1과목 : 시스템 보안

1. 다음 윈도우 운영체제의 기능은?

> - 강제적 접근제어를 구현
> - 컴퓨터 설정을 변경하는 작업을 하거나 소프트웨어를 설치할 때 이 대화상자가 나타나 관리자 암호를 요구함

① Privileged Access Management
② Privileged Account Management
③ User Access Control
❹ User Account Control

2. 보기의 취약점 또는 사이버 공격 중 그 원인이 하드웨어에 기반하는 것은?

① Heartbleed ② Shellshock
❸ Spectre ④ WannaCry

3. 리눅스 설정 파일의 일부이다. 이 설정 파일로 알맞은 것은?

```
systat 11/tcp users
daytime 13/tcp
ftp-data 20/tcp
ftp 21/tcp
```

❶ /etc/services ② /etc/ports
③ /etc/protocols ④ /etc/resolv.conf

4. 좀비 프로세스의 존재를 확인하기 위한 명령어들로 올바르게 짝지어진 것은?

```
(가) top -b -n 1 I grep zombie
(나) ps -ef  I  grep defunct
(다) ps -ef  I  grep zombie
(라) top -b -n 1  I  grep defunct
```

① (가), (다) ② (나), (라)
❸ (가), (나) ④ (다), (라)

5. 홈페이지 회원 계정 및 패스워드 보안 강화를 위해 홈페이지 서버 관리자가 수행할 내용과 가장 거리가 먼 것은?

❶ 패스워드 무작위 대입 공격에 대응하기 위해 서버를 이중화 하였다.
② 초기 설정한 암호는 반드시 바꾸도록 설정하였다.
③ /etc/shadow 파일에서 사용기간 및 만료일을 설정하였다.
④ 5회 연속 암호 실패 시, 일정시간이 경과한 후 재 로그인 하도록 계정 Lock을 설정하였다.

6. Null Session 취약점을 갖는 것은?

① Admin$ ② C$
❸ IPC$ ④ D$

7. 리눅스/유닉스 시스템에서 최상위 디렉터리를 올바르게 짝지은 것은?

> (㉠) : 시스템의 환경 설정 및 주요 설정 파일을 담고 있다.
> (㉡) : 프로그램 실행 시 생성되는 임시 파일을 담고 있다.
> (㉢) : 프린터나 터미널 같은 물리적인 장치를 다루기 위한 특수 파일을 담고 있다.

① ㉠ /usr ㉡ /tmp ㉢ /var ② ㉠ /usr ㉡ /temp ㉢ /dev
③ ㉠ /etc ㉡ /temp ㉢ /var ❹ ㉠ /etc ㉡ /tmp ㉢ /dev

8. 'X'가 해킹을 위해 사용했을 것으로 의심되는 위치는?

> Black Hacker인 X는 리눅스 서버의 보안 취약점을 이용하여 root 권한을 획득하는데 우연히 성공했다. X는 이후 시스템이 시작될 때마다 자신이 만들어 놓은 해킹 툴을 자동으로 구동시키기 위하여 관련된 파일을 변조하였다.

① /etc/crontab ② /etc/resolv.conf
③ /etc/sysconfig/network ❹ /etc/rc.d/rc.local

9. ftp 접근 여부를 검토할 수 있는 로그는?

① wtmp ② utmp
③ sulog ❹ xferlog

10. 트로이목마의 기능과 가장 거리가 먼 것은?

① 패스워드 가로채기 ② 원격 조정
③ 시스템 파일 파괴 ❹ 악성코드 전파

11. 로그인 실패 시 로그가 저장되는 파일은?

① utmp ② pacct
③ wtmp ❹ btmp

12. 유닉스 또는 리눅스에서 실행 파일 a.out의 소유자가 root, 그룹은 staff이라고 할 때, chmod 4755 a.out 명령을 수행한 후의 a.out의 특성에 대해 올바르게 설명하고 있는 것은?

① 그룹이 staff인 모든 사용자에 한해 a.out을 읽고 실행시킬 수 있다.
② root만이 a.out을 읽고 실행시킬 수 있다.
❸ 실행하는 사용자에 관계없이 a.out은 root의 권한으로 실행된다.
④ 실행하는 사용자에 관계없이 a.out은 staff의 권한으로 실행된다

13. 리눅스 사용자 'test_user'에게 60일 마다 패스워드의 교체를 의무화시키기 위한 보안정책을 반영하기 위한 명령어에 해당하는 것은?

❶ passwd -x 60 test_user
② useradd -e 60 test_user
③ passwd +x 60 test_user
④ usermod -f 60 test_user

14. 아래 지문이 설명하는 평가인증 제도는 무엇인가?

보안기능 요구사항은 11개 클래스로 구성: FAU(보안감사), FCO(통신), FCS(암호지원), FDP(사용자 데이터 보호), FMT(보안관리), FIA(식별 및 인증), FPR(프라이버시), FPT(TOE 보안기능의 보호), FRU(자원활용), FTA(TOE 접근), FTP(안전한 경로/채널)
- 평가보증등급은 7등급(EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7)으로 구분되며 등급이 높아질수록 보증요구사항이 강화된다.

① TCSEC ② KTSEC
③ ITSEC ❹ CC

15. 윈도우 레지스트리 중 등록된 응용 프로그램과 확장자 사이의 관계 정보를 담고 있는 곳은?
❶ HKEY_CLASSES_ROOT
② HKEY_LOCAL_MACHINE＼SYSTEM
③ HKEY_CURRENT_CONFIG
④ HKEY_USERS

16. rlogin은 원격 시스템에 접속할 때 사용하는 서비스로 사전에 서버의 특정 파일에 호스트를 등록하여 클라이언트가 패스워드를 입력할 필요 없이 로그인이 가능하게 하는 서비스이다. 다음 중 호스트를 등록하는 파일은?
① /etc/hosts ❷ /etc/hosts.equiv
③ /etc/resolv.conf ④ /etc/syslog.conf

17. 다음 지문에서 설명하는 파일시스템으로 옳은 것은?

- 초창기 리눅스용으로 개발되었으며, 최대 2GB까지 파일시스템 크기를 지원한다.
- 256byte까지 파일명을 지원한다.
- 접근제어, inode 수정, 타임스탬프 수정 등의 기능이 불가능하다.
-사용할수록 단편화가 심해진다.

① FAT16 ② FAT32
③ NTFS ❹ EXT

18. 리눅스용 패킷 필터 기반 시스템 접근통제 도구와 거리가 먼 것은?
① iptables ② ipfwadm
③ ipchains ❹ modsecurity

19. 지문의 내용에 해당하는 것으로 가장 적절한 것은?

한정된 자원을 동시에 이용하려는 여러 프로세스가 자원의 이용을 위해 경쟁을 벌이는 현상을 의미하는 것으로, 취약 프로그램이 생성하는 임시 파일과 같은 이름의 파일을 생성한 후 생성한 임시 파일에 대한 심볼릭 링크를 설정한다.

① Format String ② Heap Spray
❸ Race Condition ④ Buffer Overflow

20. Users 그룹에 대한 설명 중 틀린 것은?

윈도우에서는 사용자 계정을 추가하면 일반 사용자 그룹인 Users 그룹에 자동으로 포함된다. NTFS로 포맷된 볼륨에서는 이 그룹의 구성원이 운영체제 및 설치된 프로그램의 무결성을 손상시킬 수 없도록 새로 설치된 시스템의 기본 보안 설정이 지정된다.

❶ Users 그룹의 구성원은 워크스테이션을 종료할 수 있고, 서버도 종료할 수 있다.
② Users 그룹의 구성원은 관리자가 설치하거나 배포한 인증된 프로그램을 실행할 수 있다.
③ Users 그룹의 구성원은 로컬 그룹을 만들 수는 있지만 자신이 만든 로컬 그룹만 관리할 수 있다.
④ Users 그룹의 구성원은 자신의 모든 데이터 파일(%userprofile%) 및 레지스트리에서 자신에 속하는 부분(HKEY_CURRENT_USER)을 완전하게 제어할 수 있다.

2과목 : 네트워크 보안

21. ㉠, ㉡, ㉢에 적합한 내용으로 짝지어진 것은?

- 이더넷은 네트워크 인터페이스 카드에 설정된 (㉠) 물리 주소를 사용한다.
- 인터넷 계층의 주소는 (㉡) 논리 주소를 사용한다.
- 전송 계층의 주소는 (㉢) 포트 주소를 사용한다.

① 8Byte, 2Byte, 1Byte ② 8Byte, 4Byte, 2Byte
❸ 6Byte, 4Byte, 2Byte ④ 6Byte, 2Byte, 1Byte

22. 분산서비스 거부공격(DDoS)의 구성요소가 아닌 것은?
① 마스터(Master) ❷ 포트 미러링(Port Mirroring)
③ 에이전트(Agent) ④ 공격자(Attacker)

23. SSL Handshake 프로토콜에 대한 설명으로 옳지 않은 것은?
① Cipher Suite은 공개키 암호 시스템, 대칭키 암호 시스템, 해시 알고리즘 등 3개의 정보로 구성된다.
② SSL Handshake 프로토콜 동작과정을 통해 SSL 클라이언트와 서버가 공유하는 암호 알고리즘들과 키 값들이 생성된다.
③ SSL 클라이언트는 통신 상대인 서버의 신원확인을 위해 전자인증서 기반의 인증을 수행한다.
❹ SSL 클라이언트와 서버의 전자인증서는 대칭키 암호 시스템을 이용한다.

24. VLAN에 대한 설명이다. 빈칸에 들어갈 내용을 순서대로 나열한 것은?

VLAN이란 (㉠) 트래픽을 제한하여 불필요한 트래픽을 차단하기 위한 (㉡) LAN이다. 스위치는 허브처럼 한 포트에서 발생한 데이터를 모든 포트에 전달하지 않기 때문에 스위치에 흐르는 데이터를 분석하려면 허브와는 달리 (㉢) 기능을 사용해야 한다.

① ㉠ 멀티캐스팅 ㉡ 논리적인 ㉢ Port Mirroring
❷ ㉠ 브로드캐스팅 ㉡ 논리적인 ㉢ Port Mirroring
③ ㉠ 브로드캐스팅 ㉡ 물리적인 ㉢ Port Filtering
④ ㉠ 멀티캐스팅 ㉡ 물리적인 ㉢ Port Filtering

25. TTL의 의미를 맞게 설명한 것은?

```
C:\>ping 127.0.0.1
Ping 127.0.0.1 32바이트 데이터 사용
127.0.0.1의 응답 바이트=32 시간 <1ms TTL=128
127.0.0.1의 응답 바이트=32 시간 <1ms TTL=128
127.0.0.1에 대한 Ping 통계
패킷 보냄 = 4, 받음 =4, 손실 = 0 (0% 손실),
왕복 시간(밀리초)
최소 = 0ms, 최대 = 0ms, 평균 = 0ms
```

① Echo Reply 패킷 크기
② Reply 패킷을 받기까지의 시간
❸ 라우팅 정보가 잘못되어 발생하는 패킷 무한 반복을 제어하기 위한 값
④ 손실된 패킷의 수

26. TCP 플래그 값을 모두 off(비활성화)한 패킷들을 이용하여 스캔하는 기법은?

① FIN 스캔 ② TCP SYN 스캔
❸ Null 스캔 ④ XMAS 스캔

27. 공격 특징 및 대응방안과 관련성이 가장 높은 것은?

웹서버 OS의 TCP 스택(Stack) 자원을 소모하는 특징을 갖는 웹서버 자원 소모 공격으로 사용될 수 있으며, 그 대응방법으로 Anti-DDoS 장비에서 소스 IP별로 PPS 임계치를 설정하거나 패킷 헤더 검사를 통해 정상적인 옵션 필드값을 갖지 않는 비정상 패킷을 차단할 수 있다.

① UDP Flooding ❷ SYN Flooding
③ GET Flooding ④ ICMP Flooding

28. 수동적 공격과 가장 거리가 먼 것은?

① 도청 ❷ 메세지 수정
③ 감시 ④ 메시지 내용 절취

29. 3계층 터널링 프로토콜은?

① PPTP VPN ② L2TP VPN
❸ IPSec VPN ④ SSL VPN

30. iptables 설정 내용을 /etc/iptables.tmp 파일에 저장하는 명령어로 적절한 것은?

① iptables -store > /etc/iptables.tmp
② iptables -config > /etc/iptables.tmp
③ iptables -restore > /etc/iptables.tmp
❹ iptables -save > /etc/iptables.tmp

31. 포트의 open 여부를 확인하는 방법이 다른 하나는?

① Null 스캔 ② FIN 스캔
❸ SYN 스캔 ④ XMAS 스캔

32. 공격자는 공격대상 시스템을 10.10.10.5로 에이전트가 있는 네트워크를 192.168.3.0/24로 설정하고 패킷 생성도구를 이용하여 패킷을 보냈다. 다음 보기 중 이러한 공격 행위와 가장 관련이 있는 것은?

```
hping 192.168.0.255 -a 10.10.10.5 --icmp --flood
```

① SYN Flooding ② Ping of Death
③ LAND ❹ Smurf

33. 어떤 공격을 방어하기 위한 것인가?

- 콘텐츠 요청 횟수에 대한 임계치 설정에 의한 차단
- 시간별 웹페이지 URL 접속 임계치 설정에 의한 차단
- Web-Scraping 기법을 이용한 차단

❶ Get Flooding 공격 방어 ② ICMP Flooding 공격 방어
③ SYN Flooding 공격 방어 ④ TCP Session 공격 방어

34. 공격 대상이 방문할 가능성이 있는 합법적인 웹 사이트를 미리 감염시킨 뒤, 잠복하고 있다가 피해자가 방문하면 피해자의 컴퓨터에 악성코드를 설치하는 공격 방법은?

① Malicious Bot 공격 ❷ Watering Hole 공격
③ Spear Phishing 공격 ④ Pharming 공격

35. 스위칭 환경에서 스니핑을 수행하기 위한 공격이 아닌 것은?

① ICMP 리다이렉트 ② ARP 스푸핑
③ 스위치 재밍 ❹ IP 스푸핑

36. 다음 설명에 해당하는 시스템은?

- 네트워크에 접근하는 접속 단말의 보안성을 검증하여 보안성을 강제화하고 접속을 통제할 수 있는 보안 인프라이다.
- 사용 단말이 내부 네트워크에 접속하기 전에 보안정책을 준수했는지 여부를 검사해 네트워크 접속을 통제하는 보안 솔루션이다.
- 주요 기능으로는 접근제어/인증, PC 및 네트워크 장비 통제, 해킹, 웜, 유해 트래픽 탐지 및 차단 등이 있다.

❶ NAC ② ESM
③ SIEM ④ IDS

37. 다음 중 내부망에서 외부망을 향하는 패킷들을 모니터링하고 통제하여 비인가 트래픽이나 악성 트래픽이 내부망을 벗어나지 않도록 만드는 방식의 필터링으로 알맞은 것은?

① Contents Filtering ② Blacklist Filtering
❸ Egress Filtering ④ Inference Filtering

38. IP Fragmentation을 이용하여 공격을 수행하는 공격 기법은?

❶ Teardrop ② SYN Flooding
③ ICMP Flooding ④ LAND Attack

39. IPSec 프로토콜의 설명 중 옳지 않은 것은?

❶ IPSec은 전송데이터 보호 구간에 따라 트랜스포트 모드와 터널 모드로 나뉘며, End-to-End 전송 데이터 보호를 위해서는 터널 모드를 사용해야 한다.
② ESP를 설정하면 데이터 기밀성을 제공하여 데이터가 노출되는 것을 차단할 수 있다.
③ AH를 설정할 시 데이터가 수정되지 않았음을 보장할 수 있다.
④ 트랜스포트 모드 AH헤더는 IP헤더와 IP페이로드 사이에 삽입된다.

40. TTL 필드가 0이 되었으나 아직 목적지에 도달하지 못한 경우 발생하는 ICMP 메시지로 알맞은 것은?

① 목적지 도달 불가능(destination-unreachable)
❷ 시간 경과(time-exceeded)
③ 매개변수 문제(parameter-problem)
④ 발신지 억제(source-quench)

3과목 : 어플리케이션 보안

41. 다음 지문에서 설명하고 있는 DB 보안 요구사항으로 적절한 것은?

- 데이터베이스 내에 있는 자료값들이 정확하도록 보장하는 관리 작업
- 잘못된 갱신으로부터의 보호나 불법적인 조작에 대한 보호를 통한 정확성 유지

① 감사 기능 ② 추론 방지
❸ 데이터 무결성 ④ 접근 통제

42. 디지털포렌식 과정 중 수집된 디지털 증거를 이송, 분석, 보관, 법정 제출 등 각 단계에서 담당자 및 책임자를 명확히 함으로써 증거물의 진정성을 판단하는 중요한 기준을 지칭하는 원칙은?

❶ 관리 연속성 ② 독수독과성
③ 전문 배제성 ④ 증거 무결성

43. 전자상거래 환경에서 구매자의 신용카드 정보 등 중요 지불정보를 이용하여 판매자 대신 신용카드사 등 금융기관에 결제를 요청하고 처리하는 기관의 명칭은?

① CA(Certification Authority)
❷ PG(Payment Gateway)
③ TGS(Ticket Granting Service)
④ KDC(Key Distribution Center)

44. 웹에서 보안 문제 발생 시 아파치 로그를 분석하여 문제를 해결하는 방법으로 가장 부적절한 것은?

① 클라이언트의 IP 주소, 클라이언트의 접속시간 정보에 대한 로그 내용을 분석한다.
② 클라이언트의 요청방식(GET, POST) 및 요청 내용(URL)에 대한 로그 내용을 분석한다.
③ 특정 파일에 대한 연속적인 요청이 있을 시 로그 패턴을 분석한다.
❹ 웹서버에서 특정 웹페이지(파일)의 요청이 많은 경우에 대한 로그 패턴을 분석한다.

45. FTP bounce 공격과 거리가 먼 것은?

① 익명 FTP 서버를 이용해 그 FTP 서버를 경유해서 호스트를 스캔
② FTP 서버를 통해 임의의 네트워크 접속을 릴레이함으로써 수행
③ 네트워크에 대한 포트 스캐닝에 이용
❹ 익명 사용자가 서버에 쓰기 권한이 있을 때 악성코드 생성

46. 다음 중 DB 보안 강화를 위한 지침으로 가장 부적절한 것은?

① 노출 및 기능 최소화 ② 관리자 최소화
❸ 로컬 계정 사용 금지 ④ Guest 계정 사용 금지

47. KISA에서 발표한 생체인식기반 간편 공인인증 가이드라인의 보안 요구사항으로 부적합한 사항들은?

ⓐ 루팅 및 탈옥 등 스마트폰이 불법 변경되면 모든 저장소에 접근이 가능하여 안전한 하드웨어 저장소를 활용할 것을 권고한다.
ⓑ 생체정보 등의 로컬인증 실패 횟수는 제한하지 않되 비밀번호 등은 실패 횟수를 제한하여야 한다.
ⓒ 장치의 오인식률(FAR)은 5%미만이어야 한다.
ⓓ 스마트폰 내 지문인식 장치의 취약점이 발견되는 즉시 보안조치가 이루어져야 한다.

① ⓐ, ⓓ ② ⓐ, ⓒ
❸ ⓑ, ⓒ ④ ⓑ, ⓓ

48. DRM에 대한 설명 중 적절하지 못한 것은?

① 커널에 삽입된 DRM 모듈은 응용 프로그램이 작성한 문서를 암호화하여 하드디스크에 저장한다.
② 문서보안 기술의 하나로서 문서의 열람, 편집, 인쇄에 접근권한을 설정하여 통제한다.
③ 관리자는 각 개인의 DRM 인증서에 권한을 설정하여 각 개인의 문서에 대한 접근권한을 관리할 수 있다.
❹ DRM은 과거 IP 관리 시스템이 발전한 형태의 솔루션으로서, MAC 주소를 기반으로 접근제어 및 인증을 수행한다.

49. 서버 측 스크립트 언어가 아닌 것은?

① JSP ② ASP
❸ HTML ④ PHP

50. OWASP TOP 10 - 2017과 거리가 먼 것은?

❶ DDoS : UDP 등 사용하지 않는 프로토콜 차단 및 모니터링 체계 구성이 필요함

② 민감한 데이터 노출 : 중요한 데이터를 저장 및 전송할 때 암호화 같은 추가적인 보호 조치가 요구됨

③ 취약한 인증 : 인증 및 세션 관리와 관련된 애플리케이션 기능이 잘못 구현되어 있는 상황에서 발생

④ 불충분한 로깅 &모니터링 : 로깅과 모니터링을 적절히 수행하지 않을 경우 사고에 대한 적절한 대응이 불가

51. 휘발성의 순위가 가장 높은 것은?

❶ Register, Cache

② Routing Table, ARP Cache

③ Temporary File System

④ Disk

52. FTP 서비스에 대한 공격과 거리가 먼 것은?

① Sniffing 공격

② 비밀번호에 대한 Brute Force 공격

③ 비밀번호에 대한 Brute Force 공격

❹ CSRF 공격

53. SSL 프로토콜에 대한 설명 중 잘못된 것은?

① SSL 프로토콜에 지정된 포트는 443임

❷ 세션 계층에서 적용되며, FTP, TFTP, SYSLOG 등과 같은 응용 계층 프로토콜의 안전성 보장을 위해 사용될 수 있음

③ 웹 서버와 브라우저 간의 안전한 통신을 위해 넷스케이프에 의해 개발됨

④ SSL을 사용하기 위해서는 우리가 흔히 사용하는 URL 표기 방식인 “http://*” 대신에 “https://*”를 사용해야 함

54. 제3자가 소비자의 상품 대금을 보관하고 있다가 상품배송이 완료된 후 통신판매업자에게 지급하는 서비스로 알맞은 것은?

① 선불전자지급 수단발행 서비스

② 전자지급결제대행(PG) 서비스

❸ 결제대금예치(Escrow) 서비스

④ 전자고지결제(EBPP) 서비스

55. 다음 지문에서 설명하는 웹 서버 애플리케이션의 취약점은?

> 게시판의 글에 원본과 함께 악성코드를 삽입하여 글을 읽을 경우 악성코드가 실행되도록 한다. 이는 클라이언트의 정보를 유출하는 공격기법으로, 웹 페이지가 사용자에게 입력 받은 데이터를 필터링하지 않고 그대로 동적으로 생성된 웹 페이지에 포함하여 사용자에게 재전송할 때 발생한다.

① SQL Injection

② Buffer Overflow

③ Security Misconfiguration

❹ Cross-Site Scripting(XSS)

56. 경계 검사의 미비로 버퍼 오버플로우를 발생시킬 우려가 있어 사용하지 않도록 권고되는 C 라이브러리 함수에 포함되지 않는 것은?

① strcpy( ) ❷ fgets( )

③ sscanf( ) ④ gethostbyname( )

57. 다수의 부분 문자열을 입력하여 공격 문자열을 완성하는 공격기법으로 질의 결과로 참과 거짓만을 확인하며 수행하는 공격 기법은?

① SQL Injection ❷ Blind SQL Injection

③ Union SQL Injection ④ Mass SQL Injection

58. 웹 취약점을 보완하기 위한 내용 중 설명이 틀린 것은?

① 서버 통제 적용 ② 특수문자 필터링

❸ 쿠키(cookie)의 사용 ④ 지속적인 세션 관리

59. CSRF 공격에 대한 설명이 틀린 것은?

① 자신의 의도와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록, 송금 등)를 하게 만드는 공격이다.

② 특정 사용자를 대상으로 하지 않고 불특정 다수를 대상으로 한다.

③ 기본적으로 XSS 공격과 매우 유사하며 XSS 공격의 발전된 형태로 보기도 한다.

❹ XSS 공격은 사용자가 악성스크립트를 서버에 요청하는데 반해 CSRF는 악성스크립트가 클라이언트에서 실행된다.

60. 다음 취약점 및 버그 방지 개발 방법 중 새로운 프로세스를 생성하여 사용할 경우의 보안 대책과 거리가 먼 것은?

① 모든 파일 기술자들을 닫았는지 확인한다.

❷ strncat( ) 함수나 vfscanf( ) 함수의 사용을 제한한다.

③ 자식 프로세스에 전달된 환경변수를 확인한다.

④ 프로그램을 실행할 때 전체 경로 이름을 사용하는지 확인한다.

4과목 : 정보 보안 일반

61. 블록암호 모드로 알맞은 것은?

> 초기치를 암호화한 값과 평문 블록을 XOR하여 암호문 블록을 생성하고 그 암호문을 입력으로 사용하여 다시 암호화한 값과 평문 블록을 XOR하여 암호문 블록을 생성하는 과정을 반복하는 방식이다. 암호화에서는 특정 입력이 이후에 계속 영향을 미치지만, 복호화에서는 특정 암호문의 오류가 계속적으로 이후에 영향을 미치지는 않는다는 특징이 있다.

① Electronic CodeBook Mode

❷ Cipher FeedBack Mode

③ Output FeedBack Mode

④ Counter Mode

62. 해시함수 h에 대해 h(x)=h(x')을 만족하는 2개의 서로 다른 입력 x, x'를 찾는 것이 계산적으로 불가능한 것을 의미하는 것은?

① 일방향성 ② 무결성

③ 두 번째 역상 저항성 ❹ 충돌저항성

63. Active Attack과 Passive Attack이 올바르게 짝지어진 것은?
① 재생 공격, 메시지 변조 공격
② 트래픽분석 공격, 전송파일 도청
❸ 메시지 변조, 전송파일 도청
④ 삽입 공격, 삭제 공격

64. 단일 치환 암호를 해독할 수 있는 방법으로 알맞은 것은?
❶ 빈도 분석법 ② 치환 분석법
③ 알파벳 분석법 ④ 순서 분석법

65. 전자서명 생성과 검증 과정에 사용되는 키가 올바르게 짝지어진 것은?
① 생성 - 수신자의 공개키 검증 - 송신자의 개인키
② 생성 - 송신자의 공개키 검증 - 송신자의 개인키
❸ 생성 - 송신자의 개인키 검증 - 송신자의 공개키
④ 생성 - 수신자의 공개키 검증 - 수신자의 개인키

66. 다음 전자서명 기술은?

> 전자상거래 SET 프로토콜에서 도입된 기술로 고객의 구매 요청은 지불정보와 더불어 일단 상인에게 전달되면 상인은 그 구매 요청에 포함된 지불정보를 이용하여 지불 게이트웨이에게 유효성을 확인하게 된다. 또한 구매자의 자세한 주문정보와 지불정보를 판매자와 금융기관에 필요 이상으로 전달하지 않아야 한다.

❶ 이중서명 ② 은닉서명
③ 공개서명 ④ 다중서명

67. 다음 중 메시지 인증 코드(MAC)의 특징으로 옳지 않은 것은?
① 메시지에 붙여지는 작은 데이터 블록을 생성하기 위해 비밀키를 이용
② 메시지와 비밀키를 입력하여 인증값으로 사용될 고정길이 값을 생성
③ 수신자는 수신된 메시지에 동일키를 이용하여 새 메시지 인증코드를 생성하기 위해 동일한 계산을 수행
❹ 송신자는 메시지를 공개키로 암호화하여 보냄으로써 메시지 송신에 대한 부인을 방지

68. 강제적 접근통제의 특징이 아닌 것은?
① 보안관리자 주도 하에 중앙집중적 관리가 가능
② 접근 규칙 수가 적어 통제가 용이
❸ 이직률이 높은 기업에 적합
④ 사용자와 데이터는 보안등급을 부여 받아 적용

69. 다음 지문에서 설명하는 대칭키 알고리즘 공격방법은?

> - 암호화 키를 알아내거나, 다른 암호문들에 대응되는 평문을 추정하는 방법
> - 암호 해독자는 일정량의 알려진 평문에 대응하는 암호문을 알고 있음

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

70. 해시함수 MD5와 SHA-1의 출력 값의 비트수를 올바르게 나열한 것은?
❶ MD5 : 128 SHA-1 : 160
② MD5 : 128 SHA-1 : 256
③ MD5 : 160 SHA-1 : 160
④ MD5 : 160 SHA-1 : 256

71. 접근통제 보안 모델은?

> 이 모델은 허가되지 않은 방식의 접근을 방지하는 모델로서, 정보 흐름 모델 최초의 수학적 모델이다. MAC(Mandatory Access Control) 방식으로 접근을 통제하며, 시스템 내부에 있는 정보의 기밀성을 보호한다. 이 모델에서 주체는 자신의 인가권 수준보다 높은 수준의 데이터를 읽을 수 없으며, 주체는 데이터를 자신의 인가권 수준보다 낮은 수준의 객체에 기록할 수 없다.

① State Machine Model ❷ Bell-LaPadula Model
③ Biba Model ④ Lattice Model

72. 은닉서명에 대한 설명으로 옳은 것은?
❶ 은닉서명은 전자화폐 이용 시 사용자의 신원 노출 문제점을 해결하는 전자서명 기술이다.
② 은닉서명은 전자서명 발급 이후에 메시지에 대한 서명의 유효성을 확인할 수 없으나, 서명 생성자는 수신자의 신원을 알 수 있다.
③ 은닉서명은 사용자 A가 서명자 B에게 자신의 메시지를 보여 주고 서명을 얻는 방법이다.
④ 은닉서명 검증자는 메시지에 대한 서명의 유효성을 확인할 수 없으나 송신자의 신원을 알 수 있다.

73. Hybrid 암호화 시스템에 관련된 설명으로 틀린 것은?
① 대칭 암호시스템은 1회용 세션키로 데이터를 암호화하는 용도로 사용한다.
② 공개키 암호시스템은 대칭 암호알고리즘에서 사용할 1회용 세션키를 분배하는 용도로 사용한다.
③ 공개키 암호시스템은 암·복호 속도가 느려 대용량 데이터 암호화에 부적합하기 때문에 속도가 빠른 대칭암호시스템을 혼용하는 것이다.
❹ 키 분배를 대칭암호시스템으로 암호화하여 분배하고, 암호화할 데이터를 공개키로 암호화한다.

74. X.509 공개키 인증서에 포함되는 내용이 아닌 것은?
① 인증서 소유자 ② 인증서 발행기관
③ 인증서 서명 알고리즘명 ❹ 인증서 소유자의 개인키

75. 블록암호의 운용 모드로 알맞은 것은?

> - 평문이 블록암호 알고리즘의 입력으로 전혀 사용되지 않음
> - 평문이나 암호문의 오류가 후속 블록에 영향을 미치지 않음
> - 블록 암호를 기반으로 한 스트림 암호

① ECB 모드 ② CBC 모드
③ CFB 모드 ❹ OFB 모드

76. 아래 함수의 용도로 가장 적절한 것은?

> H(key XOR 3636,..36, H(key XOR 5C5C,..5C, data))
> (H는 임의의 암호학적 해시 함수, key는 비밀키, 3636,..36과 5C5C,..5C 등은 key와 같은 길이의 16진수)

❶ 메시지 인증 ② 메시지 기밀성
③ 송신자 부인 방지 ④ 서비스 거부 공격 방지

77. 공개키 기반구조의 구성요소에 해당하지 않는 것은?

① 인증기관(CA)
② 등록기관(RA)
③ 공개키 인증서의 소유자
❹ 비밀키 인증서와 CRL을 저장하는 저장소

78. 대칭키 배송 문제를 해결할 수 있는 방법에 해당하지 않는 것은?

① Diffie-Hellman 키 교환 방법에 의한 해결
② 키 분배 센터에 의한 해결
❸ 전자서명에 의한 해결
④ 공개키 암호에 의한 해결

79. 메시지 인증 코드에서 재전송 공격을 방지하기 위한 방법과 가장 거리가 먼 것은?

❶ 메시지 내부에 일방향 해시값(One-Way Hash)을 추가하여 메시지 인증코드를 생성한다.
② 메시지 내부에 매회 1씩 증가하는 순서번호(Sequence Number)를 추가하여 메시지 인증코드를 생성한다.
③ 메시지 내부에 난수 형태의 일회용 Nonce 값을 추가하여 메시지 인증코드를 생성한다.
④ 메시지 내부에 현재 시각 정보(Timestamp)를 추가하여 메시지 인증코드를 생성한다.

80. SSL, IPSec 등 대부분의 네트워크 보안 프로토콜에서 RSA 공개키 암호를 이용하여 송신자(A)와 수신자(B) 간에 비밀 세션키를 공유하는 키분배 방식을 지원하고 있다. 이때, 송신자(A)가 수신자(B)에게 전달하는 세션키를 암호화할 때 필요로 하는 키 정보에 해당하는 것은?

① 송신자(A)의 개인키 ② 송신자(A)의 공개키
③ 수신자(B)의 개인키 ❹ 수신자(B)의 공개키

5과목 : 정보보안 관리 및 법규

81. OECD 개인정보보호 8개 원칙 중 다음에서 설명하는 것은?

> 개인정보 침해, 누설, 도용을 방지하기 위한 물리적·조직적·기술적인 안전조치를 확보해야 한다.

① 수집 제한의 원칙(Collection Limitation Principle)
② 이용 제한의 원칙(Use Limitation Principle)
③ 정보 정확성의 원칙(Data Quality Principle)
❹ 안전성 확보의 원칙(Security Safeguards Principle)

82. 정보통신기반보호위원회의 기능에 대한 설명 중 잘못된 것은?

① 주요정보통신기반시설의 지정 및 지정 취소
② 주요정보통신기반시설 보호정책의 조정
③ 주요정보통신기반시설에 관한 보호계획의 종합·조정
❹ 주요정보통신기반시설 보호대책의 수립

83. 공인인증서의 폐지사유가 아닌 것은?

① 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우
❷ 공인인증서의 유효기간이 경과한 경우
③ 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 사실을 인지한 경우
④ 가입자가 사위 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우

84. 전자서명법에서 정의된 용어에 대한 설명으로 적절하지 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.
❸ "전자서명 검증"이라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말한다.
④ "공인인증업무"라 함은 공인인증서 발급, 인증관련 기록의 관리 등 공인인증역무를 제공하는 업무를 말한다.

85. 정보보호 관리체계에 대한 설명 중 적절하지 못한 것은?

① 정보보호 관리체계는 경영과 IT영역의 중요한 위험 관리 활동의 하나이다.
② 정보보호 관리체계는 정보보호에 관한 경영관리 시스템이다.
❸ 정보보호 관리체계는 기업에 있는 정보자산 보호를 목적으로 주로 기술적인 면을 고려하며, 일반적으로 정보보호 운용 또는 인적관리는 관리대상에서 배제한다.
④ 정보보호 관리체계는 통상적으로 PDCA 사이클을 기반으로 실행된다.

86. 위험의 구성요소가 아닌 것은?

① 자산 ② 위협
③ 취약점 ❹ 정책

87. 정보보호 위험의 정량적 평가방법이 아닌 것은?

① 수학공식 접근법 ② 과거자료 분석법
③ 확률분포법 ❹ 델파이법

88. ISMS-P 인증제도에 관련된 설명으로 틀린 것은?

① ISMS-P에서는 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항의 102개 인증기준이 존재한다.
② 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도이다.

❸ ISMS-P 인증기관 및 심사기관의 유효기간은 5년이며 유효기간이 끝나기 전 6개월부터 끝나는 날까지 재지정을 신청할 수 있다.

④ 정보통신기반 보호법에 따른 주요통신기반시설의 취약점 분석·평가에 따른 정보보호 조치를 취한 경우 인증심사 일부를 생략할 수 있다.

89. 국내 정보보호 및 개인정보보호 관리체계(ISMS-P)의 관리체계 수립 및 운영 4단계 중 위험 관리 단계의 통제항목에 해당하지 않는 것은?

① 정보자산 식별 ② 현황 및 흐름 분석

❸ 보호대책 구현 ④ 위험 평가

90. 정보주체의 권리에 해당하지 않는 것은?

① 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람을 요구할 권리

② 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리

③ 개인정보의 처리에 관한 정보를 제공받을 권리

❹ 개인정보의 처리로 인하여 발생한 금전적 이익에 대해 배상받을 권리

91. 자동화된 위험분석 도구의 특징이 아닌 것은?

① 위험분석의 일반적인 요구사항과 절차를 자동화한 도구이다.

❷ 위험분석에 소요되는 시간과 비용을 절감할 수 있다.

③ 분석 과정에서 정확한 자료의 입력이 매우 중요하다.

④ 수작업 시의 실수로 인한 오차를 줄일 수 있기 때문에 수작업에 비해 결과에 대한 신뢰도가 높다.

92. 정보통신기반 보호법상 '전자적 침해행위'로 규정한 공격행위에 속하지 않는 것은?

① 고출력 전자기파 ❷ 영업목적의 스팸메일

③ 메일폭탄 ④ 컴퓨터바이러스

93. 다음의 보기는 침해사고 등이 발생한 경우 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」에 따른 클라우드서비스 제공자의 의무를 설명한 것이다. 잘못 설명되어 있는 것은?

① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.

❷ 클라우드컴퓨팅서비스 제공자는 사전예고 없이 대통령령으로 정하는 기간 이상 서비스 중단이 발생한 때에는 지체 없이 그 사실을 해당 과학기술정보통신부장관에게 알려야 한다.

③ 클라우드컴퓨팅서비스 제공자는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 침해사고가 발생한 때에는 지체 없이 그 사실을 해당 이용자에게 알려야 한다.

④ 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 지체 없이 그 사실을 해당 이용자에게 알려야 한다.

94. 영향평가를 하는 경우에 고려해야 할 사항 중에서 가장 적합하지 않은 것은?

① 개인정보의 제3자의 제공 여부

② 처리하는 개인정보의 수

③ 정보주체의 권리를 해할 가능성 및 그 위험 정도

❹ 개인정보를 처리하는 수탁업체 관리·감독의 여부

95. 주요정보통신기반시설 관리기관이 취약점 분석·평가를 의뢰할 수 없는 기관은?

❶ 「국가정보화기본법」 제14조의 규정에 의한 한국정보화진흥원

② 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업

③ 「정보통신기반보호법」 제16조의 규정에 의한 정보공유·분석센터

④ 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원

96. 주 센터와 동일한 수준의 정보처리시스템을 원격지에 구축하여 Standby 상태로 유지하고, 주 센터 장애 발생 시 원격지의 시스템을 운영상태로 전환하는 유형은?

① 미러 사이트 ❷ 핫 사이트

③ 웜 사이트 ④ 콜드 사이트

97. '개인정보 보호법'에서 개인정보 수집 시 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집에 대한 입증을 부담하는 담당자는?

① 개인정보 담당자 ② 개인정보 책임자

❸ 개인정보 처리자 ④ 정보주체

98. 위험처리 방식은?

> 어떤 조직이 인터넷을 이용하여 고액의 전자거래 시스템을 운영하고자 위험 분석을 수행하였다. 위험 분석의 결과는 고액의 온라인 전송에 따른 거래 금액 노출, 변조, 거래 사실 부인의 위험이 매우 높았다. 해당 조직은 이 위험을 처리하기 위해 전자서명, 암호화, 송신자 부인방지를 위한 공증 시스템과 같은 대책을 도입하였다.

① 위험 수용 ❷ 위험 감소

③ 위험 회피 ④ 위험 전가

99. 다음은 정보보호 조직의 구성원과 그 책임에 대한 설명이 옳지 않은 것은?

① 정보보호 관리자 - 조직의 정보보호 정책 표준, 대책, 실무 절차를 설계, 구현, 관리, 조사할 책임

② 최고 경영자 - 정보보호를 위한 총괄 책임

③ 데이터 관리자 - 정보시스템에 저장된 데이터의 정확성과 무결성을 유지하고 데이터 중요성 및 분류를 결정할 책임

❹ 정보보호 위원회 - 보안 목적이 적절하고 정보보호 정책, 표준, 대책, 실무 및 절차가 조직의 보안 목적에 따라 적절하게 이루어지고 있음을 독립적인 입장에서 관리자에게 보증할 책임

100. 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
❷ 업무 연속성 계획
③ 재난 대비 가용성 확보 대책
④ 피해 복구 대책

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