2007년 제1, 2차 SIS 1급 필기시험

정보보호전문가 1급 필기 시험

필 기 시 험			
시험과목	시스템보안/어플리케이션보안		
시험지역		**시험시간**	
수검번호		**성 명**	

⇒ 2007년 1·2차 시험문제 중 일부를 공개합니다.

정 보 보 호 전 문 가 1 급 필 기

과 목	시스템 보안 07년 2차

1. 다음 지문에서 설명하고 있는 '윈도우즈 서버 2003'의 보안 서비스는 무엇인가?

> IANA(Internet Assigned Numbers Authority)로부터 할당받지 않은 비공인 사설 인터넷 주소(Private IP Address)를 기업의 인트라넷에서 사용하더라도 인터넷과 통신할 수 있도록 해주는 기능으로, 라우팅이 불가능한 주소를 가진 컴퓨터가 라우팅이 가능한 인터넷상의 다른 컴퓨터와는 통신을 할 수 있지만 반대의 경우는 통신을 허용하지 않아서 외부의 침입자 접근을 차단할 수 있다.

① SSL
② NAT
③ PAP
④ MS-CHAP
⑤ IPSec

2. 프로그램에 이상이 있거나 자신이 의도하지 않는 프로그램이 백그라운드로 실행되고 있는지를 알고 싶을 때 프로세스의 확인 작업을 하게 되는데, 윈도우즈에서는 작업관리자를 통하여 프로세스를 확인할 수 있다. 아래에서 설명하고 있는 프로세스는 무엇인가?

> winlogon 서비스에 필요한 인증 프로세스를 담당한다.

① lsass.exe
② csrss.exe
③ winmgmt.exe
④ smss.exe
⑤ services.exe

3. 다음 중 파일에 대한 부적절한 접근으로부터 보호하기 위한 방법이 아닌 것은?

① 접근 제어 리스트
② 접근 제어 행렬
③ 파일 압축(Compression)
④ 파일의 명명법(Naming)
⑤ 암호화(Encryption)

4. 다음 중 XSS(Cross Site Script) 공격에서 주로 가져오는 정보는 무엇인가?

① cache
② Authentication
③ cookie
④ DB 파일
⑤ log 파일

5. 다음 중 윈도우 운영체제에서 'd$'라는 공유 자원의 공유를 제거하는 명령어로 맞는 것은?

① delete d$
② net delete d$
③ net share d$ /delete
④ delete share d$
⑤ netsh delete d$

6. 다음 지문에서 설명하고 있는 웹 브라우저의 오류 메시지에 대한 실행결과 코드는?

클라이언트가 서버에 보내는 요구 메시지를 완전히 처리하지 못한 경우와 같이 클라이언트에서 오류가 생긴 경우에 발생하는 실행결과 코드로 사용된다.

① 100번 대
② 200번 대
③ 300번 대
④ 400번 대
⑤ 500번 대

7. 다음 지문에서 설명하는 트로이목마 S/W는 어느 것인가?

◦ 자신과 다른 소프트웨어를 숨기기 위해 사용된다. ◦ 윈도우용으로는 FU-Rootkit, Hxdef100, NTRootkit 등이 있다. ◦ 리눅스용으로는 Suckit, Irk5, Idore 등이 있다.

① 넷버스
② 백오리피스
③ 루트킷
④ 스쿨버스
⑤ ack층

8. 다음은 악성 프로그램의 유형에 대한 설명이다. 잘못 설명된 것은 어느 것인가?

① 바이러스 : 바이러스는 복제와 감염의 특징을 가지며 네트워크를 통해 스스로 전파되지는 않는다.
② 웜 : 다른 컴퓨터의 취약점을 이용하여 네트워크를 통해 전파되는 특징을 지닌다.
③ 트로이목마 : 컴퓨터에 직접적인 피해를 입히진 않지만 침투한 컴퓨터를 조작할 수 있고, 자신을 다른 파일에 복제할 수 있다.
④ Hoax : 인터넷 메신저나 이메일 등에 거짓정보나 괴담 등을 실어 사용자를 속이게 된다.
⑤ Mail bomb : 특정인이나 특정 컴퓨터로 수많은 메일을 보내 해당 시스템을 마비시킨다.

9. 트로이 목마 프로그램으로 사용자의 키보드 입력을 가로채는 목적으로 사용되기 때문에 이 프로그램이 동작하는 컴퓨터에서 입력되는 모든 것이 기록되어 개인정보 등이 도용당하게 되는 해킹기법은 무엇인가?

① 포트스캔
② 쿠키
③ DoS
④ 히스토리
⑤ 키로그

10. 솔라리스 시스템에서는 TCP/IP 스택에 여러 가지 사용자 인터페이스를 제공한다. 시스템 관리자들은 네트워크 커널 변수들을 튜닝하기 위한 툴 ndd를 사용함으로써 보안을 강화할 수 있다. ndd 사용에 관한 설명으로 옳지 않은 것은?

① TCP/IP 커널에는 ARP, IP, TCP, UDP 등이 포함된다.
② ndd를 사용하여 각각의 드라이버에 대하여 모든 커널 변수들을 보는 명령어는 'ndd /dev/드라이버' 이다.
③ ndd를 사용하여 각각의 드라이버에 대하여 커널 변수를 설정하기 위해서는 'ndd -set /dev/드라이버' 명령어를 실행하면 된다.
④ ndd를 사용하여 커널 변수 변경 후에는 설정된 값이 계속적으로 적용되어 남아있기 때문에 시스템 재부팅 시에도 다시 설정할 필요가 없다.
⑤ Cache 테이블의 Lifetime 및 다수의 TCP 연결에 대한 여러 가지 옵션을 통하여 Kernel Parameter의 설정 및 제어가 가능하다.

11. 리눅스 시스템 관리자가 /var/log/messages 파일에 다음과 같은 로그 기록이 남아있는 것을 발견했다고 한다. 이 로그 분석에 대한 설명으로 옳지 않은 것은?

```
Mar 14 16:34:13 kisa sshd[1799]: Accepted password for kisa1 from 172.16.5.193 port 1035 ssh2
Mar 14 16:34:13 kisa PAM_unix[1799]: (system-auth) session opened for user kisa1 by (uid=0)
Mar 14 16:34:25 kisa PAM-Wheel[1831]: Access denied for 'kisa1' to 'root'
Mar 14 16:34:49 kisa sshd[1835]: Accepted password for kisa2 from 172.16.5.194 port 1036 ssh2
Mar 14 16:34:49 kisa PAM_unix[1835]: (system-auth) session opened for user kisa2 by (uid=0)
Mar 14 16:34:53 kisa PAM-Wheel[1860]: Access granted to 'kisa2' for 'root'
Mar 14 16:34:56 kisa PAM_unix[1860]: (system-auth) session opened for user root by kisa2(uid=500)
```

① 위의 내용은 su 명령 사용이 허용되어 있는 사용자와 그렇지 않은 사용자가 su 명령을 사용했을 경우 모두 보여주고 있다.
② 사용자 kisa2는 su 명령 사용을 위해 /etc/group 파일에서 wheel 그룹의 사용자로 등록되어 있다.
③ 사용자 kisa1은 su 명령 사용을 위해 /etc/group 파일에서 wheel 그룹의 사용자로 등록되어 있지 않다.
④ 사용자 kisa1과 kisa2는 /etc/pam.d/su 파일에 wheel 그룹뿐 아니라 사용자 계정에 대해서도 등록되어 있어야 한다.
⑤ 사용자 kisa1과 kisa2 모두 해당 시스템의 적법한 사용자들이다.

12. 아래의 로그 및 상황을 잘못 분석하고 있는 것은?

```
# cat /var/adm/messages
may 15 18:45:38 victim /usr/dt/bin/rpc.ttdbserverd[29906]:
_Tt_ftle_system::findBestMountPonint --max_match_entry is null, aborting...
may 15 18:45:39 victim inetd[147]: Segmentation Fault -core dumped
may 15 18:45:50 victim /usr/dt/bin/rpc.ttdbserverd[8206]: iserase(): 78
may 15 18:46:08 victim inetd[147]: /usr/sbin/sadmind: Bus Error -core dumped
may 15 18:46:18 victim last message repeated 1 time
may 15 18:46:28 victim inetd[147]: /usr/sbin/sadmind: Segmentation Fault - core
dumped
may 15 18:46:30 victim inetd[147]: /usr/sbin/sadmind: Hangup
may 15 18:50:15 victim login: change password failure: No account present for
user
may 15 18:52:23 victim last message repeated 2 times
may 15 18:55:25 victim inetd[147]:/usr/dt/bin/rpc.ttdbserverd:Killed
may 15 18:55:25 victim inetd[147]:/usr/dt/bin/rpc.cmsd: Killed
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
# ls -alc /tmp/.x
-rw-rw-rw-  1 root   root  48  5월 15일 18:46 /tmp/.x

# more /tmp/.x
ingreslock stream tcp nowait root /bin/sh sh-i
```

① 5월 15일 18시 45분부터 rpc.ttdbserverd, sadmaind, rpc.cmsd에 대한 공격 흔적을 볼 수 있다.
② /var/adm/messages의 로그만으로도 루트(Root)권한을 취득했는지 알 수 있다.
③ sadmind의 버퍼오플로우 취약점으로 공격당한 것으로 판단된다.
④ 공격이 이루어진 시간대에 /tmp/.x 파일이 생성되었고 ingreslock에 root shell이 바이딩 되어있는 것으로 보아 sadmind 공격이 성공한 것으로 보인다.
⑤ 로그에서 3차례 패스워드 변경 실패 사실을 확인할 수 있다.

13. 크래커들이 자주 사용하는 방법 중에는 한번 들어온 서버에 다시 쉽게 침입할 수 있도록 suid가 설정된 root 소유의 프로그램을 백도어로 설치하여 다음에도 손쉽게 root 권한을 획득할 수 있도록 하는 방법이 있다. 아래의 명령어를 사용하여 시스템관리자는 주기적으로 suid로 설정된 파일을 모니터링 하여 시스템을 안전하게 보호할 필요가 있다.
괄호( ) 안에 들어갈 옵션을 순서대로 바르게 나타낸 것은 어느 것인가?

```
#find / -( ) root -( ) 4000 -( ) ls -l { } ₩;
```

① user, exec, perm
② exec, user, perm
③ perm, user, exec
④ user, perm, exec
⑤ exec, perm, exec

14. 유닉스 계열에서는 /etc/passwd와 /etc/shadow 파일이 인증에 있어서 가장 중요한 역할을 한다. 그러나 /etc/passwd 파일은 644권한으로 할당되어 있어서 일반 사용자 계정으로도 읽을 수 있으므로 패스워드가 암호화된 /etc/shadow 파일을 생성시킬 필요가 있다. 다음 중 이를 위한 명령어는 어느 것인가?

① passwd
② pwdump3
③ chntpw
④ pwunconv
⑤ pwconv

15. 다음 중 유닉스 시스템의 syslog 레벨(level)은 심각성(severity) 레벨을 의미하는데 심각성 레벨을 심각도에 따라 바르게 분류한 것은 어느 것인가?

① emerg > alert > crit > err > warn > notice > info > debug
② emerg > err > crit > alert > warn > info > notice > debug
③ emerg > alert > crit > err > warn > info > notice > debug
④ emerg > warn > crit > err > alert > info > notice > debug
⑤ emerg > alert > crit > warn > err > notice > info > debug

16. 다음 지문은 여러 가지 시스템에서 나타나는 보안 취약점들에 대한 설명이다. 아래 보기 중 잘못 설명된 것으로 짝지어진 것은?

㉮ rsh, rlogin 등의 서비스는 시스템보안에 안전한 서비스이다. ㉯ IIS가 설치될 때 몇몇 ISAPI 확장들이 자동으로 설치됨으로써 ISAPI 확장 버퍼 오버플로우 취약점이 발생할 수 있다. ㉰ SetUID가 설정되어 있는 실행 파일은 보안이 우수하다. ㉱ 공격자는 부적절한 유니코드 UTF-8 시퀀스를 포함한 URL을 IIS서버에 전송함으로써 디렉토리를 이동할 수 있고 임의의 스크립트까지 실행시킬 수 있다. ㉲ 로컬 보안 권한 서브시스템 서비스(LSASS)의 버퍼 오버런 취약점을 이용하여 웜 바이러스의 침투 경로로 사용한다.

① ㉮, ㉰
② ㉯, ㉰
③ ㉯, ㉲
④ ㉰, ㉱
⑤ ㉱, ㉲

17. 리눅스 로그 파일 중 보안인증 관련 메시지 및 Tcp Wrapper의 메시지 등을 포함하여 아래와 같은 로그를 가지는 로그파일은?

Apr 19 23:23:35 unsecure in.telnetd[645]: connect from 172.16.2.14 Apr 19 23:23:41 unsecure login: LOGIN ON 2 BY hcjung FROM hcjung Apr 20 23:24:29 unsecure in.telnetd[1218]: refused connect from bluebird.a3sc.or.kr Apr 20 23:25:27 unsecure in.telnetd[1219]: connect from 172.16.2.161

① access log
② system log
③ secure
④ pacct
⑤ spool

18. 유닉스 환경변수 중 일부는 설정값을 조정함으로써 공격에 이용할 수 있다. 아래는 그 중 하나인 PATH 변수에 대한 예제인데, 여기서의 PATH 변수 설정에서 보안상 바람직하지 않은 부분을 바르게 설명하고 있는 것은?

```
# set | grep PATH
PATH=./:/usr/local/bin:/bin/:/usr/bin:/usr/sbin
```

① PATH에 2개 이상의 디렉토리가 지정되었다.
② 현재 디렉토리가 맨 앞에 지정되었다.
③ PATH 변수의 지정된 형식을 따르지 않아 정의가 적용되지 못한다.
④ /usr/sbin보다 /usr/bin 디렉토리가 앞에 지정되었다.
⑤ 시스템 lib 디렉토리들이 경로 설정에서 누락되어 있다.

19. 침해사고 시 로그를 분석하여 비인가자의 접근내역과 수행한 작업 등 여러 가지 상황에 대한 파악을 할 수 있다. 다음 로그 파일들 중에 해커에 의해 악용될 수 있는 위험이 가장 높은 시스템 내부의 로그 파일은 어느 것인가?

① system log
② access log
③ agent log
④ reference log
⑤ error log

20. 다음은 리눅스/유닉스 시스템의 passwd 파일의 구조이다. 패스워드가 암호화되어 shadow 파일에 저장되어 있는 것은 어느 것인가?

```
root : x : 0 : 0 : root : /root : /bin/bash
 ㉮   ㉯  ㉰  ㉱          ㉲
```

① ㉮
② ㉯
③ ㉰
④ ㉱
⑤ ㉲

21. 침해사고 시 로그를 분석하여 비인가자의 접근내역과 수행한 작업 등을 확인할 수 있다. 다음과 같은 내용을 보여주는 로그는?

로그인한 계정의 권한 변경에 대한 로그으로 이 로그는 공격자가 일반계정으로 로그인한 후 패스워드 추측공격 등을 수행했을 때 권한변경 실패를 의미하는 '-'로 저장되기 때문에 관리자가 이를 확인하여 공격의도를 가진 일반계정을 추적해 낼 수 있다.

① wtmp
② utmp
③ sulog
④ pacctcomm
⑤ lastlog

22. 다음 지문의 설명 중 잘못된 것은 어느 것인가?

㉮ 유닉스/리눅스 시스템에서는 각 파일마다 한 명의 소유자만 존재한다. ㉯ 유닉스/리눅스 시스템에서 파일은 그 파일의 소유자만 변경이 가능하다. ㉰ /etc/fstab, /etc/rc* 와 같은 파일은 root로 접근하고 변경할 수 있다. ㉱ SUID는 소유자 권한으로 프로그램을 실행할 수 있다. ㉲ umask는 시스템 파일이 만들어 질 때 퍼미션 기본값을 정하기 위해 사용된다.

① ㉮
② ㉯
③ ㉰
④ ㉱
⑤ ㉲

23. 다음 지문 중 서버관리자를 위한 보안 지침으로 옳지 않은 것은?

㉮ 관리자 그룹 사용자의 계정을 최소화한다. ㉯ 정기적으로 파일과 디렉토리의 퍼미션을 점검한다. ㉰ 관리자의 패스워드는 보안유지를 위해 주기적으로 변경한다. ㉱ 웹 서버에서 생성되는 프로세스는 관리자 권한으로 실행되도록 한다. ㉲ 중요한 파일들에 대해서는 주기적으로 백업을 받아둔다.

① ㉮
② ㉯
③ ㉰
④ ㉱
⑤ ㉲

25. 주기적으로 프로그램을 실행하기 위해 사용되는 cron데몬 설정파일의 각 필드에 대한 설명이다. 틀린 것은?

```
12  5  15-21  *  1  command
①  ②   ③    ④ ⑤
```

① 12분에 command가 실행됨.
② 5시에 command가 실행됨.
③ 15 ~ 21일에 command가 실행됨.
④ 매달 command가 실행됨.
⑤ 매주 일요일에 command가 실행됨.

28. 다음 설명에 해당되는 공격 유형은?

버그를 갖고 있는 System Program과 침입자의 Exploit Program이 거의 같은 시간대에 실행되어 System Program이 갖는 권한으로(Set-User ID가 붙은 경우 Root, Bin 등…) File에 대한 Access를 가능하게 하는 방법을 말한다.

① Hip Based Buffer Overflow
② Stack Based Buffer Overflow
③ Format String
④ Race Condition
⑤ Synchronization

29. 서비스 거부(DOS: Denial of Service) 공격은 공격자가 목표가 되는 시스템에 정상적 서비스를 하지 못하도록 목표 호스트를 무력화시키는 방법이라고 할 수 있다. 유닉스 시스템에서 내부 공격 방법으로 시스템 자원을 고갈시키는 DOS 공격의 결과로 볼 수 없는 것은?

① netstat 명령으로 관찰한 결과 다수의 SYN_RCVD 패킷이 존재한다.
② ps 명령으로 관찰한 결과 무수히 많은 수의 httpd 데몬이 실행 중이다.
③ df 명령으로 관찰한 결과가 아래와 같다.

```
Filesystem kbytes used avail capacity Mounted on
/dev/sda1 5447436 5085152 85568 98% /home/member
/dev/sda5 3099260 1192484 174934
```

④ 아래와 같은 C 프로그램이 실행 중이다.

```
void main() {
    char *c;
    while(1)
        c = malloc(10000);
}
```

⑤ ps 명령으로 관찰한 결과 몇 개의 높은 우선순위 프로세스의 누적 CPU 시간의 합계가 이들 프로세스의 실행 시작 이후의 전체 시간에 가깝다.

30. Windows는 기본적으로 여러 가지의 로그를 제공한다. 다음 중 보안에 관한 내용을 가장 많이 담고 있는 로그는?

① 파일 복제서비스 로그
② 시스템 로그
③ DNS 로그
④ 보안 로그
⑤ 응용 프로그램 로그

과 목	시스템보안	07년 1차

1. 프로세스는 상황과 조건에 따라 상태천이(State Transition)를 일으키는데 프로세스가 프로세서를 사용하여 실행할 준비가 되어 있는 준비(Ready)상태, 프로세스가 프로세서를 점유하여 실행되고 있는 실행(Run)상태 및 입출력 완료와 같이 어떤 사건이 발생하기를 기다리는 대기(Waiting)상태 등으로 나누어진다. 그러면 대기상태에서 실행상태로의 상태천이 과정을 무엇이라 하는가?

① 블록(Block)
② 디스패치(Dispatch)
③ 타이머 런아웃(Timer Runout)
④ 웨이크업(Wakeup)
⑤ 서스펜드(Suspend)

2. 프로그램의 논리적인 상대주소를 주기억장치의 물리적인 주소로 변환시켜 주는 것을 무엇이라 하는가?

① 페이징
② 세그멘테이션
③ 재배치
④ 링킹
⑤ 스와핑

3. 다음 중에서 파일 보호 방식에서 사용되는 기법이 아닌 것은?

① 접근 제어 리스트
② 접근 제어 행렬
③ 암호화(Encryption)
④ 파일의 명명법(Naming)
⑤ 파일 압축(Compression)

4. 다음 중 윈도우 운영체제에서 지원하는 네트워크 공유프로토콜인 CIFS(Common Internet File System)에 대한 설명으로 틀린 것은?

① OSI 7계층 프로토콜에서 Application/Presentation 계층에 속한다.
② 파일 공유 기능만을 제공한다.
③ 보통 TCP의 NetBIOS 프로토콜을 통해 전송된다
④ 클라이언트-서버 프로토콜이다
⑤ 공유 레벨과 사용자 레벨의 두 가지 보안 모델을 사용한다.

5. 다음 중 웹 서버에서 존재하지 않은 페이지를 요청하였을 경우 전송하는 반환 코드는?

① 200
② 304
③ 403
④ 404
⑤ 500

6. nmap 포트스캔 유틸리티의 명령어 옵션 중 방화벽을 우회하기 위하여, ping 패킷을 전송하지 않고 스캔하는 옵션은?

① -sU
② -po
③ -o
④ -p
⑤ -v

7. 윈도우즈 운영체제의 레지스트리 보안과 관련된 다음 설명 중 옳지 않은 것은?

① 실행 창에서 regedt32를 실행한 후 메뉴 중 보안을 선택하면 설정할 수 있다.
② 레지스트리를 주기적으로 백업받아야 한다.
③ 레지스트리에는 윈도우에서 컴퓨터에 관한 구성이 저장되어 있다.
④ 윈도우의 세부적 세팅을 가능하게 하기 위해 모든 사용자가 접근 가능하게 한다.
⑤ 레지스트리 키에도 사용권한을 설정할 수 있다.

8. 다음 지문에서 ( )에 들어갈 해킹기법은 무엇인가?

( )에 의한 해킹은 사용자의 키보드 입력을 가로채는 가장 악의적인 목적으로 많이 사용되는 트로이 목마 프로그램이다. 실제로 이 기능을 이용하여 타인의 계정과 패스워드를 알아내어 남의 통장에서 현금을 인출해 가는 사건도 발생하곤 한다. ( ) 프로그램이 동작되면 해당 컴퓨터에서의 모든 입력이 기록되므로 개인정보가 도용당할 수 있다. 대부분의 ( )프로그램은 트로이 목마 형태의 바이러스이기 때문에 바이러스 백신 프로그램을 설치하여 안전하게 개인 정보를 보호할 수 있다.

① 포트스캔
② 쿠키
③ DoS
④ 키로그
⑤ 히스토리

9. 다음 중 유닉스 시스템에서 TCP/IP 수퍼 데몬을 통해 제공되는 서비스의 환경을 설정하는 파일은 어느 것인가?

① /etc/smb.conf
② /etc/grub.conf
③ /etc/inetd.conf
④ /etc/resolv.conf
⑤ /var/named/named.conf

10. 다음 지문은 시스템 취약점을 점검하는 방법에 대한 설명이다. 옳지 않은 설명으로 짝지어진 것은?

(1) rc.boot, rc.local(SYSV : /etc/rc?.d/*)나 기타 시스템 시작 시 실행파일들을 점검한다. (2) inetd.conf 와 /etc/services 파일에서 침입자가 추가한 서비스가 있는지 점검한다. (3) TCP Wrapper 프로그램을 사용하여 원격으로 취약점 점검 작업을 수행한다. (4) pwunconv 명령을 사용하여 사용자 로그인 정보를 /etc/passwd 파일로 변환하여 관리한다. (5) 로그서버를 두어 모든 로그파일(pacct, wtmp, lastlog, sulog, syslog 등)들을 관리한다.

① (1), (3)
② (2), (3)
③ (2), (5)
④ (3), (4)
⑤ (4), (5)

11. 다음은 syslog에 의해 생성된 로그파일의 일부이다. 어떤 유형의 공격 로그인가?

```
Oct 19 17:21:02 qos1 sshd[5068]: User test not allowed because not listed in AllowUsers
Oct 19 17:21:02 qos1 sshd[5068]: input_userauth_request: illegal user test
Oct 19 17:21:04 qos1 sshd[5068]: Failed password for illegal user test from 211.239.[redacted] port 35951 ssh2
Oct 19 17:21:04 qos1 sshd[5068]: Received disconnect from 211.239.[redacted]: 11: Bye Bye
Oct 19 17:21:04 qos1 sshd[5069]: input_userauth_request: illegal user guest
Oct 19 17:21:07 qos1 sshd[5069]: Failed password for illegal user guest from 211.239.[redacted] port 35952 ssh2
Oct 19 17:21:07 qos1 sshd[5069]: Received disconnect from 211.239.[redacted]: 11: Bye Bye
```

① Brute Force 공격
② Buffer Overflow(버퍼 오버플로우) 공격
③ ColdFusion 취약점 공격
④ Format string(포멧 스트링) 공격
⑤ WebDAV 취약점 공격

12. 아파치 웹 서버에서 보통 httpd 로그는 /var/log/httpd/apache 디렉토리에 저장된다. 아래 보기는 HTTP에 대한 접근 로그 파일의 일부분이다. 설명으로 옳지 않은 것은?

```
172.16.0.1 -- [01/Jul/2002:13:09:46 -0700] "GET / HTTP / 1.0" 200 1879
172.16.0.1 -- [01/Jul/2002:13:09:46 -0700] "GET / HTTP / 1.0" 200 1879
172.16.0.1 -- [01/Jul/2002:13:09:46 -0700] "GET /mmback.gif HTTP / 1.0" 404 204
172.16.0.1 -- [01/Jul/2002:13:09:46 -0700] "GET /mmback.gif HTTP / 1.0" 404 204
172.16.0.1 -- [01/Jul/2002:13:09:46 -0700] "GET /head.gif HTTP / 1.0" 200 17446
172.16.0.1 -- [01/Jul/2002:13:09:46 -0700] "GET /head.gif HTTP / 1.0" 200 17446
```

① 누가, 언제, 어떻게 서버에 접속을 했는지에 대한 정보를 저장하는 access_log 파일이다.
② 172.16.0.1은 방문객의 IP 주소로 볼 수 있다.
③ 'GET / HTTP/1.0' 혹은 'POST /HTTP/1.0'은 클라이언트의 명령과 요구를 보여주고 있다.
④ 각 로그의 끝에서 두 번째 필드는 HTTP 상태코드로서 404는 클라이언트가 승인 없이 데이터 접근을 시도했다는 것을 보여주고 있다.
⑤ 각 로그의 마지막 필드는 전송된 데이터 파일의 크기를 나타낸다.

13. 침해당한 유닉스 시스템을 점검하는 방법 중 올바르지 않은 것은?

① 원하지 않은 프로세스가 없는지 "rpcinfo -p"를 이용하여 점검한다.
② cron과 at으로 수행되는 모든 파일을 검사한다.
③ passwd 및 su 명령이 SetUID 파일인지 조사한다.
④ /etc/inetd.conf와 /etc/services 파일에서 침입자가 추가한 불법 서비스 프로그램이 있는지 점검한다.
⑤ 로그 파일들을 통해 침입자의 침해 과정을 분석한다.

14. 다음 지문은 백업의 종류에 대한 설명이다. 잘못된 설명으로 짝지어진 것은?

(1) Day-zero Backup은 시스템 설치 후 시스템 사용 전에 모든 파일과 프로그램을 백업하는 것 (2) Full Backup은 일반적 기준에 의해 주기적으로 시스템 전체를 백업하는 것 (3) Incremental Backup은 Differential Backup보다 백업속도가 느리다. (4) Incremental Backup은 Differential Backup보다 복원속도가 빠르다. (5) Real-time Backup은 추가 데이터 발생 즉시 실시간으로 백업에 반영하는 것

① (1), (3)
② (2), (3)
③ (2), (5)
④ (3), (4)
⑤ (4), (5)

15. 시스템 해킹은 정보 시스템 운영체제의 결함으로 생기는 보안 허점을 활용하는데 일반적으로 시스템 해킹이 이루어지는 절차는 다음 지문에서 보는 것과 같다. 괄호 안에 들어갈 말로 순서대로 짝지어 진 것은 어느 것인가?

정보 시스템에 잠입 – ( ) – ( ) – 침입 흔적 삭제

① 백도어 설치, 관리자 권한 획득
② 관리자 시스템 추적, 백도어 설치
③ 핵심 시스템 탐지, 관리자 권한 획득
④ 관리자 권한 획득, 백도어 설치
⑤ 백도어 설치, 핵심 시스템 탐지

16. 다음 지문에서 설명하는 정보를 획득하기 위한 유닉스 명령어는 무엇인가?

① 시스템에서 수행 중인 PID 정보 ② 시스템에서 수행 중인 명령어의 TTY 정보 ③ 시스템에서 수행 중인 프로세스의 사용자 정보 ④ 시스템에서 로딩된 쉘 정보

① at
② cat
③ ps
④ find
⑤ cron

17. 다음 지문은 여러 가지 시스템에서 나타나는 보안 취약점들에 대한 설명이다. 아래 보기 중 윈도우 시스템에 대한 보안 취약점이 아닌 것으로 짝지어 진 것은?

(1) rsh, rlogin 등의 서비스는 시스템보안에 가장 취약한 약점을 가지고 있어서 최상의 보안을 요구하는 사이트는 이러한 서비스를 사용하지 않는다.
(2) IIS가 설치될 때 몇몇 ISAPI 확장들이 자동으로 설치됨으로써 ISAPI 확장 버퍼 오버플로우 취약점이 있다.
(3) SetUID가 설정되어 있는 실행 파일에 경쟁 조건을 발생시켜 관리자 권한을 획득할 수 있는 취약점이 존재한다.
(4) 공격자는 부적절한 유니코드 UTF-8 시퀀스를 포함한 URL을 IIS서버에 전송함으로써 디렉토리를 이동할 수 있고 임의의 스크립트까지 실행시킬 수 있다.
(5) 로컬 보안 권한 서브시스템 서비스(LSASS)의 버퍼 오버런 취약점을 이용하여 웜 바이러스의 침투 경로로 사용한다.

① (1), (3)
② (2), (3)
③ (2), (5)
④ (3), (4)
⑤ (4), (5)

18. 다음은PAM(Pluggable Authentication Modules)에 대한 설명이다. 틀린 것은?

① PAM은 응용프로그램들이 사용자를 인증하는 방법을 선택할 수 있도록 해주는 공유 라이브러리 묶음 임.
② mySQL은 PAM이 아닌 DB 자체의 인증 방식을 이용 함.
③ PAM은 통합 인증을 위해서만 이용 됨.
④ PAM 모듈의 설정파일은 /etc/pam.d/ 디렉토리에 있고 모듈 파일들은 /lib/security 디렉토리에 위치 함.
⑤ PAM을 사용하는 응용프로그램을 재컴파일 하지 않고도 인증 방법을 변경할 수 있음.

19. TCP Wrapper는 네트워크 접근제어 환경설정을 구성하는 프로그램이다. 사용 시 구성해야 할 설정환경 파일은?

① /etc/passwd
② /var/log/syslog
③ /etc/rc.d/init.d/lpd
④ /etc/hosts.allow, /etc/hosts.deny
⑤ /etc/tcpd.cf

20. 크래커들이 자주 사용하는 방법 중에는 한번 들어온 서버에 다시 쉽게 침입할 수 있도록 suid가 설정된 root 소유의 프로그램을 백도어로 설치하여 다음에도 손쉽게 root 권한을 획득할 수 있도록 하는 방법이 있다. 다음 지문의 명령어를 사용하여 시스템관리자는 주기적으로 suid로 설정된 파일을 모니터링하여 시스템을 안전하게 보호할 필요가 있다. 괄호 안에 필요한 퍼미션 값은 얼마인가?

```
#find / -user root -perm ( ) -exec ls -l { } ₩;
```

① 0755
② 0644
③ 1000
④ 2000
⑤ 4000

21. 침해사고 시 로그를 분석하여 비인가자의 접근내역과 수행한 작업 등 여러 가지 상황에 대한 파악을 할 수 있다. 다음과 같은 접근 내역의 내용을 보여주는 로그는?

```
SU 04/18 18:41 + ttypb guard-wkshin
SU 04/18 18:44 + ttypb guard-wjshin
SU 04/19 00:50 + ttyp2 chester-guard
SU 04/19 06:27 - ttyp1 hacker-root
SU 04/19 06:29 + ttyp1 hacker-root
```

① wtmp
② utmp
③ sulog
④ pacctcomm
⑤ lastlog

22. 서버관리자를 위한 보안 지침 중 옳지 않은 것은?

① 관리자 그룹 사용자의 계정을 최소화한다.
② 정기적으로 파일과 디렉토리의 퍼미션을 점검한다.
③ 관리자로 작업한 후에는 반드시 패스워드를 변경한다.
④ 웹 서버에서 생성되는 프로세스는 관리자 권한으로 실행되지 않도록 한다.
⑤ 중요한 파일들에 대해서는 주기적으로 백업을 받아둔다.

23. 유닉스 서버에서 로그 파일이 남는 디렉토리를 변경하려고 한다. 이를 위한 설정에 사용되는 파일은?

① /etc/inetd.conf
② /etc/syslog.conf
③ /var/log/messages
④ /var/log/syslog
⑤ /etc/hosts

24. ls 명령의 결과로 다음과 같이 표시되는 파일에 대한 설명으로 가장 부적절한 것은?

```
-rwxr-sr-x 2  root  sys  1024  Dec 4  10:20   /bin/sh
```

① 이 파일의 소유자는 root이다.
② 이 파일에는 SetGID 비트가 설정되어 있다.
③ 이 파일은 아무 사용자나 실행할 수 있다.
④ 이 파일은 아무 사용자나 수정할 수 있다.
⑤ 이 파일은 sys라는 그룹에 허용된 권한으로 실행된다.

25. 아래 지문이 설명하는 유닉스 데몬의 이름은 무엇인가?

시스템에서 일어나는 모든 상황들을 기록하는 데몬으로 외부 비인가자가 루트 권한을 획득한 후 제일 먼저 kill 시키는 행동을 할 만큼 시스템의 주요 사건들을 기록하는 데몬

① xinetd
② inetd
③ syslogd
④ lpd
⑤ rlogind

26. 다음 지문에서 설명하고 있는 공격방식을 무엇이라 하는가?

네트워크 패킷이나 버스를 통해 전달되는 중요한 정보를 엿보고 가로채는 공격행위로 암호화하지 않고 랜 라인을 통해서 전송되는 대화내용, 계정정보, 카드번호, 주민등록번호 등의 내용을 도청할 수 있는 방식의 공격

① 스니핑 공격
② 패킷 변조 공격
③ 서비스 거부 공격
④ 사회공학 공격
⑤ 스푸핑 공격

27. 다음은 리눅스/유닉스 시스템의 백업을 위한 방법들이다. 틀린 것은?

① tar 명령을 이용한다.
② dd 명령을 이용한다.
③ MD5를 이용한다.
④ Norton Ghost를 이용한다.
⑤ Encase를 이용한다.

28. 클라이언트가 웹서버에게 한 요청(request)에 대한 권한이 없을 때, 예를 들어 홈페이지 관리자의 IP만 접속이 가능한 웹페이지에 권한이 없는 사용자가 접속을 시도했을 경우, 웹서버는 어떤 에러 코드를 리턴 하는가?

① 400
② 403
③ 404
④ 500
⑤ 503

29. 해커들은 악성 파일 업로드 공격과 같은 웹 해킹을 통하여 시스템 내부에 쉘 명령을 내릴 수 있다. 시스템 관리자가 디렉토리에 권한을 적절하게 부여하면 웹 서버 권한(예 : nobody, daemon 등)으로 침입한 해커가 특정 디렉토리 내에 있는 파일 목록을 읽어볼 수 없게 할 수 있다. 다음 중 적절한 명령은 무엇인가?
(아래 조건을 참고해서 답하라)

[조건] - 홈페이지 운영에 지장이 없어야 한다. - 웹 서버 데몬이 특정 디렉토리 내의 파일을 읽는 데 문제가 없어야 한다.

① chmod 701 /home/testman/public_html/inc
② chmod 755 /home/testman/public_html/inc
③ chmod 700 /home/testman/public_html/inc
④ chmod 707 /home/testman/public_html/inc
⑤ chmod 777 /home/testman/public_html/inc

30. 침입당한 시스템은 공격자의 흔적을 감춰주는 다양한 루트킷, 트로이목마, 백도어 프로그램의 존재 가능성 때문에 모든 프로그램을 다시 설치하는 것이 좋다. 아래는 프로그램의 변조를 확인하는 방법이다. 옳지 못한 것은?

① 시스템 프로그램 파일 크기, Timestamp(생성시간, 변경시간 등)를 확인한다.
② Tripwire는 파일에 대한 기본 체크섬을 데이터베이스로 만들어 이를 통해 공격자들에 의한 파일변조 여부를 판별한다.
③ truss 또는 strace 명령을 이용하여 시스템 콜을 추적한다.
④ TCP Wrapper와 같은 파일 무결성 검사도구를 사용한다.
⑤ OS 벤더에서 제공하는 Checksum 값을 이용한다.

정 보 보 호 전 문 가 1 급 필 기

과 목	어플리케이션 보안	07년 2차

1. 다음 중 SQL Injection 공격에 대한 설명 중 맞는 것은?

① GET 방식과 POST 방식을 이용하여 위조된 쿠키를 통해 인증을 통과한다.
② 타겟 서버 데이터베이스의 테이블 이름과 칼럼 이름 등의 정보를 알고 있다면 UNION 문을 이용하면 좀 더 강력하게 데이터베이스를 직접 조작할 수 있는 공격을 가할 수가 있다.
③ 공격자가 데이터베이스 서버에 조작한 패킷을 교묘히 전송하는 공격이다.
④ DBMS 프로토콜의 구조적 취약점을 이용한 공격 기법으로 포트 스캐닝 등에 활용되는 공격 기법이다.
⑤ 웹서버에 SQL Injection 공격이 발생하였으면 200번대 로그를 중점적으로 확인해 보면 된다.

2. 아래는 스팸 메일의 헤더 부분이다. 이에 대한 설명으로 옳지 못한 것은?

```
Received: from gateway.sis.co.kr by sis.co.kr (8.9.2/8.8.8)  with SMTP id l16L44TQ007880
        for <test@sis.co.kr>; Wed, 7 Feb 2007 06:04:04 +0900 (KST)
Date: Wed, 7 Feb 2007 06:04:04 +0900 (KST)
Received: from unknown (HELO mail.polestar.uk) (222.112.171.101)
  by unknown with SMTP; 7 Feb 2007 06:06:06 +0900
X-RCPTTO: test@sis.co.kr
Received: from abc.kit.hot.com ([221.122.46.38]) by mail.polestar.jp with ESMTP id jp;
            Wed, 7 Feb 2007 06:27:19 +0900
Message-ID: <HNOXWHXMLCHEGHPRQUGQIK@DVQAT>
From: "왕궁타"<pe8exzwkqlj7yyg6xc6f@polestar.jp>
```

① mail.polestar.uk는 메일 서버가 설치되어 있는 경유 노드로 추정된다.
② 스패머가 abc.kit.hot.com라는 컴퓨터를 이용해 메일을 보낸 것으로 추정되고 이 정보는 위장할 수 없으므로 스패머를 밝히는데 중요한 정보가 된다.
③ test@sis.co.kr가 메일 수신자이다.
④ Message-ID는 최초에 메일을 발송한 컴퓨터에서 메일에 붙이는 고유번호로 때로는 유용한 정보를 줄 수 있다.
⑤ From 헤더는 변경 가능하므로 스패머를 밝히는 단서가 될 수 없다.

3. DB 관리자들은 특별한 연산을 수행하여야 하므로 데이터베이스 관리자 username은 보다 안전한 방법으로 인증되어야 한다. 따라서 운영체제에서 제공하는 인증 또는 네트워크 인증 서비스에 의한 인증 등을 사용한다. 다음 중 네트워크 인증 서비스의 하나인 Kerberos 에 대한 설명으로 틀린 것은?

① Kerberos에서 TGS(Ticket Granting Server)는 서버에 서비스 요청 시 사용할 서비스 승인 티켓을 발급한다.
② 전자서명을 지원하여 클라이언트가 다른 사용자로 사칭할 수 없다.
③ Kerberos Version 4에서는 암호화(encryption)와 인증(authentication) 작업을 위해서 DES를 사용했다.
④ Kerberos Version 5에서는 Kerberos Version 4에서 연속되어 사용되는 Session Key로 인한 Replay attack 공격을 방지하기 위해 단 1회에 한하여 사용되는 Subsession Key 가 사용되었다.
⑤ Kerberos 서버 자체의 보안 취약성으로 인해 Kerberos 서버가 침해되는 경우 네트워크 전체가 침해될 수 있다.

4. 다음 지문은 무엇에 대한 취약점을 설명한 것인가?

웹 서버는 동시에 많은 HTTP 요청을 취급한다. 사용자의 요구를 동시에 처리하기 위해서 사용하는 이 방식은 여러 개의 프로그램을 한 개의 데몬에서 처리하기 때문에 보안 취약성이 발생할 수 있다. 또 이 방식은 사용자가 서비스를 요청하는 경우에 메소드 영역에 프로그램 변수들을 저장한다. 이 때 두명의 사용자가 동시에 이 메소드 영역에 접근하려고 할 때 우선순위에 따라 먼저 도달한 사용자의 요청이 실행되나 거의 동시에 요청이 이루어지면 두 사용자를 한명의 사용자로 인식될 수 있다. 따라서 관리자와 동시에 인증을 요청하면 관리자의 페이지가 보여지는 현상이 발생한다.

① 프로세스 방식
② 쓰레드 방식
③ 트리거 방식
④ 데몬 방식
⑤ 동시성 방식

5. 전자메일에 대한 안전성을 확보하기 위해 제안된 시스템이 PGP이다. PGP는 기밀성, 인증 및 무결성, 부인방지 기능을 제공하기 위해 여러가지 알고리즘을 사용하고 있다. 아래 내용 중 PGP에서 적용한 방법 중에서 잘못 설명된 것은 ?

① 전자메일에 대한 기밀성을 제공하기 위해 IDEA 세션키로 메시지를 암호화하고 RSA 알고리즘을 사용하여 세션키를 암호화한다.
② 메시지에 대한 인증을 위해 MD5 알고리즘을 적용한다. ECC 알고리즘은 공개키 기반 암호알고리즘이다. 해쉬코드 생성을 위해서 사용하는 Message Digest 알고리즘으로 MD5를 사용한다.
③ 메시지의 양을 줄이기 위해 서명과정을 수행하기 이전에 메시지에 대한 ZIP 압축 알고리즘을 사용한다.
④ 메일 메시지에 대한 호환성을 제공하기 위해 옥텟 기반 전자메일 메시지를 ASCII 문자 형태로 변환하기 위해 BASE-64 기반 변환법을 적용한다.
⑤ 일반적으로 50,000 바이트 이상의 메시지에 대해서는 분할 과정을 수행하여 전송하고 수신자 시스템에서 재결합하는 기능을 제공하여 큰 메일 메시지도 보낼 수 있다.

6. 다음 중 트로이잔 목마를 이용한 공격에 관해 바르게 설명한 것은?

① 일반 사용자 컴퓨터에 악성 코드를 숨겨두고 악성 코드가 실행될 때 사용자 패스워드와 같은 정보를 수집한다.
② 지정된 버퍼의 크기보다 더 많은 Data를 받아들임으로써 프로그램이 비정상적으로 수행하거나 종료하도록 한다.
③ 메일 열람 시 HTML 기능이 있는 클라이언트나 웹 브라우저를 이용하는 사용자를 대상으로 한다.
④ 메일 프로그램이 메일 메시지를 처리할 때 내장된 쉘 명령어를 조작한다.
⑤ 공격자의 메일 발송 도메인주소를 실제 도메인 주소와 유사하게 만들어 피해자로 하여금 발송자의 이메일주소 구분이 어렵도록 하여 피해자를 속이는 방법이다.

9. 다음은 /etc/inetd.conf 파일의 tftp에 대한 설정이다. 설명 중 틀린 것은?

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot
```

① tftp는 udp 21번 포트를 사용한다.
② 보안상 tftp를 사용하지 않는다면 inetd.conf 파일에서 주석 처리를 권장한다.
③ -s옵션을 설정한 것은 chroot( ) 기능을 이용해 보안상의 문제를 해결하기 위해서이다.
④ tftp접속을 할 경우 /tftpboot 디렉토리만 접근이 가능하다.
⑤ xinetd를 사용하면 /etc/xinetd.d/tftp 파일을 삭제하거나 파일내의 disable 옵션을 "on"로 설정한다.

10. 다음 중 스팸 방지 기술과 관련이 없는 것은?

① SPF(Sender Policy Framework)
② RBL(Real-time Spam Black Lists)
③ PGP(Pretty Good Privacy)
④ Sender ID
⑤ Domain Key

11. 일반적인 FTP 서버가 사용자의 접근을 검사하는 절차들이다. 틀린 것은?

① /etc/shell에 등록되어 있지 않은 쉘(shell)을 이용하는 사용자이면 접근을 거부한다.
② 특정 IP에 대한 접속통제가 필요할 경우 host.allow와 host.deny를 이용한다.
③ 게스트 유저의 경우 /etc/passwd와 /etc/shadow에 ftp란 ID가 있는지만 보고 별도의 검사는 수행하지 않는다.
④ /etc/ftpusers에 사용자 ID가 들어 있으면 접근을 거부한다.
⑤ /etc/passwd, /etc/shadow에 사용자가 있는지 그리고 유효한지를 검사한다.

12. 아래의 지문은 무엇에 대한 설명인가?

메일의 From 헤더에 foo@spammer.com 라고 적혀있으면 spammer.com 을 관리하는 DNS를 통해서 해당 메일이 실제 spammer.com에서 설정한 IP와 수신된 메일헤더의 IP와 비교해서 다르면 수신을 거부하게 된다. 즉, 실제로 hanmail.net에서 보내지 않지 않았으면서 메일주소는 @hanmail.net 로 속여서 발송한 메일을 필터링할 수 있다.

① Procmail 을 통한 SPAM 필터링 기법
② Joe job attack 에 대한 설명
③ spamassassin 에 대한 설명
④ SPF(Sender Policy Framework) 에 대한 설명
⑤ RBL, SURBL(Spam URI Realtime Blocklist) 에 대한 설명

13. 다음 중 mail 서버 관리자가 할 수 있는 스팸 릴레이(spam relay) 차단 대책이 아닌 것은?

① sendmail에서 anti-spam 기능과 Access DB를 이용한 스팸 릴레이 차단
② sendmail.cf에서의 보안 설정
③ qmail에서의 스팸 릴레이 차단
④ MS Exchange에서의 기능 설정이나 레지스트리 설정을 통한 스팸 릴레이 차단
⑤ Outlook Express 메일 필터링을 통한 스팸 릴레이 차단

14. 검색엔진의 무분별한 검색을 사전에 방지하기 위해 "로봇 제한 기준 (standard for robot exclusion)"이라는 것이 만들어졌고 검색 엔진이 이를 따르도록 되어있다. 아래는 로봇을 허용 및 제한하는 "robots.txt" 파일이다. 잘못 설명된 것은?

```
㉮ User-Agent:*
   Disallow:/
㉯ User-Agent:*
   Disallow:/admin
㉰ User-Agent:Googlebot
   Disallow:/cgi-bin
```

① ㉮는 모든 로봇 Agent의 모든 웹페이지를 거부한다.
② ㉯는 "/admin" 디렉토리의 검색을 제한한다.
③ ㉰는 googlebot 만을 허용한다.
④ Robots.txt 설정은 강제성은 없다.
⑤ 검색 및 링크검색불가는 Robots.txt 이외에도 웹 페이지마다 메타 태그를 등록하는 방법도 있다.

15. 다음 지문은 OWASP TOP 10의 어떤 보안 취약점을 설명하는 것인가?

> 웹 요청 정보가 웹 어플리케이션에 의하여 처리되기 이전에 적절한 검증이 이루어지고 있지 않다. 공격자는 이 취약점을 이용하여 웹 어플리케이션의 백엔드 컴포넌트를 공격할 수 있다.

① 입력값 검증 부재
② XSS 취약점
③ 버퍼 오버플로우
④ 취약한 정보 저장 방식
⑤ 부적절한 환경설정

16. 다운로드를 위한 게시판의 파일을 이용하여 임의의 문자나 주요 파일명의 입력을 통해 웹 서버의 홈 디렉토리를 벗어나 시스템 내부의 다른 파일로 접근하여 다운로드하는 공격은?

① File Download
② CSS
③ SQL Injection
④ XSS
⑤ 쿠키/세션위조

17. 다음 중 PGP에 대한 설명으로 틀린 것은?

① 이메일 주소 등의 사용자 ID를 통하여 공개키를 얻을 수 있다.
② 키 서명 파티를 이용하여 사용자가 신뢰할 수 있는 웹을 확장할 수 있다.
③ RSA와 Diffie-Hellman 공개키 생성을 지원한다.
④ PGP 키 인증서 소유자만 자신의 PGP 키 인증서에 서명할 수 있다.
⑤ 인증과 기밀성을 제공하여 전자우편보안에 사용된다.

18. 다음 중에서 SQL 인젝션 공격에 대한 보호 대책으로 거리가 먼 것은?

① 사용자 입력이 SQL 문장으로 사용되지 않도록 한다.
② 사용자 입력으로 특수문자의 사용은 제한하도록 한다.
③ 원시 ODBC 오류를 사용자가 볼 수 없도록 코딩해야 한다.
④ DB 사용자의 권한을 제한한다.
⑤ 테이블 이름, SQL 구조 등이 외부 HTML에 포함되어 나타나도록 해야 한다.

19. mail 서비스를 구성하는 프로토콜 중 SMTP에 대한 설명으로 옳은 것은?

① 메일서버가 사용자를 위해 전자우편을 수신하는 프로토콜이다.
② MTA(Message Transfer Agent) 간의 직접 메일 전송과 전달 과정을 제어하는 프로토콜이다.
③ 메일을 안전하게 전송하기 위한 메시지 암호화를 처리하는 프로토콜이다.
④ 메일 열람 시 HTML 기능이 있는 E-mail 클라이언트 프로토콜이다.
⑤ MTA 상에서 동작하는 Spam 메일 차단 프로토콜로 RSA 공개키를 지원한다.

20. 다음 중 FTP 프로토콜에 대한 설명으로 틀린 것은?

① FTP 서버는 클라이언트가 지시한 곳으로 자료를 전송할 때 그 목적지가 '어떤 곳'인지 검사하지 않는다.
② FTP는 파일전송 프로토콜로 21번 포트를 사용한다.
③ 클라이언트는 FTP 서버를 거쳐 간접적으로 임의의 IP에 있는 임의의 포트에 접근할 수 있다.
④ FTP 프로토콜에서 파일을 다운로드 하는 명령은 DOWNLOAD이다.
⑤ FTP 프로토콜에서 파일을 업로드하는 명령은 PUT이다.

22. 다음은 DB보안 방법에 관한 내용이다. 틀린 것은?

① 데이터베이스에 허가된 사용자만이 접속하도록 통제해야 한다.
② 데이터베이스의 용량이 작은 경우 보안은 중요하지 않다.
③ 조직의 많은 사용자가 접근하는 대형 통합 데이터베이스 일수록 보안이 더욱 중요하다.
④ DBA는 접근하는 사용자의 권한을 적절히 부여해야 한다.
⑤ 중요한 데이터베이스인 경우 보안솔루션 적용을 검토할 수 있다.

23. Apache 웹서버 보안 설정 방법 중의 하나로 웹서버 설정파일인 httpd.conf 파일의 Directory 지시어내의 Indexes 옵션을 제거하여 DocumentRoot 디렉토리 내의모든 파일들의 열람을 방지하는 방법은?

① 서버의 정보표시 제한
② CGI 스크립트 실행 제한
③ SSI 실행 제한
④ HTTP 요청방식 제한 설정
⑤ 디렉토리 리스팅 제거

24. IETF에서 표준화하고 개발한 것으로 중앙 집중적으로 키 관리를 수행하는 이메일 보안 시스템은?

① PGP
② PEM
③ RPM
④ SET
⑤ TLS

25. 다음 지문의 로그파일을 보고 위험도를 옳게 설명한 것은?

```
[Wed Jan 11 14:32:53 2007] [alert] [client 127.0.0.1] client denied by server configuration: ...
```

① 시스템 사용이 불가인 긴급 상황
② 긴급 조치가 필요함
③ 에러상황
④ 경고사항
⑤ 정상이지만 중요한 사항

26. 비대칭키 암호 시스템에 대한 설명 중 틀린 것은?

① 암호화 키, 복호화 키가 구분된다.
② 소인수 분해 문제 등의 어려운 수학 문제를 응용한 알고리즘을 이용한다.
③ 키 관리가 용이하고 안전성이 뛰어나 다양한 응용에 활용된다.
④ DES가 비대칭키의 대표적인 암호화 알고리즘이다.
⑤ 전자서명에 응용된다.

27. 무선플랫폼에서 보안 기술을 제공하기 위해 제시된 기술 중에서 WAP 기반 클라이언트/서버 간의 인증을 제공하며 적합한 인증서를 발급, 운영 관리하는 등 무선망에서의 공개키 기반 구조를 의미하는 것은 무엇인가?

① WPKI
② WML
③ WTLS
④ WIPI
⑤ WiBro

28. 다음은 SET 프로토콜에 대한 내용이다. 카드매입사에서 이중 서명을 확인하는 과정에 대한 설명으로 틀린 것은?

고객은 상인에게 주문정보와 결제정보를 모두 전송한다. 그러나 상인은 결제정보를 확인할 수 없으며 변경할 수도 없다. 상인이 결제정보를 변경하지 않았고 고객이 보낸 데이터 원본임을 증명하기 위하여 이중서명을 하게 된다. 따라서 카드 매입사에서는 이중서명을 확인해 봄으로써 결제정보의 무결성을 확인하게 된다.

① 카드매입사는 결제정보와 이중서명을 전송 받는다.
② 카드매입사는 결제정보의 메시지 다이제스트를 구한다.
③ 카드매입사는 이중서명을 고객의 서명확인용 공개키로 풀어 고객이 보낸 메시지 다이제스트를 구한다.
④ 카드매입사는 주문정보의 메시지 다이제스트를 전송 받는다.
⑤ 카드매입사는 결제정보의 메시지 다이제스트와 고객이 보낸 메시지 다이제스트를 비교함으로써 서명을 확인한다.

29. 다음 중 SET 프로토콜의 단점으로 가장 거리가 먼 것은?

① 암호화 프로토콜이 복잡하다.
② RSA 동작은 프로토콜의 속도를 크게 저하시킴.
③ 카드 소지자에게 별도의 전자지갑 소프트웨어를 필요로 하지 않음.
④ 지불게이트웨이에 거래를 전자적으로 처리하기 위한 별도의 하드웨어와 소프트웨어를 요구함.
⑤ 상점에 소프트웨어를 요구함.

30. 네트워크형 전자지불 시스템만으로 바르게 나타낸 것은?

① Ecash, NetCash
② PC Pay, NetCash
③ Mondex, VisaCash
④ DigiCash PC Pay
⑤ PC Pay, NetCash

31. 다음 중 OCSP(Online Certificate Status Protocol)에 대한 설명으로 옳은 것은?

① PKI에서 사용하는 표준 인증서 프로토콜로 VeriSign, RSA와 같은 외부 CA (Certificate Authority) 기관에서 승인과정을 거친다.
② 고객과 서버 및 CA로 구성되어 인증서 상태에 대한 검색 등의 기능을 제공하기 위해 개발된 프로토콜이다.
③ 인터넷 상에서 파일 및 메일 전송 등에 사용되는 암호화 프로토콜이다.
④ Phillip Zimmermann이 만든 프로토콜로 각 사용자들이 자신의 전자 인증을 서명하는 방식으로 인증 받는 online 인증 프로토콜이다.
⑤ SSL/TLS 다음 버전의 인터넷 보안 프로토콜이다.

32. 다음 중 전자지불시스템에 관한 설명으로 틀린 것은?

① 전자지불시스템은 완전한 전자상거래 시스템을 구현하기 위한 필수적인 기술이다.
② 네트워크형 전자화폐시스템은 스마트카드와 같은 하드웨어를 필요로 하지 않는 이점이 있다.
③ 다양한 전자상거래 객체간의 통신을 SSL로 보호하는 것만으로는 전자지불의 다양한 보안요구사항을 만족시키기 어렵다.
④ 전자화폐의 보안요구사항 중에서 불연계성이란 동일 사용자의 지불내용을 연결시킬 수 없어야 한다는 것을 말한다.
⑤ K-Cash 시스템은 한국형 전자화폐시스템으로서 은닉서명 기법을 이용한 Ecash 시스템을 발전시켜서 표준화한 것이다.

33. XML 디지털 서명 표준에서 XML 서명 결과를 나타내는 <Signature> 원소 안에 XML 서명 대상 데이터를 포함할 수 있다. 이 때 사용되는 XML 원소는 무엇인가?

① <SignedData>
② <EnvelopedData>
③ <Object>
④ <Reference>
⑤ <SignInfo>

34. 다음 지문의 내용이 설명하는 것은?

◦ 일종의 비밀 채널로 지적 재산권을 보호하기 위한 수단으로 사용 ◦ 파일 내부에 비밀 정보를 삽입시켜 합법적인 소유자를 확인할 수 있게 함 ◦ 그래픽, 오디오, 컴퓨터 프로그램 등 다양한 분야에 응용

① 워터 마크
② 암호화
③ 전자 서명
④ 저작권
⑤ 해시 알고리즘

35. 다음은 SSL handshake 과정이다. 순서를 올바르게 나열한 것은?

㉮ 클라이언트는 Premaster secret 정보를 서버의 공개키로 암호화하여 전송한다. ㉯ 서버는 premaster secret 정보를 이용하여 master secret 을 생성하고, 세션키를 생성한다. ㉰ 클라이언트는 생성된 세션키를 이용하여 암호통신 수행을 서버에게 알리고 SSL handshake 프로토콜을 완료한다. ㉱ 클라이언트의 SSL 버전번호, 암호세팅, 랜덤데이터, 기타정보를 서버에게 전송한다. ㉲ 서버의 SSL 버전번호, 암호세팅, 랜덤데이터, 기타정보, 서버인증서를 클라이언트에게 전송한다. ㉳ 서버는 생성된 세션키를 이용하여 암호통신 수행을 클라이언트에게 알리고 SSL handshake 프로토콜을 완료한다.

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

36. 다음 중 전자 입찰 프로토콜에 대한 설명으로 틀린 것은?

① 실세계의 입찰 모델을 네트워크로 적용하여 구현하는 프로토콜이다.
② 아무도 입찰 결과를 변조할 수 없으며, 일정 시한까지 입찰 내용의 비밀성이 보장되어야 한다.
③ 부정 입찰자의 방해에 강인성을 제공해야 한다.
④ 입찰 내용의 부인이 불가능해야 한다.
⑤ 입찰 기간이 만료된 후에도 그 내용이 공개되어서는 안 된다.

37. XML 기반 보안 기술이 아닌 것은?

① XPKI
② SAML
③ XKMS
④ XACML
⑤ XML Signature

38. 다음 중 전자상거래 보안 프로토콜 SSL에 대한 설명으로 맞는 것은?

① 응용계층의 프로토콜이다.
② transport mode와 tunnel mode 2가지 방식이 있다.
③ 110번 포트를 사용한다.
④ record 계층에서는 메시지 캡슐화를 수행한다.
⑤ ssl을 통해 웹서버에 접근하려면 브라우저 외에 별도의 클라이언트 프로그램이 설치되어야 한다.

39. 전자화폐의 안전성을 제공하기 위해 요구되는 기능 중에서 이중지불(double spending)을 방지할 수 있는 기능에 해당하는 것은?

① 익명성
② 양도성
③ 분할성
④ 오프라인성
⑤ 익명성 취소 기능

40. ebXML의 구성요소가 아닌 것은?

① 비즈니스 프로세스
② EDI 문서
③ 핵심컴포넌트
④ 등록저장소
⑤ 전송, 교환 및 패키징

41. 다음 중 프로그래머의 관점에서 버퍼 오버플로우 공격에 취약하지 않도록 사용 자제를 권고하는 함수는 무엇인가?

① sprintf( )
② strncpy( )
③ vfscanf( )
④ fgets( )
⑤ strncat( )

42. 다음 중 포맷 스트링에 대한 설명으로 틀린 것은?

① printf(str)와 같은 코드에서 printf가 “str”을 포맷 스트링으로 인식하고 연산을 수행하는데, 이 때 존재하는 취약점을 포맷 스트링 버그라 한다.
② 포맷 스트링 취약점을 이용하여 프로그램 파괴, 프로세스 메모리 보기 등을 할 수 있다.
③ ltarce, strace 등과 같은 포맷 스트링 취약점 점검 도구들을 사용하여 취약점을 점검할 수 있다.
④ 포맷 스트링 취약점을 이용하여 스택에 할당된 메모리 버퍼 크기를 초과하는 코드를 기록하고 저장된 복귀 주소를 변경하여 임의의 코드를 실행 시킬 수 있다.
⑤ 포맷 스트링 버그를 이용하여 임의의 메모리 덮어쓰기 프로세스의 명령 포인터의 통제권을 장악할 수 있다.

43. TLS에 대한 설명으로 틀린 것은?

① 웹 보안에 사용된다.
② RSA 암호화 값은 PKCS#1 block type 2에 의해 암호화 된다.
③ RSA, DSS 등을 이용한 전자서명 기능을 제공한다.
④ Public key ring의 Owner_trust, Key_legitimacy, Signature, Signature_trust 등을 이용하는 인증 방식을 사용한다.
⑤ TLS는 레코드 프로토콜과 핸드쉐이크 프로토콜로 구성된다.

45. 무선 PKI (Public Key Infrastructure)에 대한 설명으로 올바른 것은?

① 보안을 강화하기 위해 인증서 검증 메커니즘의 복잡도를 높여야 한다.
② 무선 PKI는 유선 환경을 고려하지 않고 무선 환경에 적합하도록 새로운 기능으로 만든 것이기 때문에 차후 유선 환경과의 통합 절차가 필요하다.
③ WAP(Wireless Application Protocol)에서는 WTLS(Wireless Transport Layer Security) 인증서의 사용을 권고하고 있다.
④ 핸드오버 시 인증서 획득시간이 매우 짧기 때문에, 이 시간을 이용하여 인증서 검증 시간을 늘림으로써 보안을 강화할 수 있다.
⑤ 무선 단말기에서는 RSA를 이용한 키 생성이 용이하다.

46. 다음에서 설명하는 DRM기술은 무엇인가?

불법으로 유통되는 복사본들을 감시하거나 추적할 때 유용한 방법으로 제품마다 서로 다른 유일한 코드를 부여하여 구매자의 정보를 표시한다. 따라서 구매자가 불법적으로 컨텐츠를 분배하는 것을 방지할 수 있다.

① 디지털 워터마킹
② 핑거프린팅
③ INDECS
④ DOI(Digital Object Identifier)
⑤ URI

47. 다음 중 EAM (Extranet Access Management : 통합 인증 및 접근제어 관리 기술)에 관한 설명으로 적절하지 않은 것은?

① 단일 로그인을 제공한다.
② 로그인 세션의 보안기술 적용을 통해 Replay Attack 또는 네트워크상의 위변조를 방지해준다.
③ ERP(Enterprise Resource Planning)의 또 다른 명칭이다.
④ PKI와 연동하여 암호화 및 전자서명 지원이 가능하다.
⑤ 기대 효과로는, 기업자원과 정보에 대한 단일화 된 인터페이스 접근 가능, 개별화 (personalization) 기능 등이 존재한다.

49. 마이크로 칩을 내장한 태그, 라벨, 카드 등에 저장된 데이터를 무선 주파수를 이용하여 자동 인식하는 기술은 무엇인가?

① IDEA
② RFID
③ EDI
④ SAML
⑤ DRM

과 목	어플리케이션 보안	07년 1차

1. 네트워크를 통해 결제하는 수단인 사이버머니가 갖추어야 할 속성이 아닌 것은?

① 복제를 방지할 수 있어야 한다.
② 사용자의 신원이 드러나지 않도록 익명성이 보장되어야 한다.
③ 한번 사용한 돈을 동일한 사람이 또 다시 사용할 수 없도록 해야 한다.
④ 다른 사람에게서 받은 돈을 또 다른 사람에게 지불할 때 사용할 수 있어야 한다.
⑤ 여러 차례 걸쳐서 지불된 돈이 동일한 사람한테서 나왔는지 알 수 있어야 한다.

2. 다음 중에서 웹 서버 운영의 보안 사항이 아닌 것은?

① 파일 무결성 점검 도구 사용
② 새로운 보안 취약점에 대한 주기적인 모니터링
③ 웹 서버 설정 파일 제거
④ 주기적인 로그 점검 및 백업
⑤ 안전한 동적 콘텐츠의 사용

3. 다음 중 웹 서버를 설치할 때 보안관련 조치 사항과 거리가 먼 것은?

① 소스코드 형태의 배포본 설치
② 설치시 네트워크 접속 차단
③ 로그파일의 보호
④ 웹 서비스 영역과 시스템영역의 통합
⑤ 자동 디렉터리 리스팅 제거

4. 다음 중 IIS에서 웹 사이트의 허가를 얻기 위해 선택할 수 있는 인증 방법만 열거한 것은?

① 다이제스트 인증, 서버인증, 클라이언트 인증
② 폼 기반 인증, 서버인증, 클라이언트 인증
③ 기본 인증, 다이제스트 인증, 윈도우즈 통합 인증
④ 서버인증, 윈도우즈 통합 인증, 클라이언트 인증
⑤ 기본 인증, 다이제스트인증, 폼 기반 인증

5. 다음 중에서 SQL 인젝션 공격에 대한 보호 대책으로 거리가 먼 것은?

① 사용자 입력이 직접 SQL 문장으로 사용되지 않도록 한다.
② 사용자 입력으로 문자, 기호문자 그리고 구두문자까지만 사용하도록 한다.
③ SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정한다.
④ DB 사용자의 권한을 제한한다.
⑤ 모든 스크립트에 대한 모든 파라미터를 점검하여 사용자 입력 값이 공격에 사용되지 않도록 한다.

6. 전자화폐에 사용되는 은닉서명(blind signature)은 사용자가 서명자로부터 전자서명을 얻기 위한 프로토콜이다. 이에 대한 설명으로 적합하지 않은 것은?

① 서명자는 자신이 어떠한 메시지에 대해 서명하는지 알 수 없다.
② 언제든지 불법 사용자에 대한 추적 기능을 제공한다.
③ 제3자는 사용자가 유효한 서명을 얻었음을 확인할 수 있다.
④ 일반적으로 전자화폐 발행 은행이 은닉 서명을 수행한다.
⑤ 디지털 봉투 개념을 실현한 것으로 전자화폐에 필수적으로 적용되는 전자서명 알고리즘이다.

7. VISA와 Master Card가 신용카드를 기반으로 한 인터넷 상의 전자결제를 안전하게 수행할 수 있도록 마련한 전자결제 과정 표준안은 다음 중 어느 것인가?

① SSL
② TLS
③ SEED
④ SET
⑤ SNMP

8. 전자입찰에 대해 잘못 설명한 것은?

① 입찰 단계에서 입찰 내용의 비밀이 보장되어야 한다.
② 입찰자와 입찰공고자와의 공모에 의한 위협은 없는지 고려해야 한다.
③ 여러 개의 입찰 서버가 있을 경우 동시에 입찰을 마감하여야 한다.
④ 부정한 사용자의 입찰 개입을 방지할 수 있어야 한다.
⑤ 낙찰자 보호를 위해 낙찰자의 신원과 낙찰 가격은 비공개가 원칙이다.

9. 아래에 기술된 내용은 무엇에 관한 설명인가?

- CA(인증기관)은 인증 정책 수립, 인증서 및 인증서 취소 목록을 관리한다. - 인증서는 버전, 일련 번호, 유효 기간, 식별자 등을 포함한다. - 인증서 취소 목록은 서명 알고리즘, 발급자, 폐지 인증서 목록을 포함한다. - 인증서의 형식은 X.509이다. - 계층적 구성 또는 네트워크 구성 형태를 이루고 있다.

① PKI
② DNS
③ WML
④ EDI
⑤ SMS

10. 전자상거래 보안 기술 중 아래에서 설명하는 보안기술은 무엇인가?

- 세션 계층에 적용되며 FTP, TELNET, HTTP, MAIL 등의 프로토콜에 안전성을 제공할 수 있다. - 보안기술을 적용하면 http://* 대신에 https://* 를 사용해야 한다. - Handshake Layer에서는 암호화 알고리즘을 선택하고 암호화 키를 계산한다. - Record Layer에서는 메시지 캡슐화를 수행한다.

① S-HTTP
② ebXML
③ SSL
④ SET
⑤ WPKI

11. PKI 운영 프로토콜 중 인증서 및 CRL 보관소에 저장되어 있는 PKI 정보를 추가, 삭제, 변경하는 절차를 규정하고, 보관소 읽기, 보관소 탐색 및 보관소 내용의 변경 등의 역할을 수행하는 프로토콜은?

① SET
② LDAP
③ RADIUS
④ X.509
⑤ OCSP

12. 아래는 스팸 메일의 헤더 부분이다. 이에 대한 설명으로 옳지 못한 것은?

```
Received: from gateway.sis.co.kr by sis.co.kr (8.9.2/8.8.8)  with SMTP id I16L44TQ007880
        for <test@sis.co.kr>; Wed, 7 Feb 2007 06:04:04 +0900 (KST)
Date: Wed, 7 Feb 2007 06:04:04 +0900 (KST)
Received: from unknown (HELO mail.polestar.jp) (221.112.171.101)
  by unknown with SMTP; 7 Feb 2007 06:06:06 +0900
X-RCPTTO: test@sis.co.kr
Received: from jfb.lxl.haxim.com ([222.122.46.38]) by mail.polestar.jp with ESMTP id jp;
          Wed, 7 Feb 2007 06:27:19 +0900
Message-ID: <HNOXWHXMLCHEGHPRQUGQIK@DVQAT>
From: "왕궁타"<pe8exzwkqlj7yyg6xc6f@polestar.jp>
```

① mail.polestar.jp는 메일 서버가 설치되어 있는 경유 노드로 추정된다.
② 스패머가 jfb.lxl.haxim.com라는 컴퓨터를 이용해 메일을 보낸 것으로 추정할 수 있지만 이 정보는 위장되었을 수도 있다.
③ test@sis.co.kr가 메일 수신자이다.
④ Message-ID는 최초에 메일을 발송한 컴퓨터에서 메일에 붙이는 고유번호로 때로는 유용한 정보를 줄 수 있다.
⑤ From 헤더는 변경할 수 없으므로 스패머를 밝히는 중요한 단서가 된다.

13. 다음 중 SQL Injection 공격에 대한 설명 중 틀린 것은?

① 아이디와 비밀번호 입력란에 ‘ or ’1 ‘=' 1 을 입력하여 아이디/패스워드 인증공격을 시도할 수 있다.
② 만일, 타겟 서버 데이터베이스의 테이블 이름과 칼럼 이름 등의 정보를 알고 있다면, UNION 문을 이용하면 좀 더 강력하게 데이터베이스를 직접 조작할 수 있는 공격을 가할 수가 있다.
③ 알아내고자 하는 정보의 답변을 미리 대략적으로 예측해서 그것이 참인지 거짓인지를 질의하고, 서버의 반응으로 참/거짓 여부를 판단하면서 참이 될 때까지 시도함으로서 정보를 알아내는 방법을 블라인드 인젝션이라 한다.
④ 인젝션 공격 실패 시 SQL query 에러 메세지가 출력되면, 더 많은 정보를 얻기 위해서 고의적으로 에러를 발생시키고 에러 메시지를 분석하는 방법도 시도할 수 있다.
⑤ 웹서버에 SQL Injection 공격이 발생하였으면 200번대 로그를 중점적으로 확인해 보면 된다.

14. 아래의 지문은 xferlog의 내용이다. 다음 중 틀린 설명은?

```
Thu Oct 13 14:11:30 2005 18 220.74.193.24 61175472 /home/user/test.txt b _ci r user
ftp 0 * c
```

① 파일 전송 대상 원격 호스트의 주소가 220.74.193.24이다.
② 파일전송에 18초가 소요 되었다.
③ 파일 전송 시 오류가 발생하였다.
④ 220.74.193.24에서 서버로 test.txt 파일을 업로드 하였다.
⑤ 로그온 한 id는 user 이다.

15. MS-SQL 서버 구축 시 DB 보안을 위해 고려하여야 하는 작업들이 있다. 다음 중 가장 부적절한 것은?

① MS-SQL 보안을 위해 수시로 최신 서비스 팩과 보안 패치를 설치하고, 정기적으로 모든 데이터를 백업, 복사본을 조직 외부의 안전한 위치에 보관한다.
② 관리자 기능을 최소화하고 sysadmin 역할의 구성원만 xp_cmdshell을 실행할 수 있도록 설정한다.
③ 외부에서도 원활한 원격 DB 사용을 지원하기 위해 guest 계정을 제공한다.
④ SQL Injection 공격을 방어하기 위해 데이터베이스 내장 프로시저를 사용하여 DB 어플리케이션을 개발한다.
⑤ 가급적 SQL Server 계정에 복잡한 암호를 사용하도록 권장한다.

16. 다음 중 FTP 바운스 공격을 이용해 전자 메일을 보내 송신자를 알 수 없는 메일의 성격을 가지는 공격을 무엇이라 하는가?

① Fack 메일
② Spam 메일
③ 광고 메일
④ Anonymous 메일
⑤ Bounce 메일

17. mail 서비스를 구성하는 프로토콜 중 MTA(Message Transfer Agent) 간의 직접 메일 전송과 전달 과정을 제어하는 것은 다음 중 어느 것인가?

① MAP
② SMTP
③ POP
④ sendmail
⑤ MIME

18. 다음 중 데이터베이스 보안 요구사항이 아닌 것은?

① 부적절한 접근 방지
② 추론 방지
③ 데이터 무결성
④ 사용자 인증
⑤ 대칭키 암호 알고리즘 적용

19. 전자 우편 보안을 위해 PGP와 S/MIME이 널리 사용되고 있다. 아래 설명 중 틀린 것은?

① PGP의 초창기 버전들은 필 짐머맨이 독자적으로 개발한 것으로 공개키 암호화 방식을 지원한다.
② S/MIME은 MIME 기능에 RSA 기반 보안 기능을 추가한 프로토콜이다.
③ S/MIME은 X.509 Ver.3 형식의 사용자 인증서를 지원한다.
④ PGP는 IETF에서 표준화하고 개발한 것으로 중앙 집중적으로 키관리를 수행한다.
⑤ PGP는 키 링과 키 식별자를 이용한 키 관리 기법을 제공한다.

20. FTP 공격중 Bounce Attack 공격에 대한 설명 중 틀린 것은?

① 익명 FTP 서버를 이용해 그 FTP 서버를 경유해서 호스트를 스캔하는 공격
② FTP PORT 명령어를 이용한다.
③ 익명 사용자가 서버에 쓰기 권한이 있을 때 악성 코드를 생성하여 공격
④ 네트워크에서의 포트 스캐닝 방식으로 사용한다.
⑤ FTP 서버를 통해 임의의 네트워크 접속을 릴레이하면서 작동하는 공격

21. 전자우편은 많은 보안상의 취약점을 가지고 있다. 이에 전자우편의 보안성을 향상시키기 위한 보안도구나 표준들이 제시되었다. 다음 중 전자우편의 보안성을 향상시키기 위한 보안도구나 표준들로 짝지어진 것은?

(1) PEM (2) RSA (3) DES (4) S/MIME (5) PGP

① (1), (2), (3)
② (2), (3), (5)
③ (1), (4), (5)
④ (2), (4), (5)
⑤ (3), (4), (5)

22. 웹서비스용 포트 80에 대한 공격이 다수 탐지되고 있다. 다음 중 웹 서비스에 대한 공격 형태에 대하여 잘못 설명한 것은?

① 웹 어플리케이션의 취약점을 이용한 공격에는 SQL Injection, LDAP Injection, HTML Injection, PHP Injection 등이 있다.
② CGI 스크립트를 어느 디렉토리에서나 실행할 수 있도록 할 경우 악의적인 사용자가 CGI 프로그램을 업로드하여 실행해서 임의의 명령을 실행시킬 수 있다.
③ 클라이언트에 전달된 쿠키값들을 분석하여 공격하는 기법이 쿠키/세션위조 공격으로서 대표적인 공격이 codered공격이다.
④ 조작된 SQL 질의문을 통해서 공격자가 원하는 SQL구문을 실행시키는 공격기법은 SQL injection이라고 한다.
⑤ 게시판 소스 코드 중 include문을 이용하여 passthru나 system과 같이 원격에서 명령 실행이 가능한 함수를 추가하여 원격지에서 명령을 실행할 수 있다.

23. 다음의 보기 중 FTP(File Transfer Protocol) 및 TFTP(Trivial File Transfer Protocol)에 대한 설명으로 틀린 것은?

① 정상적인 서비스 Connection을 위해 1개의 포트만을 사용한다.
② 클라이언트에서 FTP모드를 Active 또는 Passive모드로 전환할 수 있다.
③ TFTP는 기본적으로 UDP 69번 포트를 사용한다.
④ /etc/ftpusers에 사용자 ID를 등록하여 접근을 제한할 수 있다.
⑤ TFTP는 FTP와 비슷한 역할을 하지만 인증과정을 거치지 않고 바로 원격 파일을 읽거나 저장할 수 있는 프로토콜이다.

24. 안전한 DNS 서비스를 위하여 설명한 아래의 보기 중 바르게 설명하고 있는 것은?

① DNS Dynamic Updates를 방지하기 위해서 URL을 이용하여 사용을 제한한다.
② DNS Spoofing을 방지하기 위하여 Nonrecursive Server의 설정을 해지한다.
③ DNS서비스 상의 취약점을 진단할 수 있는 방법은 없다.
④ 내부 및 외부를 위한 Split DNS를 구성하면 DNS 서비스의 안전에 치명적이다.
⑤ Zone Transfer, Dynamic Updates 등과 같은 DNS 취약점에 대응하기 위하여 named.conf 파일의 설정값을 변경 적용한다.

25. 다음의 보기는 XML기반의 보안 기술을 나열한 것이다. 해당되지 않는 것은?

① XML 전자서명
② XML Encryption
③ XKMS (XML Key Management Specification)
④ SAML(Security Assertion Markup Language)
⑤ SGML (Standard Generalized Markup Language)

26. 아래의 무선 콘텐츠 지불 서비스에 대한 설명으로 가장 거리가 먼 것은?

① End-to-End 간의 Transaction 안전성 보장을 위하여 S-HTTP, SSL, TLS 등의 보안 프로토콜이 존재한다.
② 전자상거래 지불 시 안전성 보장을 위한 SET, InstaBuy 등이 존재하며 InstaBuy는 기존 사이버지갑(Cyberwallet)을 개선한 것이다.
③ 전자수표 기반 전자지불 시스템은 실 세계의 수표와 유사한 형태로 전자서명과 같은 암호화 기술을 사용함으로써 배서 등의 효과를 제공한다.
④ 전자수표기반 전자지불 시스템으로는 Millicent, NetBill 등이 대표적이다.
⑤ 가치저장형 프로토콜로는 Mondex, VisaCash, Proton 등이 있다.

27. 전자 입찰시스템에서 필요한 5가지 보안 요구사항과 가장 거리가 먼 것은?

① 독립성
② 효과성
③ 비밀성
④ 무결성
⑤ 안전성

28. 다음 중 전자화폐 프로토콜/시스템이 아닌 것들로만 이루어진 것은?

① SET, SSL
② PGP, 몬덱스
③ 넷캐쉬, e-캐쉬
④ VISA, 밀리센트
⑤ 몬덱스, SET

29. 고객과 서버 및 CA로 구성되어 인증서 상태에 대한 검색 등의 기능을 제공하기 위해 개발된 프로토콜은 무엇인가?

① SET
② LDAP
③ RADIUS
④ X.509
⑤ OCSP

30. 전자투표 시스템이 갖추어야 하는 기능에 대해 잘못 제시된 것은?

① 완전성 - 모든 투표가 정확하게 집계되어야 한다.
② 익명성 - 투표결과로부터 투표자를 구별할 수 없어야 한다.
③ 건전성 - 부정한 투표자에 의해 선거가 방해되는 일이 없어야 한다.
④ 이중투표방지 - 정당한 투표자가 두 번 이상 투표할 수 없어야 한다.
⑤ 제한적 검증기능 - 선거 결과에 대해 일부 권한이 부여된 자에 의해서만 투표결과를 확인할 수 있어야 한다.

31. 동일한 메시지를 인터넷상의 서로 상관없는 여러 뉴스그룹에 올리는 행위를 무엇이라 하는가?

① 폭탄메일(Mailbombing)
② 스푸핑(Spoofing)
③ 훔쳐보기(Shoulder surfing)
④ 스패밍(Spamming)
⑤ 하이재킹(Hijacking)

32. 보안 도구에 대한 설명 중 아래의 괄호 안의 내용이 설명하는 것은?
(전자우편 메시지에 보안 기능을 적용하는 것으로 전자우편 보안에 활용)

① SSL (Secure Socket Layer)
② S-HTTP (Secure HTTP)
③ IPsec (IP Security)
④ PGP (Pretty Good Privacy)
⑤ IDS (Intrusion Detection System)

33. 다음 중 XSS(Cross Site Scripting) 기술에 대한 설명으로 옳은 것은?

① 루트권한과 관련된 프로그램에 예상치 못한 입력값을 보내 해당 프로그램의 오류를 유발하여 원하는 정보를 빼가는 공격 기법
② 게시판의 글에 원본과 함께 악성 코드를 삽입하여 글을 읽는 순간 악성 코드가 실행되어 클라이언트의 정보를 유출하는 클라이언트 공격 기법
③ GET, POST 방식을 이용하여 위조된 쿠키를 이용하여 클라이언트 정보를 유출하는 클라이언트 공격 기법
④ 공격자가 게시판의 입력값을 조작하여 오류를 발생시킨 후, SQK 구문을 확인하는 공격 기법
⑤ 게시판 소스 코드 중 include문을 이용하여 passthru나 system과 같이 원격에서 실행 가능한 함수를 추가하여 원격지에서 명령을 실행하는 공격 기법

34. 다음 중 OWASP TOP 10에 속하지 않는 것은?

① 입력 값 검증 부재
② XSS 취약점
③ 부적절한 에러 처리
④ 서비스 방해 공격
⑤ 트로이 목마 공격

35. XML과 HTTP 통신을 기반으로 네트워크상에 존재하는 각종 시스템간의 호출을 효율적으로 실현하기 위한 방법으로 제시된 통신규약은?

① UDDI
② WASP
③ SOAP
④ WSDL
⑤ XACML

36. HTTP 쿠키에 관한 설명으로 올바른 것은?

① Set-Cookie 헤더에 키워드 secure를 표시하는 것은 쿠키 전송에 SSL을 사용하기 위해서다.
② 보안이 취약한 클라이언트에서 실행될 때, 사용자가 원하지 않는 작업이 수행될 수 있다.
③ 쿠키의 사용으로 인해 프라이버시의 침해나 특정 사이트에 대한 보안을 완벽하게 유지 할 수 있다.
④ 넷스케이프 커뮤니케이터나 인터넷 익스플로러 등의 브라우저에서는 쿠키 차단 옵션이 없다.
⑤ 쿠키를 제공한 서버는 쿠키의 유효 기간을 지정할 수도 있으나 삭제를 지시할 수는 없다.

37. 다음의 보기 중 FTP(File Transfer Protocol)의 기본적인 명령으로 허용되어 있지 않은 명령어는?

① Rename
② Send
③ Status
④ Exit
⑤ Prompt

38. 다음 괄호에 들어갈 내용의 순서가 올바른 것은?

( )은 기존 전자우편 보안시스템의 문제점인 ( ) 구현의 복잡성, ( )의 낮은 보안성과 기존 시스템과의 통합이 용이하지 않다는 점을 보완하기 위해 IETF의 작업그룹에서 RSADSI(RSA Data Security Incorporation)의 기술을 기반으로 개발된 전자우편 보안이다.

① S/MIME, PEM, PGP
② PGP, PEM, S/MIME
③ S/MIME, PGP, PEM
④ PGP, S/MIME, PEM
⑤ PEM, PGP, S/MIME

39. SSL의 Handshake 프로토콜에서 수행하는 내용이 아닌 것은 무엇인가?

① 서버와 고객간의 상호 인증
② 암호알고리즘 선택
③ 부인방지를 위한 메시지에 대한 전자서명
④ 인증서 전송
⑤ 암호키 계산

40. 무선전자상거래(m-commerce)는 이동통신 네트워크 기술과 무선단말기를 이용하여 언제 어디서나 참여할 수 있는 상거래를 의미한다. 여기에서 사용되는 무선 단말기의 성능상의 제약사항이 아닌 것은?

① CPU, OS의 성능 제한
② 메모리의 제한
③ 기밀정보의 저장에 부적합
④ 소비전력의 제한
⑤ 통신속도의 제한

41. 다음 중 스마트카드에 대한 설명으로 잘못된 것은?

① 한 번 기록된 내용의 변경이 불가능한 WROM 메모리를 사용
② 외부 인터페이스를 통해 입력된 명령어를 인식
③ 외부와의 통신은 직렬 포트를 동기식 또는 비동기식으로 작동
④ 사용되는 주파수는 5에서 14Hz
⑤ 마이크로프로세서와 메모리를 내장

42. 생체인식 기술에 관한 다음 설명 중 틀린 것은?

① 음성인식 기술 중 discrete speech system은 화자가 천천히, 뚜렷하게 발음을 해야 정확한 인식이 가능하다.
② 망막인식은 적색 광선을 이용, 망막에 있는 모세혈관에 반사된 역광을 측정하는 방식을 사용한다.
③ 망막은 크기가 작기 때문에, 망막인식은 안구 내 질병이나 눈의 충혈에 영향을 받지 않는다.
④ 홍채 패턴은 평생토록 변하지 않으며, 좌우측도 서로 다르고 일란성 쌍둥이도 홍채가 서로 다르기 때문에, 홍채 인식은 개인 식별에 적합하다.
⑤ 망막인식 시, 망막에 비추는 적외선이 인체에 해롭지는 않으나 사용하기에는 거부감을 줄 수 있다.

43. SSL(Secure Socket Layer), TLS(Transport Layer Security), IPsec(Internet Protocol Security) 등의 보안 프로토콜이 보장할 수 없는 것은?

① 메시지 기밀성
② 메시지 무결성
③ 송신자 인증
④ 부인방지
⑤ 재전송 방지

44. 버퍼 오버플로우를 예방하는 방법 중 프로그래머가 코딩 시 입력버퍼의 경계값을 검사하는 안전한 함수를 사용하는 방법이 있다. 다음 중 여기에 해당하지 않는 함수는?

① strncpy()
② snprintf()
③ fgets()
④ getopt()
⑤ getcwd()

45. 다음 중 SSO(Single Sign On)에 관한 설명으로 올바른 것은?

① 단 한 번의 사용자 인증 및 권한 부여로 그 사용자가 가진 권한 범위내에서 모든 컴퓨터와 시스템에 접근이 가능하도록 하는 메커니즘이다.
② 각각의 컴퓨터나 시스템에 접근 시 동일한 아이디를 사용할 수 있지만, 보안을 위해 각기 다른 비밀번호를 입력하여야 한다.
③ 구현이 쉽다는 장점이 있는 반면, 사용자 오류나 시스템 오류가 늘어날 수 있다는 단점이 있다.
④ 패스워드 기반 어플리케이션에는 사용할 수 없다.
⑤ 시스템 관리가 어려워지고, 사용상의 불편함이 다소 가중될 수 있으나, 보안은 훨씬 강화시킬 수 있다.

46. 사용자 인증과 식별에 다양한 기법이 사용되는 데 가장 경제적이긴 하지만 또한 도청 공격에 가장 취약한 방법은 무엇인가?

① 사용자 ID와 패스워드
② 생물학적 잠금장치(Biometrics Door Locks)
③ 스마트 토큰
④ 메모리 토큰
⑤ 일회성 패스워드

47. 다음 중 RFID 산업화에 관한 이슈 사항과 가장 거리가 먼 것은?

① RFID가격 최소화
② 주파수 확보
③ 프라이버시 침해 방지
④ RFID 응용분야 확보
⑤ 네트워크간 호환성 확보

48. 다음 중 DRM과 가장 관련이 깊은 것은?

① 중앙 집중화된 모니터링
② 암호화된 통신
③ 주변기기 매체 제어
④ 접근 권한 통제
⑤ 침입 방지 시스템

49. 다음 중 버퍼 오버플로우 취약점이 존재하는 함수가 아닌 것은?

① strcpy()
② strcat()
③ scanf()
④ gets()
⑤ printf()

50. 새로운 프로세스의 생성 시, 보안을 위해 취해야 할 사항으로 옳지 않은 것은?

① system() 함수를 사용하지 않는다.
② 프로그램을 종료하기 전에 모든 파일을 close 한다.
③ 프로그램을 실행할 때 전체 경로 이름을 사용한다.
④ 파일 open은 popen() 함수를 사용한다.
⑤ Child process에 전달된 환경 변수를 확인한다.