1과목 : 시스템 보안

1. 어떤 공격을 방지하기 위한 것인가?

Data Execution Prevention(DEP), NX(No Execute)

① XSS 공격 ② 힙 스프레이 공격
③ CSRF 공격 ④ SQL 인젝션 공격

2. 다음 중 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.

3. 적절하게 고른 것은?

가. 시스템의 환경 설정 및 주요 설정 파일 나. 프로그램 실행시 생성되는 임시 파일 다. 프린터나 터미널 같은 물리적인 장치를 다루기 위한 특수 파일

① 가 /usr 나/temp 다/dev ② 가 /usr 나/tmp 다/var
③ 가 /etc 나/temp 다/var ④ 가 /etc 나/tmp 다/dev

4. 인적자원 관리자가 특정 부서 사용자들에게 같은 직무를 수행할 수 있는 접근 권한을 할당하고 있다. 이것은 다음 중 어느 것의 예인가?
① 역할기반 접근 통제 ② 규칙기반 접근 통제
③ 중앙집중식 접근 통제 ④ 강제적 접근 통제

5. 윈도우 레지스트리 하이브 파일이 아닌 것은?
① HKEY-CLASSES-ROOT ② HKEY LOCAL-MACHINE
③ HKEY-CURRENT-SAM ④ HKEY-CURRENT-USER

6. 윈도우 NTFS에서 모든 파일들과 디렉터리에 대한 정보를 포함하고 있는 것은?
① MFT(Master File Table) ② FAT(File Allocation Table)
③ $Attr Def ④ $LogFile

7. 리눅스/유닉스 시스템에서 로그를 확인하는 명령어나 로그파일과 가장 거리가 먼 것은?
① wtmp ② history
③ pacct ④ find

8. 다음 지문이 설명하는 데이터베이스 보안 유형은 무엇인가?

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

① Access Control ② Encryption
③ Views ④ Authorization Rules

9. 패스워드와 함께 일방향 해시함수에 입력되는 12비트 난수값은?
① 세션키 ② 메시지
③ 솔트(salt) ④ 멜로리

10. 아이노드(i-node)가 가지고 있지 않은 정보는?
① 파일의 이름 ② 파일의 링크 수
③ 파일 수정시각 ④ 파일 유형

11. 다음 악성코드에 대한 설명 중 옳지 않은 것은?
① 루트킷(Rootkit)은 단일 컴퓨터 또는 일련의 컴퓨터 네트워크에 대해 관리자 레벨의 접근을 가능하도록 하는 도구의 집합이다.
② 웜(Worm)은 네트워크 등의 연결을 통하여 자신의 복제품을 전파한다.
③ 트로이목마(Trojan Horse)는 정상적인 프로그램으로 가장한 악성 프로그램으로 보통 복제 과정을 통해 스스로 전파된다.
④ 트랩도어(Trapdoor)는 정상적인 인증 과정을 거치지 않고 프로그램에 접근하는 일종의 통로이다.

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

13. 다음 중 파일 시스템의 무결성 보장을 위해 점검해야 할 사항으로 옳지 않은 것은?
① 파일의 소유자, 소유그룹 등의 변경 여부 점검
② 파일의 크기 변경 점검
③ 최근에 파일에 접근한 시간 점검
④ 파일의 symbolic link의 수 점검

14. 다음 파일시스템(FAT, NTFS)에 대한 설명 중 옳지 않은 것은?
① FAT 뒤의 숫자는 표현 가능한 최대 클러스터 개수와 관련되어 있다.
② NTFS 파일시스템은 대용량 볼륨, 보안 및 암호화를 지원한다.
③ NTFS 파일시스템은 타 운영체제 호환이 용이하다.
④ 저용량 볼륨에서는 FAT가 NTFS보다 속도가 빠르다.

15. 다음 중 SECaaS에 대한 설명으로 적합하지 않은 것은?
① 클라우드 컴퓨팅 환경 하에서 인터넷을 통하여 보안서비스를 제공하는 것을 두고 SECaaS(Security as a Service)라고 한다.
② SECaaS는 Standalone으로 클라우드 기반 보안서비스를 제공하는 형태와 클라우드 서비스 제공업체가 자사의 고객에게 보안기능을 제공하는 형태로 나뉠 수 있다
③ SECaaS는 보안서비스를 ASP 형태로 공급한다는 측면에서 넓은 의미의 PaaS(Platform as a Service) 로 볼 수 있다.
④ SECaaS는 인증, 안티바이러스, 침입탐지, 모의침투, 보안이벤트 관리 등의 다양한 보안 기능을 제공할 수 있다.

16. SAM에 대한 설명으로 옳지 않은 것은?
① 사용자 패스워드는 해시된 상태로 저장된다.

② SID를 사용하여 각 자원에 대한 접근권한을 명시한다.
③ SAM 파일은 사용자, 그룹 계정 및 암호화된 패스워드 정보를 저장하고 있는 데이터베이스이다.
④ 사용자 로그인 정보와 SAM 파일에 저장된 사용자 패스워드 정보를 비교해 인증 여부가 결정된다.

17. 로그분석에 사용되며 문자열을 처리하는 Unix 명령어와 가장 거리가 먼 것은?
① awk ② wc
③ grep ④ nohup

18. 다음 지문에서 설명하고 있는 침입탐지 기술이 무엇인지 고르시오.

> - 공격자의 동작에 관한 정보를 수집한다.
> - 공격자가 시스템에 충분히 오랜 시간 동안 머무르기를 유도함으로써 관리자가 반응할 수 있도록 한다.

① IDS(Instrusion Detection System)
② IPS(Instrusion Prevention System)
③ UTM(Unified Threat Management)
④ Honeypot

19. 다음 중 Unix 시스템에서 secure.txt 파일의 소유자에게는 읽기와 실행권한을 부여하고 다른 사용자에게는 읽기 권한을 제거하라는 권한 변경 명령으로 알맞은 것은?
① #chmod 306 secure.txt
② #chmod 504 secure.txt
③ #chmod otrx, a-r secure.txt
④ #chmod u=rx, o-r secure.txt

20. 리눅스에서 관리하는 주요 로그파일에 대한 설명으로 옳지 않은 것은?
① /var/log/cron : 시스템의 정기적인 작업에 대한 로그
② /var/log/messages : 커널에서 보내주는 실시간 메시지
③ /var/log/secure : 시스템의 접속에 관한 로그로 언제/누가/어디의 정보를 포함
④ /var/log/xferlog : 메일 송수신에 관한 로그

2과목 : 네트워크 보안

21. 다음은 PORT 스캔 공격에 관한 설명이다. 설명 중 맞는 것을 모두 고른 것은?

> 가. PORT 스캔은 공격대상 시스템의 포트가 열려 있는지 확인하는 일종의 공격이다.
> 나. Stealth 스캔의 대표적인 경우로 TCP Half-Open 스캔이 있다.
> 다. Null 스캔은 포트가 열려 있을 경우에는 응답이 없고, 닫혀있을 경우에만 RST/ACK 패킷이 되돌아 온다.
> 라. UDP Open 스캔은 포트가 열려 있을 경우에는 아무런 응답이 없고, 포트가 닫혀있을 경우에는 ICMP Unreachable 패킷을 받게 된다.

① 가, 나 ② 가, 나, 다.
③ 가, 나, 라 ④ 가, 나, 다, 라

22. 다음의 포트 스캔 중 플래그 (SYN, RST, ACK, AN, PS URG)을 모두 off하여 스캔하는 것은?
① TCP SYN 스캔 ② Fin 스캔
③ Null 스캔 ④ Xmas 스캔

23. 오용탐지 방법으로 적당하지 않은 것은?
① 시그니처 분석 ② 페트리넷(Petri-net)
③ 상태전이 분석 ④ 데이터마이닝

24. 공격 대상이 방문할 가능성이 있는 합법적인 웹 사이트를 미리 감염시킨 뒤, 잠복하고 있다가 공격 대상이 방문하면 대상의 컴퓨터에 악성코드를 설치하는 공격 방법은?
① 악성 봇(Malicious Bot) 공격
② 워터링 홀(Watering Hole) 공격
③ 스피어 피싱(Spear Phishing) 공격
④ 피싱(Phishing) 공격

25. 다음 중 패킷의 출발지와 목적지 모두를 반영하여 주소 변환을 수행하는 NAT(Network Address Translation)는?
① 동적 NAT ② 정적 NAT
③ 바이패스 NAT ④ 폴리시 NAT

26. 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

27. 다음 용어 중 개념상 나머지와 가장 거리가 먼 것은?
① sniffing ② eavesdropping
③ tapping ④ spoofing

28. 다음 중 end point에 설치되어 다양한 보안 기능을 통합적으로 수행하는 보안 시스템을 지칭하는 것은?
① IPS ② NAC
③ Firewall ④ UTM

29. 다음 중 전문가 시스템(Expert System)을 이용한 IDS에서 사용되는 침입 탐지기법은?
① Behavior Detection
② State Transition Detection
③ Knowledge Based Detection
④ Statistical Detection

30. Snort의 각 규칙은 고정된 헤더와 옵션을 가지고 있다. 패킷의 payload 데이터를 검사할 때 사용되는 옵션에 포함되지 않는 필드는?
① ttl ② content
③ depth ④ offset

31. 이래 지문 빈칸에 들어갈 용어를 바르게 짝지은 것은?

> Tcpdump는 네트워크 인터페이스를 거치는 패킷의 내용을 출력해 주는 프로그램이다. 스니핑 도구의 일종으로 자신의 컴퓨터로 들어오는 모든 패킷의 내용을 모니터링 할 수 있다. LAN 상의 모든 트래픽을 모니터링 하기 위해서는 이더넷 스위치에서의 (가)을 통해 다른 컴퓨터로 향하는 트래픽도 수 신하도록 한다. 이 때 이더넷 모드를 (나)로 변경하여야 컴 퓨터로 들어온 패킷을 운영체제에서 확인할 수 있다.

① 가 : 포트 미러링(Port Mirroring) 나: 수집 모드 (Acquisition Mode)
② 가 : 포트 미러링(Port Mirroring) 나 : 무차별 모드 (Promiscuous Mode)
③ 가 : 패킷 포워딩(Packet Forwarding) 나 : 수집 모드 (Acquisition Mode)
④ 가 : 패킷 포워딩(Packet Forwarding) 나 : 무차별 모드 (Promiscuous Mode)

32. 다음 중 VoIP 서비스에 대한 공격과 가장 거리가 먼 것은?
① Register 플러딩 공격 ② GET 플러딩 공격
③ INVITE 플러딩 공격 ④ RTP 플러딩 공격

33. 3개의 IP 패킷으로 fragmentation 되는 과정을 설명한 것이다. 세 번째 패킷의 필드에 들어갈 값으로 적절한 것은?

패킷사이즈	flag	offset
1500	1	0
1500	1	185
(가)	0	(나)

① 가: 1040 , 나: 130 ② 가: 1000 , 나: 370
③ 가: 1040 , 나: 370 ④ 가: 1000 , 나: 125

34. 스위치 장비가 동작하는 방식 중 전체 프레임을 모두 받고 오류 검출 후 전달하는 방식은?
① Cut-through 방식 ② Fragment-Free 방식
③ Direct Switching 방식 ④ Store and Forward 방식

35. VPN의 기능과 가장 거리가 먼 것은?
① 데이터 기밀성 ② 데이터 무결성
③ 접근통제 ④ 시스템 무결성

36. 스위칭 환경에서의 스니핑 공격 유형 중, 공격자가 “나의 MAC 주소가 라우터의 MAC 주소이다."라는 위조된 ARP Reply를 브로드캐스트로 네트워크에 주기적으로 보내어 스위칭 네트워크상의 다른 모든 호스트들이 공격자 호스트를 라우터로 믿게 하는 공격은?
① Switching Jamming ② ICMP Redirect
③ ARP Redirect ④ DNS Spoofing

37. 보안 위협과 공격에 대한 설명 중 옳지 않은 것은?
① 분산 반사 서비스 거부 공격(DRDoS : Distributed Reflection DoS)은 DDoS의 발전된 공격 기술로서 공격자의 주소를 위장하는 IP Spoofing 기법과 실제 공격을 수행하는 좀비와 같은 감염된 반사체 시스템을 통한 트래픽 증폭 기법을 이용한다.
② 봇넷을 이용한 공격은 봇에 의해 감염된 다수의 컴퓨터가 좀비와 같이 C&C 서버를 통해 전송되는 봇 마스터의 명령에 의해 공격이 이루어지므로 공격자 즉 공격의 진원지를 추적하는데 어려움이 있다.
③ Smurf 공격은 ICMP Flooding 기법을 이용한 DoS 공격으로 Broadcast address 주소의 동작특성과 IP Spoofing 기법을 악용하고 있다.
④ XSS(Cross-Site Scripting) 공격은 공격 대상 사용자가 이용하는 컴퓨터 시스템의 브라우저 등에서 악성코드가 수행되도록 조작하여 사용자의 쿠키 정보를 탈취, 세션 하이재킹과 같은 후속 공격을 가능하게 한다.

38. 다음 지문의 방법들이 탐지하려는 공격은?

> - 비동기화 상태 탐지
> - Ack Storm SATI
> - 패킷의 유실과 재전송 증가 탐지
> - 예상치 못한 접속의 리셋

① MITM 공격 ② TCP 세션 하이재킹
③ 스푸핑 공격 ④ 스머프 공격

39. L2 스위치로 구성된 네트워크 환경에서 스니핑 공격에 대한 설명으로 옳지 않은 것은?
① L2 스위치로 구성된 네트워크 환경에서 스니핑 공격을 시도하기 위해 사용되는 주요 방법들로는 ARP Spoofing ICMP Redirect, MAC Address Flooding 등이 있다.
② ARP Spoofing 공격은 공격자가 대상 시스템에 조작된 ARP Request를 지속적으로 전송함으로써 이루어지며, 대상시스템의 ARP cache table을 변조한다.
③ ICMP Redirect 공격은 공격자가 ICMP Redirect 메시지를 생성하여 공격 대상 시스템에게 전송함으로써 공격대상 시스템이 전송하는 패킷이 공격자에게 먼저 전송되도록 한다.
④ MAC Address Flooding 공격은 공격자가 조작된 MAC 주소를 프레임의 출발지 MAC 주소에 설정하여 보내는 과정을 반복함으로써 스위치가 더미허브처럼 동작하도록 한다.

40. IDS의 동작 순서를 바르게 나열한 것은?

> 가. 데이터 가공 및 축약
> 나. 데이터 수집
> 다. 분석 및 침입탐지 단계
> 라. 보고 및 대응(Reporting and Response)

① 가 - 나 - 다 - 라 ② 나 - 가 - 다 - 라
③ 나 - 다 - 가 - 라 ④ 나 - 다 - 라 - 가

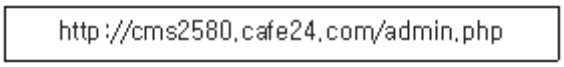
3과목 : 어플리케이션 보안

41. 다음 중 XML 기반 Web 기술과 관련성이 가장 적은 것은?
① OCSP ② UDDI
③ WSDL ④ SOAP

42. 전자입찰시스템 및 프로토콜의 특징에 대한 설명 중 틀린 것은?

① 전자 입찰 도구로는 자바, 디지털서명, XML 등이 이용될 수 있다.
② 입찰 기간 마감은 여러 개의 입찰 서버가 있을 경우 단계적으로 마감된다.
③ 전자 입찰은 입찰자, 입찰 공고자, 전자입찰시스템으로 구성된다.
④ 전자 입찰 시 독립성, 비밀성, 무결성 등이 요구된다.

43. 아래 그림은 공격자가 웹 해킹을 시도하는 화면이다. 이래 화면의 URL을 고려할 때, 공격자가 이용하는 웹 취약점으로 가장 적절한 것은?



① 관리자 페이지 노출 취약점
② 파일 다운로드 취약점
③ 파일 업로드 취약점
④ 디렉터리 리스팅(Directory Listing) 취약점

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

45. 보안담당자 A씨는 자바스크립트 코드를 분석하기 위해 파일을 열었더니 아래와 같은 내용을 확인할 수 있었다. 아래와 같은 기법의 명칭은? (문제 복원 오류로 그림이 없습니다. 정확한 그림 내용을 아시는분 께서는 오류신고 또는 게시판에 작성 부탁드립니다.)
① 암호화 ② 난독화
③ 복호화 ④ 정규화

46. 다음 지문에서 설명한 프로토콜을 올바르게 나열한 것은?

가: 사용자와 은행 사이에서 수행되는 프로토콜로서 은행이 사용자에게 전자 화폐를 발급해 주는 절차를 명세한 프로토콜이다.
나: 사용자와 상점 사이에서 수행되는 프로토콜로서 사용자가 구매 대금으로 자신의 전자 화폐를 상점에 지불하는 과정을 명세한 프로토콜이다.
다: 상점과 은행 사이에서 수행되는 프로토콜로서 상점이 사용자로부터 받은 전자 화를 은행이 결제해 주는 프로토콜이다.

① 가:인출 프로토콜 나:지불 프로토콜 다:예치 프로토콜
② 가:인출 프로토콜 나:예치 프로토콜 다:지불 프로토콜
③ 가:지불 프로토콜 나:인출 프로토콜 다:예치 프로토콜
④ 가:예치 프로토콜 나:지불 프로토콜 다:인출 프로토콜

47. 다음의 지문이 설명하는 무선 랜 보안 표준은?

이 무선 랜 보안 표준은 IEEE 802.11(2004년)을 준수하며, 별도의 인증 서버를 이용하는 EAP 인증 프로토콜을 사용하 고 암호 키를 동적으로 변경 가능하며, AES 등 강력한 블록 암호 알고리즘을 사용한다.

① WLAN ② WEP
③ WPA ④ WPA2

48. 다음 지문이 설명하고 있는 DRM의 구성요소는?

지적재산권으로 보호되어야 할 정보의 단위로 일반적으로 패 키지를 통해 패키징 되기 이전의 원본을 의미한다.

① 콘텐츠 ② 워터마크
③ DOI ④ 컨트롤러

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

50. 다음 중 디지털 핑거프린팅 기술에 대한 설명으로 옳지 않은 것은?
① 디지털 핑거프린팅 기술은 콘텐츠 내에 소유자 정보와 구매자 정보를 함께 포함하는 핑거프린트 정보를 삽입하여 후에 불법으로 배포된 콘텐츠로부터 배포자가 누구인지를 역추적 할 수 있도록 해 주는 기술이다.
② 핑거프린팅된 콘텐츠는 서로 다른 구매자 정보를 삽입하기 때문에 구매자에 따라 콘텐츠가 조금씩 다르다.
③ 공모공격 (collusion attack)이란 여러 개의 콘텐츠를 서로 비교하여 워터마킹된 정보를 제거하거나 혹은 유추하여 다른 워터마크 정보를 삽입할 수 있는 것을 의미하는데, 이처럼 워터마킹은 공모공격에 취약하지만 디지털 핑거프린팅 기술은 이 공격에 매우 안전하다.
④ 디지털 핑거프린팅 기술은 워터마킹 기술과 같이 삽입과 추출기술로 분류하는데 삽입기술은 삽입하는 정보만 다를뿐 워터마킹 기술과 동일하다.

51. 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..... 121.254.229.1621
```

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

52. 아래는 vsftp의 설정파일인 vsftpd.conf에 대한 설명이다.

올바른 내용을 모두 고르시오.

> 가: amonymous_erable : 익명 접속 설정으로 권장은 NO이다.
> 나: port_enable : YES 값은 데이터 전송을 위해서 Passive Mode를 사용하도록 설정한다.
> 다: xferlog_enable : FTP 로그를 남길 것인지에 대한 설정으로 로그 위치는 vsftpd_log file에서 설정한다.
> 라: local enable : 로컬 계정 사용자들의 접속 허용을 설정한다.

① 가, 나, 다 ② 가, 다
③ 가, 나, 다, 라 ④ 가, 다, 라

53. 다음에서 설명하는 정보보호 기술은?

> 전달하려는 정보를 이미지, 오디오 파일에 인간이 감지할 수 없도록 숨겨 상대방에게 전달하는 기술을 총칭한다.
> 일반 암호화 방법은 암호화를 통해 정보의 내용을 보호하는 기술인 반면에 이 기술은 정보의 존재 자체를 숨기는 보안 기술이다.

① 핑거프린트(Fingerprint)
② DOI(Digital Object Identifier)
③ 디지털 워터마크(Digital watermark)
④ 스테가노그래피(Steganography)

54. 다음 지문은 무엇을 설명한 것인가?

> - TCP/IP 프로토콜에서 전송 계층 바로 위에 위치하며 보안기능을 수행한다.
> - 사용자 상호인증, 데이터 기밀성, 메시지 무결성 등의 보안서비스를 제공한다.
> - Handshake 프로토콜, Change Cipher Spec, Aler 프로토콜 Record 프로토콜로 구성된다.

① IPSec ② PGP
③ SSL/TLS ④ SHTTP

55. 다음 지문이 설명하는 전자 거래 문서의 유형으로 알맞은 것은?

> 데이터의 저장 및 교환을 위한 대표적 문서교환 표준인 SGM (Standard Generalized Markup Language)과 HIM (Hyper Tel Merkup Largage)의 장점을 모두 가지고 있다.
> 1996년 W3C에서 제안하였으며, 웹상에서 구조화된 문서를 전송 가능하도 록 설계된 웹표준이며, 최근 전자거래 및 각종 업무에서 표준으로 폭넓게 채택되어 사용되고 있다.

① SWIFT
② ebXML
③ EDI(Electronic Data Interchange)
④ XML(Extensible Markup Language)

56. 다음 보기가 설명하는 취약성은?

> 이것은 암호화를 위해 대중적으로 사용되는 OpenSSL 라이브 러리에서 서버 메모리 중 64KB의 데이터에 대해 공격자가 덤프를 뜰 수 있게 하는 취약점이다. 해당 취약점을 이용하여 시스템 메모리에 저장되어 있는 무의미한 작은 정보들을 지속적으로 유출시키면, 이러한 무의미한 정보들이 모여 하나의 완전한 유의미한 정보가 될 수 있다. 특히 개인키의 경우 암 호화하여 전달되는 데이터를 모두 열람할 수 있는 핵심정보 이기때문에 매우 심각한 취약성이라 할 수 있다.

① Poodle ② Ghost
③ Shellshock ④ Heartbleed

57. 다음 표는 Apache 웹 서버의 주요 파일에 대한 접근권한을 나타낸다. 각각에 들어갈 내용으로 적절한 것은?

디렉터리	소유자	그룹	권한
bin	root	root	755
httpd	root	root	(가)
passwd	root	(나)	640
httpd.conf	root	nobody	(다)
log	root	root	755

① 가:640 나:root 다:511 ② 가:511 나:nobody 다:640
③ 가:640 나:nobody 다:511 ④ 가:511 나:root 다:640

58. SSL/TLS에 대한 설명으로 옳은 것은?

① 상위계층 프로토콜의 메시지에 대해 기밀성과 부인방지를 제공한다.
② 종단 대 종단 간의 안전한 서비스를 제공하기 위해 UDP를 사용하도록 설계하였다.
③ 레코드(Record) 프로토콜에서는 응용계층의 메시지에 대해 단편화, 압축, MAC 첨부, 암호화 등을 수행한다.
④ 암호명세 변경(Change Cipher Spec) 프로토콜에서는 클라이언트와 서버가 사용할 알고리즘과 키를 협상한다.

59. 다음 중 PGP의 기능이 아닌 것은?

① 기밀성 ② 전자서명
③ 단편화와 재조립 ④ 송수신 부인방지

60. 다음 중 데이터베이스 보안 유형이 아닌 것은?

① 접근 제어(Access Control)
② 허가 규칙(Authorization Rule)
③ 암호화(Encryption)
④ 집합(Aggregation)

4과목 : 정보 보안 일반

61. 국내 암호모듈 검증에 있어 검증대상 암호알고리즘으로 지정된 비밀키 블록암호 알고리즘으로 구성된 것은?

① 가:AES, 나:LEA 다:SEED
② 가:AES, 나:LEA 다:ARIA
③ 가:ARIA, 나:LEA 다:SEED
④ 가:ARIA, 나:AES 다:SEED

62. 사용자 인증에서는 3가지 유형의 인증방식을 사용하고 있으며, 보안을 강화하기 위하여 2가지 유형을 결합하여 2 factor 인증을 수행한다. 다음 중 2 factor 인증으로 적절하지 않은 것은?
① USB 토큰, 비밀번호
② 스마트카드, PIN(Personal Identification Number)
③ 지문, 비밀번호
④ 음성인식, 수기서명

63. 강제적 접근통제 정책에 대한 설명으로 옳지 않은 것은?
① 모든 주체와 객체에 보안관리자가 부여한 보안레이블이 부여되며 주체가 객체를 접근할 때 주체와 객체의 보안 레이블을 비교하여 접근허가 여부를 결정한다.
② 미리 정의된 보안규칙들에 의해 접근허가 여부가 판단되므로 임의적 접근통제 정책에 비해 객체에 대한 중앙 집중적인 접근통제가 가능하다.
③ 강제적 접근통제 정책을 지원하는 대표적 접근통제 모델로는 BLP(Bell-Lapadula), Biba 등이 있다.
④ 강제적 접근통제 정책에 구현하는 대표적 보안 메커니즘으로 Capability List와 ACL(Access Control List) 등이 있다

64. 다음 지문이 설명하고 있는 프로토콜은?

- 공유할 암호키를 계산하여 만들어낸다. - 유한체상의 이산대수문제를 풀기 어려움에 기반한다. - 중간자 공격이나 재전송 공격에는 취약하다.

① Needham-Schroeder 프로토콜
② 공개키 암호
③ KDC 기반 키 분배
④ Diffie-Hellman 프로토콜

65. 아래 보기에서 설명하고 있는 공격기법은?

1997년 Diffie와 Hellman이 제안하였으며 암호화할 때 일어날 수 있는 모든 가능한 경우에 대하여 조사하는 방법으로 경우 의 수가 적을 때는 가장 정확한 방법이지만, 일반적으로 경우의 수가 많은 경우에는 실현 불가능하다.

① 차분 공격(Differential Cryptanalysis)
② 선형 공격(Linear Cryptanalysis)
③ 전수 공격(Exhaustive key search)
④ 통계적 분석(Statistical analysis)

66. 소프트웨어로 구성되는 난수 생성기를 가장 적절하게 표현한 것은?
① SRNG ② HRNG
③ PRNG ④ RRNG

67. 아래 보기에서 설명하고 있는 공격기법은?

1990년 Bham과 Sharir에 의하여 개발된 선택 평문 공격법 으로, 두 개의 평문 블록의 비트 차이에 대하여 대응되는 암호문 블록들의 비트 차이를 이용하여 사용된 암호키를 찾아 내는 방법이다.

① 차분 공격(Differential Cryptanalysis)
② 선형 공격(Linear Cryptanalysis)
③ 전수 공격(Exhaustive key search)
④ 통계적 분석(Statistical analysis)

68. 다음의 장·단점을 가진 인증기술은?

- 장점 : 데이터의 기밀성, 무결성 보장 - 단점 : 키 분배센터(인증서버 & 티켓발급서버)에 오류 발생시 전체 서비스 이용불가

① 커버로스(Kerberos) 프로토콜 ② OTP 인증
③ ID/패스워드 인증 ④ 메시지 출처 인증

69. 키 관리는 키 생성, 분배, 설치, 갱신, 취소 폐기, 저장, 복구 등을 요구하는 포괄적인 개념이다. 한 사용자 또는 기관이 비밀키를 설정하여 다른 사용자에게 전달하는 기술을 키 분배라고 하며, 둘 또는 그 이상의 사용자가 공개된 통신 채널을 통하여 비밀키를 설정하는 것을 키 합의라고 한다. 다음 중 키 분배 방식에 해당되는 것은?
① Diffie-Hellman 방식
② Matsumoto-Takashima-Imai 방식
③ Okamoto-Nakamura 방식
④ Needham-Schroeder 방식

70. 다음 중 해시함수의 특징이 아닌 것은?
① 고정된 크기의 해시코드를 생성함
② 일방향성(one-wayness)
③ 강 · 약 충돌 회피성이 보장됨
④ 안전한 키를 사용할 경우 결과값의 안전성이 보장됨

71. 다음 중 암호시스템에 대한 수동적 공격은?
① 트래픽 분석 ② 메시지 순서 변경
③ 메시지 위조 ④ 삭제 공격

72. 다음 중 스트림 암호의 특징으로 알맞지 않은 것은?
① 원타임 패스워드를 실용적으로 구현할 목적으로 개발되었다.
② 짧은 주기와 높은 선형복잡도가 요구되며 주로 LFSR을 이용한다.
③ 블록단위 암호화 대비 비트단위로 암호화하여 암호화 시간이 더 빠르다.
④ 블록 암호의 CFB, OFB 모드는 스트림 암호와 비슷한 역할을 한다.

73. "한 단계 앞의 암호문 블록"을 대신할 비트열을 무엇이라 하는가?
① 패딩 ② 초기화 벡터
③ 스트림 블록 ④ 운영모드

74. 이중서명(Dual Signature)은 사용자가 구매정보와 지불정보를 각각 해시한 후 해시값을 합하여 다시해시 그리고 최종 해시값을 카드 사용자의 개인키로 암호화한 서명을 말하는 것으로 이중서명 절차이다. 이중서명을 사용하는 것으로 적합한 것은?

① SET ② PKI
③ 전자화폐 ④ 전자수표

75. 다음 지문이 설명하는 것은?

> 이것은 MIT(Massachusetts Institute of Technology) 대학에서 개발한 분산 환경 하에서 개체 인증서비스를 제공하는 네트워크 인증시스템이다. 비밀키 암호작성법에 기초를 둔 자주 이용되는 온라인 암호키 분배 방법이다. 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

76. 다음 중 임의적 접근통제(DAC : Dscretionary access control) 에 해당하는 특징이 아닌 것은?

① 사용자 기반 및 ID 기반 접근통제
② 중앙 집중적 관리가 가능
③ 모든 개개의 주체와 객체 단위로 접근권한 설정
④ 객체의 소유주가 주체와 객체 간의 접근통제 관계를 정의

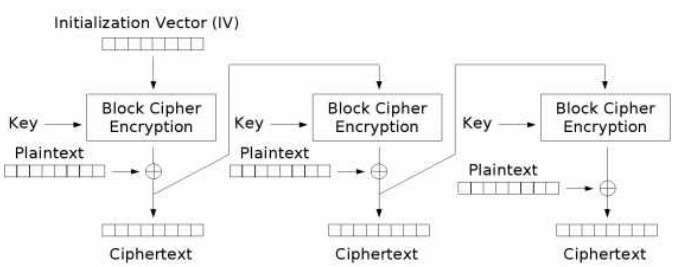
77. 다음 중 대칭 암호 알고리즘이 아닌 것은?

① BlowFish ② SEED
③ Diffie-Hellman ④ 3DES

78. 다음 중 인증서가 폐지되는 사유가 아닌 것은?

① 인증서 발행 조직에서 탈퇴
② 개인키의 손상
③ 개인키의 유출 의심
④ 인증서의 유효기간 만료

79. 다음 그림은 블록암호 운용모드의 한 종류를 나타낸 것이다. 다음 그림에 해당하는 블록암호 운용모드는?



① CBC(Cipher Block Chaining)
② ECB(Electronic CodeBook)
③ CTR(CounTeR)
④ CFB(Cipher FeedBack)

80. n명의 사람이 대칭키 암호화 통신을 할 경우 몇 개의 대칭키가 필요한가?

① n(n+1)/2 ② n(n-1)/2
③ n(n-1) ④ n(n+1)

5과목 : 정보보안 관리 및 법규

81. 괄호에 공통적으로 들어갈 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. 위험분석 방법론으로 적절히 짝지은 것은?

> 가: 그 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하며 일정 조건 하에서 위협에 대한 발생 가능한 결과를 추정하는 방법
> 나: 시스템에 관한 전문적인 지식을 가진 전문가 집단을 구성하고 위협을 분석 및 평가하여 정보시스템이 직면한 다양 한 위협과 취약성을 토론을 통해 분석하는 방법

① 가: 확률분포법 나: 순위결정법
② 가: 시나리오법 나: 델파이법
③ 가: 델파이법 나: 확률분포법
④ 가: 순위결정법 나:시나리오법

83. 「개인정보보호법」에 의거하여 개인정보처리자는 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다. 동의를 서면으로 받을 때에는 중요한 내용을 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하도록 되어 있다. 이때 중요한 내용에 해당되지 않는 것은?

① 동의를 거부할 권리가 있다는 사실 및 거부에 따른 불이익이이 있을 경우에는 불이익에 대한 내용
② 개인정보를 제공받는 자
③ 개인정보를 제공받는 자의 개인정보 이용 목적
④ 개인정보의 보유 및 이용 기간

84. 「개인정보보호법」에 의거하여 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보 파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험 요인의 분석과 개선사항 도출을 위한 영향평가를 하고 그 결과를 행정안전부장관에게 제출하여야 한다. 영향평가를 하는 경우에 고려해야 할 사항으로 적합하지 않은 것은?

① 처리하는 개인정보의 수
② 개인정보의 제3자의 제공 여부
③ 정보주체의 권리를 해할 가능성 및 그 위험 정도
④ 개인정보를 처리하는 수탁업체 관리·감독의 여부

85. "개인정보 보호법"에서 개인정보의 파기 및 보존 시 가장 적절하지 않은 경우는?
① 개인정보의 이용목적이 달성된 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.

86. 「개인정보보호법」에 의거하여 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 정보주체에게 알려야 하는 사항들에 해당되지 않는 것은?
① 개인정보 처리의 정지를 요구할 권리가 있다는 사실
② 개인정보의 보유·이용 기간
③ 개인정보의 수집 출처
④ 개인정보의 처리 목적

87. 다음 지문이 설명하는 위험분석방법론은?

- 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.
- 위험 분석을 짧은 기간에 도출할 수 있어 시간과 비용을 절약할 수 있지만, 추정의 정확도가 낮다.

① 과거자료 분석법 ② 확률 분포법
③ 델파이법 ④ 시나리오법

88. 정보보호 사전점검에 대한 설명으로 옳은 것은?
① 정보보호 사전점검은 전자적 침해행위에 대비하기 위한 정보시스템의 취약점 분석 평가와 이에 기초한 보호대책의 제시 또는 정보보호 관리체계 구축 등을 주된 목적으로 한다.
② 방송통신위원회는 사업자가 사전점검을 실시하거나 실시계약을 체결한 경우 해당 사업 또는 서비스에 대하여 가점을 부여하는 등 우대조치를 할 수 있다.
③ 사전점검 수행기관으로 지정받으려는 자는 수행기관 지정 신청서를 방송통신위원회에 제출하여야 한다.
④ 사전점검 대상 범위는 제공하려는 사업 또는 정보통신서비스를 구성하는 하드웨어, 소프트웨어, 네트워크 등의 유무형 설비 및 시설을 대상으로 한다.

89. 도출된 위험이 해당 사업에 심각한 영향을 주는 관계로 보험에 가입하였다. 이런 식으로 위험을 경감 또는 완화시키는 처리 유형은 무엇인가?
① 위험 감소(reduction) ② 위험 전가(transfer)
③ 위험 수용(acceptance) ④ 위험 회피(avoidance)

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

91. 고유식별정보는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보이다. 다음 중 개인정보처리자가 고유식별정보를 처리할 수 있는 경우에 해당하는 것은?
① 정보주체의 동의를 받지 않은 경우
② 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우
③ 교통단속을 위하여 필요한 경우
④ 시설 안전 및 화재 예방을 위하여 필요한 경우

92. 다음 중 이래 지문의 빈칸 안에 들어가야 할 단어 또는 문장으로 가장 적합한 것은?

개인정보 보호법」 제2조(정의) 이 법에서 사용하는 용어의 뜻 은 다음과 같다.
"개인정보'란 살아 있는 개인에 관한 정보로서 성명 (가) 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 (해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보 와 쉽게 (하여 알아볼 수 있는 것을 포함한다)를 말한다.
「정보통신망법」 제2조정의) 1이 법에서 사용하는 용어의 뜻 은 다음과 같다. "개인정보란 생존하는 개인에 관한 정보로서 성명 (가) 등에 의하여 특정한 개인을 알아볼 수 있는 부호 · 문자· 음성 · 음향 및 영상 등의 정보(해당 정보만으로는 특 정 개인을 알아볼 수 없어도 다른 정보와 쉽게 (나)하여 알아 볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

① 가:주민등록번호 나: 구분 ② 가:성별 나: 유추
③ 가:주민등록번호 나: 결합 ④ 가:성별 나: 구분

93. 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

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

95. 다음은 정보통신기반 보호법에 따른 주요 정보통신기반시설의 지정요건이다. 빈칸 가 ~ 마 에 들어갈 알맞은 단어를 바르게 나열한 것은?

중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.
1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 (가)
2. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 정보통신기반시설에 대한 (나)
3. 다른 정보통신기반시설과의 (다)
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 (라) 또는 그 복구의 (마)

① 가:중요성 나:기밀성 다:의존도 라:발생가능성 마:용이성
② 가:기밀성 나:중요성 다:의존도 라:용이성 마:경제성
③ 가:중요성 나:의존도 다:상호연계성 라:발생가능성 마:용이성
④ 가:의존도 나:중요성 다:상호연계성 라:발생가능성 마:용이성

96. 「개인정보보호법」상에서 민감정보로 명시되어 있는 것은?
① 혈액형 ② 사상·신념
③ 결혼 여부 ④ 성별

97. 다음 정보보호 관리체계 인증제도에 대한 설명으로 가장 적절하지 않은 것은?
① 정보통신서비스와 직접적인 관련성이 낮은 전사적 자원관 리시스템(ERP), 분석용 데이터베이스(DW), 그룹웨어 등 기업 내부 시스템, 영업/마케팅 조직은 일반적으로 인증 범위에서 제외해도 된다.
② 인증범위는 신청기관이 제공하는 정보통신서비스를 기준으로 해당 서비스에 포함되거나 관련 있는 자산(시스템, 설비, 시설 등), 조직 등을 포함하여야 한다.
③ ISMS 의무인증범위 내에 있는 서비스, 자산, 조직(인력)을 보호하기 위한 보안시스템은 포함 대상에서 제외해도 된다.
④ 해당 서비스의 직접적인 운영 및 관리를 위한 백오피스 시스템은 인증범위에 포함되며, 해당 서비스와 관련이 없더라도 그 서비스의 핵심정보자산에 접근 가능하다면 포함하여야 한다.

98. 다음 지문이 설명하는 인증제도는?

현재 사용되는 IT 보안제품에 대해 보안성을 평가하는 제도로 제품유형별 PP(Prolection Profile)를 정의하고, 8개 군의 평가항 목을 대상으로 평가가 이루어진다. 평가결과는 IT 보안제품의 보안위협 및 자산가치의 정도에 따라 EAL1(Evaluation Assurance Level 1) - EAL7(Evaluation Assurance Level 7) 까지 7단계로 부여하여 인증서가 제공된다.

① ISO 27001 ② ITSEC
③ CC(Common Criteria) ④ ISMS

99. 다음의 지문이 설명하는 정보보호 용어는?

이것은 각종 재해나 재난의 발생을 대비하기 위하여 핵심 시스템의 가용성과 신뢰성을 회복하고 사업의 지속성을 유지하기 위한 일련의 계획과 절차를 말한다. 이것은 단순한 데이터의 복구나 신뢰도를 유지하는 것 뿐 아니라 나아가 기업의 전체적인 신뢰성 유지와 가치를 최대화하는 방법과 절차이다.

① 재난 예방 계획 ② 업무연속성 계획
③ 기업 안정성 확보 계획 ④ 시스템 운영 계획

100. 개인정보처리자는 다음 지문의 사항이 포함된 것을 정하고 이를 정보주체가 쉽게 확인할 수 있게 공개하도록 되어 있다. 다음 지문의 사항이 포함된 문서의 법률적 명칭은 무엇인가?

1. 개인정보의 처리 목적
2. 개인정보의 리 및 보유 기간
3. 개인정보의 제3자의 제공에 관한 사항(해당도는 경우에만 정한다.)
4. 개인정보처리의 위탁에 관한 사항해당도는 경우에만 정한다.)
5. 정보주체의 권리의무 및 그 행사방법에 관한 사항
6. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

① 개인정보 보호정책 ② 표준 개인정보 보호지침
③ 개인정보 보호지침 ④ 개인정보 처리방침

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