2019년04월14일년 인터넷보안전문가 2급 필기시험 기출문제 답안

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

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

【3과목 : 15문제】 네트워크	31	32	33	34	35	36	37	38	39	40
	③	③	③	③	④	①	②	④	②	②
	41	42	43	44	45					
	④	①	③	③	③					

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

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. 다음 중 유형이 다른 보안 알고리즘은?

❶ SEED 알고리즘
② RSA 알고리즘
③ Rabin 알고리즘
④ ECC 알고리즘

2. 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

3. 전자서명이 가지고 있어야 할 특성으로 거리가 먼 것은?

① 위조 불가
② 변경 불가
❸ 재사용 가능
④ 서명자 인증

4. IPSec 프로토콜에 대한 설명으로 옳지 않은 것은?

① 네트워크 계층인 IP 계층에서 보안 서비스를 제공하기 위한 보안 프로토콜이다.
② IP 스푸핑(Spoofing)이나 IP 스니핑(Sniffing)을 방지할 수 있다.
③ 인증, 무결성, 접근제어, 기밀성, 재전송 방지 등의 서비스를 제공한다.
❹ 키 관리는 수동으로 키를 입력하는 수동방법(Manual)만이 존재한다.

5. 전자 상거래의 보안이 중요시되고 있는 현시점에서 은행 카드 사용자에게 안전한 상거래를 할 수 있도록 보장해 주는 보안 프로토콜은?

① SSL
❷ SET
③ PEM
④ PGP

6. 불법적인 공격에 대한 데이터 보안을 유지하기 위해 요구되는 기본적인 보안 서비스로 옳지 않은 것은?

① 기밀성(Confidentiality)
② 무결성(Integrity)
③ 부인봉쇄(Non-Repudiation)
❹ 은폐성(Concealment)

7. 서버를 안전하게 유지하는 방법으로 옳지 않은 것은?

① 운영체제를 정기적으로 패치하고, 데몬을 최신 버전으로 갱신하여 설치한다.
② 불필요한 SUID 프로그램을 제거한다.
③ 침입차단시스템의 정책을 적절하게 적용하여 내부 자원을 보호한다.
❹ 사용자의 편리성과 가용성을 위하여 시스템이 제공하는 모든 데몬들을 설치하여 사용한다.

8. 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 미국표준기술연구소(NIST)에 의해 암호화 표준으로 결정됐다.
④ 암호화 방식의 전자 코드 북과 암호 피드백으로 이루어졌다.

9. 응용계층 프로토콜로 옳지 않은 것은?

① SMTP
② FTP
③ Telnet
❹ TCP

10. 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 관계없이 사용자 ID를 변경함을 제시한다.
④ 시스템에 허용되는 접근의 종류는 반드시 제시해야 한다.

【2과목】 운영체제 (20문제)

11. Linux의 VI 편집기에서 수정하던 파일을 저장하지 않고 종료시키는 명령은?

❶ :q!
② :w!
③ :WQ!
④ :Wq!

12. '/data' 라는 디렉터리는 40개의 텍스트 파일과 2개의 디렉터리가 들어있는 상태이다. root 유저로 로그인 한 후 alias 목록을 확인한 결과 alias rm='rm -i' 라고 지정되어 있었다. root 유저가 이 data 라는 디렉터리를 확인 메시지 없이 한 번에 지우려면 다음 중 어떤 명령을 내려야 하는가?

① rm data
② rm -r data
③ rm –f data
❹ rm -rf data

13. Linux 시스템에서 현재 구동되고 있는 특정 프로세스를 종료하는 명령어는?

① halt
❷ kill
③ cut
④ grep

14. 인터넷에서 도메인 이름을 IP Address로 변환하여 주는 서버는?

① NT서버
❷ DNS서버
③ 웹서버
④ 파일서버

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

① halt
❷ reboot
③ restart
④ poweroff

16. Linux의 기본 명령어들이 포함되어 있는 디렉터리는?

① /var
② /usr
❸ /bin
④ /etc

17. 파일의 허가 모드가 '-rwxr---w-'이다. 다음 설명 중 옳지 않은 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.
❹ 동일한 그룹에 속한 사용자는 실행 권한을 갖는다.

18. Linux 시스템에서 다음의 역할을 수행하는 데몬은?

> 시스템에서 여러 가지 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

19. Windows Server에서 제공하고 있는 VPN 프로토콜인 L2TP(Layer Two Tunneling Protocol)에 대한 설명 중 옳지 않은 것은?

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

20. Linux에서 root 유저로 로그인 한 후 'cp -rf /etc/* ~/temp' 라는 명령으로 복사를 하였는데, 여기서 '~' 문자가 의미하는 뜻은?

① /home 디렉터리
② /root 디렉터리
❸ root 유저의 home 디렉터리
④ 현재 디렉터리의 하위라는 의미

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

① 파일의 접근허가 모드

② 파일 이름

③ 소유자명, 그룹명

❹ 파일의 소유권이 변경된 시간

22. 현재 Linux 서버에 접속된 모든 사용자에게 메시지를 전송하는 명령은?

❶ wall

② message

③ broadcast

④ bc

23. 커널의 대표적인 기능으로 옳지 않은 것은?

① 파일 관리

② 기억장치 관리

❸ 명령어 처리

④ 프로세스 관리

24. Linux에서 su 명령의 사용자 퍼미션을 확인한 결과 'rws' 이다. 아래와 같이 사용자 퍼미션에 's' 라는 속성을 부여하기 위한 명령어는?

```
[root@vs1 /bin]# ls -l su

-rwsr-xr-x 1 root root  14124 Aug 18  1999 su
```

① chmod 755 su

② chmod 0755 su

❸ chmod 4755 su

④ chmod 6755 su

25. 아파치 데몬으로 웹서버를 운영하고자 할 때 반드시 선택해야 하는 데몬은?

❶ httpd

② dhcpd

③ webd

④ mysqld

26. IIS 웹 서버를 설치한 다음에는 기본 웹사이트 등록정보를 수정하여야 한다. 웹사이트에 접속하는 동시 접속자수를 제한하려고 할때 어느 부분을 수정해야 하는가?

① 성능 탭

❷ 연결 수 제한

③ 연결 시간 제한

④ 문서 탭

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

① domon

② cs

③ cp

❹ ps

28. 다음 중 Windows 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

29. 삼바서버의 설정파일 안에 보면 'Interfaces = 192.168.1.1/24' 라고 표현되는 부분이 있다. 여기서 '/24' 는 서브넷 마스크를 의미하는데, 다음 중 서브넷 마스크의 해석으로 옳지 않은 것은?

① 255.255.255.192 = /26

② 255.255.255.128 = /25

❸ 255.255.255.248 = /30

④ 255.255.255.0 = /24

30. DHCP(Dynamic Host Configuration Protocol) Scope 범위 혹은 주소 풀(Address Pool)을 만드는데 주의할 점에 속하지 않는 것은?(오류 신고가 접수된 문제입니다. 반드시 정답과 해설을 확인하시기 바랍니다.)

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.

❹ 하나의 서브넷에는 여러 개의 DHCP 범위가 사용될 수 있다.

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

【3과목】 네트워크 (15문제)

31. 인터넷 IPv4 주소는 Class, NetworkID, HostID 부분으로 구성되어 있다. '203.249.114.2'가 속한 Class는?

① A Class
② B Class
❸ C Class
④ D Class

32. 전송을 받는 개체 발송지에서 오는 데이터의 양이나 속도를 제한하는 프로토콜의 기능은?

① 에러제어
② 순서제어
❸ 흐름제어
④ 접속제어

33. IPv6 프로토콜의 구조는?

① 32bit
② 64bit
❸ 128bit
④ 256bit

34. OSI 7 Layer에서 암호/복호, 인증, 압축 등의 기능이 수행되는 계층은?

① Transport Layer
② Datalink Layer
❸ Presentation Layer
④ Application Layer

35. 다음의 매체 방식은?

- 현재의 네트워크 사용여부를 점검한다.
- 만약에 네트워크가 대기 중이면 바로 패킷을 전송한다.
- 이때 패킷이 충돌하게 되면 노드는 충돌신호를 전송한 후 설정된 시간만큼 기다린 후 다시 전송된다.

① Token Passing
② Demand Priority
③ CSMA/CA
❹ CSMA/CD

36. TCP 헤더 필드의 내용으로 옳지 않은 것은?

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

37. 자신의 물리 주소(MAC Address)를 알고 있으나 IP Address를 모르는 디스크가 없는 호스트를 위한 프로토콜로서, 자신의 IP Address를 모르는 호스트가 요청 메시지를 브로드 캐스팅하고, 이의 관계를 알고 있는 서버가 응답 메시지에 IP 주소를 되돌려 주는 프로토콜은?

① ARP(Address Resolution Protocol)
❷ RARP(Reverse Address Resolution Protocol)
③ ICMP(Internet Control Message Protocol)
④ IGMP(Internet Group Management Protocol)

38. 다음 프로토콜 중 OSI 7 Layer 계층이 다른 프로토콜은?

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

39. 홉 카운팅 기능을 제공하는 라우팅 프로토콜은?

① SNMP
❷ RIP
③ SMB
④ OSPF

40. 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 'netstat'으로 상태를 확인하였을 때 나타나는 메시지는?

① SYN_PCVD

❷ ESTABLISHED

③ CLOSE_WAIT

④ CONNECTED

41. TCP/IP 프로토콜을 이용해 클라이언트가 서버의 특정 포트에 접속하려고 할 때 서버가 해당 포트를 열고 있지 않다면 응답 패킷의 코드 비트에 특정 비트를 설정한 후 보내 접근할 수 없음을 통지하게 된다. 다음 중 연결 문제 등의 상황 처리를 위한 특별한 초기화용 제어 비트는?

① SYN

② ACK

③ FIN

❹ RST

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

❶ 물리 계층

② 세션 계층

③ 네트워크 계층

④ 트랜스포트 계층

43. TCP 포트 중 25번 포트가 하는 일반적인 역할은?

① Telnet

② FTP

❸ SMTP

④ SNMP

44. Star Topology에 대한 설명 중 올바른 것은?

① 시작점과 끝점이 존재하지 않는 폐쇄 순환형 토폴로지이다.

② 모든 노드들에 대해 간선으로 연결한 형태이다.

❸ 연결된 PC 중 하나가 다운되어도 전체 네트워크 기능은 수행된다.

④ 라인의 양쪽 끝에 터미네이터를 연결해 주어야 한다.

45. 방화벽에서 내부 사용자들이 외부 FTP에 자료를 전송하는 것을 막고자 한다. 외부 FTP에 Login 은 허용하되, 자료전송만 막으려면 몇 번 포트를 필터링 해야 하는가?

① 23

② 21

❸ 20

④ 25

【4과목】 보안 (15문제)

46. HTTP Session Hijacking 공격 방법으로 옳지 않은 것은?

① 공격자는 Session을 가로 채기 위해 웹 서버와 웹 클라이언트의 트래픽을 직접적으로 Sniffing하는 방법

② 웹 서버 상에 공격 코드를 삽입하고 사용자의 실행을 기다리는 방법

③ Session ID 값을 무작위 추측 대입(Brute-Force Guessing)함으로써 공격하는 방법

❹ 웹 서버의 서비스를 중단 시키고, 공격자가 서버에 도착하는 모든 패킷을 가로채는 방법

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

❶ SSL에서는 키 교환 방법으로 Diffie_Hellman 키 교환 방법만을 이용한다.

② SSL에는 Handshake 프로토콜에 의하여 생성되는 세션과 등위간의 연결을 나타내는 연결이 존재한다.

③ SSL에서 Handshake 프로토콜은 서버와 클라이언트가 서로 인증하고 암호화 MAC 키를 교환하기 위한 프로토콜이다.

④ SSL 레코드 계층은 분할, 압축, MAC 부가, 암호 등의 기능을 갖는다.

49. 다음에서 설명하는 것은?

> %d, %f, %c, %s, %x, %p 등과 같이 정형화된 문자열은 printf(), sprintf(), vprintf()등에 쓸때 printf('%d',i)처럼 변수와 같이 쓰이면 변수값을 일정한 형태로 출력하는 기능을 하지만 printf('%x')처럼 변수없이 쓰게 되면 메모리의 값들을 순서대로 출력하게 되므로 메모리 구조를 파악할 수 있게 되는 문제점이 있다.

① Sniffing

② IP Spoofing

③ Race Condition

❹ Format String Bug

50. SYN 플러딩 공격에 대한 설명으로 올바른 것은?

❶ TCP 프로토콜의 3-way handshaking 방식을 이용한 접속의 문제점을 이용하는 방식으로, IP 스푸핑 공격을 위한 사전 준비 단계에서 이용되는 공격이며, 서버가 클라이언트로부터 과도한 접속 요구를 받아 이를 처리하기 위한 구조인 백로그(backlog)가 한계에 이르러 다른 클라이언트로부터 오는 새로운 연결 요청을 받을 수 없게 하는 공격이다.

② 함수의 지역 변수에 매개변수를 복사할 때 길이를 확인하지 않은 특성을 이용하는 공격 방법이다.

③ 네트워크에 연결된 호스트들의 이용 가능한 서비스와 포트를 조사하여 보안 취약점을 조사하기 위한 공격방법이다.

④ 패킷을 전송할 때 암호화하여 전송하는 보안 도구이다.

51. 네트워크 취약성 공격으로 옳지 않은 것은?

① Scan 공격

② IP Spoofing 공격

③ UDP 공격

❹ Tripwire 공격

52. 다음 빈칸 [ ]에 들어갈 용어는?

> 사용자가 원격 호스트에서 접속하여 ftp나 telnet 서비스를 이용할 경우, 데이터는 암호화되지 않는 상태로 전송된다. 이러한 데이터는 네트워크상에서 제3자의 네트워크 패킷도청에 그대로 노출된다. 즉, 제3자는 귀중한 데이터나 패스워드를 쉽게 얻을 수 있다. [ ]은/는 원격호스트로 전송되는 데이터를 Triple DES, IDEA나 RSA로 암호화함으로서 제3자의 네트워크 패킷도청으로부터 데이터를 보호한다.

① SSL(Secure Socket Layer)

② Nessus

③ HostSentry

❹ SSH(Secure Shell)

53. PGP(Pretty Good Privacy)에서 지원하지 못하는 기능은?

① 메시지 인증(Message Integrity) : 전송도중에 내용이 불법적으로 변경되었는가를 확인해 주는 기능

② 사용자 인증(User Authentication) : 메일을 실제로 보낸 사람이 송신자라고 주장한 사람과 일치하는 가를 확인해 주는 기능

③ 송신부인방지(Nonrepudiation of Origin) : 송신자가 메일을 송신하고서 송신하지 않았다고 주장하는 경우, 이를 확인해 주는 기능

❹ 수신부인방지(Non-deniability of receipt) : 메일을 수신하고서 나중에 받지 않았다고 주장하지 못하게 해주는 기능

54. 대형 응용 프로그램을 개발하면서 전체 시험실행을 할 때 발견되는 오류를 쉽게 해결하거나 처음부터 중간에 내용을 볼 수 있는 부정루틴을 삽입해 컴퓨터의 정비나 유지 보수를 핑계 삼아 컴퓨터 내부의 자료를 뽑아가는 해킹 행위는?

❶ Trap Door

② Asynchronous Attacks

③ Super Zapping

④ Salami Techniques

55. IP 스푸핑 공격에 대한 설명으로 옳지 않은 것은?

① 공격자가 자신으로부터 전송되는 패킷에 다른 호스트의 IP 주소를 담아서 전송하는 공격 방법이다.

② 이 공격은 TCP 세그먼트의 일련번호를 예측 여부에 따라서 Non-Blinding IP 스푸핑 공격과 Blinding IP 스푸핑 공격으로 분류될 수 있다.

③ IP 스푸핑 공격의 주요 요소는 공격 호스트, 공격에 이용되는 호스트, 그리고 공격당하는 호스트로 이루어진다.

❹ 모든 운영체제는 64K 법칙을 이용하여 순서번호를 생성하므로 이 공격에 매우 취약하다.

56. 서비스 거부 공격(Denial of Service)의 특징으로 옳지 않은 것은?

❶ 공격을 통해 시스템의 정보를 몰래 빼내가거나, 루트 권한을 획득할 수 있다.

② 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다.

③ 다수의 시스템을 통한 DoS 공격을 DDoS(Distributed DoS)라고 한다.

④ 라우터, 웹, 전자 우편, DNS 서버 등 모든 네트워크 장비를 대상으로 이루어질 수 있다.

57. 근거리통신망에서 NIC(Network Interface Card) 카드를 Promiscuous 모드로 설정하여 지나가는 프레임을 모두 읽음으로써 다른 사람의 정보를 가로채기 위한 공격 방법은?

❶ 스니핑

② IP 스푸핑

③ TCP wrapper

④ ipchain

58. 방화벽의 주요 기능으로 옳지 않은 것은?

① 접근제어

② 사용자 인증

③ 로깅

❹ 프라이버시 보호

59. 다음 사용자 중 Windows Server 시스템상의 백업과 복구능력을 지닌 소유자는?

(계정 : 소속그룹)
ㄱ. Sharp : administrator
ㄴ. Kelley : backup operators
ㄷ. Wan : power users
ㄹ. Shell : users, guest

① ㄱ,ㄴ,ㄷ,ㄹ

② ㄱ,ㄴ,ㄷ

③ ㄱ,ㄴ,ㄹ

❹ ㄱ,ㄴ

60. 버퍼 오버플로우(Buffer Overflow)의 설명으로 옳지 않은 것은?

① 지정된 버퍼(Buffer)의 크기보다 더 많은 데이터를 입력해서 프로그램이 비정상적으로 동작하도록 만드는 것을 의미함

❷ 대부분의 경우 버퍼가 오버플로우 되면 프로그램이 비정상적으로 종료되면서 루트 권한을 획득할 수 있음

③ 버퍼가 오버플로우 되는 순간에 사용자가 원하는 임의의 명령어를 수행시킬 수 있음

④ 버퍼 오버플로우를 방지하기 위해서는 시스템에 최신 패치를 유지해야 함