

1과목 : 정보보호개론

- 컴퓨터 바이러스 예방법에 대한 설명으로 틀린 것은?
 - 중요한 프로그램이나 자료는 항상 백업한다
 - 'autoexec.bat' 파일에는 항상 최신 버전의 컴퓨터 바이러스 예방 프로그램과 디스크 시스템 영역 저장 프로그램을 실행 시켜 놓는다.
 - 컴퓨터는 플로피디스크로만 부팅 시킨다.
 - 워드 매크로 바이러스와 관련이 있는 자동 매크로를 비활성화 시킨다.
- 방화벽 환경설정 과정에 대한 설명 중 틀린 것은?
 - 백업 및 복구 방법에 설명되어 있는대로 긴급 부트 디스크를 만든다.
 - 내부 호스트와 ISP 호스트가 방화벽으로 라우팅할 수 없도록 셋팅한다.
 - 내부 웹 서버가 있는 경우 HTTP 프록시를 설정하고 내부와 외부에서 제대로 접근이 되는지 확인한다.
 - 방화벽에서 name system을 사용하고 싶은 경우에는 DNS 설정을 해야 한다.
- 다음의 특징을 지니고 있는 방화벽은?

- 대부분의 라우터 소프트웨어의 기본 기능이므로 거의 비용이 들지 않는다.
 - 처리 속도가 빠르다.
 - OSI 7계층의 3, 4에서 처리되므로 필터링 속도가 빠르고 가격이 저렴하다.

 - 패킷 필터링 게이트웨이
 - 응용 게이트웨이
 - 서킷 게이트웨이
 - 하이브리드 게이트웨이
- 일반적인 서명문 생성을 위한 과정으로 가장 널리 이용되고 있는 것은?
 - 메시지 생성 - 메시지 압축 - 해쉬 과정 - 서명문 생성
 - 메시지 생성 - 암호문 생성 - 서명문 생성 - 해쉬 과정
 - 메시지 생성 - 해쉬 과정 - 암호문 생성 - 서명문 과정
 - 메시지 생성 - 서명문 생성 - 암호 과정 - 해쉬 과정
- 서버를 안전하게 유지하는 방법이 아닌 것은?
 - 운영체제를 정기적으로 패치하고, 데몬을 최신 버전으로 갱신하여 설치한다.
 - 불필요한 suid 프로그램을 제거한다
 - 침입차단시스템의 정책을 적절하게 적용하여 내부 자원을 보호한다.
 - 사용자의 편리성과 가용성을 위하여 시스템이 제공하는 모든 데몬들을 설치하여 사용한다.
- 안전한 전자지불 프로토콜에서 사용자가 상점으로 가는 정보와 지불게이트로 가는 정보를 암호학적으로 묶기위하여 사용하는 기법을 가장 잘 설명한 것은?
 - 이중 서명 방식(해쉬+서명)
 - 인증서 방식
 - 무결성 제공을 위한 해쉬 방식

④ 암호 방식

- 일반적으로 시스템 해킹이 일어나는 절차를 올바르게 나열한 것은?
 - 정보시스템에 잠입 - 루트권한 취득 - 백도어 설치 - 침입 흔적 삭제
 - 루트 권한 획득 - 정보시스템에 잠입 - 침입 흔적 삭제 - 백도어 설치
 - 정보시스템에 잠입 - 백도어 설치 - 루트권한 취득 - 침입 흔적 삭제
 - 루트권한 취득 - 정보시스템에 잠입 - 침입 흔적 삭제 - 백도어 설치
- 종단간 보안 기능을 제공하기 위한 SSL 프로토콜에서 제공되는 보안 서비스가 아닌 것은?
 - 통신 응용간의 기밀성 서비스
 - 인증서를 이용한 클라이언트와 서버의 인증
 - 메시지 무결성 서비스
 - 클라이언트에 의한 서버 인증서를 이용한 서버 메시지의 부인방지 서비스
- 해킹 방법들에 대한 설명 중 틀린 것은?
 - 지나가는 패킷 흐름에서 로그인, 패스워드 등을 유출하는 스니퍼(Sniffer)
 - 공격자가 다른 호스트 IP 주소를 자신의 패킷에 부착하여 보내는 공격 방법인 스푸핑(Spoofing)
 - 특정 서버의 서비스 기능을 마비하여 다른 정당한 클라이언트가 서비스를 제공받지 못하게 하는 DOS(Denial of Service)
 - 네트워크에 연결된 호스트의 이용 가능한 서비스와 포트를 조사함으로써 원격 공격자들이 공격에 이용할 수 있는 보안 취약점들을 조사하게 하는 TCP 랩퍼
- 인증 서비스를 제공하기 위한 공개키 인증서(Public-key Certificate)에 포함되어 있지 않은 내용은?
 - 가입자의 이름
 - 가입자의 전자서명 검증키(공개키)
 - 인증서의 유효기간
 - 가입자의 주민등록번호, 거주 주소, 전화번호 등의 개인 정보

2과목 : 운영체제

- 다음 중 네트워크 또는 응용을 위한 보안 대책으로 잘못 연결된 것은?
 - SSL-종단간 보안
 - PGP-안전한 전자메일
 - Single Sign On - 무선 링크 보안
 - Kerberos - 사용자 인증
- 다음중 유형이 다른 암호 알고리즘은?
 - RSA(Rivest-Shamir-Adelman)
 - AES(Advanced Signature Algorithm)
 - DSA(Digital Signature Algorithm)
 - KCDSA(Korea Certification-based Digital Signature Algorithm)

13. 전자문서의 신뢰성을 보장하기 위한 전자서명법의 주요 내용이 아닌 것은?
- ① 공인 인증기관의 지정 기준, 인증업무준칙, 인증 업무의 휴지 등에 관한 사항
 - ② 인증서의 발급, 효력 정지, 폐지에 관한 사항
 - ③ 비공인 인증기관의 지정 기준, 인증업무준칙 등의 제반 필요사항
 - ④ 전자 서명 생성키의 관리 등의 인증 업무의 안전과 신뢰성을 확보하기 위한 사항
14. 악성 프로그램에 대한 대응책으로 틀린 것은?
- ① 신규 파일을 실행하기 이전에 최신 버전의 백신 프로그램을 이용하여 검사한다.
 - ② 보안 관련 최신 정보를 항상 숙지한다.
 - ③ 백신 프로그램의 사용을 숙지하고, 정기적으로 최신 버전으로 업데이트 한다.
 - ④ 자신이 잘 알고 있는 송신자로부터 수신된 전자메일의 첨부파일은 안심하고 실행해도 무방하다.
15. 아파치 웹서버에 대하여 잘못 설명한 것은?
- ① 초기엔 유닉스 계열의 운영체제에서 동작하는 웹 서버였다.
 - ② 공개 프로그램이므로 소스 형태로 배포되기도 하며, 다양한 시스템 환경에 적합하도록 실행 가능한 형태로 배포되기도 한다.
 - ③ http.conf는 웹 서버를 위한 환경 설정 파일로써, 서비스 타입, 포트 번호, 사용자 그룹, 웹서버 관리자 전자메일 주소, 서버 루트를 지정하는 디렉토리, 에러 로그가 기록될 파일 경로 등을 포함한다.
 - ④ 설정 파일에서 웹 서버가 사용할 사용자와 그룹을 나타내는 설정 변수인 User와 Group은 'root'로 설정해야 한다.
16. Windows NT 보안 서브시스템(security sub-system)의 기능들로 짝지어진 것은?
- ① 사용자 인증 - 사용자 행동에 대한 감시 및 로그 기록 - 메모리 영역의 비인가된 접근통제
 - ② 사용자 인증 - 도메인에 존재하는 개체의 저장-사용자가 소유한 자원에 대한 접근 통제
 - ③ 사용자 인증 - 도메인에 존재하는 개체의 저장 - 시스템 정보의 저장
 - ④ 사용자 인증 - 도메인에 존재하는 개체의 저장-디렉토리의 사용 권한을 설정함
17. Windows 2000 서버에서 유지하는 중요 로그 유형에 해당하지 않은 것은?
- ① Firewall log ② Security log
 - ③ System log ④ Application log
18. Windows 2000 서버에서 보안로그에 대한 설명이 아닌 것은?
- ① 보안 이벤트의 종류는 개체 액세스 제어, 계정 관리, 계정 로그온, 권한 사용, 디렉토리 서비스, 로그온 이벤트, 시스템 이벤트, 정책 변경, 프로세스 변경 등이다.
 - ② 보안 이벤트를 남기기 위하여 감사 정책을 설정하여 누가 언제 어떤 자원을 사용했는지를 모니터링할 수 있다.
 - ③ 보안 이벤트 기록되는 정보는 이벤트가 수행된 시간과 날짜, 이벤트를 수행한 사용자, 이벤트가 발생한 소스,

이벤트의 범주 등이다.

- ④ 데이터베이스 프로그램과 전자메일 프로그램과 같은 응용 프로그램에 의해 생성된 이벤트를 포함한다.
19. 다음 중 TCP 프로토콜의 연결 설정을 위하여 '3 way handshaking'의 취약점을 이용하여 실현되는 서비스 거부 공격은 무엇인가?
- ① ping of death
 - ② 스푸핑(spoofing)
 - ③ 패킷 스니핑(packet sniffing)
 - ④ SYN flooding
20. 리눅스에서 침입차단시스템 설정에서, 외부 임의의 호스트에서 210.119.227.226으로 telnet 접속을 막는 규칙을 삽입하기 위한 올바른 iptables 명령어는 어느 것인가?
- ① /sbin/iptables -A INPUT -i eth0 -s 0/0 -d 210.119.227.226 -p tcp --dport telnet -j drop
 - ② /sbin/iptables -A OUTPUT -i eth0 -s 0/0 -d 210.119.227.226 -p tcp --dport telnet -j drop
 - ③ /sbin/iptables -A INPUT -i eth0 -s 0/0 -d 210.119.227.226 -p tcp --dport telnet -j accept
 - ④ /sbin/iptables -A OUTPUT -i eth0 -s 0/0 -d 210.119.227.226 -p tcp --dport telnet -j accept
21. 각 사용자의 가장 최근 로그인 시간을 기록하는 로그파일은?
- ① cron ② messages
 - ③ netconf ④ lastlog
22. 파일 바이러스의 진단법으로 옳바르지 않은 것은?
- ① 부팅시 몇 번 부팅하는 지를 조사한다.
 - ② 파일 실행시 속도를 검사해 본다.
 - ③ 파일 크기 증가 여부를 확인한다.
 - ④ 시스템 수행 속도를 검사한다.
23. 현재 수행되는 백그라운드 작업을 출력하는 명령어는?
- ① jobs ② kill
 - ③ ps ④ top
24. 다음 중 vi 화면 편집기 모드가 아닌 것은?
- ① 명령모드 ② 라스트라인모드
 - ③ 입력모드 ④ 변경모드
25. rpm으로 설치된 모든 패키지를 출력하는 명령어는?
- ① rpm -qa ② rpm -qf /etc/bashrc
 - ③ rpm -qi MySQL ④ rpm -e MySQL
26. 다음 중 리눅스 기본 명령어가 포함되어 있는 디렉토리는?
- ① /boot ② /etc
 - ③ /bin ④ /lib
27. 다음 중 성격이 다른 용어는?
- ① FTP(File Transfer Protocol)
 - ② SMTP(Simple File Transfer Protocol)
 - ③ HTTP(Hyper Text Transfer Protocol)
 - ④ LAN(Local Area Network)

28. 리눅스에서 네트워크 계층과 관련된 상태를 점검하기 위한 명령어와 유형이 다른 것은?
- ① ping ② traceroute
 - ③ netstat ④ nslookup
29. Windows 2000 서버에서 그룹은 글로벌 그룹, 도메인 그룹, 유니버설 그룹으로 구성되어 있다. 도메인 로컬 그룹에 대한 설명이 아닌 것은?
- ① 도메인 로컬 그룹이 생성된 도메인에 위치하는 자원에 대한 허가를 부여할 때 사용하는 그룹이다.
 - ② 내장된 도메인 로컬 그룹은 도메인 제어기에만 존재한다. 이는 도메인 제어기와 액티브 디렉토리에서 가능한 권한과 허가를 가지는 그룹이다.
 - ③ 내장된 로컬 도메인 그룹은 'administrators', 'account operators', 'server operators' 등이 있다.
 - ④ 주로 동일한 네트워크를 사용하는 사용자들을 조직하는데 사용된다.
30. 어떤 파일의 허가 모드가 -rwxr--w-- 이다. 다음 설명 중 틀린 것은?
- ① 소유자는 읽기 권한, 쓰기 권한, 실행 권한을 갖는다.
 - ② 동일한 그룹에 속한 사용자는 읽기 권한만을 갖는다.
 - ③ 다른 모든 사용자는 쓰기 권한 만을 갖는다.
 - ④ 동일한 그룹에 속한 사용자는 실행 권한을 갖는다.

3과목 : 네트워크

31. LAN의 구성 요소 중 브로드 밴드 LAN에서의 모뎀 및 베이스밴드 LAN에서 사용되는 송수신과 같이 통신망에 노드를 접속하기 위한 것은?
- ① CIU ② BIU
 - ③ MAU ④ MSU
32. 인터넷 주소 체계에 대한 설명으로 틀린 것은?
- ① 현재 인터넷 주소는 32비트로 구성되어 있다.
 - ② IP 주소는 4개의 10진수 숫자로 표기되며, 각각의 숫자는 점(Dot)으로 구분된다.
 - ③ B클래스는 전용회선을 통해 인터넷을 사용하는 일반 사용자가 갖는 형식이다.
 - ④ B클래스는 A클래스보다 규모가 작으며, 2개의 네트워크 부분(Octet)과 2개의 호스트 부분 옥텟으로 나뉜다.
33. OSI 7계층 모델에서 오류 검출 기능은 다음 중 어느 계층에서 주로 수행되는가?
- ① 물리 계층 ② 데이터 링크 계층
 - ③ 네트워크 계층 ④ 응용 계층
34. 다음 보기에서 ISO/OSI 7계층에서 트랜스포트 계층 이하인 하위 계층 프로토콜이며, 비트 방식(bit oriented)프로토콜에 해당되는 것만을 짝지어 놓은 것은?
- | | |
|--------|--------------------|
| a. BSC | b. X.25 |
| c. XNS | d. LLC(IEEE 802.2) |
- ① a, b ② b, c
 - ③ a, d ④ a, c

35. 근거리 통신망 이더넷 표준에서 이용하는 매체 액세스 제어 방법은 무엇인가?
- ① Multiple access(MA)
 - ② Carrier sense multiple access(CSMA)
 - ③ Carrier sense multiple access/collision detection(CSMA/CD)
 - ④ Token 패싱
36. 다음 중 라우터에 로그인할 수 있는 방법이 아닌 것은?
- ① TFTP ② Console
 - ③ Telnet ④ Auxiliary Port
37. 다음 중 MAC 주소를 가지고 IP주소를 알아내기 위한 프로토콜은 무엇인가?
- ① ARP ② ICMP
 - ③ BootP ④ RARP
38. 다른 호스트와 세션을 맺을 때 TCP, UDP에서 사용되는 포트번호는 무엇인가?
- ① 1-25 ② 6-17
 - ③ 1023 이상 ④ 6, 17
39. 라우터가 목적지 네트워크에 대한 경로를 알 수 있는 라우팅방법이 아닌 것은?
- ① Static ② Default
 - ③ Dynamic ④ Routing Tables
40. 다음 중 스위치의 특징으로 옳바른 것은?
- ① 스위치는 프레임의 IPX 또는 IP 주소를 기반으로 패킷을 포워딩한다.
 - ② 스위치는 패킷의 IP 주소만을 기반으로 패킷을 포워딩한다.
 - ③ 스위치는 프레임의 MAC 주소를 기반으로 패킷을 포워딩한다.
 - ④ 스위치는 프레임의 IP 주소를 기반으로 패킷을 포워딩한다.
41. 다음 중 서로 성격이 다른 프로토콜을 고른다면?
- ① TCP ② UDP
 - ③ IP ④ SNMP
42. 다음 보기 중 서비스, 포트, 프로토콜의 연결이 적당하지 않은 것은?
- ① ftp - 21 - tcp ② smtp - 25 - tcp
 - ③ dns - 53 - tcp ④ snmp - 161 - tcp
43. 네트워크 주소에 대한 설명 중 잘못된 것은?
- ① X.121 : X.25 공중네트워크에서의 주소지정 방식
 - ② D Class 주소 : 맨 앞의 네트워크 주소가 1111 으로서 멀티캐스트그룹을 위한 주소이다
 - ③ A Class 주소 : 하나의 A Class 네트워크는 16,777,216(2²⁴)개 만큼의 호스트가 존재할 수 있다
 - ④ B Class 주소 : 네트워크 주소 부분의 처음 2개의 비트는 10 이 되어야 한다.
44. 다음 프로토콜 중 가장 관계가 없는 하나는?

- ① IP ② X.25
③ X.500 ④ UDP

45. 통신 에러제어(Error Control)에서는 수신 측이 에러를 탐지하여 송신자에게 재전송을 요구하는 ARQ(Automatic Repeat Request)를 이용하게 된다. 다음 보기 중 ARQ 전략이 아닌 것은?

- ① Windowed Wait and Back ARQ
② Stop and Wait ARQ
③ Go Back N ARQ
④ Selective Repeat ARQ

4과목 : 보안

46. SET의 기술구조에 대한 설명으로 틀린 것은?

- ① SET은 기본적으로 X.509 전자증명서에 기술적인 기반을 두고 있다.
② SET에서 제공하는 인터넷에서의 안전성을 모두 암호화에 기반을 두고 있고, 이 암호화 기술은 제 3자가 해독하기가 거의 불가능하다.
③ 암호화 알고리즘에는 공개키 암호 시스템이 사용된다.
④ 이 방식은 n명이 인터넷상에서 서로 비밀통신을 할 경우 $n(n-1)/2$ 개의 키를 안전하게 관리해야 하는 문제점이 있다.

47. 공격자가 호스트의 하드웨어나 소프트웨어 등을 무력하게 만들어 호스트에서 적법한 사용자의 서비스 요구를 거부하도록 만드는 일련의 행위는?

- ① 스푸핑 ② DoS
③ 트로이목마 ④ Crack

48. 다음에 나열된 기능 중 방화벽에 해당하는 기능을 옳게 연결한 것은?

- | | |
|------------|------------|
| ㉠ 접근 제어 기능 | ㉡ 분쟁 해결 기능 |
| ㉢ 인증 기능 | ㉣ 신분 확인 기능 |
| ㉤ VPN 기능 | ㉥ 검색 기능 |

- ① ㉠, ㉡, ㉢ ② ㉠, ㉢, ㉤
③ ㉢, ㉡, ㉤ ④ ㉢, ㉤, ㉥

49. 아래의 내용이 설명하는 것은?

패킷 필터링 형태의 방화벽 기능을 관리하기 위한 도구로 패킷 헤더의 정보(프로토콜, 발신지, 목적지 등)를 토대로 패킷을 선택적으로 통과시키는 역할을 수행한다.

- ① ipconfig ② IPCHAINS
③ imap ④ inet

50. BS7799에 관한 설명 중 옳지 않은 것은 ?

- ① 1995년 영국에서 개발되었고, 호주등 여러 국가에서 이용되고 있으며, 최근 Part I이 ISO 표준으로서 등록되었다.
② Part I, Part II가 있으며, 보안관리체계에 대한 기본적인 가이드라인을 제공한다.
③ Part I은 총 10개의 기본적인 통제 항목 분야로 나뉘어지고 있으며, Part II는 총 5단계의 구축 절차를 제시한

다.

- ④ BS7799는 인터넷 및 IT분야 뿐 아니라 조직 전반적인 보안관리를 제시한다.

51. 보안OS(Secure OS)에 대한 설명 중 가장 거리가 먼 것은?

- ① D1급은 보안에 대한 기능이 없는 것으로, MS-DOS 등이 이에 해당한다.
② C1급은 사용자의 접근제어, Auditing, Shadow Password 등의 부가적인 기능이 제공된다.
③ B급의 보안OS는 다단계 보안을 제공하며, 필수적인 접근제어 등이 제공된다.
④ A급은 검증된 설계 수준으로서 수학적인 검증 과정이 요구된다.

52. 인터넷 보안 프로토콜에 대한 설명 중 옳바른 것은?

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

53. 침입탐지시스템에 대한 설명 중 옳지 않은 것은?

- ① False Negative는 감소시키고 False Positive는 증가시켜야 한다.
② 침입탐지방식으로서 Misuse Detection, Anomaly Detection 으로 나뉜다.
③ 공개된 IDS 제품으로 널리 알려진 Snort 는 Misuse Detection 기반이다.
④ NFR은 Signature Filter 방식이다.

54. 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

55. 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

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

- ① Tripwire : 유닉스 파일시스템의 취약점(bug)을 점검하는 도구이다.
② Tiger : 유닉스 보안 취약점을 분석하는 도구로서 파일시스템 변조 유무도 알 수 있다.

