root root 312 Nov 30 13:05 listner.ora

10. 다음 빈 칸 들어갈 서비스명으로 적절한 것은?

> (㉠) 서비스는 별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게 해주는 프로세스 간 프로토콜로써 어떤 프로그램이 네트워크상의 다른 컴퓨터에서 작동하는 프로그램에 서비스를 요청하는 데 사용되는 프로토콜이다.
> XML(㉠)라는 서비스는 XML 기반의 분산시스템 통신방법으로, (㉠) 호출에 대해 XML 형태로 매개변수나 리턴값을 반환하는 방식이다.

   ① RPC ② SSHD
   ③ Bluetooth ④ NFS

11. 다음 지문에서 설명은?

> - MINIX File System을 보완하며, 최대 2G까지 파일시스템 크기를 지원한다.
> - 255byte까지 파일명을 지원한다.
> - 접근제어, inode 수정, 타임스탬프 수정 등의 기능이 불가능하다.
> - 사용할수록 단편화가 심해진다.

   ① FAT16 ② FAT32
   ③ NTFS ④ EXT

12. 다음 중 윈도우 로그 종류와 설명이 가장 바르게 짝지어진 것은?
   ① 계정 관리 감사 - 사용자 권한 할당 정책, 감사 정책, 신뢰 정책의 변경과 관련된 사항을 로깅한다.
   ② 정책 변경 감사 - 권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.
   ③ 개체 액세스 감사 - 특정 파일이나 디렉터리, 레지스트리 키 등과 같은 객체에 대한 접근을 시도하거나 속성 변경 등을 탐지한다.
   ④ 로그인 이벤트 감사 - 시스템의 시작과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.

13. tcpwrapper의 설정파일의 내용이 다음과 같을 때, 어떤 현상이 발생하는가?

```
/etc/hosts.deny
All: All
/etc/hosts.allow
All: All
```

   ① 모든 접속이 허용된다.
   ② 모든 접속이 차단된다.
   ③ 일부 서비스는 모두 허용되고 일부 서비스는 모두 차단된다.
   ④ 알 수 없다.

14. wtmp 로그 파일에 대한 설명 중 옳지 않은 것은?
   ① 사용자의 로그인 및 로그아웃 정보 포함

② 로그인 실패 정보 포함
③ 바이너리 형태로 저장
④ 시스템 종료 및 부팅 정보 포함

15. 다음 지문에서 설명하고 있는 것은?

> 리눅스에서 시스템 관리자가 응용프로그램들이 사용자를 인증하는 방법을 선택할 수 있도록 해주는 공유라이브러리 묶음으로 이것을 사용하는 응용프로그램을 재컴파일 하지 않고, 인증방법을 변경할 수 있다.

① sudo ② PAM
③ Shell script ④ Batch file

16. 리눅스 운영체제 특수 권한에 대한 설명으로 틀린 것은?
① SetGID가 부여된 파일은 소유 그룹의 실행 권한이 x에서 s로 변경
② SetUID가 부여된 파일은 소유자의 실행 권한이 x에서 s로 변경
③ Sticky bit가 부여된 디렉터리는 그 외 사용자의 실행 권한이 x에서 s로 변경
④ Sticky bit는 /tmp와 같은 777 권한의 공용 디렉터리에서 파일 삭제 문제를 해결

17. 각 파일확장자에 대한 정보와 관련 응용프로그램 간의 연결에 대한 정보를 포함하고 있는 윈도우 레지스트리 키는?
① HKEY_CLASSES_ROOT ② HKEY_LOCAL_MACHINE
③ HKEY_CURRENT_CONFIG ④ HKEY_USERS

18. 다음 지문에서 설명하는 것은?

> 이것은 실시간 트래픽 분석과 IP 네트워크상에서 패킷 로깅이 가능한 가벼운(Lightweight) 네트워크 침입탐지시스템이다. 또한 프로토콜 분석, 내용 검색/매칭을 수행할 수 있으며, 오버플로우, Stealth 포트스캔, CGI 공격, SMB 탐색, OS 확인 시도 등의 다양한 공격과 스캔을 탐지할 수 있다.

① wireshark ② tripwire
③ snort ④ iptables

19. 빈칸 ㉠, ㉡에 들어갈 용어를 바르게 짝지은 것은?

> (㉠) 공격 기법이란 해커가 홈페이지를 해킹한 후, 취약점에 따른 (㉡) 코드가 있는 악성 스크립트를 은닉시키고 취약한 PC 환경의 이용자가 접속할 경우 악성코드가 다운로드 되는 공격 기법으로, 사용자의 개입 없이 접속만으로도 악성코드에 감염될 수 있다.

① ㉠ Web Shell ㉡ Fuzzing
② ㉠ Spear Phishing ㉡ Fuzzing
③ ㉠ File Upload ㉡ Exploit
④ ㉠ Drive By Download ㉡ Exploit

20. UNIX 또는 리눅스 시스템에서 똑같은 작업을 사용자가 지정된 시간에 반복 작업하기 위해서 cron 테이블을 작성한다. 사용자가 매주 토요일 오전 10시 정각에 'mytest' 라는 프로그램을 주기적으로 수행시키기 위해 작성한 cron 테이블 내용으로 맞는 것은?
① 0 10 6 * * mytest ② 0 10 * * 6 mytest
③ 0 10 * 6 * mytest ④ 0 10 6 * * mytest

2과목 : 네트워크 보안

21. 다음 지문에서 설명하고 있는 보안 기술은?

> 이 기술은 정보유출 사고들이 증가함에 따라 내부의 모든 문서의 중요한 자료에 대한 정보유출을 방지하기 위한 기술로, 매체제어(USB, 하드디스크 등), 통신규격 제어(블루투스, LTE 등)를 통해 기밀 자료가 유출되는 것을 막는 솔루션이다.

① DRM ② DLP
③ IPS ④ Firewall

22. DDoS(Distributed Denial of Service) 공격에 대한 공격유형을 파악하려고 한다. 이때 유입 트래픽을 확보하기 위해 사용될 수 있는 도구로는?
① argus ② ngrep
③ tcpdstat ④ tcpdump

23. NAC의 주요 기능으로 옳지 않은 것은?
① PC 및 네트워크 장치 통제
② 접근제어 및 인증
③ 폭탄 메일이나 스팸 메일 차단
④ 해킹, 웜, 유해 트래픽 탐지 및 차단

24. 스머프 공격에서 echo request 패킷을 수신 서브넷 전체에 전달하기 위해 라우터의 해당 인터페이스에서 활성화해야 하는 것은?
① ip direct broadcast ② ICMP Redirect
③ ARP Spoofing ④ Switch Jamming

25. 다음 중 침입탐지시스템 및 침입방지시스템에 대한 설명으로 틀린 것은?
① 침입탐지시스템에서 문자열을 비교하여 네트워크 패킷을 검사하는 방법은 Signature-based Detection의 일종이다.
② Anomaly Detection은 정상 행위를 규정하여 공격을 탐지하는 방법이다.
③ 알려지지 않은 공격을 Signature-based Detection 방법으로 탐지할 수 있다.
④ 침입방지시스템은 침입자에게 시스템이나 네트워크를 사용하지 못하게 하는 등 능동적인 기능을 수행할 수 있다.

26. 다음 중 방화벽의 기능과 가장 거리가 먼 것은?
① 접근제어 ② 데이터 필터링과 축약
③ 로깅과 감사추적 ④ 인증

27. 다음 빈칸 ㉠에 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 ② SCADA
③ Modbus ④ Stuxnet

28. 다음 보기 중 서비스 이름과 잘 알려진 포트(well-known port) 번호가 잘못된 것은?
① IMAP - 134 ② HTTPS - 443
③ SMTP - 25 ④ FTP - 20, 21

29. 다음 괄호에 들어갈 내용으로 올바르게 순서대로 나열한 것은?

DHCP에서는 전송계층으로 (㉠) 프로토콜을 사용하는데, 서버는 잘 알려진 (㉡) 포트를 사용하고, 클라이언트는 잘 알려진 (㉢) 포트를 사용한다.

① ㉠ UDP ㉡ 67 ㉢ 68 ② ㉠ TCP ㉡ 67 ㉢ 68
③ ㉠ TCP ㉡ 68 ㉢ 67 ④ ㉠ UDP ㉡ 68 ㉢ 67

30. DDoS 공격을 인지하기 위해 사용하는 방법으로 부적절한 것은?
① 방화벽, IDS 등에서 유입 트래픽 크기를 조사한다.
② 동시 접속정보에 대하여 평시 대비 증감율을 비교한다.
③ 웹서버 접속로그를 확인하여 비정상 접속 증가여부를 확인한다.
④ 서버에서 유출되는 트래픽을 샘플링하여, 실제 트래픽을 분석한다.

31. 다음 지문에서 설명하는 DDoS 공격은?

TCP/IP 스택(Stack) 자원을 소모하는 특징이 있으므로 소스 IP별로 PPS 임계치를 설정하거나 패킷 헤더 검사를 통해 정상적인 옵션 필드값을 갖지 않는 비정상 패킷을 차단한다.

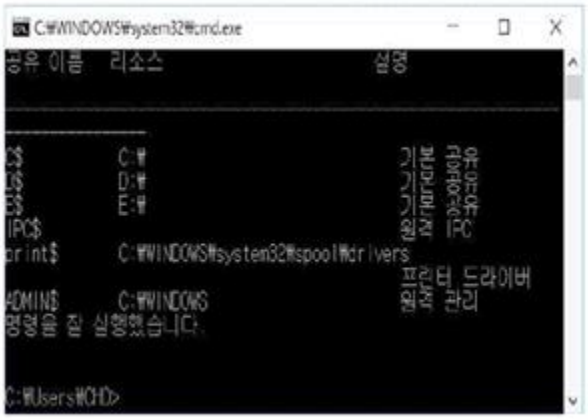
① UDP Flooding ② SYN Flooding
③ Slow Header Flooding ④ ICMP Flooding

32. 네트워크 기반 공격 기술 중 DDoS 공격의 설명으로 옳은 것은?

㉠ DDoS 공격이란 다수의 컴퓨터를 이용하여 특정 사이트를 공격하는 방식이다.
㉡ DDoS 공격의 목표는 공격 대상 서버가 처리할 수 없는 과도한 접속(트래픽)을 유발하여 시스템을 마비시키는 것이다.
㉢ 일반적으로 좀비 PC들이 이 공격에 활용된다.

① ㉠ ② ㉡, ㉢
③ ㉠, ㉡ ④ ㉠, ㉡, ㉢

33. 윈도우 명령어는?



① net use ② net share
③ net share ④ net computer

34. IP Spoofing 공격과 가장 거리가 먼 것은?
① SYN Flooding 공격 ② RST를 이용한 접속 끊기
③ 순서번호 추측 ④ slowloris 공격

35. 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.

36. 포트가 열린 경우 응답이 다른 것은?
① NULL 스캔 ② TCP SYN 스캔
③ FIN 스캔 ④ XMAS 스캔

37. WPA2 CCMP 모드에서 무선구간 데이터 보호를 위해 사용되는 암호화 알고리즘은?
① AES ② RC5
③ TKIP ④ DES

38. 다음 지문에서 설명하는 것은?(문제 복원 오류로 지문 내용이 없습니다. 정확한 지문 내용을 아시는분 께서는 오류신고를 통하여 내용 작성 부탁 드립니다. 정답은 3번 입니다.)
① Threat Profiling ② Heuristic Analysis
③ Sandbox ④ Injector

39. 다음 지문이 설명하는 컴퓨팅 기술은? <17.10회.기사>

기존 기술에 없었던 가상화와 공유 및 임대 서비스 등은 시스템 체계 및 네트워크 체계에 큰 변화를 예고하고 있다. 컴퓨팅 서비스로 IaaS, PaaS, SaaS 등이 대표적이다.

① 마스터/슬레이브 ② 클라이언트/서버
③ 클라우드 ④ 피어 투 피어

40. 빈 칸에 들어갈 용어를 바르게 짝지은 것은?

> 802.11 무선 표준에서는 무선랜의 구성에 따라 2개의 구성유형이 제시되고 있다. 첫 번째는 (㉠) 모드로 무선 AP와 무선 단말기로 구성되는 방식과, 두 번째는 무선 단말기 사이에 직접 통신이 이뤄지는 (㉡) 모드이다.

① ㉠ WLAN ㉡ Broadcast
② ㉠ Infrastructure ㉡ Ad Hoc
③ ㉠ APD ㉡ Peer to Peer
④ ㉠ VPN ㉡ Peer to Peer

3과목 : 어플리케이션 보안

41. 다음 지문에서 설명하고 있는 공격은?

> FTP 서버에 PORT 명령을 전송하여 서버로 하여금 공격 대상 호스트에 접속하게 하는 공격
> 공격자 호스트의 IP를 숨긴 채 공격 대상 호스트의 포트를 모두 조사하는 데 사용될 수 있음

① port attack ② bounce attack
③ IP Spoofing ④ port scan

42. 포렌식 조사 원칙 중 틀린 것은?

① 기밀성의 원칙: 수집 증거가 명백히 허가된 대상에게만 제공되어야 함.
② 무결성의 원칙: 수집 증거가 위·변조 되지 않았음을 증명해야 함.
③ 재현의 원칙: 같은 조건에서 항상 같은 결과가 나와야 함.
④ 신속성의 원칙: 전 과정이 지체 없이 신속하게 진행되어야 함.

43. 합법적으로 소유하고 있던 사용자들의 도메인을 탈취하거나 DNS 조작을 통해 사용자들이 정확한 웹페이지 주소를 입력하더라도 가짜 웹페이지에 접속하도록 유도하여 개인정보를 훔치는 공격 방식은?

① 피싱 공격 ② 스피어 피싱 공격
③ 파밍 공격 ④ 워터링 홀 공격

44. 이메일 공격유형 중 HTML 기능이 있는 클라이언트나 웹브라우저 사용자를 대상으로 하는 공격기법은?

① Buffer Overflow 공격 ② Active contents 공격
③ 스팸메일 공격 ④ 트로이목마 공격

45. FTP 서비스를 운영할 때 준수하여야 할 보안사항으로 부적절한 것은?

① FTP 서비스는 필요한 경우에만 활성화하며, Secure FTP 또는 Trivial FTP 등을 사용한다.
② 관리자 외에는 읽기권한만 부여한다.
③ FTP 연결시간(timeout)을 제한한다.
④ FTP 서버에는 중요 문서 또는 보안파일을 저장하지 않는다.

46. 다음 중 포맷 스트링 취약점 동작과 가장 거리가 먼 것은?

① 프로세스 권한 상승 ② 임의의 코드 실행
③ 메모리 내용 변경 ④ 프로세스 메모리 보기

47. XSS 공격에 대한 설명으로 옳은 것은?

① 자료실에 올라간 파일을 다운로드할 때 전용 다운로드 프로그램이 파일을 가져오는데, 이때 파일 이름을 필터링 하지 않아서 취약점이 발생한다.
② 악성 스크립트를 웹 페이지의 파라미터 값에 추가하거나, 웹 게시판에 악성 스크립트를 포함시킨 글을 등록하여 이를 사용자의 웹 브라우저 내에서 적절한 검증 없이 실행되도록 한다.
③ 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법이다.
④ 데이터베이스를 조작할 수 있는 스크립트를 웹 서버를 이용하여 데이터베이스로 전송한 후 데이터베이스의 반응을 이용하여 기밀 정보를 취득하는 공격 기법이다.

48. 사용자가 http://www.kisa.or.kr에 접속하기 위해 IP 주소를 얻어오는 순서는?

① 로컬 DNS 서버 → 캐시 → Hosts 파일
② Hosts 파일 → 캐시 → 로컬 DNS 서버
③ 로컬 DNS 서버 → Hosts 파일 → 캐시
④ 캐시 → Hosts 파일 → 로컬 DNS 서버

49. SET에서 주문정보와 지불정보의 해시값을 결합하여 생성된 메시지에 다시 해시함수를 적용한 후 그 결과를 고객의 개인키로 암호화하는데 이 과정을 의미하는 용어는?

① 전자 서명 ② 은닉 서명
③ 이중 서명 ④ 영지식 서명

50. CPU 하드웨어에 존재하는 부채널 관련 버그로써 빠른 수행을 위해 개발된 캐싱 및 추측 실행 기능을 악용하는 공격의 명칭은?

① merkle tree ② spectre
③ man-in-the-middle ④ covert channel

51. SQL 인젝션 공격에 대응하는 효과적인 방법이 아닌 것은?

① 데이터베이스 내장 프로시저를 사용
② 원시 ODBC 에러를 사용자가 볼 수 없도록 코딩
③ 사용자가 입력하여 서버로 전송되는 파라미터값을 검증
④ DB 애플리케이션의 접근권한을 최대한 허용

52. 다음에서 설명하는 웹 서비스 공격은?

> 공격자가 사용자의 명령어나 질의어에 특정한 코드를 삽입하여 DB 인증을 우회하거나 데이터를 조작한다.

① 직접 객체 참조 ② Cross Site Request Forgery
③ Cross Site Scripting ④ SQL Injection

53. 다음 지문에서 설명하는 공격 기법은?

이것은 보안장비에서 사용하는 도메인네임 기반 탐지/차단을 우회하기 위하여 사용하는 기법으로 희생자를 악성코드 유포서버에 접속시키고자 유도할 때, 바로 악성코드 유포서버로 접속시키지 않고, 먼저 중간 단계의 서버에 접속시킨 다음, 그곳으로부터 악성코드 유포서버로 접속시키는 기법을 사용한다. 이때 중간 단계의 서버 및 유포 서버를 지정할 때 사용되는 기법이다.

① DNS Zone transfer ② Domain Shadowing
③ DNS Spoofing ④ Fast Flux Hosting

54. 스마트카드 보안 기술에 대한 설명 중 틀린 것은?
① 사용자 식별과 인증을 위해 필요한 정보를 저장하고 관리하는 모듈로 WIM(Wireless Identity Module)을 사용한다.
② 개인 이동성과 서비스 이동성을 겸비한 이동 통신용 스마트카드를 USIM(Universal Subscriber Identity Module)이라고 한다.
③ USIM은 ME(Mobile Equipment)와 인터페이스하기 위해 T=0 통신 프로토콜을 사용한다.
④ WIM은 WTLS와 연계하여 사용할 수 없다.

55. SSL 핸드셰이크 과정에서 End-to-End에 오류가 발생하면 사용자에게 경고하는 프로토콜은?
① 핸드셰이크 프로토콜 ② 암호규격변경 프로토콜
③ Alert 프로토콜 ④ SSL Record 프로토콜

56. 다음 중 SSO 방식과 가장 거리가 먼 것은?
① RADIUS ② SPNEGO
③ Kerberos ④ SESAME

57. SSL/TLS에 대해 잘못 설명한 것은?
① SSL/TLS는 메시지의 기밀성 및 무결성을 보장한다.
② Null cipher suites는 encryption을 지원하지 않는다.
③ SSL2.0/SSL3.0은 취약한 버전이라 더 이상 사용하지 않는 것이 좋다.
④ 최신 버전의 HTTP/2를 사용하려면 TLS 1.0 이상이 활성화되어 있어야 한다.

58. 다음 지문에서 설명하는 테스트 방식은?

모의해킹 중 프로그램 내부 구조에 대한 타당성 여부를 시험하는 방식으로 프로그램 내부 구조를 분석하여 프로그램의 모든 처리 루틴을 테스트 하는 방식

① 시스템 하드닝 ② 코드 리뷰
③ 블랙박스 테스트 ④ 화이트박스 테스트

59. E-Mail 관련 프로토콜이 아닌 것은?
① S/MIME ② IRC
③ IMAP ④ SMTP

60. HTTP 상태 코드에 대한 해석 중 옳지 않은 것은?
① 400 - Bad Request ② 401 - Authorized
③ 403 - Forbidden ④ 404 - Not Found

4과목 : 정보 보안 일반

61. 메시지 인증 코드에 대한 설명으로 옳지 않은 것은?
① MAC 값은 메시지와 함께 송신자 및 수신자만이 공유하고 있는 키값을 함께 해시함수로 처리하여 계산한다.
② 송신자가 전송한 MAC 값을 검증에 성공하는 경우 수신자는 메시지의 무결성과 메시지의 출처를 확인할 수 있다.
③ MAC 값을 활용하면 메시지에 대한 해시값만을 이용하는 경우 발생할 수 있는 메시지 내용과 해시값이 동시에 변조되는 위협에 대응할 수 있다.
④ MAC 값을 활용하면 전자서명과 동일한 보안 서비스를 얻을 수 있다.

62. BLP에 대한 설명으로 옳지 않은 것은?
① BLP 모델이 개발된 주요 목적은 정보의 비밀성과 무결성 보호에 있다.
② 모든 주체의 객체에는 보안 레이블이 부여되며 보안 레이블에 의해 접근이 통제된다.
③ 주체가 객체에 정보를 기록(write)하려 할 때 *(star) 규칙이 적용되며 객체의 보안 레이블이 주체의 보안 레이블을 지배하는 경우 기록(write)이 허용된다.
④ 주체가 객체에 포함된 정보를 조회(read)할 때 simple security 규칙이 적용되며 주체의 보안 레이블이 객체의 보안 레이블을 지배하는 경우 조회(read)가 허용된다.

63. 다음 지문에서 설명하는 대칭키 암호 공격방식은?

일종의 선택된 평문공격법으로 두 개의 평문 블록들의 비트의 차이에 대하여 대응되는 암호문 블록들의 비트의 차이를 이용하여 사용된 비밀키를 찾아내는 방법이다.

① 선형 공격 ② 차분 공격
③ 통계적 분석 ④ 전수 공격

64. 다음 중 전자서명 알고리즘이 아닌 것은?
① DSA ② KCDSA
③ ECDSA ④ A5

65. 일회용 패스워드 생성방식은?

- 사용자가 OTP 인증 요청 시 인증서버로부터 받은 질의값을 직접 OTP 토큰에 입력하여 응답값(난수 형태)을 생성한다.
- OTP 토큰과 인증서버 간에 동기화해야 할 기준 정보가 없기 때문에, 동기화할 필요가 없다.
- 사용자와 서버 간에 상호 인증을 제공하는 방식으로 쉽게 확장이 가능하다.
- 인증서버도 해당 사용자의 질의값을 관리해야 하는 부담이 있다.

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

66. 타원곡선 암호를 적용하기에 적합한 공개키 암호 알고리즘

은?

① ElGamal ② Rabin
③ HIGHT ④ RSA

67. 사용자 인증방식 중 동일한 기술로 바르게 짝지어진 것은?

㉠ 홍채	㉡ 스마트 카드	㉢ OTP
㉣ 음성	㉤ 지문	㉥ USB 토큰

① [㉠, ㉢, ㉣] [㉡, ㉤, ㉥]
② [㉠, ㉡, ㉢] [㉣, ㉤, ㉥]
③ [㉠, ㉣, ㉤] [㉡, ㉢, ㉥]
④ [㉠, ㉣, ㉥] [㉡, ㉢, ㉤]

68. 강제적 접근통제의 특징과 가장 거리가 먼 것은?

① 보안관리자 주도하에 중앙 집중적 관리가 가능
② 접근규칙 수가 적어 통제가 용이
③ 이직률이 높은 기업에 적합
④ 사용자와 데이터에 보안 등급을 부여하여 적용

69. 인증서 관리와 관련한 설명으로 틀린 것은?

① 인증서 폐지 요청은 인증서 소유자에 의해서만 가능함
② 폐지된 인증서에 대한 목록을 공개하고 디렉터리에 보관
③ 인증서 폐지 목록은 주기적으로 또는 실시간으로 생성할 수 있음
④ OCSP로 인증서 유효성 검증을 할 수 있음

70. 블록 암호 종류에 해당되지 않는 것은?

① 3DES ② AES
③ SEED ④ RC4

71. 해시함수 h( )에 대한 설명 중 틀린 것은?

① 해시함수는 임의의 길이 메시지를 고정된 길이의 해시값으로 출력한다.
② 해시함수는 주어진 결과값으로부터 입력값을 찾는 것이 계산적으로 어렵다.
③ $h(x_1)=h(x_2)$가 임의의 $x_1 \neq x_2$를 찾는 것은 계산적으로 어렵다.
④ x_1과 $h(x_1)$ 그리고 h( ) 함수를 알고 있다면 $h(x_1)=h(x_2)$인 임의의 x_2를 찾는 것이 계산적으로 용이하다.

72. 국내에서 개발된 암호 알고리즘이 아닌 것은?

① AES ② ARIA
③ SEED ④ LEA

73. 공격자는 전송 중인 메시지와 MAC 값을 중간에 가로채 가지고 있다가 반복하여 재전송함으로써 잘못된 반복 처리가 가능하다. 이를 방지하기 위한 방법이 아닌 것은?

① 순서번호 ② 타임스탬프
③ CBC ④ 비표

74. 다음 지문에서 설명하고 있는 접근통제 모델은?

- 허가되지 않은 방식의 접근을 방지하는 모델이다.
- 정보흐름 모델 최초의 수학적 모델이다.
- 주체는 보다 높은 보안 수준의 데이터를 읽을 수 없다.

① 비바모델 ② 상태머신 모델
③ 클락-윌슨 모델 ④ 벨-라파듈라 모델

75. 인증서의 유효성 확인이 주 기능인 것은?

① PKI ② CA
③ RA ④ CRL

76. 다음 보기 중 FDS에 해당하는 통제는?

① 예방 통제 ② 탐지 통제
③ 교정 통제 ④ 복구 통제

77. 생체인증 요구사항의 특성에 해당되지 않는 것은?

① 유일성 ② 보편성
③ 지속성 ④ 시간의존성

78. 블록 암호 종류에 해당되지 않는 것은?

① 3DES ② AES
③ SEED ④ RC4

79. 인가된 사용자가 조직의 정보자산에 적시에 접근하여 업무를 수행할 수 있도록 유지하는 것을 목표로 하는 정보 보호 요소는?

① 기밀성(confidentiality) ② 무결성(integrity)
③ 가용성(availability) ④ 인증성(authentication)

80. 어떠한 사용자가 실제 사람인지 컴퓨터 프로그램인지 구별하기 위한 목적으로 사용되는 것은?

① 무결성 점검 도구 ② PKI
③ 전자서명 ④ CAPTCHA

5과목 : 정보보안 관리 및 법규

81. 다음 빈 칸에 들어가야 할 내용으로 올바르게 나열된 것은?

정보보호관리를 이행하기 위해서 조직은 (㉠) 및 조직수립, 범위설정 및 (㉡), (㉢), 구현, 사후관리활동으로 구성된 5단계의 논리적이고 체계적인 정보보호관리 (㉣)를 수립하고, 기획, 관리하여야 한다.

① ㉠ 프레임워크 ㉡ 정보자산 식별 ㉢ 위험관리 ㉣ 정보보호 정책
② ㉠ 정보보호 정책 ㉡ 취약점 ㉢ 정보자산 식별 ㉣ 프레임워크
③ ㉠ 프레임워크 ㉡ 취약점 ㉢ 정보자산 식별 ㉣ 정보보호 정책
④ ㉠ 정보보호 정책 ㉡ 정보자산 식별 ㉢ 위험관리 ㉣ 프레임워크

82. 조직의 정보자산을 보호하기 위하여 정보자산에 대한 위협

과 취약점을 분석하여 비용 대비 적절한 보호 대책을 마련함으로써 위험을 감수할 수 있는 수준으로 유지하는 일련의 과정은?

① 업무 연속성 계획 ② 위험관리
③ 정책과 절차 ④ 탐지 및 복구 통제

83. 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」에서 "해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태"로 정의된 용어는?

① 침해사고 ② 보안사고
③ 물리적 공격 ④ 사이버 공격

84. 위험 분석에 대한 설명으로 옳지 않은 것은?

① 자산의 식별된 위험을 처리하는 방안으로는 위험 수용, 위험 회피, 위험 전가 등이 있다.
② 자산의 가치 평가를 위해 자산구입비용, 자산유지보수비용 등을 고려할 수 있다.
③ 자산의 적절한 보호를 위해 소유자와 책임소재를 지정함으로써 자산의 책임추적성을 보장받을 수 있다.
④ 자산의 가치 평가 범위에 데이터베이스, 계약서, 시스템 유지보수 인력 등은 제외된다.

85. 다음 지문은 업무연속성계획(BCP)의 접근 5단계 방법론에 따라 업무의 순서대로 작성되었다. 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

86. 다음 제도는?

이것은 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 제도이다.

① CC ② ISMS
③ PIMS ④ ISMS-P

87. 정보보호 최고책임자에 대한 다음의 설명 중 적절하지 못한 것은?

① 정보통신서비스 제공자는 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다.
② 정보보호 최고책임자는 법에서 정한 업무 이외에도 기업의 형편에 따라 다른 업무를 겸직할 수 있다.
③ 정보통신서비스 제공자는 침해사고에 대한 공동 예방 및 대응과 필요한 정보의 교류 등의 사업을 수행하기 위하여 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있다.
④ 정보보호 최고책임자는 정보보호관리체계의 수립 및 관리·운영, 정보보호 취약점 분석·평가 및 개선, 침해사고의 예방 및 대응 등의 업무를 총괄한다.

88. 개인정보 안전성 확보를 위한 암호화에 대한 설명으로 적절하지 않은 것은?

① 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
② 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만 비밀번호를 저장하는 경우에는 양방향 암호화하여 저장하여야 한다.
③ 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
④ 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

89. A사의 개인정보처리자는 A사에서 수집한 개인정보를 사용 목적이 종료되어 파기하고자 한다. 이때 파기하기 위한 조치사항으로 부적절한 것은?

① 하드디스크의 개인정보를 파기하기 위해 하이레벨 포맷 수행
② 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
③ 전용 소자장비를 이용하여 개인정보 파기 수행
④ 기록물, 인쇄물, 서면, 그 밖의 기록매체의 일부만 파기할 경우 해당 부분을 마스킹, 천공 등으로 삭제

90. 침해사고 등이 발생한 경우 클라우드서비스 제공자의 의무로 적절하지 않은 것은?

① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.
② 클라우드컴퓨팅서비스 제공자는 사전예고 없이 대통령령으로 정하는 기간 이상 서비스 중단이 발생한 때에는 지체 없이 그 사실을 과학기술정보통신부장관에게 알려야 한다.
③ 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 지체 없이 그 사실을 해당 이용자에게 알려야 한다.
④ 클라우드컴퓨팅서비스 제공자는 「정보통신망법」에 따른 침해사고가 발생한 때에는 지체 없이 그 사실을 해당 이용자에게 알려야 한다.

91. 개인정보보호 원칙에 대한 설명으로 올바르지 않은 것은?

① 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리해야 한다.
② 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 해야 한다.
③ 정보주체의 사생활 침해를 최소화하기 위해 개인정보의 익명처리가 가능한 경우에도 개인정보를 식별하여 처리해야 한다.
④ 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개해야 한다.

92. 다음 중 「개인정보보호법」상 정보주체의 동의를 받아야 개인정보를 수집·이용할 수 있는 경우는?

① 경력직 직원의 채용을 위해 지원자의 종교, 질병, 범죄경력 등의 개인정보를 수집·이용한 경우
② 개인정보처리자가 도난 또는 화재 예방을 위하여 자재창고 앞에 CCTV를 설치한 경우

③ 소비자가 주문한 세탁기를 배달하기 위하여 소비자의 집 주소와 전화번호를 수집·이용한 경우

④ 교통사고로 인해 정보주체가 의식이 없는 상태에서 급박한 수술을 위해 보호자의 전화번호를 수집·이용한 경우

93. 개인정보 영향평가 시 고려 사항에 해당되지 않는 것은?

① 처리하는 개인정보의 수

② 개인정보 처리 방법

③ 개인정보 보유기간

④ 정보주체의 권리를 해할 가능성 및 그 위험 정도

94. 다음의 개인정보보호법 제17조 ①항에 따라 개인정보처리자가 정보주체의 개인정보를 수집한 목적범위 안에서 제3자에게 제공할 수 있는 경우로 <보기>에서 옳은 것만을 모두 고른 것은?

<보기1>
제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

<보기2>
ㄱ. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하에 필요한 경우
ㄴ. 공공기관의 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
ㄷ. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

① ㄱ ② ㄷ

③ ㄴ,ㄷ ④ ㄱ,ㄴ,ㄷ

95. 빈 칸 ㉠, ㉡에 들어갈 적합한 단어는?

정량적 위험분석 방법으로는 연간 예상 손실, 과거자료 분석법, 수학공식 접근법, 확률 분포법 등이 있다.
이 중 예상 손실은 단일 예상 손실과 연간 예상 손실을 계산할 수 있는데, 단일 예상 손실을 산출하기 위한 공식은 다음과 같다.
(㉠) * (㉡) 계수 = 단일 예상 손실

① 자산 가치, 소비 ② 소비 가치, 노출

③ 자산 가치, 노출 ④ 소비 가치, 생산

96. 「개인정보보호법」 제34조 및 관련 시행령에 따른 개인정보 유출 통지 및 신고에 대한 설명이다. 빈 칸 ㉠, ㉡에 들어갈 알맞은 용어는?

개인정보 유출 시 신고 방법
- 대상: (㉠) 이상의 정보주체에 관한 개인정보가 유출된 경우
- 기관: 행정안전부, 전문기관(㉡)
- 시기: 지체없이
- 방법: 전화, 전자우편, 팩스
- 내용: 통지내용, 유출피해 최소화 대책 및 조치 결과

① ㉠ 1천명 ㉡ 한국인터넷진흥원

② ㉠ 1만명 ㉡ 한국인터넷진흥원

③ ㉠ 5천명 ㉡ 한국정보화진흥원

④ ㉠ 1만명 ㉡ 한국정보화진흥원

97. 정보보호 내부 감사 시 고려해야할 사항으로 가장 부적합한 것은?

① 내부감사를 수행하는 구성원은 정보보호 전문가들로 제한한다.

② 감사의 범위는 다양한 위험을 분석 및 검토할 수 있도록 가능한 포괄적이어야 한다.

③ 내부감사는 조직의 위험을 파악하여 개선사항을 제시할 수 있다.

④ 감사활동은 기업 내외부로부터 독립성을 유지할 수 있도록 해야 한다.

98. 「개인정보 보호법」 제23조(민감정보의 처리 제한), 「개인정보 보호법 시행령」 제18조(민감정보의 범위)에서 규정하고 있는 민감정보에 대한 내용으로 가장 적절하지 않은 것은?

① 범죄경력자료 ② 성생활에 관한 정보

③ 여권번호 ④ 유전정보

99. 「개인정보보호법 제25조의1」에 따르면 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다. 각 호에 해당하지 않은 것은?

① 교통단속을 위하여 필요한 경우

② 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

③ 시설안전 및 화재 예방을 위하여 필요한 경우

④ 소관 업무의 수행을 위하여 불가피한 경우

100. 다음 사건 중 피의자 K씨가 한 행위와 가장 관련 있는 법률은?

피의자 K씨는 어느 사이트를 운영하며 이용자의 개인정보를 수집하였다. 이에 그치지 않고 경품 추첨을 진행한다는 거짓 이벤트를 통해 이용자의 민감한 정보까지 수집하였다. 하지만 K씨는 이를 동의 없이 개인정보 목적 외 이용 및 제3자에게 제공한 사실이 드러났고, 사이트를 통해 악성 프로그램을 유포하였다.

① 정보통신망 이용촉진 및 정보보호 등에 관한 법률

② 통신비밀보호법

③ 정보통신기반 보호법

④ 사행행위 등 규제 및 처벌 특례법

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