

## 1과목 : 정보보호개론

1. 이산대수 문제에 바탕을 두며 인증메시지에 비밀 세션키를 포함하여 전달 할 필요가 없고 공개키 암호화 방식의 시초가 된 키 분배 알고리즘은?

- ① RSA 알고리즘
- ② DSA 알고리즘
- ③ MD-5 해쉬 알고리즘
- ④ Diffie-Hellman 알고리즘

2. 다음 중 유형이 다른 암호 알고리즘은?

- ① RSA(Rivest-Shamir-Adelman)
- ② AES(Advanced Signature Algorithm)
- ③ DSA(Digital Signature Algorithm)
- ④ KCDSA(Korea Certification-based Digital Signature Algorithm)

3. SEED(128 비트 블록 암호 알고리즘)의 특성으로 옳지 않은 것은?

- ① 데이터 처리단위는 8, 16, 32 비트 모두 가능하다.
- ② 암·복호화 방식은 공개키 암호화 방식이다.
- ③ 입출력의 크기는 128 비트이다.
- ④ 라운드의 수는 16 라운드이다.

4. Kerberos 의 다음 용어 설명 중 옳지 않은 것은?

- ① AS : Authentication Server
- ② KDC : Kerbers 인증을 담당하는 데이터 센터
- ③ TGT : Ticket을 인증하기 위해서 이용되는 Ticket
- ④ Ticket : 인증을 증명하는 키

5. 암호의 목적에 대한 설명 중 옳지 않은 것은?

- ① 비밀성(Confidentiality) : 허가된 사용자 이외 암호문 해독 불가
- ② 무결성(Integrity) : 메시지 변조 방지
- ③ 접근 제어(Access Control) : 프로토콜 데이터 부분의 접근 제어
- ④ 부인봉쇄(Non-Repudiation) : 송수신 사실 부정방지

6. 안전한 Linux Server를 구축하기 위한 방법으로 옳지 않은 것은?

- ① 불필요한 데몬을 제거한다.
- ② 불필요한 Setuid 프로그램을 제거한다.
- ③ 시스템의 무결성을 주기적으로 검사한다.
- ④ 무결성을 검사하기 위한 데이터베이스를 추후 액세스가 용이하게 하기 위하여 검사할 시스템에 저장하는게 좋다.

7. IP 계층에서 보안 서비스를 제공하기 위한 IPsec에서 제공되는 보안 서비스로 옳지 않은 것은?

- ① 부인방지 서비스
- ② 무연결 무결성 서비스
- ③ 데이터 원천 인증
- ④ 기밀성 서비스

8. 인터넷에서 일어날 수 있는 대표적인 보안사고 유형으로 어떤 침입 행위를 시도하기 위해 일정기간 위장한 상태를 유지하며, 코드 형태로 시스템의 특정 프로그램 내부에 존재 하는 것은?

- ① 논리 폭탄
- ② 웜
- ③ 트로이 목마
- ④ 잠입

9. WWW에서의 보안 프로토콜로 옳지 않은 것은?

- ① S-HTTP(Secure Hypertext Transfer Protocol)
- ② SEA(Security Extension Architecture)
- ③ PGP(Pretty Good Privacy)
- ④ SSL(Secure Sockets Layer)

10. 다음 중 방화벽의 유형으로 옳지 않은 것은?

- ① Packet Filtering Gateway
- ② Circuit Level Gateway
- ③ Screened Host
- ④ Proxy서버/응용 Gateway

## 2과목 : 운영체제

11. SSL 레코드 계층의 서비스를 사용하는 세 개의 특정 SSL 프로토콜 중의 하나이며 메시지 값이 '1'인 단일 바이트로 구성되는 것은?

- ① Handshake 프로토콜
- ② Change cipher spec 프로토콜
- ③ Alert 프로토콜
- ④ Record 프로토콜

12. Linux의 기본 디렉터리에 해당하지 않는 것은?

- ① /etc
- ② /root
- ③ /grep
- ④ /home

13. Linux 시스템에서 '-rwxr-xr-x' 퍼미션을 나타내는 숫자는?

- ① 755
- ② 777
- ③ 766
- ④ 764

14. vi의 3가지 모드중에서 실제로 vi편집기의 내용을 수정할때 사용하며 i, a, o등을 누른 후, 텍스트를 입력할 수 있는 상태모드는?

- ① 명령모드
- ② 실행모드
- ③ 편집모드
- ④ 치환모드

15. RPM의 설치나 제거시에 사용하는 옵션 중에서 '--nodeps'의 의미는?

- ① 어떤 패키지의 의존성을 무시하고 설치하고자 할때
- ② 디렉터리를 마치 '/'처럼 생각하고 설치하고자 할때
- ③ 패키지를 실제로 설치하지 않고 충돌이나 의존성 문제가 있는지 검사만 할 때
- ④ 새로운 패키지를 지우고 구 버전의 패키지로 교체할때

16. Linux에서 TAR로 묶인 'mt.tar'를 풀어내는 명령은?

- ① tar -tvf mt.tar
- ② tar -cvf mt.tar
- ③ tar -cvvf mt.tar
- ④ tar -xvf mt.tar

17. Linux 명령어에 대한 설명으로 옳지 않은 것은?

- ① ls : 디렉터리를 변경할 때 사용한다.
- ② cp : 파일을 다른 이름으로 또는 다른 디렉터리로 복사할 때 사용한다.

- ③ mv : 파일을 다른 파일로 변경 또는 다른 디렉터리로 옮길 때 사용한다.
- ④ rm : 파일을 삭제할 때 사용한다.
18. 프로토콜을 POP3 대신에 IMAP를 쓰는 환경에서 vi편집기를 이용해서 POP 프로토콜을 주석처리 하고, IMAP 프로토콜의 주석을 제거 하였지만 서비스가 정상적으로 이루어지지 않고 있다면 그 원인에 해당하는 것은?
- ① IMAP 프로토콜은 POP3를 대신할 수 없기 때문이다.
- ② Sendmail과 IMAP는 근본적으로 상관이 없기 때문이다.
- ③ 데몬 설정 파일을 변경한 후 데몬을 재실행 해주지 않았기 때문이다.
- ④ 해당 포트가 열렸기 때문이다.
19. 아파치 웹서버 Type중에서 오직 유닉스 플랫폼만 지원하며, 웹서버 설정 변경시 웹서버를 리부팅 할 필요가 없으나 새로운 프로세서를 만들 때 마다 설정 파일을 참고하기 때문에 속도가 느린 Type은?
- ① inetd                      ② standalone
- ③ main server              ④ virtual hosts
20. 아파치 웹서버 운영시 서비스에 필요한 여러 기능들을 제어하기 위하여 설정해야 하는 파일은?
- ① httpd.conf                ② htdocs.conf
- ③ index.php                 ④ index.cgi
21. DHCP(Dynamic Host Configuration Protocol) Scope 범위 혹은 주소 풀(Address Pool)을 만드는데 주의할 점에 속하지 않는 것은?
- ① 모든 DHCP 서버는 최소한 하나의 DHCP 범위를 가져야 한다.
- ② DHCP 주소 범위에서 정적으로 할당된 주소가 있다면 해당 주소를 제외해야 한다.
- ③ 네트워크에 여러 DHCP 서버를 운영할 경우에는 DHCP 범위가 겹치지 않아야 한다.
- ④ 하나의 서브넷에는 여러 개의 DHCP 범위가 사용될 수 있다.
22. Windows 2003 Server에서 FTP 서비스에 대한 설명으로 옳지 않은 것은?
- ① 웹 사이트가 가지고 있는 도메인을 IP Address로 바꾸어 주는 서비스를 말한다.
- ② IIS에서 기본적으로 제공하는 서비스이다.
- ③ 기본 FTP 사이트는 마우스 오른쪽 버튼을 눌러 등록정보를 수정할 수 있다.
- ④ FTP 서비스는 네트워크를 통하여 파일을 업로드 및 다운로드 할 수 있는 서비스를 말한다.
23. Windows 2003 Server의 DNS 서비스 설정에 관한 설명으로 옳지 않은 것은?
- ① 정방향 조회 영역 설정 후 반드시 역방향 조회 영역을 설정해 주어야 한다.
- ② Windows 2003 Server는 고정 IP Address를 가져야 한다.
- ③ Administrator 권한으로 설정해야 한다.
- ④ 책임자 이메일 주소의 at(@)은 마침표(.)로 대체된다.
24. Windows 2003 Server에서 제공하고 있는 VPN 프로토콜인 L2TP(Layer Two Tunneling Protocol)에 대한 설명 중 옳지

않은 것은?

- ① IP 기반의 네트워크에서만 사용가능하다.
- ② 헤드 압축을 지원한다.
- ③ 터널 인증을 지원한다.
- ④ IPsec 알고리즘을 이용하여 암호화 한다.

25. 'shutdown -r now' 와 같은 효과를 내는 명령어는?

- ① halt                      ② reboot
- ③ restart                  ④ poweroff

26. Linux에서 'ls -al' 명령에 의하여 출력되는 정보로 옳지 않은 것은?

- ① 파일의 접근허가 모드
- ② 파일 이름
- ③ 소유자명, 그룹명
- ④ 파일의 소유권이 변경된 시간

27. Linux 시스템에서 다음의 역할을 수행하는 데몬은?

시스템에서 여러가지 일어나고 있는 상황을 기록해 주는 데몬으로, 시스템에 이상이 발생했을 경우 해당 내용을 파일에 기록하거나 다른 호스트로 전송할 수 있다.

- ① inet                      ② xntpd
- ③ syslogd                  ④ auth

28. 삼바 데몬을 Linux에 설치하여 가동하였을 때 열리는 포트 로 알맞게 나열한 것은?

- ① UDP 137, 139            ② TCP 137, 139
- ③ TCP 80, 25              ④ UDP 80, 25

29. RedHat Linux에서 사용자의 'su' 명령어 시도 기록을 볼 수 있는 로그는?

- ① /var/log/secure          ② /var/log/messages
- ③ /var/log/wtmp            ④ /var/log/lastlog

30. Linux에서 현재 위치한 디렉터리를 표시해 주는 명령어는?

- ① mkdir                    ② pwd
- ③ du                        ④ df

### 3과목 : 네트워크

31. 데이터 링크 오류제어를 위한 ARQ 방식 중 전송 성능이 가장 우수한 방식은?

- ① Stop-and-Wait ARQ
- ② Go-back-N ARQ
- ③ Selective Repeat ARQ
- ④ 모든 ARQ는 전송 성능이 동일하다.

32. 프로토콜의 기능 중 전송을 받는 개체에서 발송지로부터 오는 데이터의 양이나 속도를 제한하는 기능은?

- ① 흐름 제어                ② 에러 제어
- ③ 순서 제어                ④ 접속 제어

33. Star Topology에 대한 설명 중 올바른 것은?

- ① 시작점과 끝점이 존재하지 않는 폐쇄 순환형 토폴로지이다.
- ② 모든 노드들에 대해 간선으로 연결한 형태이다.
- ③ 연결된 PC 중 하나가 다운되어도 전체 네트워크 기능은 수행된다.
- ④ 라인의 양쪽 끝에 터미네이터를 연결해 주어야 한다.

34. 네트워크에 스위치 장비를 도입함으로써 얻어지는 효과로 옳지 않은 것은?

- ① 패킷의 충돌 감소
- ② 속도 향상
- ③ 네트워크 스니핑(Sniffing) 방지
- ④ 스푸핑(Spoofing) 방지

35. Routed Protocol로 옳지 않은 것은?

- ① TCP/IP                      ② OSPF
- ③ IPX/SPX                    ④ Appletalk

36. OSI 7 Layer 중에서 암호, 복호, 인증, 압축 등의 기능이 수행되는 계층은?

- ① 전송 계층                      ② 네트워크 계층
- ③ 응용 계층                      ④ 표현 계층

37. '192.168.0.0/255.255.255.0' 네트워크에서 '192.168.0.3/255.255.255.0' 컴퓨터가 'ping 192.168.0.255' 라는 명령을 내렸을 때 예상되는 동작은?

- ① 네트워크 주소이므로 ping 프로그램은 아무런 메시지도 출력하지 않고 종료한다.
- ② 패킷이 내부망을 떠돌아다니다가 TTL 이 만료되어 에러 메시지를 출력한다.
- ③ 같은 네트워크 내에 있는 모든 컴퓨터들이 응답패킷을 보낸다.
- ④ 자기 자신에게 'ICMP\_ECHO\_REQUEST' 패킷을 보낸다.

38. 프로토콜 스택에서 가장 하위 계층에 속하는 것은?

- ① IP                                  ② TCP
- ③ HTTP                            ④ UDP

39. '서비스' - 'Well-Known 포트' - '프로토콜'의 연결이 옳지 않은 것은?

- ① FTP - 21 - TCP                      ② SMTP - 25 - TCP
- ③ DNS - 53 - TCP                      ④ SNMP - 191 - TCP

40. IPv6 프로토콜의 구조는?

- ① 32bit                                  ② 64bit
- ③ 128bit                                ④ 256bit

41. 패킷 내부의 ICMP 메시지로 옳지 않은 것은?

- ① 에코 요청 및 응답                      ② 패킷의 손실과 손실량
- ③ 목적지 도달 불가                      ④ 시간 초과

42. TCP/IP 프로토콜을 이용해서 서버와 클라이언트가 통신을 할 때, Netstat 명령을 이용해 현재의 접속 상태를 확인할 수 있다. 클라이언트와 서버가 현재 올바르게 연결되어 통신 중인 경우 Netstat으로 상태를 확인하였을 때 나타나는

메시지는?

- ① SYN\_PCVD                      ② ESTABLISHED
- ③ CLOSE\_WAIT                      ④ CONNECTED

43. TCP와 UDP의 차이점을 설명한 것 중 옳지 않은 것은?

- ① TCP는 전달된 패킷에 대한 수신측의 인증이 필요하지만 UDP는 필요하지 않다.
- ② TCP는 대용량의 데이터나 중요한 데이터 전송에 이용되지만 UDP는 단순한 메시지 전달에 주로 사용된다.
- ③ UDP는 네트워크가 혼잡하거나 라우팅이 복잡할 경우에는 패킷이 유실될 우려가 있다.
- ④ UDP는 데이터 전송 전에 반드시 송수신 간의 세션이 먼저 수립되어야 한다.

44. TCP 헤더 필드의 내용으로 옳지 않은 것은?

- ① TTL(Time To Live)                      ② 발신지 포트번호
- ③ 윈도우 크기                              ④ Checksum

45. 패킷(Packet)에 있는 정보로 옳지 않은 것은?

- ① 출발지 IP Address                      ② TCP 프로토콜 종류
- ③ 전송 데이터                              ④ 목적지 IP Address

4과목 : 보안

46. Windows 2003 Server의 보안영역에는 각각 클라이언트 보안, 네트워크 보안, 물리적인 보안, 원격 액세스 보안, 인터넷 정책, 인적보안, 사용자 정책 등이 있다. 이에 대한 설명으로 옳지 않은 것은?

- ① 원격 액세스 보안 : 직접 원격 접속을 통한 인증되지 않은 액세스로부터 네트워크 시스템을 보호
- ② 클라이언트 보안 : 클라이언트 컴퓨터들을 인증된 사용자 또는 인증되지 않는 사용자로부터 보호
- ③ 네트워크 보안 : 외부인으로 부터 하드웨어 침입에 대비하여 물리적인 시스템을 보호
- ④ 물리적인 보안 : 네트워크 시스템들이 있는 컨테이너 공간, 설비들을 안전하게 관리

47. SSH(Secure Shell)에 대한 설명으로 옳지 않은 것은?

- ① 안전하지 못한 네트워크에서 안전하게 통신할 수 있는 기능과 강력한 인증방법을 제공한다.
- ② 문자를 암호화하여 IP Spoofing, DNS Spoofing으로부터 보호할 수 있다.
- ③ 쌍방 간 인증을 위해 Skipjack 알고리즘이 이용된다.
- ④ 네트워크의 외부 컴퓨터에 로그인 할 수 있고 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해주는 프로그램이다.

48. Linux에서 root 권한 계정이 'a' 라는 파일을 지우려 했을때 나타난 결과이다. 이 파일을 지울 수 있는 방법은?

```
[root@linux /root]# rm a -rf
rm: cannot unlink 'a': Operation not permitted
[root@linux /root]# ls -l a
-rw-r--r-- 1 root root 0 Aug 31 16:59 a
[root@linux4u /root]
```

- ① 파일크기가 0 바이트이므로 지워지지 않는다. 파일에 내용을 넣은 후 지운다.

- 최강 자격증 기출문제 전자문제집 CBT :
- [www.comcbt.com](http://www.comcbt.com)

전자문제집 CBT PC 버전 : [www.comcbt.com](http://www.comcbt.com)  
 전자문제집 CBT 모바일 버전 : [m.comcbt.com](http://m.comcbt.com)  
 기출문제 및 해설집 다운로드 : [www.comcbt.com/x](http://www.comcbt.com/x)

#### 전자문제집 CBT란?

종이 문제집이 아닌 인터넷으로 문제를 풀고 자동으로 채점하며 모의고사, 오답 노트, 해설까지 제공하는 무료 기출문제 학습 프로그램으로 실제 시험에서 사용하는 OMR 형식의 CBT를 제공합니다.

PC 버전 및 모바일 버전 완벽 연동  
 교사용/학생용 관리기능도 제공합니다.

오답 및 오탈자가 수정된 최신 자료와 해설은 전자문제집 CBT에서 확인하세요.

1	2	3	4	5	6	7	8	9	10
④	②	②	②	③	④	①	③	③	③
11	12	13	14	15	16	17	18	19	20
②	③	①	③	①	④	①	③	①	①
21	22	23	24	25	26	27	28	29	30
④	①	①	①	②	④	③	①	②	②
31	32	33	34	35	36	37	38	39	40
③	①	③	④	②	④	③	①	④	③
41	42	43	44	45	46	47	48	49	50
②	②	④	①	②	③	③	④	①	④
51	52	53	54	55	56	57	58	59	60
②	④	①	④	②	④	④	③	④	③