2010년10월03일년 인터넷보안전문가 2급 필기시험 기출문제 답안

【1과목 : 10문제】 정보보호개론	1	2	3	4	5	6	7	8	9	10
	②	③	①	①	③	④	③	①	③	①

【2과목 : 20문제】 운영체제	11	12	13	14	15	16	17	18	19	20
	②	①	①	③	④	①	④	②	③	③
	21	22	23	24	25	26	27	28	29	30
	①	②	②	②	③	③	③	②	①	②

【3과목 : 15문제】 네트워크	31	32	33	34	35	36	37	38	39	40
	②	③	③	②	②	③	③	②	②	②
	41	42	43	44	45					
	③	③	①	③	②					

【4과목 : 15문제】 보안	46	47	48	49	50	51	52	53	54	55
	③	①	③	④	①	④	④	④	②	④
	56	57	58	59	60					
	①	③	③	③	④					

전자문제집 CBT 홈페이지 : https://www.cbtestpro.kr

최신 수정 자료와 해설(오타・오답・규정변경)은 cbtestpro.kr 웹 및 앱에서 확인하세요.

기출문제의 저작권은 출제기관에 있습니다. cbtestpro.kr 및 관련 앱에서는 편집 및 재구성 작업만 하였음을 밝힙니다.

CBT기출문제

전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!

Download on the App Store

GET IT ON Google Play

【1과목】정보보호개론 (10문제)

1. DES(Data Encryption Standard)에 대한 설명 중 옳지 않은 것은?

① 1970년대 초 IBM이 개발한 알고리즘이다.

❷ 2048 비트까지의 가변 키 크기가 지원되고 있다.

③ NIST + NSA가 개발에 참여했다.

④ 암호화 방식의 전자 코드 북과 암호 피드백으로 이루어졌다.

2. 시스템관리자가 사용자의 인증을 위한 사용자 ID 발급 시에 주의할 점으로 옳지 않은 것은?

① 시스템에 의해 식별 될 수 있는 유일한 사용자 ID를 발급해야 한다.

② 사용자 ID와 패스워드의 두 단계 인증을 하는 ID를 발급해야 한다.

❸ 일정기간 후에는 개별 사용자의 의지와는 관계 없이 사용자 ID를 변경함을 제시한다.

④ 시스템에 허용되는 접근의 종류는 반드시 제시하고 제한한다.

3. 우리나라에서 개발된 표준 암호 알고리즘으로 구성된 것은?

❶ 암호 : SEED, 해쉬 : HAS-160, 서명 : KCDSA

② 암호 : DES, 해쉬 : HAS-160, 서명 : DSS

③ 암호 : SEED, 해쉬 : MD-5, 서명 : RSA

④ 암호 : IDEA, 해쉬 : HAS-160, 서명 : DSS

4. 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. 보안의 4대 요소로 옳지 않은 것은?

① 기밀성

② 무결성

❸ 확장성

④ 인증성

6. 암호화 메커니즘에 의한 설명 중 옳지 않은 것은?

① 문서구조 : PKCS.7, PEM 또는 PGP

② 서명 알고리즘 : RSA 또는 DSA

③ 문서 축약 알고리즘 : MD2, MD5 또는 SHA

❹ 제한 모드 : RSA, In-band, Out-band, D-H Kerberos

7. 패킷 필터링의 단점으로 옳지 않은 것은?

① 현재의 필터링 도구는 모든 패킷에 대해 완벽한 필터링을 하지 못한다.

② NFS와 같은 일부 프로토콜은 패킷 필터링에 어울리지 않는다.

❸ 필터링은 클라이언트 컴퓨터에 대한 특정한 환경설정이나 사용자에 대한 훈련이 요구되지 않는다.

④ 패킷 필터링이 실패하면 거부되어야 하는 패킷을 통과시키는 경우가 많다.

8. 전자 서명문 생성 시에 이용되는 인증서에 대한 설명으로 옳지 않은 것은?

❶ 인증기관이 한번 발행하면 영원히 취소되지 않는다.

② 근본적으로 사용자의 이름과 공개키를 인증기관의 개인키로 서명한 서명문이다.

③ 주체 이름은 일반적으로 X.500 DN(Distinguished Name)형식을 갖는다.

④ 주체 이름을 대신하는 주체 대체 이름으로 사용자ID, E-mail 주소 및 IP Address, DNS이름 등을 사용한다.

9. 네트워크 또는 응용을 위한 보안 대책으로 옳지 않은 것은?

① SSL - 종단간 보안

② PGP - 안전한 전자메일

❸ Single Sign On - 무선 링크 보안

④ Kerboros - 사용자 인증

10. 이산대수 문제에 바탕을 둔 대칭형 암호 알고리즘을 위한 공개키 방식의 키 분배 알고리즘은?(오류 신고가 접수된 문제입니다. 반드시 정답과 해설을 확인하시기 바랍니다.)

❶ RSA 알고리즘

② DSA 알고리즘

③ MD-5 해쉬 알고리즘

④ Diffie-Hellman 알고리즘

【2과목】운영체제 (20문제)

11. 어떤 서브넷의 라우터 역할을 하고 있는 Linux 시스템에서 현재 활성화 되어있는 IP Forwarding 기능을 시스템 리부팅 없이 비활성화 시키려 한다. 올바른 명령어는? (이 시스템의 커널 버전은 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

12. Linux에서 사용하는 에디터 프로그램으로 옳지 않은 것은?

❶ awk

② pico

③ vi

④ emacs

13. 30GB의 하드디스크를 모두 Linux 파티션으로 사용하고자 한다. RedHat 6.0을 설치하던 중 Disk Druid에서 30GB를 "/(root)" 파티션으로 생성하려 하였으나 실패하였다. 해결방법은?

❶ 1024 실린더 내에 "/boot" 파티션을 생성하고 나머지를 "/" 로 파티션 한다.

② 1024 실린더 내에 "/kernel" 파티션을 생성하고 나머지를 "/" 로 파티션 한다.

③ 1024 실린더 내에 "/etc" 를 파티션하고 나머지를 "/" 로 파티션 한다.

④ 1024 실린더 내에 "/home" 을 파티션하고 나머지를 "/" 로 파티션 한다.

14. Linux 시스템을 곧바로 재시작 하는 명령으로 옳지 않은 것은?

① shutdown -r now

② shutdown -r 0

❸ halt

④ reboot

15. 아파치 웹서버는 access.conf를 사용하여 외부접근 제어를 한다. 각 설정에 대한 설명으로 옳지 않은 것은?

① order deny, allowallow from linux1.nycom.netdeny from alllinux1.nycom.net 부터의 연결 요구만을 허락한다.

② order deny, allowallow from linux1.mydom.net linux2.mydom.net linux3.mydom.netdeny from alllinux1.mydom.net, linux2.mydom.net, linux3.mydom.net부터의 연결 요구만을 허락한다.

③ order deny, allowallow from alldeny from hackers.annoying.nethackers.annoying.net부터의 연결 요구만을 거절한다.

❹ order mutual-failureallow from foobirds.orgdeny from linux1.foobirds.org linux2.foobirds.orgfoobirds.org에 있는 모든 호스트로부터의 연결 요구만을 허락한다.

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

❶ 네임서버 주소, DNS 서버 IP Address

② 네임서버 주소, Linux 서버 랜 카드 IP Address

③ 네임서버 주소, 홈페이지 도메인

④ 네임서버 주소, 서버 도메인

17. Linux에서 네트워크 계층과 관련된 상태를 점검하기 위한 명령어와 유형이 다른 것은?

① ping

② traceroute

③ netstat

❹ nslookup

18. Wu-FTP 서버로 FTP 서버를 운영하고 있는 시스템에서 파일의 송수신 기록이 저장되는 파일은?

① /var/log/access-log

❷ /var/log/xferlog

③ /var/log/wtmp

④ /var/log/message

19. 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
❸ syslogd
④ auth

20. NFS 서버에서 Export 된 디렉터리들을 클라이언트에서 알아보기 위해 사용하는 명령은?

① mount
② showexports
❸ showmount
④ export

21. Linux MySQL 서버를 MySQL 클라이언트 프로그램으로 연결하였다. 새 사용자를 등록하려 하는데, 등록해야하는 데이터베이스이름, 테이블이름, 등록 시 사용하는 쿼리가 알맞게 나열된 것은?

❶ mysql ,user, insert
② mysql, host, insert
③ sql, user, update
④ sql, host, update

Download on the App Store 전자문제집 CBT(App Store) :[다운로드]
GET IT ON Google Play 전자문제집 CBT(Google Play) :[다운로드]

22. Linux 시스템에서 현재 구동 되고 있는 특정 프로세스를 종료하는 명령어는?

① halt
❷ kill
③ cut
④ grep

23. 인터넷에서 도메인 이름을 IP Address로 변환하여 주는 서버는?

① NT서버
❷ DNS서버
③ 웹서버
④ 파일서버

24. 기존의 지정된 PATH 의 맨 마지막에 “/usr/local/bin” 이라는 경로를 추가하고자 한다. 올바르게 사용된 명령은?

① $PATH=$PATH:/usr/local/bin
❷ PATH=$PATH:/usr/local/bin
③ PATH=PATH:/usr/local/bin
④ PATH=/usr/local/bin

25. 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.

26. Windows 2000 Server 환경에서 그룹계정의 설명 중 옳지 않은 것은?

① User - 제한된 권한을 제공
② Administrator - 시스템에 대한 전체적인 권한을 가짐
❸ Guest - 시스템에 대한 관리 권한을 가짐
④ Guest - 부여된 권한을 수행하거나 허가된 자원에 접근

27. Linux의 기본 명령어들이 포함되어 있는 디렉터리는?

① /var
② /usr
❸ /bin
④ /etc

28. Microsoft사에서 제공하는 Windows 2000 Server에서 사용하는 웹 서버는?

① RPC
❷ IIS
③ Tomcat
④ Apache

29. Windows 2000 Server의 사용자 계정 중 해당 컴퓨터에서만 사용되는 계정으로, 하나의 시스템에서 로그온을 할 때 사용되는 계정은?

❶ 로컬 사용자 계정(Local User Account)

② 도메인 사용자 계정(Domain User Account)

③ 내장된 사용자 계정(Built-In User Account)

④ 글로벌 사용자 계정(Global User Account)

30. LILO(LInux LOader)에 대한 설명으로 옳지 않은 것은?

① LILO는 일반적으로 Distribution Package에 포함되어 있다.

❷ Floppy Disk에는 설치할 수 없다.

③ Linux 부팅 로더로 Linux 시스템의 부팅을 담당한다.

④ LILO는 보통 첫 번째 하드디스크의 MBR에 위치한다.

【3과목】 네트워크 (15문제)

31. 네트워크 아키텍쳐에 관한 설명으로 옳지 않은 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.

32. 다른 호스트와 세션을 맺을 때 TCP, UDP에서 사용되는 포트번호는?

① 1 ~ 25

② 6 ~ 17

❸ 1023 이상

④ 6, 17

33. 응용 서비스와 프로토콜 쌍이 바르게 짝지어지지 않은 것은?

① 전자메일 서비스: SMTP, POP3, IMAP

② WWW: HTTP 프로토콜

❸ 원격 접속: ARP 프로토콜

④ 파일전송: FTP

34. 홉 카운팅 기능을 제공하는 라우팅 프로토콜은?

① SNMP

❷ RIP

③ SMB

④ OSPF

35. 네트워크 주소에 대한 설명 중 옳지 않은 것은?

① X.121 : X.25 공중네트워크에서의 주소지정 방식

❷ 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 2개 비트는 10이 되어야 한다.

36. ISDN(Integrated Service Digital Network)의 설명 중 옳지 않은 것은?

① 제공되는 서비스는 베어러 서비스(Bearer Service)와 텔레 서비스(Tele Service)로 나눌 수 있다.

② 네트워크 종단 장치는 물리적이고 전기적인 종단을 제어하는 NT1과, OSI 모델의 계층 1에서 계층 3까지의 연관된 기능을 수행하는 NT2의 두 가지 종류가 있다.

❸ BRI(Basic Rate Interface)는 3개의 B(64Kbps) 채널과 하나의 D(16Kbps) 채널을 제공한다.

④ BRI의 전송 속도는 192Kbps 이고, PRI(Primary Rate Interface)의 전송속도는 북미방식의 경우 1.544Mbps 이다.

37. HDLC 프레임의 구조 순서로 올바르게 연결된 것은?

① 플래그 시퀀스 - 제어부 - 어드레스부 - 정보부 - 프레임 검사 시퀀스 - 플래그 시퀀스

② 플래그 시퀀스 - 어드레스부 - 정보부 - 제어부 - 프레임 검사 시퀀스 - 플래그 시퀀스

❸ 플래그 시퀀스 - 어드레스부 - 제어부 - 정보부 - 프레임 검사 시퀀스 - 플래그 시퀀스

④ 제어부 - 정보부 - 어드레스부 - 제어부 - 프레임 검사 시퀀스 - 플래그 시퀀스

38. OSI 7 Layer 중에서 IEEE802 규약으로 표준화되어 있는 계층은?

① Session Layer
❷ Physical Layer
③ Network Layer
④ Transport Layer

39. Fast Ethernet의 주요 토폴로지로 올바른 것은?

① Bus 방식
❷ Star 방식
③ Cascade 방식
④ Tri 방식

40. 인터넷에 접속된 호스트들은 인터넷 주소에 의해서 식별되지만 실질적인 통신은 물리적인 MAC Address를 얻어야 통신이 가능하다. 이를 위해 인터넷 주소를 물리적인 MAC Address로 변경해 주는 프로토콜은?

① IP(Internet Protocol)
❷ ARP(Address Resolution Protocol)
③ DHCP(Dynamic Host Configuration Protocol)
④ RIP(Routing Information Protocol)

41. IP Address의 부족과 Mobile IP Address 구현문제로 차세대 IP Address인 IPv6가 있다. IPv6는 몇 비트의 Address 필드를 가지고 있는가?

① 32 비트
② 64 비트
❸ 128 비트
④ 256 비트

42. ISO/OSI 7 Layer에서 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
❸ a, d
④ a, c

43. 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

44. TCP/IP Sequence Number(순서 번호)가 시간에 비례하여 증가하는 운영체제는?

① HP-UX
② Linux 2.2
❸ Microsoft Windows
④ AIX

45. “10.10.10.0/255.255.255.0”인 사설망을 사용하는 사내 망 PC에 “10.10.10.190/255.255.255.128”이란 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.

【4과목】 보안 (15문제)

46. IP Spoofing의 과정 중 포함되지 않는 것은?

① 공격자의 호스트로부터 신뢰받는 호스트에 SYN-Flooding 공격으로 상대방 호스트를 무력화 시킨다.
② 신뢰받는 호스트와 공격하려던 타겟호스트간의 패킷교환 순서를 알아본다.
❸ 신뢰받는 호스트에서 타겟호스트로 가는 패킷을 차단하기 위해 타겟호스트에 Flooding 과 같은 공격을 시도한다.
④ 패킷교환 패턴을 파악한 후 신뢰받는 호스트에서 보낸 패킷처럼 위장하여 타겟호스트에 패킷을 보낸다.

47. 웹 해킹의 한 종류인 SQL Injection 공격은 조작된 SQL 질의를 통하여 공격자가 원하는 SQL구문을 실행하는 기법이다. 이를 예방하기 위한 방법으로 옳지 않은 것은?

❶ 에러 감시와 분석을 위해 SQL 에러 메시지를 웹상에 상세히 출력한다.

② 입력 값에 대한 검증을 실시한다.

③ SQL 구문에 영향을 미칠 수 있는 입력 값은 적절하게 변환한다.

④ SQL 및 스크립트 언어 인터프리터를 최신 버전으로 유지한다.

48. IIS를 통하여 Web 서비스를 하던 중 .asp 코드가 외부 사용자에 의하여 소스코드가 유출되는 버그가 발생하였다. 기본적으로 취해야 할 사항으로 옳지 않은 것은?

① 중요 파일(global.asa 등)의 퍼미션을 변경 혹은 파일수정을 통하여 외부로부터의 정보유출 가능성을 제거한다.

② .asp의 권한을 실행권한만 부여한다.

❸ C:\WINNT\System32\inetsrv\asp.dll에 매칭되어 있는 .asp를 제거한다.

④ .asp가 위치한 디렉터리와 파일에서 Read 권한을 제거한다.

49. SSL(Secure Socket Layer)의 설명 중 옳지 않은 것은?

① 두 개의 응용 계층사이에 안전한 데이터의 교환을 위한 종단 간 보안 프로토콜이다.

② 응용 계층과 전송 계층 사이에 존재한다.

③ Handshake 프로토콜, Change Cipher Spec 프로토콜, Alert 프로토콜, 그리고 레코드 프로토콜로 구분될 수 있다.

❹ 레코드 계층의 데이터 처리 순서는 데이터 압축 - 데이터 암호화 - 인증코드 삽입 순으로 진행된다.

50. 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

51. Windows 2000 Server에서 보안 로그에 대한 설명으로 옳지 않은 것은?

① 보안 이벤트의 종류는 개체 액세스 제어, 계정 관리, 계정 로그온, 권한 사용, 디렉터리 서비스, 로그온 이벤트, 시스템 이벤트, 정책 변경, 프로세스 변경 등이다.

② 보안 이벤트를 남기기 위하여 감사 정책을 설정하여 누가 언제 어떤 자원을 사용했는지를 모니터링 할 수 있다.

③ 보안 이벤트에 기록되는 정보는 이벤트가 수행된 시간과 날짜, 이벤트를 수행한 사용자, 이벤트가 발생한 소스, 이벤트의 범주 등이다.

❹ 데이터베이스 프로그램이나 전자메일 프로그램과 같은 응용 프로그램에 의해 생성된 이벤트를 모두 포함한다.

52. TCP_Wrapper의 기능으로 옳지 않은 것은?

① inetd에 의하여 시작되는 TCP 서비스들을 보호하는 프로그램으로써 inetd가 서비스를 호출할 때 연결 요청을 평가하고 그 연결이 규칙에 적합한 정당한 요청인지를 판단하여 받아들일지 여부를 결정한다.

② 연결 로깅과 네트워크 접근제어의 주요 기능을 주로 수행한다.

③ TCP_Wrapper 설정 점검 명령어는 tcpdchk와 tcpmatch등이 있다.

❹ iptables이나 ipchains 명령을 이용하여 설정된다.

53. 암호와 프로토콜 중에서 서버와 클라이언트 간의 인증으로 RSA방식과 X.509를 사용하고 실제 암호화된 정보는 새로운 암호화 소캣채널을 통해 전송하는 방식은?

① S-HTTP

② DES

③ FV

❹ SSL

54. 인터넷 공격 방법 중 성격이 다른 것은?

① TCP Session Hijacking Attack

❷ Race Condition Attack

③ SYN Flooding Attack

④ IP Spoofing Attack

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

① PATH

② export

③ $1

❹ IFS

56. System 또는 Software의 취약점을 악용한 공격 방법은?

❶ Buffer Overflow 공격

② IP Spoofing 공격

③ Ping Flooding 공격

④ SYNC Flooding 공격

57. 유닉스의 로그에 대한 설명 중 옳지 않은 것은?

① syslog : 시스템 정보, 트랩된 커널과 시스템 메시지, /var/adm/messages에 기록

② pacct : 사용자가 실행한 모든 명령어 및 자원 사용현황으로서, /var/adm/pacct에 기록

❸ wtmp : 현재 로그인한 사용자 현황, /var/adm/wtmp에 기록

④ sulog : 모든 su 명령어의 사용기록, /var/adm/sulog에 기록

58. SSL(Secure Socket Layer)에 관한 설명으로 옳지 않은 것은?

① 서버 인증, 클라이언트 인증, 기밀성 보장의 세 가지 서비스를 제공한다.

② SSL 프로토콜은 SSL Hand Shake 프로토콜과 SSL Record 프로토콜로 나뉜다.

❸ SSL Record 프로토콜은 서버·클라이언트 인증 기능과 암호 통신에 사용할 대칭키를 분배하는 역할을 수행한다.

④ 데이터 암호화를 위한 비밀키를 Hand Shake 프로토콜 단계에서 정한 후에 키를 사용하여 암호화된 메시지로 상대방의 신원을 증명할 수 있다.

59. SSI(Server-Side Includes)의 기능으로 옳지 않은 것은?

① 접속한 현재 날짜와 시간을 출력한다.

② cgi를 실행시킬 수가 있다.

❸ 파이어월(Firewall) 기능이 있다.

④ 파이어월(Firewall) 기능이 없다.

60. 암호 프로토콜로 옳지 않은 것은?

① 키 교환 프로토콜

② 디지털 서명

③ 전자 화폐

❹ 비밀키 암호