정보보호전문가(SIS)
1급, 2급
공개 기출문제('05)

○ 2005년 1~3회차 시험문제 중 일부를 공개합니다.
○ 정답은 필기문제와 단답형 문제만 공개합니다.
○ 서술형과 실무형 문제는 채점기준에 따라 부분점수가 인정됩니다.

2006. 02.

KISA 한국정보보호진흥원 Korea Information Security Agency
한국정보통신교육원

SIS 1급 시스템 보안

1. 유닉스의 특징이 아닌 것은?

① 다중 작업 기능을 제공한다.
② 다중 사용자 기능을 제공한다.
③ 이식이 타 운영체제보다 떨어진다.
④ 계층적 트리 구조 파일 시스템을 가진다.
⑤ 하드웨어 메모리 이상의 가상 메모리 사용이 가능

2. 다음 중 알고리즘 종류와 설명이 바르게 짝지어 진 것은?

① FCFS : FIFO라고도 하며, 준비상태 큐에 들어온 프로세스들 중에서 우선순위가 가장 높은 프로세스를 먼저 CPU에 할당하여 실행시키되, 새로 들어온 것과 선점되어 다시 들어온 것 모두를 대상으로 선택하는 기법
② SRT : 준비상태 큐에서 기다리고 있는 Job들 중에서 실행시간이 가장 짧은 프로세스를 먼저 실행시키는 기법
③ SJF : 새로 도착한 프로세스와 선점되어 다시 준비된 프로세스를 포함하여, 처리가 완료되는데 가장 짧은 시간이 소요될 프로세스를 먼저 CPU에 할당하여 실행하는 기법
④ HRN : Time Sharing System을 위해 고안된 방식, 긴 작업에는 불리하고 짧은 새로운 작업에 대해서는 유리한 SJF의 단점을 개선한 방법
⑤ Round Robin : 성능은 Time Quantum의 크기에 큰 영향을 받는데, Time Quantum이 무한대일 경우 FCFS 기법과 같아지고, 너무 작으면 문맥교환이 자주 일어남.

3. 웹 브라우저를 사용하면 쿠키, 히스토리, 캐시 등과 같은 흔적이 남는다. 이에 대한 설명 중 잘못된 것을 고르시오.

① 쿠키에는 개인ID와 비밀번호, 방문한 사이트 등의 정보가 담겨 있어, 사용자의 다음 방문시 웹서버는 그가 누구인지 등에 대하여 바로 파악할 수 있다.
② 쿠키는 암호화되어 있으므로, 지우지 않아도 무방하다.
③ 히스토리는 사용자가 방문한 웹사이트의 내역을 저장하고 있으므로, 사용자의 웹서핑 기록을 알아낼 수 있다.
④ 캐시는 임시 인터넷 파일이라고도 하며, 웹페이지의 로딩 시간을 줄이기 위해 이미지 파일과 같은 용량이 큰 파일을 하드디스크에 저장시켜놓은 것이다.
⑤ 하드디스크에 담겨있는 캐시의 내용을 보면, 방문한 사이트와 그 곳에서 다운로드한 파일 목록까지 확인할 수 있다.

4. 다음은 포트스캔에 대한 설명이다. 이중 잘못된 것을 고르시오.

① 공격하려는 컴퓨터에서 열려있는 포트를 검색하는 것이다.
② 포트를 검색하기 위해서는 먼저 IP를 알아내야 한다.
③ 컴퓨터에 존재하는 포트는 232개이다.
④ TCP 또는 UDP 포트가 어떤 서비스를 하고 있거나 LISTENING 상태이면 이 포트는 열려있다.
⑤ 포트 검색은 자신의 시스템의 취약점을 스스로 분석하는데도 사용할 수 있다.

5. 다음은 누킹에 대한 설명이다. 이중 잘못된 것을 고르시오.

① 목표 시스템을 다운 시키는 것으로, 작업 중이던 자료의 손실, 재부팅이 필요한 악성 코드를 실행시키기 위한 방법으로도 사용될 수 있다.
② DoS의 한 방법이다.
③ 사용자의 IP 주소와 누킹 소프트웨어를 사용해서 사용자의 시스템을 다운 시킬 수 있다.
④ 사용되는 소프트웨어로 Vconnect, Cgsioob 등이 있다.
⑤ 목표 시스템에 누킹 소프트웨어가 설치되어 있어야만 공격이 가능하며, 공격자는 백도어 등을 이용해서 목표 시스템에 누킹 소프트웨어를 설치한 후 공격을 시도한다.

6. 새롭게 부임된 서버 관리자 A씨는 PATH의 설정으로 보고 지난 서버 관리자가 실수 한 것을 알아냈다. 다음은 PATH 설정이다.

PATH= ./ :/bin:/home/user1 이 경우 (①)가 문제되어 (②) 디렉터리에 있는 트로이화된 명령어(예.ls)가 실행 될 경우 문제가 심각해진다.

① ①/home/user1 ②홈
② ①/home/user1 ②루트(/)
③ ① ./ ②현재
④ ① ./ ②루트(/)
⑤ ① ./ ②/tmp

7. Apache 1.3.12 이후 버전을 사용하는 웹 서버 관리자 A씨는 Apache의 버전 노출을 막고자 한다. 다음 중 Server Tokens 디렉티브를 이용하여 httpd.conf에 추가해 주어야 할 키워드는 무엇인가?

① NoVersion
② Minimal
③ Prod
④ OS

⑤ Full

8. 다음은 리눅스의 ps명령에 aux인자를 주어 실행된 결과이다. 이에 대한 설명으로 틀린 것을 고르시오.

```
USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
root       1  0.0  0.2 1412  468 ?        S  Oct06 0:05  init[5]
```

① USER : 프로세스 소유자의 로그인 이름
② STAT : 현재 프로세스의 상태
③ VSZ : 프로세스가 사용하는 파일의 I-NODE 번호
④ TTY : 프로세스 제어 터미널
⑤ COMMAND : 프로세스의 이름과 명령 라인 인자

9. 다음 중 시스템 로그 파일에 대한 설명으로 잘못된 것을 고르시오.

① cron 파일은 주기적으로 자주 실행되는 cron 프로그램에 대한 로그파일이다.
② xferlog 파일은 ftp 서비스 접속에 관한 사항을 기록하는 파일이다.
③ wtmp 파일은 utmp와 같은 데이터 구조를 사용하고 있으며, 주로 login이나 reboot와 관련된 정보를 담고 있다.
④ utmp 파일은 현재 사용자의 리스트를 저장하는 파일이다. w, who와 같은 명령을 통해 현재 사용자 상황을 파악할 수 있다.
⑤ dmsg 파일은 시스템 종료시에 발생하는 콘솔 출력 메시지들을 기록한 파일이다.

10. 다음은 보안책임을 맡은 서버 관리자의 업무를 나열한 것이다. 이중 부적합한 것을 고르시오.

① 시스템 로그 파일들을 주기적으로 분석해서 서버의 상태 및 공격 시도가 있었는지를 분석하여 이에 대처한다.
② 서버 관리자는 서버에서 반드시 필요한 서비스 포트는 활성화 시키고 불필요한 서비스 포트들을 비활성화 시켜야 한다.
③ 패치가 이루어지지 않았거나 오래된 보안상의 약점을 가진 소프트웨어를 직접 찾아낼 수는 없으므로, 이에 대해서 사용자에게 주지시킨다.
④ 외부 공격자의 공격을 막기 위해 안전한 방화벽 시스템을 구축한다.
⑤ 안티 바이러스 프로그램을 주기적으로 업데이트 시킨다.

11. 네트워크 스캐닝 기법 중 TCP 패킷에 URG(긴급), ACK(확인), RST(연결 재설정), SYN(접속 동기화 요청), FIN(연결 종료)과 같이 모든 플래그를 셋팅해서 보내는 스캐닝 기법은 무엇인가?

① TCP SYN 스캔
② TCP connect() 스캐닝
③ NULL 스캐닝
④ SYN/ACK 스캐닝
⑤ XMAS(크리스마스 트리) 스캐닝

12. 다음의 보안 점검 도구와 그에 대한 설명이 틀린 것은?

① COPS - 잘못된 SUID 비트, 패스워드, 체크섬 등을 체킹한다.
② SATAN - 네트워크의 취약점을 찾아주는 네트워크 스캐너이다.
③ SAINT - CGI 취약점, DoS취약점, ssh 취약점등을 찾아주는 도구이다
④ John The Ripper - 패스워드 점검 도구이다.
⑤ Tripwire - clinet/server 방식으로 동작하며 파일 암호화 도구이다.

13. 인터넷 익스플로러에서는 보안 설정을 지정할 웹 컨텐츠 영역을 지정할 수 있다.다음 중 지정할 수 없는 영역은 어느 것인가?

① 인터넷
② 로컬 인트라넷
③ 신뢰할 수 있는 사이트
④ 보안 등급 지정 가능한 사이트
⑤ 제한된 사이트

14. UNIX 또는 리눅스 시스템에서 똑 같은 작업을 사용자가 지정된 시간에 반복 작업하기 위해서 cron 테이블을 작성한다. 만약 사용자가 매주 토요일 오전 10시 정각에 'mytest' 라는 프로그램을 주기적으로 수행시키기 위해 작성한 cron 테이블 내용 중 맞는 것은?

① 0 10 6 * * mytest
② 0 10 * * 6 mytest
③ 0 10 * 6 * mytest
④ * * * 10 0 mytest
⑤ 0 10 6 * * mytest

15. 사용자가 지신의 홈 디렉토리 내에서 새롭게 생성되는 서브 파일에 디폴트 파일 허가권을 파일 소유자에게는 읽기와 쓰기, 그룹과 other에게는 읽기만 가능하도록 부여하고 싶다. 로그인 쉘에 정의해야 되는 umask의 설정 값은 어느 것인가?

① umask 133
② umask 644
③ umask 022
④ umask 330
⑤ umask 033

16. 다음 중 페이지 교환 알고리즘이 아닌 것은?

① FIFO : 주기억 장치에 가장 먼저 들어와서 가장 오래 있었던 페이지를 교체하는 기법
② LFU : 사용 빈도가 가장 적은 페이지를 교체하는 기법
③ NRU : 최근에 사용하지 않은 페이지를 교체하는 기법
④ LRU : 최근에 가장 오랫동안 사용되지 않은 페이지를 교체하는 기법
⑤ MFU : 사용 빈도가 가장 많은 페이지를 교체하는 기법

17. 다음은 계정 보안 방법에 관한 설명이다. 틀린 것은?

① 사용자 패스워드에 대한 암호화를 위해 MD5를 사용한다.
② SSL, PGP와 같은 암호화 프로토콜을 사용한다.
③ 시스템관리의 편의를 위해 계정과 패스워드를 일치시킨다.
④ PAM모듈을 이용하여 특정 그룹 및 계정의 접속을 제한한다.
⑤ 시스템에서 기본적으로 사용하지 않는 계정을 삭제한다.

18. 다음 지문이 설명하는 E-mail 공격 방법은 무엇인가?

> 메일 열람시 HTML 기능이 있는 E-mail 클라이언트나 웹 브라우저를 이용하는 사용자를 대상으로 하는 공격기법으로 클라이언트 프로그램의 버그나 시스템 버그로 인한 것이 아니므로 보안 패치로 해결되지 못한다.

① 액티브 컨텐츠 공격
② 버퍼 오버플로우 공격
③ 트로이잔 목마 공격

④ 메일용 쉘 스크립트 공격
⑤ 코드기반 공격

19. 다음 중 크래킹의 기법과 거리가 먼 것을 선택하시오.

① 시스템의 사용자나 관리자를 속여서 시스템에 접근할 수 있는 권한을 얻어 침투하는 것
② 정당한 사용자의 정보를 훔쳐내어 사용자를 사칭하는 방법
③ 사용자와 사용자 접속 사이트의 매개자 역할을 하면서 사용자의 모든 정보를 알아내는 법
④ 대상 시스템이나 시스템의 사용자가 특정한 자원에 접근하는 것을 방해
⑤ 시스템이나 네트워크의 정상적인 동작과 서비스를 방해하거나 정지시키는 행위

20. 웹 기반 메일 서비스의 보안을 강화시키기 위해서 SSL(Secure Socket Layer)를 사용할 수 있다. SSL의 실제 동작과정을 순서에 맞게 나열한 것은?

가. 클라이언트는 인증서가 CA로부터 서명된 유효한 것인지를 확인
나. 클라이언트는 공개키(Public Key)를 사용해서 랜덤 대칭 암호화키를 비롯한 URL, Http 데이터들을 암호화해서 전송
다. 클라이언트는 SSL로 암호화된 페이지를 요청
라. 서버는 요청받은 URL에 대한 응답을 클라이언트로부터 받은 랜덤 대칭 암호화키를 이용하여 암호화한 후 클라이언트에게 전송
마. 서버는 공개키를 인증서와 함께 클라이언트에게 전송
바. 서버는 비밀키(Private Key)를 사용해서 랜덤 대칭 암호화키를 비롯한 URL, Http 데이터들을 복호화

① 가 → 마 → 나 → 다 → 바 → 라
② 다 → 마 → 가 → 나 → 바 → 라
③ 다 → 라 → 나 → 가 → 바 → 마
④ 다 → 나 → 바 → 가 → 마 → 라
⑤ 다 → 바 → 나 → 라 → 가 → 마

21. 방화벽의 이점에 대한 설명으로 옳지 않은 것은?

① 위협에 취약한 서비스에 대한 보호를 제공한다.
② 호스트 시스템에 대한 액세스를 제어한다.
③ 보안 관리가 분산된다.
④ 네트워크 사용에 대한 로깅과 통계 자료를 제공한다.
⑤ 네트워크 액세스 제어 정책에 대한 구현을 제공한다.

22. 다음 중 키로그 프로그램에 대한 내용을 잘못 설명한 것은 무엇인가?

① 키로그 프로그램은 사용자의 키 입력을 텍스트 파일로 받아서 정보를 빼내는 것이다.
② 키로그 프로그램은 트로이 목마의 기능보다 키 입력 내용의 검출 기능이 강화된 것이다.
③ 로그 파일은 임의의 디렉토리를 지정하므로 찾기가 불가능하다.
④ 키로그 프로그램을 제거하고자 하면 regedit를 실행하여 KiD Vid 항목을 제거하면 된다.
⑤ 키로그 프로그램을 설치한 후 레지스트리에 등록해야 한다.

23. NCSC(National Computer Security Center)는 컴퓨터 시스템에서 정부, 기업, 개인 유저들의 Private Data에 대한 보호 평가 기준으로 다음과 같은 보안 등급(Security Ratings)을 만들었다. 이중 C2 등급은 범용 OS를 위해 충분한 안전성을 제공하는 등급으로 간주된다. 다음 보기 중 C2 등급의 요구사항을 올바로 나열한 것을 고르시오.

Rating	Description
A1	Verified Design
B3	Security Domains
B2	Structured Protection
B1	Labeled Security Protection
C2	Controlled Access Protection
C1	Discretionary Access Protection (obsolete)
D	Minimal Protection

① Secure Network Management Trusted Facility Management
② Discretionary access control Security auditing
③ Trusted path functionality Security auditing
④ Trusted path functionality Trusted Facility Management
⑤ Object reuse protection Trusted path functionality

24. 파일의 무결성을 검사해 주는 도구들에 대해 설명한 것이다. 이중 올바른 것을 고르시오.

① fport - 주요한 파일들에 대한 체크섬을 점검하여 이전의 점검 결과와 비교하여 변동사항 이 있을 경우, 관리자에게 통지함
② aide - tripwire를 대신할 수 있는 도구로서 message digest 알고리즘을 사용하여 파일의 변조를 점검하는 도구
③ fcheck - 유닉스 파일시스템의 변조유무를 점검하기 위한 shell script 도구이며, 관리자에게

파일의 변조 여부를 통지하는 기능이 있음
④ claymore - cron 데몬을 이용하여 실시간으로 파일시스템의 변조유무를 점검하는 도구
⑤ slipwire - 파일의 MD-5 해쉬값을 비교하여 변경될 경우, 사용자에게 이를 통지하는 기능이 있음

25. 시스템 침입 흔적을 조사하는 도구로서 실행 중인 프로세스가 참조하는 파일에 대한 정보를 제공하며 특정 포트를 사용하는 프로세스의 정보도 알 수 있어 해킹 당한 시스템을 조사할 때 유용한 툴은 무엇인가?

① lsof
② fport
③ stjude
④ TCP wrapper
⑤ kstat

26. 다음에서 서로 관계가 가장 부적합한 것끼리 연결된 것 하나를 고르시오.

(1) 다중등급보안(multilevel security)	(가) Bell & LaPadula Model
(2) 무결성(Integrity)	(나) 보안 레이블링(Security Labeling)
(3) 감사정보(Audit Log)	(다) Covert Channel(비밀 통로)
(4) 강제적 접근제어(Mandatory Access Control)	(라) Biba 모델
(5) 신뢰경로(Trusted Path)	(마) 패스워드 변경

① (1) → (나)
② (2) → (라)
③ (3) → (다)
④ (4) → (가)
⑤ (5) → (마)

27. 다음은 크래커 A가 남긴 C소스 코드와 바이너리 파일이다. 이에 대한 설명으로 적합한 것은?

```
[user@localhost test]$ ls -l
total 20-rwsr-xr-x    1 root     root        13923 Oct  7 21:13 test
-rw-rw-r--   1 root     root                   88 Oct  7 21:12 test.c
[user@localhost test]$ cat test.c
#include <stdlib.h>
void main()
{
setuid(0);
setgid(0);
system("/bin/sh");
}
```

① setgid 시스템 콜의 인자를 0으로 준 것으로 보아 Race condition 기법의 공격이다.
② /bin/sh를 실행시키는 것으로 보아 sniffing 기법이다.
③ setuid 시스템 콜의 인자가 0이고 컴파일된 바이너리 파일의 퍼미션이 4755인 것으로 보아 루트 권한을 탈취하는 백도어이다.
④ 쉘 코드가 있는 것으로 보아 stack overflow 기법이다.
⑤ main 함수의 리턴형태가 void 이므로 Format String Attack으로 보인다.

28. 국제공통평가기준(Common Criteria)과 보호 프로파일(Protection Profile)의 설명으로 잘못된 것은 ?

① 공통평가기준 Part 3에서 보호 프로파일을 작성하는 방법을 제공하고 있다.
② 보안 요구사항을 클래스-패밀리-컴포넌트의 순으로 계층화하고 있다.
③ 정보보호시스템의 개발자와 평가자가 보호 프로파일을 만들 수 있으며, 사용자는 평가 제 품을 사용할 권리만을 갖는다.
④ EAL1부터 EAL7까지의 7개 계층적인 평가등급이 TOE(Target of Security)의 보증을 위해 정의된다.
⑤ 공통평가기준은 일반모델, 보안기능요구사항 및 보증요구사항으로 크게 구성된다.

29. 아래의 예문의 취약점을 이용해 공격하는 방법은?

> 컴퓨터 프로그램의 입력값 크기를 제한하지 않았거나 또는 입력값의 크기를 확인하는 과정을 설정하지 않았을 때 발생하는 취약점

① 서비스 거부 공격
② 버퍼 오버플로우 공격
③ 비동기 공격
④ 컴퓨터 바이러스
⑤ 트로이 목마

30. 리눅스 시스템에서 실행되던 파일이 스왑되지 않고, 항상 주 메모리에 남아 있도록 하기 위해 실행 파일의 속성에 sticky 비트를 세트한다. 자신의 실행 파일 이름이 aaa일 때, 다음 중 sticky bit를 세트하도록 허가권을 부여한 명령어는 어느 것인가?

① chmod 1700 aaa
② chmod 2700 aaa
③ chmod 4700 aaa
④ chmod 6700 aaa
⑤ chmod 700 aaa

31. 어떤 운영체제에서 아래와 같이 3개의 프로세스가 동시에 도착하였다. SJF(Shortest Job First) 스케줄링 알고리즘에 대하여 프로세스의 평균 대기시간(Average waiting time)을 구하라.

Process	CPU Burst time (ms)
P1	9
P2	23
P3	3

① 3 ms
② 4 ms
③ 5 ms
④ 9 ms
⑤ 11.7 ms

32. 임계영역과 관련하여 다중 프로세스들 간의 상호배제를 위하여 만족되어야 할 요구 조건과 가장 먼 것은?

① 임의의 시점에 반드시 하나의 프로세스만이 임계영역에 있어야 한다.
② 임계영역에 접근하고자 하는 프로세스의 수행이 무한히 미루어져서는 아니 된다.
③ 사용되고 있지 않은 임계영역에 대한 사용 요구는 즉시 받아 들여져야 한다.
④ 우선순위가 가장 높은 프로세스는 항상 언제라도 임계영역에 들어갈 수 있다.
⑤ 임계영역에서의 수행 시간은 한계가 있어야 한다.

33. 다음 중 포트 스캔의 설명으로 틀린 것은?

① 포트가 열려 있는 것을 확인하면 시스템의 활성화 정보도 얻을 수 있다.
② 열린 포트라 하더라도 아무 응답이 없는 경우가 있다.
③ 상대방에 세션 로그를 남기지 않기 위해서는 포트 활성화 확인 후 RST를 보낸다.
④ 닫힌 포트에서는 TCP의 SYN 연결요청에 대하여 ACK가 오지 않는다.
⑤ TCP의 NULL 패킷으로도 포트의 활성화 여부를 알아 낼 수 있다.

34. 어떤 시스템을 포트 스캔하였더니 다음과 같은 포트들이 열려 있었다. 윈도우 운영체제임을 알려주는 단서의 역할을 하는 것은?

① 25
② 21
③ 80
④ 161
⑤ 3389

35. 다음 프로그램 중 무결성 검사 기능을 가지지 않은 것을 고르시오.

① TAMU
② Tripwire
③ ATP
④ Hobgoblin
⑤ Crack

36. 리눅스 서버에서 아래의 설정에 대한 설명 중 바르게 설명한 것은 무엇인가?

<예시> echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects

① 해당 시스템을 통해 다른 시스템으로 패킷이 포워딩되지 않도록 하는 설정이다.
② 스푸핑된 패킷이나 소스라우팅에 대해 로그를 남기는 설정이다.
③ 공격자가 임의의 라우팅 테이블을 변경하는 공격에 대한 대응 설정이다.
④ Syn flooding 공격에 대한 대응 설정이다.
⑤ Smurf 공격에 대한 대응 설정이다.

37. 강제적 접근제어(Mandatory Access Control)에서 사용하는 접근제어 방법과 가장 관계가 깊은 것은?

① 허가 비트(Permission Bit)
② 접근제어 목록(Access Control List)
③ Bell & LaPadula 모델
④ 역할 기반 접근제어(Role Based Access Control) 모델
⑤ 접근 행렬(Access Matrix)

38. UNIX 시스템에서 다음의 chmod 명령어 실행 후의 파일 test1의 허가 비트(8진법 표현)는?

<예시>
% ls - l test1
- rw-r- -r- - 1 root user 2320 Feb 9 13:20 test1
% chmod o-r test1
% chmod g-r test1

① 644
② 244
③ 600
④ 640
⑤ 744

39. 컴퓨터 사용자가 UNIX OS를 사용하는 서버에 로그인(log-in)했을 때 로그인한 사용자 관련 정보가 utmp, wtmp, lastlog 등의 로그 파일에 기록된다. 로그 파일에 대한 내용 중 틀린 것은?

① utmp 파일은 현재 컴퓨터를 사용하고 있는 사용자 정보를 저장한다.
② wtmp 파일은 모든 사용자들의 로그인과 로그아웃에 대한 정보를 저장한다.
③ 원격지에서 로컬 호스트로 접근하는 경우에는 로그가 생성되지 않는다.
④ wtmp 파일은 디스크 절약을 위해 주기적으로 기존 정보를 제거할 필요가 있다.
⑤ lastlog 파일은 사용자의 가장 최근 로그인 정보를 저장한다.

40. 시스템 로그 파일은 사용자의 정보를 기록하는 중요한 파일이다. 침입자가 있을 경우 그를 추적하거나 접근한 내용을 검사할 수 있는 정보를 제공하여 주기 때문에 침입자는 로그 파일에 접근하여 자신의 기록을 삭제하려고 한다. 침입자로부터 로그 파일을 보호하는 방법 중 가장 옳지 못한 것은?

① 로그 파일을 가능한 한 여러 곳에 만든다.
② 과도한 크기에 대비하여 로그 파일의 크기는 일정 용량으로 제한해야 한다.

③ 로그 파일의 권한을 write only로 설정해야 한다.
④ 로그 파일의 내용을 암호화하여 기록한다.
⑤ CD-ROM 등에 기록하는 다른 시스템에 별도로 보관한다.

41. 다음에 설명하는 시스템으로 가장 적합한 것은?

<예시>
불법적 침해 및 해킹에 대한 상세한 로그 및 휘발성 미디어 정보에 대한 수집, 인증, 문서화, 증거로서의 제출, 분석 및 해석방법과 원인분석 방법에 대한 종합적인 작업을 포함한다.

① Intruder Tracing System
② Enterprise Log Management System
③ Computer Forensic System
④ Honey-pot System
⑤ Intrusion Prevention System

42. 리눅스 파일시스템에서 SetUID, SetGID, Sticky 비트의 역할로 틀린 것은?

① 파일에 SetUID 비트가 설정되어도 사용자는 겉으로 확인할 수 없다.
② 파일에 대한 접근권한이 '7777'이면 문자로는 'rwsrwgrwt'로 표현된다.
③ SetUID 비트가 세트된 파일을 실행하면 파일의 소유자 권한으로 수행된다.
④ SetUID 비트가 세트되어 있어도 루트권한으로 실행되는 일은 없다.
⑤ SetUID 비트가 세트되어 실행된 파일의 UID는 내 패스워드 파일 내의 ID이다.
43. 다음 중 백도어를 설치할 수 있는 도구는 무엇인가?

① Libpcap
② Solarwinds
③ Sing
④ NetBus
⑤ Whois

44. 다음 중 패킷 필터링 시에 패킷 헤더에서 검출할 수 있는 정보가 아닌 것은?

① 소스 IP 주소
② 목적지 IP 주소
③ TCP/UDP 소스 포트
④ ICMP 메시지 타입
⑤ 패킷의 생성 시간

45. 파일 시스템 점검의 명령어는?

① chgrp
② userdel
③ mount
④ fsck
⑤ df

SIS 1급 어플리케이션 보안

1. TFTP에 대한 설명으로 올바르지 않은 것은 ?

① TFTP는 사용자 인증과정을 거치지 않고 곧바로 원격 파일을 읽거나 저장할 수 있는 프로토콜이다.
② TFTP는 보안상 별로 권장할 만한 서비스가 아니다.
③ 디스크 없는 호스트가 부팅 이미지를 읽어 들여야 하는 경우처럼, TFTP가 꼭 필요한 경우도 있다.
④ TFTP 서비스가 허가된 시스템은, 전체 파일 시스템에 대하여 동일한 접근 권한이 부여된다.
⑤ TFTP 서비스는, TCP Wraper를 이용하여 IP별로 접속 요청을 받을 것인지, 받지 않을 것인지를 설정함으로써 보안을 강화할 수 있다.

2. 다음 중, sendmail 프로토콜에 대한 설명으로 올바르지 못한 것은 ?

① Sendmail은 발신자의 호스트 이름을 RFC1413: Identification protocol을 이용하여 확인한다.
② “Received” 헤더에는 거짓 정보가 들어갈 수 없다.
③ “Received” 헤더에는 sendmail이 확인한 발신자 정보가 기록된다.
④ “From” 헤더에는 거짓 정보가 들어갈 수 없다.
⑤ “ From” 헤더에는 발신자가 입력한 호스트 이름이 그대로 나타난다.

3. 다음 중 안전한 웹서버를 만들기 위한 방법으로 올바르지 못한 것은 ?

① Cgi 프로그램은 쉘 스크립트로 구성된 것 보다는 컴파일된 것을 사용하도록 한다.
② 컴파일한 Cgi 프로그램의 실행 권한은 755로 준다.
③ 쉘 명령어를 실행해야 하는 경우 절대경로로 실행한다.
④ CGI 프로그램의 설치는 일반 사용자에게 허가하지 않도록 한다.
⑤ 웹 서버의 자식 프로세스는 루트 권한으로 실행하지 않는다.

4. 다음 중 SMTP VRFY 명령어에 대한 설명으로 올바른 것은 무엇인가 ?

① VRFY 명령어는 사용자 이름과 이메일 주소가 적정한지를 확인해주는 명령이다.
② VRFY 명령어는 사용자 이름과 이메일 주소를 확장하여 알려주는 명령이다.
③ VRFY 명령어는 smtp 프로토콜의 적정성을 확인해 주는 명령이다.
④ VRFY 명령어는 sendmail.cf의 존재를 알려주는 명령이다.
⑤ VRFY 명령어는 telnet 접속 여부를 알려주는 명령이다.

5. 다음 중 전자화폐의 주요기능에 되지 못하는 것은 무엇인가?

① 유동성(circulativity)
② 범용성(universality)
③ 실명성(real naming)
④ 결제완료성(finality)
⑤ 연속적 양도 가능성(successive transferability)

6. 여러 가지 공격유형에 대해 방어할 수 있는 보안 대책을 숙지해야 한다. 다음 중 여러 가지 공격 중에서 발생할 수 있는 보안 대책이 아닌 것은 무엇인가?

① Anonymous FTP 보안 대책은 Anonymous 사용자의 루트 디렉토리, bin, etc, pub 디렉토리의 소유자와 퍼미션을 정확히 해야 한다.
② Anonymous FTP 보안 대책은 $root/etc/passwd 파일에서 anonymous ftp에 불필요한 항목을 제거한다.
③ TFTP보안 대책은 TFTP가 불필요한 경우 제거한다.
④ TFTP보안 대책은 TFTP가 필요한 경우에는 secure mode로 운영한다.
⑤ FTP는 자체적으로 보안 취약점을 가지고 있으므로 패치는 빈번히 시행하지 않는다.

7. PGP(Pretty Good Privacy)에 대한 설명 중 틀린 것은?

①IDEA 암호화 알고리즘을 이용하여 암호화 한다.
②세션키로서 128비트 랜덤키를 사용한다
③PGP는 메시지 인증 기능도 지원한다.
④발신자로부터 메시지를 받으면 자신의 비밀키를 이용해서 세션키를 복구한다.
⑤수신자는 세션키를 자신이 생성한다.

8. 다음은 sendmail 8.9에서 사용하는 '액세스 데이터베이스 (access database)'에 대한 설명이다. 올바르지 못한 것은 무엇인가 ?

① '액세스 데이터베이스'를 이용함으로써 메일서버가 특정 도메인으로부터 오는 메일들을 받지 않도록 할 수 있다.
② '액세스 데이터베이스' 파일은 sendmail 프로그램이 쉽게 검색할 수 있도록 텍스트 형태가 아닌 DB 형태로 구성하는 것이 좋다.
③ Sendmail과 같이 배포되는 makemap 이란 프로그램은, 텍스트 형식의 파일을 DB 형태로 변환해 준다.
④ '액세스 데이터베이스' 내의 'spammer@spam.com REJECT"의 의미는 spammer@spam.com에서

오는 메일은 거절하라는 의미이다.
⑤ '액세스 데이터베이스' 내의 'spam.com REJECT"의 의미는 spam.com 도메인에서 오는 메일 중 일부는 거절하라는 의미이다.

9. S/MIME(Secure/Multipurpose Internet Mail Extension)은 기존 전자우편 보안시스템의 문제점인 PEM 구현의 복잡성, PGP의 낮은 보안성과 기존 시스템과의 통합이 용이하지 않다는 점을 보완하기 위해 IETF의 작업그룹에서 RSADSI(RSA Data Security Incorporation)의 기술을 기반으로 개발된 전자우편 보안이다. S/MIME이 달성하고자 하는 목표가 아닌 것은?

① 강력한 암호화
② 디지털 서명
③ 상호 운영성
④ 키 관리의 간소화
⑤ 수출 가능성

10. S-HTTP의 필수 헤더라인은 두 가지이다. 이에 대한 내용으로 옳지 않은 것을 고르시오

① S-HTTP 메시지 내에 들어 있는 내용의 유형을 나타내는 라인과 이용된 일반적인 암호 구현을 나타내는 라인이다.
② 옵션형 헤더들의 용도는 포장된 데이터의 데이터 재현 방식을 나타낸다.
③ 세션키 전송 및 포장 된 데이터와 관련된 기타 정보를 표시한다.
④ MAC 헤더에 따라 디지털 서명 전용, 암호화 전용, 서명과 암호화 모두 이용이 가능하다.
⑤ 반드시 서명과 암호화가 이용되어야 한다.

11. 다음은 XML 보안에 관한 내용이다. 틀린 것은?

① 디지털 서명을 사용하여 SOAP 본문 요소가 전송 중에 손상되지 않았는지 확인할 수 있습니다.
② XML에서 사용된 데이터를 보호하려면 데이터 저장소를 방화벽 내부에 보관하는 것이 좋다.
③ XML은 사용자에 대한 인증만을 제공한다.
④ XML에서는 기존의 PKI 기반 구조를 이용할 수 있다.
⑤ XML 문서의 암호화 기능이 제공된다.

12. MySql에서 GRANT 선언문은 새로운 사용자를 추가하고, MySQL에 대한 액세스를 허가하는 데 쓰인다. 다음 예제에 대한 설명으로 올바르지 않은 것은 무엇인가?

```
GRANT SELECT (title, authirID) ON Library.Book TO andy;
```

① andy라는 사용자에게 권한을 부여한다.
② Library라는 데이터베이스에 있는 Book 테이블에 접근이 가능하다.
③ SELECT 선언문으로 테이블에 있는 데이터를 읽을 수 있는 권한이다.
④ Library라는 데이터베이스에 있는 Book 테이블에서 title과 authorID에 대한 SELECT 권한을 부여한다.
⑤ SELECT 선언문은 열, 테이블, 데이터베이스에 접근이 가능하다.

13. X.500 인증서 V3의 각 필드에 대한 다음 설명 중 옳지 않은 것은?

① Signature Algorithm Identifier: CA가 인증서를 서명하기 위하여 사용한 암호알고리즘 정의
② Issuer Name: 인증서를 발급하고 서명한 CA명
③ Valid Period: 인증서가 유효한 기간을 설명, 유효기간이 지나면 CA는 인증서 정보를 삭제함
④ Subject Name : 인증서의 소유자명으로서, 인증서 공개키 항목의 공개키 소유자를 의미함
⑤ Version : 인증서 형식의 연속된 버전의 구분

14. 인터넷 보안 프로토콜에 대한 설명 중 올바른 것은?

① IPSec은 인터넷 프로토콜의 설계시의 문제점인 IP Spoofing, Sniffing 등에 대한 취약점 때문에 개발되었다고 볼 수 있다
② SSL은 넷스케이프사에서 개발된 웹보안 만을 위한 프로토콜이다.
③ TLS는 IETF에서 SSL에 대항하기 위하여 제정된 표준 프로토콜이다.
④ SSL에서는 SSL동작 관리를 위한 프로토콜로서 SSL Record Protocol 이 있다.
⑤ CRL은 인증서를 이용한 인터넷 표준 프로토콜이다.

15. 암호프로토콜 서비스에 대한 설명이다. 맞지 않는 것은 무엇인가?

① 비밀성(Confidentiality) : 자료 유출 방지
② 무결성(Integrity) : 메시지 변조 방지
③ 접근제어(Access Control) : 프로토콜 데이터 부분의 접근제어
④ 부인봉쇄(Non-Repudiaton) : 송수신 사실 부정방지
⑤ 인증(Authentication) : 정확한 출처의 확인

16. 다음은 방화벽(침입탐지시스템, Firewall)에 대하여 설명을 한 것이다. 잘못된 설명은 어느 것인가 ?

① 프락시 서버는 방화벽이 설치되어 있는 호스트에서 동작하는 서버로서, 방화벽 내에 있는 사용자들에게 방화벽 밖에 있는 서버로의 자유로운 인터넷 서비스를 제공받기 위한 수단으로 이

용되는 서버이다.
② 방화벽은 해킹 등 외부로의 정보 유출을 막기 위한 장치로 내부 네트워크와 외부 네트워크 경계에 설치되어야 한다.
③ 패킷 필터링(packet filtering) 방식은 응용 계층에서 동작하며, 주로 WWW 서비스를 위한 방화벽 기능을 수행한다.
④ 베스천 호스트(Bastion Host)는 네트워크 보안에 있어서 가장 강력한 부분으로 방화벽 관리자에 의해 정해지는 시스템이다.
⑤ 방화벽의 종류는 패킷 필터링(packet filtering) 방식, 회선 게이트웨이(circuit gateway) 방식, 그리고 응용 게이트웨이(application gateway) 방식 등 이다.

17. 공격자가 IP 원천지 주소만을 이용하여 송신자를 인증하는 수신 시스템에 침입하기 위하여 다른 신뢰성 있는 호스트로 위장하는 공격 방식은 ?

① DNS 해킹
② 제3자 인증
③ 패킷 탐지기(스니퍼, sniffing)
④ IP 스푸핑(spoofing)
⑤ 윈속(Winsock)

18. 다음은 SET에서 사용하는 보안 메커니즘을 설명한 것이다. 다음의 설명된 내용이 해당하는 것은 무엇인가 ?

고객의 지불 정보(신용카드 번호 등)는 상점이 알지 못하게 하고, 주문 정보(상품 품목 등)는 은행이 알지 못하게 함으로써 고객의 프라이버시가 보호되도록 한다.

① 전자 봉투(Digital Envelop)
② 인증서(Certificate)
③ 이중 서명(Dual Signature)
④ 해쉬 함수(Hash Function)
⑤ 사용자 인증

19. 전자서명법의 주요 내용이 아닌 것은 ?

① 공인인증기관의 지정, 인증업무준칙, 인증업무의 휴지 및 폐지
② 인증서에 포함될 사항, 인증서의 효력 및 효력정지
③ 전자문서의 시점확인, 전자서명 생성키의 관리
④ 전자서명의 국가간 상호인정
⑤ 비공인 인증기관의 설립 및 지정 방안

20. SSL(Secure Socket Layer)에서 제공되는 정보보호 서비스가 아닌 것은?

① 두 응용간의 기밀성 서비스
② 클라이언트와 서버간의 상호 인증 서비스
③ 교환되는 메시지의 무결성 서비스
④ 상거래에 응용하기 위한 부인 방지서비스
⑤ TCP를 이용하여 신뢰할 수 있는 종단-대-종단 보안서비스

21. 파일 시스템 프로그래밍 보안에 대한 설명 중 잘못된 것은?

① umask가 안전하지 않은 권한으로 설정되어 있을 때, 허가되지 않은 사용자에게 파일 접근이 허가 될 수 있다.
② 임시 파일을 생성하기 위한 /tmp 디렉토리 안에 추가 디렉토리를 생성한다.
③ /tmp 디렉토리 안에 임시파일을 생성하도록 한다.
④ 임시파일을 생성하는 인터페이스를 제공하는 시스템을 사용한다.
⑤ 임시 파일의 이름을 예측할 수 있는 이름으로 생성하지 말고 랜덤하게 생성한다.

22. 다음 보기 중 무선 PKI를 이용한 인증서비스를 받을 때 고려해야 할 사항이 아닌 것은?

① 제한된 입력 및 출력장치를 고려해야 한다.
② 모바일 기기의 CPU성능 및 메모리 용량의 제한을 고려해야 한다.
③ 인증서 검증에 필요한 정보를 최대화 한다.
④ 네트워크 자원의 부족으로 인한 특성을 고려해야 한다.
⑤ 제한된 전원 공급장치의 특성을 고려해야 한다.

23. 다음 중 W-PKI와 M-VPN 에 대한 비교 설명한 것 중 잘못된 것은?

① W-PKI는 불특정 다수의 사람들에게 보안 서비스를 제공해주는 시스템이다.
② M-VPN은 기존의 보안 정책을 적용할 수 있다.
③ W-PKI는 이동통신 서비스 사업자의 네트워크에 영향을 받는 시스템이다.
④ W-PKI는 N/W 보안이 취약하다.
⑤ M-VPN은 특정 사용자를 위한 규모의 응용 서비스다.

24. 다음은 안전한 프로그래밍을 할 때 주의해야 할 사항이 아닌 것은?

① C++로 프로그래밍시 다중상속을 지향한다.
② C로 프로그래밍시 버퍼범위를 검사하지 않는 루틴을 사용하지 않는다.
③ Perl 실행파일을 WWW 서버의 cgi-bin 에 절대 넣지 않는다.
④ CGI프로그래밍시 해석기(interpreter, Perl 이나 csh 같은)를 cgi-bin 에 두지 않는다.
⑤ 응용프로그래밍시 모든 사용자들에게 Root권한을 최대한 보장될 수 있도록 조치한다.

25. 두개이상의 프로세스가 동시에 동작할 경우, 두 대의 프로세스들은 서로 CPU를 선점하기 위하여 경쟁하는 관계가 성립되는데, 이러한 특성을 악용하여 불법행위를 하는 공격을 무엇이라고 하는가?

① 스택 오버플로우 공격(Stack Overflow Attack)
② 힙 오버플로우 공격(Heap Overflow Attack)
③ 서비스거부공격(DOS Attack)
④ 경쟁조건 공격(Race Condition)
⑤ 포맷스트링 공격(Format String Attack)

26. 다음은 FTP 공격에 대한 대처 방안들이다. 올바르지 못한 것은 무엇인가 ?

① FTP 관리자는 사용하고 있는 FTP 서버 프로그램을 항상 최신의 버전으로 유지하도록 해야 한다.
② FTP 관리자는 FTP 취약사항들을 염두에 두고, 설정에 문제가 없는지 주기적으로 점검해야 한다.
③ FTP 관리자는 FTP 프로그램이 실행하면서 만들어 주는 로그를 정기적으로 분석해 보는 것이 필요하다.
④ FTP 프로그램의 로그 분석에는 다양한 스크립트 도구들을 사용하는 것도 권장된다.
⑤ FTP 프로그램의 로그 생성은 시스템의 성능을 현저히 저하시키므로, 사용하지 않는 것이 권장된다.

27. 다음은 sendmail 8.9에서 제공하는 FEATURE 매크로에 대한 설명이다. 이들 중 설명이 올바르지 못한 것은 ?

① FEATURE(‘promiscuous_relay’) - 메일 릴레이를 기본적으로 허용
② FEATURE(‘relay_based_on_MX’) - 송신자의 메일 주소가 메일을 받아들이는 서버가 속 한 로컬 도메인의 것이라면 해당 메일의 릴레이를 허용
③ FEATURE(‘accept_unresolved_domains’) - 제대로 DNS 서비스를 받지 못하는 경우에도 메

일 받기를 허가
④ FEATURE(‘accept_unqualified_senders’) - 온전한 근원지 주소를 가지지 않은 메일들도 받기를 허가
⑤ FEATURE(‘rbl’) - 메일을 보내는 호스트가 rbl (Realtime Blackhole List)에 등록된 호스트인 경우 메일을 거부

28. 메일 시스템에 대한 취약성 중 버그를 이용한 다수의 공격법이 있다. 다음 중 메일 시스템의 버그를 이용한 공격이 아닌 것은?

① 바이러스 공격
② 버퍼 오버플로우 공격
③ 트로이 목마 공격
④ 액티브 컨텐츠 공격
⑤ 셀 스크립트 공격

29. 다음 보기 중 IMAP4과 POP3에 대한 설명으로 틀린 것은?

(약어:SSH (Secure Shell))

① IMAP4은 저속의 회선 환경에서도 간단히 메일헤더만을 전송받아 확인해볼 수 있는 장점을 가지고 있다.
② 일반적인 IMAP4나 POP3은 자체적인 강력한 보안 기능이 없어 연결 시 보안에 취약한 약점을 가지고 있다.
③ IMAP4를 사용하는 서버, 클라이언트 프로그램 사용자는 서버에서 메일을 다운받은 다음 오프라인에서 작업을 해야 한다.
④ 프로토콜에서 지원하는 단순한 암호인증 이외에 암호화된 채널을 SSH 클라이언트를 통해 구현할 수 있다.
⑤ IMAP4와 POP3는 서버가 사용자 확인을 위하여 아이디와 패스워드를 입력 받을 때 버퍼 오버플로우 공격에 취약하므로 최신 버전으로 패치해야 한다.

30. 현재 WWW 서비스에 많이 사용되고 있는 보안 프로토콜인 SSL에 대한 설명으로 틀린 것은?

① SSL은 인증, 무결성, 기밀성을 보장하기 위한 보안 프로토콜이다.
② SSL은 서버와 클라이언트 간에 키 교환 방법을 제공한다.
③ SSL은 디지털 서명과 관련하여 부인방지 서비스를 제공한다.
④ 현재의 웹 서비스에서 SSL을 위해 제공되는 인증 구조는 대부분 인증기관과 사용자들 간에 star 형태의 인증구조 이다.
⑤ 넷스케이프, 인터넷 탐색기 등의 웹 브라우저는 SSL 접속을 위해 다수의 인증기관들에 대한 인증서 정보를 갖고 있다.

31. 다음은 Web에 대한 취약성 및 해결책에 대한 설명이다. 이것 중 잘못된 것은?

① Web 서버도 다른 서버들이 가지고 있는 일반적인 취약성을 모두 가지고 있다.
② Web을 통한 정보의 불법적인 이용을 방지하기 위해서는 우선 서버의 보안 및 접근통제를 통해 사용자의 정보 접근권한을 통제할 필요가 있다.
③ CGI는 사용자와 상호작용을 할 수 있도록 해주는 프로그램이지만 외부에서 실행되기 때문에 특별한 보안대책이 필요하지 않다.
④ 정당한 권한이 있는 사용자가 안전한 스크립트를 작성할 수 있다면 작성된 모든 스크립트에 대한 검토를 통해 보안성을 확보할 수 있다.
⑤ Web 서버가 접근할 수 있는 파일 시스템을 올바로 설정하지 못하면, 공격자가 외부 프로그램을 Web 서버에 올리고, 이것을 실행할 수 있는 취약점이 있다.

32. 다음 S/MIME 설명 중 틀린 것은?

① 메시지 다이제스트를 만들기 위해, DSS 키와 RC5 키쌍을 필수적으로 생성할 수 있어야 한다.
② 디지털 서명을 구성하기 위한 메시지 다이제스트 암호화를 하기 위해 DSS 지원한다.
③ 전송을 위한 세션키 암호화를 위해 반드시 Differ-Hellman를 지원해야 한다.
④ 일회용 세션키로 전송을 위한 메시지 암호화에 3DES를 지원한다.
⑤ X.509 버전 3 공개키 인증서를 사용한다.

33. 다음은 POP 프로토콜에 대한 설명이다. 잘못된 것은?

① POP은 클라이언트/서버형 프로토콜이다.
② 클라이언트에서 POP3 데몬을 통해 메일을 직접 내려 받는다.
③ POP3 데몬은 110번 포트를 사용한다.
④ 사용자가 고정적인 위치에서 메일을 받을 경우에 유리하다.
⑤ 메일 서버에는 원본 메일이 항상 남아 있고 복사본만 내려 받는다.

34. 최근에 이메일 추출기의 판매 및 이메일 주소의 매매 행위로 인해 스팸 매일이 극성을 부리면서 스팸메일을 지우는 데에 많은 시간을 소비하고 있다. 그리고 최근에 우리나라가 세계적인 스팸메일 발생지 및 릴레이서버로 보도되어 일부 IP 대역이 블록되는 일까지 일어나고 있으므로 메일서버 관리자들은 스팸메일의 경유지가 되지 않게 각각의 메일서버의 메일 릴레이 관련 설정을 확인할 필요가 있다. Sendmail 설치 후 spam relay 설정으로 올바르지 않은 것은?

```
spam@hacker.com REJECT
spammail.com REJECT
```

```
useful.org OK
211.252.150 RELAY
211.252.151 RELAY
```

① spam@hacker.com, spammail.com 및 211.252.150과 같은 첫번째 필드는 e-mail 주소, 도메인 네임, 네트웍 넘버 등이 올 수 있다
② 두번째 필드는 해당 주소로부터 오는 메일을 어떻게 처리할 것인가를 결정하는 데에 사용한다.
③ spam@hacker.com의 메일사용자 및 spammail.com 도메인으로부터 오는 모든 메일은 거절된다.
④ 마지막의 것은 C-Class의 네트워크가 211.252.150, 211.252.151의 IP를 사용하는 모든 IP주소에 대하여 릴레이를 허가된다.
⑤ 오직 useful.org 도메인으로부터 오는 모든 메일은 받아들인다는 설정

35. 다음은 FTP 공격방법 중 하나에 대한 설명이다. 어떤 공격에 대한 설명인가?

FTP 프로토콜은 단순히 데이터를 전송할 목적지는 확인하지 않고 데이터만 전송한다는 FTP 프로토콜 자체의 취약성을 이용한 공격 방법으로 오래 전부터 문제시된 공격방법으로써 최근 이러한 취약성을 해결한 프로그램이 개발되었지만, 아직 FTP에서 매우 위협적인 공격이며 이를 이용한 공격이 인터넷상에서 쉽게 이루어진다.

① FTP 데몬 버그
② 트로이 목마
③ FTP 바운스
④ 포트 스캐닝
⑤ Anonymous FTP 버그

36. 다음의 메일 관련 프로토콜들이 사용하는 다음 서비스들의 포트 번호를 바르게 기술한 것은 무엇인가?

Sendmail - POP3 - IMAP - IMAP4

① 25-110-155-220
② 21-110-155-220
③ 21-110-140-200
④ 21-110-140-220
⑤ 25-110-143-220

37. 메일 관련 시스템들에 대하여 바르지 못하게 기술 된 것은 무엇인가?

① POP2는 메일을 가져오지만 IMAP은 메일을 메일 서버에 그냥 둔 채로 메일을 읽을 수 있다.
② MTA 에 속하는 대표적인 것으로 sendmail 이 있다.
③ MDA 에 해당하는 대표적인 것으로 procmail 이 있다.
④ MUA 에 해당하는 대표적인 적으로 mail, K-mail, 아웃룩 익스프레스 등이 있다.
⑤ SMTP는 UDP 접속을 통하여 메일을 주고받는다.

38. FTP 서버를 실행 제어하는 inetd 슈퍼서버의 이름은?

① /usr/sbin/inetd.ftpd
② /etc/ftpd
③ /etc/ftphosts
④ /etc/ftpusers
⑤ /usr/sbin/in.ftpd

39. CGI를 사용함에 있어 발생할 수 있는 보안적 취약점에 대한 해결책으로 틀린 것은?

① CGI 프로그램 내에 쉘 명령어를 실행시킬 수 있는 제어문자 들을 제거한다.
② Chroot를 수행해서 필요한 명령어와 치명적으로 동작할 수 있는 명령어의 루트를 분리한 수행 환경에서 CGI를 실행한다.
③ CGI의 프로그램의 디렉토리 권한을 711로 한다.
④ CGI 프로그램은 소스를 볼 수 없도록 컴파일해서 사용한다.
⑤ 웹 서버의 자식 프로세스가 루트권한으로 동작하므로 실행할 수 있는 쉘 명령을 신중히 검토하여 제한하여야 한다.

40. 다음은 PGP에 대한 설명이다. 잘못된 것은?

① PGP는 여러 가지 암호화 알고리즘을 복합적으로 사용한다.
② PGP는 메시지 암호화에는 관용키 암호화 방식을 사용하고, 메시지를 암호화한 관용키를 암호화하기 위하여 공개키 암호화 방식을 사용한다.
③ PGP는 메시지를 암호화하기 위하여 128 bit의 랜덤키를 생성하여 사용한다.
④ PGP는 인증 기능을 제공하기 위하여 메시지를 MD5 해쉬함수를 이용하여 128 bit 해쉬값을 생성하여 수신자의 공개키로 암호화해서 보낸다.
⑤ 수신자의 PGP는 수신자의 비밀키를 이용하여 메시지 암호화에 사용된 관용키를 복호화 하고, 이 관용키를 이용하여 메시지 내용을 복호화한다.

41. 다음 중 유형이 다른 보안 알고리즘은?

① DES 알고리즘
② RSA 알고리즘
③ Rabin 암호화 알고리즘
④ Diffie-Hellman 알고리즘
⑤ Elliptic Curve Cryptography

42. 사용자를 대신하여 서버가 인증 경로를 발견해주고, 인증경로의 유효성을 확인하기 위한 프로토콜은 다음 중 무엇인가?

① OCSP(Online certificate status protocol)
② SCVP(simple certificate validation protocol)
③ CRL
④ LDAP
⑤ SSL

43. 전자화폐의 지불방식에 따른 분류가 아닌 것은?

① 온라인 지불
② 오프라인 지불
③ 신용카드 지불
④ 선불 방식
⑤ 고액 지불

44. 전자서명법에 대한 설명 중 틀린 것은?

① 전자서명법은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위한 기본적인 사항을 정하는 법이다.
② 전자서명 검증키는 전자 서명의 유효성을 검증하기 위한 공개키이다.
③ 공인 인증기관의 지정, 공인 인증기관의 인증 업무준칙, 인증 업무의 제공, 공인 인증기관의 업무 수행 등에 대한 내용 등을 포함하고 있다.
④ 공인 인증기관은 정보통신부가 발행하는 인증서형태로 자신의 전자서명 검증키를 인증 받아야 하고, 전자서명 생성키를 이용하여 인증 업무를 수행한다.
⑤ 전자서명법에 의한 공개키 기반구조로서 정보통신부가 공인 인증기관에 대한 정책, 감독기관으로서 기능을 수행한다.

45. 다음 빈 곳에 들어갈 내용으로 올바르게 짝지워진 것은?

WTLS는 두 응용간의 기밀성, 사용자 인증, 메시지 무결성 등의 보안 서비스를 제공하나, ( ) 서비스는 제공하지 않는다. 기밀성 서비스는 ( ) 등과 같은 대칭키 암호 알고리즘을 사용하며, 대칭키 암호를 위한 세션키는 클라이언트와 서버간의 Handshake 프로토콜을 이용하여 세션개시 시에 생성된다. 클라이언트와 서버간의 상호 인증은 핸드세이크 과정에서 ( )과 무선 X.509 인증서를 이용하여 수행된다. 메시지 무결성 서비스는 ( ) 기법을 이용하여 데이터 변조 여부를 확인할 수 있다.

① 부인방지 - RSA, IDEA - 키분배 암호방식 - SHA1withDSA
② 부인방지 - DES, IDEA - 공개키 암호방식 - HMAC
③ 부인방지 - DES, AES - 비밀키 암호방식 -HMAC
④ 부인방지 - Diffie-Hellman, IDEA - 비밀공유방식 - SHA1withDSA
⑤ 부인방지 - DES, IDEA - 비밀키 암호방식 - HMAC

46. DRM(Digital Rights Management)에 관한 설명 중 틀린 것은?

① DRM은 복사된 컨텐츠 사본의 감지는 불가능하다.
② 광범위하게는 watermarking와 fingerprinting등의 기술을 포함한다.
③ 디지털 상품의 소비에 관한 정책, 이용에 관한 데이터, 자금 집행, 키 관리 등 네트워크 상에서 발생하는 전자상거래의 보안에 관한 기술 등을 포함하는 포괄적인 기술이다.
④ 오디오 파일과 뮤직 비디오 등에도 쉽게 적용 가능하다.
⑤ 암호화 기술을 이용해 디지털 콘텐츠를 암호화시킴으로써 적법한 사용자만 복호화해서 사용할 수 있도록 한다.

47. 유선 인터넷상에서와는 달리 무선 인터넷 환경에서는 최소한의 계산 복잡도와 저장 공간을 요구하는 암호 알고리즘이 필요하게 된다. 그렇다면, 무선 인터넷 환경에서 활용 가능한 공개키 암호 알고리즘으로 가장 적합한 것은 어떤 것인지 고르시오.

① ECC
② RSA
③ ElGarmal
④ SKIPJACK
⑤ IDEA

48. 인터넷을 이용한 전자 상거래에서 멀티미디어 컨텐츠의 지적 소유권 보호를 위해 컨텐츠에 사용자 정보를 숨겨 저작권 및 소유권을 보호하는 방법은?

① Watermarking
② 암호화
③ PGP (Pretty Good Privacy)
④ SHTTP (Secure-HTTP)
⑤ SSL

49. 다음 PKI 구조에 대한 설명 중 틀린 것은?

① 계층적 구조는 네트워크 구조에 비해 인증 경로 탐색이 어렵다.
② 네트워크 구조는 인증기관의 비밀키 노출시 해당 인증 도메인에만 영향을 미친다.
③ 계층적 구조는 단일화된 인증 정책과 중앙 집중적인 조직체계에 적절하다.
④ 네트워크 구조는 계층적 구조에 비해 구조가 유연하여 기존에 구축된 서로 다른 도메인간을 연결할 때 유리하다.
⑤ PKI를 구성하는 최소 객체들은 등록기관(RA), 인증기관(CA), 디렉토리, 사용자 이다.

50. 스마트카드 보안 기술에 대한 설명 중 틀린 것은?

① 사용자 식별과 인증을 위해 필요한 정보를 저장하고 관리하는 모듈로 WIM(Wireless Identity Module)를 사용한다.,
② 개인이동성과 서비스 이동성을 겸비한 이동 통신용 스마트카드를 USIM(universal Subscriber Identity Module)이라고 한다.
③ USIM의 기본형태는 ID-1 Type(카드)와 Plug-in Type(칩)으로 되어 있다.
④ WIM은 WTLS와 연계하여 사용할 수 없다.
⑤ USIM은 ME(Mobile Equipment)와 인터페이스하기 위해 T=0통신 프로토콜을 사용한다.

51. 암호 알고리즘에 대한 안정성 평가에 대한 설명 중 틀린 것은?

① 암호모듈의 안전성 평가는 암호알고리즘의 안정성과 무관하게 잘못된 암호기술의 사용 및 해석에 대한 취약성을 검증한다.
② 암호모듈의 안정성 평가는 암호기술의 구현 적합성 평가, 암호키 운용 및 관리, 물리적 보안으로 나누어 평가한다.
③ 암호모듈의 안정성 평가는 암호모듈이 탑재된 제품과 독립적으로 검증한다.
④ 암호모듈 안정성 평가는 CC(Common Criteria)에 평가기준 및 방법이 정의되어 있다.
⑤ 암호모듈 안정성 평가프로그램 중 미국의 NIST에서 실시하고 있는 CMVP(Cryptographic Module Validation Program) 대표적이다.

52. 파일 전송 보안과 관련된 다음 설명 중 옳지 않은 것은?

① Passive FTP는 방화벽 뒤에 위치한 FTP 서버에 대한 접근 문제를 해결한다.
② FTP 프로토콜은 패스워드를 암호화하지 않고 전달한다.
③ FTP 프로토콜은 전송 데이터를 암호화하지 않는다.
④ FTP 서버에 대한 바운스(bounce)공격은 Active FTP 방식을 사용하는 경우에만 적용될 수 있다.
⑤ SSH에서는 안전한 인증과 안전한 데이터 전송을 제공하는 파일 전송 보안 기능을 제공한다.

53. 다음 중 악의적 액티브X 컨트롤에 의한 직접적 피해를 당할 수 있는 시스템은?

① 액티브X 컨트롤을 제공하는 웹 서버
② 액티브X 컨트롤의 인증을 위한 PKI 관련 서버
③ 방화벽이나 캐시 기능을 수행하는 웹 프록시 서버
④ 액티브X 컨트롤을 다운로드하여 실행하는 클라이언트 컴퓨터
⑤ 액티브X 컨트롤 전달에 관여하는 ISP

54. 웹 버그(web bug)에 대한 올바른 설명은?

① 웹 서버 어플리케이션에 존재하는 프로그램 오류
② 웹 스크립트에 존재하는 프로그램 오류
③ 웹 브라우저 코드에 존재하는 보안 결함
④ 웹 페이지 안에 숨어 있으며 웹 페이지 사용자를 감시하기 위한 코드나 콘텐츠
⑤ 웹 페이지에 숨겨져 전달되는 악성 바이러스

55. HTTP 인증 방식에 대한 설명으로 잘못된 것은?

① 기본 인증(Basic Authentication) 방식은 서버측에서 "WWW-Authenticate" 헤더를 통해 인증을 요청하고 클라이언트측은 "Authentication" 헤더로 인증정보를 전송한다.
② 기본 인증방식에서는 인증정보 보호를 위해 사용자 ID와 비밀번호는 암호화되어 전송된다.
③ 다이제스트 인증(Digest Authentication) 방식에서는 Challenge-Response 구조의 사용자 인증이 사용된다.
④ 다이제스트 인증 방식에서는 사용자 ID와 비밀번호의 해쉬값이 전송된다.
⑤ 기본 인증과 다이제스트 인증 방식 모두 인증 영역 지정에 이용되는 realm 정보가 이용된다.

56. 다음은 IPSec 전송 모드와 터널 모드에 대한 설명이다. 틀린 것은 ?

① IPSec 전송모드(transport mode)는 단말과 단말 간에 설정되는 것이 일반적이며 IP 패킷의 페이로드 부분을 보호한다.
② IPSec 전송모드(transport mode)는 단말과 단말 간에 설정되는 것이 일반적이며 IP 패킷 전체를 AH 또는 ESP 프로토콜을 이용하여 보호한다.
③ IPSec 터널모드(tunnel mode)는 라우터와 라우터 간에 설정되는 것이 일반적이며 inbound IP 패킷 전체에 대해서 IPSec AH 또는 ESP 프로토콜을 적용한다.
④ IPSec 전송모드와 터널모드는 중첩하여 적용할 수 있다.
⑤ IPSec 터널모드(tunnel mode)에서의 IP 패킷 인증의 범위는 출발지 IP 패킷의 헤더 부분을 포함한다.

57. 다음은 S/MIME 프로토콜을 이용한 이메일 메시지 전자서명 절차이다. 틀린 곳은 ?

① 단계 1 - 원본 메시지(메일)를 MIME 형태로 변환한다. 이때 전송을 위해 사용되는 base-64 인코딩 등이 수행된다.
② 단계 2 - 전자서명 메시지를 만들기 위해 먼저 SHA-1과 같은 해쉬 알고리즘을 이용해 임의의 크기를 갖는 메시지를 20바이트(160비트)의 데이터로 압축한다.
③ 단계 3 - 압축된 데이터를 자신의 공개키로 서명(암호화)한다.
④ 단계 4 - 전자서명이 이루어진 데이터는 전송을 위해 base-64 인코딩을 한다.
⑤ 단계 5 - 원본 메시지와 전자서명 데이터를 MIME 형태로 변환하여 결합한다.

58. 지문은 일반적인 FTP command session의 일부 입니다. 이 session 에 해당하는 server 에서 사용되고 있을 data port 는 무엇입니까?

```
<예시>
testbox1: {/home/p-t/slacker/public_html} % ftp -d testbox2
Connected to testbox2.slacksite.com.
220 testbox2.slacksite.com FTP server ready.
Name (testbox2:slacker): slacker
---> USER slacker
331 Password required for slacker.
Password: TmpPass
---> PASS XXXX
230 User slacker logged in.
---> SYST
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
```

```
ftp> ls
---> PASV
227 Entering Passive Mode (192,168,150,90,14,178).
---> LIST
150 Opening ASCII mode data connection for file list
drwx------   3 slacker    users         104 Jul 27 01:45 public_html
226 Transfer complete.
ftp> quit
---> QUIT
221 Goodbye.
```

① 21
② 20
③ 3762
④ 178
⑤ 14

59. 다음 중 Melissa worm 에 대한 주요 설명 중 옳지 않은 것은?

① 감염된 컴퓨터 내의 주소록에서 2차 감염대상을 찾아 웜을 전송한다.
② 이메일에 첨부된 LIST.DOC 이란 파일을 통해 감염을 시킨다.
③ Microsoft 사의 MUA 인 Outlook 97 이나 Outlook 98 이 주된 감염 대상이 된다.
④ 감염되기 위해서 user 의 action 이 필요하므로 virus 로도 구분할 수도 있다.
⑤ Windows 의 buffer overflow 의 취약점을 노린 웜의 일종이다.

60. 다음 중 FTP 프로토콜에 대한 설명으로 올바르지 못한 것은?

① FTP 서버는 클라이언트가 지시한 곳으로 자료를 전송할 때 그 목적지가 '어떤 곳' 인지 검사하지 않는다.
② 클라이언트는 FTP 서버를 거쳐 간접적으로 임의의 IP에 있는 임의의 포트에 접근할 수 없다.
③ ~ftp/etc/passwd나 ~ftp/etc/group 파일 내에는, 패스워드, 사용자 이름, 홈 디렉토리, 쉘 등의 정보는 기록하지 않는 것이 바람직하다.
④ FTPD가 실행하는 프로그램은 일반적으로 ls 밖에 없으므로 ~ftp/bin 디렉토리에 ls 이외의 프로그램은 넣지 않는 것이 좋다.
⑤ FTP Control connection의 세션은 단 한번만 열리고, 세션 자체는 암호화되지 않는다.

61. 전자우편 메시지를 전송하는 과정은 연결설정, 전자우편 전송 및 연결 종료로 구성된다. 메일 전송을 위한 연결이 구축된 다음에 수행되는 다음 메시지 전송 과정에서 괄호 안에 들어갈 내용으로 올바르게 나열한 것은?

> 클라이언트는 송신자의 메일 주소를 포함하여 (1) 메시지를 보내어 메시지의 송신자를 알린다. 만일 연결을 승인할 경우 수신자는 250번 코드 등을 통해 응답하고, 클라이언트는 수신자의 전자우편 주소를 포함하는 (2) 메시지를 전송한다. 다시 수신자는 250번 코드나 다른 적절한 코드를 사용하여 응답한다. 이제 클라이언트는 (3) 메시지를 보내어 메시지 전송의 시작을 알린다. 서버는 354번 코드나 적절한 메시지를 사용하여 응답한다. 이제 클라이언트는 메시지 내용을 연속된 라인으로 전송한다. 각 라인은 CR이나 LF 문자로 된 EOL 토큰으로 끝난다. 메시지는 단 하나의 마침표만을 갖는 라인에 의해 종료되고, 최종적으로 수신자는 250번 코드나 적절한 코드로 응답한다.

① 1 - MAIL FROM 2 - RCPT TO 3 - EXPN
② 1 - HELO 2 - RSET 3 - DATA
③ 1 - MAIL FROM 2 - RCPT TO 3 - DATA
④ 1 - HELO 2 - RCPT TO 3 - DATA
⑤ 1 - MAIL FROM 2 - RSET 3 - EXPN

62. 아래 내용은 데이터베이스에 대한 공격 기술을 나타낸 것이다. 해당되는 공격 기술은 무엇인가?

> 데이터베이스가 방화벽 뒤에 설치되어 있다고 해서 공격에 안전한 것은 아니다. 본 공격은 데이터베이스에 대한 직접적인 공격이라기보다는 데이터베이스에 전달되는 SQL 문장을 바꾸는 등 웹 응용프로그램에 전달되는 SQL 변수를 수정하려는 시도에 의해서 발생한다.

① 버퍼 오버플로우 공격
② 크로스 사이트 스크립팅 (XSS) 공격
③ 서비스 거부 공격
④ SQL 인젝션 공격
⑤ 세션 가로채기 공격

63. 다음 중 telnet 보안에 대한 설명 중 틀린 것은?

① TELNET 세션은 암호화 및 무결성 검사를 지원하지 않는다.
② SSH(Secure Shell)는 암호화를 하지 않는다.
③ 패스워드가 암호화 되어 있지 않아 스니퍼를 이용하여 제 3자에게 노출 될 수 있다.
④ UNIX 시스템에서 해커가 in.telnetd를 수정하여 클라이언트의 특정 터미널 종류에 대해 인증 과정 없이 쉘을 부여할 수도 있다.
⑤ BSD 소스코드 계열의 많은 운영체제에서 사용하는 텔넷데몬에서 원격 버퍼오버플로우 취약성이 존재한다.

64. 대칭키 암호 알고리즘의 블록 암호방식 문제를 해결하기 위한 운용 모드가 아닌 것은?

① ECB(Electronic Codebook)
② Cipher Block Chaining(CBC)
③ Cipher Feedback(CFB)
④ Input Feedback(IFB)
⑤ Counter(CTR)

65. 다음 중 웹 전송 보안 프로토콜인 SSL을 무선 환경에 맞게 수정하여 만들어진 무선 전송계층 프로토콜은?

① WLAN
② WAP
③ WTLS
④ WVML
⑤ WPKI

66. 아래의 Http daemon들의 설치 및 운영시 잘못된 방법을 고르시오.

① 아파치 웹 서버 1.3.24, 2.0.36이하 버전에서는 Http 프로토콜의 기능인 'chunked' 엔코딩을 이용한 DOS 공격에 취약하므로 1.3.26, 2.0.39로 업그레이드해야 한다.
② 웹 서버는 http daemon과는 별개로 webresolve와 같은 프로그램에 의해 로컬 버퍼 오버플로우가 발생할 수 있으므로 제한한다.
③ IIS 등록정보에서 홈 디렉터리의 구성 창에서 응용프로그램 매핑 부분에 htw가 등록되어 있다면 인덱스 서버 관련 백도어이므로 삭제해야 한다.
④ IIS의 익명 계정인 IUSER_REVOLVER의 권한 설정을 통해 로컬 리소스의 접근을 제어한다.
⑤ IIS의 보안을 강화하기 위해, Administrator 계정은 해킹의 대상이 되므로 삭제하고 대체한다.

67. 전자서명에서 사용되는 해쉬 함수(H)와 관련한 설명으로 옳지 않은 것은?

① 해쉬 값 h가 주어져 있을 때 h = H(M)인 메시지 M을 찾는 일은 시간이 아주 많이 걸리는 일이어야 한다.
② 메시지 M이 주어져 있을 때, H(M) = H(M')인 다른 메시지 M'을 찾는 일은 시간이 아주 많이 걸리는 일이어야 한다.
③ H(M) = H(M')인 서로 다른 두 메시지 M과 M'을 찾는 일은 시간이 아주 많이 걸리는 일이어야 한다.
④ 해쉬 함수의 출력의 크기는 해쉬 함수의 안전성과는 무관하지만, 해쉬 함수 계산 시간에는 많은 영향을 미친다.

⑤ 전자 서명에서 해쉬 함수를 사용하는 이유는 서명 계산 시간과 서명이 차지하는 공간을 줄이기 위함이다.

68. 다음 중 나머지와 종류가 다른 전자화폐는?

① E-Cash
② Cyber Cash
③ Mondex
④ Digital Cash
⑤ iCash

69. 인증서(Certificate)가 취소 또는 폐기되었을 때에 이러한 인증서들을 따로 모아서 관리하는 목록을 CRL(Certificate Revocation List) 이라고 한다. CRL 목록을 유지 및 관리해야 되는 이유는?

① 인증서가 폐기되기 이전에 사용된 전자 거래 문서의 타당성을 증빙하기 위해서 보관해야 한다.
② 사용자의 비밀키를 분실했을 경우에 인증서 취소 요청을 한다.
③ 등록기관은 사용자의 인증서 취소 요구를 상위 기관인 인증기관에 보고한다.
④ CRL 목록은 디렉토리에 저장되며 루트 CA에서 관리한다.
⑤ 인증서 폐기는 인증서 유포 기간이 만료되거나 발급한 CA의 비밀키가 노출되었을 때 이루어진다.

70. 공개키 기반 구조에서 사용하는 인증서 및 인증서 취소 목록(CRL)에 대한 아래 설명 중에서 옳지 않은 것은?

① 소유자가 인증서를 받은 조직을 탈퇴하거나 공개키에 해당하는 비밀키가 손상되었을 경우 인증서를 취소할 필요가 있다.
② 인증서를 취소하기 위해 X.509에서 정의된 메커니즘이 CRL이다.
③ X.509 v3인 경우 v2 인증서에 비해 근본적인 변화는 확장자를 도입하여 필요로 하는 용도로 인증서 내용을 정의할 수 있다.
④ 인증서의 검증은 소유자의 개인키를 사용하여 수행되며, CA의 공개키는 네트워크를 통해 쉽게 접근할 수 있는 영역에 두어 필요로 할 때마다 다운받아 사용한다.
⑤ 인증서 취소 요구는 원칙적으로 인증서 소유자 혹은 대리인에 의해 요구되며, 취소된 인증서에 대한 목록을 공개 디렉토리에 보관하여 네트워크를 통해 접근할 수 있도록 한다.

71. 전자화폐에서 아래와 같은 기능을 제공하기 위해 사용되는 전자서명 기법은 무엇인가?

<보기>
가. D.Chaum이 제시한 특수 형태의 전자서명 기법이다.
나. 전자화폐를 사용하는데 있어서 사용자의 사생활을 보호하는 차원에서 제시된 서명 기법이다.
다. 이 방식은 사용자가 서명자 즉 은행에게는 서명을 받으려는 문서를 비밀로 한 채 은행의 서명을 받는 방법으로 전자화폐에 대한 추적을 불가능하게 할 수 있는 기능을 제공한다.

① Fail-Stop Signature
② Blind Signature
③ One-Time Signature
④ Arbitrated Signature
⑤ Undeniable Signature

72. 스마트카드 운영체제가 제공하는 기본 기능으로 가장 적절하지 않은 것은?

① 데이터 전송 기능
② 데이터 접근 제어
③ 메모리 관리
④ 암호 알고리즘 관리 및 실행
⑤ 사용자 인터페이스 제공

73. DRM 기술요소에 관한 다음 설명 중 올바르지 않은 것은?

① TRM : 콘텐츠 보호메커니즘을 구성하는 하드웨어나 소프트웨어 내부 동작원리 분석이나 변경을 불가능하게 한다.
② S/D(Super-Distribution) : 콘텐츠 구매자가 제3자에게 콘텐츠를 이용할 수 있도록 배포한다.
③ XrML : XML 기반의 콘텐츠에 대한 권리명세 언어
④ 하드웨어바인딩 : 콘텐츠를 특정 하드웨어에서만 이용할 수 있게 한다.
⑤ 워터마킹 : 콘텐츠에 대한 불법적 접근이나 이용을 사전 차단한다.

74. 다음 프로그램 중 버퍼오버플로우 공격이 성공, root shell이 실행될 수 있는 가능성이 높은 것은?

① -rwxr-xr-x root root a.out*
② -r-xr-xr-x root root bof*
③ -r-sr-xr-- bin bin attack*
④ -r-sr-xr-x root root readme*
⑤ -rwxrwxrwx root root bof_attack*

75. 다음은 디지털 워터마킹에 대한 요구사항에 대해서 설명하고 있다. 틀린 것은?

① 분할성(Divisibility) : 삽입된 워터마크를 추출하여 복수 저작권자의 권리를 위하여 여러 개의 워터마크로 분할하여 다중 검증할 수 있어야 한다.
② 비가시성(Invisibility) : 삽입 후에도 원본의 변화가 거의 없고, 워터마크의 삽입여부를 감지 할 수 없어야 한다.
③ 강인성(Robustness) : 워터마크를 신호의 중요한 부분에 삽입하여 전송이나 저장을 위해 압축할 때 워터마크가 깨지지 않아야 하다.
④ 원본 없이 추출(Blindness) : 원본 영상 없이 워터마킹된 영상만으로 워터마크를 검출할 수 있어야 한다.
⑤ 보안성(Security) : 관련된 키 값 등을 알고 있을 경우에 워터마크의 확인이 가능해야 된다.

SIS 1급 네트워크보안

1. 다음 [ ]에 들어갈 용어로 알맞은 것은?

( )는(은) 도메인간의 라우팅에 사용되는 인터넷 주소를 원래의 IP 주소 클래스 체계를 쓰는 것보다 더욱 융통성 있도록 할당하고 지정하는 방식으로서 IP 주소의 네트워크 ID를 결정하는 방법으로 클래스 기준을 사용하지 않는 라우터들 간이 라우팅이 가능하도록 한다.

① ICMP
② ATM
③ SONET
④ CIDR
⑤ VPN

2. 다음 중 라우팅 프로토콜과 가장 관련이 적은 것은?

① RIP
② OSPF
③ BGP
④ IDRP
⑤ RSVP

3. TCP Sync 플러딩(Flooding) 공격은 악의의 사용자가 목표시스템에 Sync를 무한히 보내서 접속을 위한 큐가 계속적으로 메모리 버퍼에 저장되면서, 이 큐의 크기로 인해 오버플로우(overflow)가 생기는 것이다. 다음 보기중 이를 방지하기 위한 방법들로만 짝지어진 것은?

가. 사용자가 만들 수 있는 최대 프로세스 수를 제한한다.
나. 외부에서 들어오는 패킷을 필터링하여 송신지 IP주소의 인증 절차를 거친 후에 TCP 연결을 수행한다.
다. 큐의 크기가 오버플로우가 되려고 할 때, 큐의 크기를 가상으로 증가시킨다.
라. 역 DNS 매핑으로 등록된 IP 주소(공인 IP 주소)인지 확인 후 TCP 연결을 수행한다.

① 가, 다
② 나, 다
③ 가, 라
④ 다, 라

⑤ 나, 라

4. 다음 설명 중 ping과 가장 관련이 적은 것은?

① ICMP
② RTT
③ TTL
④ 패킷 손실율
⑤ 경로 테이블 생성

5. 다음 설명 중 nbstat가 제공하는 정보가 아닌 것은?

① MAC address
② login name
③ NetBIOS 사용 서버 이름
④ NetBIOS 사용 클라이언트 이름
⑤ 라우팅 테이블

6. 다음은 네트워크 기반 유틸리티에 대한 설명이다. 틀린 것은?

① ipconfig : 해당 컴퓨터의 IP 설정과 관련된 기능 수행
② ping : 지정한 목적지 IP 주소까지의 연결 상태 확인
③ arp : 라우팅 테이블에 대한 정보 출력
④ tracert : 목적지 IP 주소까지의 경로에서 중계 역할을 하는 라우터의 주소 표시
⑤ nslookup : DNS 서버에 연결해서 IP주소나 도메인 이름에 대한 질의

7. 다음은 데이터 통신에 있어서 사용되는 통신방식에 대한 설명이다. 옳은 것은?

① Half-duplex 방식은 한쪽에서 데이터를 보내고 나면 다른 한쪽에서 데이터 전송이 가능하다.
② Full-duplex 방식은 여러 개의 전송로를 이용하여 한쪽방향으로 한번에 많은양의 데이터 전송이 가능하다.
③ Half-duplex 방식은 근거리통신망에서는 한 워크스테이션이 데이터를 수신하는 중에도 그 회선을 통해 다른 워크스테이션으로 데이터를 보낼 수 있다.
④ Full-dulex 방식은 데이터가 양쪽 방향으로 전송될 수 있지만, 동시에 전송할 수 없는 것을 의미한다.
⑤ Half-duplex 방식은 양방향 회선에 필수적으로 적용된다.

8. 아래 지문은 신문에서 발췌한 기사이다. 이와 같은 현상을 무엇이라고 하는가?

"최근 외신에 의하면 미국의 인터넷 제공업체인 패닉스는 1996년 9월에 무차별 전자우편 공격이 가해져 서비스에 차질뿐만 아니라, 도산 지경에 이르고 있다고 보도되고 있다. 전자우편 공격은 익명의 발신자 전자우편을 지속적으로 보내게 되면, 시스템이 전자우편 처리에 모든 프로세스를 소비하거나, 하드디스크를 사용할 수 없게 만든다. 이러한 공격을 하는 "유나메일러(Unamailer)"라는 별명의 폭탄테러 공격자로 말미암아 미국의 클린턴 대통령, 빌게이츠 등 유명 인사에 대한 테러가 이루어지기도 하였다. 우리나라에서도 1996년 초 포항공대에 메일공격(Mail Storm)이 일어났었다"

① 인터넷 웜
② 러브 바이러스
③ 트로이 목마
④서비스 거부 공격(Denial of Service)
⑤ 스니핑

9. 다음은 SYN Flooding Attack에 대한 설명이다. 잘못된 것은?

① TCP/IP의 결함을 이용한 공격 방법으로 대표적인 서비스 거부 공격이다.
② 리눅스에서 커널 컴파일시 CONFIG_SYN_COOKIES 옵션으로 막을 수 있다.
③ TCP 연결시에 half-open상태를 이용하여 TCP연결을 방해한다.
④ TCP 연결을 위한 백로그 큐가 너무 크기 때문에 작게 해줘야 한다.
⑤ 백로그 큐에 저장되어진 내용을 제거하는 시간을 줄여야 한다.

10. cisco 라우터에서 제공하는 명령어중 echo, discard, chargen 등의 서비스를 disable 하기 위해서는 다음의 명령어를 실행하면 된다. 이때 ( ) 에 들어갈 적당한 용어는 무엇인가?

no service tcp-(   )-servers
no service udp-(   )-servers

① few
② little
③ minor
④ bad
⑤ small

11. 다음 중 VPN 의 장점이 아닌 것은 무엇인가?

① 터널링과 보안 프로토콜을 통한 데이터의 기밀유지 가능
② 기업의 광범위한 intranet 및 extranet 지원 가능
③ 공중망을 이용하여 저렴한 비용으로 전용망과 같은 효과
④ signature 를 기반으로 한 공격탐지
⑤ 공중망을 통한 연결을 전용망처럼 이용하는 가설사설망

12. 다음은 어떤 공격에 대한 대응을 하기 위한 설정인가?

```
Router(config)# access-list 110 deny ip any host 14.2.6.255
Router(config)# access-list 110 deny ip any host 14.2.6.0
Router(config)# interface interface serial 2/0
Router(config-if)# ip access-group 110 in
```

① SYN Flooding Attack
② Smurf Attack
③ Fragmentation Attack
④ UDP Flooding Attack
⑤ DRDOS Attack

13. 다음은 웜(worm)에 대한 특징에 대해 설명한 것입니다. 해당하는 웜(worm)의 종류는 무엇인가?

감염시 특정 네트워크 포트를 열어 해커의 침입을 유발하고, 백신 프로그램을 강제 종료하며, 시스템에 존재하는 HTM 및 HTML 파일에서 추출한 메일 주소로 같은 웜 메일을 발송한다. 특히 윈도NT 계열 시스템의 관리자 네트워크 공유(IPC$ 공유) 권한을 획득해 다른 시스템으로 공격을 시도하고, 지속적으로 다른 사람에게 바이러스 메일을 보내기 때문에 네트워크 속도를 저하시키는 특징을 갖고 있다.

①코드레드 웜(W32.code red,worm)
②슬래머 웜(W32.Slammer,worm)
③스파이봇 웜 (W32/Spybot.worm)
④러브게이트 웜(Win32/LovGate.worm)
⑤소빅 웜(Win32/Sobig.worm)

14. DNS 서버의 앞단에 방화벽을 설치하고자 할 때 허용하여야 할 포트(port)를 설정하려고 한다. 다음 중 가장 권장할만한 방식은 무엇인가?

① 소스포트 : 0 부터1023 목적지포트 : 53
② 소스포트 : 1024부터 끝까지 목적지포트 : 0부터 1023
③ 소스포트 : 53 목적지포트 : 53
④ 소스포트 : 53 및 1024부터 끝까지 목적지포트 : 53
⑤ 소스포트 : 모든 포트 목적지포트 : 53

15. 다음은 보안장비의 어떤 기능 또는 특징에 대한 설명인가?

* 서비스 수준 동의와 application 성능을 보장하기 위해 끝단과 끝단에 대역폭 관리와 QoS
* 공격하에서 특정 application 을 보장하기 위한 트래픽.
* 대역폭 저축

① 고립화(isolcation)
② 방지(Prevention)
③ Deep Packet Inspection
④ Anomaly detection
⑤ Traffic shaping

16. 일반적으로 Handshake 프로토콜에서 수행되는 기능이 아닌 것은?

① 보안 알고리즘, 매개변수 등을 설정
② Alarm 정보교환
③ 세션 정보교환
④ 서버교환
⑤ 클라이언트 인증

17. 다음 중 Windows 2000 시스템의 Active Directory 기능이 아닌 것은?

① 모든 네트워크 자원들을 계층적으로 관리한다.
② 클라이언트 컴퓨터의 DNS 설정이 필요 없다.
③ 디렉토리는 조직구조 단위로 자원을 그룹화한다.
④ 여러 가지 공통 이름 포맷을 지원한다.
⑤ 디렉토리와 응용 프로그램 간에 정보를 교환하기 위해 사용한다.

18. 다음 설명 가운데 틀린 것은?

① TCP 프로토콜은 연결형 서비스를 허용한다.
② TCP 프로토콜은 IP 프로토콜 상위에 존재한다.
③ UDP 프로토콜은 오류가 발견되어도 재전송을 요구하지 않는다.
④ TCP 프로토콜은 UDP에 비해 신뢰성이 높다.
⑤ UDP는 TCP에 비해 오버헤드가 적어 멀티미디어응용에 부적합하다.

19. 다음 중 설명 가운데 틀린 것은?

① 라우터는 네트워크 계층 접속을 지원한다.
② 브리지는 데이터링크 계층 접속을 지원한다.
③ 리피터는 감쇄된 신호를 재생하는 장치이다.
④ 게이트웨이는 프로토콜이 다른 네트워크들을 연결한다.
⑤ 더미 허브는 모뎀 기능과 경로선택 기능을 모두 수행한다.

20. 다음 중 무선 LAN에 대한 설명으로 거리가 가장 먼 것은?

① 무선 LAN 전송 매체에 따라 적외선, 레이저, 전파의 세 가지 방식이 있다.
② AP(Access Point)는 유선 LAN과 무선 LAN을 연동시키는 장비이다.
③ 무선 LAN이 갖는 이점은 유연성, 용이성, 그리고 신뢰성이다.
④ AP를 이용하여 서로 독립적으로 동작하는 Ad Hoc 방식이 주로 사용된다.
⑤ 무선 LAN의 MAC 프로토콜은 주로 CSMA/CA 방식을 이용한다.

21. DSL(Digital Subscriber Line)은 일반 구리 전화선을 통하여 가정이나 소규모 기업에 고속으로 정보를 전송하기 위한 기술이다. DSL의 종류에는 여러 가지가 있는데, 다음 중 이에 대한 설명으로 거리가 가장 먼 것은?

① ADSL(Asymmetric DSL) : 양방향 또는 전이중방식 대역폭의 대부분이 데이터를 사용자 측으로 전송하는 하향방향에 전념한다.
② CDSL(Consumer DSL) : ADSL보다 다소 느리지만 사용자 측에 신호분할기를 설치할 필요가 없는 장점이 있다.
③ SDSL(Symmetric DSL) : G.Lite라고도 불려지며, 사용자 측에서 회선의 분할이 필요치 않는 저속의 ADSL이다.
④ HDSL(High bit-rate DSL) : 기업 사이트 내부와 전화회사의 고객 사이의 광대역 디지털 전송을 위해 사용되었고, 양방향의 대역폭의 크기가 같다.
⑤ VDSL(Very high data rate DSL) : 국내에서 2002년도 하반기부터 서비스되고 있는 기술로 비교적 가까운 거리에서 더 빠른 속도를 보장한다.

22. 공격자가 로컬 네트워크에서 스니퍼를 이용, 패킷을 모니터링하여 순서제어번호를 가로채어 원하는 작업을 수행하는 공격방법은?

① TCP Sequence number Prediction
② Session Hijacking
③ DOS
④ UDP Flooding
⑤ Fragment Overlap

23. 다음 중 TCP/IP의 결함을 이용한 공격방법이 아닌 것은?

① Syn flooding
② IP Spoofing
③ Teardrop
④ TCP Sequence number Prediction
⑤ Backorifice

24. 다음 방화벽 (Firewall) 설명 가운데 틀린 것은?

① 방화벽은 신뢰할 수 없는 네트워크를 연결하기 위해 사용한다.
② 패킷 필터링 라우터가 IP와 TCP 또는 UDP 헤더를 점검한다.
③ 방화벽은 내부 공격에도 대처할 수 있다.
④ 방화벽은 바이러스에 감염된 파일을 차단할 수 없다.
⑤ Proxy 서버가 패킷 필터링보다는 더 안전하다.

25. 침입탐지 시스템의 탐지 기법에 대한 설명으로 잘못된 것은?

① 지식기반 침입탐지는 시스템의 알려진 취약점들을 이용하여 공격하는 행위들을 사전에 공격에 대한 특징 정보를 가지고 있다가 침입을 탐지하는 방법이다.
② 전문가 시스템은 공격에 관한 규칙집합을 가지고 있어 감사 이벤트가 전문가시스템 내에서 의미를 가지는 사실로 변환되고, 추론엔진은 이 규칙들과 사실을 기반으로 침입을 판단한다.
③ 시그네쳐 분석은 감사이벤트를 감사 자료에서 곧바로 검색이 가능한 데이터 패턴으로 변경하여 침입을 탐지한다.
④ 패트리넷은 기존의 패턴 매칭 방법을 개선한 것으로 시그너쳐와 감사자료를 비교하는데 많은 계산 비용이 요구되지 않는다.
⑤ 신경망은 사용자의 정상적인 행동 패턴을 시스템의 로그파일로부터 추출하여 학습한 후 모델링하여 정상적인 행동과 비정상적인 행동을 구별한다.

26. 다음은 TEST-NET IP 대역인 192.0.2.0/24 를 소스로 한 패킷을 필터링 하려고 한다.( ) 에 들어갈 적당한 mask 를 지정하라.

```
Router(config)# access-list 150 deny ip 192.0.2.0 (          ) any
Router(config)# int serial 0
Router(config-if)# ip access-group 150 in
```

① 255.0.0.0
② 255.255.0.0
③ 0.0.0.255
④ 0.0.255.255
⑤ 0.255.255.255

27. 다음 방화벽에 대해 설명하는 내용 중 다른 것들과 다른 하나는 무엇인가?

① Dynamic packet filtering 이라고도 한다.
② 네트워크의 연결 상태를 모니터하고 상태 테이블을 참고한다.
③ 오직 패킷의 헤더정보만 참고한다.
④ 필터링시 이전의 성립된 패킷 정보를 참고한다.
⑤ 상태정보를 추적하기 위해 별도의 메모리가 필요하다.

28. 다음은 최근 알려진 취약성에 대하여 IDS에서 탐지한 로그이다. 다음 중 아래에 탐지된 로그 및 공격에 대해 틀리게 분석한 것은 무엇인가?

```
[**] [1:2523:2] DOS BGP spoofed connection reset attempt [**]
[Classification: Attempted Denial of Service] [Priority: 2]11/18-19:08:20.3
11264 0:50:56:40:0:6D -> 0:4:76:45:61:39 type:0x800 len:0x3C
172.20.11.80:179 -> 10.10.10.195:2844 TCP TTL:62 TOS:0x0 ID:0 IpLen:20
DgmLen:40 DF*
**A*R** Seq: 0x0  Ack: 0x3254E63C  Win: 0x0  TcpLen: 20
[Xref => http://www.uniras.gov.uk/vuls/2004/236929/index.htm][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0230]
```

① 목적지 포트를 179로 향하는 udp 패킷도 탐지에 해당한다.
② IP packet 의 length 는 20 byte이다.
③ Do Not Fragment Flag 가 설정되어 있다.
④ Win: 0x0 은 Window Size를 의미한다.
⑤ 공격지의 소스 IP 는 위조되었을 가능성이 있다.

29. 최근 Cisco 라우터에서는 한번의 명령어로 라우터의 보안 구성을 자동으로 할 수 있는 서비스를 제공하고 있다. 이를 이용해 공격의 여지가 될 수 있는 몇몇 IP 서비스를 중지하고, 방어 기능을 제공하는 서비스를 가동하는 등 라우터 보안을 강화할 수 있는 이 명령어는 무엇인가?

① auto secure
② ios security
③ one secure
④ ip security
⑤ port security

30. 아래는 모 신문기사 중 일부분이다. 아래 기사에서 설명하는 ( )은 무엇인가?

미국 신용카드 업체인 비자 인터내셔널이 정부기관들과 공동으로 ( )과(와)의 전쟁'을 선포했다고 월스트리트저널이 보도했다. ( )은(는) 유명 사이트와 유사한 가짜 웹 사이트에 고객이 접속해 로그인하고 신용카드 비밀번호 같은 개인정보를 넘기도록 하는 일종의 온라인 사기 수법을 말한다. 비자USA는 재무부, BBB, 연방무역위원회(FTC) 등과 공동으로 ( )의 위험성에 대한 계몽 활동에 나선다는 계획이다.

① 스파이웨어
ⓢ 파싱
③ 피싱
④ 하니넷
⑤ 제로데이

31. 패킷(Packet)들이 라우터에서 라우터로 전달될 때 데이터링크와 네트워크 계층의 출발지와 목적지 주소는 어떻게 변경되는가?

① 출발지 주소와 목적지 주소의 변경은 발생하지 않는다.
② 출발지와 목적지 IP 주소는 변경이 없고, MAC 주소만 라우팅 테이블에 저장된 정보에 의해 다시 초기화된다.
③ 출발지의 IP, MAC 주소는 변경이 없고, 목적지 IP와 MAC 주소만 각각 다음 라우터의 IP 와 MAC 주소로 대체된다.
④ 출발지의 IP와 MAC 주소가 각각 이전 라우터의 IP와 MAC으로 대체되고, 목적지 IP와 MAC 주소는 변경이 없다.
⑤ 출발지 IP, MAC 주소는 이전 라우터의 IP와 MAC 주소로, 목적지 IP, MAC 주소는 다음 라우터의 IP와 MAC 주소로 각각 대체된다.

32. 망 내 교환장비들이 오류 상황에 대한 보고를 할 수 있게 하고, 예상하지 못한 상황이 발생한 경우 이를 알릴 수 있도록 지원하는 프로토콜은 무엇인가?

① ICMP
② ARP
③ RARP
④ RIP
⑤ IGMP

33. 어떤 네트워크에서 만약 어떠한 연결 링크가 끊어졌을 때 해당되는 특별한 링크의 터미널만 연결이 중지되었다. 이 네트워크 토폴로지는 무엇인가?

① 스타(star) 토폴로지
② 트리(tree) 토폴로지
③ 링(ring) 토폴로지
④ 버스(bus) 토폴로지
⑤ 혼합형(mixed) 토폴로지

34. 다음은 리눅스에서 'netstat' 명령의 수행 결과이다. 사용된 옵션은 무엇인가?
<보기>

```
Active Internet connections (severs and established)
Proto    Recv-Q   Send-Q       Local Address                Foreign Address
State
tcp         0       0  *:32768           *.*                                    LISTEN
tcp         0       0  *:32769           *.*                                    LISTEN
tcp         0       0  *:mysql           *.*
LISTEN
tcp         0       0  *:x11             *.*                                    LISTEN
tcp         0       0  *:ftp             *.*                                    LISTEN
tcp         0       0  sign.:domain      *.*                                    LISTEN
tcp         0       0  sign.:ftp             203.252.53.60:2555          ESTABLISHED
tcp         0       0  sign.:ftp             203.252.53.60:2548          ESTABLISHED
tcp         0       0  sign.:ftp-data      203.252.53.60:2596          TIME_WAIT
tcp         0       0  sign.:ftp-data      203.252.53.60:2597          TIME_WAIT
```

① -ra
② -ia
③ -ca
④ -na
⑤ -ta

35. 고정 라우팅 방식의 설명으로 틀린 것은?

① 미리 만들어둔 테이블에 의존해 경로를 정한다.
② 작은 규모의 안정된 네트워크에서 주로 사용한다.
③ 수시로 네트워크에 변동이 발생할 때는 사용하기 어렵다.
④ 경로계산 시간이 짧다.
⑤ 플러딩에 비해 네트워크 부담이 더 크다.

36. 다음 설명 중 버스 토폴로지의 설명으로 적합하지 않은 것은?

① 트래픽의 유무를 감지한 후 전송해야 한다.
② LAN에 적합하다.
③ 네트워크 구성이 쉽다.
④ 버스에 연결된 기기는 모든 통신내용을 들을 수 있다.
⑤ 중재자가 없어 오히려 충돌이 발생하지 않는다.

37. WAP 프로토콜 스택의 최상위계층에 해당하는 것은?

① WAE
② WSP
③ WTLS
④ WDP
⑤ WTP

38. TCP의 FIN, URG, PUSH 상태 플래그를 설정, 패킷을 전송하여 포트가 열린경우 패킷이 오지 않고, 닫힌 경우 RST 패킷이 오는 원리를 이용한 스캔 방법은?

① SYN Scan
② FIN Scan
③ XMAS Scan
④ NULL Scan
⑤ Decoy Scan

39. 세션 하이재킹에 대한 최우선의 방어책은?

① 암호화
② 주기적인 패스워드 변경
③ 일회용 패스워드 사용
④ 정적 라우팅 설정
⑤ 커버로스 이용

40. 스위칭 환경에서 스니핑 기법들 중 '3계층에서 스니핑 시스템이 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꿈'으로써 스니핑을 수행하는 기법은?

① ARP Redirect
② ICMP Redirect
③ ARP spoofing
④ Switch jamming
⑤ SPAN port tapping

41. 다음 중 SSL 연결(connection) 상태 변수는 어느 것인가?

① 세션 확인자(session identifier)
② 등위 인증서(peer certificate)
③ Cipher spec
④ Server write key
⑤ Maser secret

42. 다음 지문의 내용을 설명하는 보안 시스템은 무엇인가?

<예시>
"접근제어목록에 따른 접근제어와 탐지 후 통보라는 수동적인 방어 개념의 침입차단시스템이나 침입탐지시스템과는 달리 이상 징후가 탐지되면 이를 자동적으로 사전에 차단하는 보안 솔루션이다"

① 보안라우팅 장비(Secure Router)
② 통합보안관리시스템(Enterprise Security Management System)
③ 바이러스 월(VirusWall)
④ 침입방지시스템(Intrusion Prevention System)
⑤ 침입감내시스템(Intrusion Tolerant System)

43. 다음은 IDS를 구현하기 위한 방법이다. 알려지지 않은 공격을 탐지하기 위한 방법으로 가장 적합하지 않은 것은 무엇인가?

① 정상행위 프로파일링 (normal behavior profiling)
② 비정상행위 프로파일링 (abnormal behavior profiling)
③ 특징 기반 탐지 (signature-based detection)
④ 정책 기반 탐지 (policy-based detection)
⑤ 면역 시스템 (immune system)

44. 다음 중 VPN 이 갖추어야 할 기본요건이 아닌 것은 무엇인가?

① 사용자인증
② 주소 관리
③ 키관리
④ 패킷필터링
⑤ 데이터암호화

45. 다음은 두 신종 해킹 기법에 대한 설명이다. 두 괄호 안에 순서대로 들어갈 수 있는 적당한 명칭들을 고르시오.

<보기>
(　　)은 정상적인 웹서버를 해킹해 위장사이트를 개설한 후, 인터넷 이용자들의 금융정보 등을 빼내는 사회공학적인 신종 사기수법으로 뱅크 프라우드(bank proud) 또는 스캠(scam)이라고도 한다. 보통 금융기관 등의 웹사이트에서 보낸 이메일로 위장, 링크를 유도해 개인의 인증번호나 신용카드번호, 계좌정보 등을 빼내간다.
(　　)은 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인네임시스템(DNS) 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도, 개인정보를 훔치는 새로운 수법이다. 이 방법은 사용자가 익숙하게 이용해온 인터넷 주소 자체를 강탈해 사용하기 때문에 사용자들이 아무리 도메인 주소나 URL 주소를 주의해 본다 해도 쉽게 속을 수밖에 없어 발생시 대규모 피해를 볼 수밖에 없다.

① 피싱, 랜섬
② 피싱, 파밍
③ 랜섬, 피싱
④ 파밍, 랜섬
⑤ 파밍, 피싱

SIS 1급 정보보호론

1. 대칭키 암호 알고리즘과 공개키 암호 알고리즘에 대한 설명 중 잘못된 것은?

① 대칭키 암호 알고리즘은 실행 속도가 빠르기 때문에 다양한 암호의 핵심함수로 사용된다.
② 공개키 암호는 대칭키 암호에 비해 키의 길이가 상대적으로 크다.
③ 대칭키 암호의 경우 키를 자주 변경해야 하는 불편함이 있다.
④ 대칭키 암호 알고리즘은 비밀키 공유를 위한 키분배가 필요하지 않으면서도 암호화 및 복호화의 속도가 빠르다.
⑤ 공개키 암호 알고리즘은 자신만이 보관하는 비밀키를 이용하여 인증, 전자서명 등에 적용이 가능하다.

2. 다음 중 스트림 암호에 관한 설명으로 잘못된 것은?

① 스트림 암호란 작은 길이의 키로부터 긴 길이의 난수를 발생시켜 평문과 XOR 하는 방법을 말하며 SEAL, A5, f8 등이 있다.
② 동기식 스트림 암호는 암호문 중 한 비트가 손실되거나 추가되면 복호화가 불가능 하다.
③ LFSR의 선형 복잡도는 매우 높기 때문에 단독으로 사용한다.
④ 스트림 암호 알고리즘은 수학적 분석이 가능하여 주기, 선형복잡도 등의 수치에 대한 이론적인 값을 정확히 계산할 수 있다는 장점이 있다.
⑤ Nonlinear Combination Generator란 여러 개의 LFSR의 비선형 결합으로 만들어진 스트림암호를 말한다.

3. 다음 중 전자서명(digital signature)에 관하여 잘못 기술한 것은?

① 그림, 영상 등 대량의 메시지에 대한 전자서명을 위하여 문서 자체보다는 메시지의 해쉬값에 서명하게 된다.
② 타인에게 자신의 서명을 검증 받아야 하므로 전자서명 알고리즘은 주로 대칭키를 사용하는 블록암호를 기반으로 설계한다.
③ 전자서명된 문서를 타인이 검증해야 하므로 전자서명 알고리즘은 공개해야 한다.
④ 전자서명은 서명 된 문서의 내용을 삭제 또는 변경하는 것과 서명사실을 추후 부인하는 것 등이 불가능하도록 무결성 및 메시지 출처 인증 등을 제공한다.
⑤ 현재 사용되는 인감과는 달리 각 문서마다의 서명이 다르며, 다른 문서에 이미 사용된 서명을 재사용 할 수 없다.

4. 공개키 암호 알고리즘에 관한 다음 질문 중 잘못된 것은?

① RSA 암호는 임의의 정수에 관한 소인수분해 문제가 어렵다는 것에 기반하며, 같은 메시지에 대한 암호문이 항상 동일한 결정적(deterministic) 알고리즘이다.
② 확률 공개키 암호(probabilistic public-key encryption)는 같은 메시지라도 암호화 할 때마다 서로 다른 암호문을 얻는다.
③ 배낭(knapsack) 공개키 암호는 빠른 암복호화 속도와 안전성 때문에 널리 사용되는 대표적인 공개키 암호이다.
④ 유한체 위에 정의된 타원곡선을 기반으로 하는 타원곡선 암호는 빠른 속도와 제한된 대역폭을 요구하는 환경에 적합한 알고리즘이다.
⑤ Error-correcting code를 이용한 McEliece 공개키 암호 알고리즘은 공개키의 크기가 매우 커 실용적인 가치가 적다.

5. 다음 중 암호해독 방법이 아닌 것은?

① 암호문 단독 공격
② 기지 평문 공격
③ 기지 암호방식 공격
④ 선택 평문 공격
⑤ 선택 암호문 공격

6. 다음 중 디지털서명(Digital Signature)의 조건에 대한 설명으로 틀린 것은?

① 위조 불가 조건 (Unforgeable): 합법적인 서명자만이 전자 문서에 대한 전자 서명을 생성할 수 있어야 한다.
② 서명자 인증 조건(Authentic) : 전자 서명의 서명자를 누구든지 검증할 수 있어야 한다.
③ 부인 불가 조건 (Nonrepudiation) : 서명자는 서명 후에 자신의 서명 사실을 부인할 수 없어야 한다
④ 변경 불가 조건 (Unalterable) : 서명한 문서의 내용은 변경될 수 없어야한다
⑤ 재사용 조건(Reusable) : 전자 문서의 서명은 다른 전자 문서의 서명으로 사용될 수 있어야 한다.

7. 스트림암호 설계원리 중 시각제어논리가 아닌 것은?

① Casecade Generator
② Stop and Go Generator
③ Alternating Step Generator
④ Nonlinear Filter Generator
⑤ Shringking Generator

8. 주어진 암호문에서 평문과 연관이 있는 다른 암호문을 생성하는 것이 불가능한 성질을 무엇이라 하는가?

① Non-malleability(NM-안전성)
② 다항식 안전성
③ 계산적 안전성
④ 구별불능 안전성
⑤ 무조건적 안전성

9. 정보보호조직과 관련된 설명 중 잘 못된 것은 ?

① 정보보호위원회의 주된 역할은 정보보호정책을 수립하는 것이고, 정보보호에 관한 명령체계와 정보보호 표준 및 지침을 승인한다.
② 정보보호위원회에서는 정보보호 프로그램을 실행해서, 그 효과를 검토하며 이에 필요한 인적 및 물적 자원을 마련하는 것이다.
③ 정보보호관리자는 비상상황 발생시에, 장애 및 재난 복구를 수행한다.
④ 정보보호관리자의 책임은 정보보호 프로그램을 실행을 감독하고, 정보보호에 관한 정책, 명령체계, 정보보호의식 프로그램 등을 유지관리 하는 것이다.
⑤ 정보보호관리자는 정보보호 사고를 조사하고, 정보보호위원회에 제반사항을 보고하는 것이다.

10. 정보보호정책의 중요성에 대한 설명 중 틀린 것은 ?

① 정보보호정책은 정보보호제품의 구입이나 개발의 방향을 제시해 주고, 조직의 실제적인 정보보호 요구사항을 충족시키게 해준다.
② 정보보호정책은 조직 내의 하부구조가 정보보호 제품 및 시스템을 수용 및 구축을 가능케 하는 출발점이다.
③ 정보보호정책은 조직 내의 모든 부서에 적용할 수 있는 최저의 정보보호수준을 정의하기 위해서 사용될 수 없다.
④ 정보보호정책은 최고 관리자가 정보자원의 보호에 대한 지원을 제시한 중요 문서이다.
⑤ 정보보호정책은 정보보호에 대한 예산 및 인력을 확보하고, 투자의 중복을 회피할 수 있게 한다.

11. 위험관리 관점에서 아래 대안 중 수용하기 어려운 대안은?

① 위험을 사전에 예방
② 위험을 보험회사에 가입함으로써 제3자에게 전가
③ 위험을 정보보호 대책을 구현함으로써 감소
④ 위험을 지연시키는 방안
⑤ 잔여 위험을 수용

12. 논리적/물리적/관리적 정보보호대책(safeguards 혹은 controls)의 분류체계 중에서 논리적 정보보호대책이 아닌 것은 ?

① 소프트웨어 접근제어
② 임무분리(seperation of duty)
③ 소프트웨어 개발 및 변경통제
④ 데이터 정보보호
⑤ 통신 정보보호

13. 국제공통평가기준(CC: Common Criteria)에서 보안요구사항의 계층관계에 대한 설명 중에서 틀린 것은 ?

① 보안요구사항은 클래스 - 패밀리 - 컴포넌트 순의 계층관계를 갖는다.
② 클래스는 보안요구사항에 대한 가장 일반적인 그룹을 나타내며, 한 클래스 내의 구성요소는 패밀리라는 용어로 정의된다.
③ 패밀리는 보안요구사항들의 집합으로서, 한 패밀리 내의 구성요소를 컴포넌트라고 한다.
④ 각 컴포넌트 간에는 독립성이 존재한다.
⑤ 각 컴포넌트 마다 반복, 할당, 선택, 정교화 등 허용 오퍼레이션을 정의한다.

14. 업무연속성계획(BCP)을 검토할 경우, 정보보호관리자는 다음 시나리오 중에서 가장 중요하게 검토해야 하는 것은 어느 것인가?

① 가장 발생확률이 높은 시나리오.
② 낙관적인 시나리오.
③ 비관적인(최악의) 시나리오
④ 비용이 가장 많이 소요되는 시나리오
⑤ 모든 가능한 시나리오

15. 정보보호 관리자의 역할 중 가장 먼저 수행되어야 하는 작업은?

① 통제
② 계획 수립
③ 조직화
④ 명령/지시
⑤ 조정

16. 정보보호 조직의 위상은 보고(reporting) 대상을 누구로 결정하는 가에 달려 있다. 이때 고려해야 할 점 중 틀린 것은?

① 가능한 한 높은 위치에 있는 관리자에게 보고하는 것이 좋다
② 기술적인 내용을 이해할 수 있는 정보시스템 부서장이나 감사 부서장에게 보고하는 것이 좋다
③ 이상적으로는 CIO, COO에게 보고하는 것이 바람직하다
④ 조직 내 자원을 많이 가지고 있으며 최고경영자와 의사소통이 가능한 고위직 관리자에게 보고하는 것이 좋다
⑤ 조직 내 위험관리 부서나 정보자원관리 부서장에게 보고하는 것이 바람직하다.

17. 조직은 정보시스템 보안 기능을 어떻게 간주하는 것이 가장 바람직한가?

① profit center
② cost center
③ risk center
④ business enabler
⑤ business inhibitor

18. 다음 중 정보시스템 보안 관리자의 기능이 아닌 것은?

① 새로운 사용자 계정의 생성
② 새로운 사용자 계정의 승인
③ 새로운 보안 소프트웨어의 구현
④ 새로운 보안 대책의 설치 및 운영
⑤ 새로운 패스워드의 발부

19. 보안 관리자가 업무연속성계획을 검토할 때, 다음 중 어떤 시나리오를 가장 면밀하게 검토해야 하는가?

① 낙관적인 시나리오 (optimistic case)
② 비관적인 시나리오 (pessimistic case)
③ 가능성이 높은 시나리오 (most likely case)
④ (A)와 (B)의 중간 시나리오
⑤ 모든 시나리오

20. 보안위험을 평가하는 과정에서 사용하는 기법들 중에서 전문가 그룹을 활용하여 의사결정을 하는 방법은?

① 델파이 기법 (Delphi method)
② 전문가 시스템 (expert system)
③ 위험평가 감사 (risk assessment audit)
④ 동료 검토 (peer review)
⑤ 시나리오 기반 평가 (scenario-base evaluation)

21. 최고경영자나 주주들에게 정보보호에 대한 투자의 필요성을 주장하고자 할 때, 정보보호 투자수익율(ROSI)을 기반으로 정당화할 수 있다. ROSI에 대한 설명 중 틀린 것은 무엇인가?

① 분석단계에서의 ROSI가 운영단계에서의 ROSI보다 높다
② 수익(Return)은 흔히 손실규모의 감소 정도로 측정된다
③ 수익(Return)은 조직 전반에 걸친 정보보호 투자효과를 모두 고려해서 산정할 필요가 있다
④ ROSI가 낮을수록 좋다
⑤ 계량화 안되는 수익은 ROSI에 포함될 수 없다

22. 금융·통신 등 분야별 정보통신기반시설을 보호하기 위한 업무를 수행하고자 하는 자에 관한 설명으로 틀린 것은?

① 정보공유·분석센터의 구축, 운영시 정부의 기술적 지원
② 센터 업무종사자의 인적사항을 관계중앙행정기관의 장에게 통지
③ 외부의 정보침해에 대비하여 정보공유·분석센터의 구축, 운영의 제한
④ 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
⑤ 침해사고가 발생하는 경우 실시간 경보·분석체계 운영

23. 다음 중 정보화시책의 기본원칙에 속하지 아니하는 것은?

① 청소년보호, 스팸메일의 차단 및 정보등급제 시행을 위한 대책강구
② 지역적·경제적 차별이 없는 균등한 조건의 보편적 역무 제공
③ 정보통신기반에 대한 자유로운 접근과 활용
④ 환경변화에 능동적으로 대응하는 제도의 수립·시행
⑤ 민간투자의 확대와 공정경쟁 촉진

24. 전자서명법에 규정한 전자서명의 효력을 바르게 설명한 것은?

① 다른 법령에서 문서 또는 서면에 서명날인을 요하는 경우 전자문서에 공인전자서명이 있을 때에는 이를 충족한 것으로 추정한다.
② 다른 법령에서 문서 또는 서면에 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 추정한다.
③ 공인전자서명 외의 전자서명은 당사자 간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.
④ 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 간주한다.
⑤ 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 간주한다.

25. 다음중 개인정보 보호와 관련하여 14세미만 아동의 법정대리인이 행사할 수 있는 권리에 해당하지 않는 것은 ?

① 개인정보 수집, 이용 및 제3자 제공에 대한 동의권한
② 동의철회권
③ 개인정보 열람청구권
④ 개인정보 오류정정청구권
⑤ 자료요청권

26. 공개키 암호 시스템의 장점이 아닌 것은?

① 키의 분배가 용이함
② 키의 길이가 짧음
③ 사용자의 증가에 따라 관리할 키의 개수가 상대적으로 적음
④ 키 변화의 빈도가 적음
⑤ 개인키만 비밀로 보관하면 됨

27. 1985년 Miller와 Koblitz에 의해 독립적으로 제한된 암호 알고리즘으로 디지털 서명, 비밀키의 안전한 분배 그리고 보안을 요하는 정보의 안전한 전송에 이용되므로 무선통신, 서명, 인증 등 빠른 속도와 제한된 대역폭 등이 요구되는 무선통신 분야에 유용한 암호 알고리즘은?

① 타원곡선 공개키 암호
② ElGamal 공개키 암호
③ RSA 공개키 암호
④ Rabin 공개키 암호
⑤ Diffie-Hellman 공개키 키 공유 알고리즘

28. 다음 위임서명의 설명 중 틀린 것은?

① 서명을 해야 할 사람이 부재중에 자신을 대리해서 서명을 할 수 있는 서명 방식이다
② 위임서명에서 서명자는 위임 서명자에게 자신의 비밀키를 포함시킨 위임 서명키를 비밀리에 위임 서명자에게 전달해야 한다.
③ 위임서명은 위임 서명키 생성 및 전달과정과 위임서명과정으로 구성된다
④ 위임서명을 확인하는 검증자는 위임서명을 위임한 원래 서명자의 동의가 있었음을 확인하기 위해 서명자에게 확인절차를 거쳐야 한다.
⑤ 위임서명을 생성할 수 있는 사람은 서명자로부터 위임 서명자로 지정된 사람만이 가능하고 제삼자는 생성할 수 없다.

29. 다음은 RSA 공개키 암호의 시스템 변수와 관련된 내용으로 잘못된 것은?

① 공개키 e와 개인키 d는 $ed \equiv \mod(f(n))$의 관계식을 만족한다.
② 암호화의 속도를 증가하기 위하여 공개키의 크기를 작게 선택하면 일반적으로 복호화는 암호화보다 속도가 느리다.
③ 두 소수 p와 q는 거의 같은 크기로 선택한다.
④ p-1과 q-1은 작은 소인수들로 이루어져야 한다.
⑤ 두 소수의 곱 n=pq을 인수분해 하는 것과 f(n)의 값을 구하는 것은 동치이다

30. 다음 지문은 DSA 알고리즘의 서명 생성과정을 설명하고 있다. 잘못된 것은?

① 미국 NIST에서 제안된 표준 디지털 서명 알고리즘이다.
② 서명 생성 및 검증 과정을 위해서는 modular 연산의 구현이 필요하다.
③ ElGamal 형태의 메시지 부가형 서명 알고리즘이다.
④ 메시지 m에 대한 서명 (r, s)를 생성한다.
⑤ 비밀키 생성을 위한 256비트 소수인 p와 q를 사용한다.

31. 다음 중 개인 식별 방법이 아닌 것은?

① 사용자의 공개키를 이용하는 방법
② 사용자의 고유의 물리적 특성을 이용하는 방법
③ 사용자가 알고 있는 정보를 이용하는 방법
④ 사용자가 소지하고 있는 것을 이용하는 방법
⑤ 영지식 개인 식별 방식을 이용하는 방법

32. 해쉬함수 h의 성질에 관한 설명 중 틀린 것은?

① 역상저항성은 주어진 임의의 출력값 y에 대해 y=h(x)를 만족하는 입력값 x를 찾는 것이 계산적으로 불가능한 성질이다.
② 두 번째 역상 저항성은 주어진 입력값 x에 대해 h(x)=h(x')를 만족하는 다른 입력값 x'(^{1}x)을 찾는 것이 계산적으로 불가능한 성질이다.
③ 충돌 저항성은 h(x)=h(x')를 만족하는 두 입력값 x와 x'을 찾는 것이 계산적으로 불가능한 성질이다.
④ 충돌 저항성은 두 번째 역상 저항성을 보장한다.
⑤ 충돌 저항성은 역상 저항성을 보장한다.

33. 블록 암호의 공격법에 대한 설명으로 올바르지 않은 것은 무엇인가?

① 암호 함수의 입력을 특정한 형태로 변경시켰을 때 높은 확률로 출력이 특정한 형태로 변경되는 특성을 찾아 공격하는 방법을 차분공격(Differential Cryptanalysis)이라 한다.
② 비선형성 암호 논리와 높은 확률로 일치하는 선형 함수를 찾아 공격하는 방법을 선형공격(Linear Cryptanalysis)이라 한다.
③ 여러 개의 입력을 변화시켰을 때 암호 함수의 출력이 유사한 유형으로 변경되는 특성을 찾아 공격하는 방법을 포화공격(Saturation Attack)이라 한다.
④ 높은 확률의 차분 특성에 선형근사식의 개념을 적용하여 공격하는 방법을 차분-선형 공격(Differential -Linear Cryptanalysis)이라 한다.
⑤ 라운드 함수와 라운드 키가 동일한 경우 효과적으로 키를 찾는 방법을 Slide attack이라 한다.

34. 정보보호관리 프로세스의 구체적인 과정으로 올바른 것은?

(1) 전사적인 정보보호정책 수립
(2) 정보보호조직의 역할과 책임
(3) 위험분석전략의 선택
(4) 정보시스템에 대한 정보보호 정책 및 계획 수립
(5) 위험의 평가 및 정보보호(통제)대책의 선택
(6) 정보보호(통제)대책의 설치 및 보안의식 교육
(7) 보안감사 및 사후관리

① 1 - 2 - 3 - 4 - 5 - 6 - 7
② 1 - 2 - 4 - 3 - 5 - 6 - 7
③ 1 - 4 - 2 - 3 - 5 - 6 - 7
④ 1 - 2 - 4 - 5 - 3 - 6 - 7
⑤ 1 - 2 - 3 - 5 - 4 - 6 - 7

35. 업무연속성관리(BCM: Business Continuity Management)를 위한 여러 활동은 일종의 생명주기(life-cycle)로서 간주할 수 있다. 아래 설명은 어떤 단계에 대한 설명인가?

재해가 업무에 미치는 잠재적인 영향 및 위험을 평가하고 위험감소 및 업무 프로세스 복구를 위한 여러 옵션을 파악한 후 평가하여, 업무연속성관리를 위한 비용효과적인 전략을 수립하는 프로세스이다. 이 단계에 업무영향분석(BIA: Business Impact Analysis) 및 위험평가를 실행한다.

① 개시단계
② 전략수립단계
③ 구현단계
④ 운영관리단계
⑤ 위험감소단계

36. 조직의 정보시스템에 대한 보안성을 확보하는데 궁극적인 책임이 있는 사람은?

① 현업 관리자
② 시스템 소유자(owner)
③ 보안 관리자
④ 시스템 관리자
⑤ 사용자

37. 다음 중 업무연속성계획이 추구하는 가장 중요한 목적은?

① 신속한 서비스 재개를 통한 고객 불편의 최소화
② 재해로 인한 조직의 생존성 위협으로부터 지속적인 업무의 수행
③ 고품질의 대량생산을 위한 중단 없는 연속된 업무의 흐름
④ 대외 신인도 저하 방지
⑤ 보험 가입을 통한 피해액 보전

38. 정보보호 정책, 절차 및 대책을 수립하면서 부서간 이해 대립이 발생하였을 경우, 가장 적절한 해결책은?

① 최고 경영자에게 유권 결정을 요청한다.
② 보안 관리자의 전문가로서의 판단에 따른다.
③ 정보시스템 감사인이 사안을 평가한 후 결정을 내린다.
④ 각 부서장들로 구성된 정보보호 위원회에 안건을 회부한다.
⑤ 해당 부서 당사자 간의 해결을 기다린다.

39. 다음 중 정보보호 관리의 목적으로 가장 적절한 것은?

① 모든 정보보호 위험을 제거한다.
② 구성원들의 정보보호 인식을 제고한다.
③ 고객의 개인정보를 안전하게 보호한다.
④ 수용 가능한 수준으로 정보보호 위험을 통제한다.
⑤ 정보보호 사고를 예방한다.

40. 다음 중 매우 큰 규모의 조직에서 처음으로, 또는 기존에 위험분석을 수행한 조직에서 재차 위험분석을 수행할 때 적합한 분석 방법은?

① 베이스라인 접근법
② 비정형 접근법
③ 상세 위험분석
④ 베이스라인 접근법과 상세위험분석을 결합한 혼합 접근법
⑤ 상위 수준 위험분석

41. 다음 중 취약점에 대한 설명으로 맞지 않는 것은?

① 주기적인 취약점 진단과 패치의 적용으로 취약점의 완전 제거가 가능하다.
② 위협에 의하여 이용된다.
③ 취약점이 없는 시스템은 없다.
④ 정보시스템 또는 정보보호시스템의 결함 또는 손실을 말한다.
⑤ 정보보호 대책은 정보보호 취약점을 감소시키는 것이다.

42. 다음 사항 중 정보보호에 대한 일반적인 원칙이 아닌 것은?

(1) 정보보호의 궁극적인 목적은 완벽한 정보보호 시스템을 구축하는 것이다.
(2) 정보보호는 조직문화에 의해 제한을 받아야 한다.
(3) 정보보호는 포괄적이고 통합적인 접근방법으로 접근해야 한다.
(4) 정보보호는 조직의 관리활동에 있어 적절한 주의 의무(due care)에 포함되어야 한다.
(5) 외부위탁으로 수행되는 정보서비스에 대한 정보보호의 궁극적인 책임은 위탁서비스 제공 업체에 있다.

① 1, 2
② 1, 4
③ 2, 5
④ 1, 5
⑤ 2, 4

43. 주요 정보통신기반시설의 지정 및 취약점 분석에 해당하는 내용으로 잘못된 것은?

① 주요 정보통신기반시설의 지정 및 지정 취소 등에 필요한 사항은 이를 대통령령으로 정한다.
② 관계 중앙행정기관의 장은 관리기관이 해당 업무를 폐지, 정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다.
③ 지방 자치단체의 장이 관리, 감독하는 기관의 정보통신기반시설에 대하여는 행정자치부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정할 수는 있으나 그 지정을 취소할 수는 없다.
④ 중앙행정기관의 장은 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하여야 한다. 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 아니할 수 있다.
⑤ 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석, 평가하여야 한다.

44. BS 7799에 대한 설명 중 틀린 것은?

① 영국 표준으로서 두 개의 문서로 구성되어 있다
② Part 1은 2000년 국제표준이 되었으며 ISMS 인증을 위한 문서이다.
③ Part 1은 정보보호 관리를 위한 모범적 실무사례(best practices)을 포함하고 있다
④ Part 2는 P-D-C-A 사이클에 따라 정보보호관리체계를 서술하고 있다
⑤ Part 2는 2002년에 경영시스템 관점에서 재구성되어 V.2가 발표되었다.

45. 조직에서 정보보호가 성공적으로 정착되기 위해서 필요한 요인이 아닌 것은?

① 정보보호에 대한 부정적인 결과(손실)보다는 긍정적인 영향(비교우위 창출)을 강조함으로써 정보보호에 대한 인식을 전환시킬 필요가 있다.
② 조직의 특성에 적절한 정보보호 조직을 구성하고 조직 구성원에 대한 역할과 책임을 명확히 할 필요가 있다.
③ 최고경영층의 지원이 절대적이며 이를 위해서는 위험분석이나 타이거팀을 통한 침투훈련 등을 사용하여 최고경영층의 경각심을 높일 필요가 있다.
④ 정보보호가 효과적으로 수행되기 위해서는 적절한 투자와 인력이 배치되어야 한다.
⑤ 반드시 정량적 위험분석을 통해 객관적이고 통계에 기초한 위험을 산출하고 이에 근거하여 정보보호 프로그램을 수립해야 한다.

46. 다음 중 효과적인 전사적 정보보호 정책 수립을 위해 가장 중요하고 근본적인 성공 요소는?

① 비용 대비 효과를 극대화하기 위한 철저한 타당성 분석
② 최고 경영진의 적극적인 참여와 지원
③ 위반자에 대한 처벌을 포함한 가시적인 보안규칙의 집행

④ 타사 보안정책에 대한 포괄적인 벤치마킹
⑤ 조직 전체 구성원의 참여와 의견수렴

47. 전자거래기본법상 용어의 정의로 틀린 것은?

① 정보처리시스템이라 함은 전자문서의 작성, 송신, 수신 또는 저장을 위하여 이용되는 정보처리 능력을 가진 전자적 장치 또는 체계를 말한다.
② 작성자라 함은 전자문서를 작성하여 송신하는 자를 말한다.
③ 수신자라 함은 작성자가 전자문서를 송신하는 상대방을 말한다.
④ 전자거래라 함은 재화나 용역을 거래함에 있어서 그 전부 또는 일부가 전자문서에 의하여 처리되는 거래를 말한다.
⑤ 전자거래사업자라 함은 전자거래를 이용하는 자로서 전자거래이용자라고도 한다.

48. 정보화촉진기본계획수립에 관한 다음 설명으로 틀린 것은?

① 민간업무의 정보화촉진에 관한 사항
② 정보통신부장관이 관계중앙행정기관별 부문계획을 종합하여 수립하며, 정보화추진위원회의 심의를 거쳐 확정한다.
③ 산업분야의 정보화촉진에 관한 사항
④ 재정, 금융 분야의 정보화촉진에 관한 사항
⑤ 교육, 연구, 과학기술분야의 정보화촉진에 관한 사항

49. 전자거래기본법상 전자거래의 안전성 확보 및 소비자보호에 관한 설명으로 틀린 것은?

① 전자거래사업자는 전자거래이용자의 영업비밀을 보호하기 위한 조치를 강구하여야 한다.
② 정부는 전자거래의 안전성 및 신뢰성을 확보하기 위하여 전자거래이용자의 영업비밀을 보호하기 위한 시책을 수립하여 시행하여야 한다.
③ 정부는 국가안전보장을 위하여 필요하다고 인정하는 경우에는 암호제품의 사용을 제한하고, 암호화된 정보의 원문 또는 암호기술에의 접근에 필요한 조치를 할 수 있다.
④ 전자거래사업자는 특수한 경우에는 전자거래이용자의 동의를 얻지 아니하고 당해 이용자의 영업비밀을 타인에게 제공할 수 있다.
⑤ 정부는 전자거래와 관련된 부당행위가 발생하지 아니하도록 전자거래사업자 및 사업자단체에게 자율적으로 행동규범을 제정할 것을 권장할 수 있다.

50. 다음 중 정보통신서비스제공자의 개인정보보호 의무에 관한 설명으로 옳은 것은?

① 개인정보라 함은 생존여부와 관계없이 개인에 관한 정보로서 성명, 주민등록번호 등에 의해 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보를 말한다.

② 정보통신망법의 개인정보보호조항은 정보통신서비스제공자 이외의 자에게도 준용된다.
③ 정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우 당해 이용자의 서면동의를 얻어야 한다.
④ 개인정보관리책임자는 임원만으로 지정하여야 한다.
⑤ 이용자가 개인정보를 제공하지 아니하는 경우 정보통신서비스제공자는 무조건 서비스 제공을 거부할 수 있다.

51. 정보통신서비스 제공자는 이용자의 동의를 얻어 개인정보를 수집하는 경우에 이용자에게 고지하거나 정보통신서비스 이용약관에 그 내용을 명시하여야 한다. 이에 속하지 않는 것은?

① 개인정보의 보호를 위한 기술적 방법
② 개인정보관리책임자의 성명, 소속부서, 직위 및 전화번호 기타 연락처
③ 개인정보의 수집목적 및 이용목적
④ 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공목적 및 제공할 정보의 내용
⑤ 개인정보 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항

52. 대화형 프로토콜이 대화형 증명 시스템(Interactive proof system)이 되기 위해서 필요한 조건은 무엇인가?

가. 영지식성(Zero-Knowledge)
나. 완전성(Completeness)
다. 건전성(Soundness)
라. 구별불가능성(indistinguishable)

① 가, 나
② 나, 다
③ 다, 라
④ 나, 라
⑤ 가, 다,

53. RSA 암호를 구현하기 위한 parameters의 설정에 관한 설명 중 잘못된 것은?

① 개인의 비밀정보인 p와 q의 크기는 거의 같아야 한다.
② 개인의 비밀정보인 p와 q 값을 설정할 때, p - q의 값은 크게 선택해야 한다.
③ 개인의 비밀정보인 p를 설정할 때, p - 1이 큰 소수를 갖도록 선택해야 한다.
④ 개인의 비밀정보인 p를 선택할 때, p + 1이 큰 소인수를 가져야 한다.
⑤ 개인의 비밀정보인 p와 q가 충분히 큰 경우라도 랜덤(random)하게 선택할 수 없다.

54. AES 알고리즘으로 선정된 RIJNDAEL에 관한 설명으로 올바른 것은?

① 블록암호로서 블록의 크기는 128비트를 기본으로 하며 160, 192비트를 이용할 수 있다.
② 키의 길이는 안전성 확보를 위해 160비트를 기본으로 한다.
③ 암호화 및 복호화 과정에 필요한 라운드 수는 고정값이며 총 12라운드이다.
④ Rijndael은 블록암호로서 SPN 구조와는 달리 Feistel 구조를 갖는다.
⑤ 대칭키 암호 알고리즘이지만 암호화 과정과 복호화 과정은 서로 일치하지 않는다

55. 다음 중 난수(random number) 발생 방법에 관한 설명 중 잘못 된 것은?

① 난수란 주어진 구간에서 통계적 독립이고 예측 불가능하며 편중되지 않은 수를 말한다.
② ANSI X9.17에서는 블록암호에 기반한 난수 발생기를 정의한다.
③ 카오스 방정식 또는 선형 합동법(LCM : Linear Congruential generators)을 이용한 난수 발생기는 출력값이 난수성을 갖는 우수한 난수 발생기이다.
④ RSA와 같은 공개키 암호를 이용하는 난수발생기는 효율성이 떨어지지만, 암호학적으로 안전한 난수 발생기를 제공한다.
⑤ Blum-Blum-Shub 의사 난수 발생기는 인수분해 문제가 어렵다는 가정 하에 암호학적으로 안전한 의사 난수 발생기이다.

56. 다음 중 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 초기치환(initial permutation)은 입력 64비트를 출력 64비트로 변환하는 과정이다.
④ DES의 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.

57. 다음 설명 중 틀린 것은?

① 다항식 시간 내에 해결 가능한 모든 결정 문제의 집합을 복잡도 P라 한다
② 복잡도 NP는 No의 응답이 다항식 시간의 certificate라는 부가 정보를 사용하여 다항식 시간 내에 검증 가능한 모든 문제의 집합이다.
③ n이 입력의 크기이고 k가 상수일 때 가장 나쁜 경우의 수행시간이 O(nk)인 알고리즘을 다항식 시간 알고리즘(polynomial time algorithm) 이라 한다
④ 주어진 암호 시스템이 임의의 평문 x와 암호문 y에 대해서 조건부 확률 p(x|y)와 확률 p(x)가 같으면 절대적 안전성을 갖는다고 한다
⑤ 유한개의 사건을 가지는 확률변수 X에 대한 확률분포 p(X)를 알 때, 발생하지 않은 사건의 불확실도를 엔트로피(entropy)라 하여 정보량 또는 정보의 불확실도를 측정하는 수학적 개념이다.

58. 다음 타원곡선 암호시스템의 설명 중 틀린 것은?

① 타원곡선 암호는 타원곡선 상에 정의된 군(타원곡선군)에서의 이산대수 문제(ECDLP)를 기반으로 한다
② RSA와 ElGamal 보다 키 사이즈가 작고 효율적이어서 스마트카드, 핸드폰 등 모바일 환경에 적합하다
③ 일반적인 타원곡선 이산대수문제를 구하는 준지수 알고리즘이 존재한다
④ 기존의 공개키 암호시스템과 같은 안전도를 제공하는데 더 작은 키의 길이를 가지고 가능하다
⑤ 타원곡선에서의 연산은 유한체에서의 연산을 기반하므로 하드웨어와 소프트웨어로 구현하기 용이하다

59. 위험 분석 전략의 선택으로 네 가지 접근 방법은 무엇인가?

① 통합적인 접근, 비공식적인 접근, 세부적인 접근, 복합적인 접근
② 기본적인 접근, 공식적인 접근, 세부적인 접근, 복합적인 접근
③ 기본적인 접근, 비공식적인 접근, 세부적인 접근, 복합적인 접근
④ 통합적인 접근, 공식적인 접근, 세부적인 접근, 복합적인 접근
⑤ 기본적인 접근, 비공식적인 접근, 세부적인 접근, 통합적인 접근

60. 보안사고 대응 계획 구축단계로 올바른 것은?

<보기>

(가) 문서화
(나) 공지와 알림
(다) 보안사고 판단
(라) 손실범위 평가
(마) 사고원인 제거
(바) 복구
(마) 사고범위 식별

① (가) → (나) → (다) → (라) → (마) → (바) → (사)
② (가) → (나) → (다) → (라) → (마) → (사) → (바)
③ (가) → (다) → (나) → (사) → (라) → (마) → (바)
④ (가) → (사) → (다) → (라) → (마) → (바) → (나)
⑤ (가) → (다) → (나) → (라) → (마) → (바) → (사)

61. 위험 관리와 위험 분석에 대한 설명 중 잘못된 것은?

① 위험 관리는 위험 분석과 위험 평가로 주된 활동이 결정된다.
② 위험 관리는 보호 대상, 위협 요소, 취약성 분석 등을 통한 위험 분석이 포함된다.
③ 위험 평가는 분석 결과를 기초로 현황을 평가하고 적절한 방법을 선택하여 효과적으로 위험수준을 낮추기 위한 과정이다.
④ 위험 관리는 적절한 메커니즘의 선택, 선택된 메커니즘의 구현과 시험, 구현된 메커니즘의 보안성 평가, 종합적인 보안의 재평가를 포함한다.
⑤ 위험 분석은 위험을 분석하여 적절한 보안 대책을 결정하는 단계이다.

62. 보안 관리는 통상적인 정보 시스템 관리에 추가되어 관리되어야 한다. 다음 중 보안 관리 영역이 아닌 것은?

① 식별자(ID) 관리
② 인증 관리
③ 권한 부여 관리
④ 모니터링
⑤ 책임 추적성(accountability) 관리

63. 위험 분석 방법론에는 정량적 위험 분석 방법과 정성적 위험 분석 방법이 있다. 다음 중 정량적 위험 분석 방법이 아닌 것은?

① 과거 자료 분석법
② 수학 공식 접근법
③ 점수법
④ 델파이법
⑤ 확률분포법

64. 시스템 복구를 위해서 다양한 방식들이 사용되는데 다음은 어떤 방식을 설명한 것인가?

<보기>
재난 발생으로 영향을 받는 업무 기능을 즉시 복구할 수 있도록 전산 센터와 동일한 모든 설비와 자원을 보유하고 있는 거의 완전한 시설로서 수 시간 안에 가동이 이루어 질 수 있다.

① 중복 시스템 운영
② 핫 사이트(hot site) 운영
③ 웜 사이트(warm site) 운영

④ 콜드 사이트(cold) 운영
⑤ 레드 사이트(red site) 운영

65. COBIT에 대한 설명으로 옳지 않은 것은?

① COBIT은 정보시스템관리를 위한 기술적인 표준이다
② COBIT은 IT 보호 및 통제 부분에서의 모범적인 업무 수행 방법에 대한 일반적으로 적용 가능하고 인정되는 기준이다
③ COBIT은 1996년에 최초로 초판이 나오게 되었다
④ 2판까지는 정보시스템이라는 관점에서 구성되어 있었다
⑤ COBIT의 프레임워크는 통제목표를 달성하기 위한 전체적인 틀을 제시하고 있다

66. 업무 연속성 관리 과정에서 테스트, 교육과 경각심 제고, 훈련, 변경, 보증 등과 같은 프로세스로 구성되어 있는 단계는?

① 평가 단계
② 시작 단계
③ 구현 단계
④ 전략 수립 단계
⑤ 운영 관리 단계

67. 다음은 무엇을 설명하는 것인가?

<보기>

(가) 정보보호 시스템의 성능과 신뢰도를 평가하기 위한 정보보호 평가 기준
(나) 1980년대부터 작성
(다) 오렌지 북
(라) A, B, C, D 등 네 개의 등급으로 나눔

① FC
② CSSI
③ TDI
④ TNI
⑤ TCSEC

68. 다음 중 BS7799 기준에서 제시한 정보보호 관리체계를 수립하는 절차를 순서대로 올바르게 기술한 것은?

① 보안정책 수립-> 정보보호 관리체계 범위 수립 ->위험평가 -> 위험관리 ->통제 및 통제 목표 선정 -> 통제사항 적용명세서 작성
② 정보보호 관리체계 범위 수립 -> 보안 정책 수립-> 위험평가 -> 위험관리 ->통제 및 통제목표 선정 -> 통제사항 적용명세서 작성
③ 보안정책 수립 -> 정보보호 관리체계 범위 수립 -> 위험관리 -> 위험평가 ->통제 및 통제목표 선정 -> 통제사항 적용명세서 작성
④ 정보보호 관리체계 범위 수립 -> 보안정책 수립 ->-> 위험관리 -> 위험평가 ->통제 및 통제목표 선정 -> 통제사항 적용명세서 작성
⑤ 정보보호 관리체계 범위 수립 -> 보안정책 수립 -> 위험관리 -> 위험평가 -> 통제사항 적용명세서 작성-> 통제 및 통제목표 선정

69. 국제 공통기준(CC)은 크게 3가지 부분으로 되어 있는데 제 1부는 일반적인 소개와 일반 모델을 소개하고 있으며, 제 2부는 보안 기능 요구 사항, 제 3부는 보증 요구 사항을 제시하고 있다. 다음 중 보안 기능 요구 사항이 아닌 것은?

① 취약성 분석
② 보안 감사
③ 통신
④ 암호 지원
⑤ 사용자 개인 데이터 보호

70. 다음 기능 중 정보보증의 기능이 아닌 것은?

① 기밀성
② 무결성
③ 인증
④ 부인봉쇄
⑤ 신뢰성

71. 위험 관리를 위험 평가와 위험 완화 단계로 나눈다면, 다음 중 위험 완화 단계의 활동이 아닌 것은?

① 위험 측정
② 가능한 보안대책의 식별
③ 적절한 보안대책의 선택

④ 보안대책의 구현과 시험
⑤ 잔여 위험의 수용

72. 전자거래기본법상 전자문서의 보관에 관한 설명으로 잘못된 것은?

① 전자문서가 법이 정한 일정 요건을 갖춘 경우에는 그 전자문서의 보관으로 관계 법령이 정하는 문서의 보관에 갈음할 수 있다.
② 전자문서의 보관요건으로서 전자문서의 내용을 열람할 수 있어야 한다.
③ 전자문서의 보관요건으로서 전자문서가 작성 및 송신·수신된 때의 형태 또는 그와 같이 재현될 수 있는 형태로 보존되어 있어야 한다.
④ 전자문서의 보관요건으로서 전자문서의 작성자, 수신자 및 송신·수신일시에 관한 사항이 포함되어 있는 경우에는 그 부분이 보존되어 있어야 한다.
⑤ 전자문서의 보관요건으로서 전자문서의 송신 또는 수신만을 위하여 필요한 부분을 포함하여 전체에 관하여 기록이 완전하여야 한다.

73. 전자서명법상 공인인증기관이 당해 공인인증서를 폐지하여야 할 사유가 아닌 것은?

① 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우
② 가입자의 파산 또는 금치산 선고 사실을 인지한 경우
③ 가입자의 사망·실종선고 또는 해산 사실을 인지한 경우
④ 가입자가 사위(詐僞) 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우
⑤ 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 사실을 인지한 경우

74. 정보화촉진기본법상 정보화촉진시행계획의 수립 시행에 관한 설명이다. ( ) 안에 알맞은 말은?

<보기>
관계 중앙행정기관의 장은 정보화촉진기본계획에 따라 매년 정보화촉진시행계획을 수립 시행하여야 하고, 전년도의 (a)와[과] 다음 연도의 시행계획을 (b)에 제출하여 그 심의를 받아야 하며, 심의를 거쳐 확정된 정보화촉진시행계획의 시행에 필요한 (c)을 우선적으로 확보하여야 한다.

① a-시행계획 추진실적, b-국무회의, c-시설
② a-시행계획 추진실적, b-정보화추진위원회, c-재원
③ a-시행계획 평가결과, b-국무회의, c-시설
④ a-시행계획 추진실적, b- 정보화추진위원회, c-재원
⑤ a-시행계획 평가결과, b-국무회의, c-시설

75. 정보통신망이용촉진및정보보호등에관한법률상 정보통신망침해행위에 관한 규정의 내용 중 옳지 않은 것은?

① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하여서는 아니된다.
② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하여서는 아니된다.
③ 정당한 사유가 있는 경우에는 정보통신시스템, 데이터 또는 프로그램 등을 그 운용을 방해 할 수 있는 프로그램을 전달 또는 유포할 수 있다.
④ 정당한 사유가 있는 경우에는 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내는 방법으로 정보통신망에 장애를 발생하게 할 수 있다.
⑤ 정보통신부장관은 필요한 경우 침해사고에 적절히 대응하기 위한 업무의 전부 또는 일부를 보호진흥원으로 하여금 수행하게 할 수 있다.

SIS 1급 단답형

1. VPN에서 터널링 기술 중 많이 사용하는 (A) 기술은 MS사가 개발한 프로토콜로서 TCP연결을 사용하여 IP, IPX, NetBEUI 트래픽을 암호화하고 IP헤더를 캡슐화 하여 인터넷을 경유하여 전송하며, 하나의 터널에 하나의 연결만 지원한다. (B)기술은 (A)와 시스코에서 제안한 L2F기술을 결합한 방법으로써 터널을 유지하기 위하여 UDP와 일련의
(B)메시지를 사용한다

2. 가장 대중적으로 사용되는 스캐닝 프로그램인 nmap 은 많은 스캔 옵션을 제공한다. 이 중 아래는 TCP SYN 스캔에 대한 설명인데, 아래 설명에서 ( ) 에 공통적으로 들어가는 용어는 무엇인가? "SYN 스캔은 Full TCP 접속을 하지 않으므로 'half-open' 스캐닝이라 한다. 하나의 SYN 패킷을 보내어 SYN|ACK 응답이 오면 그 포트는 리슨하고 있는 상태이고, ( ) 응답이 오면 리슨하지 않는 것을 나타낸다. 이 기술은 하나의 패킷을 보내어 SYN|ACK 응답을 받으면 그 즉시 ( ) 패킷을 보내서 접속을 끊어버린다.

3. 다음은 어떤 해킹기술에 대한 대책이다. 어떠한 공격기법에 대한 대책인가?

* 운영체제의 커널 패치
* 함수로부터 복귀하기 전에 스택의 무결성 검사
* 스택에서의 쓰기 권한 제한
* 스택에서의 프로그램 실행금지
* 가능성이 있는 SUID 프로그램 제한

4. TCP/IP 프로토콜 그룹에 속한 프로토콜로서, RFC 792에 의하여 규정되어 있으며, echo, timestamp, redirects 등을 비롯한 다양한 작업 type들이 제공되는 프로토콜의 명칭은 무엇인가?

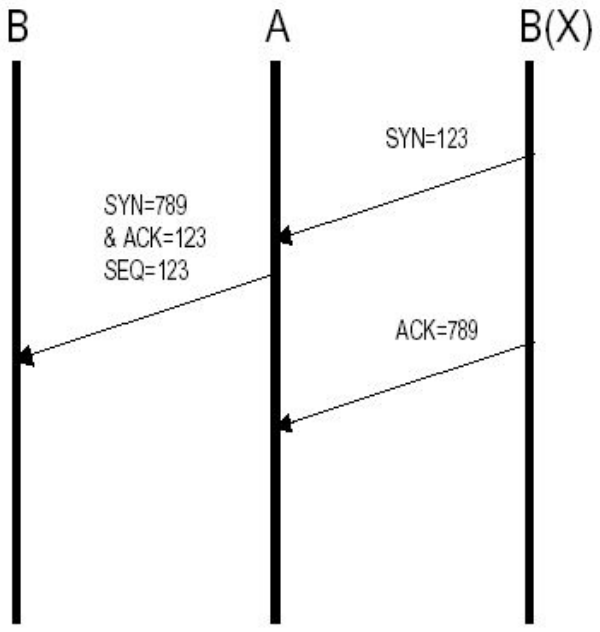
5. IDS의 탐지(Detection)와 Firewall의 차단(Blocking)능력을 결합하여 비정상행위(Anomaly detection)을 통해 알려지지 않은 공격 Pattern에 대응하여 명백한 공격(Attack)에 대해서는 사전 방지(Prevention) 조치하는 것으로 주로 In-Line방식으로 설치 및 운영되는 보안방식을 무엇이라고 하는가?

6. 중앙행정기관의 장은 소관분야의 정보통신기반시설중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을주요정보통신기반시설로 지정할 수 있으며, 그 해당 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 하며, 이 경우 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다.

이때에, 해당 관리기관의 장은 취약점을 분석·평가하고자 하는 경우에는 다음에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다. 다만, 이 경우 위의 전담반을 구성하지 아니할 수 있다.

여기에서 다음에 해당하는 기관(명)들을 모두 나열하시오.

7. 아래 그림은 tcp 의 취약성을 이용한 ip spoofing 공격방법에 대해 설명하고 있다. tcp 의 어떠한 취약성을 이용한 공격기법을 설명하고 있는가?
(참고 : B(X) 가 B 인 것처럼 가장하는 것을 나타낸다)



8. 다음은 모 월간 정보보호잡지 2002년 8월호에 실린 기사 중 일부이다.
아래 기사에서는 최근 보안업계에서 화자가 되고 있는 특정 보안 용어에 대한 역할을 업체마다 다르게 정의하고 있는 것을 보여주고 있는데, 여기에서 설명하는 보안 제품의 알맞은 용어는 무엇인가?

A 사 : 전사적 차원의 일관된 정책을 가지고 통합적으로 관제 및 운영관리 업무를 수행하는 체계
B 사 : User Administration 과 Management 취약점 분석이나 위험 평가 등의 Risk Assessment
C 사 : 각 정보보호 시스템으로부터 추출되는 이벤트로부터 의미 있는 데이터, 즉 정보보호 활동 또는 관리행위가 필요한 지를 판단해 주는 시스템
D 사 : 보안과 관련된 정책을 펼칠 수 있도록 이에 대한 제어까지 포함한 시스템

9. ( )은/는 기존의 전자우편 보안시스템의 문제점인 PEM 구현의 복잡성, PGP의 낮은 보안성과 기존 시스템과의 통합이 용이하지 않다는 점을 보완하기 위해 IETF의 작업 그룹에서 RSADSI(RSA Data Security Incorporation)의 기술을 기반으로 개발된 전자우편 보안시스템이다. ( )이 달성하고자 하는 목표는 강력한 암호화, 디지털 서명, 사용의 용이성, 융통성, 상호운용성, 수출가능성 등이 있다. 괄호에 공통으로 들어갈 적당한 것을 쓰시오.

10. 자산의 가치에 대한 손실이나 영향의 크기를 측정한 값으로 어떤 위협 사건으로부터 발생하는 자산가치의 손실을 백분율로 나타내는 수를 ( )계수라 한다. 괄호에 적합한 단어를 쓰시오.

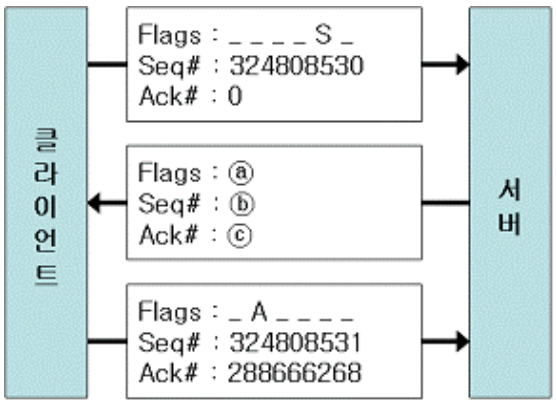
11. UNIX나 Linux 운영체제 프로그램 중 프로그램이 실행되는 동안 프로그램 소유자의 권한을 가지게 지정하는 방법을 (A) 비트로 표현한다. 만일 어떤 프로그램이 이 비트가 설정되어 있으면 파일 권한(permission bit)을 나타내는 정보 중 'x' 글자가 (B) 글자로 바뀌어 표시된다.

12. 침입탐지시스템(IDS)에는 호스트 컴퓨터에 저장된 로그 정보를 이용하여 침입을 탐지하는 (A), 통신망을 통해 전송되는 패킷 데이터를 분석하여 침입여부를 판정하는 (B)가 있다.
IDS 오동작으로 실제 이루어진 침입을 탐지하지 못하는 (C), 정상적인 행위를 침입으로 잘못 판정하는(D) 현상이 나타날 수 있다.

13. SSL 보안 프로토콜과는 달리 (A)은 IP 계층에서 다양한 보안 서비스 제공을 위한 프로토콜 보안 구조이다. (A)의 보안 프로토콜로는 (B)와 (C) 프로토콜이 있으며 각 보안 프로토콜은 Transport 모드와 Tunnel 모드로 동작한다.
(B)와 (C) 보안 프로토콜에서 사용하는 보안 파라미터들은
Security Association변수에 정의되어 있다

14. 국제 웹 보안 협회인 OWASP(Open Web Application Security Project) 에서 발표한 10대 웹 취약점 중 입력값 검증 공격은 모든 수정 가능한 데이터가 표적으로 이를 통해 발생 가능한 공격은 데이터베이스와 연동되어 있는 애플리케이션의 입력값을 조작하여 DBMS가 의도되지 않는 결과를 반환하도록 하는 (A)과 화면의 출력을 담당하고 있는 애플리케이션의 입력값에 Javascript와 같은 스크립트를 삽입하여 사용자 측에서 비정상적인 조작이 일어나도록 유도하는 (B)와 같은 공격 가능하다.

15. TCP 연결 설정은 3-웨이 핸드셰이크(3-way handshake) 방법이 사용된다. 다음 그림에서 두 번째 패킷의 내용을 기재하시오.



SIS 1급 서술형

1. 아래는 라우터에서의 Blackhole filtering(Null routing) 의 설정 예를 보여주고 있다. 이 설정을 통해 특정한 ip 나 ip 대역에 대하여 Null 0 인터페이스로 보내어 공격을 차단할 수 있는데, 이때 반드시 "no ip unreachables" 을 설정할 것을 권장하고 있다. 굳이 이 인터페이스가 아니더라도 모든 인터페이스에 이 설정을 하는 것이 좋은데, 이 설정이 필요한 두 가지 이유를 보안의 관점에서 서술하시오.

```
Router# config t
Router (config)# interface null0
Router (config-if)# no ip unreachables
Router (config-if)# exit
Router (config)# ip route 10.0.0.0 255.0.0.0 nul
```

2. 스팸메일과 관련하여 최근에 나타난 특이한 현상으로 스패머(스팸 메일을 보내는 사람)가 메일서버가 아닌 프락시 서버(Proxy Server)를 이용하여 스팸 메일을 발송하는 방식이 등장하여 앞으로 더욱 주목할 필요가 있다. 그렇다면 프락시 서버를 스패머가 이용할 수 있는 기술적 배경을 요약한 후, 이에 대한 대비책을 간단하게 제시하라.

3. 다음은 라우터에 대한 다양한 보안 설정을 변경하고 있는 과정을 나타내고 있다. 각 번호에 대하여 정확하게 설명하시오.

```
Router(config)#enable secret erqdfjz83                          (1)
-------------------------------------------------------------------
Router(config)#access-list 50 permit host 192.168.0.70          (2)
Router(config)#access-list 50 deny any                          (2)
Router(config)#snmp-server community iofdakdfja ro 50           (2)
-------------------------------------------------------------------
Router(config)#line con 0                                       (3)
Router(config)#exec-timeout 5 0                                 (3)
-------------------------------------------------------------------
Router(config)#loggin on                                        (4)
Router(config)#logging trap debugging                           (4)
Router(config)#logging 192.168.0.10                             (4)
```

SIS 1급 실무형

1. 일반적으로 방화벽의 설정을 다룰 때 가장 복잡하고 어려운 서비스가 바로 ftp 이다. 왜냐하면 ftp 의 경우 두 가지 서로 다른 작동방식이 있으며 다른 일반적인 tcp 프로토콜과 전혀 다른 방식으로 작동하기 때문이다. 여기에서 아래의 물음에 답하여라.

1) ftp 의 두 가지 작동 방식이 각각 어떠한 차이점이 있는지에 대해 설명하고
2) 각각의 방식이 보안의 관점에서 어떠한 단점이 있는지 비교하여 서술하라.

(그림과 함께 설명해도 된다)

2. Sendmail은 버전 8.9부터는 스팸 메일에 대한 예방책으로 anti-spam기능이 추가되었다. 구체적으로 보면, Access DB라는 새로운 데이터베이스를 도입해서 이것의 설정에 따라 특정 메일들을 받지 않도록 할 수가 있으며, 스팸 메일 릴레이 기능도 막을 수 있다. 다음과 같은 조건을 만족하도록 Access DB를 구성한 후, 이를 반영하여 실행되도록 sendmail 관련 작업을 기술하라. 관련된 파일이나 명령을 정확하게 표현하도록 한다.

- spammer.org에서 들어오는 모든 메일은 막는다.
- friend.edu에서 들어오는 모든 메일은 허용한다.
- 210.110.30.X부터 210.110.31.X의 IP 주소로부터 메일 릴레이는 허용한다.

3. 아래 C 코드에서 보안상 문제를 일으킬 수 있는 부분을 찾아 설명하고 안전한 코드로 수정하라.

```
...
char   id[10], title[20], *p;
int    tab[20], i, n, sum;
...
printf("Input TITLE (20자 미만의 영문자): ");
gets( title);
printf("Input the data size: ");
scanf("%d", &n);
for (i = 0; i < n; i++) {
    printf("Input data %d: ", i);
    scanf(" %d", &tab[i]);
}
...
p = (char *) malloc(11);
strncpy(p, 10, id);
p[10] = 0;
...
printf("Input USER-ID (10자 미만의 영문자): ");
scanf("%s", id);
for (i = sum = 0; i < n; i++) {
    sum += tab[i];
}

printf("title: %s, id: %s, sum = %d₩n", title, id, sum);
...
```

SIS 2급 시스템보안

1. 시스템 보안 수준을 높이기 위한 방법의 하나로서 불필요한 인터넷 서비스를 제거하고자 한다. 이와 관련하여 직접 다뤄야 할 Unix 파일은?

① /var/adm/sulog
② /etc/passwd
③ /etc/crontab
④ /etc/rc*.d
⑤ /etc/inetd.conf

2. 윈도우 운영체제의 인증 프로토콜 중에서, 클라이언트가 디렉토리 정보에 접근할 수 있도록 하기 위해 만든 것은?

① MSV1_0
② NTLM v2
③ PPTP
④ LDAP
⑤ L2TP

3. 생체학적 접근 통제 기법에는 지문, 망막, 음성 등이 사용된다. 이와 관련된 접근 통제 용어는?

①Identification
②Authentication
③Authorization
④Accountability
⑤Integrity

4. 화일 보호 방법과 거리가 가장 먼 것은?

① naming
② caching
③ password
④ access control
⑤ cryptography

5. 프로세스 스케줄링 기법 중 하나인 RR (Round Robin)에서 time quantum의 크기가 무한히 커진다면, 다음 중 어느 기법과 같은 효과를 가지는가?

① preemptive SJF (Shortest Job First)
② nonpreemptive SJF
③ FIFO (First In First Out)
④ RM (Rate Monotic)
⑤ HRN (Highest Response ratio Next)

6. 다음은 바이러스 및 악성 프로그램에 대해서 설명한 것이다. 이중 잘못된 것을 고르시오.

① 웜 바이러스는 자기 복제 및 자체 메일 전송이 가능해 이메일이나 IRC(Internet Relay Chatting)를 통해 순식간에 전파 될 수 있다.
② DoS는 시스템에서 제공하는 서비스를 일반 사용자가 받을 수 없도록 네트워크 트래픽 양을 증가시켜서 서비스 제공이 마비되도록 하는 공격이다.
③ 컴퓨터 바이러스가 불특정 다수를 대상으로 시스템에 피해를 주는데 반해, 트로이목마 프로그램은 특정 시스템에서만 피해를 준다.
④ 일반적으로 시스템에 접근하기 위해서는 로그인과 같은 절차를 거치지만 백도어 프로그램을 이용할 경우 불법적인 시스템 접근이 가능하다.
⑤ 스니퍼(Sniffer)는 다른 사람의 시스템 자원에 액세스할 목적으로 인테넷 주소를 거짓으로 만들어 정당한 사용자처럼 승인 받아 시스템에 접근해 정보를 수집하는 것이다.

7. 웹 브라우저를 사용하면 쿠키, 히스토리, 캐시 등과 같은 흔적이 남는다. 이에 대한 설명 중 잘못된 것을 고르시오.

① 쿠키에는 개인ID와 비밀번호, 방문한 사이트 등의 정보가 담겨 있어, 사용자의 다음 방문시 웹서버는 그가 누구인지 등에 대하여 바로 파악할 수 있다.
② 쿠키는 암호화되어 있으므로, 지우지 않아도 무방하다.
③ 히스토리는 사용자가 방문한 웹사이트의 내역을 저장하고 있으므로, 사용자의 웹서핑 기록을 알아낼 수 있다.
④ 캐시는 임시 인터넷 파일이라고도 하며, 웹페이지의 로딩 시간을 줄이기 위해 이미지 파일과 같은 용량이 큰 파일을 하드디스크에 저장시켜놓은 것이다.
⑤ 하드디스크에 담겨있는 캐시의 내용을 보면, 방문한 사이트와 그 곳에서 다운로드한 파일 목록까지 확인할 수 있다.

8. 다음은 키로그에 대한 설명이다. 이중 잘못된 것을 고르시오.

① 키보드 하드웨어로 입력되는 모든 키 누름을 감지하여 침입자에게 알려준다.
② 침입자가 시스템 안에 존재하지 않더라도, 파일 등으로 남겨두었다가 침입자에게 알려줄 수 있다.
③ 한글로 입력하여도, 그 자리에 대응하는 영어 키보드로 기록된다.
④ 키로그 프로그램을 목표 시스템에 깔지 않아도 네트워크를 통해서 볼 수 있다.
⑤ 시스템의 Low-Level에서 작동한다 하여도, 백신 프로그램으로 검색/치료가 가능하다.

9. 윈도우에서 악성 프로그램이 사용하는 자동 실행 설정 방법이 아닌 것은?

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

10. 웹에서 인증서는 사용자를 식별하는 강력한 시스템을 생성하기 때문에 익명성을 제거할 때 도움이 된다. 다음 중 클라이언트 인증서를 사용하는 이유가 아닌 것은?

① 인증서를 사용하면 성명, 이메일 주소, 기타 다른 추적 가능한 정보를 남기게 된다.
② 인증서는 익명성을 배제한다.
③ 인증서를 만든 목적은 개인 정보를 노출하는 데 있다.
④ 신분확인 분야에 중요한 분야로 신용적인 상거래를 가능하게 한다.
⑤ 웹브라우저는 사용자의 허가를 받지 않고 인증서를 서버에게 반드시 전송한다.

11. 다음 SSL에 대한 설명 중 틀린 것은?

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.

12. 보안 시스템들의 필터링을 피하기 위해 스캔 기법에서는 stealth기법을 쓴다. 다음 포트스캔의 기법 중 stealth 기법에 속하지 않는 것은?

① Fin flag 기법
② Tcp fragment 기법
③ Ack flag 기법
④ Syn flag 기법
⑤ xmas 기법

13 아래는 john the ripper의 실행 화면이다. 이에 대한 설명으로 부적절한 것은?

<보기>

```
[root@forensic run]# ./john /etc/shadow
Loaded 4 passwords with 4 different salts (FreeBSD MD5 [32/32])
istree            (carrot)
guesses: 1  time: 0:00:00:12 8% (2)  c/s: 2895  trying: greg1
guesses: 1  time: 0:00:00:13 8% (2)  c/s: 2891  trying: Duke1
guesses: 1  time: 0:00:00:14 9% (2)  c/s: 2893  trying: Badboy1
guesses: 1  time: 0:00:00:14 10% (2)  c/s: 3044  trying: istree
```

① john the ripper는 패스워드 크래킹 도구이다.
② 사전 파일을 이용한 패스워드 공격이 가능하다.
③ 기존에 크랙된 패스워드를 보려면 ?show 옵션을 사용하면 된다.
④ 패스워드 크랙의 원리는 역암호화 알고리즘을 이용하여 가능하다.
⑤ john the ripper는 윈도우 패스워드 크래킹도 지원한다.

14. 서브세븐(SubSeven)에 대한 설명 중 틀린 것은?

① 매우 강력하여 한번 설치되면 MS 윈도우를 재설치 해야 한다.
② 서브세븐 기본 포트는 27374 포트를 사용한다.
③ 프로세스가 시작될 때마다 바뀌므로 눈으로 식별하기 힘들다.
④ 서브세븐 자체에 스캔 기능을 제공하여 외부에 서브세븐이 설치되어있는 컴퓨터도 찾을 수 있다.
⑤ 백오리피스와 비슷한 기능을 하며, 서버와 클라이언트 프로그램으로 이루어져 있다.

15. 다음 윈도우 보안 점검 리스트 중 고려 사항이 아닌 것은?

① NTFS에 대한 적당한 ACL을 설정한다.
② 익명 사용자를 위해 guest 계정을 활성화 한다.
③ 계정 데이터베이스를 보호하기 위해 Syskey를 활용한다.
④ 알려진 취약점에 대해 hotfix를 설치한다.
⑤ 관리용 공유폴더를 제거한다.

16. 다음은 삼바(Samba)에 대한 설명이다. 이중 잘못된 것을 고르시오.

① 리눅스에서 삼바 패키지는 두 개의 데몬을 제공한다. 이중 smdb 데몬은 삼바 서버이고, nmdb 데몬은 NETBIOS 네임 서버이다.
② 삼바(Samba)는 파일이나 프린터 자원을 공유할 수 있도록 해주는 프로그램이다. 단 프린터의 경우 리눅스 머신 사이에서만 공유가 가능하다.
③ SWAT(Samba Web Administration Tool)는 공식 삼바 GUI 툴로 웹 기반의 설정 툴이다.
④ 리눅스 사용자가 윈도우 파일 서버를 사용할 수 있게 하려면, smbfs(SMB 파일 시스템)를 사용하여 윈도우 디스크와 디렉토리를 리눅스 시스템에 마운트 시켜야 한다.
⑤ 리눅스에서 smbpasswd 프로그램을 사용해 각 사용자에 대해 암호화된 삼바(Samba) 패스워드를 만들 수 있다.

17. 리눅스 운영체제를 설치하는 과정 중에 파티션을 설정하는 부분이 있다. 다음 중 파티션 설정에 대한 설명 중 잘못된 것을 고르시오.

① ext2 파일 시스템은 리눅스에서 사용하는 기본 파일 시스템이다.
② 리눅스를 설치할 때 Fdisk나 Disk Druid를 사용해서 파티션을 설정할 수 있다.
③ 기존에 설치되어 있는 윈도우 운영체제의 파티션이 있을 경우 시스템은 이중 부팅(dual-boot) 되도록 만들 수 있다.
④ 리눅스의 기본 파티션인 ext2 파일 시스템 뿐 아니라 FAT32와 같은 윈도우 계열의 파티션도 설정할 수 있다.
⑤ swap 파티션의 설정은 생략해도 된다.

18. 다음은 보안책임을 맡은 서버 관리자가 서버의 보안 최적화를 위해 필요한 작업을 나열한 것이다. 이중 부적합한 것을 고르시오.

① /etc/inetd.conf에서 불필요한 서비스를 제거한다.
② 시스템에 대한 백업 스케줄을 만들어 시스템의 모든 파일을 정기적으로 백업한다.
③ 새로운 버전의 OS가 출시될 때마다 새로운 OS로 시스템을 업그레이드 시킨다.

④ PAM을 사용해 인증 프로세스를 최적화 시킨다.
⑤ 가능하다면 파일 시스템을 읽기 전용으로 마운트 시킨다.

19. 다음은 서버 해킹 기법 중 하나인 TCP Hijacking에 대한 설명이다. 이중 잘못 설명한 것을 고르시오.

① TCP Hijacking의 원리는 TCP/IP 패킷을 속여서 정보의 흐름 속에 삽입하도록 하고, 그것에 의해서 원격 호스트에서 실행되는 명령을 가능하게 한다.
② TCP Hijacking 툴의 하나인 Hunt는 원격 시스템에서도 실행할 수 있는 명령을 보낼 수 있다.
③ TCP Hijacking 툴의 하나인 Juggernaut은 단방향 연결 하이잭(Simplex Connection Hijack)이라는 특성이 있으며, 이것은 침입자가 로컬 시스템에 명령을 보낼 수 있게 해준다.
④ 스위치된 네트워킹 기법을 사용해서 TCP Hijacking에 대한 공격을 완벽히 차단할 수 있다.
⑤ IPSec이나 SSH와 같은 암호화된 통신 프로토콜의 채택은 TCP Hijacking 같은 도청 침입의 효과를 많이 감소시키거나 제거할 수 있다.

20. 커버로스(Kerberos) 인증에 대한 설명으로 틀린 것은?

① 커버로스는 분산 인증 서비스 상에서 무결성과 기밀성을 제공한다.
② 인증을 위해 네트워크상에서 패스워드가 전송된다.
③ 키분배 센터에서는 모든 사용자들과 서비스들의 암호화 키를 저장하고 있다.
④ 키분배 센터는 인증 기능도 제공한다.
⑤ 분산 환경을 위한 단일 사용승인(SSO: Single Sign-On)을 사용한다.

21. 다음과 같이 user 라는 유저의 홈디렉토리 하단에 오직 root만이 읽을 수 있는 root 소유의 파일이 있어 다음과 같이 test 디렉토리에 있는 1.txt 파일을 삭제하는 명령어를 실행하였다. 이때 예상되는 결과에 대해 바르게 설명한 것은 무엇인가?

```
[user @www user]$ id
uid=687(user) gid=687(user) groups=687(user)
[user @www user]$ ls -la
drwxr-xr-x    2 user   user       4096  7월 20 20:43 test/
[user @www user]$ ls -la test/
drwxr-xr-x    2  user   user       4096  7월 20 20:43 ./
drwx-----x    8 user    user       4096  7월 20 20:35 ../
-r--------    1 root     root          0  7월 20 20:45 1.txt
[user @www user]$rm -f test/1.txt
```

① 파일의 소유권이 root 만이 읽을 수 있으므로 삭제되지 않는다.

② 파일만 삭제할 수는 없지만 디렉토리 통째로 삭제하면 삭제할 수 있다.
③ user 소유의 디렉토리 하단에 있으므로 삭제된다.
④ 현재의 상태에서는 삭제할 수 없지만 디렉토리 퍼미션을 777 로 변경하면 삭제할 수 있다.
⑤ 답이 없다.

22. 기억장소가 모두 할당된 경우, 새로운 페이지를 할당하기 위하여 기존의 어떤 페이지를 교체할 것인지를 결정하는 것을 페이지 교체라고 부른다. 이러한 페이지 교체 방식들에 대한 다음 설명 중에서 옳지 않은 것은?

① LRU 방식: 사용횟수가 가장 적은 페이지를 찾아 교체한다.
② NUR 방식: 최근에 사용되지 않은 페이지를 찾아 교체한다.
③ 최적화 방식: 이후에 가장 오랫동안 사용되지 않을 페이지를 찾아 교체한다.
④ 무작위 방식: 임의의 페이지를 찾아서 교체한다.
⑤ FIFO 방식: 가장 오래 전에 할당된 페이지를 찾아 교체한다.

23. 다중 프로그래밍 시스템에서 아무리 기다려도 결코 일어나지 않을 사건을 기다리고 있는 프로세스를 교착 상태(Deadlock)에 빠졌다고 한다. 다음 중 교착 상태가 존재하기 위한 4가지 필수 조건에 해당하지 않는 것은?

① 상호배제 조건 : 프로세스들이 그들이 필요로 하는 자원에 대해 배타적인 통제권을 요구한다.
② 비중단 조건 : 자원은 사용이 끝날 때까지 이들이 갖고 있는 프로세스로부터 제거할 수 없다.
③ 대기 조건 : 프로세스가 다른 자원을 기다리면서 이들에게 이미 할당된 자원을 갖고 있다.
④ 환형대기 조건 : 프로세스의 환형 사슬이 존재해서 이를 구성하는 각 프로세스는 사슬 내의 다음에 있는 프로세스가 요구하는 하나 또는 그 이상의 자원을 갖고 있다.
⑤ 무한대기 조건 : 프로세스가 필요한 자원을 무한히 기다린다.

24. 다음 중 윈도우 시스템을 최적화 하는 방법으로 가장 적합하지 못한 것은?

① 캐쉬(Cache)의 설정 - 메모리에서 가능한 많은 캐쉬를 설정한다.
② 필요 없는 파일 삭제 - 임시 파일, 백업 파일, 디스크 검사 과정에서 생성되는 파일을 찾아내어 검사한 후 삭제한다.
③ 바이오스(BIOS)를 통한 부팅 과정 줄이기 - 특별한 경우를 제외하고 부팅 과정에서 필요 없는 플로피 드라이브나 CD_ROM에서 부팅하는 과정을 BIOS에서 제거해 준다.
④ 타임 슬라이스(Time slice) - 타임 슬라이스를 짧게 잡아주면 멀티태스킹(mult tasking)능력을 향상 시켜주기 때문에 그것을 가능한 작게 한다.
⑤ 디스크 검사와 조각 모음 - 파일 링크정보가 손상되었을 경우 디스크검사를 통해 바로잡을 수 있고 또한 조각모음을 실행시켜 여기저기 흩어진 파일조각(단편화현상)을 연속된 공간으로 다시 정렬해주며 자주 사용하는 프로그램을 우선적으로 배치하는 등의 반드시 필요한 작업이다.

25. 운영 체제의 일괄 처리 방법 중 버퍼링(buffering)과 스풀링(Spooling)이라는 것이 있다. 다음 중 버퍼링과 스풀링에 대한 설명의 틀린 것은?

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.

26. 다음의 디스크 스케줄링 알고리즘 중에서 "엘리베이터 알고리즘"이라고도 불리는 기법은?

① SSTF
② FCFS
③ C-Scan
④ RR
⑤ Scan

27. Unix 시스템에서 서버에 현재 login한 사용자의 정보를 알 수 있게 해주는 명령어는 무엇인가?

① ping
② rlogin
③ finger
④ ftp
⑤ uname

28. S/MIME에 대한 설명 중 틀린 것은?

① 인터넷 전자우편 형식 표준인 MIME의 보안기능을 강화하기 위해 공개키 암호 기술을 적용한 것이다.
② 네트워크 계층에서 보안을 제공한다.
③ MIME 객체에 암호화와 전자서명기능을 추가한 프로토콜이다.
④ 기존의 전자우편 보안도구들의 단점을 개선하고자 RSA Data Security, INc.에서 처음 개발하였다.
⑤ MIME 객체를 전송할 수 있는 모든 프로토콜에 대해 보안 서비스 제공한다.

29. 다음은 트로이목마 프로그램인 백오피스에 대한 설명이다. 이 중 잘못된 것을 고르시오.

① MS의 윈도우 운영체제에서만 작동한다.
② 정식적 경로를 통하지 않고 불법적인 경로를 통해 시스템에 접근하기 위한 백도어 프로그램이다.
③ 백도어를 통해 정보를 빼갈 수 있는 것뿐만이 아니라, 시스템을 조작할 수도 있다.
④ 자기 복제를 하여 다른 컴퓨터에 백오피스를 설치함으로써 그 피해가 커질 수 있다..
⑤ 최신 백신 프로그램으로 쉽게 감지/치료할 수 있다.

30. 다음 중 각 계층별 웹 보안 프로토콜로 잘못 짝지어진 것은?

① APPLication Level : S/MIME, SET
② Network Level : TLS
③ APPLication Level : PGP
④ Transport Level : SSL
⑤ Network Level : IPSec

31. 다음 nmap 포트 스캐너의 명령어와 결과에 대한 설명으로 틀린 것은?

```
[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 값 이다.
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.

32. 다음 설명 중 틀린 것은?

① 안전한 이메일 시스템을 위해서는 PKI와의 연동이 중요하다.
② PGP는 공개키 암호시스템을 사용하지 않는다.
③ PEM은 공개키 시스템과 공용키 시스템을 모두 사용한다.
④ S/MIME은 안전한 이메일을 위해 RSA 사에서 제안한 표준이다.
⑤ 안전한 이메일 시스템에서 공개키는 비밀키 키관리를 위해서 사용한다.

33. 다음 해킹 도구 중 사용자의 key stroke를 훔치는 도구는?

① Passpy
② Voob
③ Satan
④ Nuke
⑤ Goldeneye

34. 다음 중 시스템 내부의 트로이목마 프로그램을 감지하기 위해 가장 알맞은 툴은 무엇인가?

① Nmap
② Saint
③ Tripwire
④ Snort
⑤ nessus

35. 다음은 방화벽에 대한 기본 개념이다. 이중 잘못된 것을 고르시오.

① 패킷 필터링은 외부에서 들어오는 패킷을 분석하여 허가된 패킷만 통과시키는 것으로, IP 스푸핑에 취약하다.
② DMZ에는 가장 안전한 내부 네트워크를 위치시키고, 인가되지 않은 외부에서의 접근은 완전 차단한다.
③ Dual-homed Host Firewall은 두 개의 NIC를 두어 내부와 외부를 각각 연결한다.
④ 프록시 서버는 인터넷의 속도를 높이는 캐쉬 기능과 함께 방화벽 기능을 제공한다.
⑤ 방화벽 내부에 있는 사용자는 외부에 자유롭게 접근할 수 있다.

36. 다음은 사용자 계정에 대한 패스워드 보호 기법에 대해 설명한 것이다. 이중 잘못된 것을 고르시오.

① 패스워드는 주기적으로 자주 바꿔주는 것이 좋다.
② 자신에게는 의미가 있고 타인에게는 단지 의미 없는 문자의 배열에 지나지 않는 것을 패스워드로 사용하는 것이 기억하기도 쉽고 관리하기가 편리하다.
③ 원타임 패스워드 방식 중 하나인 Challenge Response 인증 방식은 HHA(Hand Held Authenticator) 또는 토큰이라 불리는 소형 기기가 필요하다.
④ 원타임 패스워드 방식 중 하나인 S/Key 방식에서는 사용자 개개인에게 패스 플레이즈라고 불리는 고유의 비밀 데이터가 주어진다.
⑤ 외부에서 서버의 계정에 접근할 때 한번밖에 사용할 수 없는 패스워드를 Shadow Password라고 한다.

37. NCSC(National Computer Security Center)는 컴퓨터 시스템에서 정부, 기업, 개인 유저들의 Private Data에 대한 보호 평가 기준으로 다음과 같은 보안 등급(Security Ratings)을 만들었다. 이중 C2 등급은 범용 OS를 위해 충분한 안전성을 제공하는 등급으로 간주된다. 다음 중 C2 등급에 해당하지 않는 것을 고르시오.

① Trusted path functionality
② A secure logon facility
③ Discretionary access control
④ Security auditing
⑤ Object reuse protection

38. 다음 설명에 해당하는 침입 대응 시스템의 한 방법은?

<보기>

증거로 사용될 컴퓨터 미디어에 대한 보존, 증명, 검출, 문서화, 해석방법 그리고 근본적인 원인분석 방법에 대한 내용들을 포함한다.

① Intruder tracing system
② Recovery system
③ Forensic system
④ Honeynet system
⑤ Intrusion Prevention system

39. 다음 공유폴더 취약성을 이용한 공격에 대한 설명 중 잘못된 내용은?

① Microsoft 파일/프린터 공유 프로그램 서비스가 등록된 경우 공격될 수 있다.
② 공유폴더 취약성을 이용한 공격을 위해서는 해킹툴이 있어야 한다.
③ NetBIOS over TCP/IP 기능을 이용해 공격한다.
④ 임의의 사용자가 원격 PC의 공유된 디스크나 폴더를 공격한다.
⑤ 바이러스 확산의 근원지가 될 수 있으며, 바이러스에 감염될 확률이 높다.

40. 감사로그는 보안 통제가 제공하는 서비스 중 어떤 기능에 속하는가?

① 예방(preventive)
② 탐지(detective)
③ 억제(deterrent)
④ 복구(recovery)
⑤ 보상(compensation)

41. 한번 호출된 자료나 명령은 곧바로 다시 사용될 가능성이 높으며, 한 기억장소가 호출되면 인접한 장소들이 연속되어 사용될 가능성이 높다고 하는 것을 무엇이라 하는가?

① 지역성(locality)
② 스래싱(thrashing)
③ 스와핑(swapping)
④ 중첩(overlay)
⑤ 재배치(relocation)

42. UNIX에서 각 파일에 대한 정보를 기억하고 있는 자료구조로서, 파일 소유자의 식별번호, 파일 크기, 파일의 최종 수정시간, 파일의 링크 수 등의 내용을 가지고 있는 것은?

① 슈퍼블록(super block)
② inode(index node)
③ 디렉터리(directory)
④ 파일 시스템 마운팅(mounting)
⑤ 프로세스 제어 블록(process control block)

43. 다음 중 Linux 시스템의 스케줄링 기법과 관련하여 옳지 않은 것은?

① 우선순위 기반 선점형(preemptive) 스케줄링 기법을 사용한다.
② 높은 우선순위의 task에게 더 긴 time quantum이 할당된다.
③ 우선순위 값이 클수록 우선순위도 높음을 의미한다.
④ 각 CPU마다 runqueue라는 자료구조를 사용하며 이에 runnable task와 expired task를 구분하여 스케줄링 한다.
⑤ I/O를 많이 하는 프로세스의 우선순위를 상대적으로 높게 한다.

44. 다음 페이지 참조열(page reference string)의 실행 과정이 진행되는 동안 발생하는 페이지 부재(page fault)의 횟수를 구하시오. 단, 이 프로세스에게 3개의 페이지 프레임이 고정 할당되어 있고 초기에 이들이 모두 비어 있다고 가정하며, 페이지 교체 기법으로는 LRU 기법을 사용한다고 가정한다.

페이지 참조열: 1-2-3-4-1-2-3-1-2-3

① 3회
② 4회
③ 5회
④ 6회
⑤ 7회

45. 다음 중 프로세스가 CPU나 메모리가 아닌 어떤 자원의 할당을 기다리거나 또는 특정 이벤트의 발생을 기다리는 상태를 의미하는 용어는?

① Running
② Ready
③ Preempted
④ Suspended
⑤ Blocked

46. 메모리의 내부 단편화(internal fragmentation) 문제를 해결할 수 있는 방법은?

① 세그멘테이션
② 스레싱(thrashing)
③ 페이징
④ 스와핑
⑤ preemption

47. 다음 보기 중 Unix 디렉토리 권한(permission)에 대한 설명으로 맞는 것만을 모은 것은?

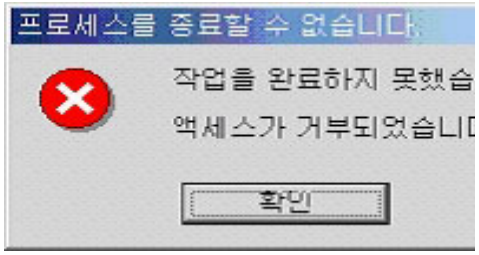
가. 읽기 권한은 있는데, 실행권한이 없으면 파일 리스트를 볼 수 없다.
나. 디렉토리 권한을 0700으로 설정하면 소유자만 디렉토리 내의 파일을 읽을 수 있다.
다. 디렉토리 소유자라도 해당 디렉토리에 대한 실행 권한이 없으면 디렉토리 내의 파일에 접근할 수 없다.
라. 읽기 권한은 없고, 실행 권한이 있으면 디렉토리 내의 파일의 목록을 얻을 수 있다.

① 가, 나
② 다, 라
③ 나, 다
④ 나, 라
⑤ 가, 라

48. 김씨는 자신의 윈도우 PC가 언제 재부팅되었는지 알기 위해 command상에 어떤 명령어를 입력하려고 한다. 어떤 명령어를 입력하여야 알 수 있을지 아래 보기 중에서 골라라.

① net computer boot time
② net time boot
③ net reboot time
④ net statistics workstation
⑤ net localgroup

49. 웜 등과 같이 비정상적인 프로세스를 종료하려고 할 때 아래와 같이 프로세스를 종료할 수 없다고 나오는 경우가 있다. 이는 해당 프로세스가 다른 파일과 같이 실행 중이기 때문인데, 이러한 경우 어떻게 조처하여야 하는가?



① 파일의 생성 날짜를 변경한다.
② 현재 프로세스가 실행 중이므로 잠시 후에 재시도한다.
③ 파일이 속한 폴더권한을 변경한다.
④ IIS 서비스를 재시작한다.
⑤ 안전모드로 시작해 해당 파일을 삭제한다.

50. 피싱은 개인정보를 도용하기 위해서 설계된 속임수의 한 유형이며 스팸 전자메일, 전화, 팝업 창 등으로 사용자들이 중요 개인정보(신용카드번호, 주민번호, 계좌정보 등)를 스스로 제공토록 유도하여 개인정보를 도용하는 기법이다. 다음 중 피싱에 대한 적절한 대처 방법이 아닌 것은 무엇인가?

① 금융관련회사에서 개인정보 확인메일이 오는 경우는 해당기관에 직접 확인 전화한다.
② 최신 보안패치, 최신 업데이트된 바이러스 백신, 스파이웨어 방지 프로그램, 방화벽 등으로 대처한다.
③ 전자메일 링크주소 클릭 시 보이는 팝업 창에서는 보안인증서를 위조하기 어려워 상대적으로 신뢰할 수 있으므로 금융거래 정보를 입력해도 된다.
④ PC방 등 개방된 컴퓨터에서의 금융거래는 되도록 지양한다.
⑤ 의심스런 전자메일 메시지의 링크주소는 함부로 클릭하지 않는다.

51. 다음 중 웹 어플리케이션 해킹에 대한 대응 방법으로 옳지 않은 것은?

① 버퍼 오버플로우에 대한 일반적인 공격 대응 방법으로 운영 중인 시스템을 최신의 패치 버전으로 유지하고 불필요한 서비스 및 권한을 제거함으로써 외부로부터의 보안취약점을 최소화하는 방법이 있다.
② 원격 관리 프로그램 공격에 대한 일반적인 대응 방법으로 신뢰할 수 있는 네트워크에서만 운영 중인 시스템에 접근할 수 있도록 강력한 접근 통제를 수행하는 방법이 있다.
③ 명령어 삽입에 대한 일반적인 대응 방법으로 주기적인 로그 점검 및 감사를 하고 주기적로 보안 정책을 재검토하며 불필요한 계정 및 권한을 제거하는 방법이 있다.
④ 오류 처리를 이용한 공격에 대한 일반적인 대응 방법으로 웹 어플리케이션이 잘못된 요청으로 오류를 반환할 때 자체 제작한 오류만을 보여주도록 설정하는 방법이 있다.
⑤ 암호화 공격에 대한 일반적인 대응 방법으로 SHA-1과 같은 단방향 해시 함수를 사용하는 방법이 있다.

52. 다음 중 윈도우 운영체제에서 디렉토리 및 파일에 대한 접근권한 설정규칙 중 맞는 것은?

① 개별 사용자가 그룹 A와 그룹 B에 속해 있을 경우에 특정 파일이나 디렉토리에 대한 접근 권한은 그룹 A와 그룹 B의 권한을 모두 가진다.
② 디렉토리에 대한 접근 권한보다 파일에 대한 접근 권한이 우선한다.
③ '거부'보다는 '허용'이 우선한다.
④ NTFS 접근 권한 중 '쓰기' 권한은 해당 디렉토리의 서브 디렉토리와 파일을 생성할 수 있으나, 소유권이나 접근 권한의 설정 내용을 확인할 수는 없다.
⑤ 암호화된 파일 또는 디렉토리는 생성자만 읽을 수 있다.

53. 다음 지문은 포트 스캐닝 프로그램인 'nmap' 도구를 이용하여 수행된 결과를 보여주고 있다. 다음 중 이에 대한 설명으로 옳지 않은 것은?

```
[root@Linux root]# nmap -sS -O -f 192.168.0.1
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
445/tcp    filtered    microsoft-ds
6000/tcp   open        X11
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Uptime 0.051 days (since Mon Oct 17 21:01:05 2005)
Nmap run completed -- 1 IP address (1 host up) scanned in 19 seconds
```

① -sS 옵션은 half-open 스캐닝의 방법으로서 완전한 tcp connection을 맺지 않도록 하는 옵션이다.
② 192.168.0.1의 호스트는 리눅스 시스템이며 현재 열린 포트는 3개이다.
③ -f 옵션은 패킷을 아주 작게 쪼개서 보내는 옵션이다.
④ -O 옵션은 ping을 보내지 않고 스캐닝하는 옵션이다.
⑤ 445번 포트는 192.168.0.1에서 자체 방화벽을 통해 막혔거나 nmap에서 정확하게 판별하지 못한 경우이다.

54. 다음 중 포맷 스트링 취약점이 존재하는 함수가 아닌 것은?

① printf
② fprintf
③ scanf
④ sprintf
⑤ snprintf

55. 다음 중 컴퓨터 바이러스에 대한 설명으로 옳지 않은 것은?

① 부트 바이러스란 플로피디스크나 하드디스크의 부트섹터를 감염시키는 바이러스를 말한다.
② 파일 바이러스는 숙주 없이 독자적으로 자신을 복제하고 다른 시스템을 자동으로 감염시켜 자료를 유출, 변조, 삭제하거나 시스템을 파괴한다.
③ 이메일 또는 프로그램 등의 숙주를 통하여 전염되어 자료를 변조, 삭제하거나 시스템을 파괴한다.
④ 최근 들어 암호화 기법을 기반으로 구현된 코드를 감염 시마다 변화시킴으로써 특징을 찾기 어렵게 하는 다형성(Polymorphic) 바이러스로 발전하고 있다.
⑤ 확장자가 COM, EXE 등인 실행 파일을 감염시키는 파일 바이러스로는 CIH, Win32/Kriz가 있다.

56. 백오리피스 2000의 특징이 아닌 것은?

① 백오리피스 2000은 windows95/98/NT를 지원한다.
② Plug-in 기능은 지원하지 않는다.
③ XOR, 3DES를 지원한다.
④ Default 설정을 바꿀 수 있다.
⑤ GUI 방식을 지원한다.

57. 다음은 UNIX 시스템의 보안 취약성을 이용한 침입을 막기 위한 일반적인 방법들이다. 다음 중 보안을 위한 방법으로 적합하지 않은 것은?

① shadow 패스워드 시스템을 사용한다.
② /var/adm/messages, /var/adm/sulog 등을 scan하여 su 사용을 점검한다.
③ 외부 사용자를 위해서는 anonymous ID만을 제공한다.
④ root는 콘솔 상에서 로그인 할 수 있게 한다.
⑤ 패스워드 크랙(crack) 프로그램을 사용하여 수시로 패스워드를 검사한다.

58. 다음 중 패킷 필터링 시에 패킷 헤더에서 검출할 수 있는 정보가 아닌 것은?

① 소스 IP 주소
② 목적지 IP 주소
③ TCP/UDP 소스 포트
④ ICMP 메시지 타입
⑤ 패킷의 생성 시간

59. 다음 중 지문의 설명에 해당하는 시스템 취약점 스캐너는 무엇인가?

- 유닉스에서 컴파일되며 자신의 컴퓨터나 네트워크뿐만 아니라 원격지 네트워크에서 타겟 시스템의 취약점을 스캔한다. - HTML 형식으로 결과를 리포팅한다. - 연관된 호스트의 스캐닝이 가능해서 네트워크의 구조를 파악하기 편리하다.

① SAINT
② LANguard
③ Typhoon
④ nmap
⑤ nessus

60. 다음 중 유닉스 계열의 운영체제에서 네트워크 연결에 대한 접근제어 도구로 사용되는 것은?

① Tripwire
② inetd
③ TCPWrapper
④ nmap
⑤ nessus

SIS 2급 어플리케이션 보안

1. 메일 서버에 도착한 메일을 자신이 사용하고 있는 컴퓨터로 다운로드하여 메일의 내용을 확인할 수 있도록 해주는 것이 다음 중 어떤 것인가?

① SNTP
② SNMP
③ POP
④ FTP
⑤ TFTP

2. 다음중 전자우편의 보안을 위한 요구사항이 아닌 것은 무엇인가?

① 기밀성 : 전자우편 수신자가 아닌 다른 사용자들이 내용을 볼 수 없어야 한다.
② 무결성 : 전자우편 전송 도중에 내용이 다른 사용자에 의해 불법적으로 변경되지 않아야 한다.
③ 사용자 인증 : 전자우편을 실제로 보낸사람과 송신자가 동일해야 한다.
④ 수신부인방지 : 전자우편을 수신하고도 받지 않았다고 부인하지 않아야 한다.
⑤ 데이터 공유 : 양질의 데이터를 포함한 전자우편은 공유를 위해 관리자가 복사를 해두어도 된다.

3. S/MIME 전자우편 보안 프로토콜에 대한 설명으로 틀린 것은?

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.

4. 웹 로그 보안에 관련된 사항이 아닌 것은?

① 웹 서버의 로그 감사 기능을 활성화 시킨다.
② 로그감사 절차, 주기 및 방법은 각 서버의 지침 및 절차에 의거한다.
③ 웹서버 중에는 로그라는 디렉토리와 access.log만 갖는 파일이 있다.
④ 로그를 주기적으로 점검한다.
⑤ 로그점검 결과서를 IT 보안관리자에게 제출한다.

5. 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 다운로드 후 메일 서버의 메일 박스에서는 삭제
(4) 사용자가 고정적인 위치에서 메일을 사용시 유리

① SNMP
② SMTP
③ IMAP
④ PGP
⑤ POP

6. 데이터베이스를 개발하는 업체들의 각기 다른 API를 공통의 인터페이스로 사용하기 위한 Micro-soft의 인터페이스는?

① Powerpoint
② ODBC(Open DataBase Connectivity)
③ HTML
④ Windows CE
⑤ CDMA

7. 다음 중 CGI script의 문제점 및 대응책으로 잘못 기술되어 있는 것은 ?

① CGI script에는 항상 버그가 발견될 가능성이 있다.
② CGI script는 보안상 허점이 없도록 주의하여 작성되어야 한다.
③ 웹서버를 chroot 디렉토리에서 수행하여도, 버그가 있는 CGI zcript라면 정보를 유출시킬 우려가 있다.
④ 웹서버를 "nobody" 권한으로 실행하면, CGI script의 위험성이 없어진다.
⑤ 원격 사용자의 입력을 처리하는 CGI script의 경우, 원격 사용자가 "명령 실행"을 하도록 하는 우회적 공격에 취약할 수 있다.

8. 다음 중 S-HTTP에 대한 설명으로 틀린 것은 ?

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.

9. 다음은 CGIWrapper를 이용했을 때에 대한 설명이다. 이중 잘못된 설명은?

① CGI 프로그램이 어느 사용자의 디렉토리에 있는지 보고 판단해서 그 사용자의 권한으로 CGI 프로그램을 실행시킨다.
② 권한 설정을 적절히 한다면 다른 내부 사용자는 웹을 통해 쓰기와 읽기가 가능한 파일이라도 다른 CGI 프로그램을 통해서 접근을 할 수 있다.
③ CGI 프로그램이 어느 사용자의 디렉토리에 있는지 검사를 하고 그 CGI 프로그램의 소유자를 검사해서 두 사용자가 일치하지 않더라도 프로그램을 실행한다.
④ CGI 프로그램의 보안성을 한층 높여주지만 초보자기 잘못 사용하면 아주 위험할 수 있다.
⑤ CGIWraper를 설치하게 되면 cgiwrap이라는 실행파일이 /cgibin에 만들어진다.

10. ftp 서버가 호스트와 사용자 기반의 네트워크 접근제어를 위해 사용하는 기본 파일은 어느 것인가?

① ftpusers
② ftpwatch
③ htphosts
④ htpaccess
⑤ ncftp

11. PKCS7-mime 응용에서, MIME 타입 별로 지정된 파일 확장자 명이 올바른 것은 ?

① MiME 타입: Applicatio/pkcs7-mime (signedData, envelopedData) → 파일확장자: .p7m
② MIME 타입: Applicatio/pkcs7-mime (signedData, envelopedData) → 파일확장자: .p7c
③ MIME 타입: Application/pkcs7-mime (degenerate signedData "certs-only" message) → 파일확장자: .p7m
④ MIME 타입: Application/pkcs7-mime (degenerate signedData "certs-only" message) → 파일확장자: .p7s
⑤ MIME 타입: Application/pkcs7-signature → 파일확장자: .p7c

12. ftp는 두 가지의 연결 모드를 지원한다. 다음 중 능동 모드에 대한 설명 중 틀린 것은?

①제어 연결이 이루어지면 사용자의 인증 정보 명령을 이용하여 사용자를 인증한다.
②파일의 전송을 위해서 소켓을 새로 생성한다.
③소켓생성시 포트 번호는 특정 포트 번호로 고정되어 있다.
④서버에 PORT 명령을 보내는데 PORT 명령어는 6개의 인자를 갖는다.
⑤서버에서 할당해준 포트 번호를 이용해서 클라이언트와 데이터 연결을 설정한다.

13. 웹 보안 개발 사항 중 틀린 것은?

① Cross-site scripting Flaw는 전체적인 대응은 불가능하고 실행파일을 실행하지 않도록 Brower에서 설정하는 방법이 존재할 수 있음
② Buffer Overflow는 IDS 에서 주로 대응을 하거나 Patch를 이용
③ Command Injection flaws는 개발자가 생길 수 있는 모든 경우의 에러에 대항할 수 있도록 적용해야 한다.
④ Remote Administration Flaws는 가급적 원격에서 제어가 불가능하도록 해야 하나 안된다면 VPN과 같은 암호화는 반드시 이루어져야 한다.
⑤ Web and Application Server Misconfiguration은 최신 patch의 적용이나 보안정책의 준수, logging등이 존재한다.

14. xml기반 web 보안에 관련된 내용이 아닌 것은?

① SAML표준은 오아시스 XML보안서비스 기술위원회와 국내의 PKI 업체들이 참여해 만든 표준이다.
② 한국정보인증, 이니텍, 비씨큐어 등 공개키기반구조(PKI)업계 등이 기술개발을 진행중.
③ 전자서명인증 솔루션을 XML을 기반으로 개발했을 경우 전자서명을 담당과장과 부장 등으로 세분화시킬 수 있다.
④ XML 보안 기술은 ETRI등 국책연구기관에서도 연구를 진행, 한국전산원과 함께 전자상거래통합포럼에서 국내 표준화를 진행 중에 있다.
⑤ 이니텍은 웹서비스용 XML보안을 책임지고 있다.

15. SAINT에 관한 설명이다. 설명이 잘못된 것은?

① 방화벽 및 CERT와 CIAC에서 알려주는 각종 보안 문제들을 검사한다.
② 기본 적으로 finger, NTS, NIS, ftp, tftp, statd 등의 서비스를 검사한다.
③ SAINT로 얻은 데이터는 네트워크 호스트간의 신뢰성 및 안전도를 평가할 수 있는 중요한 자료로 활용된다.
④ 보안 관리자와의 인터페이스는 html 형식으로 제공되며, 여러 가지 색으로 위험의 정도를 알려준다.
⑤ 현재의 인터넷에서 가장 많이 사용되고 있는 포트 스캐너이다.

16. 다음은 SET 프로토콜에 대한 설명이다. 잘못된 것은?

① 인터넷상에서 안전한 신용카드 기반의 전자상거래를 위해 개발
② 마스터카드사의 SEPP와 비자사의 STT의 결합형태이다.
③ 보안제어를 OSI 7계층 모델에 있어서 응용계층에서 실시하고 있다.
④ SET는 공개키 암호방식만을 사용하여 안전성을 보장한다.
⑤ 사용자의 사생활 보장을 위한 이중서명을 사용한다.

17. 다음은 어떤 전자서명 방식에 대한 설명인가?
(1) 미국의 NIST에서 발표한 표준 전자서명 방식이다.
(2) DSA 알고리즘을 사용한다.
(3) 트랩도어가 존재할 가능성이 있다.
(4) Schnorr 방식과 비슷한 구조를 가지고 있다.

①KCDSA
②DSS
③FFS
④ElGamal
⑤Signcryption

18. 전자화폐와 전자투표 등에서는 익명성을 제공하기 위하여 서명자가 문서의 내용을 보지 않는 상태에서 전자서명을 생성하는 기법이 반드시 필요하다. 이 경우에 사용되는 전자서명은?

① 그룹서명
② 은닉서명
③ 부인봉쇄서명
④ 검증자지정서명
⑤ 다중서명

19. 다음은 RSA 전자서명에 대한 설명이다. 틀린 것은?

① 소인수 분해의 어려움을 이용한 전자서명이다.
② $n = p \times q$ 이고, p 와 q 는 큰 자리 소수이다
③ $\Phi(n) = (p-1) + (q-1)$
④ 공개키 e 는 $\gcd(e, \Phi(n)) = 1$
⑤ 비밀키 d 는 $e \times d = 1 \bmod \Phi(n)$

20. SET의 특징 중 하나는 이중서명(dual signature) 방식이다. 이 방식을 사용하는 이유를 바르게 설명한 것은?

① 신용카드 소지자와 상인간의 데이터 기밀성을 강화하기 위하여
② 신용카드 소지자와 은행간의 데이터 인증을 강화하기 위하여
③ 신용카드 소지자의 카드 정보를 상인이 볼 수 없게 하고 은행은 신용카드 소지자의 구입정보를 알 수 없게 하기 위하여
④ 상인과 은행간의 상호 인증을 강화하기 위하여
⑤ 신용카드 소지자의 카드 정보와 구입 정보를 은행만이 볼 수 있도록 하기 위하여

21. 다음은 FTP 보안에 대해 설명한 것이다. 다음 중 잘못 설명된 것은?

① Anonymous FTP 서버를 구축할 때 /etc/passwd의 FTP user에는 실행할 수 있는 쉘(Shell)을 지정하지 않도록 한다.
② TFTP 서비스는 주로 디스크 없는 호스트가 부팅할 때 사용되므로 TFTP 서버 구성 시 클라이언트의 홈 디렉토리는 서버의 루트 디렉토리로 지정하여야한다.
③ FTP bounce attack은 다운로드할 파일의 IP주소와 포트를 지정할 수 있도록 한 FTP 규약의 설계상의 문제를 이용한 해킹 방법이다.
④ FTP 서비스 외의 다른 서비스는 가능한 같은 시스템에서 운영하지 않도록 한다.
⑤ 안전한 FTP서버 운영을 위하여 접속할 때 나타나는 로그인 배너를 삭제하거나 변경하여 해커에게 서비스 중인 FTP 서버의 종류와 버전을 숨기도록 한다.

22. 다음 웹기반 HTTP 보안 중 해쉬 알고리즘을 이용한 보안방식은 어느 것인가?

① Secure HTTP 방식
② SSL(Secure Socket Layer) 방식
③ IP Filtering을 이용한 접근제어 방식
④ PGP를 이용한 방식
⑤ Message Digest를 이용한 사용자 인증

23. 최근 쿠키(Cookie)가 인터넷 보안에 심각한 허점이 있는 것으로 드러나 쿠키의 사용을 제한하려는 움직임이 있다. 쿠키가 갖는 특성에 대해 설명한 것 중 올바르지 않은 것은?

① 서버가 클라이언트에 코드를 기록하고, 읽는 방식이다.
② 바이러스 코드를 기록할 경우 시스템에 심각한 위해를 가할 수 있다.
③ 상업적으로 쿠키를 이용할 경우 사용자의 관심분야, 쇼핑정보, 개인정보, 웹서핑 경로 등의 정보를 알아낼 수 있다.
④ 회원 인증정보를 담은 쿠키를 중간에 가로챌 경우 해커는 회원의 권한을 빼앗을 수 있다.
⑤ 쿠키는 서버와 클라이언트간의 정보교환에 의해 어플리케이션의 효율을 높인다.

24. 다음 보기 중 Nimda Worm(W32/Nimda Worm)에 대한 설명으로 맞지 않는 것은?

① 컴퓨터의 플래시 메모리(Flash Memory)의 BIOS 내용과 하드디스크의 데이터를 파괴하는 증상을 보인다.
② 실행 가능한 바이너리 코드인 "readme.exe"이름의 파일을 포함하고 있다.
③ 오픈된 네트웍 자원(공유폴더)를 통해 감염될 수 있다.
④ 감염된 클라이언트는 Windows address book에 있는 모든 주소로 Nimda worm을 포함한 email을 전송하려고 시도한다.
⑤ Code Red II와 sadmin/IIS 웜에 의해서 만들어진 백도어를 스캐닝하여 DOS를 발생시키기도 한다.

25. 다음 중 mail bombs에 대한 설명으로 올바른 것은?

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 설치하는 것

26. 데이터 웨어 하우스가 구현되었을 때의 특징 중 잘못된 것은?

① 조직의 많은 자원이 소요되고, 많은 비용이 들지만 높은 투자수익률을 달성할 수 있다.
② 데이터 웨어 하우스를 사용함으로써 경쟁우위를 획득할 수 있다.
③ 데이터 웨어 하우스는 유지보수가 거의 필요 없기 때문에 비용이 매우 절감된다.
④ 다양한 기존 시스템에 저장된 각종 데이터의 통합은 상당한 시간과 난이도가 필요하다.
⑤ 데이터 웨어 하우스를 전체구축의 부담으로 특정부서나 업무만 지원하는 데이터 마트만 구축하기도 한다.

27. 다음 중 전자우편 보안과 직접 관련있는 것으로만 짝지어진 것은?

① SSL, SSH
② SEA, PGP
③ SSH, SET
④ PGP, PEM
⑤ SSL, PEM

28. TFTP(Trivial File Transfer Protocol)에 대한 설명으로 틀린 것은?

① FTP보다 간단한 네트워크 어플리케이션이다.
② 사용자 인증이 필요 없다.
③ 디렉토리를 보여주지 않아도 되는 곳에서 사용할 수 있다.
④ FTP처럼 TCP를 사용한다.
⑤ 패스워드 없이 접속하여 파일을 가져올 수 있다.

29. 다음에서 설명하는 전자우편의 보안요소로 옳은 것은?

"중간에서 지나가는 메일을 잡아 놨다가 다시 보내는 공격 방법을 방지해 주는 기능"

① 메시지 무결성(Message Integrity)
② 메시지 재생 방지(Message replay prevention)
③ 사용자 인증(User Authentication)
④ 송신자 부인 방지(Nonrepudiation of origin)
⑤ 암호화(Confidentiality)

30. TLS (Transport Layer Security) 의 기본 구조에서 그 구성 요소가 아닌 것은 무엇인가?

① Handshake Protocol
② Http protocol
③ Alert Protocol
④ Record Protocol
⑤ Change Cipher Spec Protocol

31. 다음은 스팸 메일을 추적하는 내용이다. 추적과 관련된 내용이 틀린 것을 고르시오.

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 스퍼머 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.

32. 인터넷에서 이용되고 있는 IP프로토콜은 패킷 교환망에서 단순히 데이터의 신뢰성 있는 전송만을 염두에 두고 개발한 것이기 때문에 IP spoofing이나 IP sniffing과 같은 보안 허점이 생겨나게 되었는데, 이를 해결하기 위한 방안으로 등장한 것은?

① SSL
② IPsec
③ TLS
④ WAP
⑤ IPv6

33. 다음 중 웹 서버 로그를 분석하기 위하여 사용될 수 있는 프로그램은?

① snort
② webalizer
③ sniffer
④ CUSeeMee
⑤ satan

34. 다음 중 공개키 기반구조(Public Key Infrastructure)의 의미를 가장 잘 표현한 것은?

① 모든 암호 알고리즘을 사용하기 위해서 반드시 필요한 기반구조
② 전자서명 알고리즘의 사용을 위해서만 제공되는 전자서명 알고리즘 기반구조
③ 공개키 암호 알고리즘의 원활한 사용을 위해서 인증서를 발급할 수 있는 기반구조
④ 암호시스템을 사용하기 위해 공개키를 발급할 수 있는 기반구조
⑤ 사용자 인증만을 수행하기 위한 사용자 인증 기반구조

35. 인증서 및 CRL 보관소에 저장되어 있는 PKI 정보를 추가, 삭제 및 변경을 수행하기 위한 프로토콜은 다음 중 어떤 것인가?

① CCF
② LRA
③ PMA
④ OCSP
⑤ LDAP

36. SSL(Secure Socket Layer)은 넷스케이프 사에서 개발한 프로토콜로 인터넷상에서 교환되는 정보들을 보호하는 암호 프로토콜이다. SSL에 사용되는 암호 기술과의 관계가 잘못 설명된 것은?

① 키교환 프로토콜 ---- RSA
② 메시지 암호화 ---- DES
③ 디지털 서명 ---- ElGamal
④ 메시지 무결성 ---- RC2
⑤ 해쉬함수 ---- MD5

37. 공개키 기반구조를 위한 요소 시스템이 아닌 것은?

① 인증서를 발행하는 인증기관(certification authority)
② 사용자 신원을 확인하는 등록기관(registration authority)
③ 인증서와 인증서 폐지 목록을 공개하기 위한 디렉토리(directory)
④ 인증서를 발행받는 최종 개체(end entity)
⑤ 인증서 발행 업무를 효율적으로 수행하기 위한 인증기관 웹 서버

38. 공개키 암호 시스템의 안전성은 어렵다고 알려진 문제의 난이도에 그 기반을 두고 있다. 다음 중 공개키 암호 시스템과 그 시스템의 안전성을 보장하는 문제가 올바르게 연결된 것을 고른 것은?

가. Rabin 공개키 암호 - 2차 잉여류(quadratic residue)의 제곱근 계산 문제
나. RSA 공개키 암호 - 배낭(Knapsack sum) 문제
다. ElGamal 공캐키 암호 - 이산대수(discrete log) 문제
라. 타원곡선 공개키 암호 - 소인수분해(factoring) 문제

① 나. 라
② 가. 다
③ 나. 다
④ 가. 라
⑤ 가, 나

39. SSL 핸드쉐이크 프로토콜에서 서버가 클라이언트의 인증서를 요청할 경우 클라이언트가 자신의 인증서를 보내는데 이용되는 핸드쉐이크 메시지는 무엇인가?

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

40. 다음 중 전자 지불에서 사용되는 SET (Secure Electronic Transaction) 프로토콜에 대한 암호 기술에 속하지 않는 것은 무엇인가?

① Change Cipher Spec Protocol 의 보안 기능 제공
② RSA의 보안 기능 제공
③ SHA-1의 보안 기능 제공
④ X.509 ver. 3를 이용한 공개키의 인증
⑤ DES의 보안 기능 제공

41. 다음 중 FTP 공격 방법 중 바운스 공격(bounce attack)에 대한 설명으로 틀린 것은?

① FTP 바운스 공격(bounce attack)은 최신 버전의 FTP 서버로 패치함으로써 어느 정도 예방될 수 있다.
② FTP 바운스 공격(bounce attack)은 공격자의 익명성(anonymity)을 보장 할 수 없다.
③ FTP 바운스 공격(bounce attack)은 제3의 FTP 서버를 이용해 공격 대상의 포트를 스캐닝하는 공격 방법이다.
④ Control connection을 맺는 호스트와 data connection을 맺는 호스트가 항상 같도록 설정하면 자신의 FTP 서버가 FTP 바운스 공격(bounce attack)에 이용되지 않을 수 있다.
⑤ FTP control connection이 20번 포트와 같은 예약된 포트에 연결되는 것을 방지하는 것이 FTP 바운스 공격(bounce attack)에 대한 예방책이 될 수 있다.

42. 다음 중 전자우편의 안전성을 제공하기 위해 PGP, PEM 및 S/MIME 등의 시스템에서 제공해야 하는 보안 요구사항 중에서 스팸 방지 기술에 적용 가능하도록 밀접한 관련성이 있는 기술은 무엇인가?

① 기밀성- 전자우편 수신자가 아닌 다른 사용자들이 내용을 볼 수 없어야 한다.
② 무결성- 전자우편 전송 도중에 내용이 다른 사용자에 의해 불법적으로 변경되지 않아야 한다.
③ 사용자 인증 - 전자우편을 실제로 보낸 사람과 송신자가 동일해야 한다.
④ 수신부인방지 - 전자우편을 수신하고도 받지 않았다고 부인하지 않아야 한다.
⑤ 데이터 공유 - 양질의 데이터를 포함한 전자우편은 공유를 위해 관리자가 복사를 해두어도 된다.

43. 다음은 IPSec의 AH 프로토콜이 하는 역할에 대한 설명이다. 맞는 것은?

① 라우터와 라우터 간의 IP 패킷을 암호화한다.
② 단말과 단말 간의 IP 패킷을 암호화 한다.
③ 단말과 라우터 간의 IP 패킷에 대한 송신 인증 및 무결성 서비스를 제공한다.
④ 단말과 라우터 간의 IP 패킷에 대한 송신 인증, 무결성 그리고 암호화 서비스를 제공한다.
⑤ AH 프로토콜은 트랜스포트 모드에서만 사용되고 터널 모드에서는 적용될 수 없다.

44. Anonymous FTP 보안과 관련한 다음 설명 중 가장 적절하지 않은 것은?

① Anonymous FTP가 제공하는 디렉토리나 파일의 소유주를 ftp로 두어 Anonymous FTP 보안 관리를 일관성 있게 처리한다.
② ~ftp/etc/passwd 파일에는 /etc/passwd 안의 일반 사용자 계정 및 패스워드 정보가 들어가지 않도록 주의하여 일반 사용자 패스워드 노출 가능성을 줄인다.
③ FTP 데몬의 최신 버전을 유지함으로써 알려진 FTP 데몬 취약점의 이용 가능성을 줄인다.
④ Anonymous FTP가 제공하는 디렉토리나 파일에 대해서는 특별한 이유가 없는 한 쓰기 권한을 막음으로써 공격 가능성을 줄인다.
⑤ Anonymous FTP 사용자가 쉽게 접근할 수 있는 ~ftp/etc 디렉토리에는 시스템 파일들을 두지

않도록 유의한다.

45. 다음은 인터넷 보안 응용 기술에 대해서 설명하고 있다. 틀린 것은?

① 침입차단 시스템 - 인터넷과 같은 외부 네트워크에 연결된 내부 네트워크를 외부의 불법적인 사용자의 침입으로부터 안전하게 보호하기 위한 정책을 비롯하여 이를 지원하는 하드웨어 및 SW를 총칭한다.
② 가상사설망 - 분산된 기업의 네트워크를 구성할 때 전용 임대 회선 대신 공중망을 사용하고, 암호 및 인증 보안 기능을 이용하여 구축된 네트워크이다.
③ 침입탐지 시스템 - 네트워크 패킷을 분석하고 이러한 패킷 중 해킹의 징후를 띄고 있는 것을 발견할 경우에 관리자에게 경보 메일 송신, 공격 세부사항 로깅 또는 접속 단절 등 여러 가지 다양한 대응 옵션을 제공한다.
④ 취약성 분석 시스템 - 취약성 분석 시스템이란 시스템에 존재하는 알려진 버그나 공격에 이용될 수 있는 취약성을 진단하는 프로그램이다.
⑤ 컴퓨터 바이러스 - 정상적인 프로그램에 악성코드를 내장하여 인터넷에서 쉐어웨어 등의 형태로 배포하여 사용자 시스템의 정보를 수집하는 프로그램이다.

46. 웹 서비스는 기업에서 웹을 통해 모든 업무를 처리할 수 있도록 웹 기반 분산 시스템을 지원하기 위해 만들어진 것이다. 웹 서비스에서 분산시스템 상의 어플리케이션들 사이의 통신을 지원하기 위한 기술과 가장 관련이 적은 것은?

① ERP(Enterprise Resource Planning)
② XML (eXtensible Markup Language)
③ SOAP (Simple Object Access Protocol)
④ WSDL (Web Services Description Language)
⑤ UDDI (Universal Description, Discovery and Integration)

47. 데이터베이스 복구를 위해 만들어지는 체크포인트에 대한 설명으로 가장 적절한 것은?

① 장애를 일으킨 트랜잭션들의 기록
② 데이터베이스 장애 발생 직전에 수행된 트랜잭션 기록
③ 이미 처리된 트랜잭션 중 영구 저장장치에 반영되지 않은 부분
④ 일정 시간 간격으로 만들어지는 DBMS의 현재 상태에 대한 기록
⑤ 데이터베이스 복구에 필요한 점검 항목 목록

48. SSL 보안 프로토콜에 대한 설명 중 잘못된 것은?

① SSL 프로토콜은 응용 계층과 전송계층 사이에 위치한다.
② SSL 프로토콜은 Handshake, Alert, Record Layer, Change Cipher 프로토콜들로 이루어져 있다.
③ 대칭키, 공개키 암호 알고리즘과 해쉬 알고리즘은 Change Cipher 프로토콜에 의해 결정된다.

④ 클라이언트에서 생성한 데이터 암호용 대칭키 생성용 정보는 서버의 인증서에 포함된 공개키를 이용하여 서버에게 안전하게 전달된다.
⑤ 데이터 암호화, 해쉬, 압축 기능은 Record Layer 프로토콜에서 이루어진다.

49. PGP가 제공하는 보안 서비스에 대한 설명 중 잘못 된 것은?

① CAST, IDEA, Triple DES와 같은 대칭키 암호 알고리즘을 이용하여 전자메일의 비밀성을 보장한다.
② 전자메일 송신자의 신원확인을 위해 DSS, RSA 암호 알고리즘을 이용한 전자서명 기능을 제공한다.
③ 대칭키 암호 알고리즘에 사용되는 대칭키(세션키) 교환을 위해 RSA 공개키 암호 시스템이나 ElGamel 키 전송 알고리즘, Diffie-Hellman 키 교환 알고리즘이 이용된다.
④ PGP 개발 초기부터 안전한 대칭키 교환을 위해 PKI 기반의 인증서 내에 포함된 메일 수신측의 공개키를 이용한다.
⑤ PGP는 필요에 따라 인증서비스, 암호서비스, 인증-암호 서비스를 제공한다.

50. Apache 웹 서버를 안전하게 유지하기 위한 설정방법들을 설명한 것이다, 잘못된 것은?

① DocumentRoot는 /etc 디렉토리 대신 다른 디렉토리로 변경하여 설정한다.
② 웹 서버를 실행할 때 root 권한이 아닌 nobody 계정으로 실행한다.
③ 웹 서버를 실행하는 사용자 계정으로 로그인이 허용되지 않도록 /etc/passwd 파일을 설정한다.
④ 디렉토리 리스팅이 불가능하도록 Indexes 설정을 삭제하고 FollowSymLinks는 설정한다.
⑤ Apache 버전과 운영체제 종류를 외부에게 알려지지 않도록 ServerToken이나 ServerSignature를 이용하여 설정한다.

51. Microsoft IIS 웹 서버에 대한 보안 설정 중 잘못된 설명은?

① 파일이 업로드 되는 디렉토리 외의 모든 디렉토리에 '쓰기' 권한을 설정하지 않는다.
② IIS에 의해 실행될 수 있는 파일(.asp, .asa, .hta 등)에 의해 실행될 수 있는 HTTP 메소드 중 GET을 제외한 불필요한 메소드는 삭제한다.
③ 웹 사이트 운영자는 Administrators 그룹으로 한정한다.
④ 특정 주소나 네트워크에 대한 IIS 접근을 거부하도록 설정한다.
⑤ IIS 하위 구성요소 중 불필요한 요소는 설치하지 않는다.

52. SMTP 구성요소와 동작 절차에 대한 설명 중 잘못된 것은?

① MUA - MTA와 사용자간 인터페이스 프로그램으로 Outlook이나 /bin/mail 등이 있다.
② MTA - 메일 메시지를 저장하고 전달, 전송하는 역할을 수행하며 sendmail, MS Exchange 등이 있다.
③ MDA 메일 서버에서 사용자 메일 박스로 복사하는 기능을 수행하는 대표적인 예로 procmail등이 있다.
④ MUA에서 MTA로 메일을 보낼 때 사용되는 프로토콜은 SMTP이며 25번 포트를 이용한다.
⑤ 메일 서버에서 MUA로 메일을 받을 때 사용되는 프로토콜로는 POP(포트번호 143)과 IMAP(포트번호 110)이 있다.

53. 다음 커버로스 v4 의 동작에 관한 설명 중 잘못 된 것은?

① 사용자는 인증 서버로부터 티켓승인서버에 로그인 할 수 있는 티켓을 요청한다.
② 사용자는 티켓 승인 서버로부터 원하는 서비스를 받을 수 있는 승인 티켓을 얻는다.
③ 사용자는 응용서버에게 서비스 요청을 위하여 로그온 한 후 , 커버로스 티켓서버로부터 받은 패스워드를 입력한다.
④ 사용자는 인증서버로부터 티켓을 얻기 위해 로그온 하여 인증 절차를 거친다.
⑤ 사용자는 필요한 응용 서비스를 받을 때 마다, 티켓 승인 서버로부터 응용서버로부터 서비스 받을 수 있는 승인 티켓을 얻는다.

54. 다음 중 FTP(File Transfer Protocol) 서버에 가해질 수 있는 공격에 대한 설명으로 가장 적당하지 않은 것을 고르시오.

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.

55. 다음 중 FTP 보안을 강화하기 위한 방안이 아닌 것은 무엇인가?

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.

56. 각 계층에서 동작하는 암호화 프로토콜이 잘못 연결된 것은?

① Transport Layer - SSL
② Session Layer - IPSec
③ Datalink Layer - PPTP
④ Datalink Layer L2TP
⑤ Datalink Layer L2F

57. 다음은 인증기관(CA:Certificate Authority)에 대한 설명이다. 잘못된 것은?

① 사용자의 공개키 인증서를 발급한다.
② 필요에 따라 사용자의 공개키 인증서를 취소한다.
③ 자신의 공개키와 상위 인증기관의 공개키를 사용자에게 전달한다.
④ 인증서와 인증서 소유자의 정보를 관리하는 데이터베이스를 관리한다.
⑤ 사용자 신분 확인을 수행하며 인증서 발급은 상위 인증기관에 요청한다.

58. 다음 중 발신자의 신원 인증 및 메시지 무결성을 보장할 수 있는 방법이 아닌 것은?

① 메시지에 송신자의 개인키로 계산되는 DSA 서명을 함께 전송한다.
② 메시지에 송신자의 개인키로 계산되는 RSA 서명을 함께 전송한다.
③ 메시지에 사전 공유키를 사용한 HMAC-MD5 함수의 결과를 함께 전송한다.
④ 사전 공유키를 사용하여 메시지를 블록 암호로 암호화하여 전송한다.
⑤ 메시지에 SHA-1 해쉬 함수로 계산된 메시지 다이제스트를 함께 전송한다.

59. 다음 중 X.509 공개키 인증서의 필수 항목이 아닌 것은?

① 공개키 소유자의 식별정보
② 공개키
③ 공개키의 용도를 나타내는 정보
④ 공개키 유효기간
⑤ 인증기관에 의한 디지털 서명

60. 전자인증서 구성요소와 기능에 대한 설명으로 잘못된 것은?

① Version X.509 표준의 인증서 버전 번호
② Subject name 인증서 소유자(발급대상자) 정보
③ Issuer name 인증서 발급자(인증기관) 정보
④ Signature algorithm parameters 전자서명에 이용되는 공개키 알고리즘과 해쉬 함수 정보
⑤ Signature 전자인증서 내용에 대한 Root CA의 전자서명 결과 값

SIS 2급 네트워크보안

1. 다음 중 UDP 프로토콜의 기능이 아닌 것은?

① 실시간 통신실현이 가능하다.
② 신뢰성이 보증 되지 않는다.
③ 비 연결형(connectionless) 통신 방식이다.
④ 윈도우 사이즈(window size)를 설정할 수 있다.
⑤ 사용자 데이터 그램이다.

2. 다음 패킷교환의 특징에 해당되는 것은?

① 이기종간 통신시 속도변환과 프로토콜 변환이 용이하다.
② 패킷 전송지연이 발생하지 않는다.
③ 전용 통신채널 설정이 용이하다.
④ 전송대역폭이 고정 대역폭이다.
⑤ 오류제어가 되지 않는다.

3. 다음 중 브릿지(Bridge) 기능에 해당되는 것은?

① IP주소를 분해하여 다음 네트워크에 전송한다.
② 코드 변환을 수행한다
③ 목적지 주소와 수신지 주소를 변환한다.
④ 물리계층 및 데이터링크 계층을 연결하며 상위계층과는 무관하다
⑤ 메시지크기를 변환한다.

4. 다음 중 ATM전송에 해당되지 않는 것은?

① 셀의 길이는 53옥텟(octets)으로 구성 되었다.
② 셀의 구성은 데이터가 48옥텟이고 헤더가 5옥텟이다.
③ 고정셀 구조를 가지고 있다.
④ 물리적 계층에서는 48옥텟으로만 셀이 이동한다.
⑤ 1 옥텟의 길이는 32비트로 구성된다.

5. 다음은 DOS 창에서 어떤 명령어를 실행시킨 결과인가?

```
C:₩Documents and Settings₩Administrator>???? 203.252.53.47
???? 203.252.53.47 with 32 bytes of data:
Reply from 203.252.53.47: bytes=32 time<1ms TTL=128
Reply from 203.252.53.47: bytes=32 time<1ms TTL=128
Reply from 203.252.53.47: bytes=32 time<1ms TTL=128
Reply from 203.252.53.47: bytes=32 time<1ms TTL=128
???? statistics for 203.252.53.47:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
       Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

① ping
② traceroute
③ date
④ netstat
⑤ snmpwalk

6. 다음 중 라우터의 환경 설정 수단이 아닌 것은?

① 콘솔(console) 이용
② NMS(Network Management System) 이용
③ 가상 터미널(Virtual Terminal) 이용
④ TFTP(Trivial File Transfer Protocol) 서버를 이용
⑤ WAP(Wireless Application Protocol) 이용

7. 회선 교환 방식은 정보전송의 필요성이 생겼을 때 먼저 상대방을 호출하여 물리적인 연결을 구성한 후 정보를 전송하는 방식을 말한다. 다음 중에서 회선 교환 방식의 특징이 아닌 것은?

① 전송 중 항상 동일한 경로를 이용한다.
② 대체적으로 point-to-point 의 전송구조를 갖는다.
③ 경로 설정에는 짧은 시간이 걸리며 전송지연은 거의 없다.
④ 고정적인 대역폭을 사용한다.
⑤ 길이가 긴 연속적인 데이터 전송에 적합하다.

8. 인터넷 등에서 패킷 교환 방식을 많이 채택하고 있어서 최근 정보통신망의 주력 교환 기술로 자리매김하고 있다. 다음 중 패킷 교환 기술의 특징을 잘못 설명한 것은 무엇인가?

① 패킷 교환 방식은 회선 교환방식과 메시지 교환 방식의 장점을 결합하고 단점을 최소화한 방식이다.
② 패킷 교환 방식은 패킷 형태로 만들어진 데이터를 패킷 교환기가 목적지 주소에 따라 적당한 통신경로를 선택하여 송신하는 방식이다.
③ 고속 패킷 교환 방식에는 프레임 릴레이, X.25, 셀 릴레이 등이 있다.
④ 셀 릴레이 방식의 패킷 교환은 음성, 데이터, 영상 등 모든 형태의 정보 전송에 적합하다.
⑤ 고속 패킷 교환 방식 중에서 최초 ATM 방식이 각광을 받고 있다.

9. 오늘날은 인터넷에 대한 이해가 없이는 사회생활을 영위하기가 어려운 시대가 되고 있다. 이러한 인터넷의 특징 중에서 잘못 설명된 것을 고르시오.

① 인터넷은 호스트와 라우터로 구성되는 데이터 통신망이다.
② 인터넷을 구성하는 주요 프로토콜에는 IP와 TCP가 대표적이다.
③ ISO의 OSI 7계층 구조에 의하면 TCP 프로토콜은 계층 4, IP 프로토콜은 계층 3에 해당한다.
④ 인터넷에서 서브 네트워크간을 상호 연결하는 장치에는 라우터와 게이트웨이가 있다.
⑤ 인터넷에서 패킷의 전송 및 전달은 IP 어드레스를 근거로 하여 결정된다.

10. 다음중 ftp bounce scanning 에 대해 바르게 설명한 것은 무엇인가?

① ftp 데몬의 버전을 스캔하기 위해 사용된다.
② anonymous ftp 가 열려있는지를 스캔하기 위해 사용된다.
③ ftp 데몬의 보안설정이 제대로 되어 있는지 확인하기 위해 사용된다.
④ 최대 ftp 접속자수를 테스트하기 위해 사용된다.
⑤ 주로 공격자의 위치를 은닉하기 사용된다.

11. CGI 서버 보안 대책에 대한 설명이 아닌 것은?

① CGI 코드를 검사한다.
② 침입차단시스템 외부에 CGI를 설치한다.
③ 사용자의 데이터를 다른 프로그램의 입력으로 사용제한 한다.
④ 보안 메일링 리스트와 유즈넷 뉴스 그룹을 활용한다.
⑤ 최소한의 특권만으로 CGI를 수행한다.

12. 다음 중 인터넷상의 패킷 가로채기를 하기 위한 공격은 무엇인가?

① 순차적 번호 예측공격
② 패킷 스니핑
③ 도스 공격
④ 암호에 관한 공격
⑤ 취약점 악용 공격

13. 다음 중 Syn Flooding 공격에 대한 설명 중 틀린 것은 어느 것인가?

① 공격자 IP 주소를 쉽게 속일 수 있어 역추적 및 차단이 어렵다.
② 네트워크 연결 대기 큐(backlog queue)의 사이즈를 증가시키고, Syncookies 기능을 사용함으로 공격을 완화할 수 있다.
③ 불완전한 TCP 연결 요청을 이용한 공격이다.
④ Netstat 명령으로 확인해 보면 많은 수의 TIME_WAIT 상태의 연결을 확인할 수 있다.
⑤ RFC에 따른 네트워크 필터링을 통하여 공격을 완화하거나 예방할 수 있다.

14. 다음은 IDS의 문제점을 설명하고 있다. 거리가 멀다고 생각되는 것은?

① IDS는 insertion attack 에 취약할 수 있다.
② Misuse detection 방식은 신종 공격기법에 취약할 수 있다.
③ Anomaly detection 방식은 신종 공격기법에도 탐지할 가능성이 높다
④ 호스트 기반 IDS는 침입이 이루어진 이후의 탐지가 많을 수 있다.
⑤ 네트워크기반의 IDS 는 호스트 내부에서의 침입을 탐지하는데 어려움이 있다.

15. 다음 중 성격이 다른 공격 유형은?

① Land attack
② Session Hijacking attack
③ Ping of Death attack
④ Resource Starvation attack
⑤ Smurf attack

16. 다음 중 패킷 필터링 방식의 장점이 아닌 것은?

① 처리속도가 상대적으로 빠르다.
② 사용자에게 투명성이 보장된다.
③ 광범위한 분야에 사용될 수 있다.
④ 사용자별 인증을 할 수 있다.
⑤ 시스템 비용이 적게 든다.

17. 관리자가 라우터의 처리 능력이 갑자기 떨어지는 것 같아 이를 조사해 보고자 할 때, 사용할 수 있는 Cisco 라우터의 명령으로 적당한 것은?

① show access-lists
② router rip
③ show ip route
④ ping
⑤ show process cpu

18. 라우터 외부로 나가는 패킷의 소스 IP 를 체크하여 필터링하는 것으로 라우터 내부의 네트워크에서 SYN Flooding 등 소스IP 를 위조하여 다른 네트워크를 공격하는 형태의 공격을 차단하고자 할 때 어떤 필터링을 하여야 하는가?

① egress filtering
② black hole filtering
③ ingress filtering
④ as_path filtering
⑤ Reflexive filtering

19. 다음은 특정 시스템에 대한 분류 또는 기능에 대한 정의이다. 특성이 다른 하나는 무엇인가?

① 단일 호스트 기반
② 네트워크 기반
③ 베스천 호스트
④ 비정상적인 행위탐지
⑤ 오용 침입탐지

20. 다음 중 두 개의 다른 네트워크 인터페이스를 통해 내부 네트워크와 외부 네트워크를 분리하여, 양 네트워크 간의 직접적인 접근을 차단하는 방식의 시스템은?

①듀얼-홈드 게이트웨이
②회선-레벨 게이트웨이
③프록시 서버
④스크린드 서브넷 게이트웨이
⑤패킷 필터링

21. 다음 중 IPv6에 대한 설명으로 틀린 것은?

① 주소에 128비트를 배정한다.
② 보안 기능을 포함하고 있다.
③ IPv6는 유니캐스트, 애니캐스트, 멀티캐스트, 브로드캐스트를 지원한다.
④ IPNG 또는 IPng로 불리기도 한다.
⑤ IPv6 옵션 헤더는 라우터 처리속도를 향상시킬 수 있도록 설계되었다.

22. 라우터는 네트워크와 네트워크를 접속시키기 위한 통신기기를 지칭하며 인터넷은 바로 이 라우터에 의해 연결된 네트워크라 할 수 있다. 다음은 라우터의 특징에 대하여 설명한 것이다. 잘못 설명된 것을 고르시오.

① 라우터는 송신할 경로를 설정한 후, 수신한 패킷을 해당 경로를 통해 가장 가까운 라우터로 중계하는 기능을 수행한다.
② 수신지에 가장 가까운 라우터를 선택하기 위해 라우터는 라우팅 테이블을 사용한다.
③ 라우팅 테이블의 설정은 라우팅 프로토콜에 의해서만 할 수 있다.
④ 각 라우터는 패킷 속에 포함된 수신지 IP 어드레스를 보고 수신지를 결정한다.
⑤ 라우팅 테이블은 수신지 IP 어드레스와 네트워크상에서 가장 가까운 라우터의 IP 어드레스와의 관련표를 갖추고 있다.

23. 다음 설명 가운데 틀린 것은?

① TCP 프로토콜은 연결형 서비스를 허용한다.
② TCP 프로토콜은 송신한 순서대로 패킷을 수신한다.
③ UDP 프로토콜은 오류가 발견되면 해당 패킷을 버린다.
④ TCP 프로토콜은 오류가 발견되면 재전송을 요구한다.
⑤ UDP는 TCP에 비해 오버헤드가 많아 멀티미디어 응용에 적합하다.

24. 호스트의 물리주소를 알면 그것의 IP 주소를 찾아서 알려주는 프로토콜은?

① IP
② RARP
③ ICMP
④ ARP
⑤ IGMP

25. 다음은 라우터의 어떤 환경을 설정하는 것인가?

```
router(config)# line console 0
router(config-line)# login
router(config-line)# password cisco
```

① 가상 터미널 상에서 라우터의 암호를 설정하는 명령어이다.
② 가상 터미널 상에서 라우터의 관리자를 변경하는 명령어이다.
③ 가상 터미널 상에서 라우팅 테이블을 변경하는 명령어이다.
④ 콘솔(console) 상에서 라우터의 암호를 설정하는 명령어이다.
⑤ 콘솔 상에서 라우터의 관리자를 변경하는 명령어이다.

26. 다음 중 CDMA/CD의 운용상의 특징이 아닌 것은?

① 다수의 사용자가 매체를 공유하는 방식이다.
② 통신량이 많아지면 충돌의 횟수가 증가하면서 채널 이용률이 떨어진다.
③ 지연 시간을 예측할 수 있다.
④ 채널의 제어가 각 기기에 완전히 분배된다.
⑤ 어느 한 기기가 고장이 나도 다른 기기의 통신에 전혀 영향을 미치지 않는다.

27. 동일한 LAN간에 리피터(Repeater)를 연결하였다. 어떠한 기능을 수행하는가?

① 데이터 프레임을 저장 후 전송한다.
② 데이터 패킷을 저장 후 전송한다.
③ 네트워크의 전송신호를 단순 재생하여 연결된 네트워크로 전송한다.
④ 상위계층에 인터페이스를 제공한다.
⑤ 프로토콜 변환을 수행한다.

28. TCP는 신뢰성 서비스를 제공한다. 다음 중 신뢰성을 제공하기 위해 TCP 프로토콜에서 제공하는 기능으로 옳지 않은 것은?

① 바이트 스트림 교환
② 중복된 데이터 폐기
③ 세그먼트 분할 전송
④ 타이머를 이용한 재전송
⑤ 흐름 제어 기능

29. 다음 중 기가비트 이더넷(Gigabit Ethernet)에 대한 설명으로 잘못된 것은?

① 기가비트 이더넷은 IEEE 802 위원회에서 표준을 정의하고 있다.
② 매체로서 TP(Twisted Pair)를 사용할 수 있다.
③ 기존의 이더넷 및 고속 이더넷(Fast Ethernet)과 호환을 이루도록 설계되었다.
④ 매체로 동축케이블을 사용할 때 긴 거리에서 이용 가능하다.
⑤ CSMA/CD를 사용한다.

30. 기존에 알려진 침입 방법에 기초한 오용 침입탐지(Misuse Detection) 방식이라 볼 수 없는 것은?

① 규칙기반 전문가 시스템
② 상태 전이 분석
③ 패턴 매칭
④ 모델 기반 탐지
⑤ 통계적 방법

31. 지정된 버퍼크기보다 더 많은 양의 데이터를 버퍼에 입력하여 다른 영역까지 영향을 미치게 만드는 공격을 무엇이라 하는가?

① IP 스푸핑 공격
② 버퍼 오버플로우 공격
③ 분산 서비스 거부 공격
④ 전자우편 공격
⑤ 스팸메일

32. 침입차단 시스템 중 프록시 게이트웨이를 사용할 경우 장점으로 볼 수 없는 것은?

① 게이트웨이가 외부에 알려진 유일한 주소이다.
② 내부 호스트에 도착하기 전에 인증 시도를 한다.
③ telnet의 다운로드/업로드를 통제한다.
④ spam메일, 메일내용 검색, 바이러스 검색 등을 할 수 있다.
⑤ 암호화/무결성 등 추가적인 보안 기능을 위한 S/W, H/W는 제공되지 않는다.

33. 다음은 해킹 방법의 결과들을 설명한 것들이다. 이중 옳지 않은 결과는 무엇인가?

① /cgi-bin/ 인터프리터 이용 - /cgi-bin/에 pel.exe등의 인터프리터를 이용하여 외부에서 임의의 명령 수행 가능
② 취약한 CGI이용 - 외부 사용자가 임의의 명령을 수행, 디렉토리 내의 파일 목록을 열람 가능
③ www서버 구성상 문제 이용 - 부적절한 구성으로 임의의 문서에 접근
④ 입력 FORM 이용 - FORM의 e-mail주소 입력부에 임의의 명령을 추가, 외부에서 임의의 명령 수행
⑤ 서비스 거부 공격 - 일반 호스트에 대한 원격 공격과 마찬가지 방법을 이용, 시스템 루트권한을 획득

34. 다음 중 SYN/FIN 스캔 방식이 다른 방식에 비해 자주 사용되는 이유는 무엇인가?

① SYN/FIN 스캔은 udp 포트도 스캔할 수 있다.
② SYN/FIN 스캔은 속도가 빠르다.
③ SYN/FIN 스캔은 정확도가 높다.
④ SYN/FIN 스캔은 SYN 만을 필터링한 Stateless 방화벽을 통과할 수 있다.
⑤ SYN/FIN 스캔은 소스포트를 자유자재로 설정할 수 있다.

35. 침입차단시스템(Firewall)에 대한 설명 중 틀린 것은?

① 침입차단시스템의 기능 중 하나는 패킷 필터링이다.
② 침입차단시스템을 설치하면 보안 정책 수립의 필요성이 감소한다.
③ 침입차단시스템의 구현 형태는 스크린 라우터, 배스천 호스트, 응용 게이트웨이 등이 있다.
④ VPN 기능을 제공하는 침입차단시스템도 있다.
⑤ 프록시는 응용 레벨에서 이루어지는 방식이다.

36. 다음은 스팸메일로 인하여 피해를 본 사람이 받은 메일의 헤더이다. 실제로 메일을 보낸 도메인 또는 시스템의 IP 주소는?

```
From help@aaa.com  Wed Jan  6 01:51:51 1999
Return-Path: <help@aaa.com>
Received: from mail.rrr.com (mail.rrr.com.elias [xxx.xxx.xxx.xxx] (may be forged))
        by aaa.com (8.9.1/8.9.1) with SMTP id BAA24672
        for <help@aaa.com>; Wed, 6 Jan 1999 01:51:51 +0900
Received: from [yyy.yyy.yyy.yyy] ([yyy.yyy.yyy.yyy])
              by mail.rrr.com (8.6.12h2/8.6.9) with SMTP id BAA05012
              for help@aaa.com; Wed, 6 Jan 1999 01:38:48 +0900
Date: Wed, 6 Jan 1999 01:38:48 +0900
From: help@aaa.com
Message-Id: <199901051638.BAA05012@mail.rrr.com>
X-Authentication-Warning: mail.rrr.com: Host [yyy.yyy.yyy.yyy] didn't use HELO protocol
subject: Mail Delivery Problems
Apparently-To: help@aaa.com
```

① aaa.com
② rrr.com
③ yyy.yyy.yyy.yyy
④ xxx.xxx.xxx.xxx
⑤ 없음

37. 다음은 attacker 호스트에서 victim 서버에 ACK 스캔을 하였을 때의 tcpump 결과를 보여주고 있다. 여기에서 victim 서버에서는 525번 포트가 작동하지 않고 있었는데, victim 에서는 어떻게 응답할 지 ( ) 에 적당한 것은 무엇인가?

```
16:20:17.006389 eth0 < attacker.36217 > victim.525:  .  3296924072:3296924072(0)  ack
1081196972 win 4096
16:20:17.006473 eth0 > victim.525 > attacker.36217: (    ) 1081196972:1081196972(0) win 0
(DF)
```

① R
② P
③ .
④ S
⑤ F

38. 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?

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

39. 다음 중 Cisco 라우터에서 Access-list 번호가 100-199인 경우에 해당하는 것은?

① IP standard access list
② IPX standard access list
③ IP extended access list
④ IPX extended access list
⑤ IPX SAP access list

40. Cisco 라우터에서 내부 네트워크에 있는 123.11.11.15 서버에 대하여 모든 Telnet 접속을 차단하고자 할 때 사용할 수 있는 명령은 무엇인가?

① access-list 110 deny tcp any 123.11.11.15 0.0.255.255 eq 23
② access-list 110 deny tcp any host 123.11.11.15 eq 23
③ access-list 10 permit tcp any host 123.11.11.15 eq 23
④ access-list 10 deny tcp any host 123.11.11.15 eq 23
⑤ access-list deny any host 123.11.11.15 23

41. 다음의 설명은 네트워크 서비스 중의 하나이다. 어느 것에 관한 설명인가?

TCP/IP 프로토콜 그룹을 이용하여 인터넷에서 장치를 관리하기 위한 서비스의 기반 프로토콜이다. 이것은 인터넷을 감시하고 관리하기 위한 기본적인 운영을 제공한다. 이것은 상호 동작하는 프로토콜을 사용함으로써 이루어지는데, 최상위 레벨에서 관리는 SMI(Structure of Management Information)와 MIB(Management Information Base)를 통해 이루어진다.

① IGMP
② CM IP
③ SMTP
④ TFTP
⑤ SNMP

42. NAT을 사용하는 가장 중요한 이유는 무엇인가?

① 데이터를 암호화하기 위하여
② 네트워크 속도를 빠르게 하기 위하여
③ ip 주소의 부족을 해결하기 위하여
④ 해커의 공격을 막기 위하여
⑤ 데이터의 흐름을 바꾸기 위하여

43. ICMP를 이용해 공격 대상 시스템의 활성화 여부를 알아보는 방법이 아닌 것은?

① Echo Request(Type 8)와 Echo Reply(Type 0)를 이용한 방법
② Exceed Request(Type 4)와 Exceed Reply(Type 5)를 이용한 방법
③ Timestamp Request(Type 13)와 Timestamp Reply(Type 14)를 이용한 방법
④ Information Request(Type 15)와 Information Reply(Type 16)를 이용한 방법
⑤ ICMP Address Mask Request(Type 17)와 ICMP Address Mask Reply(Type 18)를 이용한 방법

44. 라우터에서 제공하는 명령어 중 패스워드를 암호화할 때 사용할 수 있는 명령어는?

① config terminal
② service password-encryption
③ network 200.100.10.0 255.255.255.
④ show memor
⑤ enable

45. Tcpdump 프로그램은 주어진 조건식을 만족하는 네트워크 인터페이스를 거치는 패킷들의 헤더를 출력해 주는 프로그램이다. 보기 중 다음의 예제로 설명 할 수 없는 것은 어느 것인가?

```
tcpdump -xte not dst port 80 or src host host1.com
```

① 각 패킷의 16진수 값을 알 수 있다.
② 각 패킷의 timestamp를 알 수 있다.
③ 각 패킷의 link-level 헤더를 알 수 있다
④ 각 패킷에서 목적지 포트가 80인 것은 볼 수 없다
⑤ 각 패킷에서 출발지 호스트가 host1.com인 것을 볼 수 있다.

46. Windows의 Tracert 프로그램을 ICMP 프로토콜로 구현하고자 할 때, 사용되는 메시지를 올바르게 짝 지은 것은?

① Echo Request Time Exceeded
② Echo Request Destination Unreachable
③ Echo Request Echo Reply
④ Router Solicitation Router Advertisement
⑤ Time Stamp Request Time Stamp Reply

47. TCP의 '3-way 핸드세이킹'의 취약점을 이용한 공격 기법은?

① Land 공격
② Ping of Death 공격
③ Teardrop 공격
④ SYN Flooding 공격
⑤ Smurf 공격

48. 다음은 어떤 공격에 대한 패킷 로그를 검출한 것을 보여준다. 어떠한 공격인가?

Source: 10.10.10.10
Destination: 10.10.10.10
Protocol: UDP
Src Port: 32767
Dst Port: 32767

① UDP Flood Attack
② Ping of Death Attack
③ SYN Flooding Attack
④ Land Attack
⑤ Ping of Death Attack

49. nmap을 이용하여 스텔스 스캔에 사용하는 옵션이 아닌 것은?

① -sF
② -sN
③ -sS
④ -sV
⑤ -sX

50. 버퍼 오버플로우 방지방법으로 가장 적합하지 않는 것은?

① 메모리와 스택영역 할당을 랜덤화한다.
② 방화벽이나 침입탐지시스템을 설치한다.
③ 버퍼 오버플로우 발생프로그램에 대한 보안패치를 실행한다.
④ 스택가드와 포인트 가드와 같은 스택보호프로그램을 설치한다.
⑤ 스택영역을 비실행영역으로 설정한다.

51. 서버 관리자 A는 Web Server의 접속이 원활하지 않다는 연락을 받고 점검 중이다. 다음은 해당 서버에서 netstat명령을 실행한 결과이다. 이것을 보고 어떠한 공격으로 유추할 수 있는가?

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	155.131.44.3:80	123.12.85.123:1004	SYN_RECV
TCP	0	0	155.131.44.3:80	15.124.23.100:12	SYN_RECV
TCP	0	0	155.131.44.3:80	89.125.111.89:123	SYN_RECV
TCP	0	0	155.131.44.3:80	45.98.25.255:252	SYN_RECV
TCP	0	0	155.131.44.3:80	133.111.89.125:36	SYN_RECV
TCP	0	0	155.131.44.3:80	76.25.98.211:1024	SYN_RECV
TCP	0	0	155.131.44.3:80	176.12.1.129:1555	SYN_RECV

① Smurf
② Land
③ SYN Flood
④ Ping of Death
⑤ SSPin

52. 다음 내용은 어느 공격기법에 관한 설명인가?

침해 시스템을 분석하던 중 test라는 계정의 홈 디렉토리에서 C언어로 작성된 Exploit 코드와 컴파일된 바이너리파일을 발견할 수 있었다. 이 Exploit은 stack에 할당 되어진 변수에 데이터 사이즈를 초과 입력하여 RET를 덮어 씌워 ShellCode를 실행하는 코드였다.

① Buffer Overflow
② Format String
③ Race condition
④ Brute force
⑤ IP spoofing

53. 트러스터 관계가 맺어져 있는 서버와 클라이언트를 확인한 후, 클라이언트에 DoS 공격을 하여 끊은 후, 공격자가 클라이언트의 IP 주소를 확보하여 서버에 실제 클라이언트처럼 패스워드 없이 접근하는 공격방법은?

① IP Spoofing 공격
② IP Sniffing 공격
③ ARP Spoofing 공격
④ ARP Sniffing 공격
⑤ Trinoo 공격

54. 라우터에서 제공되는 로그관리에 대한 설명으로 잘못된 것은?

① 라우터의 로그는 관리상의 목적으로나 보안상의 목적으로 반드시 설정할 것을 권장한다.
② Buffered 로깅은 라우터의 버퍼에 로그를 남기도록 하는 방법으로 가장 많이 사용되는 기법이다.
③ Buffered 로깅은 매번 라우터에 로그인해야만 로그를 확인할 수 있다.
④ Buffered 로깅은 로그를 남길 수 있는 용량에 한계가 있다.
⑤ Syslog 로깅은 로그를 라우터에 남기지 않고 556/tcp를 통해 원격지의 호스트에 저장한다.

55. IP(Internet Protocol)에 보안기능을 제공하기 위하여 IETF(Internet Engineering Task Force)에 의하여 표준화된 IPSEC의 기능이 아닌 것은?

① 인증
② 암호화
③ 무결성
④ 접근통제
⑤ 키 교환(Key exchange)

56. 다음 괄호 안에 들어갈 수 있는 적절한 용어는?

라우터를 활용하여 네트워크 보안을 강화하기 위한 방법으로 access-list와 함께 유용하게 사용할 수 있는 기법으로는 ( ) 필터링이라는 것이 있다. 이는 access-list와 비슷한 효과를 내면서도 더욱 간편하게 사용할 수 있는데, 다음과 같은 경우를 생각해보자. 만약 시스템이나 네트워크를 모니터링하던 중 특정 ip 또는 특정 대역에서 비정상적인 시도가 감지되었을 경우 해당 ip를 차단하기 위해 매번 기존 access-list를 지우고 새롭게 ip를 추가하여 작성하는 것은 여간 번거로운 일이 아닐 수 없다. 이 필터링은 이때 사용될 수 있는데 명령어 자체는 특정한 목적지 ip 또는 ip 대역에 대하여 라우팅 테이블을 생성하는 방식과 동일하다. 다만 특정한 ip 또는 ip 대역에 대해서 Null이라는 가상의 쓰레기 인터페이스로 보내도록 함으로써 패킷의 통신이 되지 않도록 하는 것이다.

① Blackhole 필터링
② Unicast RPF를 이용한 필터링
③ Ingress filtering
④ Egress filtering
⑤ Multicast RPF를 이용한 필터링

57. 침입차단 시스템(Firewall)은 컴퓨터 네트워크 환경에서 네트워크 보안 사고가 주변 혹은 내부로 확대되는 것을 막기 위해 내부 네트워크와 외부 네트워크 사이의 정보 흐름을 안전하게 통제하는 시스템을 의미한다. 패킷 필터링을 이용한 방화벽의 단점이 아닌 것은 무엇인가?

① 속도가 다른 방화벽에 비해 느리다
② 패킷 헤더의 조작을 파악할 수 없다.
③ 데이터 부분에 바이러스가 감염되었을 경우 확인이 어려움
④ 접속제어 규칙의 개수 및 순서에 따라 부하 가중
⑤ 상대적으로 약한 logging 및 사용자 인증기능

58. 네트워크 공격이 의심이 갈 경우, Router 또는 Switch의 Netflow 기능을 이용해서 트래픽의 흐름을 모니터링 할 수 있다. 또는 Netflow 관련 Third-party tool을 이용한 분석도 가능하다. Netflow을 이용해서 다음 중 분석 할 수 없는 트래픽은 어느 것인가?

① Source Address
② Source Port
③ Window Size
④ Layer 3 Protocol
⑤ TOS Byte(DSCP)

59. iptables는 리눅스에서 기본적으로 작동하는 NetFilter 도구이며 방화벽 도구이다.
보기 중 iptables 설명 중 틀린 것은 어떤 것인가?

① 상태추적에 따라 매칭할 수 있는 기능이 있다.
② INPUT, FORWARD, OUTPUT chain을 통한 패킷 필터링 기능이 있다.
③ nat 테이블을 사용하여 패킷의 TOS값 등을 지정할 수 있다.
④ 라우팅 전에 IP 패킷의 TOS값을 지정할 수 있다.
⑤ 방화벽을 통해 어떠한 패킷이 통과했는지의 기록을 보관한다.

60. 라우터에 아래와 같은 ACL 정책을 설정하였다. 괄호 안에 들어갈 수 있는 조합으로 적당한 것은?

```
Router(config)#access-list 115 deny ip 130.18.0.0 0.0.255.255 any (      )
Router(config)#access-list 115 permit ip any any
Router(config)#interface FastEthernet0/0
Router(config-if)#ip (     ) 115 in
Router(config-if)#^Z
```

① log-input, access-group
② log-input, access-class
③ eq telnet, access-group
④ eq telnet, access-class
⑤ any, permit

SIS 2급 정보보호론

1. 다음 중 스트림 암호의 특성에 대한 설명이 잘못된 것은?

① One Time Pad를 실용적으로 구현할 목적으로 개발되었다.
② 안전하기 위해서는 다음에 출력 비트를 예측할 확률이 1/2이어야 한다.
③ 블록 암호의 OFB 모드를 사용하면 스트림 암호로 사용할 수 있다.
④ 긴 주기와 높은 선형복잡도가 요구된다.
⑤ 다양한 응용이 가능하여 난수 발생기, 해쉬 함수, 키 암호화 등 여러 분야에 활용된다.

2. 다음 중 성격이 다른 공개키 암호는 어떤 것인가?

① Rabin 공개키 암호
② 타원곡선 공개키 암호
③ ElGamal 공개키 암호
④ Braid 공개키 암호
⑤ XTR 공개키 암호.

3. 다음의 디지털 서명 중 특성이 다른 것은?

① Schnorr 서명 기법
② DSA
③ KC-DSA
④ Fiat-Shamir 서명 기법
⑤ Nyberg-Rueppel 서명 기법

4. 암호화 알고리즘 중 대칭 되는 두 개의 키를 이용하여 암호화 및 복호화를 수행하며, 두개의 키를 키 생성 알고리즘을 이용하여 생성하고 사용하는 암호 방식은 어느 것인가?

① 공통키 암호방식
② 관용키 암호방식
③ 공용키 암호방식
④ 공개키 암호방식
⑤ 단일키 암호방식

5. 다음 중 비밀키 암호화 알고리즘과 공개키 암호화 알고리즘에 대한 비교 설명한 것 중 잘못된 것은?

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.

6. 다음 설명은 무엇에 대한 것인가?

개방형 네트워크 환경에서 보안 요구 사항을 만족시키기 위해서 공개키 암호와 인증서의 사용을 가능하게 해주는 새로운 기반구조

① PGP
② RSA
③ MD5
④ SSL
⑤ PKI

7. 다음은 각 암호 알고리즘들이 개발된 배경을 설명한 것이다. 틀린 것은?

① 스트림 암호는 One Time Pad를 실용적으로 구현할 목적으로 개발되었다.
② 블록 암호는 암호문의 위·변조를 막기 위해서 개발되었다.
③ 공개키 암호는 키관리 문제를 극복하기 위해 개발되었다.
④ 해쉬 함수는 디지털 서명을 효과적으로 수행하기 위해 개발되었다.
⑤ 디지털 서명은 공개키 암호의 부산물로 개발되었다.

8. 다음에 열거된 사람들 중에 현대암호학과 관계가 큰 사람이 아닌 것은?

① R. L. Rivest
② C. E. Shannon
③ T. ElGamal
④ I. Einstein
⑤ W. Diffie

9. 보안 기술에 대한 설명으로 적절한 것은?

① 침해사고 예방에 필요한 특정한 기술을 말한다.
② 침해사고 후 시스템 복구를 위해 사용되는 툴 제작 기술을 말한다.
③ 침해사고 예방을 위해서 사용되는 암호화 분야의 기술을 말한다.
④ 침해사고 예방과 복구를 위한 전반적인 기술을 말한다.
⑤ 침해사고 예방과 복구를 위한 기술로써 컴퓨터 분야에 대한 설명이다.

10. 다음 중에서 일반적인 신분 확인 수단에 해당하지 않는 것은?

① 망막
② 스마트카드
③ 음성
④ 손톱모양
⑤ 지문

11. 기업의 시스템은 언제나 외부로부터의 위협에 노출되어 있다. 기업은 자사가 외부로부터 공격을 받았을 경우 어느 정도의 경제적 손실을 받는가에 대한 관심이 증대되고 있다. 다음 중 경제적인 범위에서 위험을 최소화하는 보안 대책을 작성하는데 필요한 정보를 제공하는 목적으로 하는 과정은?

① 정책 분석
② 위험 분석
③ 정보시스템 분석
④ 보안 관리
⑤ 위험 관리

12. 다음 중 프로그램 변경 통제절차에 포함되는 사항이 아닌 것은?

① 변경인가 수준에 대한 기록 유지
② 변경된 프로그램의 실무 도입을 위한 업무 중단
③ 모든 소프트웨어 갱신에 대한 버전 통제의 유지
④ 변경 업무 시작 전에 상세한 제안서에 대한 공식적 인가 획득
⑤ 프로그램 변경으로 인해 보안 및 무결성 통제 절차가 침해 받지 않았다는 것을 보장하기 위한 점검

13. 다음 위험분석 도구 선정기준에 대한 설명 중 틀린 것은?

① 데이터 입력, 도움말, 출력결과 등의 한글화 지원 기능은 위험분석도구의 유용성을 평가하는 중요한 선정기준요소이다.
② 사용자가 사용하기에 편하고 비용이나 결과보고방식 면에서 유용해야 한다.
③ 위험분석 요소가 전부 완전할 수 없으므로 해당 도구의 자산 및 취약성, 보도대책 등의 리스트를 사용자가 수정 및 추가 가능해야 한다.
④ 위험분석의 결과가 100% 신뢰할 수 있어야 한다.
⑤ 위험분석 시 사용되어지는 용어나 분류방식, 평가방법 등이 상이하지 않고 전체 프로세스에서 일관성을 유지해야 한다.

14. 정보보안 관리 방법 중 BS7799 정보보안 관리 시스템의 요구사항이 아닌 것은?

① 관리 프레임워크의 구축
② 조직은 선정한 통제 목표 및 방안을 구현
③ 정보보안관리 시스템은 문서화 되어져 관리된다.
④ 조직을 통제하기 위한 문서의 내용은 단순, 명료해야 한다.
⑤ 조직은 준수를 실증할 수 있는 기록을 식별, 유지, 보관, 폐기하여야 한다.

15. 다음 보기는 위험관리를 받을 조직 구성원의 기본 요건이다. 만약 다음 사항에 조직이 만족되지 못한다면 그에 대한 대응책으로 옳지 못한 것은?

< 보기>
가. 행위 자체의 옳고 그름을 판단할 수 있는 인식부분
나. 부적절한 행위를 문제/사고라는 관점에서 인식하고 실질적/적극적으로 대응하는 수준
다. 부적절한 행위를 처리/보고하는 정형화된 사고 대응 체계의 이해 정도.

① 정보보호 인식 훈련
② 정보보호 정책 수립
③ 정보보호 기반체계 구축
④ 정보보호 절차수립
⑤ 조직 내 실무자 교육

16. 잔여 위험에 대한 설명으로서 옳은 것은?

① 잔여 위험이 너무 작은 것도 바람직하지 않다.
② 잔여 위험은 음(-)의 값을 가질 수도 있다.
③ 잔여 위험이 작을수록 통제 구현 비용이 절약 된다.
④ 잔여 위험의 비율이 낮을수록 위험관리를 효율적으로 하는 것이다.
⑤ 통제가 증가하면 잔여 위험은 항상 감소한다.

17. 다음은 "정보통신망이용촉진 및 정보보호 등에 관한 법률"의 목적규정 내용 중 ( )에 적합한 내용은?

"이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 (가)을(를) 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성함으로써 (나)의 향상과 (다)의 증진에 이바지함을 목적으로 한다".

① 가: 권익보호, 나: 서비스의 품질, 다: 공공복리
② 가: 개인정보, 나: 정보통신기술, 다: 이용자의 권익보호
③ 가: 인격보호, 나: 보안의식, 다: 표준화
④ 가: 이용권, 나: 정보통신기술, 다: 정보화
⑤ 가: 개인정보, 나: 국민생활, 다: 공공복리

18. 다음 내용 중 현행 전자서명법의 규정내용에 비추어 타당한 것은?

① 전자서명은 전자상거래에 한정하여 사용된다.
② 공인인증기관이 발급한 인증서는 정부기관이 발급한 것과 같은 효력을 인정한다.
③ 어떠한 전자서명방식이라도 공인인증기관이 사용하는 것이면 법률에서 허용한다.
④ 인증기관의 임원 중 미성년자가 있는 경우에도 공인인증기관으로 지정 받을 수 있다.
⑤ 전자서명법상 공인인증기관에 관한 규정은 전자거래기본법상 인증기관과 전혀 관계없다.

19. 다음 중 정보화촉진기본법에 규정한 정보화시책의 기본원칙이 아닌 것은?

① 민간투자의 확대와 공정경쟁 촉진
② 국내 전자상거래 및 전자무역의 확대
③ 환경변화에 능동적으로 대응하는 제도의 수립, 시행
④ 정보통신기반에 대한 자유로운 접근과 활용
⑤ 개인의 사생활 및 지적재산권의 보호와 각종 정보자료의 안전성 유지

20. 다음 중 한국전산원이 수행하는 사업이 아닌 것은?

① 공공기관의 정보통신망 관리 및 운영의 지원
② 공공기관의 정보자원 관리의 지원
③ 정보문화의 확산 지원
④ 공인인증기관의 전자서명검증키에 대한 인증
⑤ 공공기관의 정보화사업에 대한 평가 지원

21. 스트림 암호 시스템에 대한 설명 중 옳지 않은 것은?

① 스트림 암호시스템은 LFSR(Linear Feedback Shift Register)를 이용한 이진수열 발생기를 이용한다.
② 스트림 암호는 비트 단위로 암호화하기 때문에 블록 암호에 비해 속도가 빠르다.
③ 이진 키 수열의 특성 및 이진 키 수열의 발생방법은 안전성 평가에 핵심이 된다.
④ 대표적인 암호화 알고리즘은 DES이다.
⑤ 다른 암호 알고리즘과 달리 수학적 분석이 가능하다.

22. 다음 중 블록 암호 동작모드가 아닌 것은?

① ECB(Electronic Code Book) 방식
② ECC(Error Correction Code) 방식
③ CFB(Cipher feedBack) 방식
④ CBC(Cipher Block Chaining) 방식
⑤ OFB(Output feedBack) 방식

23. 다음 중 RSA 암호 알고리즘을 이용, 응용 시스템을 구현하는데 있어서 가장 큰 문제점은 무엇인가?

① 알고리즘의 안전성
② 알고리즘에 사용되는 큰 수
③ 암호화/복호화 과정에 필요한 계산 능력
④ 알고리즘의 공개
⑤ 알고리즘에 사용되는 소수

24. 해시(Hash) 함수(H: 식 참조)의 사용 목적은 파일이나 메시지의 지문과 같은 고유의 인증요소를 제공하는데 있다. 다음 중 해시 함수의 특성이 될 수 있는 것은?

h = H(M)
H: 해시 함수
M: 메시지
h: 해시 값

① $y \neq x$ 인 경우, H(y) = H(x)가 성립한다.
② 인증절차의 간소화를 위해 H는 메시지(M)의 크기를 제한하는 것이 바람직하다.
③ 상호인증을 실현하기 위해서, 역으로 H(x) = h에서 x 값을 찾을 수 있다.
④ H는 고정된 길이의 해시 값을 출력한다.
⑤ 수신자는 메시지를 인증하기 위해서 해시 값을 재계산할 필요가 없다.

25. 암호화 방식을 분류하는 방법에서 암호 방식에 따른 종류 중 암호화 과정과 복호화 과정에서 같은 키를 사용하는 암호 방식을 무엇이라고 하는가?

① 공개키 암호방식
② 비밀키 암호방식
③ 치환키 암호방식
④ 교환키 암호방식
⑤ 혼합키 암호방식

26. 다음 중 대칭키 암호방식에 근거한 키 분배 알고리즘은 어느 것인가?

① Diffie-Hellman
② PKI
③ RSA
④ Kerberos
⑤ DSS

27. 다음은 공개키 암호 알고리즘에 대한 설명이다. 올바른 것은 어느 것인가?

① ElGamal은 이산대수의 어려움을 이용한 공개키 암호 알고리즘이다.
② Diffie-Hellman의 알고리즘은 소인수 분해의 어려움을 이용한 것이다.
③ RSA는 정보의 비밀성 보장을 위한 암호화에만 사용된다.
④ Rabin 암호 알고리즘은 소인수 분해의 어려움을 이용하는 Diffie-Hellman 알고리즘과 비하다.
⑤ ECC는 RSA에 비하여 사용되는 키의 길이가 길다.

28. 컴퓨터 보안에서 사용되는 암호에 관한 설명 중 옳은 것은?

① 암호는 정당한 권한이 부여된 사용자만이 데이터의 내용을 파악할 수 있는 데이터의 가용성을 보장해 준다.
② 암호는 수신된 메시지가 불법적으로 재생된 것인지 또는 전송과정에서 변조, 재구성되었는지 등을 확인할 수 있는 무결성을 보장한다.
③ 암호는 수신된 메시지가 정당한 송신자로부터 전송된 것인지를 확인할 수 있는 기밀성을 보장한다.
④ 암호는 메시지를 특정 수신자에게 전송할 때 송신자는 그 메시지의 발송을 나중에 부인할 수가 없고 또한 송신자에 의해서 발송되지 않은 메시지를 받았다고 수신자가 주장할 수 없도록 하는 인증을 보장한다.
⑤ 암호는 주어진 기간 동안 주어진 데이터를 사용할 수 있도록 하는 서명을 보장한다.

29. Rijndael 암호에 관한 설명 중에 맞지 않는 것은?

① 벨기에 수학자 Rijmen과 Daemen에 의하여 설계된 암호이다.
② 2000년에 AES로 최종 선택된 암호이다.
③ 블록의 길이와 키의 길이는 128비트, 192비트 또는 256비트로 가변적이다.
④ XOR 연산 및 모듈라 연산이 사용된다.
⑤ Feistel 구조이다.

30. 다음 중 전자서명(digital signature)에 관하여 잘못 기술한 것은?

① 그림, 영상 등 대량의 메시지에 대한 전자서명을 위하여 메시지 자체보다는 메시지의 해쉬값에 서명하게 된다.
② 타인에게 자신의 서명을 검증 받아야 하므로 전자서명 알고리즘은 주로 대칭키를 사용하는 블록암호를 기반으로 설계한다.
③ 전자서명된 문서를 타인이 검증해야 하므로 전자서명 알고리즘은 공개해야 한다.
④ 전자서명은 서명 된 문서의 내용을 삭제 또는 변경하는 것과 서명사실을 추후 부인하는 것 등이 불가능하다.
⑤ 현재 사용되는 인감과는 달리 각 문서마다의 서명이 다르며, 다른 문서에 이미 사용된 서명을 재사용을 할 수 없다.

31. 다음의 해쉬함수 중에서 성격이 틀린 것은?

① SHS
② MD1
③ MD4
④ MDC-4
⑤ MD5

32. 다음 중 공개키 기반구조(PKI)가 제공하는 보안 서비스가 아닌 것은?

① 비밀성
② 무결성
③ 사용자 인증
④ 침입탐지
⑤ 부인방지

33. 정보보호관리체계 인증에서 사용하는 용어의 정의는 다음과 같다. 틀린 것은?

① "신청인"이라 함은 인증심사를 신청한 신청기관의 책임자 또는 대표자를 말한다.
② "인증기관"이라 함은 정보통신망이용촉진 및 정보보호 등에 관한 법률 제52조의 정보통신위원회를 말한다.
③ "인증"이라 함은 신청인이 수립하여 운영하고 있는 관리체계가 인증심사기준에 적합함을 인증기관이 승인하는 것을 말한다.
④ “재심사”라 함은 인증을 취득한 기관이 인증의 유효기간 내에 인증 받은 관리체계의 범위 내에서 중대한 변화가 발생되었을 경우 신청인의 신청에 의하여 인증기관이 실시하는 인증심사를 말한다.
⑤ “인증심사원”이라 함은 인증심사를 수행하는 자를 말한다.

34. 위험 분석, 위험 관리와 위험 평가에 대한 설명 중 잘못된 것은?

① 위험 관리는 위험 분석과 위험 평가로 주된 활동이 결정된다.
② 위험 분석은 위험을 식별, 분석하고 적절한 보안 대책을 결정하는 단계이다.
③ 위험 관리는 보호 대상, 위협 요소, 취약성 분석 등을 통한 위험 분석이 포함된다.
④ 위험 관리는 적절한 보호 메커니즘을 선택, 선택된 메커니즘의 구현과 시험, 구현된 보호 메커니즘의 보안성 평가, 종합적인 보안의 재평가를 포함한다.
⑤ 위험 평가는 위험을 평가하여 적절한 보안 대책을 결정한다.

35. 패스워드의 할당은 규정된 관리 절차에 의해 통제한다. 다음 중 패스워드 관리에서 옳지 않은 것은?

① 패스워드를 사용자들이 직접 관리하는 경우, 초기에 관리자에 의해 제공되는 임시 패스워드를 사용자들이 즉시 바꾸어 관리하도록 한다.
② 패스워드를 잊은 경우 시스템 관리자는 신속하게 패스워드를 알려줘야 하며, 전자우편 등 신속하고 안전한 방법으로 전달한다.
③ 패스워드 분실로 임시 패스워드를 교부하는 경우 사용자의 신원을 확인한다.
④ 패스워드의 안전성을 확보하기 위해 스마트카드, 일회용 패스워드, 지문인식 등의 다른 방법 등의 사용을 고려한다.
⑤ 사용자들은 각자의 패스워드를 비밀스럽게 유지하고, 그룹의 패스워드를 그룹 구성원들 내부에서만 사용하도록 하는 문서에 서명한다.

36. 일반적인 위험관리 프로세스에서 가장 먼저 수행되는 단계는?

① 자산 및 프로세스 평가
② 위협 및 영향 평가
③ 취약성 분석

④ 통제 및 보안 분석
⑤ 위협의 확률(발생 가능성과 빈도의 결합) 평가

37. 정보보호 사후관리 활동을 포함하는 것은?

<보기>
1. 보안감사, 모니터링, 변경관리, 보안사고 대응
2. 준거성 체크, 모니터링, 변경관리, 시스템 유지보수, 보안사고 대응
3. 모니터링, 변경관리, 시스템 유지보수, 보안사고 대응
4. 구성관리, 변경관리, 보안감사, 보안사고 대응
5. 정보보호정책수립, 모니터링, 변경관리, 보안사고 대응

① 1, 4
② 2, 3
③ 4, 5
④ 1, 5
⑤ 3, 4

38. 아래와 같은 정보보호문제와 가장 밀접하게 관계된 것은?

전자상거래 지불시스템에서 송신자가 일정금액을 보냈는데 수신자가 금액을 받지 않았다고 부인하는 경우도 있고, 송신자가 보내고 수신자가 이를 받았는데 나중에 송신자가 보내지 않았다고 부인하는 경우가 있다.

①암호화
②디지털서명
③메시지인증
④인증서
⑤공개키

39. 데이터 등급 분류와 관련하여 맞는 것은?

① 데이터 등급 분류 체계는 정교해야 하며 단순해서는 안된다.
② 컴퓨터 자원에 대한 과잉보호를 줄인다.
③ 컴퓨터 자원의 접근은 관리인이 허가한다.
④ 시스템 개발 직원은 테스트 환경에서 접근해선 안된다.
⑤ 등급이 정해진 데이터는 변경이 불가능하다.

40. 정보화촉진기본법상 정부가 강구하여야 하는 시책으로 보기 어려운 것은?

① 전자적 방식에 의한 정보의 소재 안내에 관한 사항의 우선적인 시행
② 공공기관 간 정보의 독자적 활용을 위하여 필요한 사항의 우선적인 시행
③ 암호기술의 개발과 이용의 촉진
④ 이용자의 권익보호를 위한 시책의 강구
⑤ 합리적인 지적소유권의 보호시책의 강구

41. 정보통신망이용촉진및정보보호등에관한법률의 내용으로 볼 수 없는 것은?

① 이용자는 정보통신서비스제공자 등에 대하여 언제든지 정보통신망이용촉진및정보보호등에관한 법률의 규정에 의한 동의를 철회할 수 있다.
② 이용자는 정보통신서비스제공자등에 대하여 자신의 개인정보에 대한 열람을 요구할 수 있으며, 자신의 개인정보에 오류가 있는 경우에는 그 정정을 요구할 수 있다.
③ 정보통신서비스제공자가 만 14세 미만의 아동으로부터 정보통신망이용촉진및정보보호등에관한 법률의 규정에 의하여 개인정보를 수집하거나 이용 또는 제3자에게 제공하고자 하는 경우에는 그 법정대리인의 동의를 얻어야 한다.
④ 이용자가 정보통신서비스제공자등에 대하여 손해배상을 청구하는 경우 당해 정보통신서 비스제공자 등은 민법상 손해배상 책임 및 입증책임의 법리에 따라 배상을 하여야 한다.
⑤ 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁의 조정을 신청할 수 있으며 당사자가 조정안을 수락하고 조정서에 기명날인한 때에는 당사자간에 조정서와 동일한 내용의 합의가 성립된 것으로 본다.

42. 비밀키 암호화 방식 중 암호강도를 향상시키기 위해 대치(Substitution)암호와 전치(Transposition)암호를 혼합한 혼합변환식 암호 방식을 이용한 알고리즘은 어떤 것인가?

① SSL
② RSA
③ DES
④ MD5
⑤ IDS

43. 다음은 SHA-1과 MD5에 대한 비교 내용이다. 설명이 잘못된 것은 어느 것인가?

① SHA-1이 전수공격에 상대적으로 강하다.
② MD5가 SHA-1보다 암호 해독이 어렵게 설계되었다.
③ MD5가 동일한 플랫폼에서는 속도가 빠르다.
④ 두 알고리즘 모두 구현이 간단하다.
⑤ MD5는 메시지를 32-bit 단어의 연속으로 해석하는 little-endian 방식을 사용한다.

44. 다음은 DSS(Digital Signature Standard)에 대한 설명 중 잘못된 것은 어느 것인가?

① SHA-1을 사용한다.
② 전자서명 기술을 제공하기 위해서 설계된 알고리즘이다.
③ 비밀키 암호화 방식이다.
④ 해쉬 함수를 사용한다.
⑤ 해쉬 코드와 난수가 서명함수의 입력으로 제공된다.

45. 다음 중 스트림 암호에 관한 설명으로 잘못된 것은?

① 스트림 암호란 작은 길이의 키로부터 긴 길이의 난수를 발생시켜 평문과 XOR 하는 방법을 말하며 SEAL, A5, f8 등이 있다.
② 동기식 스트림 암호는 암호문 중 한 비트가 손실되거나 추가되면 복호화가 불가능 하다.
③ LFSR의 선형 복잡도는 매우 높기 때문에 단독으로 사용한다.
④ Cascade generator 스트림 암호란 하나의 LFSR이 다른 LFSR을 제어하는 구조를 말한다.
⑤ Nonlinear Combination Generator란 여러 개의 LFSR을 비선형 결합하여 만들어진 스트림암호를 말한다.

46. 공개키 암호인 RSA 암호에 관한 설명 중 잘못된 것은?

① 알고리즘의 안전성을 유지하기 위해서 비밀키는 공개키와 무관하게 생성해야 한다.
② 각 사용자는 개인의 비밀키 및 공개키를 setup 하기 위하여 큰 소수(prime number)를 생성하는 알고리즘이 필요하다.
③ 암호학적 안전성은 소수(prime number) 2개의 곱으로 이루어진 자연수를 소인수분해하는 것이 계산량적으로 어려움에 기반한다.
④ RSA 암호의 공개키는 암호화 키와 암호화 과정에 필요한 modulus인 n 값으로 구성된다.
⑤ 효과적인 RSA 암호 구현을 위해서는 큰 수에 관한 modular 연산 알고리즘이 필요하다.

47. 암호 프로토콜에 관한 설명 중 잘못된 것은?

① 영지식 식별 프로토콜이란 증명자가 자신이 올바른 비밀정보를 소유하고 있음을 소유한 비밀정보의 노출 없이도 검증자에게 확인시키는 방법이다.
② 개체 인증 프로토콜이란 증명자 A가 검증자 B에게 자신의 신원이 A임을 확인시키는 동시에 공격자 C가 A인 것으로 위장(impersonation)하지 못하게 하는 방법이다.
③ 키 복구(key recovery)란 신뢰하는 서버가 비밀 키 값을 생성하여 각 사용자에게 분배함으로써 사용자간에 분배된 정보를 이용하여 계속적으로 복구된 키를 사용하는 방법이다.
④ Challenge-response 식별 프로토콜이란 시간에 따라 변화되는 시도(challenge)에 대한 정확한 응답(response)을 제시하는 것으로 식별하는 방법이다.
⑤ 공개키 방식에 기반한 키 전송(key transport)은 한쪽 사용자가 대칭키를 선택하여 다른 사용자에게 이 대칭키를 그 사용자의 공개키로 암호화해서 전송하는 방법이다.

48. 블록암호의 사용에 관한 다양한 mode에 관한 설명으로 에러의 전이가 없고 키수열이 평문과 무관하여 미리 계산이 가능하고 또한 스트림 암호로 사용이 가능한 것은?

① CBC mode
② OFB mode
③ ECB mode
④ CFB mode
⑤ CTR mode

49. 해쉬함수에 대한 설계 조건이라 할 수 없는 것은?

① 가변 길이의 입력을 받아 고정된 길이의 해쉬 값을 출력한다.
② 해쉬 값이 주어졌을 때, 입력 값을 계산하는 것은 계산상 불가능하다.
③ 해쉬 값이 같으면서 입력값이 서로 다른 충돌쌍을 찾는 것은 계산상 불가능하다.
④ 어떤 길이의 입력 값이 주어지더라도 쉽게 해쉬 값을 구할 수 있어야 한다.
⑤ 일대일 대응 함수이다.

50. 정보보호 수립의 5단계를 올바르게 나타낸 것은?

① 조사와 분석 - 정보보호 - 보안탐지 - 대응 사후검토
② 조사와 분석 - 보안탐지 - 정보보호 - 대응 사후검토
③ 보안탐지- 조사와 분석 - 정보보호 - 대응 사후검토
④ 조사와 분석 - 보안탐지 - 대응 - 정보보호 사후검토
⑤ 보안탐지- 조사와 분석 - 대응 - 정보보호 사후검토

51. 단순한 DES 암호화 알고리즘은 다섯 단계의 함수로 이루어졌다. 다음의 다섯 단계의 DES 암호화 과정 중 잘못된 것은 어느 것인가?

① 1단계 : 초기 순열 함수 단계
② 2단계 : Key를 적용하고 순열과 치환을 포함하는 함수 단계
③ 3단계 : 데이터를 해쉬코드화 하는 함수 단계
④ 4단계 : Key를 적용한 순열과 치환을 포함하는 함수 단계
⑤ 5단계 : 초기 순열의 역 순열 함수

52. 정보보호 정책은 최소한의 표준을 포함하여야 한다. 다음 중 그 최소한의 표준이 아닌 것은?

① 필요한 보호의 수준에 따른 자산의 분류
② 비 인가된 접근으로부터의 정보보호 원칙
③ 물리적, 논리적, 환경적 보안 및 통신 보안
④ 시스템 개발 및 유지 방법론
⑤ 모든 직원에 대한 인사 관리

53. 다음은 내부 감사에 대한 설명으로 알맞지 않은 것은?

① 효과적으로 실행되고 유지되는지 여부를 결정하기 위하여 내부감사를 수행 하여야 한다
② 감사자는 자신의 업무에 대하여도 감사를 수행하여야 한다.
③ 문서화된 절차에는 감사의 계획, 수행, 감사의 독립성 보장, 결과의 기록 및 보고에 대한 책임과 요구사항을 정하여야 한다.
④ 감사대상 업무에 책임을 지는 경영자는 발견된 부적합 및 원인을 제거하기 위한 조치가 적시에 취해질 수 있도록 보장하여야 한다.
⑤ 후속 조치는 취해진 조치의 검증 및 검증 결과의 보고를 포함하여야 한다.

54. 보안 관리는 통상적인 정보 시스템 관리에 추가되어 관리되어야 한다. 다음 중 보안 관리 영역이 아닌 것은?

① 식별자(ID) 관리
② 인증 관리
③ 권한 부여 관리
④ 모니터링
⑤ 책임 추적성(accountability) 관리

55. 위험분석, 위험 관리와 위험 평가에 대한 설명 중 잘못된 것은?

① 위험 관리는 위험 분석과 위험 평가로 주된 활동이 결정된다.
② 위험 분석은 위험을 식별, 분석하고 적절한 보안 대책을 결정하는 단계이다.
③ 위험 관리는 보호 대상, 위협 요소, 취약성 분석 등을 통한 위험 분석이 포함된다.
④ 위험 관리는 적절한 보호 메커니즘을 선택, 선택된 메커니즘의 구현과 시험, 구현된 보호 메커니즘의 보안성 평가, 종합적인 보안의 재평가를 포함한다.
⑤ 위험 평가는 위험을 평가하여 적절한 보안 대책을 결정한다.

56. 정보통신기반보호법상 주요 통신기반시설의 지정에 관한 설명 중 틀린 것은?

① 중앙행정기관의 장은 소관분야의 정보통신기반시설중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요 정보통신기반시설로 지정할 수 있다.
② 중앙행정기관의 장은 위 ①의 규정에 의한 지정 여부를 결정하기 위하여 필요한 자료의 제출을 해당 관리기관에 요구할 수 있다.
③ 관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요 정보통신기반시설의 지정을 취소할 수 있다.
④ 중앙행정기관의 장이 위 ① 또는 ③의 규정에 의하여 지정 또는 지정 취소를 하고자 하는 경우에는 정보통신기반보호위원회의 심의를 받아야 한다.
⑤ 중앙행정기관의 장은 위 ①또는 ③의 규정에 의하여 주요 정보통신기반시설을 지정 또는 지정취소한 경우 국가안전보장을 위하여 필요한 경우에는 정보통신기반보호위원회의 심의 없이 이를 고시하지 아니할 수 있다.

57. 모니터링의 정도는 위험 분석에 의해서 결정되어야 한다. 다음 중 기본적인 감시 사항이 아닌 것은?

① 사용자 계정
② 입출력 장치 장착/탈착
③ 중요 사건의 날짜와 시각
④ 사건의 유형
⑤ 사용된 프로그램/유틸리티들

58. 정보통신 기반보호법상 정보통신기반보호위원회(지문에서 "위원회"라 한다)에 관한 규정의 내용으로서 틀린 것은?

① 위원회는 주요 정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 정보통신부장관 소속하에 둔다.
② 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.
③ 위원회의 위원은 대통령령이 정하는 중앙행정기관의 장과 위원장이 위촉하는 자로 한다.
④ 위원회의 효율적인 운영을 위하여 위원회에 실무위원회를 둔다
⑤ 위원회 및 실무위원회의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

59. 정보통신망이용촉진및정보보호등에관한법률상 정보통신서비스제공자가 이용자의 개인정보를 수집하는 것이 허용되는 경우로서 명시되어 있지 않은 것은?

① 이용자의 동의를 얻은 경우
② 정보통신서비스 이용계약의 이행을 위하여 필요한 경우
③ 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
④ 신용정보기관이 개인정보 제공을 위하여 필요한 경우
⑤ 법률에 특별한 규정이 있는 경우

60. 정보통신기반보호법상은 주요 정보통신기반시설 침해에 대하여 일정한 행위를 금지하고 있는 바, 이에 해당하지 않는 것은?

① 접근권한을 가지지 아니하는 자가 주요 정보통신기반시설에 접근하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
② 접근권한을 가진 자가 그 권한을 초과하여 주요 정보통신기반시설에 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
③ 주요 정보통신기반시설의침해에 대응할 목적으로 논리폭탄 프로그램을 투입하는 행위
④ 주요 정보통신기반시설의운영을 방해할 목적으로 일시에 대량의 신호를 보내는 방법으로 정보처리에 오류를 발생하게 하는 행위
⑤ 주요 정보통신기반시설의운영을 방해할 목적으로 부정한 명령을 처리하도록 하는 방법으로 정보처리에 오류를 발생하게 하는 행위

SIS 2급 단답형

1. 다음 각각의 괄호에 들어갈 약어는?

이메일을 암호화하는 방법으로 널리 쓰이는 (　　)는 Phil Zimmerman의 고안으로 키 관리에는 RSA를, 데이터 암호화 알고리듬으로는 (　　)를 사용한다.

2. 다음 문제의 괄호 안에 알맞은 단어나 기호를 넣으시오.

RSA 알고리즘은 다음과 같이 구성된다.

1. 매우 큰 두 소수 p 와 q 를 선정한다.
2. $n = pq$, $z = (p-1)(q-1)$ 을 계산한다.
3. z 와 서로소인 정수 d 를 고른다.
4. $ed = 1 \mod z$ 인 e 를 고른다.

RSA 알고리즘에서 공개키는 d , 비밀키는 (　　)이다. 물론 이 방법에서는 n 을 공개한다. 그런데 만일 공개된 합성수 n 을 (　　)분해해서 p 와 q 를 알아낼 수 있다면 RSA 알고리즘은 더 이상 안전하지 않다.

3. 1995년 케빈 미트닉이라는 해커가 최초로 시도한 해킹방법으로, 자신의 IP를 프록시 서버를 이용하여 속여 해킹을 시도하는 것을 무엇이라고 하는가?

4. 다음의 방식은 WWW상의 데이터를 안전하게 교환될 수 있게 해주는 방법들이다. 빈칸에 들어갈 용어는 무엇인가?

(①　　)은 EIT(Enterprise Integration Technologies)에서 제안한 WWW에서 보안을 강화할 수 있도록 구성되어진 메시지 기반 프로토콜이다. 그리고 광범위한 응용 레벨에서 상업적인 트랜잭션을 수행하기 위하여 클라이언트-서버간 안전한 통신 기법을 제공하도록 개발되었으며 세션으로 주고받는 정보를 암호화하고 전자서명을 실행할 수 있도록 보안기능을 제공한다. 또한 요청(request)과 응답(response) 구조로 되어 있는 메커니즘이다.
반면에 (②　　)는 테리사(Terrisa)가 개발해 Netscape사가 Netscape과 NetSite의 암호화 중심 프로토콜로 사용하는 프로토콜이다. 이 프로토콜은 서버와 클라이언트간에 인증으로 RSA방식과 X.509를 사용하고 실제 암호화된 정보는 새로운 암호화 소켓채널을 통해 전송하는 방식이다. 그래서 WWW뿐 아니라 NNTP, FTP등에도 사용할 수 있는 장점이 있다. 또한 양자간의 안전한 접속을 이루고 상대방의 비밀키 없이 암호요소를 전달하여 새로운 공개키나 데이터 암호방법을 적용시킬 수 있다.

5. 시스템내의 메모리 접근, 프로세스 생성 및 관리, 입출력 디바이스 관리, 파일 시스템을 통한 파일의 관리, 사용자에게 서비스 제공 등의 역할을 수행하고 이것은 쉘과 대비될 수 있는데, 쉘은 운영체제의 가장 바깥부분에 위치하고 있으면서, 사용자 명령어에 대한 처리를 담당하면서 운영체제의 핵심 부분인 것은 무엇인가?

6. 공격자가 임의의 평문을 선택하면 대응하는 암호문을 획득할 수 있는 능력을 보유하고서 주어진 암호문에 대응하는 평문이나 키를 알아내고자 하는 암호공격 방식을 무엇이라고 하는가?

7. 신분을 근거하여 데이터에 대한 접근을 제한하는 시스템 접근통제 기술로 주체의 신분에 근거하기 때문에 데이터의 의미에 대한 지식이 없으며, 트로이목마 공격에 취약성을 가지고 있고, 하나의 주체와 객체에 대한 관계를 정의되어 객체를 복사하는 경우에도 객체의 접근통제 정보가 전파되지 않는 접근통제 방법을 무엇이라고 하는가?

8. 개방 네트워크상에서 안전하고 건전한 서비스가 이루어 질 수 있도록 통신 정보의 비밀성, 인증성, 무결성, 부인방지 등 기본적인 보안 서비스를 가장 효과적으로 제공하는 기술로서, 인터넷상에서 메시지 송신자를 인증하거나 메시지를 암호화하는데 있어 가장 보편적인 이 방법은?

9. 아래에서 말하는 이것이란 무엇인가?

> 이것은 인터넷에서 강력하고 우수한 보안 기능을 제공하는 보안 메커니즘을 위한 기술로서 그 중에서도 트래픽 제어와 인증 및 암호화를 제공하여 점대 점(Point to Point) 사용자들 간의 안전한 트래픽 제공을 위한 서비스이다.
> 이것이 제공하는 보안 서비스들은 접근통제(access control), 비연결형 무결성(connectionless integrity), 데이터 근원 인증(data origin authentication), 재연공격 방지(protection against replays), 비밀성(confidentiality) 등을 포함하고 있다.

10. 웹 브라우저 개발로 잘 알려져 있는 넷스케이프 사에서 처음으로 제안되어, 자사의 웹 어플리케이션에 처음으로 구현함으로써 현재 웹 보안의 대명사로 알려진 보안기술로, TCP/IP 계층과 어플리케이션계층(HTTP, Telnet, FTP 등) 사이에 위치하여 데이터를 송수신하는 두 컴퓨터 사이 즉, 종단간 보안서비스는?

11. 다음은 OSI 7레이어의 어떤 계층을 설명하고 있다. 빈칸을 채우시오.

OSI 참조모델의 두 번째 계층인 (ⓐ) 계층은 데이터 패킷을 생성하고 전송하는 방법을 규정하는 프로토콜에 대한 계층이다. 이 계층은 보통 (ⓑ) 과 (ⓒ) 라는 두 가지 계층으로 다시 세분화할 수 있다. (ⓑ) 계층은 동일 채널을 공유하는 통신 방법을 제어하기 위한 것이고, (ⓒ) 계층은 데이터 전송을 위해 물리적 장치를 논리적으로 연결하고, 연결을 유지하는 역할을 담당한다.

12. 다음은 무선 인터넷 보안기술에 대한 설명이다. 빈칸을 채우시오.
(ⓐ)은(는) 무선 인터넷 환경에서 기존의 인터넷 프로토콜을 사용할 경우에 발생하는 문제점들을 해결하고, 기존 인터넷 중심의 데이터 서비스를 무선환경에서 효율적으로 처리하기 위해 제안된 프로토콜이다. (ⓐ)은(는) 전송 계층에서 동작하는 보안 프로토콜인 (ⓑ)을(를) 이용하여 기밀성, 무결성, 인증 및 부인봉쇄의 기능을 제공한다.

13. 다음은 스머프(smurf) 공격에 대한 설명이다. 빈칸을 채우시오.
스머프 공격이란 공격자가 자신의 소스주소를 마치 다른 주소인 것처럼 위조하여 특정 네트워크의 (ⓐ) 주소로 icmp (ⓑ) 패킷을 보낸다. 보내진 패킷은 브로드캐스트 영역 내에 있는 모든 컴퓨터에게 그대로 전달되고 icmp (ⓑ) 패킷을 받은 모든 컴퓨터는 패킷의 소스주소(위조된 IP)로icmp (ⓒ) 패킷을 보내어 응답하게 된다. 이 때 (ⓐ) 주소로 요청을 받아 응답한 네트워크의 증폭기, 공격자가 위조한 IP는 희생자가 된다.

14. OSI Layer 2의 MAC 주소에서 브로드캐스트 주소는 (A)이며
161.134.4.0/22 네트워크의Directed 브로드캐스트 주소는(B)이다

15. (A)는 오픈 소스 네트워크 침입탐지 시스템으로서 IP 네트워크에서 실시간 트래픽 분석과 패킷 로깅 작업을 수행할 수 있다. (A)는 프로토콜 분석, 컨텐츠 검색/비교 작업을 할 수 있으며 다양한 공격과 스캔을 탐지 할 수 있다. (A)는 패킷 로거, 스니퍼, 네트워크 침입 탐지 모드에서 동작할 수 있다. 그 중 (B)모드는 단순히 네트워크에서 패킷을 읽어서 콘솔에 출력하는 모드이다.

SIS 2급 서술형

1. 다음은 네트워크 모니터링 툴을 이용해 트래픽을 감시하던 중 이상 징후를 포착하고 Cisco 사의 라우터에 접속하여 시스템의 CPU, Memory 사용량을 출력한 로그이다. 이상 징후가 나타나기 전의 출력 로그와 이상 징후를 포착한 이후의 로그를 비교하여 볼 때 유추할 수 있는 현재의 네트워크 상태와 이상 징후에 대한 정보를 기술하시오.

(작성 가능한 답안의 범위를 축소하기 위하여 가급적 서술 및 작업형태를 명확히 지정 요망)

참고 1) 이상징후 나타나기 전 출력 로그

```
CPU utilization for five seconds : 3%/2%; one minute : 2%; five minutes: 2%
PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min  TTY  Process
 1         80     344071      0    0.00%  0.00%  0.00%   0  Load Meter
 2        320     70615       1    0.00%  0.00%  0.00%   0  OSPF Hello
      ..........
```

참고 2) 이상징후 포착 후 출력 로그

```
CPU utilization for five seconds: 28%/3%; one minute:24%; five minutes:7%
PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min  TTY  Process
 1         232    359182      0    0.00%  0.00%  0.00%   0  Load Meter
 2         340     90615      3    0.00%  0.00%  0.00%   0  OSPF Hello
      ..........
      28   45991444 328773859    139   0.16%   0.04%  0.02%   0  IP Input
           ..........
```

참고 3) 로그 설명

최근 5초 동안의 CPU 활용도(CPU utilization for five seconds)에서 처음 숫자는 전체 CPU 사용률을 명기하고 있고, 두 번째 숫자는 인터럽트 레벨에서 사용된 CPU 시간의 비율을 의미한다

2. 다음은 Apache 웹 서버 프로그램을 설치한 후, 성능 향상 및 보안 강화를 위하여 다루게 되는 환경파일 httpd.conf 파일 안의 항목들을 나열한 것이다. 각 항목이 어떤 의미를 가지고 있는지 할당 값(혹은 추천하는 값)과 함께 간단하게 서술하라.

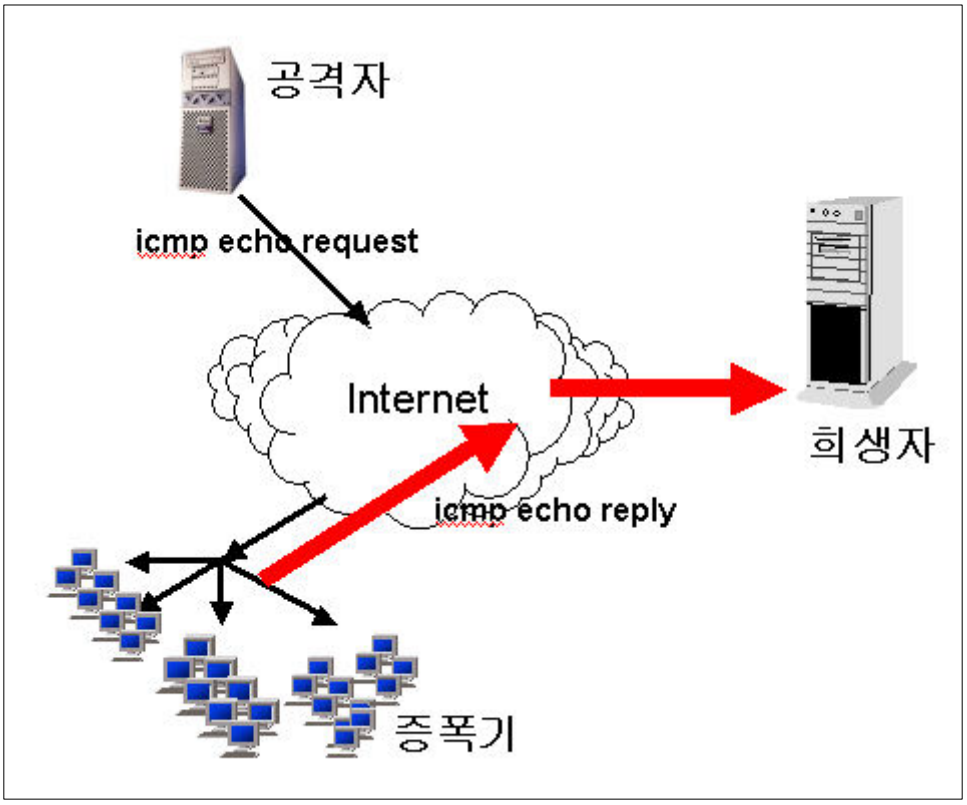
1. Port
2. ServerAdmin
3. Timeout
4. PidFile
5. User와 Group

3. ARP 스푸핑에 대하여 다음 각 질문에 답하시오.

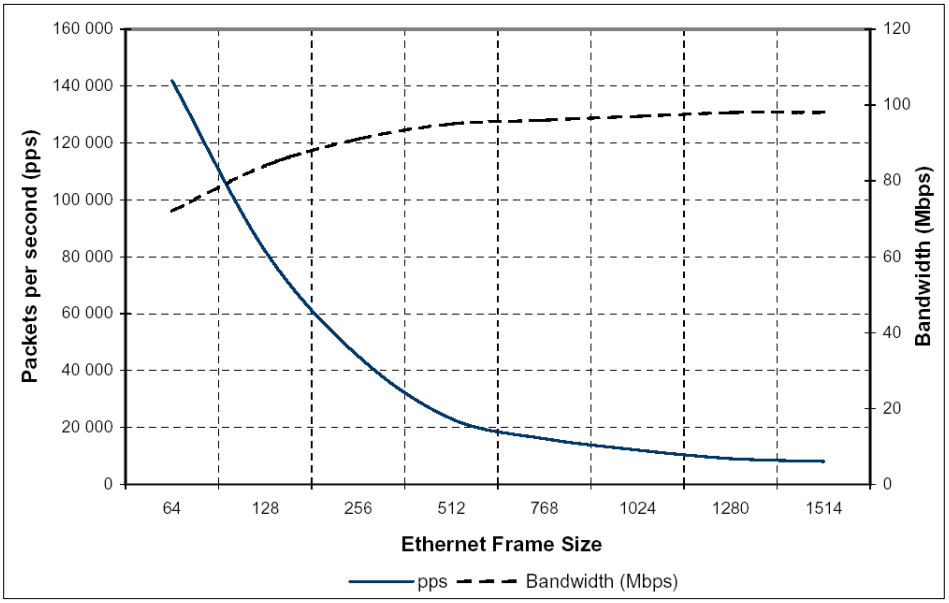
(1) ARP 스푸핑이란 무엇인가? 간단히 답하시오.
(2) ARP 스푸핑은 공격대상이 어디에 존재할 때 가능한가? 이유는?
(3) 철수와 영희 사이에서 공격자가 ARP 스푸핑하는 과정을 기술하시오.
단, 철수(ip:192.168.0.1, MAC:A), 영희(ip:192.168.0.2, MAC: B), 공격자(ip:192.168.0.3, MAC:C)
(4) 철수는 영희와는 안전하게 통신하고 싶다. 다른 툴을 사용하지 않고 간단하게 ARP 스푸핑을 막을 수 있는 방법은 무엇인가?

SIS 2급 실무형

1. 다음은 서비스 거부 공격 중 하나인 스머프(smurf) 공격의 작동 원리를 보여주고 있다. 그림에서와 같이 스머프 공격은 실제 공격자와 희생자 그리고 증폭기 네트워크로 사용되는 제2의 희생자가 존재하는데, 아래에서 여러분의 네트워크가(1) 공격자 (2) 희생자 (3) 제 2의 희생자인 증폭기 네트워크로 사용되지 않기 위해서 취할 수 있는 방법은 무엇인지 각각 설명해 보시오. (단, 이로 인하여 정상적인 서비스가 영향을 받아서는 안 되며 각자 다른 네트워크라고 가정한다.)



2. 아래의 그래프는 특정한 방화벽의 성능을 측정한 결과이다. Ethernet Frame 사이즈를 64 바이트에서 1514 바이트까지 변화시키며 PPS를 측정한 결과 바이트 수가 작을수록 PPS(Packet per Second)의 수치가 높고 Frame 사이즈가 클수록 PPS값이 작은 것을 알 수 있다. 반면에 Bandwidth는 Frame 사이즈가 클수록 값이 크다. 이러한 현상은 대부분의 방화벽에서 나타난다. 이런 현상이 생기는 이유를 설명하시오.



3. 다음은 한 침입탐지시스템(snort)에 탐지된 로그를 보여주고 있다.

(1) 로그를 보고, 공격으로 탐지된 이유는 무엇인지 2가지 이유를 설명하라.
(2) 아울러 이러한 패킷을 차단할 수 있는 방법은 무엇인지 서술하라.

```
10/29-19:33:32.232372 68.127.38.3:23 -> xx.yy.200.17:23
TCP TTL:31 TOS:0x0 ID:39426 IpLen:20 DgmLen:44
******SF Seq: 0x638CECE1Ack: 0x1DB99E53Win: 0x404TcpLen: 24
TCP Options (1) => MSS: 536
```

끝.