정보보호전문가(SIS) 2급 필기 샘플문제

과 목	시 스 템 보 안	시 험 시 간	4 0 분

1. 윈도우(Windows) NT를 설치하였을 때 기본적으로 생성되는 보안 그룹에 해당되지 않는 항목은 어떤 것인가? (3)
   ① 관리자(Administrator) 그룹
   ② 백업 오퍼레이터(Backup Operators) 그룹
   ③ 루트(Root) 그룹
   ④ 복제(Replicator) 그룹
   ⑤ 사용자(Users) 그룹

2. 프로세스 동기화를 위해 사용되는 모니터(monitor) 내에서 사용되는 연산으로 이루어진 것은? (1)
   ① wait-signal
   ② read-write
   ③ test-set
   ④ compare
   ⑤ enable-disable

3. 다단계 피드백 큐 스케쥴링(multilevel feedback queue scheduling) 기법을 이용할 때, 실행시간이 긴 프로세스 혹은 백그라운드 작업들은 시간이 흐를수록 더 낮은 순위를 지니게 되어 마지막에는 가장 낮은 우선 순위의 큐에 도달하여 수행되게 된다. 이 마지막 큐에서 이용되는 스케쥴링 방식은? (2)
   ① RR
   ② FCFS
   ③ SJF
   ④ priority
   ⑤ EDF

4.메모리의 내부 단편화(internal fragmentation) 문제를 해결할 수 있는 방법은? (1)
   ① 세그멘테이션
   ② 스레싱(thrashing)
   ③ 페이징
   ④ 스와핑
   ⑤ preemption

5. 다음 중 교착상태(deadlock)의 필요조건(necessary condition)이 아닌 것은? (4)
   ① 상호배제(mutual exclusion)
   ② 환형대기(circular wait)
   ③ 비선점(nonpreemption)
   ④ 임계구역(critical section)
   ⑤ 점유 및 대기(Hold-and-wait)

6. 윈도우(Windows) 2000에서 TCP/IP 설정시 사용 가능한 호스트 IP는 어느 것인가? (2)
   ① 10.0.0.0
   ② 210.112.129.10
   ③ 155.21.255.255
   ④ 255.255.255.0
   ⑤ 203.258.11.8

7. 유닉스(UNIX) 운영체제의 디렉토리(directory)에 포함되지 않는 정보는 어느 것인가? (1)
   ① 파일의 사용자
   ② 파일의 현재위치
   ③ 파일의 이름
   ④ 파일의 보호
   ⑤ 파일의 크기

8. SSTF(Shortest Seek Time First) 방식으로 운영되는 디스크 스케줄링에서, 현재 디스크 헤더가 60 트랙에 있으며, 자료 접근을 위한 트랙 요청 큐의 내용이 (14, 230, 100, 50, 65)을 담고 있다고 가정할 때, 다음에 디스크 헤더가 움직일 트랙의 번호는? (2)
   ① 50
   ② 65
   ③ 14
   ④ 230
   ⑤ 100

9. 운영 체제의 일괄 처리 방법 중 버퍼링(buffering)과 스풀링(Spooling)이라는 것이 있다. 다음중 버퍼링과 스풀링에 대한 설명의 틀린 것은? (3)
   ① 버퍼링과 스풀링 모두 CPU 연산과 병행하여 수행된다.
   ② 버퍼링은 메모리에 대하여, 스풀링은 디스크에 대하여 행해지는 작업이다.
   ③ 버퍼링은 스풀링보다 많은 입출력 작업을 중첩시킬 수 있다.
   ④ 버퍼링과 스풀링 모두 입출력 작업을 효율적으로 운영하기 위하여 고안되었다.
   ⑤ 버퍼링과 스풀링은 CPU의 처리 속도와 입출력 장치의 속도 차이를 보완한다.

10. 다중처리(Multi-processing) 운영체제를 바르게 설명한 것은? (1)

① 2개 이상의 처리기로 구성된 시스템들을 통합적으로 제어 및 관리하는 운영체제
② 2개 이상의 처리기로 구성된 시스템에서 파일 분산처리만을 종합적으로 제어 및 관리하는 운영체제
③ 다중 사용자를 지원하는 시스템에 클라이언트가 네트워크를 통해 접속할 수 있도록 환경을 제공하는 모든 운영체제
④ 각 처리기(processor)간의 프로세스나 자료를 고립 시켜 네트워크 부하를 줄이는 방식의 운영체제
⑤ 한 순간에 하나의 프로세스만을 수행하는 운영체제

11. 다음 중 페이징 기법에 대한 설명 중 옳지 않은 것은 무엇인가? (1)

① 페이징 기법을 사용함으로써 내부 단편화 현상이 제거되어 주기억장치의 효율을 높일수 있다.
② 사용자의 논리적 주소 공간과 컴퓨터 시스템의 물리적 기억장소가 같은 크기의 단위로 나뉘어 지며 사용자 프로그램은 페이지 단위로 임의의 빈 페이지에 적재 된다.
③ 페이징 기법을 사용하면 주 기억 장치에 오버헤드가 크며, 페이지 사상표를 보관할 장소가 요구된다.
④ 페이징 시스템의 논리적 주소는 순서쌍(p,d)로 표현되며, 여기에서 p는 논리적 주소 공간 내에서 참조될 항목이 있는 페이지 번호이며, d는 p내에서 참조될 항목이 위치하고 있는 곳까지의 변위이다.
⑤ 할당된 마지막 페이지 내에는 낭비되는 기억공간이 있을 수 있다.

12. 윈도우 NT/2000 시스템에 패스워드 설정 시 고려해야 할 사항이 아닌 것은? (4)

① 주기적인 변경을 통해 패스워드를 관리한다.
② 알려진 단어나 사용자 이름은 피하도록 권고한다.
③ 반드시 7자리 안에 특수문자나 숫자를 포함하도록 한다.
④ 최소 암호길이는 8자리나 16자리를 지킨다.
⑤ 최대 암호 사용기간과 최소 암호 사용기간을 설정한다.

13. 윈도우에서 악성 프로그램이 사용하는 자동 실행 설정 방법이 아닌 것은? (4)

① 자동 시작 폴더를 이용하는 방법
② Bat 파일을 이용하는 방법
③ 특정 응용프로그램의 설정을 이용하는 방법
④ 바탕화면에 숨김 파일로 두는 방법
⑤ System.ini 파일을 이용하는 방법

14. 다음 설명 중 백업(back up)과 복구에 대한 설명으로 옳지 않은 것은? (5)

① 백업은 크게 Full 백업과 Incremental 백업으로 나뉜다.

② 백업 명령 중 tar는 디렉토리 계층을 이용한 백업에 적합한 명령으로, 가장 쉽게 서브 디렉토리를 백업할 수 있다.

③ Cpio 명령은 데이터를 테이프에 백업할 때 tar보다 더 효율적으로 백업할수 있다.

④ Dump 명령은 이전에 화일시스템을 백업한 이후에 변경된 화일들의 목록을 작성하여, 그 목록에 있는 화일들을 새로운 백업 화일로 백업받을 수 있는 점진적인 백업 기능을 제공한다. 또한 어떤 파일이 백업되어야 하는가를 알기 위해 파일시스템의 inode 테이블을 참조한다.

⑤ Dump 명령은 파일 시스템과 관계 없이 여러 개의 파티션 안의 데이터를 한번에 백업할 수 있다.

15. 윈도우 보안 관련 소프트웨어에 대한 다음 설명으로 맞는 것은? (1)

<보기>

영국에서 만든 보안 스캐너로 WWW, SQL, FTP, SMTP, POP3, DNS 등 12개의 점검 모듈로 구성되어 있으며, 세부적으로 300 여 개의 항목을 점검하는 도구이다

① CIS

② IIS Security Planning Tool

③ Windows 2000 IIS 5.0 Hotfix Checking Tool

④ Windows 2000 systemwide policy

⑤ L0pht crack

16. 윈도우 공유폴더에 대한 설명으로 틀린 것은? (2)

① Legion 도구를 이용해 공유폴더를 찾아 낼 수 있다.

② Lophtcrack을 통해 공유폴더를 크랙 할 수 있다.

③ 윈도우에는 관리를 위해 공유폴더가 설치되어 있다.

④ pqwak이라는 도구를 통해 공유폴더를 크랙 할 수 있다.

⑤ 윈도우98 공유폴더 암호 인증 방식은 한자 한자씩 판단 할 수 있다.

17. 백신 프로그램에 대한 설명 중 틀린 것은? (2)

① 네트워크를 통해 백신프로그램의 지속적인 업데이트가 가능하다.

② CIH바이러스를 통해 부팅이 되지 않을 시에 백신프로그램을 통해 복구가 가능하다.

③ 백신프로그램은 크게 진단용, 치료용, 예방용으로 나눌 수 있다.

④ 국내에는 안철수 연구소와 하우리에서 백신프로그램을 제작한다.

⑤ 컴퓨터 바이러스의 치료와 예방을 하기 위한 프로그램이다.

18. 웹의 기본 구조는 수많은 사용자에게 정보를 제공해주는데 그 목적이 있다. 이러한 목적을 위해 쿠키(cookie)라는 기법을 통해 서비스를 제공한다. 쿠키의 다음 설명 중 틀린 것은? (4)

① 쿠키는 브라우저에서 관리되고 저장되는 값이고, 웹서버에서 활용한다.
② explorer에서는 windows 디렉토리에 cookie라는 디렉토리에 파일로 저장된다.
③ 웹서버와 브라우저간의 공유가 쿠키에 의해 가능해졌다.
④ 서버에 공유메모리 공간을 할당하고 이 주소를 이용한다.
⑤ 하나의 쿠키는 4k를 넘지는 못한다.

19.이메일 보안을 위해 PGP를 사용한다. 다음 PGP에 대한 설명 중 맞지 않는 것은? (1)

① PGP는 안전성을 인정받고 있는 대칭키 암호 기술 (Secret-Key cryptography)을 사용한다.
② RSA와 DSS/Diffie-Hellman 등 두 가지 형태의 키 생성이 가능하다.
③ 전자서명 기능을 제공하여 송신자라고 주장하는 사용자와 이메일을 실제로 보낸 송신자가 동일인인지 확인 가능하다.
④ 사용자가 작성한 이메일의 내용과 첨부되는 파일을 암호화하여 이메일 수신자만이 그 내용을 볼 수 있도록 하는 기밀성을 제공한다.
⑤ 이메일 어플리케이션과 PGP를 연계하여 사용할 수 있도록 plug-in 지원한다.

20. 다음은 웹메일을 공격하는 해커의 스크린 모습이다. 다음 설명 중 틀린 것은? (5)

<보기>

```
[root@forensic root]# telnet www.your_domain.com 80
Trying 192.168.0.1...
Connected to www.your_domain.com.
Escape character is '^]'.
GET http://www.your_domain.com/user_info.html HTTP/1.0
cookie:id=webadmin

HTTP/1.1 200 OK
.....
어서 오세요. 이 화면은 쿠키 인증을 통과한 사람만 볼 수 있는 화면입니다.
Connection closed by foreign host.
```

① Telnet을 이용해 웹서비스에 접속한 형태이다.
② GET 메소드를 통해 webadmin의 user_info 웹페이지를 요청했다.
③ cookie값을 id만으로 인증했다.
④ 해커는 다른 아이디로의 접근이 가능하다.
⑤ http프로토콜의 헤더값을 해커가 설정하여 보낼 수 없다.

21. 다음 SSL에 대한 설명 중 틀린 것은? (4)

① SSL은 Netscape사에서 처음으로 제안했다.

② SSL은 SSL Handshake Protocol, SSL change Cipher Spec, SSL Alert Protocol 부분과 실질적인 보안 서비스를 제공하는 SSL Record Protocol 부분으로 나누어져 있다.

③ SSL은 상호인증과 무결성을 위한 메시지 코드, 기밀성을 위한 암호화 방법을 제공한다.

④ 실제 SSL Record Protocol부분은 TCP 계층하단에서 동작한다.

⑤ SSL에서는 전자서명과 키 교환을 위해 RSA 또는 DH 알고리즘을 이용할 수 있다.

22.다음 중 Inflex 보안 도구에 대한 설명이 틀린 것은? (3)

① 임의 파일 유형과 파일이름에 대하여 검색하고 필터링 하는 기능을 제공한다.

② 메일서버에서 로컬이나 외부로 나가는 e-mail을 검사하는 in-outbound 정책을 세울 수 있게 도와주는 도구이다.

③ 메일을 통해 첨부된 파일에 대한 바이러스를 치료하고 복구하는 기능을 제공한다.

④ Sendmail.cf 대신에 inflex.cf에 설정파일을 사용하도록 한다.

⑤ 룰셋에 차단된 메시지는 조치를 취하고 통과된 메일은 다시 sendmail.cf가 적용되어 메일이 처리된다.

23. 다음 nmap 포트 스캐너의 명령어와 결과에 대한 설명으로 틀린 것은? (2)

<보기>

```
[root@forensic run]# nmap -sS -O 192.168.0.1
Port        State        Service
21/tcp      open          ftp
22/tcp      open          ssh
23/tcp       filtered      telnet
6000/tcp    open          X11
Remote operating system guess: Linux Kernel 2.4.0 - 2.4.17 (X86)
Uptime 4.292 days (since Tue Apr  1 23:51:22 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

① O옵션은 OS판별을 위해 붙이는 옵션이다.

② 1-65535 까지 열려진 포트를 검색해서 나온 출력 값이다.

③ 23번 포트는 192.168.0.1에서 자체 방화벽을 통해 포트를 막았거나 nmap에서 정확한 판별을 하지 못한 경우이다.

④ 192.168.0.1의 호스트는 리눅스 시스템이며 현재 스캔 결과 열려진 포트는 3개이다.

⑤ sS옵션은 half-open 스캐닝의 방법으로서 완전한 tcp connection을 맺지 않는 스캐닝 방법이다.

24. 특정 웹사이트를 무차별 공격하는 기법을 통해 계정과 패스워드를 크랙하는 도구는 무엇인가? (4)
    ① John the ripper
    ② Crack
    ③ Nmap
    ④ wwwHack
    ⑤ nessus

25. 보안 시스템들의 필터링을 피하기 위해 스캔 기법에서는 stealth기법을 쓴다. 다음 포트스캔의 기법 중 stealth 기법에 속하지 않는 것은? (4)
    ① Fin flag 기법
    ② Tcp fragment 기법
    ③ Ack flag 기법
    ④ Syn flag 기법
    ⑤ xmas 기법

26. 보안 도구를 우회하기 위한 방법으로 TCP 헤더의 ACK, FIN, RST, SYN, URG, PSH 플래그를 모두 설정하여 스캔하는 기법은 무엇인가? (3)
    ① Tcp Connect 기법
    ② Reverse Ident 기법
    ③ XMAS flag 기법
    ④ Tcp sweep 기법
    ⑤ Null flag 기법

27. 다음은 Windows 2000 서버에서 외부의 공격에 대응할 수 있도록 보안 기능을 강화 시키는 기능 및 도구를 나열한 것이다. 이중 잘못된 것을 고르시오. (1)
    ① SNMP
    ② 커버로스
    ③ EFS(Encrypted File System)
    ④ IPSEC
    ⑤ ACL(Access Control List)

28. 다음 해킹 도구 중 사용자의 key stroke를 훔치는 도구는? (1)
    ① Passpy
    ② Voob
    ③ Satan
    ④ Nuke
    ⑤ Goldeneye

29. 다음 접근제어에 대한 설명 중 잘못된 것은? (4)

① 강제적 접근제어는 시스템에 의해서 사용자가 파일에 접근 할 수 있는가를 결정하기 위해 사용되는 보안 속성을 보안 관리자에 의해 부여되거나, 운영체제에 의해 부여됨으로써 사용자의 신분권한에 관계없이 강제적으로 접근을 통제하는 방법이다.

② 역할기반 접근제어(Role Based Access Control)는 정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내에서 개인의 역할(직무)에 따라서 결정되도록 한 것으로 상업적인 분야에서의 접근제어 요구 사항에 적합한 접근제어 정책이다.

③ 임의적 접근제어는 사전에 보안 정책이나 보안 담당자 등에 의해 개별 사용자에게 합법적으로 부여된 한도 내의 재량권에 따라, 사용자가 그 재량권을 적용해 접근을 통제하는 접근제어 방식이다.

④ MAC(Mandatory Access Control)의 한 가지 방식인 ACL(Access Control List)은 객체에 포함된 정보의 비밀성과 주체가 갖는 권한에 근거해 객체에 대한 접근을 제한하는 강제적 접근제어 방법을 말한다.

⑤ 역할기반 접근제어의 구성을 살펴보면 기본적으로 사용자, 역할, 권한(or 퍼미션)부분이 있고 그 외에 역할계층(Role Hierarchy), 제약조건(Constraints), 세션(Sessions) 등의 구성요소로 이루어진다.

30. 백오리피스 2000의 특징이 아닌 것은? (2)

① 백오리피스 2000은 windows95/98/NT를 지원한다.

② Plug-in 기능은 지원하지 않는다.

③ XOR, 3DES를 지원한다.

④ Default 설정을 바꿀 수 있다.

⑤ GUI방식을 지원한다.

31. 커널에 의해 디스크에 압축된 상태로 저장되도록 파일의 속성을 변화시킬 때 알맞은 명령어는? (1)

① Chattr +c [filename]

② Chattr +a [filename]

③ Chattr +i [filename]

④ Chattr +u [filename]

⑤ Chattr +d [filename]

32. 메일 폭탄(mail bomb)에 대한 설명으로 틀린 것은? (5)

① 외부 사용자에게 relay기능을 제공하는 서버를 통해 발송되기도 한다.

② 상대방에게 수백, 수천 통의 메일을 한번에 보내는 것을 말한다.

③ 메일 폭탄 도구로는 aenima가 있다.

④ 메일 폭탄은 통신망과 시스템에 악영향을 끼친다.

⑤ [광고]라는 문구를 삽입하면 합법적인 메일이 된다..

33. 스파이웨어 프로그램에 대한 설명 중 틀린 것은? (2)
① 감시하다라는 spy와 소프트웨어가 합쳐져 spy+ ware가 되었다.
② 스파이웨어 프로그램은 백오리피스처럼 서버 클라이언트 구조로 되어있다.
③ 스파이웨어 프로그램은 내 컴퓨터의 정보를 해당 프로그램의 제작자에게 전송해 버린다.
④ 스파이웨어는 백도어나 바이러스처럼 피해는 없지만 잠재적인 사생활의 노출을 가져올 수 있다.
⑤ 스파이웨어를 제거하는 도구로 OptOut이라는 프로그램이 있다.

34. 다음 침입탐지 모델 중 나머지 넷과 다른 하나는? (3)
① 통계적인 방법
② 특징 추출
③ 조건부 확률
④ 신경망
⑤ 예측 가능한 패턴생성

35. /etc/fstab의 설정으로 파티션에 대한 속성의 변화를 줄 수 있다. 이에 대한 설명으로 틀린 것은? (1)
① default : 모든 속성에 대해 제한한다.
② noexec : 실행파일을 실행 할 수 없게 한다.
③ noquota : 사용자의 하드용량을 제어할 때 사용한다.
④ nosuid : SUID/SGID엑세스를 하지 못하게 한다.
⑤ nodev : 특별한 장치나 문자 디바이스를 액세스 하지 못하게 한다.

36. RAT를 구성하는 5가지 프로그램에 대한 설명 중 틀린 것은? (1)
① Snarf : 침입탐지시스템인 snort와 연계하는 plugin 프로그램
② Ncat : rule과 환경설정파일을 읽고 CSV 형태로 출력
③ ncat_report : CSV 형태의 파일을 읽고 HTML 형태로 출력
④ Rat : 실제 점검자가 구동하는 프로그램으로 다른 프로그램들을 실행시킴
⑤ ncat_config : 각 점검 라우터의 특성에 맞도록 rule을 구성

37. 유닉스에서의 파일시스템 설정 중 가장 적합한 것은? (4)
① /home /tmp 파티션은 사용자들을 위해 suid 옵션을 적용시킨다.
② NFS에서 가능한 파일시스템을 write-only로 export한다.
③ anonymous ftp를 구성할 때 ftp 보조 디렉토리인 etc, bin 은 ftp의 소유여야 한다.
④ 아파치 보안을 위해 실행 파일인 httpd는 오직 관리자인 root 만이 읽고 쓸 수 있도록 하고 실행은 소유자와 그룹 그리고 누구나(other) 할 수 있도록 한다.
⑤ sendmail 의 spam relay 기능을 설정할 때 access DB는 /etc/mail/sendmail.cf에 저장된다.

38. 다음 xinetd에 대한 설정으로 틀린 설명은? (2)

<보기>

```
[root@forensics xinetd.d]# cat telnet
service telnet
{
        disable = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}
```

① 현재 telnet 서비스는 동작 중에 있다.
② Wait 값이 no인 것으로 보아 single thread로 실행됨을 의미한다.
③ 소켓 형태는 스트림 기반의 서비스이다.
④ 해당 서비스를 실행 할 데몬 프로그램은 /usr/sbin/in.telnetd이다.
⑤ 포트를 변경하기 위해서는 port값을 추가시키면 된다.

39. 다음 파일들에 대한 설명 중 틀린 것은? (3)

<보기>

```
-rwsr-xr-x   1 root      student      8044 Apr  5 04:32 test
drwxrwxrwt   7 root      sys           507 Apr  5 03:30 tmp
drwxrw-r--   4 root      student      9728 Mar 20 12:27 bin
```

① “test”라는 파일의 퍼미션은 “chmod 4755 test”라는 명령어로 설정할 수 있다.
② “tmp”디렉토리에서 모든 사용자는 다른 사용자 권한의 파일을 실행할 수 있지만 지울 수는 없다.
③ student group에 속한 사용자들은 bin 디렉토리를 읽고 쓰는 권한이 있어 파일을 생성할 수 있다.
④ “test”를 실행하면 student는 test프로그램을 실행하는 동안 root의 권한을 가지게 된다.
⑤ “tmp” 디렉토리에 설정된 허가권 중에 ‘t’는 “sticky bit”가 설정된 부분이다.

40. 트로이 목마 프로그램에 대한 설명으로 올바른 것은? (5)

① 시스템의 정상적인 보호수단을 우회하기 위하여 사용하는 은닉 메커니즘
② 다른 프로그램을 감염시키지 않으면서도 자기 자신을 복제하여 통신망 등을 통해서 널리 퍼짐
③ 제작자가 의도적으로 사용자에게 피해를 주고자 만든 모든 악의의 목적을 가진 프로그램
④ 자기 자신을 복제할 수 있는 기능을 가지고 있으며 컴퓨터 프로그램이나 실행 가능한 부분을 변형시킴
⑤ 정상적인 기능을 하는 프로그램처럼 나타나지만 실제로는 불법적인 일을 수행하며 사용자가 모르는 다른 기능을 포함시킨 프로그램

정보보호전문가(SIS) 2급 필기 샘플문제

과 목	네 트 워 크 보 안	시 험 시 간	4 0 분

1. 다음의 DoS 공격중 통상적으로 시스템에서 허용된 65535 byte 보다 큰 IP 패킷을 발송하여 서비스 거부를 일으키는 형태의 공격은 무엇인가? (1)
   ① ping of death
   ② Jolt
   ③ Teardrop
   ④ Land attack
   ⑤ smurf

2. 패킷정보를 전송하기 위하여 사용되는 계층은? (3)
   ① Physical Layer
   ② Link Layer
   ③ Network Layer
   ④ Presentation Layer
   ⑤ Application Layer

3. 인터넷의 IP 데이터그램의 포맷에 규정된 필드가 아닌 것은? (3)
   ① 목적지 주소 필드
   ② 발신지 주소 필드
   ③ 목적지 도메인 이름 필드
   ④ 프로토콜 타입 필드
   ⑤ 수명 필드

4. 다음은 ICMP가 호스트 및 라우터에 의해 사용되는 보편적인 용도 중 몇 가지이다. ICMP 용도와 다른 것은? (1)
   ① 라우터는 다른 호스트나 라우터가 현재 도달 가능한지의 여부를 결정할 수는 없다.
   ② 라우터는 특정 목적지 네트워크로 후속 IP 데이터그램을 보내는데 사용할 수 있는 더 나은 경로가 있음을 근원지 호스트에 통지할 수 있다.
   ③ 라우터는 그들이 처리하기에는 너무 빠르게 IP 데이터 그램이 도착함을 다른 시스템에 통지할 수 있다.
   ④ 호스트들은 클럭을 동기화 하기 위해 사용되는 메시지를 서로 교환할 수 있다.
   ⑤ 호스트들은 네트워크, 또는 개개의 호스트를 식별하는 데 필요한 비트를 지시하는 특정 메시지를 교환할 수 있다.

5. 넷마스크(Netmask)에는 급이 나뉘어 있어서 각 급에 따라 확장할 수 있는 IP의 수가 제한되게 된다. 다음 중 B 클래스 IP Netmask는 어느 것인가? (3)
   ① 255.255.255.255
   ② 255.255.255.0
   ③ 255.255.0.0
   ④ 255.0.0.0
   ⑤ 0.0.0.0

6. 다음 SNMP에 의해 동작하는 네트워크 관리 구성 요소를 설명한 것으로 틀린 것은? (5)
   ① NMS(Network management Station)은 인터넷에서 네트워크 관리 응용을 수행하는 호스트이다.
   ② NMA(Network management Application)은 하나 이상의 네트워크 요소를 감시하고 제어하는 네트워크 관리 스테이션에서 실행되는 프로그램이다.
   ③ NE(Network Element)는 관리 객체를 포함하는 MIB의 일부와 관리 에이젼트를 유지하는 인터넷상의 구성요소이다.
   ④ MA(Management Agent)는 네트워크 관리 응용에 의해 요청된 네트워크 관리 기능을 수행할 책임이 있는 네트워크 요소에서 실행되는 프로그램이다.
   ⑤ MC(Management Control) 네트워크 관리 응용에 의해 요청된 네트워크 통제 기능을 수행할 책임이 있는 네트워크 요소에서 실행되는 프로그램이다.

7. 사내에 LAN을 구축하고 인터넷 전용선과 연결하는 사내의 LAN을 구축 할 때 필요한 장비가 아닌 것은? (1)
   ① 리피터(Repeater)
   ② 라우터(Router)
   ③ DSU/CSU
   ④ 허브(Hub)
   ⑤ 이더넷 카드

8. 클라이언트와 서버에 관한 설명으로 옳지 않는 것은? (4)
   ① 서비스 요청을 보내는 응용요소를 클라이언트라고 한다.
   ② 클라이언트는 로컬 호스트에서 실행되는 요소와 원격 호스트에서 실행되는 서버요소 간의 통신 채널을 열어 통신을 시작한다.
   ③ 서버는 채널을 열 때 어떠한 통신 행위도 하지 않는다.
   ④ Interactive server는 한 순간에 여러 클라이언트의 요청을 처리할 수 있다.
   ⑤ 서버가 각 요청을 만족시키는데 요구되는 시간을 미리 알지 못할 경우 concurrent server를 사용한다.

9. 다음 설명 중 틀린 것은? (5)
   ① LAN을 구성하는 장비에는 랜 카드, 허브, 스위치, 브리지, 라우터 등이 있다.
   ② NIC(Network Interface Card)는 PC를 LAN에 연결시키는 장비이다.
   ③ NIC는 전세계에서 유일한 MAC 주소를 사용하며, OSI 2계층의 기능을 수행한다.
   ④ NIC를 선택할 때는 네트워크 구조, NetBIOS, 전송매체, 전송 속도, 토폴로지 등을 고려해야 한다.
   ⑤ 일반적으로 LAN에서 사용되는 UTP 케이블은 신호감쇄를 개선하여 500m 이상 연결이 가능하다.

10. 다음 Traceroute 프로그램에 대한 설명으로 틀린 것은? (3)
   ① Traceroute 프로그램은 패킷이 목적지에 도달하는 경로를 추적하는 프로그램이다.
   ② Traceroute 프로그램은 자신의 컴퓨터가 인터넷을 통해 목적지를 찾아가면서 거치는 게이트웨이 컴퓨터를 기록한다.
   ③ Traceroute 프로그램은 UDP와 TCP 헤더의 TTL 필드를 이용한다.
   ④ Traceroute 프로그램은 인터넷 상에 문제가 있는 네트워크를 파악하는데 편리하다.
   ⑤ Traceroute 프로그램은 각 홉에 걸리는 시간의 합을 표시해 준다.

11. 다음 중 인터넷 전용회선을 설치할 때 반드시 필요한 장비로만 짝지어진 것은? (3)
   ① LAN card - Router - IP - Switch - CSU
   ② MODEM - DSU - Router - Hub
   ③ LAN card - Hub - Router - DSU
   ④ MODEM - Hub - Router - CSU
   ⑤ LAN card - CSU - DSU - Router

12. 네트워크 상에서 드라이브나 폴더 공유 시 각 장치의 등록 정보에서 설정할 수 있는 내용이 아닌 것은? (4)
   ① 읽기 전용, 읽기/쓰기에 대한 사용권한 설정
   ② 네트워크 상에서 검색할 때 공유할 자원의 공유 이름에 대한 설정
   ③ 암호에 대한 사용 권한 설정
   ④ 특정 문자열을 이름으로 사용한 장치에 대한 찾기 기능의 설정
   ⑤ 자원에 대한 접근 권한을 암호로 대체할 수 있다.

13. Ping 연결성 시험에 대한 설명으로 틀린 것은? (3)
   ① Ping은 응용 계층 서비스로 인터넷 호스트간의 연결 여부를 검사하는데 사용된다.
   ② Ping 명령어를 사용할 때 호스트의 이름이나 인터넷 주소와 함께 사용한다.
   ③ Ping은 도달 가능한 호스트와의 왕복 전파지연 시간에 대한 평균값만을 알려준다.
   ④ Ping 명령은 ICMP의 Echo Request 메시지를 보낸 이후로 경과한 시간을 계산한다.
   ⑤ Ping 명령은 Packet InterNet Groper의 약자이다.

14. 다음 라우터(router)에 대한 설명으로 옳지 않는 것은? (5)
① 라우터는 OSI 3계층의 기능을 수행하는 네트워크 장비이다.
② 라우터는 LAN을 WAN에 접속시킬 때 뿐만 아니라 패킷의 경로를 결정하는 인터넷 백본망의 핵심 장비이다.
③ 라우터의 핵심기능은 패킷의 최적 경로를 설정하는 것이다.
④ 일반적으로 라우터는 외부망에서 내부망으로의 접근 시작점으로 방화벽의 기본적인 기능을 탑재하는 경우가 있다.
⑤ 라우터는 브로드캐스팅 신호에 대해서는 차단할 수 없다.

15. 무선인터넷 서비스의 방식과 특징에 대한 설명으로 옳지 않는 것은? (4)
① WAP 방식은 무선망과 유선 인터넷의 연동을 위해서 WAP 게이트웨이를 두고 있다.
② 무선 컨텐츠 업체는 WML(Wireless Markup Language)로 WAP 서비스를 구현해야 한다.
③ MS가 제공하고 있는 ME(Mobile Explorer)는 WAP 게이트웨이 기능을 무선 단말기 내의 브라우저가 한다.
④ MS는 기존의 HTTP와 호환성이 떨어져 사용을 기피하고 있다.
⑤ 무선인터넷 환경은 위치 기반 정보 서비스로 확장될 전망이다.

16. 다음 Finger 프로토콜에 대한 설명으로 틀린 것은? (5)
① Finger 프로토콜은 특정 호스트상의 사용자에 관한 정보를 제공한다.
② Finger 프로토콜은 그 시스템의 최종 로그아웃 시간, ID가 무엇인지를 알 수 있게 한다.
③ Finger 프로토콜은 개인정보 유출의 우려가 있어 사용에 신중을 기해야 한다.
④ 프로토콜 관점에서 Finger 서버는 79번 포트를 사용한다.
⑤ 서버와 클라이언트간의 질문과 답변에 사용되는 문자 코드는 EBCDIC 코드이다.

17. 다음은 tcpdump 프로그램에 대한 내용이다. 맞지 않는 것은? (5)
① Tcpdump 프로그램은 NIC를 무차별 모드(promiscuous)로 설정해서 동작한다.
② Tcpdump 프로그램을 사용할 경우 회선상에 흐르는 모든 패킷을 받을 수 있다.
③ Tcpdump 4.4BSD, BSD/386, SunOS, Ultrix, Hp-UX와 같은 UNIX 시스템에서 지원된다.
④ BSD 방식의 커널은 tcpdump를 사용하기 위해 BPF(BSD Packet Filter)를 제공한다.
⑤ Tcpdump 프로그램 변형으로 솔라리스에서는 iptrace를 제공한다.

18. RIP(Routing Information Protocol)에 대한 설명으로 틀린 것은? (4)
① RIP는 홉 수가 15이상인 네트워크에서는 사용할 수 없다.
② RIP는 거리 단위를 홉 수로 제한하고 있으므로 빠른 경로 선택이 어렵다.
③ 라우팅 정보가 30초마다 교환되므로 장애시 복구에 많은 시간이 소요된다.
④ 작은 규모의 네트워크에 적용하므로 네트워크 변화를 즉시 라우팅 경로에 반영할 수 있다.
⑤ RIP는 요청과 응답 2가지 종류의 메시지로 구성된 단순 구조를 갖는다.

19. IPv6의 주소 체계와 특징에 대한 설명으로 틀린 것은? (5)
① 128비트 주소체계로 구성된다.
② 고속과 저속 망 모두에서 효율적인 동작을 할 수 있다.
③ 실시간으로 멀티미디어 데이터를 처리할 수 있다.
④ 16비트씩 8개 부분으로 나누어 각 부분을 콜론(:)으로 구분한다.
⑤ IPv4와 같이 10진수 체계를 이용해서 표기한다.

20. 다음 중 네트워크 관리 프로토콜과 가장 거리가 먼 것은? (4)
① HEMS(HighLevel Entity management System)
② SGMP(Simple Gateway Monitoring Protocol)
③ CMISE/CMIP(Common Management Information Service Element/Protocol)
④ ARP(Address resolution Protocol)
⑤ SNMP(Simple Network Management Protocol)

21. 다음 공격 형태 중 특성이 다른 하나는 무엇인지 골라라. (3)
① Trinoo
② Tribe Flood Network
③ TearDrop
④ Stacheldraht
⑤ Shaft

22. 네트워크 기반의 분산서비스거부공격(DDoS) 을 예방하고 차단하기 위한 방법중 틀린 것은 무엇인가? (3)

① 사용하지 않은 포트는 라우터 등에서 필터링한다.
② IP directed broadcasts 기능을 사용하도록 한다.
③ RFC 1918 에 정의된 사설IP 를 소스로 한 패켓을 필터링 한다.
④ 별도의 IDS나 Firewall 장비를 도입한다.
⑤ 일종의 QoS인 rate-limit를 이용해 유입되는 트래픽을 제한한다.

23. hunt 나 dsniff 와 같은 프로그램을 이용하면 스위치 환경에서도 다양한 방법을 이용하여 스니핑(sniffing) 공격이 가능하다. 다음 보기 중 이러한 공격과 직접적으로 거리가 먼 것은 무엇인가? (3)

① Switch Jam(MAC Flooding)
② ARP Redirect
③ ARP Cache
④ ARP Spoofing
⑤ MAC Duplicating

24. 아래의 결과를 보았을 때 이 네트워크는 어떠한 공격에 취약하다고 추측할 수 있는가?(2)
<보기>

```
# ping 202.102.233.255
PING 202.102.233.255 (202.102.233.255) from 211.13.2.1 : 56(84) bytes of data.
64 bytes from 202.102.233.207: icmp_seq=0 ttl=126 time=3345.4 ms
64 bytes from 202.102.233.194: icmp_seq=0 ttl=126 time=3542.7 ms (DUP!)
64 bytes from 202.102.233.193: icmp_seq=0 ttl=126 time=3738.8 ms (DUP!)
64 bytes from 202.102.233.214: icmp_seq=0 ttl=126 time=4053.1 ms (DUP!)
64 bytes from 202.102.233.207: icmp_seq=1 ttl=126 time=3316.3 ms
64 bytes from 202.102.233.194: icmp_seq=1 ttl=126 time=3541.0 ms (DUP!)
```

① land attack
② smurf attack
③ syn flooding attack
④ ping of death attack
⑤ winnuke attack

25. 각종 스캔 프로그램에는 원격지 시스템의 OS 나 OS 버전 정보를 알기 위해 OS fingerprinting 을 scan할 수 있는 기능을 제공하고 있다. 따라서 일부 서버에서는 패치 등을 통해 이러한 OS 스캔 결과를 위조할 수 있는데, 다음 중 OS fingerprint 결과를 위조하여 얻을 수 있는 효과는 무엇인가? (1)

① OS 정보를 위조할 경우 공격자를 혼란스럽게 함으로써 공격시간을 지연시킬 수 있다.
② OS 정보를 위조할 경우 열린포트수 등의 포트스캔 결과를 위조할 수 있다.
③ OS 정보를 위조할 경우 exploit 코드의 실행자체를 차단할 수 있다.
④ OS 정보를 위조할 경우 자동화된 스캔 프로그램의 스캔속도를 느리게 할 수 있다.
⑤ (1),(2),(3),(4) 모두 정답이다.

26. 다음중 대표적인 스캔 프로그램인 nmap 이 제공하거나 스캔할 수 있는 기능이 아닌 것은? (2)

① 시스템의 OS 버전정보
② 시스템에 설치되어 있는 응용 프로그램의 버전정보
③ open되어 있는 포트가 어떤 사용자의 권한으로 실행중인지 검사
④ 열려있는 포트가 tcp/udp 인지 여부에 대한 정보
⑤ 네트워크의 어느 호스트가 살아있는지에 대한 정보

27. 다음은 어떠한 형태의 공격에 대한 대비 또는 대응방법인가? (3)

<보기>

1. 시스템의 백로그큐 크기를 늘려준다.
2. 리눅스계열의 경우 syncookies 기능을 이용하고
   Windows 계열의 경우 레지스트리를 변경한다.
3. 라우터에서는 방어 솔루션인 tcp intercept를 설정한다

① land attack
② smurf attack
③ syn flooding attack
④ ping of death attack
⑤ winnuke attack

28. 아래는 특정 웹서버의 로그파일이다. 아래의 로그파일을 근거로 유추할 수 있는 것은?(2)

<보기>

```
alzza.test.com - - [28/Aug/2002:23:21:32 +0900] "GET /cgi-bin/phf" 200 1262
alzza.test.com - - [28/Aug/2002:23:21:32 +0900] "GET /cgi-bin/test-cgi" 200 420
alzza.test.com - - [28/Aug/2002:23:21:32 +0900] "GET /cgi-bin/handler" 404 -
alzza.test.com - - [28/Aug/2002:23:28:55 +0900] "GET /cgi-bin/phf" 200 1262
alzza.test.com - - [28/Aug/2002:23:28:55 +0900] "GET /cgi-bin/test-cgi" 200 420
alzza.test.com - - [28/Aug/2002:23:28:55 +0900] "GET /cgi-bin/handler" 404 -
```

① alzza.test.com 에서 서비스거부(Dos) 공격을 시도하였다.
② alzza.test.com 에서 mscan 과 같은 스캔 프로그램을 이용하여 cgi 프로그램의 존재유무를 스캐닝하였다.
③ 공격자는 공격에 성공하여 서버의 접근권한을 획득하였다.
④ 공격자가 스캔한 파일은 모두 서버에 존재하고 있었다.
⑤ 공격자는 자신의 소스IP 를 위조하여 스캔하였다.

29. hijacking 공격에 대한 탐지 방법은 몇 가지가 있다. 다음중 hijacking 공격에 대한 탐지 방법과 거리가 먼 것은? (1)

① Covert Channel 탐지
② desynchronized 상태 탐지
③ Ack storm 탐지
④ 특정 세션에서 패킷 유실 및 재전송 증가 탐지
⑤ 기대치 않은 접속 리셋

30. 다음 중 udp 스캔의 특징에 대해 잘못 설명한 것은 무엇인가? (4)

① 라우터에서 udp 패킷이 drop 될 수 있다.
② 많은 올바른 udp 서비스에서 제대로 응답을 하지 않는다.
③ 대부분의 방화벽에서는 udp 패킷을 drop 하도록 되어 있다.
④ udp 스캔의 결과는 매우 신뢰할 만 하다.
⑤ icmp port unreachable 메시지로 살아있지 않은 udp 포트의 응답에 의존한다.

31. 단편화(Fragment) 와 관련하여 아래 패킷을 보면 (DF) 라는 bit 가 설정 되어 있는 것을 알 수 있는데, DF 의 의미와 관련하여 바르게 설정한 것은 무엇인가? (4)

<보기>

```
192.168.1.4.45080 > 10.10.10.3.www: P 1:146(145) ack 1 win 5840 (DF)
```

① DF 가 설정된 것으로 보아 Dos 공격을 시도하는 패킷임을 추측할 수 있다.
② DF 가 설정된 것으로 보아 방화벽이나 IDS를 우회하려는 시도임을 추측할 수 있다.
③ DF 는 Do Fragment 의 의미로 라우터에서 단편화를 하여야 할 경우 별도의 추가적인 변화없이 단편화를 하라는 의미이다.
④ DF 는 Do not Fragment 의 의미로 단편화를 하지 말라는 의미로 라우터에서 단편화를 하여야 할 경우 이 비트가 설정되어 있는 파일은 패킷을 drop 하게 된다.
⑤ DF 가 설정된 것으로 보아 백도어를 스캔하는 것임을 추측할 수 있다.

32. 다음은 내부 네트워크의 130.100.1.1 에서 외부 인터넷으로 tcp 접근은 가능하지만 외부 인터넷에서 내부 네트워크로 접근하는 것은 차단하려고 할 경우 다음과 같이 설정할 수 있다. 이때 ( ) 에 설정되어야 할 명령어는 무엇인가? (5)

<보기>

```
Router(config)# access-list 100 permit tcp any host 130.100.1.1 (  )
Router(config)# int serial 0
Router(config-if)# ip access-group 100 in
```

① permitted
② allowed
③ connected
④ received
⑤ established

33.단편화된(fragmented) 패킷이 해당하는 목적지까지 전송된 후 정상적으로 재조합(reassembled) 되기 위해서는 몇 가지 단편화 규칙을 따라야 하는데, 다음 중 옳지 않은 설명은 무엇인가? (3)

① 단편화된 패킷끼리는 동일한 fragment id 를 공유하여야 한다.
② 각각의 단편화된 패킷은 단편화되기 이전 패킷에서의 위치를 알기 위해 offset 번호를 지정하여야 한다.
③ 각각의 단편화된 패킷은 단편화되기 이전 패킷에서의 순서를 알기 위해 순서번호를 지정하여야 한다.
④ 각각의 단편은 단편화된 패킷의 사이즈를 지정하여야 한다.
⑤ 자신의 단편이 마지막 단편인지 아니면 추가적인 단편이 있는지 여부를 지정하여야 한다.

34. 라우터에서 제공하는 보안 명령어중 하나인 "service password-encryption" 를 실행하면 라우터의 config 파일에 저장되어 있는 항목 중 plain text 부분을 일부 암호화 시켜준다. 다음 보기 중 "service password-encryption" 실행 시 암호화되는 부분은 무엇인가? (2)

① login username
② enable password
③ snmp community string
④ enable secret
⑤ (1),(2),(3),(4) 모두

35. 다음은 방화벽(firewall)의 어떤 특성에 대한 설명인가? (2)
<보기>

1. 단순 패킷 필터링에서 진일보한 방식
2. 패킷의 현 상태를 파악하여 해킹에 가까운 패킷인지 아닌지를 능동적으로 판단.
3. 동적으로 포트가 변동되는 FTP같은 서비스도 인식.
4. 패킷의 송수신 상황을 실시간으로 메모리에 기억하여 기존의 접속을 가장하고 들어오는 고급화되고 지능화된 공격을 차단.

① Network Address Translation
② stateful inspection
③ Transparent & Threaded Proxy
④ URL Filtering
⑤ High Availability

36. 다음 중 라우터를 안전하게 운영하는 방안에 대해 옳지 않은 것은 무엇인가? (2)
① 사용하지 않는다면 SNMP 을 disable 한다.
② CDP (Cisco Discovery Protocol) 기능을 작동하도록 하여 네트워크를 관리한다.
③ console에서만 접근할 경우 telnet으로 접근할 수 없도록 telnet listener 자체를 다운시킨다.
④ 로그를 남기도록 설정하여 로그를 관리한다.
⑤ 로그인 배너를 남기도록 설정하여 접근 시도시 경고 메시지를 보이도록 설정한다.

37. 다음은 사무실 등에서 특정 기능과 관련된 프로그램을 차단하기 위한 설정이다. 아래 설정은 어떤 기능을 차단하기 위한 것인지 다음 보기 중 하나를 골라라. (4)
<보기>

```
(config)#access-list 101 deny tcp any any range 137 139
(config)#access-list 101 deny udp any any range 137 139
(config)#access-list 101 deny tcp any any eq 445
(config)#access-list 101 permit ip any any
(config)#interface serial0
(config-if)#ip access-group 101 in
```

① 백오리피스 프로그램 차단
② 메신저 프로그램 차단
③ X-Windows 프로그램 차단
④ Windows 공유 차단
⑤ 프록시 프로그램 차단

38. 다음은 사설IP 대역인 192.168.0.0 /16 을 소스로 한 패킷을 필터링 하려고 한다.
( ) 에 들어갈 적당한 mask 를 지정하라. (4)
<보기>

```
Router(config)# access-list 101 deny ip 192.168.0.0 (        ) any
Router(config)# int serial 0
Router(config-if)# ip access-group 100 in
```

① 255.0.0.0
② 255.255.0.0
③ 255.255.255.0
④ 0.0.255.255
⑤ 0.255.255.255

39. 방화벽에서 TCP나 UDP 등의 프로토콜에 대해 필터링 정책을 세우기 위해서는 각각의 포트를 기준으로 필터링을 한다. 그렇다면 icmp 프로토콜에 대해서는 일반적으로 어떠한 기준으로 필터링을 하는가? (4)

① 포트번호
② TOS 값
③ 패킷의 id
④ 타입과 코드
⑤ 패킷의 flag

40. 방화벽에서는 tcp 기반의 스캔이나 공격을 차단하기 위해 tcp의 flag를 기준으로 특정 tcp 패킷을 필터링 할 수 있다. 다음 중 방화벽 쪽으로 들어오는(inbound) 트래픽에 대해 필터링하지 말아야 할 트래픽은 무엇인가? (2)

① SYN,FIN
② SYN,ACK
③ SYN,ACK,FIN
④ SYN,FIN,RST
⑤ SYN,ACK,FIN,RST,PSH

정보보호전문가(SIS) 2급 필기 샘플문제

과 목	어플리케이션 보안	시 험 시 간	4 0 분

1. SMTP에 대한 설명으로 다음중 틀린 것은? (1)

① TCP/IP의 트랜스포트 계층에서 동작하는 프로토콜이다.
② 컴퓨터간에 전자우편을 전송하기 위한 프로토콜이다.
③ RFC 821에 규정되어 있다.
④ 개방형시스템간 상호접속(OSI)의 메시지 통신시스템(MHS)에 대응한다.
⑤ 2개의 전자우편 시스템간에 어떻게 대화하는지를 지정하고 전자우편을 전송하기 위해 교환하는 제어메시지의 형식을 규정한다.

2. 다음은 스팸 메일을 추적하는 내용이다. 추적과 관련된 내용이 틀린 것을 고르시오.(4)

① 메일 헤더에 있는 From: 필드는 대부분 가짜이므로 무시해도 좋다.
② 메일이 중계된 경로상의 IP 주소는 중요하지 않다.
③ 메일 헤더에 있는 Date: 필드 즉 날자는 스패머 시스템의 시간이므로 무시해도 좋다.
④ 중계된 IP 주소를 ping과 nslookup등을 활용하여 해당 시스템이 변동 IP를 쓰는지 고정 IP를 쓰는지를 확인할 필요가 없다.
⑤ 이 스팸 머신에 DNS 서비스를 어떤 호스트가 하는지를 알기 위해서 whois등을 활용한다.

3. 다음 중 FTP 보안을 강화 하기 위한 방안이 아닌 것은 무엇인가? (1)

① /etc/ftpusers의 usenet, uucp, bin, daemon등의 사용을 허가 한다.
② ftp 로깅 - ftp 서비스 접속 기록을 유지하기 위해서 /etc/inetd.conf의 ftpd에 "-l'' 옵션 추가 한다.
③ # vipw 와 # vi ~ftp/etc/passwd 명령을 사용하여 안전한 anonymous FTP를 설치한다.
④ /etc/ftpusers 사용하여 root 사용자의 ftp 사용을 불허한다.
⑤ chmod 600 /etc/ftpusers 명령을 이용하여 허가상태를 root 소유자만 읽고 쓸 수 있도록 한다.

4. 다음은 E-Mail 보안을 위해 가장 많이 사용되는 표준 프로토콜인 S/MIME 과 PGP에 대한 설명이다. 이 중 잘못 표현된 것은? (5)
   ① 메시지 암호에는 비밀키암호화 알고리즘이 사용되며 비밀키는 공개키 암호화 알고리즘으로 암호된다.
   ② S/MIME과 PGP는 공개키 분배를 위하여 X.509 인증서를 사용할 수 있다.
   ③ S/MIME과 PGP는 전송되는 메시지에 대하여 암호화된 메시지, 서명된 메시지, 암호화 및 서명된 메시지 형식을 지원한다.
   ④ 전송되는 암호화 메시지에 서명을 추가하기 위해서는 송신자의 개인키가 존재하여야 한다.
   ⑤ S/MIME과 PGP를 사용하여 보안메일시스템을 구축하려면 이를 지원하는 메일 서버를 설치하여야 한다.

5. 다음 중 FTP(File Transfer Protocol)의 보안에 관한 설명으로 옳지 않은 것은? (2)
   ① FTP는 사용자이름/패스워드(username/password) 인증방법을 사용한다.
   ② FTP에서의 패스워드는 디폴트(default)로 DES 암호화 되어 전송된다.
   ③ FTP 서비스를 이용함에 있어서 항상 사용자 자신의 계정을 가질 필요는 없다.
   ④ FTP "control connection"의 세션은 단 한번만 열리고, 세션 자체는 암호화되지 않는다.
   ⑤ FTP "data connection"의 세션은 여러 번 열릴 수 있고, 세션 자체는 암호화되지 않는다.

6. 다음 중 FTP(File Transfer Protocol) 서버에 가해질 수 있는 공격에 대한 설명으로 가장 적당하지 않은 것을 고르시오. (3)
   ① FTP 서버의 배너(banner) 정보는 서버 공격에 이용될 수 있다.
   ② FTP의 "PORT" 명령은 FTP 바운스 공격(bounce attack)에 이용될 수 있다.
   ③ FTP의 "PASV" 명령은 패스워드 브루트 포스(brute force) 공격에 이용될 수 있다.
   ④ FTP의 "PORT" 명령은 포트 스캐닝 공격(port scanning attack)에 이용될 수 있다.
   ⑤ FTP의 "PASV" 명령은 데이터 하이잭킹(data hijacking)에 이용될 수 있다.

7. 다음중 SSL에서 제공하는 보안서비스가 아닌 것은? (3)

   ① 기밀성
   ② 상호인증
   ③ 송수신부인방지
   ④ 무결성
   ⑤ MAC(Message Authentication Code)

8. 다음 중 mail bombs에 대한 설명으로 올바른 것은? (2)

① 불특정 다수를 상대로 메일 수신자가 원하지 않는 메일을 보내는 것
② 다수 또는 대용량 메일을 보내 메일서버를 다운 시키는 것
③ 메일을 통해 악성 프로그램을 실행시켜 정보를 유출시키는 것
④ 메일 제목과는 다르게 악성 바이러스를 첨부하여 유포시키는 것
⑤ 메일을 통해 상대방 시스템에 백도어를 설치 하는 것

9. 다음은 메일의 주요 공격 방법들이다. 다음의 설명에 맞는 메일 공격 방법은 어느 것인가? (1)

공격자가 조작된 메일헤드를 포함한 메일을 보내 해당 시스템에서 특정 명령이 수행되도록 하는 메일 공격 방법이다.

① 셸 스크립트 공격
② 트로이잔 목마 공격
③ 바이러스 공격
④ 버퍼 오버플로우 공격
⑤ 액티브 컨텐츠 공격

10.다음은 FTP의 취약점과 공격 유형에 대한 설명이다. 이들 중 옳은 것은? (3)

① 익명 FTP 취약점이란 FTP 서버의 in.ftpd 프로세스가 core라는 파일을 생성하면서 발생하는 문제점이다.
② FTP 데몬 버그는 임의의 프로세서를 중단시킬 수는 있지만 삭제 시킬 수는 없다.
③ FTP 바운스 공격은 FTP 프로토콜의 취약점을 이용한 공격 방법으로써 예전부터 문제시 되어왔던 공격 방법이다.
④ FTP 바운스 공격을 통해 보내지는 메일은 비익명성으로 송신지를 알 수 없는 fake mail 성격을 띄게 된다.
⑤ 포트 스캐닝이란 공격한 후에 이루어지는 재공격으로써 임의의 호스트에서 어떤 포트를 사용하는지 알아내는 공격이다.

11.스팸 메일에 대한 내용이다. 옳지 않는 것은 무엇인가? (5)

① 스팸 메일은 추적이 가능하다.
② 스팸 메일은 헤더 부분에 중요한 정보를 담고 있다.
③ 사용자는 스팸 메일이 전달되어 오는 서버로부터 메일을 차단하는 것이 가장 최선의 방법이다.
④ 스팸 메일의 정보는 스패머의 시스템에서 생성되었으므로 신뢰할 수 없다.
⑤ ISP에서는 IPAD를 사용하고 있다. 따라서 메일 수신 시간이 제대로 되어 있는지 확신할수 있다.

12. S-HTTP에 대한 설명으로 옳지 않은 것을 고르시오. (2)

① EIT사의 HTTP에 보안 요소를 첨가한 확장판으로 설계되었다.
② S-HTTP를 수용하기 위해서는 웹서버와 브라우져 프로그램이 불필요한다.
③ S-HTTP는 보안 프로토콜인 SSL의 대안으로 설계되었다.
④ S-HTTP프로토콜은 어플이케이션 수준에서 보안을 추가하도록 설계되었다.
⑤ S-HTTP는 브라우져와 서버간의 HTTP 정보들을 캡슐화한다.

13. S-HTTP는 일련의 Security Negotiation Header들을 추가, 보안 옵션에 고려하여 이용한다. 이때 서버와 브라우저 사이에 발생하는 문제점이 아닌 것은? (5)

① 보안 조치의 선정에 따른 전송의 적용 문제
② 특정 구현 알고리즘 적용의 문제
③ 서버와 브라우저 사이의 최대 보안 수준의 협상 문제
④ 보안이 강화된 데이터들을 송신측과 수신측 어느 곳에서 먼저 보내고 받을 것인지에 대한 협상 문제
⑤ 보안 강화 옵션에 대한 선택 문제

14. 정보시스템의 위기 관리에 관하여 정보보호 관점에서 크게 5단계로 구체화 되어 있다. 순서가 올바른 것을 고르시오. (1)

① 신호탐색 - 예방 및 준비 - 손실축소 - 재난 복구 - 학습
② 신호탐색 - 손실축소 - 예방 및 준비 - 재난 복구 - 학습
③ 예방 및 준비 - 신호탐색 - 손실축소 - 재난 복구 - 학습
④ 신호탐색 - 예방 및 준비 - 손실축소 - 학습 - 재난 복구
⑤ 학습 - 예방 및 준비 - 손실축소 - 재난 복구 - 신호탐색

15. 다음 중 RFC 2228에서 규정한 FTP 보안 확장 명령어의 설명으로 틀린 것은? (5)

① AUTH 명령어는 클라이언트가 정보를 전송할 때 어떤 보안 방법을 사용하여 전송되는 지를 설명한다.
② CCC 명령어는 보안 실행의 사용을 종료할 때 쓰인다.
③ PBSZ 명령어는 파일이 전송될 동안 전송될 기호화된 데이터 블록의 최대 크기를 의미한다.
④ MIC 명령어는 데이터 보안 수준이 safe로 설정되었을 때 데이터의 전송을 위해 사용된다.
⑤ ENC 명령어는 데이터 보안 수준 Confidencial로 설정되어 있을 때 데이터 전송을 위해 사용된다.

16. 파일전송 프로토콜(FTP)은 하나의 시스템에서 또 다른 시스템으로 파일을 전송하기 위한 기본적인 방법이다. 다음의 ftp 설명중 틀린것은? (4)

① ftp는 표준 사용자명/패스워드 인증 방법을 사용한다.
② ftp는 기본적으로 패스워드를 일반적인 텍스트로 전달한다.
③ ftp 세션은 암호화되어 있지 않기 때문에 사생활 보호 기능을 제공하지 않는다.
④ ftp 서버는 주어진 사용자가 정당한 사용자인지 확실하게 확인한다.
⑤ 공격자로 하여금 전기적인 도청을 통한 패스워드의 획득을 가능하게 한다.

17. 전자 지불 시스템의 위협 요소로 옳지 않는 것은 무엇인가? (5)

① 위조 : 디지털 정보인 전자화폐는 디지털 데이터이기 때문에 누구나 쉽게 복사가 가능하다.
② 국가 통화 문제 : 국가별로 관리하던 통화 관리 체계를 글로벌 개념으로 확대할 필요가 있어 국제 통화 관리를 관장할 수 있는 국제 기구의 출현이 요구될 것으로 전망
③ 이중사용 : 전자화폐는 그 자체가 가치를 가진 디지털 정보이기 때문에 원본과 사본의 구별이 불가능하다 따라서 불법 복제하여 반복적인 사용이 가능하는 위협 요소가 있다.
④ 위장 : 모든 거래 당사자들이 직접 대면하지 않고 네트워크를 통해 상거래에 필요한 정보를 주고 받게 되므로 당사자들간의 위장이 가능한 위험 요소가 있다.
⑤ 익명성 제어 : 모든 전자 화폐 시스템에서는 사용자가 물건을 구입하고 대금을 지불하는 동안에 사용자의 익명성을 제공하는 위험성이 있다.

18. ftp 공격의 사전공격 형태로써, 임의의 호스트에서 몇번의 포트를 사용하는지 알아내는 공격은 다음 중 어느 것인가? (2)

① ftp bounce attack
② ftp port scanning
③ Anonymous ftp attack
④ Brute force attack
⑤ ftp daemon bug

19. SMTP에 대한 설명으로 다음중 틀린 것은? (1)

① TCP/IP의 트랜스포트 계층에서 동작하는 프로토콜이다.
② 컴퓨터간에 전자우편을 전송하기 위한 프로토콜이다.
③ RFC 821에 규정되어 있다.
④ 개방형시스템간 상호접속(OSI)의 메시지 통신시스템(MHS)에 대응한다.
⑤ 2개의 전자우편 시스템간에 어떻게 대화하는지를 지정하고 전자우편을 전송하기 위해 교환하는 제어메시지의 형식을 규정한다.

20. 다음은 메일과 관련된 프로토콜 중 하나에 대한 설명이다. 무엇에 대한 설명인가?

(1) 메일 서버로부터 사용자의 컴퓨터로 메일을 다운로드하여 내용 확인 (2) 데몬 프로세스는 110번 포트 사용 (3) 메일 서버로부터 메일 다운로드후 메일 서버의 메일 박스에서는 삭제 (4) 사용자가 고정적인 위치에서 메일을 사용시 유리

① SNMP
② SMTP
③ FTP
④ PGP
⑤ POP

21. SSL에 대한 다음 설명 중 잘못된 것은? (4)

① Netscape사에서 처음으로 제안했다.
② 웹과 같은 특정 응용을 위한 보안 프로토콜이 아닌 인터넷보안 프로토콜로 사용될 수 있다.
③ TCP/IP계층과 어플리케이션 계층 사이에 위치한다.
④ SSL은 하나의 프로토콜로 이루어져 있다.
⑤ 데이터를 송수신하는 두 컴퓨터 사이 즉, 종단간보안서비스를 제공한다.

22. IPsec을 통해 제공되는 대표적인 보안서비스가 아닌 것은? (5)
① 인증
② 무결성
③ 재전송공격에 대한 보호
④ 기밀성
⑤ 부인방지

23. IP보안 프로토콜에서 TCP계층 위에서 클라이언트/서버 어플리케이션 사이에 보안 서비스를 제공하기 위한 메커니즘은 무엇인가? (3)
① IPsec
② IPv4
③ TLS
④ IPv6
⑤ PPP

24.다음중 SSL에서 제공하는 보안서비스가 아닌 것은? (3)
① 기밀성
② 상호인증
③ 송수신부인방지
④ 무결성
⑤ MAC

25. 다음 POP 서비스에 대한 설명 중 틀린 것은 ? (3)
① POP은 Post Office Protocol의 약어이다.
② POP은 email을 받는 데 사용되는 프로토콜이다.
③ POP은 SMTP를 대체하여 사용되는 프로토콜이다.
④ POP이 전통적으로 사용하는 port 번호는 110이다.
⑤ POP은 Netscape 및 Microsoft Internet Explorer browser와 결합되어 사용된다.

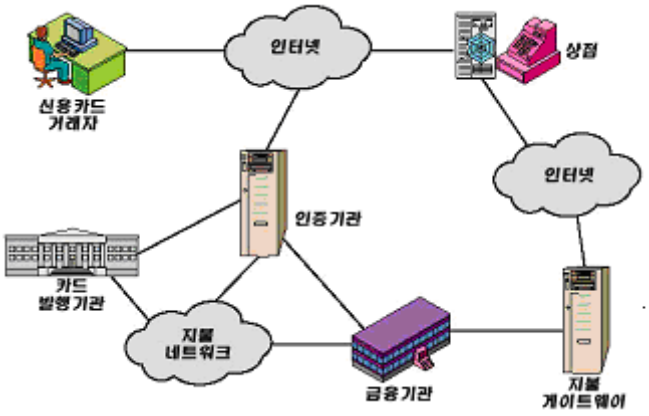
26. 웹 서버의 특정 디렉토리에 접근할 수 있는 사용자를 제한하는 것은, 시스템 설정 파일을 수정하여 시스템 전역적으로 수행할 수도 있고, 각 디렉토리 아래에 있는 설정 파일을 수정하여 디렉토리 별로 수행할 수도 있다. 두 방법의 안전도 비교에 대한 설명으로 올바른 것은 ? (4)
① 전역적 설정 방법은 안전도 면에서 전혀 의미가 없다.
② 전역적 설정 방법과 디렉토리별 설정 방법은 안전도 면에서 동일하다
③ 디렉토리별 설정 방법이, 전역적 설정 방법보다 안전도 면에서 더 권장된다.
④ 전역적 설정 방법이, 디렉토리 별 설정 방법보다 안전도 면에서 더 권장된다.
⑤ 디렉토리별 설정 방법은 안전도 면에서 전혀 의미가 없다.

27. SSL Handshake 과정 중 SSL 서버로부터 인증서를 요구받고 클라이언트 자신의 인증서를 서버로 보내는 과정은? (1)

① Client Certificate
② Client Key Exchange
③ Certificate Verify
④ Certificate Request
⑤ Client Hello

28. 다음 중 S-HTTP에 대한 설명으로 틀린 것은 ? (2)
① S-HTTP는 HTTP의 확장판으로 안전한 자료전송을 가능하게 한다.
② S-HTTP는 HTTP의 하부레이어로 SSL (Secure Socket Layer)를 사용한다
③ S-HTTP는 프로토콜 계층상으로 HTTP의 상위계층에서 동작한다.
④ S-HTTP는 디지털 인증서 (digital certificate)를 지원할 수도 있다.
⑤ S-HTTP는 단순한 사용자id-passwd에 의한 인증보다 더 안전한 인증을 제공해 준다.

29. SET(Secure Electronic Transaction)는 마스터카드사와 비자카드사가 1996년에 공동으로 개발한 것으로, 인터넷 상에서 신용카드를 이용한 거래를 보호하기 위한 보안 및 암호화 스팩이다. 아래의 그림을 참조하여 그것의 흐름(Sequence) 중 설명이 틀린 것은? (1)

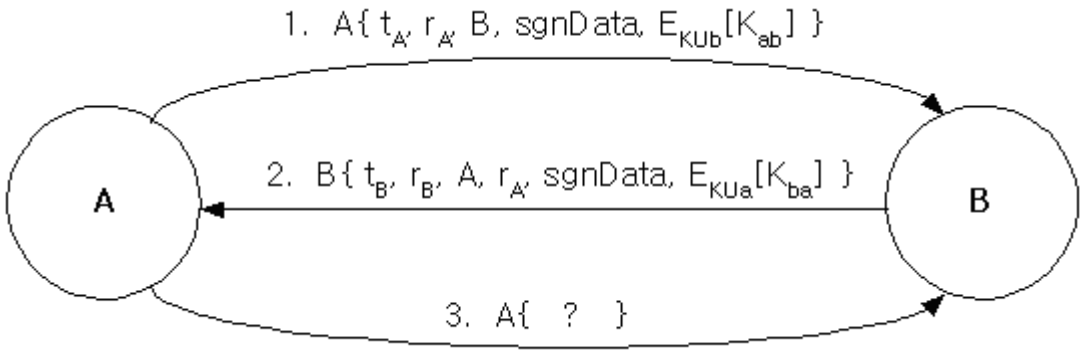


① SET를 이용한 신용카드 거래자는 이중서명(Dual Signature)을 사용하므로, 상점에서 신용카드거래자의 주문내역과 지불내역을 알 수 있다.
② 신용카드거래자는 거래의 초기 단계에서 상점의 인증서 및 지불게이트웨이의 인증서를 가지고 있어야 한다.
③ 신용카드거래자가 상점에게 보내온 주문내역은 상점에게만 유효하므로, 상점은 지불게이트웨이를 통하여 금융기관에 암호화된 지불내역만을 보낸다.
④ 위의 흐름에서 사용되는 인증서는 금융기관이 발행하는 인증서가 될 수 있다.
⑤ 지불게이트웨이와 상점간에 인증이 이루어진 뒤, 상점은 신용카드거래자가 구매한 물건에 대한 대금을 지불받게 된다.

30. X.509는 다양한 어플리케이션에 사용되기 위해 세가지로 대체 가능한 인증 절차를 제공한다. 그 중에 되풀이 공격(replay attack)을 감지할 수 있는 절차가 Three-way 인증 절차이다. 세 번째 메시지 { ? }에 들어갈 가장 알맞은 것은? (4)

※ tA , tB : 타임 스탬프 ※ rA, rB : 세션 중 한번만 사용되는 랜덤 넘버 (nonce) ※ A : A의 신분관련 내용 (identity) ※ sgnData : 송신자의 비밀키로 sign 한 데이터 ※ EKUb[Kab] : B의 공개키로 세션키 Kab를 암호화한 것 ※ X { } : 송신자 X가 상대방에게 보내는 메시지 열

<보기>



① tA
② tB
③ rA
④ rB
⑤ EKUb[Kab]

31. SSL Handshake 과정 중 SSL 서버로부터 인증서를 요구받고 클라이언트 자신의 인증서를 서버로 보내는 과정은? (1)

① Client Certificate
② Client Key Exchange
③ Certificate Verify
④ Certificate Request
⑤ Client Hello

32. 전자상거래 시스템에서 요구하는 보안 요구 조건으로서 적합하지 않는 것은? (3)
① 기밀성
② 부인봉쇄
③ 상호 운용성
④ 무결성
⑤ 인증

33. 전자화폐에 요구되는 기본 조건으로서 가장 관계가 없는 것은? (4)
① 안전성
② 양도성
③ 익명성
④ 사용자 인증
⑤ 완전 정보화

34. SET(Secure Electronic Transaction)는 인터넷 상의 신용카드 정보 거래 보호를 위한 암호 프로토콜이다. SET에 사용되고 있는 암호 기술이 아닌 것은? (3)
① 디지털 서명
② 해쉬 함수
③ 영지식증명프로토콜
④ 공개키 암호
⑤ 비밀키 암호

35. Diffie-Hellman 키 분배 프로토콜은 공개키 암호를 이용한 대표적인 키 분배 방식이다. 이 키 분배 방식과 관련이 없는 것은 어느 것인가? (3)
① 이산대수문제
② Pohlig-Hellman 알고리즘
③ 소인수분해문제
④ 중간공격(Middle Attack)
⑤ 키 교환 방식

36. 사용자의 신원을 증명하기 위한 안전한 사용자 인증 방식으로 적합하지 않는 것은? (5)
① 자신이 알고 있는 것에 바탕을 둔 패스워드 인증 기법
② 자신이 알고 있는 비밀에 대한 지식을 상대에게 누설하지 않고 자신의 신원을 증명하는 영지식 증명 인증 기법
③ 자신이 소지하고 것(스마트카드, 마그네틱 카드)을 이용하는 방법
④ 자신이 선천적으로 가지고 있는 것(생체 인증)
⑤ 수기 서명에 대한 그림 파일

37. SSL 프로토콜에서 제공되는 키 분배 프로토콜에 대한 설명 중 잘못된 것은? (4)

① 여러 가지 키 분배 메카니즘 중 (RSA, DH 등) 하나의 메카니즘이 서버와 클라이언트 간의 협상을 통하여 선택될 수 있다.

② 서버의 인증서 만을 이용한 키 분배 프로토콜이 널리 이용된다. 이 경우 클라이언트는 마스터 비밀을 생성하여 서버의 인증서에 포함된 공개키로 암호화하여 서버로 전달한다.

③ 대표적인 키 분배 메카니즘은 RSA 암호 알고리듬이다.

④ 디지털 서명용 인증서 만을 이용한 키 분배 기능을 제공한다.

⑤ 키 분배를 위한 인증서는 인증기관에 의하여 발행되어야 한다.

38. S/MIME 전자우편 보안 프로토콜에 대한 설명으로 틀린 것은? (1)

① S/MIME은 전자인증이 필요 없어 많은 사용자를 확보하고 있다.

② S/MIME은 기존의 MIME에 보안기능을 추가한 전자우편 프로토콜이다.

③ S/MIME은 RSA암호화 시스템을 사용하여 전자우편을 안전하게 보낸다.

④ S/MIME은 마이크로소프트와 넷스케이프사의 웹 브라우저에 기본적으로 포함되어 있다.

⑤ 전자우편 관련 제품을 만드는 업체와 보안 서비스 업체들에 의해 제공되고 있다.

39. 다음은 공개키 기반 구조의 구성 요소에 대한 설명이다. 잘못된 것을 고르시오. (2)

① 정책승인기관 (Policy Approving Authority) - PKI 전반에 사용되는 절차를 생성하고 PKI 구축의 루트 CA로의 역할을 한다.

② 정책인증기관 (Policy Certification Authority) - 하위 기관의 공개키를 인증하고 인증서 및 인증서 취소목록 등을 관리한다.

③ 인증기관 (Certification Authority) - 사용자의 공개키 인증서를 발급하고 또 필요에 따라 취소한다.

④ LDAP (Lightweight Directory Access Protocol) - 인증서와 사용자 관련정보, 상호 인증서 쌍 인증서 취소목록등을 저장 및 검색하는 장소이다.

⑤ 사용자 (User) - PKI내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다.

40. 전자 공증 기관의 주요 서비스 중 옳지 않은 것을 고르시오. (5)

① 증거의 제출

② 증거의 유효성 증명

③ 고객에 대한 서비스 컨설팅

④ 기본 서비스(일자/시간, 내용인증, 배달증명, 일반적인 데이터와 법적 요구 데이터의 전자 보존 서비스)

⑤ 법적 요구 데이터에 대한 법적 추적 서비스

정보보호전문가(SIS) 2급 필기 샘플문제

과 목	정보보호론	시 험 시 간	4 0 분

1. 다음 중 비밀키 암호화 알고리즘과 공개키 암호화 알고리즘에 대한 비교 설명한 것 중 잘못된 것은? (4)
   ① 비밀키 암호화 알고리즘을 암호화 / 복호화 속도가 빠르다.
   ② 공개키 암호화방식은 키의 분배가 용이하다.
   ③ 비밀키 암호화 알고리즘은 키의 변화 빈도가 높다.
   ④ 비밀키 암호화 알고리즘은 키의 길이가 길다.
   ⑤ 공개키 암호화 알고리즘은 키의 길이가 길다.

2. 다음 중 PKI의 응용분야가 아닌 것은? (3)
   ① EDI보안
   ② Web보안
   ③ IDS
   ④ SSL
   ⑤ Mail보안

3. 스트림 암호에 관한 설명으로 잘못 된 것은? (3)
   ① 암호시스템의 핵심은 이진 키 수열의 특성과 발생 방법이다.
   ② 이진수열(비트)로 된 평문과 키 이진수열을 비트단위로 XOR하여 암호화 한다.
   ③ 암호화 알고리즘에 치환변환과 전치변환이 주로 쓰인다.
   ④ 주로 유럽을 중심으로 발전하였으며 군사용으로 쓰인다.
   ⑤ 일회용 패드(one-time pad)는 스트림 암호의 한 예이다.

4. 두 사용자 A와 B가 아래와 같은 조건이 주어진 Diffie-Hellman 암호 알고리즘을 이용하여 비밀키를 교환하려고 한다.

소수 : p=13, 생성원 : g=7 A의 개인키 : 5, A의 공개키 : 11 B의 개인키 : 3, B의 공개키 : 5

비밀키는 다음 중 어느 것인가? (3)
   ① 11
   ② 33
   ③ 5
   ④ 7
   ⑤ 12

5. 암호 시스템에 대한 설명 중 잘못된 것은? (2)

① 평문의 각 원소에 다른 원소를 사상 시키는 것을 치환이라고 한다.
② 송수신자가 같은 key를 사용하는 시스템을 비대칭 암호화 방식이라고 한다.
③ 송수신자가 다른 key를 사용하는 것을 공개키 암호화 방식이라고 한다.
④ 블록 암호화 방식은 입력을 한번에 하나의 원소 블록씩 처리한다.
⑤ 스트림 암호화 방식은 입력을 한번에 하나의 요소씩 처리한다.

6. 다음의 공개키 암호에 대한 내용 중 잘못된 것은? (2)

① 하나의 알고리즘으로 암호와 복호를 위한 키 쌍으로 암호화와 복호화를 수행한다.
② 송신자와 수신자는 대응되는 키 쌍을 모두 알고 있어야 한다.
③ 두개의 키 중 하나는 비밀로 유지되어야 한다.
④ 메시지를 해독하는 것이 불가능하거나 비현실적이어야 한다.
⑤ 암호화 알고리즘, 하나의 키와 암호문에 대한 지식이 있어도 다른 하나의 키를 결정하지 못해야 한다.

7. 다음은 MD5의 메시지 처리의 5단계 과정이다. 순서가 올바른 것은 어느 것인가? (4)

a. MD 버퍼의 초기화 b. 패딩 비트의 부가 c. 메시지 길이 부가 d. 512-bit 블록 메시지 처리 e. 출력

① a – b – c – d – e
② c – b – d – a – e
③ a – c – b – d – e
④ b – c – a – d – e
⑤ d – b – c – a – e

8. 다음 설명은 정보의 속성 중에서 무엇을 설명한 것인가? (4)
송신자와 수신자간에 전송된 메시지를 놓고, 전송치 않았음을 또는 발송되지 않은 메시지를 받았다고 주장할 수 없게 한다.

① 무결성
② 비밀성
③ 인증
④ 부인방지
⑤ 액세스제어

9. 암호 알고리즘의 안전성 분석을 위한 FIPS 140-1 통계 테스트에 관한 설명 중 잘못된 것은? (4)
   ① Serial test란 0값이 출력된 이후 다시 0값이 출력될 확률과 1값이 출력될 확률이 동일한지 검증하는 것이다.
   ② Poker-n test란 출력 비트열를 n비트 블록으로 나누었을 때 생성 가능한 모든 값이 균일하게 분포하는 지 검증하는 것이다.
   ③ Run test란 연속하여 같은 비트 값이 n번 출력될 확률이 2-n 인지 검증하는 것을 말한다.
   ④ Frequency test란 00, 10, 01, 11 블록의 빈도수가 균일한 지 검증하는 것이다.
   ⑤ Autocorrelation test란 원래의 수열과 k번 후의 수열과의 연관관계를 검증하는 것이다.

10. 대표적인 해쉬함수에 대한 구체적인 설명으로 바른 것은? (4)
   ① MD5는 입력 데이터는 128비트 블록을 기본 단위로 한다.
   ② SHA 알고리즘은 초기치(initial value)를 사용하지 않는 구조이다.
   ③ SHA 알고리즘에서 입력 데이터의 크기가 512비트의 배수이면 패딩은 불필요하다.
   ④ HAS-160은 입력 데이터를 512비트 블록 단위로 처리한다.
   ⑤ 해쉬함수는 큰 데이터를 고속으로 처리하기 위하여 주로 1라운드 구조로 설계된다.

11. 다음 중 DES 및 3-DES에 관한 설명으로 잘못된 것은? (2)
   ① F-함수는 8개의 S-box로 구성되어 있다.
   ② DES의 S-box는 모두 선형(linear) 구조이며 DES의 안전성의 핵심 모듈이다.
   ③ 초기치환(Initial Permutation)은 입력 64비트를 출력 64비트로 변환하는 과정이다.
   ④ F-함수의 확장(expansion)은 입력 32비트를 출력 48비트로 확장하는 과정이다.
   ⑤ 3-DES는 2개 또는 3개의 서로 다른 키를 이용하여 DES를 반복 적용하는 것이다.

12. ElGamal 공개키 암호의 설명 중 틀린 것은? (5)
   ① 이론적으로는 이산로그가 어려운 임의의 유한 교환군에 적용 가능하다.
   ② 하나의 평문을 여러 번 암호화하면 매번 암호문이 달라진다.
   ③ 난수 생성기가 있어야만 암호화를 수행할 수 있다.
   ④ Diffie-Hellman 키 공유 프로토콜과 안전도가 동치이다.
   ⑤ 확률 공개키 암호로 안전도가 이산로그와 동치이다.

13. 다음의 해쉬 함수 중 충돌 쌍이 발견된 알고리즘은 무엇인가? (5)

① HAS
② SHA-1
③ RIPEMD-160
④ HAVAL
⑤ MD5

14. 다음 보기의 내용에 해당하는 암호시스템은 무엇인가? (3)
<보기>

제한된 대역폭 등이 요구되는 무선통신 분야에 특히 유용하여 무선통신, 전자서명, 인증 등에 쓰이며, 비밀 키의 안전한 분배와 정보의 안전한 전송에 이용된다. 또한 이 암호시스템은 유한체에서의 연산을 포함하므로 H/W와 S/W로 구현하기가 용이하다

① DES
② RSA
③ ECC
④ RIJNDAEL
⑤ ElGamal

15. 다음 중 디지털 서명으로 사용할 수 없는 공개키 암호는 ? (4)

① RSA 공개키 암호
② ElGamal 공개키 암호
③ NTRU 공개키 암호
④ MerkleHellman Knapsack 공개키 암호
⑤ 타원곡선 공개키 암호

16. 암호시스템을 설계할 경우 고려사항이 아닌 것은? (4)

① 암호화와 복호화 과정은 효율적인 계산과정으로 설계되야 한다.
② 암호시스템의 안전성은 키에만 의존하도록 구현해야 한다.
③ 암호시스템에 사용되는 암호 알고리즘은 공개해야 한다.
④ 암호화와 복호화 시에 사용되는 키의 길이는 상관 없도록 해야 한다.
⑤ 암호시스템은 손쉽게 사용할 수 있도록 해야 한다.

17. 정보보호 조직에 대한 설명으로서 옳지 않은 것은? (1)

① 정보보호 조직은 정보기술에 대한 전문적 지식을 필요로 하기 때문에 정보처리부서 내에 위치시키는 것이 바람직하다.

② 정보보호 조직의 임무는 정보보호 활동을 기획, 조정하는 역할이 더 중요하며 실제 정보보호 활동을 감시, 관제하는 역할은 수행하지 않는 것이 바람직하다.

③ 정보보호위원회는 최고경영자를 포함하여 간부급 경영자로 구성되며 주요정보보호활동에 대한 승인 및 조정 기능을 수행한다.

④ 조직의 특성을 반영하여 정보보호 인력 및 예산이 적절히 배당되어야 한다.

⑤ 정보보호 활동의 성공을 위해서는 조직 구성원 전체에 대한 구체적인 역할과 책임을 규명해야 한다.

18. 위험분석에 대한 설명 중 적절한 것만 묶은 것은 어느 것인가? (2)

<보기>

1. 위험분석은 자산가치 파악, 위협 및 취약성 분석, 잠재적 손실에 대한 영향을 분석하는 행위이다.
2. 위험분석 과정의 작업량을 결정하는 가장 중요한 부분은 위협 및 취약성 분석이다.
3. 상위 수준 위험분석을 통해 핵심업무 및 위험이 높은 업무를 선별하는 작업이 선행되어야 한다.
4. 정량적인 분석기법이 정성적인 기법보다 더 우수한 결과를 초래한다.
5. 취약성이란 자산에게 손실을 미칠 수 있는 요인을 의미한다.

① 1, 4
② 1, 3
③ 2, 3
④ 2, 5
⑤ 3, 5

19. 위협이 조직에 원하지 않는 사건이나 결말을 가져오는 것을 가능하게 만드는 통제 및 환경상의 결함이나 조건을 무엇이라고 하는가? (4)

① 통제 약점(Control Weakness)
② 위험(Risk)
③ 노출(Exposure)
④ 취약성(Vulnerability)
⑤ 제한된 내부 통제

20. 다음은 위험분석의 의미와 특징에 대한 설명이다. 틀린 것은? (2)

① 위험분석은 정보보호 대책 구현에 선행되어 수행되어야 한다.
② 효과적 정보보안 프로그램의 초석으로서 의미를 가지고 있다.
③ 정량적 분석방법이 정성적 분석방법보다 정확한 위험수준을 결정할 수 있다.
④ 자산식별, 위협분석, 취약성평가, 영향평가, 대책선정, 권고안 작성 순으로 진행
⑤ 조직의 특수 상황을 고려한 정보보호 대책을 선정할 수 있다.

21. 정보보호대책 선정과 관련된 활동에 대한 설명 중 틀린 답을 모두 묶은 것은 어느 것인가? (4)

<보기>

1. 정보보호대책은 일반적으로 기본통제 리스트에서 선정될 수도 있으며 상세 위험분석과정을 통해 선정될 수도 있다.
2. 일반적으로 기술적 정보보호대책이 우선적으로 구현되어야 한다.
3. 정보보호대책 선택은 위험평가에 근거하여 기술, 재정, 법/제도, 시간, 문화 등 여러 제약조건 등을 고려해서 선정해야 한다.
4. 정보보호대책 선정을 위한 목표위험수준은 정보기술자에 의해 결정된다.
5. 정보보호대책은 비용은 무시한 상태에서 보안효과가 최대인 것을 우선적으로 선정해야 한다.

① 2, 4
② 4, 5
③ 1, 2., 4
④ 2, 4, 5
⑤ 1, 4, 5

22.정보보호 사후관리 활동을 포함하는 것은? (1)

<보기>

1. 보안감사, 모니터링, 변경관리, 보안사고대응
2. 준거성 체크, 모니터링, 변경관리, 시스템 유지보수, 보안사고대응
3. 모니터링, 변경관리, 시스템 유지보수, 보안사고대응
4. 구성관리, 변경관리, 보안감사, 보안사고대응
5. 정보보호정책수립, 모니터링, 변경관리, 보안사고대응

① 1, 4
② 2, 3
③ 4, 5
④ 1, 5
⑤ 3, 4

23. 집권화된 환경에서의 보안 관리에 비해 분권화된 환경에서의 보안 관리가 가지는 장점이 아닌 것은? (1)

① 더 강력한 보안 수준이 유지된다.
② 해당 사이트에서 보안이 수행된다.
③ 보안 쟁점에 대한 시기 적절한 해결이 가능하다.
④ 보안 통제에 대한 감시가 더 자주 수행된다.
⑤ 보안 관리자의 책임하에 능동적인 보안을 구축할 수 있다.

24. 다음 중 비상계획 수립 절차 중 가장 먼저 수행하는 절차는? (2)

① 잠재적 재해를 예측한다.
② 핵심 기능을 식별한다.
③ 비상계획 전략을 채택한다.
④ 필요한 인원 배치를 한다.
⑤ 핵심 기능을 지원하는 자원을 식별한다.

25. 다음 중 재해복구계획(DRP)과 업무연속성계획(BCP)에 대한 설명으로 잘못된 것은? (3)

① BCP는 사고나 재해 이후 핵심 비즈니스 기능의 재개를 목표로 한다.
② DRP는 사고나 재해 이후 시스템의 정상 복구를 목표로 한다.
③ BCP는 천재지변으로 인한 업무 중단을, DRP는 주로 기계적인 원인으로 업무 중단을 다룬다.
④ DRP는 BCP보다 기술적인 면에 초점을 맞추어 수립한다.
⑤ DRP와 BCP 모두 비상계획에 포함되는 개념이다.

26. 업무지속성을 위한 백업처리능력 대안으로서 Hot site, Mirror site, Warm site가 있는데 이중 가장 빠르게 백업을 제공하는 순서를 기술한 것은? (5)

① Hot site, Warm site, Mirror site
② Hot site, Mirror site, Warm site
③ Mirror site, Warm site, Hot site
④ Warm site, Hot site, Mirror site
⑤ Mirror site, Hot site, Warm site

27. 다음 중 업무연속성계획에 대한 설명이 아닌 것은? (1)

① 전산부서가 책임과 권한을 가지고 업무연속성계획을 수립, 유지, 관리해야 한다.
② 업무연속성을 위한 전략을 수립하기 위해서는 업무영향분석을 통해 이루어져야 한다.
③ 업무영향분석결과를 기초로 업무복구 목표시간 및 복구를 위한 최소한의 요구사항이 결정된다.
④ 업무연속성계획에 대한 정기적 교육 및 훈련 프로그램과 지속적 검토 및 변경관리 수행이 매우 중요하다.
⑤ 업무연속성계획은 IT부서에서 작성한 비상계획 및 재해복구계획에 기초하여 주요 조직단위에서 업무의 연속성을 보장하기 위해 작성한 일련의 계획이다.

28. OECD 정보보호 가이드라인에서 제시하고 있는 내용 중 틀린 것은? (3)

① 정부, 기업, 개인을 포함한 모든 참여자들이 정보시스템과 네트워크의 보호를 위해 수행해야 할 9가지 원칙을 제시하고 있다.
② 전 세계적인 정보보호 문화를 구축하기 위한 공통된 접근방식을 제공하고 있다.
③ 가이드라인의 실행을 위해 해당 국가들은 정보보호 문화를 도입하기 위한 조치를 취해야 할 것을 의무화하고 있다.
④ 정보보호 담당자 주도의 기술적인 정보보호대책 중심에서 사회 문화적 정보보호대책을 포함한 포괄적인 보안대책을 요구하고 있다.
⑤ OECD 비회원국에게 적기에 적절한 방식으로 가이드라인을 활용 가능하게 하라.

29. 2003년 2월 발표된 미 사이버공간 보안 전략에서 제시한 5가지 우선 순위가 아닌 것은? (4)

① 국가 사이버공간 대응시스템 구축
② 사이버공간 위협 및 취약성 감소 프로그램 수행
③ 사이버공간 보안을 위한 인식제고 및 훈련 프로그램 수행
④ 사이버 범죄에 대한 효과적 수사체계 구축
⑤ 사이버공간 보안을 위한 국제적 협력체계 구축

30. 정보보호 패러다임이 기술적 솔루션 중심에서 관리적 정보보호 대책 중심으로 이동되고 있으며 최근에는 정보보호 활동을 제도화/조직화하려는 움직임이 활발해지고 있다. 정보보호의 제도화/조직화를 수행하기 위한 필요 요소가 아닌 것은? (5)

① 정보보호 국제표준활동의 참여와 지원
② 정보보호관리체계의 수립 및 운영에 대한 인증
③ 정보보호를 조직문화의 일부분으로 정착
④ 동태적이고 지속적인 정보보호 수준의 측정을 통한 정보보호 관리
⑤ 정보보호 솔루션 도입 확대를 통한 대외적 침투에 대한 철저한 대비

31. 정보보호관리체계 인증의 진정한 효과가 아닌 것은? (4)

<보기>

1. 제 삼자의 객관적 입장에서 정보보호관리체계를 보증함으로써 대외적 신인도를 높일수 있다.
2. 인증 획득 사실을 마케팅 수단으로 활용할 수 있으며 이를 통해 이윤 창출이나 시장 확대를 도모할 수 있다.
3. 인증을 통해 정보보호 수준을 제고시킬 수 있으며 궁극적으로 정보보호 문화를 창출할 수 있다.
4. 인증 획득 과정을 통해 전 조직 구성원의 참여와 정보보호의 생활화를 유도할 수 있다,
5. 인증을 획득하면 정보보호 사고가 거의 발생하지 않을 수 있으며 궁극적으로는 완벽한 정보보호 수준을 인정받을 수 있다.

① 2, 4
② 3, 5
③ 1, 2
④ 2, 5
⑤ 3, 4

32. 다음 중 ISO 17799 문서에 대한 설명이 아닌 것은? (3)

<보기>

1. 영국 표준인 BS7799 Part 1을 2000년 국제표준화한 문서이다.
2. 정보보호관리체계 인증을 위한 명세서라고 할 수 있다.
3. 현재 ISO에서 개정 작업 중이다.
4. 정보보호관리를 위한 모범적인 통제사항(best practices)들을 수록하고 있다.
5. 정보보호관리체계(ISMS)의 수립 및 유지관리에 대한 설명을 포함하고 있다.

① 1, 5
② 2, 3
③ 2, 5
④ 3, 4
⑤ 1, 4

33. 전자서명법상의 전자서명의 효력에 관한 설명으로 틀린 것은? (4)

① 공인인증기관이 발급한 인증서에 의한 전자서명은 법령이 정한 서명 또는 기명날인으로 본다.

② 공인인증기관에 의한 전자서명이 있는 경우에는 당해 전자서명이 당해 전자문서의 명의자의 서명 또는 기명날인이라고 추정된다.

③ 공인인증기관에 의한 전자서명이 있는 전자문서에는 당해 전자문서의 무결성(무변개성)을 추정하는 효력이 인정된다.

④ 비공인인증기관에 의한 전자서명에도 법령이 정한 서명 또는 기명날인으로서의 효력이 인정된다.

⑤ 전자서명법상의 전자서명이 있는 전자문서는 진정성립이 추정된다.

34. 정보통신망 이용촉진 및 정보보호 등에 관한 법률상 개인정보에 관한 설명으로 틀린 것은? (2)

① 정보통신서비스제공자가 통계작성, 학술연구 또는 시장조사를 위하여 필요한 경우로서 특정개인을 알아볼 수 없는 형태로 가공하여 개인정보를 제공하는 경우에는 이용자에게 고지한 수집목적 및 이용목적의 범위를 넘어서 이용하거나 제공할 수 있다.

② 정보통신서비스제공자로부터 이용자의 개인정보를 제공받은 자는 당해 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있더라도 개인정보를 제공받은 목적 외의 용도로 이용하거나 제3자에게 제공하여서는 아니 된다.

③ 정보통신서비스제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.

④ 이용자의 개인정보를 취급하거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손, 침해 또는 누설하여서는 아니 된다.

⑤ 정보통신서비스제공자등이 타인에게 이용자의 개인정보의 수집, 취급, 관리 등을 위탁하는 경우에는 미리 그 사실을 이용자에게 고지하여야 한다.

35. 정보통신기반보호법에 관한 다음의 설명중 틀린 것은? (3)

① 정보통신기반보호법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립, 시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

② 전자적 침해행위라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터 바이러스, 논리, 메일폭단, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.

③ 챔해사고란 침해행위의 종류를 묻지않고 정보통신기반시설에 대한 모든 형태의 사고를 말한다.

④ 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 정보통신기반보호위원회를 둔다.

⑤ 중앙행정기관의 장은 소관분야의 정보통신기반시설중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

36. 정보통신기반보호법에 따르면 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대한 관리기관의 장이 필요하다고 인정하여 주요정보통신기반시설보호대책의 수립 등의 기술적 지원을 요청하는 경우 국가보안업무를 수행하는 기관의 장에게 우선적으로 그 지원을 요청하여야 한다. 이 경우에 위 법이 '열거한' 주요통신기반시설이 아닌 것은? (3)

① 도로·지하철·공항 시설
② 전력, 가스, 석유 등 에너지·수자원 시설
③ 국가안보·대북전략산업·기타 관련 시설
④ 방송중계·국가지도통신망 시설
⑤ 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

37. 다음 정보통신 기반 보호위원회에 관한 내용 중 옳은 것은? (1)

① 국무총리 소속 하에 정보통신기반 보호위원회를 둔다.
② 위원장을 포함한 15인 이내의 위원으로 구성된다.
③ 위원은 정보통신부 장관이 정하는 중앙 행정기관의 장과 위원장이 위촉하는 자로 한다.
④ 위원회의 모든 업무는 정보통신부 장관이 총괄한다.
⑤ 위원회의 효율적 운영을 위하여 중앙 행정기관에 실무위원회를 둔다.

38. 개인정보 분쟁조정위원회의 관련 법률 조항이 아닌 것은? (4)

① 개인정보분쟁조정위원회의 설치 및 구성
② 분쟁의 조정
③ 조정의 효력
④ 손해 배상 청구권
⑤ 조정절차

39. 개인정보를 얻기 위해 정보통신서비스제공자가 규정에 의한 동의를 얻고자 하는 경우에는 미리 다음 사항을 이용자에게 고지하거나 정보통신서비스이용약관에 명시 하여야 한다. 다음 중 잘못된 것은? (5)

① 개인정보관리책임자의 성명,소속부서,직위 및 전화번호 기타 연락처
② 개인정보의 수집목적 및 이용목적
③ 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공목적 및 제공할 정보의 내용
④ 제30조 제1항, 제2항 및 제31조 제2항의 규정에 의한 이용자 및 법정대리인의 권리 및 그 행사방법
⑤ 개인정보 보호를 위하여 필요한 사항으로서 정보통신부장관이 정하는 사항

40. 정보통신기반보호법에 따르면 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다. 이때 관리기관의 장은 일정 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있는 바, 그에 속하지 아니 하는 기관은? (2)

① 한국정보보호진흥원
② 국가정보원
③ 대통령령이 정하는 기준을 충족하는 정보공유·분석센터
④ 정보통신기반보호법의 규정에 의하여 지정된 정보보호전문업체
⑤ 정부출연 연구기관등의설립·운영 및 육성에 관한법률의 규정에 의한 한국전자통신연구원