1과목 : 정보보호개론

1. 최근 인터넷 웜(Worm)의 공격 및 감염 경로로 가장 옳지 않은 것은?
① Email 첨부 ② 공유 네트워크
③ 감염된 웹서버 접속 ❹ Anonymous FTP

2. 이산대수 문제에 바탕을 둔 대칭형 암호 알고리즘을 위한 공개키 방식의 키 분배 알고리즘은?
❶ RSA 알고리즘
② DSA 알고리즘
③ MD-5 해쉬 알고리즘
④ Diffie-Hellman 알고리즘

3. 다음 중 유형이 다른 보안 알고리즘은?
❶ SEED 알고리즘 ② RSA 알고리즘
③ Rabin 알고리즘 ④ ECC 알고리즘

4. 다음 암호 알고리즘 중 송, 수신자가 동일한 키에 의해 암호화 및 복호화 과정을 수행하는 암호 알고리즘은?
❶ 대칭키 암호 알고리즘 ② 공개키 암호 알고리즘
③ 이중키 암호 알고리즘 ④ 해시 암호 알고리즘

5. 다음 중 불법적인 공격에 대한 데이터에 대한 보안을 유지하기 위해 요구되는 기본적인 보안 서비스로 옳지 않은 것은?
① 기밀성(Confidentiality)
② 무결성(Integrity)
③ 부인봉쇄(Non-Repudiation)
❹ 은폐성(Concealment)

6. TCSEC(Trusted Computer System Evaluation Criteria)에서 정의한 보안 등급과 설명이 일치하지 않는 것은?
① C1등급 : 사용자간에 서로 침범할 수 없게 되어 있다.
❷ A1등급 : B2의 기준을 충족시키며 추가적으로 하드웨어 자원을 포함한 보안 관리자 기능 및 위험시 스스로 탐색한다.
③ C2등급 : C1의 기준을 충족시키며, 감사와 로그 기능을 추가한다.
④ B1등급 : 등급별로 임의 접근 통제를 한다.

7. 보안 OS(Secure OS)에 대한 설명 중 가장 옳지 않은 것은?

A는 B회사의 통신망에 고의로 불법 침입하여 B회사의 컴퓨터 내부의 자료를 가져와 자료를 파괴, 변경, 장애등 혼란을 야기 시켰다.

① D1급은 보안에 대한 기능이 없는 것으로, MS-DOS 등이 이에 해당한다.
❷ C1급은 사용자의 접근제어, Auditing, Shadow Password 등의 부가적인 기능이 제공된다.
③ B급의 보안 OS는 다단계 보안을 제공하며, 필수적인 접근제어 등이 제공된다.
④ A급은 검증된 설계 수준으로서 수학적인 검증 과정이 요구된다.

8. 다음은 어떤 유형의 컴퓨터 범죄에 해당하는가?(원본 문제 오류로 정답은 1번입니다. 추후 정상적으로 복원하여 두겠습니다.
❶ 크래킹 ② 금융사기
③ 프라이버시 침해 ④ 소프트웨어 불법 복제

9. 네트워크 보안과 가장 관계가 없는 것은?
❶ 리피터 ② 방화벽
③ 개인키 ④ 공개키

10. IPSec 프로토콜에 대한 설명으로 옳지 않은 것은?
① 네트워크 계층인 IP 계층에서 보안 서비스를 제공하기 위한 보안 프로토콜이다.
❷ 기밀성 기능은 AH(Authentication Header)에 의하여 제공되고, 인증 서비스는 ESP(Encapsulating Security Payload) 에 의하여 제공된다.
③ 보안 연계(Security Association)는 사용된 인증 및 암호 알고리즘, 사용된 암호키, 알고리즘의 동작 모드, 그리고 키의 생명 주기 등을 포함한다.
④ 키 관리는 수동으로 키를 입력하는 수동방법과 IKE 프로토콜을 이용한 자동방법이 존재한다.

2과목 : 운영체제

11. Windows 2000 Server가 기본적으로 인식할 수 없는 시스템 디스크 포맷은?
① NTFS ❷ EXT2
③ FAT16 ④ FAT32

12. DHCP(Dynamic Host Configuration Protocol) 서버에서 이용할 수 있는 IP Address 할당 방법 중에서 DHCP 서버가 관리하는 IP 풀(Pool)에서 일정기간 동안 IP Address를 빌려주는 방식은?
① 수동 할당 ② 자동 할당
③ 분할 할당 ❹ 동적 할당

13. Linux 시스템에서 현재 구동 되고 있는 특정 프로세스를 종료하는 명령어는?
① halt ❷ kill
③ cut ④ grep

14. Windows 2000 Server의 기본 FTP 사이트 등록정보 설정에서 익명 연결 허용을 설정할 수 있는 탭은?
① FTP 사이트 ❷ 보안 계정
③ 메시지 ④ 홈 디렉터리

15. 다음 중 Windows 2000 Server에서 사용자 계정에 관한 옵션으로 설정할 수 없는 항목은?
❶ 로그온 할 수 있는 컴퓨터의 IP Address
② 로그온 시간제한
③ 계정 파기 날짜
④ 로그온 할 수 있는 컴퓨터 제한

16. DNS(Domain Name System) 서버를 처음 설치하고 가장 먼저 만들어야 하는 데이터베이스 레코드는?
① CNAME ② HINFO(Host Information)
③ PTR(Pointer) ❹ SOA(Start Of Authority)

17. 다음 서비스 중에서 Windows 2000 Server에 추가된 새로

운 서비스는?

❶ Active Directory ② DNS
③ DHCP ④ WINS

18. 다음 중 Windows 2000 Server 운영체제에서 이벤트를 감사할 때 감사할 수 있는 항목으로 옳지 않은 것은?

① 파일 폴더에 대한 액세스
② 사용자의 로그온과 로그오프
❸ 메모리에 상주된 프로세스의 사용 빈도
④ 액티브 디렉터리에 대한 변경 시도

19. Linux의 LILO 대신, Windows 2000 Server의 OS Loader를 이용해서 Linux를 부팅하려한다. 기존 MBR(Master Boot Record)에 설치된 LILO를 지우는 올바른 방법은?

① Linux로 부팅한 뒤 fdisk 명령을 내려 LILO를 uninstall 한다.
❷ DOS 용 Fdisk 프로그램을 이용해 fdisk /mbr 명령을 내린다.
③ hda1 파티션을 포맷시킨다.
④ LILO는 제거 되지 않으므로 fdisk로 새로 파티션 한다.

20. Linux 명령어 설명으로 옳지 않은 것은?

❶ ls : DOS의 cd와 비슷한 명령어로 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.

21. Redhat Linux 시스템의 각 디렉터리 설명 중 옳지 않은 것은?

① /usr/X11R6 : X-Window의 시스템 파일들이 위치한다.
② /usr/include : C 언어의 헤더 파일들이 위치한다.
❸ /boot : LILO 설정 파일과 같은 부팅관련 파일들이 들어있다.
④ /usr/bin : 실행 가능한 명령이 들어있다.

22. Linux의 root 암호를 잊어버려서 현재 root로 로그인을 할 수 없는 상태이다. Linux를 재설치하지 않고 root로 로그인 할 수 있는 방법은?

① 일반유저로 로그인 한 후 /etc/securetty 파일 안에 저장된 root의 암호를 읽어서 root 로 로그인 한다.
❷ LILO 프롬프트에서 [레이블명] single로 부팅한 후 passwd 명령으로 root의 암호를 변경한다.
③ 일반유저로 로그인하여서 su 명령을 이용한다.
④ 일반유저로 로그인 한 후 passwd root 명령을 내려서 root의 암호를 바꾼다.

23. Microsoft사에서 제공하는 Windows 2000 Server에서 사용하는 웹 서버는?

① RPC ❷ IIS
③ Tomcat ④ Apache

24. 다음 중 디스크의 용량을 확인하는 Linux 명령어는?

❶ df ② du
③ cp ④ mount

25. 다음 디렉터리에서 시스템에 사용되는 각종 응용 프로그램들이 설치되어 있는 것은?

❶ /usr ② /etc
③ /home ④ /root

26. 어떤 서브넷의 라우터 역활을 하고 있는 Linux 시스템에서 현재 활성화 되어있는 IP Forwarding 기능을 시스템을 리부팅하지 않고 비활성화 시키려 한다. 올바른 명령어는? (이 시스템의 커널버전은 2.2 이다.)

① echo "1" >/proc/sys/net/ipv4/ip_forward
❷ echo "0" >/proc/sys/net/ipv4/ip_forward
③ echo "1" >/proc/sys/net/conf/ip_forward
④ echo "0" >/proc/sys/net/conf/ip_forward

27. 다음 Linux 커널 버전 번호 중에서 개발 버전은?

① 2.0.2 ❷ 2.1.1
③ 2.4.16 ④ 2.6.14

28. 다음 명령어 중에서 데몬들이 커널상에서 작동되고 있는지 확인하기 위해 사용하는 것은?

① domon ② cs
③ cp ❹ ps

29. Telnet과 같은 원격 터미널 세션에서 통신을 암호화하여 중간에서 스니핑과 같은 도청을 하더라도 해석을 할 수 없도록 해주는 프로그램으로 옳지 않은 것은?

① sshd ② sshd2
③ stelnet ❹ tftp

30. Linux에 등록된 사용자들 중 특정 사용자의 Telnet 로그인만 중지시키려면 어떤 방법으로 중지해야 하는가?

① Telnet 포트를 막는다.
② /etc/hosts.deny 파일을 편집한다.
❸ Telnet 로그인을 막고자 하는 사람의 쉘을 false 로 바꾼다.
④ /etc/passwd 파일을 열어서 암호부분을 * 표시로 바꾼다.

3과목 : 네트워크

31. FDDI(Fiber Distributed Data Interface)에 대한 설명으로 옳지 않은 것은?

① 100Mbps급의 데이터 속도를 지원하며 전송 매체는 광섬유이다.
② 일차 링과 이차 링의 이중 링으로 구성된다.
③ 노드는 이중 연결국(Double Attachment Station)과 단일 연결국(Single Attachment Station)으로 구성된다.
❹ 매체 액세스 방법은 CSMA/CD 이다.

32. 24 채널을 포함하고, 신호의 속도가 1.544Mbps 인 북미 방식 신호는?

① DS-0 ❷ DS-1
③ DS-2 ④ DS-3

33. 네트워크 관리자나 라우터가 IP 프로토콜의 동작 여부를 점검하고, 호스트로의 도달 가능성을 검사하기 위한 ICMP 메

시지 종류는?

① Parameter Problem
② Timestamp Request/Response
❸ Echo Request/Response
④ Destination Unreachable

34. 네트워크 토폴로지 구성방법 중 모든 네트워크 노드를 개별 라인으로 각각 연결하며 각각의 라인을 모두 중간에서 연결 처리하는 별도의 신호를 처리하는 장치가 필요한 별모양의 네트워크 방식은?

① 메쉬(Mesh) ② 링(Ring)
③ 버스(Bus) ❹ 스타(Star)

35. 네트워크에 스위치 장비를 도입함으로서 얻어지는 효과로 가장 옳지 않은 것은?

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

36. 네트워크를 구축할 때 데이터 전송 속도를 가장 중요하게 생각할 경우 시스템 회선의 설비는?

❶ Fiber-Optic ② Thinnet
③ 등급1 UTP ④ Thicknet

37. OSL 7 Layer 중 응용 계층 간의 정보 표현 방법의 상이를 극복하기 위한 계층으로, 보안을 위한 암호화/복호화 방법과 효율적인 전송을 위한 압축 기능이 들어 있는 계층은?

① 데이터 링크 계층 ② 세션 계층
③ 네트워크 계층 ❹ 표현 계층

38. 네트워크 인터페이스 카드는 OSI 7 Layer 중 어느 계층에서 동작하는가?

❶ 물리 계층 ② 데이터 링크 계층
③ 네트워크 계층 ④ 트랜스포트 계층

39. 10.10.10.0/255.255.255.0인 사설망을 사용하는 사내 망 PC에 10.10.10.190/255.255.255.128이란 IP Address를 부여할 경우 생기는 문제점으로 올바른 것은?(단, 게이트웨이 주소는 정상적으로 설정되어 있다.)

① 해당 컴퓨터는 외부망과 통신할 수는 없지만, 내부망 통신은 원활하다.
❷ 해당 컴퓨터는 외부망 통신을 할 수 있고, 일부 내부망 컴퓨터들만 통신가능하다.
③ 해당 컴퓨터는 외부망 통신만 가능하다.
④ 해당 컴퓨터는 외부망 통신을 할 수 있고, 내부망 컴퓨터들과 원활한 통신이 가능하다.

40. 다음 프로토콜 중 계층이 다른 프로토콜은?

① ICMP(Internet Control Message Protocol)
② IP(Internet Protocol)
③ ARP(Address Resolution Protocol)
❹ TCP(Transmission Control Protocol)

41. 시간을 매체로 다중화 하는 통신방식은?

① FDM ❷ TDM
③ WDM ④ CDM

42. SNMP(Simple Network Management Protocol)에 대한 설명으로 옳지 않은 것은?

① RFC(Request For Comment) 1157에 명시되어 있다.
② 현재의 네트워크 성능, 라우팅 테이블, 네트워크를 구성하는 값들을 관리한다.
❸ TCP 세션을 사용한다.
④ 상속이 불가능하다.

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.
❹ UDP는 데이터 전송 전에 반드시 송수신 간의 세션이 먼저 수립되어야 한다.

44. TCP/IP 프로토콜에 관한 설명 중 옳지 않은 것은?

① 데이터 전송 방식을 결정하는 프로토콜로써 TCP와 UDP가 존재한다.
② TCP는 연결지향형 접속 형태를 이루고, UDP는 비 연결형 접속 형태를 이루는 전송 방식이다.
❸ DNS는 UDP만을 사용하여 통신한다.
④ IP는 TCP나 UDP형태의 데이터를 인터넷으로 라우팅하기 위한 프로토콜로 볼 수 있다.

45. TCP/IP 프로토콜을 이용해 클라이언트가 서버의 특정 포트에 접속을 하려고 할 때 서버가 해당 포트를 열고 있지 않다면 응답 패킷의 코드비트에 특정 비트를 설정한 후 보내 접근할 수 없음을 통지하게 된다. 다음 중 클라이언트가 서버의 열려있지 않은 포트에 대한 접속에 대해 서버가 보내는 응답 패킷의 코드 비트 내용이 올바른 것은?

① SYN ② ACK
③ FIN ❹ RST

4과목 : 보안

46. Windows NT 서버의 보안관리 방법 중 옳지 않은 것은?

① 방화벽 프로그램을 설치하여 서버를 보호한다.
② 사용자 그룹에 따라 서버에 접근할 수 있는 사용권한을 제한한다.
❸ 수시 및 정기적인 백업을 하여 서버 정보를 여러 클라이언트의 빈 디스크에 각각 보관하되 저장되는 클라이언트를 수시로 바꾼다.
④ 백업 도메인 컨트롤러를 설치하여 서버 정보 및 시스템 설정을 수시로 백업한다.

47. Windows 명령 프롬프트 창에서 netstat -an 을 실행한 결과이다. 옳지 않은 것은?(단, 로컬 IP Address는 211.116.233.104 이다.)

```
c:₩>netstat-an
TCP 127.0.0.1:80 127.0.0.1:1197 TIME_WAIT
TCP 127.0.0.1:80 127.0.0.1:1200 ESTABLISHED
TCP 127.0.0.1:1200 127.0.0.1:80 ESTABLISHED
TCP 211.116.233.104:139 0.0.0.0:0 LISTENING
TCP 211.116.233.104:22 211.116.233.98.22
    ESTABLISHED
TCP 211.116.233.104:23 211.116.233.124:2212
    TIME_WAIT
```

① http://localhost 로 접속하였다.

② Netbios를 사용하고 있는 컴퓨터이다.

❸ 211.116.233.124에서 Telnet 연결이 이루어져 있다.

④ 211.116.233.98로 ssh를 이용하여 연결이 이루어져 있다.

48. 프로그램이 exec()나 popen() 등을 이용하여 외부 프로그램을 실행할 때 입력되는 문자열을 여러 필드로 나눌때 기준이 되는 문자를 정의하는 변수는?

① PATH ② export

③ $1 ❹ IFS

49. root 권한 계정이 'a' 라는 파일을 지우려 했을때 나타난 결과이다. 이 파일이 왜 안 지워지는 것이며, 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.

② 현재 로그인 한 사람이 root가 아니다. root로 로그인한다.

③ chmod 명령으로 쓰기금지를 해제한다.

❹ chattr 라는 명령으로 쓰기금지를 해제한다.

50. 다음과 같은 특징이 있는 보안 툴은?

- 공격호스트로부터 finger 정보를 수집하는 것을 시도
- instant paging 지원(매분마다 갱신된 정보를 받을 수 있다.)
- 로그 파일에서 특정 상태가 발견되면 특정 명령을 실행하도록 할 수 있다.

❶ SWATCH ② PingLogger

③ LogSurfer ④ MOM

51. 다음 옵션 중에서 설명으로 올바른 것은?

① #chmod g-w : 그룹에게 쓰기 권한 부여

② #chmod g-rwx : 그룹에게 읽기, 쓰기, 실행 권한 부여

③ #chmpd a+r : 그룹에게만 읽기 권한 부여

❹ #chmod g+rw : 그룹에게 대해 읽기, 쓰기 권한 부여

52. 다음 공개된 인터넷 보안도구에 대한 설명 중 옳지 않은 것은?

❶ Tripwire : 유닉스 파일시스템의 취약점(Bug)을 점검하는 도구이다.

② Tiger : 유닉스 보안 취약점을 분석하는 도구로서 파일시스템 변조 유무도 알 수 있다.

③ TCP_Wrapper : 호스트기반 침입차단시스템, IP 필터링 등이 가능하다.

④ Gabriel : 스캔 공격을 탐지하는 도구

53. 다음 프로그램 코드에서 버퍼 오버플로우가 일어나는 이유는?

```
#include
    void main(int argc, char *argv[]) {
    char a;
    float b;
    double c;
    int *d;
    int e;
    char *f[100];
    char buffer[700];
    if(argc > 1) {
    strcpy(buffer, argv[1]);
    }
    }
```

① 버퍼의 크기가 너무 작다.

② 쉘 코드가 정교하게 숨어있다.

❸ strcpy 함수를 이용해 버퍼의 경계성 검사를 하지 않는다.

④ argv[1]의 값이 정의되지 않은 채 버퍼에 입력된다.

54. System 또는 Software의 취약점을 악용한 공격 방법은?

❶ Buffer Overflow 공격 ② IP Spoofing 공격

③ Ping Flooding 공격 ④ SYNC Flooding 공격

55. 다음 설명하는 기법은?

인터넷 프로토콜인 TCP/IP의 구조적 결함, 즉 TCP 시퀀스번호, 소스라우팅, 소스 주소를 이용한 인증(Authentication) 메커니즘 등을 이용한 방법으로써 인증(Authentication) 기능을 가지고 있는 시스템을 침입하기 위해 침입자가 사용하는 시스템을 원래의 호스트로 위장하는 방법이다.

① IP Sniffing ❷ IP Spoofing

③ Race Condition ④ Packet Filtering

56. 다음 중 서비스 거부 공격(Denial of Service)의 종류와 설명이 잘못 짝지어진 것은?

① SSPing - ICMP 패킷을 고도로 Fragment시켜 계속 전송

② Smurf - 위조된 ICMP 패킷을 브로드캐스트 주소로 전송

③ SYN Flood - 3 Way Handshake를 무시한 많은 연결을

시도

❹ Bubonic - 다수의 동일한 Fragment IP 패킷 전송

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

① SAINT ② MSCAN
③ ISS ❹ Squid

58. TCPdump 가 동작하기 위해 필요한 라이브러리는?

① ncurse ❷ libpcap
③ libmod ④ modperl

59. 인터넷 환경에서 침입차단시스템의 기능이 주로 장착되고 있는 장치는?

❶ 라우터 ② 중계기
③ 브리지 ④ ADSL 모뎀

60. 종단 간 보안 기능을 제공하기 위한 SSL 프로토콜에서 제공되는 보안 서비스로 옳지 않은 것은?

① 통신 응용간의 기밀성 서비스
② 인증서를 이용한 클라이언트와 서버의 인증
③ 메시지 무결성 서비스
❹ 클라이언트에 의한 서버 인증서를 이용한 서버 메시지의 부인방지 서비스

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