1과목 : 시스템 보안

1. 다음 중 운영체제와 무관하게 매크로 기능이 있는 MS 오피스 제품과 같은 프로그램을 통해 활동하는 컴퓨터 바이러스에 해당하는 것은?
   ① 매크로(Macro) 바이러스
   ② 다형성(Polymorphic) 바이러스
   ③ 은폐형(Stealth) 바이러스
   ④ 암호형(Encryption) 바이러스

2. chmod 명령어 실행 후의 파일 test1의 허기비트(8진법 표현)는?

```
% IS - l test1
- rw-r—r— 1 root user 2320 Feb 9 13:20 test 1
% chmod o-r test1
% chmod g-r test1
```

   ① 644 ② 244
   ③ 600 ④ 640

3. 다음 설명 중 가장 옳지 않은 것은?
   ① 리눅스 시스템에서는 계정 목록을 /etc/passwd 파일에 저장하고 있다.
   ② 일반 사용자의 사용자 번호(UID, User ID)는 0번으로 부여받게 된다.
   ③ 디렉토리의 권한은 특수권한, 파일 소유자 권한, 그룹 권한, 일반(Others) 권한으로 구분된다.
   ④ 접근 권한이 rwxr-xr-x인 경우 고유한 숫자로 표기하면 755가 된다.

4. 다음 지문이 설명하는 데이터베이스 보안유형은 무엇인가?

> 전체 데이터베이스 중 자신이 허가 받은 사용자 관점만 볼 수 있도록 한정하는 것

   ① Access Control ② Encryption
   ③ Views ④ Authorization Rules

5. 다음 중 동작 계층이 다른 하나는?
   ① S/MIME ② PGP
   ③ S-HTTP ④ SSL

6. ㉠, ㉡에 해당하는 보안도구로 적절한 것은?

> ㉠ SATAN, SAINT, COPS, Nessus, Nmap 등의 보안도구들을 통칭하는 용어
> ㉡ 유닉스에서 실시간 트래픽 분석과 IP 네트워크 상에서 패킷로깅이 가능한 대표적인 네트워크 침입탐지 시스템

   ① ㉠ 취약점 점검도구, ㉡ Snort
   ② ㉠ 도청 도구, ㉡ SNMP
   ③ ㉠ 침입 탐지 도구, ㉡ SNMP
   ④ ㉠ 무결성 검증 도구, ㉡ Snort

7. 디스크 공간 할당의 논리적 단위는?
   ① Volume ② Page
   ③ Cluster ④ Stream

8. 비선점형 스케줄링만 고르 것은?

> ㉠ FCFS ㉡ SJF ㉢ RR
> ㉣ SRT ㉤ MLQ

   ① ㉠, ㉡ ② ㉠, ㉢
   ③ ㉠, ㉣ ④ ㉢, ㉤

9. 도메인을 탈취하거나 도메인 네임 시스템 또는 프록시 서버의 주소를 변조함으로써 사용자들로 하여금 진짜 사이트로 오인해 접속하도록 유도한 뒤, 개인 정보를 탈취하는 해킹 기법은?
   ① 피싱 ② 파밍
   ③ 스미싱 ④ 봇넷

10. 특정 조건이 만족될 때까지 잠복하고 있다가 조건이 만족되면 트리거 되어 해커가 원하는 동작을 실행하는 공격방법은?
   ① 트로이 목마 ② 키로거
   ③ 논리 폭탄 ④ 백도어 (Backdoor)

11. 최근 APT공격이 지속적으로 발생하고 있다. 다음 사례에서 공통된 내용은 무엇인가?

> - 2009년 7.7 디도스
> - 2011년 3.4 디도스
> - 2013년 3.20 사이버테러

   ① DBMS 파괴 ② Ddos 공격
   ③ 홈페이지 변조 ④ 마스터부트레코더(MBR) 파괴

12. 공격의 종류가 적절하게 짝지어진 것은?

> (A) 네트워크에서 IP 주소, 하드웨어 주소등의 정보를 속임으로써 권한을 획득 또는 중요 정보를 가로채어 서비스를 방해하는 공격행위
> (B) 네트워크 패킷이나 버스를 통해 전달되는 중요 정보를 엿보고 가로채는 공격행위
> (C) 메모리에 할당된 배열의 크기를 초과하는 데이터를 입력하여 프로그램의 복귀 주소를 조작하여 해커가 원하는 코드를 실행하는 공격행위

> ㉠ 스니핑 ㉡ 스푸핑 ㉢ 버퍼 오버플로우

   ① (A) : ㉠, (B) : ㉡, (C) : ㉢
   ② (A) : ㉡, (B) : ㉢, (C) : ㉠
   ③ (A) : ㉡, (B) : ㉠, (C) : ㉢
   ④ (A) : ㉢, (B) : ㉠, (C) : ㉡

13. 가장 부적절한 행위는?
   ① 주요 개인정보는 암호화하여 저장하고 관련 키는 별도 백업하여 관리한다.
   ② /etc/passwd 파일의 변경은 자주 발생하기 때문에 무결성 점검은 의미가 없고 /etc/shadow 파일만 무결성 점

검도구로 관리하면 된다.

③ 커널로그, Cron 로그 등은 접근통제를 위한 모니터링 대상으로 내용 및 퍼미션 등을 주기적으로 확인한다.

④ 웹 서버의 환경설정 파일은 주기적으로 백업받고, 무결성 점검도구를 통해 변경 유무를 확인한다.

14. 적절하게 고른 것은?

㉠ 시스템의 환경 설정 및 주요 설정 파일
㉡ 프로그램 실행 시 생성되는 임시 파일
㉢ 프린터나 터미널 같은 물리적인 장치를 다루기 위한 특수파일

① ㉠ /usr, ㉡ /temp, ㉢ /dev

② ㉠ /usr, ㉡ /tmp, ㉢ /var

③ ㉠ /etc, ㉡ /temp, ㉢ /var

④ ㉠ /etc, ㉡ /tmp, ㉢ /dev

15. 파일 업로드 공격에 관한 설명과 가장 거리가 먼 것은?

① 공격자가 웹 서버 쪽에 업로드한 파일을 실행시키는 형태로 공격이 이루어진다.

② 업로드 된 파일에 대해 실행 속성을 제거함으로써 피해를 방지할 수 있다.

③ 화이트리스트 방식으로 허용된 확장자를 갖는 파일에 대해서만 업로드를 허용함으로써 공격을 방지할 수 있다.

④ 업로드 파일의 저장 경로를 '웹문서 루트'안으로 제한함으로써 공격자의 접근을 차단한다.

16. 실행 레벨을 적절하게 고른 것은?

㉠ 단일 사용자 모드
㉡ 재부팅
㉢ 전체 서비스를 지원하는 다중 사용자 모드

① ㉠ 실행레벨 1, ㉡ 실행레벨 6, ㉢ 실행레벨 3

② ㉠ 실행레벨 0, ㉡ 실행레벨 5, ㉢ 실행레벨 3

③ ㉠ 실행레벨 3, ㉡ 실행레벨 6, ㉢ 실행레벨 2

④ ㉠ 실행레벨 0, ㉡ 실행레벨 5, ㉢ 실행레벨 3

17. 다음 보기의 보안 지침 중 옳은 내용을 모두 고른 것은?

(ㄱ) Windows는 관리 특성상 ADMN$, C$, D$, IPC$ 등을 기본적으로 공유한다.
(ㄴ) IPC$ 및 nulSeessionShare는 제거하는 편이 안전하다.
(ㄷ) IPC$는 Windows Server 초기 버전에서 해킹된 사례가 있다.
(ㄹ) 숨김 공유를 설정해 놓으면 침입자의 위협을 막을 수 있다.

① (ㄱ), (ㄷ) ② (ㄱ), (ㄴ), (ㄷ)

③ (ㄱ), (ㄹ) ④ (ㄷ), (ㄹ)

18. 분산 처리 시스템에 대한 설명으로 틀린 것은?

① 목적은 자원의 공유, 연상 속도의 향상, 신뢰성과 컴퓨터 통신 등에 있다.

② 분산된 컴퓨터 간의 자원을 이용자가 쉽게 공유하여 액세스할 수 있다.

③ 시스템의 설계가 간단하여 확장이 용이하고 보안성을 향상시킬 수 있다.

④ 분산 운영체제는 시스템의 자원을 효율적으로 관리하기 위한 운영체제이다.

19. 인적자원 관리자가 특정 부서 사용자들에게 같은 직무를 수행할 수 있는 접근 권한을 할당하고 있다. 이것은 다음 중 어느 것이 예인가?

① 역할기반 접근 통제 ② 규칙기반 접근 통제

③ 중앙집중식 접근 통제 ④ 강제적 접근 통제

20. 형식에 대한 매개변수를 적절하게 고른 것은?

매개변수 형식
%d 정수형 10진수 상수
(㉠) 문자스트링
(㉡) 16진수 양의 정수
(㉢) %n의 반인 2바이트 단위

① ㉠ %s, ㉡ %o, ㉢ %lf ② ㉠ %s, ㉡ %x, ㉢ %hn

③ ㉠ %c, ㉡ %x, ㉢ %hn ④ ㉠ %c, ㉡ %o, ㉢ %lf

2과목 : 네트워크 보안

21. IDS의 동작 순서를 바르게 나열한 것은?

㉠ 데이터 가공 및 축약
㉡ 데이터 수집
㉢ 분석 및 침입탐지 단계
㉣ 보고 및 대응(Reproting and Response)

① ㉠ - ㉡ - ㉢ - ㉣ ② ㉡ - ㉠ - ㉢ - ㉣

③ ㉡ - ㉢ - ㉠ - ㉣ ④ ㉡ - ㉢ - ㉣ - ㉠

22. 스위치 장비가 동작하는 방식 중 전체 프레임을 모두 받고 오류 검출 후 전달하는 방식은?

① Cut - through 방식 ② Fragment - Free 방식

③ Stored and Forwading 방식 ④ Direct Switching 방식

23. 정적 라우팅에 대한 다음 설명 중 가장 부적절한 것은?

① 관리자가 수동으로 테이블에 각 목적지에 대한 경로를 입력한다.

② 라우팅 경로가 고정되어 있는 네트워크에 적용하면 라우터의 직접적인 처리 부하가 감소한다.

③ 보안이 중요한 네트워크 인 경우 정적 라우팅을 선호하지 않는다.

④ 네트워크 환경 변화에 능동적인 대처가 어렵다.

24. VPN 구현 기술과 가장 거리가 먼 것은?

① 터널링 ② 패킷 필터링

③ 인증 ④ 암호화

25. 암호가 걸려 해당 자료들을 열지 못하게 하는공격을 의미하는 것은?

① Ransomware ② DRDos

③ Stuxnet ④ APT

26. ㉠ ~ ㉢에 들어가야 할 단어로 적절 한 것은?

> IPv6는 (㉠)비트 주소체계를 사용하며, IPv4의 문제점 중이 하나인 규모 조정이 불가능한 라우팅 방법을 획기적으로 개선한 것으로 사용하지 않은 IP에 대해 통제를 할 수 있다. IPv6는 (㉡) 개의 필드로 구서된 헤더와 가변 길이 변수로 이루어진 확장 헤더 필드를 사용한다. 보안과 (㉢) 확장 헤더를 사용함으로써 인터넷 계층의 보안기능을 강화한다.

① ㉠ 128, ㉡ 8, ㉢ 인증 ② ㉠ 128, ㉡ 4, ㉢ 인식
③ ㉠ 64, ㉡ 8, ㉢ 인식 ④ ㉠ 64, ㉡ 4, ㉢ 인증

27. I/O 중심 프로세스와 CPU 중심 프로세스 모두를 만족시카는 스케줄러로 가장 적합한 것은?

① MLFQ(Multi Level Feedback Queue)
② RR(Round Robin)
③ SPF(Shortest Process First)
④ SRT(Shortest Remaining Time)

28. 다음 지문이 설명하는 것은?

> 트리누와 TFN을 참고하여 제작된 도구로서 이들이 갖고 있는 특성을 대부분 가지고 있는 공격도구이다. 마스터 시스템 및 에이전트 데몬 사이에 통신을 할 때 암호화 하는 기능이 추가 되었으며, TFN이나 TFN2K와 같이 ICMP Flood, SYN Flood, UDP Flood와 Smurt 등의 Ddos 공격을 할 수 있는 기능을 갖고 있다.

① Stacheldraht ② Targa
③ Bonk ④ Boink

29. 무선망에서의 공개키 기반 구조를 의미하는 것은?

① WPKI ② WML
③ WTLS ④ WIPI

30. 라모트 컴퓨터로부터의 ping 영령에 대한 응답으로 "Destination Unreachable"을 되돌려 주고, 접속을 거절하기 위해 라눅스 방화벽에서 설정하는 타깃 명령어는 무엇인가?

① DROP ② DENY
③ REJECT ④ RETURN

31. 다음 질문에서 설명하고 있는 것은?

> IEEE 802.11i 표준으로서 이전의 IEEE 802.11 표준의 약점을 보완하고 있다. 그리고 RSN(Robust Security Network)으로도 불리우며, AES블록 암호화를 사용하여 RC4 스트림 암호화를 사용하는 Wi-Fi Protected Access 표준과는 구별된다.

① WEP ② WPA2
③ EAP-TLS ④ WAP

32. (A). (B)에 들어갈 용어를 바르게 짝지은 것은?

> Tcpdump는 네트워크 인터페이스를 거치는 패킷의 내용을 출력해주는 프로그램이다. 스니핑 도구의 일종으로 자신의 컴퓨터로 들어오는 모든 패킷의 내용을 모두 모니터링 할 수 있다. LAN 상의 모든 트래픽을 모니터링 하기 위해서는 이더넷 스위치에 (A)을/를 통해 다른 컴퓨터의 트래픽이 도착하도록 하고 이더넷 모드를 (B)로 변경하여야 컴퓨터로들어 온 패킷을 운영체제에서 확인할 수 있다.

> ㉠ 포트 미러링 ㉡ 무차별 모드
> ㉢ 수집 모드 ㉣ 패킷 포워딩

① (A) : ㉠, (B) : ㉡ ② (A) : ㉠, (B) : ㉢
③ (A) : ㉣, (B) : ㉡ ④ (A) : ㉣, (B) : ㉢

33. 다음 보기가 설명하는 공격은?

> 출발지와 목적직의 IP 주소를 공격대상의 IP와 동일하게 만들어서 공격 대상에게 보내는 공격이다. 패킷을 만들어 전송하더라도 자신의 IP이므로 외부로 전송하지 못하고 자신의 컴퓨터에서 부하가 발생하게 되어, 루프 상태에 빠지게 된다.

① Land 공격 ② Targa 공격
③ Ping of Death 공격 ④ Smurf 공격

34. 지문의 특성을 갖는 공격 방법은 무엇인가?

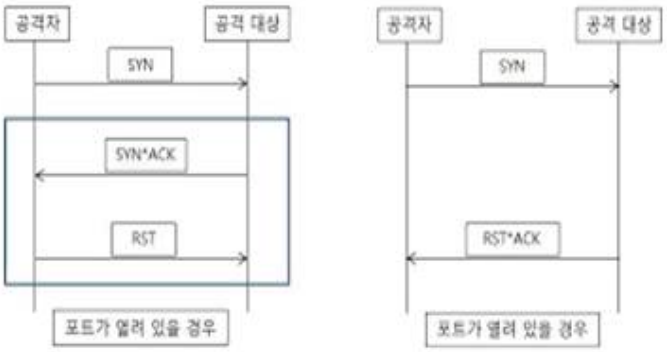
> - 출발지의 IP를 위조하여 정상 요청(request)하면 공격 대상 에 대량의 응답 값이 전달되는 것을 이용한 공격방법이다.
> - 에이전트 설치의 어려움을 보완한 공격 기법으로 TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용한 공격으로 정상적인 서바스를 제공중인 서버 Agent로 활용 하는 공격기법이다.
> - 클라이언트의 특성상 외부 인터넷 서버 접속이 잦음으로 인하여 클라이언트의 보호는 사실상 불가능하다.

① Botnet ② DRDoS
③ APT ④ Sniffing

35. 크롤러로부터 사이트를 제어하기 위해서 사용하는 파일은?

① crawler.txt ② access.conf
③ httpd.conf ④ robots.txt

36. 다음 그림에서 설명하고 있는 포트 스캔은 무엇인가?



① TCP Open 스캔
② TCP Half Open 스캔
③ TCP 단편화 (fragementation) 스캔
④ TCP FIN 스캔

37. 다음 설명에 해당하는 시스템은?

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

① NAC(Network Access Control)
② ESM(Enterprise Security Management)
③ SIEM(Security Information Event Management)
④ APT(Advanced Persistent Threat)

38. 다음 중 스위치 환경에서의 스니핑 공격 유형이 아닌 것은?
① ARP Injection ② Switch Jamming
③ ARP Redirect ④ ARP Spoofing

39. Session Hijacking에 대한 설명으로 올바르지 않은 것은?
① 세션을 Brute-Force guessing을 통해 도용하거나 가로채어 자신이 원하는 데이터를 보낼 수 있는 공격방법이다.
② 이미 인증을 받아 세션을 생성, 유지하고 있는 연결을 빼앗는 공격을 총칭한다.
③ 데이터 처리율을 감소시키고 서버가 정상 상태로 회복될 때까지 대기 상태에 빠지게 한다.
④ TCP의 세션을 끊고 순서번호(Sequence Number)를 새로 생성하여 세션을 빼앗고 인증을 회피한다.

40. 다음 설명으로 알맞은 명령어는?

> - 목적지까지의 데이터 도달 여부를 확인하는 도구이다.
> - 네트워크와 라우팅의 문제점을 찾아내는 목적으로 많이 사용되며, UDP 패킷을 이용해 진행경로의 추적과 패킷이 지나가는 IP 주소나 이름을 알아낼 수 있다.
> - 결과에서 응답시간이 *로 표시되는 경우 침입차단시스템 등의 접근통제리스트에 의해 패킷이 차단되었음을 확인할 수 있다.

① Ping ② Traceroute
③ Tcpdump ④ Netstat

3과목 : 어플리케이션 보안

41. HTTP의 요청 메소드가 아닌 것은?
① GET ② POST
③ PUSH ④ PUT

42. 다음 ㉠, ㉡에 들어갈 단어로 적절 한 것은?

> (㉠) 은(는) 악의적인 프로그램을 건전한 프로그램처럼 포장하며 일반 사용자들이 의심 없이 자신의 컴퓨터 안에서 실행시키는 프로그램을 말한다. 그리고 (㉡)은(는) OS에서 버그를 이용하여 루트권한 획득 또는 특정 기능을 수행하기 위한 공격코드 및 프로그램을 말한다.

① ㉠ Trojan, ㉡ Sniffer ② ㉠ Trojan, ㉡ Exploit
③ ㉠ Worm, ㉡ Sniffer ④ ㉠ Worm, ㉡ Exploit

43. 전자메일의 실제 발송자를 추적하기 위해 사용되는 메일헤더의 항목은?
① Message-ID ② Content-Type
③ From ④ Received

44. HTTP 응답 상태코드 기술이 잘못된 것은?
① 200 - OK ② 403 - Bad Gateway
③ 404 - Not Found ④ 500 - Internal Server Error

45. 다음은 HTTP 접속 시 노출되는 URL의 예를 보여주고 있다. URL에 보이는 메타문자를 잘못 해석한 것은?

> https://www.google.com/?gfe_rd=cr&gws_rd=cr#newwindow=1&q=%EC%B4+%EB%B3

① ? : URL 과 파라미터 구분자
② = : 파라미터 대입 연산자
③ % : HEX 값 표현에 사용
④ + : 파라미터 구분자

46. FTP 바운스 공격의 주요 목적은?
① 무작위 공격 ② IP 스푸핑
③ 포트 스캐닝 ④ 스위치 재밍

47. 다음 OTP 토큰에 대한 설명으로 적절하지 않은 것은?
① OTP 자체 생성할 수 있는 연산기능과 암호 알고리즘 등을 내장한 별도의 단말기이다.
② 외형은 USB 메모리와 비슷하다.
③ 토큰은 별도로 구매해야 한다.
④ 서버가 OTP 정보를 SMS로 전송하고 사용자는 이 정보를 이용한다.

48. DNS Cache를 확인하는 윈도우 명령어는?

```
ds,kisa,or,kr
----------------------------------
데이터 이름.....,,,ds,kisa,or,kr
데이터 유형.....,,,1
TTL(Time To Live)...,7972
데이터 길이.....5
섹션.....,,응답
(호스트)레코드.....,121,254,150,6
icms,kisa,or,kr
----------------------------------
데이터 이름.....,,,icms,kisa,or,kr
데이터 유형.....,,,1
TTL(Time To Live)...,82
데이터 길이.....5
섹션.....,,응답
(호스트)레코드.....,121,254,229,162
```

① ipconfig/ dnsdisplay ② ipconfig/ displaydns
③ ipconfig/ flushdns ④ ipconig/ dnsflush

49. 다음 중 E-mail 전송 시 보안성을 제공하기 위한 보안 전자우편 시스템이 아닌 것은?
① PGP ② S/MIME
③ PEM ④ SSL

50. HTTP 메소드(method)는?

> 요청 파라미터를 body에 붙여서 전송하며, 전송할 데이터의 양이 많은 경우 또는 민감 정보를 전송해야 하는 경우에 주로 사용함

① HEAD ② GET
③ TRACE ④ POST

51. 다음 지문은 무엇을 설명한 것인가?

> - TCP/IP 프로토콜에서 전송계층 바로 위에 위치하며 보안 기능을 수행한다.
> - 사용자 상호인증, 데이터 기밀성, 메시지 무결성 등의 보안 서비스를 제공한다.
> - Handshake 프로토콜, Charge Cipher Spec, Alert 프로토콜, Record 프로토콜로 구성된다.

① IPSec ② PGP
③ SSL/TLS ④ SHTTP

52. 콘텐츠를 메타데이터와 함께 시큐어 컨테이너 포맷 구조로 만드는 묘듈은?
① 패키지 ② DRM 제어기
③ 클리어링 하우스 ④ 식별자

53. 다음 중 SSO에 대한 설명 중 적절하지 않은 것은?
① 한번 인증을 받으면 다양안 서비스에 재인증 절차 없이 접근할 수 있다.
② SSO 서버가 단일 실패 지점이 된다.
③ 사용사는 다수의 서비스를 이용하기 위해 여러 개의 계정을 관리하지 않아도 된다.
④ 사용 편의성은 증가하지만 운영비용도 증가한다.

54. 권장하는 함수에 속하는 것은?
① strcat( ) ② gets( )
③ sprintf( ) ④ strncpy( )

55. Internet Explorer의 History 로그가 저장되는 파일은?
① system ② index.dat
③ security ④ software

56. IMAP에 대한 설명으로 틀린 것은?
① IMAP은 사용자에게 원격지 서버에 있는 e-mail을 제공해 주는 프로토콜 중의 하나이다.
② IMAP으로 접속하여 메일을 읽으면 메일 서버에는 메일이 계속 존재한다.
③ IMAP의 경우 110번 포트 사용, IMAP3의 징우 220번 포트를 사용한다.
④ 프로토콜에서 지원하는 단순한 암호인증 이외에 암호화된 채널을 SSH 클라이언트를 통해 구현할 수 있다.

57. 다음 중 정적 분석의 특징이 아닌 것은?
① 소프트웨어 실행 불필요
② stress test 나 penetration test 등의 기법
③ compile time 이나 source 수준에서 검증 가능한 coding 이나 API 보안 등의 항목 점검 수행
④ 실행 결과 보다는 실행 전 구현에 초점

58. SQL 인젝션 공격에 대한 보호 대책으로 거리가 먼 것은?
① 사용자 입력이 직접 SQL 문장으로 사용되지 않도록 한다.
② 사용사 입력으로 문자, 기호문자 그리고 구두문자까지만 사용하도록 한다.
③ SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정한다.
④ 모든 스크립트에 대힌 모든 파라미터를 점검하여 사용자 입력 값이 공격에 사용되지 않도록 한다.

59. 다음의 지문이 설명하는 무선 랜 보안 표준은?

> 이 무선 랜 보안 표준은 IEEE 802. 11i(2004년)을 준수하며, 별도의 인증 서버를 이용하는 EAP 안중 프로토콜을 사용하고, 암호 키를 동적으로 변경 가능하며, AES 등 강력한 블록 암호 알고리즘을 사용한다.

① WLAN ② WEP
③ WPA ④ WPA2

60. SET에 대한 설명 중 적절하지 않은 것은?
① 전자결제 시 교환되는 정보의 비밀 보장을 위해 공개키, 비밀키 암호 알고리즘을 사용한다.
② 데이터의 무결성을 확보하고자 전자서명과 해시 알고리즘을 사용한다.
③ 주문 정보는 상점의 공개키로, 지불 정보는 은행의 공개키로 암호화한다.
④ 지불 정보와 주문 정보는 상점과 은행이 상호 협조하여 모두 볼 수 있도록 구성되어 있다.

4과목 : 정보 보안 일반

61. 다음 설명 중 옳지 않은 것은?
① 평문을 일정한 단위로 나누어서 각 단위마다 암호화 과정을 수행하여 블록 단위로 암호문을 얻는 대칭암호화 방식이다.
② Electronic Code Book Mode, Output FeedBack Mode는 블록암호의 운용모드이다.
③ AES,SEED 등은 블록 크기로 128 비트를 사용한다.
④ SPN 구조를 사용하는 알고리즘은 DES이다.

62. 보기의 ㉠, ㉡이 설명하는 대칭키 암호 알고리즘의 동작모드는?

> ㉠ 가장 단순한 방식으로 각 블록을 독립적으로 암호화하며 동일한 평문블록이 동일한 암호문을 생성하여 안전하지 않음
> ㉡ 초기 벡터값을 암호화한 값과 평문블록을 XOR하여 암호문 블록을 생성하고, 그 암호문을 다시 암호화한 값과 평문블록을 XOR하여 암호문 블록을 반복하며 생성하는 방식

① ㉠ CFB, ㉡ CBC ② ㉠ CFB, ㉡ OFB
③ ㉠ ECB, ㉡ CFB ④ ㉠ ECB, ㉡ OFB

63. 스트림 암호 방식의 블록 암호 모드들로만 구성된 것은?
① ECB, CBC, CTR ② CFB, OFB, CTR
③ CBC, CFB, OFB ④ ECB, CFB, CTR

64. 암호 공격 유형에 대한 설명 중 적절하지 못한 것은?
① 선택 암호문 공격(Chosen-Ciphertext Attack) : 공격자가 선택한 암호문에 대한 평문을 얻을 수있다는 가정하에 수행하는 공격법
② 선택 평문 공격(Chosen-Plaintext Attack) : 공격자가 선택한 평문에 대한 키를 얻을 수 있어서 키 암호문의 쌍을 이용하는 공격법
③ 기지 평문 공격(Known-Plaintext Attack) : 공격자가 여러가지 암호뿐만 아니라 평문에 대응되는 암호문을 수집하여 암호화에 사용된 키를 찾아내는 공격법
④ 암호문 단독 공격(Ciphertext-Only Attack) : 공격자가 여러 평문에 대한 암호문을 수집하여 암호문만으로 평무을 유추하거나 키를 찾아내는 공격법

65. Diffie-Hellman 키 사전 분배에 대한 내용을 설명한 것이다. ㉠~㉣에 들어가야 할 단어로 옳은 것은?

> Diffie-Hellman 키 사전 분배 방식은 Diffie-Hellman 키 교환방식을 응용한 방식으로 (㉠)를 기반으로 구성된다. 키 분배 센터는 (㉡)p를 선정하고, Zp 위에서 원시근 g를 찾아 공개한다. 가입자는 (㉢)를 선정하여 (㉣)를 계산하여 공개한다.

① ㉠ 이산대수문제, ㉡ 큰 정수, ㉢ 공개키, ㉣ 개인키
② ㉠ 이산대수문제, ㉡ 큰 소수, ㉢ 개인키, ㉣ 공개키
③ ㉠ 소인수분해문제, ㉡ 큰 정수, ㉢ 개인키, ㉣ 공개기
④ ㉠ 소인수분해문제, ㉡ 큰 소수, ㉢ 공개기, ㉣ 개인키

66. 다음 중 이산대수 기반 암호방식이 아닌 것은?
① Elgamal 암호 ② 타원곡선 암호
③ DSA 암호 ④ 라빈(Rabin) 암호

67. 전자서명에 대한 설명으로 옳지 않은 것은?
① 전자문서의 서명은 다른 전자문서의 서명과 항상 동일해야 누구든지 검증할 수 있다.
② 전자서명을 계산하기 위해 송신자는 문서에 대해 해시값을 계산한 후 그 값올 자신의 개인키로 암호화한다.
③ 합법적인 서명자만이 전자문서에 대한 전자서명을 생성할 수 있어야 한다.
④ 어떠한 문서에 대해서도 서명의 위조가 불가능하며, 서명한 문서의 내용은 변경될 수 없어야 한다.

68. 은닉서명에 대한 바른 설명은?
① 송신자와 수신자 간에 문서의 위변조를 방지하기 위하 방법이다.
② 은닉서명 사용자가 서명자에게 자신의 메시지를 보여주지 않고 서명을 받아내는 방식이다.
③ 은닉서명을 위한 서명자의 신원은 노출되지 않고, 은닉서명 사용자는 노출될 수 있는 서명 방식이다.
④ 전자화폐 사용 시, 전자화폐 수신자의 신원 노출 방지 기능이 있다.

69. 보기에서 설명하는 ㉠ ~ ㉢에 적합한 접근통제 방법은?

> (㉠) 접근통제 : 시스템 객체에 대한 접근을 사용자 개인 또는 그룹의 식별자를 기반으로 제한하며 어떤 종류의 접근 권한을 갖는 사용자는 다른 사용자에게 자신의 판단에 의해서 권한을 줄 수 있는 방법
> (㉡) 접근통제 : 정보 시스템 내에서 어떤 주체가 특정 객체에 접근하려 할 때 양쪽의 보안 라벨(Security Label)에 기초하여 높은 보안 수준을 요구하는 정보(객체)가 낮은 보안 수준의 주체에게 노출되지 않도록 접근을 제한하는 통제 방법
> (㉢) 접근통제 : 사용자가 객체에 접근할 때, 사용자와 접근 허가의 직접적인 관계가 아닌 조직의 특성에 따른 역할을 매개자로 하여 사용자-역할, 접근 허가-역할의 관계를 통해 접근을 제어하는 방법

① ㉠ 강제적, ㉡ 임의적, ㉢ 역할기반
② ㉠ 강제적, ㉡ 역할기반, ㉢ 임의적

③ ㉠ 임의적, ㉡ 역할기반, ㉢ 강제적
④ ㉠ 임의적, ㉡ 강제적, ㉢ 역할기반

70. One Time Pad에 대한 설명 중 옳지 않은 것은?
① 최소한 평문 메시지 길이와 같은 키 스트림을 생성해야 한다.
② 암호화 키와 복호화 키가 동일하다.
③ One Time Pad 암호를 사용하려면 키 배송이 먼저 이루어져야 한다.
④ 전사 공격을 받게 되면 시간이 문제인지 궁극적으로 해독된다.

71. 다음 지문이 설명하는 것은?

> 이것은 MIT(Massachusetts Instiute of Technology) 대학에서 개발한 분산 환경 하에서 개체 인증서비스를 제공하는 네트워크 인증시스템이다. 비밀키 암호 작성법에 기초를 둔 지주 이용되는 온라인 암호키 분배방법이다. 이 시스템의 목적은 인증된 클라이언트만이 서버에 접속하도록 하는 것이다. 이것의 장점으로는 데이터의 기밀성과 무결성을 보장한다는 점을 들 수 있고, 이것의 단점으로는 키 분배센터에 장애 발생 시 전체서비스가 사용 불가 상태가 됨을 들 수 있다.

① Diffie-Hellman Protocol ② Kerberos Protocol
③ Needham-schroeder Protocol ④ SET Protocol

72. 메시지 인증에 사용하기 위한 해시 함수의 특성 중 약한 충돌 저항성이라고 부르는 해시함수 특성은?
① H(x)는 어떤 x에 대해서도 계산이 쉬워야 하고 H는 일정한 크기의 출력을 생성해야 한다.
② 어떤 주어진 값 h에 대해서 H(x)=h 가 성립하는 x를 찾는 것이 계산적으로 불가능해야 한다.
③ 어떤 주어진 블록 x 에 대해서 H(x)=H(y)를 만족하는 y (≠x)를 찾는 것이 계산적으로 불가능 해야 한다.
④ H(x)=H(y)를 만족하는 쌍 (x, y)을 찾는 것이 계산적으로 불가능해야 한다.

73. 다음 지문의 ㉠~㉢에 들어갈 단어로 적절한 것은?

> ㉠ : 어떤 실체에 대해 불법자가 정당한 사용자로 가장하여 침입하거나 정보에 대한 위협을 가하는 행위를 방지하는 것
> ㉡ : 시스템의 성능에 따라 사용자의 사용 요구가 있을 경우 시스템의 성능 명세에 따라 언제든지 접근이 가능하고 자원을 사용할 수 있도록 제공하는 서비스
> ㉢ : 통신의 한 주체가 통신에 참여했던 사실을 일부 혹은 전부를 부인하는 것을 방지

① ㉠ 접근제어, ㉡ 가용성, ㉢ 인증
② ㉠ 접근제어, ㉡ 인증, ㉢ 부인방지
③ ㉠ 인증, ㉡ 접근제어, ㉢ 가용성
④ ㉠ 인증, ㉡ 가용성, ㉢ 부인방지

74. 공개키 암호 알고리즘과 비밀키 암호 알고리증에 대한 설명으로 틀린 것은?
① RSA, ElGamal, ECC, Knapsack 암호 알고리즘은 공개키 알고리즘이다.
② 비밀키 암호 알고리즘 방식은 암호화와 복호화에 동일한 키를 사용한다.
③ 대칭키 암호 알고리즘은 스트림 암호 알고림즘과 블록 암호 알고리즘으로 나눌 수 있다.
④ 공개키 암호 알고리즘은 비밀키 암호 알고리즘보다 연산 속도가 빠르다.

75. DES 및 3-DES에 관한 설명으로 잘못된 것은?
① DES의 F-함수는 8개의 S-box로 구성되어 있으며, 각 S-box는 6비트 입력, 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.

76. 다음 지문이 설명하는 검증제도는?

> 국가&공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다.

① KCMVP 검중지제도 ② V&V 검중재도
③ NET 검증제도 ④ CAVP 감중제도

77. 다음은 BLP 모델의 특성을 나타내고 있다. 높은 보안등급과 낮은 보안등급 사이에서 읽기와 쓰기 권한이 바르게 짝지어진 것은?
① Read-Up 금지, Write-Up 금지
② Read-Down 금지, Write-Up 금지
③ Read-Up 금지, Write-Down 금지
④ Read-Down 금지, Write-Down 금지

78. 아래의 대창키 암호 알고리즘 중 Feistel 암호 구조와 SPN 구조끼리 올바르게 묶인 것은?
① (DES. SEED) : (AES. ARIA)
② (DES. ARIA) : (AES. SEED)
③ (DES. AES) : (SEED. ARIA)
④ (DES) : (SEED. AES. ARIA)

79. 보기 지문의 ㉠, ㉡ 에 적절한 것은?

> 소인수분해란 하나의 (㉠)를 소인수로 분해하는 것을 말한다. 충분히 큰 두 개의 (㉡)를 곱하는 것은 쉽지만, 이들 결과를 소인수 분해한다는 것은 계산적으로 매우 어렵다. 일부 공개키 암호알고리즘은 이렇게 소인수 분해의 어려움에 기반을 두고 설계되었다.

① ㉠ 정수, ㉡ 소수 ② ㉠ 정수, ㉡ 대수

③ ㉠ 실수, ㉡ 소수 ④ ㉠ 실수, ㉡ 대수

80. 국내 암호모듈 검증에 있어 검증대상 암호알고리즘으로 지정된 비밀키 &블록암호 알고리즘으로 구성된 것은?
① ㉠ AES, ㉡ LEA, ㉢ SEED
② ㉠ AES, ㉡ LEA, ㉢ ARIA
③ ㉠ ARIA, ㉡ SEED, ㉢ LEA
④ ㉠ ARIA, ㉡ SEED, ㉢ AES

5과목 : 정보보안 관리 및 법규

81. 보안의 특정요소에 관한 설명이다. ( )에 들어갈 암호에 적정한 것은?

> ( )은 정보시스템 또는 정보보호시스템의 결함 또는 손실에 의하여 발생되고, 정보보호 대책을 적용함으로써 감소시킬 수 있다. 그러나 ( )이 없는 시스템은 존재하지 않고, 주기적인 진단과 패치의 적용에도 불구하고, 새로운 ( )이 발생되기 때문에 완전제거는 불가능하다.

① 취약점 ② 위협
③ 위험 ④ 침해

82. 다음 중 업무연속성계획의 접근 방법론 절차에 포함되지 않는 것은?
① 사업영향평가
② 복구전략 개발
③ 프로젝트의 수행 테스트 및 유지보수
④ 교정 통제 및 잔류 위험 분석

83. 다음 ( )안에 들어갈 내용으로 맞는 것은?

> 제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부관은 정보통신망의 안정성·신뢰성 확보를 위하여 ( ) 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제3항에 따른 가준에 적합한지에 관하여 인증을 할 수 있다.

① 관리적 • 기술적 • 물리적 ② 위험 분석적
③ 기밀성 • 무결성 • 가용성 ④ 지속적 • 구조적 • 탄력적

84. 업무영향분석 시 고려해야 할 내용으로 가장 거리가 먼 것은?
① 복구 정확성, 비상시 의무사항 수행, 대체 백업 사이트의 처리 역량 검증
② 사건 발생 이후 시간이 경과함에 따라 손해 혹은 손실이 점증되는 정도
③ 최소한의 운영에 필요한 직원, 시설, 서비스를 복구하는데 소요되는 시간
④ 수입상실, 추가적 비용부담, 신용상실 등과 같은 형태의 손실

85. 정량적 위험분석 기법에 해당하는 것은?
① 델파이법 ② 시나리오법
③ 순위결정법 ④ 확률분포법

86. 다음 보기의 ㉠, ㉡에 들어가야 할 단어로 적합한 것은?

> 접근통제는 (㉠)와(과) (㉡)(이)라는 두 부분으로 나누어진다. (㉠)은(는) "그곳에 있는 사람은 누구인가?"를 의미하며, (㉡)은(는) "그 사람이 그것을 수행하는 것이 허용되었는가?"를 의미한다.

① ㉠ 보안, ㉡ 승인 ② ㉠ 배치, ㉡ 허가
③ ㉠ 인증, ㉡ 인가 ④ ㉠ 검토, ㉡ 확인

87. 개인정보보호법과 연관성이 가장 적은 것은?
① 개인정보의 수집, 이용, 제공 등 단계별 보호기준
② 공인인증기관의 지정 및 보호기준
③ 영상정보처리기기의 설치&운영 제한
④ 고유식별정보의 처리 제한

88. 정보보호정책 수립 시에 정보보호 목표를 선정함에 있어 고려해야 할 사항으로 적절하지 않은 것은?
① 사용자에게 제공하는 서비스의 이점이 위협의 비중보다 크다면 정보보호관리자는 사용자들이 위험으로부터 서비스를 안전하게 사용할 수 있도록 보호대책을 수립하여야 한다.
② 누구나 쉽게 시스템에 접근하여 사용할 수 있다면 사용하기에 편리할 수 있도록 하여야 한다. 다만 각종위협으로부터 완전히 노출되어 있이서 정보보호관리자는 시스템의 안전성을 고려하는 것보다는 시스템 사용의 용이성을 최우선과제로 선정해야한다.
③ 정보보호정책의 적용 영역은 정보기술 , 저장된 정보, 기술에 의해 조직된 정보의 모든 형태를 포함한다.
④ 정보보호를 하기 위해서는 비용이 많이 소요되므로 프라이버시 침해에 따른 손실, 서비스 침해에 따른 손실 등을 고려하여 신중하게 결정해야 한다.

89. 위험분석 방법론으로 적절히 짝지은 것은?

> ㉠ 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건 하에서 위협에 대한 발생 가능한 결과를 추정하는 방법
> ㉡ 시스템에 관한 전문적인 지식을을 가진 전문가 집단을 구성하고 위협을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법

① ㉠ 확률분포법, ㉡ 순위결정법
② ㉠ 시나리오법, ㉡ 델파이법
③ ㉠ 델파이법, ㉡ 확률분포법
④ ㉠ 순위결정법, ㉡ 시나리오법

90. 개인정보영향평가 시 반드시 고려할 사항이 아닌 것은?
① 처리하는 개인정보의 수
② 개인정보 취급자의 인가 여부
③ 개인정보의 제3자 제공 여부
④ 정보주체의 권리를 해할 가능성 및 그 위협

91. 주요 정보S신기반시설에 대한 취약점 분석 평가를 수행할 수 있는 기관이 아닌 것은?
① 한국인터넷진흥원 ② 정보보호 전문서비스 기업
③ 한국전자통신연구원 ④ 한국정보화진흥원

92. 개인정보보호법에서 정의하는 개인정보을 수집할 경우에 해당되지 않는 것은?
① 정보주체의 동의을 받는 경우
② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
③ 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
④ 정보주체의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 개인정보처리자의 권리보다 우선하는 경우

93. 다음 지문이 설명하는 인증제도는?

> 현재 사용되는 IT 보안제품에 대해 보안성을 평가하는 제도로 제품유형별 PP(Protection Profile)를 정의하고, 8개군의 평가 항목을 대상으로 평가가 이루어진다. 평가결과는 IT 보안제품의 보안위협 및 자산가치의 정도에 따라 EAL1(Evaluation Assurance Level 1) - EAL7(Evaluation Assuraxe Level 7)까지 7단계로 부여하며 인증서가 제공된다.

① CC(Common Criteria) ② ITSEC
③ BS7799 ④ ISMS

94. "개인정보 보호법"에서 개인정보의 파기 및 보존 시 가장 적절하지 않은 경우는?
① 개인정보의 이용목적이 달성될 때에는 즉시 파기하여야 한다.
② 개인정보 삭제 시 만일의 경우에 대비하여 일정기간 보관한다.
③ 개인정보를 파기하지 않고 보관할 시에는 다른 개인정보와 분리하여 저장 • 관리한다.
④ 전자적 파일 형태인 경우, 복원이 불가능한 방법으로 영구 삭제한다.

95. 다음 중 공인인증기관이 발급하는 공인인증서에 포함되어야 하는 사항이 아닌 것은 무엇인가?
① 가입자의 전자서명검증정보
② 공인인증서 비밀빈호
③ 가입자와 공인인증기관이 이용하는 전자서명방식
④ 공인인증기관의 명칭 등 공인인증기관을 확인할 수 있는 정보

96. 전자서명법에서 규정하고 있는 용어에 대한 설명 중 옳지 않은 것은?
① 전자서명 정보는 전자서명 생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 전자적 정보를 말한다.
② 전자서명은 서명자를 확인하고 서명자가 해당 전자문서에 서명하였음을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
③ 인증은 전자서명 생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말한다.
④ 전자문서는 정보 처리 시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.

97. 다음 중 아래에 대한 설명으로 가장 적합한 것은7

> 정보보호 목적과 구성, 기본 방침, 정보보호 실행계획 수립, 보안에 대한 역할과책임, 정보자산/정보시스템의 보안, 규정의 준수, 보안정책운용 정보를 포함한 문서

① 위험분석서 ② 정보보호정책서
③ 업무연속성계획서 ④ 업무영향평가서

98. 다음 업무 연속성 계획을 개발하는데 요구되는 다섯단계를 차례로 나열한 것은?

> ㉠ 계획 ㉡ 설계 ㉢ 분석
> ㉣ 구현 ㉤ 유지

① ㉠-㉡-㉢-㉣-㉤ ② ㉠-㉡-㉣-㉢-㉤
③ ㉠-㉢-㉣-㉡-㉤ ④ ㉠-㉢-㉡-㉣-㉤

99. 개인정보의 안정성 확보조치 기준(고시)의 제7조(개인정보의 암호화)에 따라 반드시 암호화하여 저장해야하는 개인정보가 아닌 것은?
① 비밀전호 ② 고유식별번호
③ 바이오 정보 ④ 전화번호

100. 아래 내용에 대한 설명으로 가장 적합한 것은?

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

① 위험분석 ② 사업영향평가
③ 업무연속싱계획 ④ 재난복구계획

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