1과목 : 정보보호개론

1. DES 암호화 기술 기법에 대한 설명으로 잘못된 것은?

❶ 송. 수신자 모두 다른 키를 갖는다.
② 스마트카드 등에 이용한다.
③ 암호화가 빠르다.
④ 키 관리와 분배의 어려움이 있다.

2. 5명의 사용자가 대칭키(Symmetric Key)를 사용하여 주고받는 메시지를 암호화 하기위해서 필요한 키의 총 개수는?

① 2개 ② 5개
③ 7개 ❹ 10개

3. 공개키 암호화 방식에 대한 설명이 잘못된 것은?

❶ 암호화할 때 사용한 키와 복호화 할 때 사용한 키가 같은 암호화 방식이다.
② 공개키 암호 알고리즘은 실질적인 산업계 표준으로 자리 매김하고 있다.
③ RSA 공개키 암호 알고리즘의 사용 시 모듈러스의 크기는 788비트 이상이 권고되고 있다.
④ 최근 타원 곡선 알고리즘이 암호 속도가 빠르고 용이하여 현재 그 활용 폭이 넓어지고 있다.

4. 전자 서명문 생성 시 이용되는 인증서(Certificate)에 대하여 잘못 설명된 것은?

① 근본적으로 사용자의 이름과 공개키를 인증기관의 개인키로 서명한 서명문이다.
② 주체 이름은 일반적으로 X.500 DN(Distinguished Name) 형식을 갖는다.
③ 주체 이름을 대신하는 주체 대체 이름으로 사용자 ID, E-mail 주소 및 IP 주소, DNS 이름 등이다.
❹ 인증기관이 한번 발행하면 영원히 취소되지 않는다.

5. 다음 중 침입차단 시스템의 문제점으로 볼 수 없는 것은?

① 제한된 서비스
② 내부 사용자에 의한 보안 침해
③ 침입차단 시스템의 네트워크 트래픽 병목발생
❹ 보안기능의 강화

6. 국내에서 1998년에 고시된 침입차단시스템의 평가등급 중 최소한의 보안 기능 요구만 만족시키고 있는 등급은?

❶ K1 ② K2
③ K3 ④ K4

7. 개인 홈페이지 서버가 크래킹(Cracking) 당하였을 때 취해야 할 행동으로 가장 적절한 것은?

① 로그분석을 통해 크래킹을 한 사람의 신원을 밝혀내어 접속한 서버를 크래킹 한다.
❷ 네트워크 분리 후 로그 분석을 통해 크래킹을 한 시점과 방법을 알아내 차후 동일수법에 의한 사고를 방지한다.
③ 백업된 자료를 이용하여 그대로 복구하여 놓는다.
④ 백도어의 염려가 있으므로 시스템을 포맷한다.

8. 정보통신 윤리위원회의 불건전 정보 심의 기준으로 짝지어지지 않은 것은?

① 반국가적인 내용, 법과 질서와 존엄성을 저해하는 내용
❷ 시민 단체 비방 내용, 경로효친 사상 위배 내용
③ 비과학적인 생활 태도 조장, 신앙의 자유에 반하는 내용
④ 의약품 등의 오남용 조장, 불건전 오락물 등의 내용

9. IPSec을 위한 보안 연계(Security Association)가 포함하는 파라미터들로만 짝지어진 것은?

① 사용자 ID/ 암호 알고리즘, 암호키, 수명 등의 ESP 관련 정보/ 발신지 IP 주소와 목적지 IP 주소
② IPSec 프로토콜 모드(터널, 트랜스포트)/ 인증 알고리즘, 인증 키, 수명 등의 AH 관련 정보/ 발신지 포트 및 목적지 포트
③ 데이터 민감도/ IPSec 프로토콜 모드(터널, 트랜스포트)/ 암호 알고리즘, 암호키, 수명 등의 ESP 관련 정보/ 발신지 IP 주소와 목적지 IP 주소
❹ IPSec 프로토콜 모드(터널, 트랜스포트)/ 인증 알고리즘, 인증 키, 수명 등의 AH 관련 정보/ 암호 알고리즘, 암호키, 수명 등의 ESP 관련 정보

10. 다음은 해쉬 함수(Hash Function)의 정의를 나타낸 것이다. 해쉬 함수에 대한 설명으로 옳지 않는 것은?

$$y = h(x)$$

① x는 가변길이의 메시지이며, y는 고정길이의 해쉬 값(Hash Code)이다.
② 주어진 x에 대하여 y를 구하는 것은 쉽다.
③ 주어진 y에 대하여 y = h(x)를 만족하는 x를 찾는 것은 불가능하다.
❹ 동일한 해쉬 값을 가지는 서로 다른 메시지가 있어야 한다.

2과목 : 운영체제

11. NTFS의 주요 기능에 대한 설명 중 잘못된 것은?

① 파일 클러스터를 추적하기 위해 B-Tree 디렉터리 개념을 사용한다.
② 서버 관리자가 ACL을 이용하여 누가 어떤 파일만 액세스할 수 있는지 등을 통제할 수 있다.
③ 교체용 디스크와 고정 디스크 모두에 대해 데이터 보안을 지원한다.
❹ FAT 보다 대체적으로 빠른 속도를 지원한다.

12. 네트워크 상에서 파일이나 폴더의 공유가 불가능한 운영체제는?

❶ MS-DOS 3.2
② Windows 95 - OSR2
③ Windows 2000 Server
④ Windows NT Workstation

13. File 시스템에서 FAT와 NTFS에 대한 설명으로 잘못된 것은?

① 설치 프로그램을 활용하면 FAT나 FAT32를 쉽게 NTFS로 변환이 가능하다.
② Convert.exe를 사용하여 설치 후에 변경할 수 있으며 Convert [드라이브:]/fs:NTFS 로 변환한다.
❸ NTFS에서 FAT로의 변환이 가능하다.
④ NTFS는 안전성, 보안성이 FAT보다 우수하다.

14. Windows 2000 Server의 기본 FTP 사이트 등록정보 설정에서 익명연결 허용을 설정할 수 있는 탭은?

① FTP 사이트 ❷ 보안 계정
③ 메시지 ④ 홈 디렉터리

15. Windows 2000 Server의 DNS(Domain Name System) 서비스 설정에 관한 설명으로 잘못된 것은?

❶ 역방향 조회 영역 설정 후 반드시 역방향 조회 영역을 설정해 주어야 한다.
② Windows 2000 Server는 고정 IP 주소를 가져야 한다.
③ Administrator 권한으로 설정해야 한다.
④ 책임자 이메일 at(@)은 마침표(.)로 대체된다.

16. Windows 98이 지원하는 기본 공유모드는?

① user level 공유모드 ❷ share level 공유모드
③ domain level 공유모드 ④ client level 공유모드

17. 기존 서버의 램(256MB)을 512MB로 업그레이드 했는데, 서버 상에서는 계속 256MB로 인식하는 문제가 발생하였다. 올바른 해결 방법은?

❶ lilo.conf 파일안에 append="mem=512M" 을 추가한다.
② /etc/conf.memory 라는 파일을 만들어서 append="mem=512M"를 추가한다.
③ swap 영역을 비활성화 시킨 다음 재부팅 한다.
④ /proc/sys/memory에다가 512 이라는 값을 넣는다.

18. Linux 시스템 파일의 설명 중 가장 거리가 먼 것은?

① /etc/passwd - 사용자 데이터베이스
② /etc/fstab - 시스템이 시작될 때 자동으로 마운트 되는 파일 시스템 목록
❸ /etc/motd - 텔넷 로그인 전 나타낼 메시지
④ /etc/shadow - 패스워드 파일

19. Linux의 기본 명령어들이 포함되어 있는 디렉터리는?

① /var ② /usr
❸ /bin ④ /etc

20. Linux에서 "ls -al" 명령에 의하여 출력되는 정보가 아닌 것은?

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

21. Linux에서 /dev 디렉터리에 관한 설명으로 거리가 먼 것은?

① 이 디렉터리는 물리적 용량을 갖지 않는 가상 디렉터리이다.
② 시스템의 각종 장치들에 접근하기 위한 디바이스 드라이버들이 저장되어 있다.
❸ 이 디렉터리에는 커널로 로딩 가능한 커널 모듈들이 저장되어 있다.
④ 대표적으로 하드 디스크 드라이브, 플로피, CD-ROM 그리고 루프백 장치 등이 존재한다.

22. Linux 파일 시스템의 마운팅과 논리적 계층 구조에 관련된 내용이라 할 수 없는 것은?

① Linux는 모든 블록 장치에 존재하는 파일 시스템들을 마운트 하여 사용한다.
② 파일 시스템이 존재하는 논리적인 파티션을 소스하고, 논리적 파일계층 구조에서 위치할 경로를 대상으로 마운트 시킨다.
❸ 마운트의 기본 디렉터리는 “/var"이다.
④ 제한된 디스크 공간을 여러 사용자가 공유하는 경우에 쿼터의 사용이 필요하다.

23. Linux 시스템에서 현재 사용자가 수행되는 백그라운드 작업을 출력하는 명령어는?

❶ jobs ② kill
③ ps ④ top

24. Linux에서 사용하는 에디터 프로그램이 아닌 것은?

❶ awk ② pico
③ vi ④ emacs

25. Linux 커널 2.2 시스템에서 매스쿼레이드(Masquerade) 기능을 이용하여 공인 IP 주소를 192.168.0.x의 IP로 공유해서 사용 중이다. 그런데 192.168.0.x를 가진 클라이언트 컴퓨터들이 인터넷에 FTP 접속을 하려면 접속이 되지 않는다. 어떤 명령을 내려야 접속을 가능하게 할 수 있는가?

① 매스쿼레이드로 IP 공유한 경우는 FTP 접속이 되질 않는다.
❷ “modprobe ip_masq_ftp”을 입력한다.
③ “modprobe ip_masq_raudio”을 입력한다.
④ “modprobe ip_masq_ftphttp”을 입력한다.

26. 기존 UNIX 운영체제 같은 경우 사용자의 암호와 같은 중요한 정보가 /etc/passwd 파일 안에 보관되기 때문에 이 파일을 이용해서 해킹을 하는 경우가 있었다. 이를 보완하기 위해서 암호정보만 따로 파일로 저장하는 방법이 생겼는데, 이 방식의 명칭은?

① DES Password System
② RSA Password System
③ MD5 Password System
❹ Shadow Password System

27. /etc/resolv.conf 파일에 적는 내용이 알맞게 나열된 것은?

❶ 네임서버 주소, DNS 서버 IP 주소
② 네임서버 주소, Linux 서버 랜 카드 IP 주소
③ 네임서버 주소, 홈페이지 도메인
④ 네임서버 주소, 서버 도메인

28. 다음 중 Apache의 기능이 아닌 것은?

① 프록시(Proxy) 기능을 가지고 있다.
② 웹 사이트의 접근을 제어할 수 있다.
③ Virtual Host 서비스를 할 수 있다.
❹ NCSA 서버의 대부분의 기능을 수행할 수 있다.

29. Telnet 을 이용해서 원격으로 서버에 있는 a.txt 파일을 vi 에디터로 편집하던 중 갑자기 접속이 끊어졌다. 다시 접속하여 a.txt 파일을 열었더니, a.txt 파일이 열리기 전에 한 페이지 가량의 에러 메시지가 출력된 후 Enter 키를 눌러야만 a.txt 파일이 열린다. 이 에러를 복구하기 위해서 vi 에디터를 실행시킬 때 가장 적합한 옵션은?

① vi a.txt ② vi -recover a.txt
③ vi -continue a.txt ❹ vi -r a.txt

30. 다음 중 Telnet 기능이 기본적으로 설치가 되어 있지 않은 운영체제는?
❶ MS-DOS 6.0 ② Windows 95
③ Linux ④ MacOS

3과목 : 네트워크

31. 다음 중 LAN의 특징이 아닌 것은?
① 고속의 전송속도
② 높은 연결성
③ 다양한 데이터처리
❹ 지역간의 연결거리 비제약

32. HDLC 프로토콜에서, 확인 응답, 오류제어, 그리고 흐름제어를 위하여 보내지는 프레임의 유형은?
① I-프레임
❷ S-프레임
③ U-프레임
④ SNRM(Set Normal Response Mode)

33. 네트워크 전송매체에 대한 설명으로 틀린 것은?
① UTP - 쉴딩(Shielding) 처리를 하지 않고 내부의 선이 꼬여 있는 형태이다.
❷ STP - UTP와 달리 내부의 8개 선에 피복이 입혀져 있지 않다.
③ Thinnet-BNC - BNC라는 커넥터가 씬넷(Thinnet) 케이블에 연결되어 있는 형태로 보통 씬넷 케이블 또는 BNC 케이블이라고 부른다.
④ Optical Fiber - 케이블 중앙에 유리섬유 코어나 플라스틱 코어가 있고 맨 바깥에 플라스틱 피복이 입혀져 있다.

34. 디지털 데이터를 디지털 신호 인코딩(Digital Signal Encoding)하는 방법이 아닌 것은?
① NRZ(Non Return to Zero)
② Manchester
❸ PCM(Pulse Code Modulation)
④ Differential Manchester

35. Peer-To-Peer 네트워크에 대한 설명으로 틀린 것은?
① Peer는 각각의 네트워크상의 PC를 말한다.
② 일반적으로 서버가 없는 네트워크 형태를 말한다.
③ 구축이 간단하고 비용이 적게 든다.
❹ 다수의 컴퓨터를 연결하기에 적당한 방식이다.

36. 전화망에 일반적으로 Twisted-Pair Cable을 많이 사용하는데, 이 Cable을 꼬아 놓은 가장 큰 이유는?
❶ 수신기에서 잡음의 효과를 감소하기 위하여
② 관리가 용이하게 하기 위하여
③ 꼬인 선의 인장 강도를 크게 하기 위하여
④ 구분을 용이하게 하기 위하여

37. Star Topology에 대한 설명 중 맞는 것은?
① 가운데 서버나 라우터를 중심으로 별모양의 네트워크를 구성한다.
② 케이블은 10BaseT, 100BaseT의 UTP 케이블과 씬넷(BNC) 케이블을 쓴다.
❸ 연결된 PC 중 하나가 다운되어도 전체 네트워크 기능은 수행된다.
④ 라인의 양쪽 끝에 테니네이터를 연결해 주어야 한다.

38. 다음 네트워크 아키텍쳐에 관한 설명으로 잘못된 것은?
① Ethernet은 가장 광범위하게 설치된 근거리 통신이다.
❷ Repeater는 긴 케이블을 따라 전달되는 신호를 증폭시켜 주는데 이때 노이즈를 제거하기 위해 별도의 게이트웨이를 연결한다.
③ Bridge는 MAC을 일일이 검사하므로 Repeater보다 속도가 떨어진다.
④ Router는 다수의 네트워크 세그먼트를 연결하는 목적에 사용하는 장치이다.

39. Routed Protocol이 아닌 것은?
① TCP/IP ❷ OSPF
③ IPX/SPX ④ Appletalk

40. OSI 7 Layer 구조에서 계층 7에서 계층 4를 차례대로 나열한 것은?
① 응용(Application) - 세션(Session) - 표현(Presentation) - 전송(Transport)
❷ 응용(Application) - 표현(Presentation) - 세션(Session) - 전송(Transport)
③ 응용(Application) - 표현(Presentation) - 세션(Session) - 네트워크(Network)
④ 응용(Application) - 네트워크(Network) - 세션(Session) - 표현(Presentation)

41. OSI 7 Layer에서 암호/복호, 인증, 압축 등의 기능이 수행되는 계층은?
① Transport Layer ② Datalink Layer
❸ Presentation Layer ④ Application Layer

42. IP Address를 Ethernet Address로 매핑하는 테이블을 동적으로 구축하는 프로토콜로 이 경우 Ethernet의 브로드캐스트 기능을 사용하게 되는 프로토콜은?
❶ ARP ② RARP
③ RIP ④ IP

43. 다음 보기 중 "서비스" - "Well-Known 포트" - "프로토콜"의 연결이 적당하지 않은 것은?
① FTP - 21 - TCP ② SMTP - 25 - TCP
③ DNS - 53 - TCP ❹ SNMP - 191 - TCP

44. 다음 중 서브넷 마스크를 설명한 것은?
① DNS 데이터베이스를 관리하고 IP 주소를 DNS의 이름과 연결한다.
❷ IP 주소지에 대한 네트워크를 분류 또는 구분한다.
③ TCP/IP의 자동설정에 사용되는 프로토콜로서 정적, 동적 IP 주소를 지정하고 관리한다.
④ 서로 다른 네트워크를 연결할 때 네트워크 사이를 연결

하는 장치이다.

45. 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 ❷ ESTABLISHED
③ CLOSE_WAIT ④ CONNECTED

4과목 : 보안

46. Windows 2000 Server에서 지원하는 신뢰성 기능에 속하지 않는 것은?

① 파일 보호 매커니즘을 사용하여 시스템에 중요한 파일을 덮어쓰지 않도록 보호한다.
② 드라이버 인증을 사용하여 드라이버의 신뢰성을 평가할 수 있다.
③ 분산 파일 시스템을 사용하여 공유된 파일에 보안을 유지한 상태로 접근할 수 있다.
❹ 커버로스(Kerberos)인증을 사용하여 윈도우 2000과 기타 지원 시스템에 한번에 로그 온할 수 있다.

47. 해킹에 성공한 후 해커들이 하는 행동의 유형이 아닌 것은?

① 추후에 침입이 용이하게 하기 위하여 트로이목마 프로그램(Rootkit)을 설치한다.
② 서비스 거부 공격 프로그램을 설치한다.
❸ 접속 기록을 추후의 침입을 위하여 그대로 둔다.
④ 다른 서버들을 스캔 프로그램으로 스캔하여 취약점을 알아낸다.

48. Linux 로그인 파일에 대한 설명이 옳지 않은 것은?

① 커널 에러, 부팅 메시지, 로긴 실패, 그리고 su 로그 등의 기록을 남기는 파일은 "/var/log/messages" 파일이다.
② FTP와 관련된 로그 파일은 "xferlog" 파일이다.
③ TCP Wrapper와 같은 보안 관련 로그 파일은 "secure" 파일이다.
❹ 현재 로그인 되어 있는 사용자의 리스트를 저장하는 파일은 "/var/log/lastlog" 파일이다.

49. 다음 중 PGP에서 사용되는 알고리즘이 아닌 것은?

① RSA ❷ DES
③ MD5 ④ IDEA

50. Linux에서 사용하는 보안 프로그램인 Npasswd 에 대한 설명으로 잘못된 것은?

① 최소한의 패스워드 길이를 조정할 수 있다.
❷ 사용자의 패스워드가 사전에 나오는 단어인지 체크하는 것은 불가능하다.
③ 단순한 패스워드를 체크해 낼 수 있다.
④ 호스트 이름, 호스트 정보 등을 체크할 수 있다.

51. 아파치(Apache)의 DSO(Dynamic Shared Object) 모듈에 대한 설명으로 잘못된 것은?

① mod_access - 호스트 기반 접근 제어
② mod_auth - 사용자 인증
❸ mod_imap - imap4 프로토콜을 이용한 인증 지원
④ mod_mime - 파일 확장자를 이용해 문서 타입을 지정

52. 버퍼 오버플로우(Buffer Overflow) 개념으로 잘못된 것은?

① 스택의 일정부분에 익스플로러 코드(Explorer Code)를 삽입하고 어떤 프로그램의 리턴 어드레스(Return Address)를 익스플로러 코드가 위치한 곳으로 돌린다.
② 대체적으로 문자열에 대한 검사를 하지 않아서 일어나는 경우가 많다.
③ 소유자가 root인 Setuid가 걸린 응용프로그램인 경우 익스플로러 코드를 이용 root의 권한을 획득할 수 있다.
❹ Main 프로그램과 Sub 프로그램의 경쟁관계와 Setuid를 이용하여 공격하는 패턴이 존재한다.

53. 다음 중 해킹 방법이 아닌 것은?

① DOS ② DDOS
③ Sniffing ❹ TCP Wrapper

54. 다음 중 IP Spoofing 과정에 포함되지 않는 것은?

① 공격자의 호스트로부터 신뢰받는 호스트에 Syn-Flooding공격으로 상대방 호스트를 무력화시킨다.
② 신뢰받는 호스트와 공격하려는 목적 호스트간의 패킷교환 순서를 알아본다.
③ 패킷교환 패턴을 파악한 후 신뢰받는 호스트에서 보낸 패킷처럼 위장하여 목적 호스트에 패킷을 보낸다.
❹ Finger에서 나오는 정보에 패스워드가 있는지를 찾아준다.

55. 다음 중 알려진 취약점을 알아보는 스캐너 프로그램의 종류에 속하지 않는 것은?

① SAINT ② MSCAN
③ ISS ❹ Squid

56. 침입 탐지 시스템을 비정상적인 침입탐지 기법과 오용탐지 기법으로 구분할 경우, 오용탐지기법에 해당하는 것은?

❶ 상태 전이 분석
② 행위 측정 방식들의 결합
③ 통계적인 방법
④ 특징 추출

57. 다음 중 성격이 다른 것은?

① Port Scan ② IP Spoofing
③ Sync Flooding ❹ Ipchains

58. 다음 중 시스템 로그데몬(syslogd)의 설명으로 옳지 않은 것은?

① 시스템 로그 데몬의 설정파일의 위치는 “/etc/syslog.conf”이다.
② 로그 데몬의 실행방법은 “/etc/rc.d/init.d/syslog start” 이다.
❸ 시스템 로그 데몬의 위치는 “/bin/syslogd” 이다.
④ 로그 데몬의 종료방법은 “/etc/rc.d/init.d/syslog stop” 이다.

59. 다음 PGP(Pretty Good Privacy)에서 제공하는 기능과 사용 암호 알고리즘이 잘못 연결된 것은?

① 메시지 기밀성 - IDEA, CAST, Triple-DES

② 전자서명 - RSA, SHA-1, MD5
③ 압축 - ZIP
❹ 전자우편 호환성 - MIME

60. 암호 프로토콜에 속하지 않는 것은?
① 키 교환 프로토콜 ② 디지털 서명
③ 전자화폐 ❹ 비밀키 암호

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