

2022년04월10일년 인터넷보안전문가 2급 필기시험 기출문제 답안

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



전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!



【1과목】 정보보호개론 (10문제)

1. IPSec을 위한 보안 연계(Security Association)가 포함하는 파라미터들로만 짚지어진 것은?

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

- IPSec 프로토콜 모드(터널, 트랜스포트)/ 인증 알고리즘,
- ④ 인증 키, 수명 등의 AH 관련 정보/ 암호 알고리즘, 암호키, 수명 등의 ESP 관련 정보

2. 다음 중 대표적인 공개키 암호화 알고리즘은?

- ① DES
- ② IDEA
- ③ RSA
- ④ RC5

3. 공격 유형 중 마치 다른 송신자로부터 정보가 수신된 것처럼 꾸미는 것으로, 시스템에 불법적으로 접근하여 오류의 정보를 정확한 정보인 것처럼 속이는 행위를 뜻하는 것은?

- ① 차단(Interruption)
- ② 위조(Fabrication)
- ③ 변조(Modification)
- ④ 가로채기(Interception)

4. 암호 알고리즘에 대한 설명 중 가장 옳지 않은 것은?

- ① 관용키 알고리즘, 공개키 알고리즘으로 나눈다.
- ② 관용키 알고리즘은 비밀키, 대칭키라고도 하며, 블록(Block)형, 시리얼(Serial)형이 있다.
- ③ 보통 관용키 방식은 속도가 빠르지만 비도는 낮은 편이라고 볼 수 있다.
- ④ 공개키 방식은 속도는 느리지만 비도는 높은 편이라고 볼 수 있다.

5. 이산대수 문제에 바탕을 두며 인증메시지에 비밀 세션키를 포함하여 전달할 필요가 없고 공개키 암호화 방식의 시초가 된 키 분배 알고리즘은?

- ① RSA 알고리즘
- ② DSA 알고리즘
- ③ MD-5 해쉬 알고리즘
- ④ Diffie-Hellman 알고리즘

6. S-HTTP(Secure Hypertext Transfer Protocol)에 관한 설명 중 옳지 않은 것은?

- ① 클라이언트와 서버에서 행해지는 암호화 동작이 동일하다.
- ② PEM, PGP 등과 같은 여러 암호 메커니즘에 사용되는 다양한 암호문 형태를 지원한다.
- 클라이언트의 공개키를 요구하지 않으므로 사용자 개인
- ③ 의 공개키를 선언해 놓지 않고 사적인 트랜잭션을 시도할 수 있다.

- ④ S-HTTP를 탑재하지 않은 시스템과 통신이 어렵다.

7. 네트워크상의 부당한 피해라고 볼 수 없는 것은?

- ① 침입자가 부당한 방법으로 호스트의 패스워드 정보를 입수한 후 유용한 정보를 가져가는 경우
- 특정인이나 특정 단체가 고의로 호스트에 대량의 패킷을
- ② 흘려 보내 호스트를 마비시키거나 패킷 루프와 같은 상태가 되게 하는 경우
- 특정인이나 특정 단체가 네트워크상의 흐르는 데이터 패
- ③ 킷을 가로채 내거나 다른 불법 패킷으로 바꾸어 보내는 경우

- ④ HTTP 프로토콜을 이용하여 호스트의 80번 포트로 접근하여 HTML 문서의 헤더 정보를 가져오는 경우

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

- ① 기밀성(Confidentiality)
- ② 무결성(Integrity)
- ③ 부인봉쇄(Non-Repudiation)
- ④ 은폐성(Concealment)

9. 보안과 관련된 용어의 정의나 설명으로 옳지 않은 것은?

① 프락시 서버(Proxy Server) - 내부 클라이언트를 대신하여 외부의 서버에 대해 행동하는 프로그램 서버

패킷(Packet) - 인터넷이나 네트워크상에서 데이터 전송을 위해 처리되는 기본 단위로 모든 인터페이스에서 항상 16KB의 단위로 처리

③ 이중 네트워크 호스트(Dual-Homed Host) - 최소한 두 개의 네트워크 인터페이스를 가진 범용 컴퓨터 시스템

④ 호스트(Host) - 네트워크에 연결된 컴퓨터 시스템

10. 인적자원에 대한 보안 위협을 최소화하기 위한 방법으로 옳지 않은 것은?

기밀 정보를 열람해야 하는 경우에는 반드시 정보 담당자 한 명에게만 전달시키고 폐쇄된 곳에서 정보를 열람 시켜 정보 유출을 최대한 방지한다.

기밀 정보를 처리할 때는 정보를 부분별로 나누어 여러 명에게 나누어 업무를 처리하게 함으로서, 전체 정보를 알 수 없게 한다.

보안 관련 직책이나 서버 운영 관리자는 순환 보직제를 실시하여 장기 담당으로 인한 정보 변조나 유출을 막는다.

④ 프로그래머가 운영자의 직책을 중임하게 하거나 불필요한 외부 인력과의 접촉을 최소화 한다.

【2과목】 운영체제 (20문제)

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

① domon

② cs

③ cp

④ ps

12. 다음이 설명하는 Linux 시스템의 데몬은?

사용자가 지정한 프로그램을 특정 시간에 주기적으로 실행할 수 있도록 해주는 데몬

① crond

② atd

③ gpm

④ amd

13. 다음 디렉터리에서 각종 라이브러리들에 관한 파일들이 설치되어 있는 것은?

① /etc

② /lib

③ /root

④ /home

14. 다음 명령어 중에서 시스템의 메모리 상태를 보여주는 명령어는?

① mkfs

② free

③ ps

④ shutdown

15. 다음 Linux 명령어 중에서 해당 사이트와의 통신 상태를 점검할 때 사용하는 명령어는?

① who

② w

③ finger

④ ping

16. Linux에서 현재 위치한 디렉터리를 표시해 주는 명령어는?

① mkdir

② pwd

③ du

④ df

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

① ping

② traceroute

③ netstat

④ nslookup

18. 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.

④ 동일한 그룹에 속한 사용자는 실행 권한을 갖는다.

19. Linux 시스템의 shadow 파일 내용에 대한 설명으로 올바른 것은?

```
Root:$1$szfVKcHi$dEFUonrDJZ2ZG0Puqq9yK0:11458:0:99999:7:::
adm:!:11458:0:99999:7:::
lp:!:11458:0:99999:7:::
named:!:11458:0:99999:7:::
gdm:!:11458:0:99999:7:::
```

① lp에서 '*'은 로그인 셸을 갖고 있으며, 시스템에 누구나 로그인할 수 있음을 의미한다.

② gdm에서 '!!'은 로그인 셸을 갖고 있지만 누구도 계정을 통해서 로그인할 수 없도록 계정이 잠금 상태라는 것을 의미한다.

③ 로그인 계정이 아닌 시스템 계정은 named와 gdm 이다.

④ root의 암호는 11458 이다.

20. Linux 시스템이 부팅될 때 나오는 메시지가 저장된 로그 파일의 경로와 명칭으로 올바른 것은?

① /var/log/boot

② /var/log/dmesg

③ /var/log/message

④ /var/log/secure

21. VI(Visual Interface) 에디터에서 편집행의 줄번호를 출력해주는 명령은?

① :set nobu

② :set nu

③ :set nonu

④ :set showno

22. 이미 내린 shutdown 명령을 취소하기 위한 명령은?

① shutdown -r

② shutdown -h

③ cancel

④ shutdown -c

23. 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

③ chmod 4755 su

④ chmod 6755 su

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

① halt

② kill

③ cut

④ grep

25. 사용자 그룹을 생성하기 위해 사용되는 Linux 명령어는?

① groups

② mkgroup

③ groupstart

④ groupadd

26. Linux 명령어에 대한 설명으로 옳지 않은 것은?

① ls : 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.

27. SSL 레코드 계층의 서비스를 사용하는 세 개의 특정 SSL 프로토콜 중의 하나이며 메시지 값이 '1'인 단일 바이트로 구성되는 것은?

① Handshake 프로토콜

② Change cipher spec 프로토콜

③ Alert 프로토콜

④ Record 프로토콜

28. 아파치 웹서버 운영 시 서비스에 필요한 여러 기능들을 제어하기 위하여 설정해야 하는 파일은?

① httpd.conf

② htdocs.conf

③ index.php

④ index.cgi

29. 일반적으로 다음 설명에 해당하는 프로세스는?

- 백그라운드로 실행한다.
- 고유한 기능에 해당되는 이벤트가 발생되면 동작한다.
- 서비스를 제공한 다음 대기 상태로 돌아간다.
- 시스템 서비스를 지원하는 프로세스이다.
- 서버의 역할을 수행하거나 그 기능을 도와준다.

① Shell

② Kernel

③ Program

④ Deamon

30. Linux에서 TAR로 묶인 'mt.tar'를 풀어내는 명령은?

① tar -tvf mt.tar

② tar -cvf mt.tar

③ tar -cvvf mt.tar

④ tar -xvf mt.tar

【과목】 네트워크 (15문제)

31. 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.

③ TCP 세션을 사용한다.

④ 상속이 불가능하다.

32. IP Address에 대한 설명으로 옳지 않은 것은?

① A Class는 Network Address bit의 8bit 중 선두 1bit는 반드시 0 이어야 한다.

② B Class는 Network Address bit의 8bit 중 선두 2bit는 반드시 10 이어야 한다.

③ C Class는 Network Address bit의 8bit 중 선두 3bit는 반드시 110 이어야 한다.

④ D Class는 Network Address bit의 8bit 중 선두 4bit는 반드시 1111 이어야 한다.

33. IPv6 프로토콜의 구조는?

① 32bit

② 64bit

③ 128bit

④ 256bit

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

① Transport Layer

② Datalink Layer

③ Presentation Layer

④ Application Layer

35. 자신의 물리 주소(MAC Address)는 알고 있으나 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)

② RARP(Reverse Address Resolution Protocol)

③ ICMP(Internet Control Message Protocol)

④ IGMP(Internet Group Management Protocol)

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

① ICMP(Internet Control Message Protocol)

② IP(Internet Protocol)

③ ARP(Address Resolution Protocol)

④ TCP(Transmission Control Protocol)

37. OSI 7 Layer 구조에서 계층 7에서 계층 4까지 차례대로 나열한 것은?

- ① 응용(Application) - 세션(Session) - 표현(Presentation) - 전송(Transport)
- ② 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)

38. 인터넷 IPv4 주소 Class에서 '203.249.114.2'가 속한 Class는?

- ① A Class
- ② B Class
- ③ C Class
- ④ D Class

39. '서비스' - 'Well-Known 포트' - '프로토콜'의 연결이 옳지 않은 것은?

- ① FTP - 21 - TCP
- ② SMTP - 25 - TCP
- ③ DNS - 53 - TCP
- ④ SNMP - 191 - TCP

40. 디지털 데이터를 디지털 신호 인코딩(Digital Signal Encoding)하는 방법으로 옳지 않은 것은?

- ① NRZ(Non Return to Zero)
- ② Manchester
- ③ PCM(Pulse Code Modulation)
- ④ Differential Manchester



전자문제집 CBT(App Store) : [\[다운로드\]](#)

전자문제집 CBT(Google Play) : [\[다운로드\]](#)

41. 근거리 통신망 이더넷 표준에서 이용하는 매체 액세스 제어 방법은?

- ① Multiple Access(MA)
- ② Carrier Sense Multiple Access(CSMA)
- ③ Carrier Sense Multiple Access/Collision Detection(CSMA/CD)
- ④ Token Passing

42. TCP는 연결 설정과정에서 3-way handshaking 기법을 이용하여 호스트 대 호스트의 연결을 초기화 한다. 다음 중 호스트 대 호스트 연결을 초기화할 때 사용되는 패킷은?

- ① SYN
- ② RST
- ③ FIN
- ④ URG

43. 오류검출 방식인 ARQ 방식 중에서 일정한 크기 단위로 연속해서 프레임 전송하고 수신측에서 오류가 발견된 프레임에 대하여 재전송 요청이 있을 경우 잘못된 프레임 이후를 다시 전송하는 방법은?

- ① 정지-대기 ARQ
- ② Go-back-N ARQ
- ③ Selective Repeat ARQ
- ④ 적응적 ARQ

44. 다음 중 IP Address관련 기술들에 대한 설명으로 옳지 않은 것은?

- DHCP는 DHCP서버가 존재하여, 요청하는 클라이언트
- ① 들에게 IP Address, Gateway, DNS등의 정보를 일괄적으로 제공하는 기술이다.
- 클라이언트가 DHCP 서버에 DHCP Request를 보낼 때
- ② 브로드캐스트로 보낸다.
- 192.168.10.2는 사설 IP Address이다.
- ③
- 공인 IP Address를 다른 공인 IP로 변환하여 내보내는
- ④ 기술이 NAT이다.

45. 다음 중 OSI 7 Layer의 각 Layer 별 Data 형태로서 옳지 않은 것은?

- ① Transport Layer : Segment
- ② Network Layer : Packet
- ③ Datalink Layer : Fragment
- ④ Physical Layer : bit

【4과목】 보안 (15문제)

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

① 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.

47. 다음에서 설명하는 것은?

공격자의 컴퓨터로부터 표적 시스템과 그 시스템이 속한 네트워크에 과다한 데이터를 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 표적 시스템에서 제공하는 서비스들을 인터넷 사용자들이 이용하지 못하게 하는 기법

① Buffer Overflow

② Sniffing

③ IP Spoofing

④ Denial of Service

48. 다음에서 설명하는 기법은?

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

① IP Sniffing

② IP Spoofing

③ Race Condition

④ Packet Filtering

49. 네트워크 취약성 공격으로 옳지 않은 것은?

① Scan 공격

② IP Spoofing 공격

③ UDP 공격

④ Tripwire 공격

50. 다음은 어떤 보안 도구를 의미하는가?

회사의 사설 네트워크와 외부의 공중 네트워크 사이의 중립 지역으로써 삽입된 컴퓨터 호스트 또는 소형 네트워크를 말한다.

① IDS

② DMZ

③ Firewall

④ VPN

51. 지정된 버퍼보다 더 많은 데이터를 입력해서 프로그램이 비정상적으로 동작하도록 하는 해킹 방법은?

① DoS

② Trojan Horse

③ Worm Virus Backdoor

④ Buffer Overflow

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

① 메시지 인증

② 수신 부인방지

③ 사용자 인증

④ 송신 부인방지

53. 방화벽의 주요 기능으로 옳지 않은 것은?

① 접근제어

② 사용자 인증

③ 로깅

④ 프라이버시 보호

54. 아래 TCP_Wrapper 설정 내용으로 올바른 것은?

```
root@db:~#
[root@icqa root]#cat /etc/hosts.deny
ALL: ALL
[root@icqa root]#cat /etc/hosts.allow
in.telnetd: LOCAL, icqa.or.kr
in.ftpd: LOCAL, icqa.or.kr, 200.200.200.0/24
in.fingerd: LOCAL, icqa.or.kr
[root@icqa root]#
```

㉠ 모든 호스트가 이 서버에 접근 불가능하다.

㉡ Telnet으로 LOCAL과 'icqa.or.kr'만이 접근 가능하다.

㉢ FTP로 LOCAL과 'icqa.or.kr' 200.200.200.0번 호스트인 경우에만 접근 가능하다.

㉣ Finger로 LOCAL과 'icqa.or.kr'만 접근 가능하다.

① ㉠, ㉡

② ㉡, ㉢

③ ㉠, ㉡, ㉢

④ ㉡, ㉢, ㉣

55. 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.
- ③ 211.116.233.124에서 Telnet 연결이 이루어져 있다.
- ④ 211.116.233.98로 ssh를 이용하여 연결이 이루어져 있다.

56. Linux 명령어 중 '/var/log/utmp'와 '/var/log/wtmp'를 모두 참조하는 명령어는?

- ① lastlog
- ② last
- ③ who
- ④ netstat

57. Windows Server의 각종 보안 관리에 관한 설명이다. 그룹정책의 보안 설정 중 옳지 않은 것은?

- ① 계정정책 : 암호정책, 계정 잠금 정책, Kerberos v5 프로토콜 정책 등을 이용하여 보안 관리를 할 수 있다.
- ② 로컬정책 : 감사정책, 사용자 권한 할당, 보안 옵션 등을 이용하여 보안 관리를 할 수 있다.
- ③ 공개키 정책 : 암호화 복구 에이전트, 인증서 요청 설정, 레지스트리 키 정책, IP보안 정책 등을 이용하여 보안 관리를 할 수 있다.
- ④ 이벤트 로그 : 응용 프로그램 및 시스템 로그 보안 로그를 위한 로그의 크기, 보관 기간, 보관 방법 및 액세스 권한 값 설정 등을 이용하여 보안 관리를 할 수 있다.

58. 스푸핑 공격의 한 종류인 스위치 재밍(Switch Jamming) 공격에 대한 순차적 내용으로 옳지 않은 것은?

- ① 스위치 허브의 주소 테이블에 오버 플로우가 발생하게 만든다.
- ② 스위치가 모든 네트워크 포트로 브로드 캐스팅하게 만든다.
- ③ 오버 플로우를 가속화하기 위하여 MAC 주소를 표준보다 더 큰 값으로 위조하여 스위치에 전송한다.
- ④ 테이블 관리 기능을 무력화 하고 패킷 데이터를 가로챈다.

59. 라우터에 포함된 SNMP(Simple Network Management Protocol) 서비스의 기본 설정을 이용한 공격들이 많다. 이를 방지하기 위한 SNMP 보안 설정 방법으로 옳지 않은 것은?

- ① 꼭 필요한 경우가 아니면 읽기/쓰기 권한을 설정하지 않는다.
- ② 규칙적이고 통일성이 있는 커뮤니티 값을 사용한다.
- ③ ACL을 적용하여 특정 IP Address를 가진 경우만 SNMP 서비스에 접속할 수 있도록 한다.
- ④ tftp-server-list' 명령으로 특정 IP Address만이 서비스에 접속할 수 있게 한다.

60. Router에서는 IP 및 패킷을 필터링 하기 위한 Access Control List를 사용할 때 주의사항으로 옳바른 것은?

- ① 라우터에 연산 부담을 덜기 위하여 상세하고, 큰 용량의 ACL을 유지하여야 한다.
- ② 시스코 라우터는 입력 트래픽 보다 출력 트래픽에 ACL을 적용하는 것이 효율적이다.
- ③ 라우터 트래픽 감소를 위해 Netflow을 함께 작동 시킨다.
- ④ ACL을 이용한 출력 트래픽 필터링은 위조된 IP가 유출되는 것을 방지한다.