

2024년10월27일년 인터넷보안전문가 2급 필기시험 기출문제 답안

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

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!

Download on the
App Store

GET IT ON
Google Play

【과목】 정보보호개론 (10문제)

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

- ① 사용자 ID/ 암호 알고리즘, 암호키, 수명 등의 ESP 관련 정보/ 발신지 IP Address와 목적지 IP Address
- ② 인증 키, 수명 등의 AH 관련 정보/ 발신지 포트 및 목적지 포트
- ③ 데이터 민감도/ IPSec 프로토콜 모드(터널, 트랜스포트)/ 인증 알고리즘, 암호키, 수명 등의 ESP 관련 정보/ 발신지 IP Address와 목적지 IP Address
- 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. 네트워크 보안을 규정하고 있는 국제 위원회는?

- ① IEEE 802.12
- ② IEEE 802.4
- ③ IEEE 802.10
- ④ IEEE 802.2

4. 다음 중 유형이 다른 보안 알고리즘은?

- ① SEED 알고리즘
- ② RSA 알고리즘
- ③ Rabin 알고리즘
- ④ ECC 알고리즘

5. 암호의 목적에 대한 설명 중 옳지 않은 것은?

- ① 비밀성(Confidentiality) : 허가된 사용자 이외 암호문 해독 불가
- ② 무결성(Integrity) : 메시지 변조 방지
- ③ 접근 제어(Access Control) : 암호화된 데이터를 포함하여 모든 정보에 대해 무제한 접근을 허용하는 기능
- ④ 부인봉쇄(Non-Repudiation) : 송수신 사실 부정 방지

6. 네트워크 또는 응용을 위한 보안 대책으로 옳지 않은 것은?

- ① TLS - 종단간 보안
- ② PGP - 안전한 전자메일
- ③ Single Sign On - 무선 링크 보안
- ④ Kerberos - 사용자 인증

7. 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



전자문제집 CBT(App Store) : [\[다운로드\]](#)



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

8. 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

9. 다음 내용은 보안 운영체제의 특정한 보안기능에 대해 설명한 것이다. 어떤 기능인가?

일반적으로 보안 관련 사건 기록의 유지를 포함하며, 발생한 각각의 사건과 관련된 사용자의 정보가 수록된다. 모든 보안 관련 사건은 반드시 이 기록부(log file)에 기록되어야 한다. 또한 이 기록부는 명백하게 보호되어야 한다.

- ① 사용자 식별 또는 인증
- ② 감사 및 감사 기록
- ③ 강제적/임의적 접근 통제
- ④ 침입 탐지

10. 보안과 관련된 용어의 정의나 설명으로 옳지 않은 것은?

- ① 프락시 서버(Proxy Server) - 내부 클라이언트를 대신하여 외부 서버와 통신을 중개하는 프로그램 서버
- ② 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

【2과목】 운영체제 (20문제)

11. Linux에서 '/dev' 디렉터리에 관한 설명으로 옳지 않은 것은?

- ① 이 디렉터리는 물리적 용량을 갖지 않는 가상 디렉터리이다.
- ② 시스템의 각종 장치들에 접근하기 위한 디바이스 드라이버들이 저장되어 있다.
- ③ 이 디렉터리에는 커널로 로딩 가능한 커널 모듈들이 저장되어 있다.
- ④ 대표적으로 하드디스크 드라이브, SSD, USB, 가상 네트워크 인터페이스, 그리고 루프백 장치 등이 존재한다.

12. Linux에서 기본적으로 지원하는 파티션의 종류가 아닌 것은?

- ① EXT4
- ② Btrfs
- ③ XFS
- ④ APFS

13. Windows Server에서 사용자 계정에 관한 옵션으로 설정할 수 없는 항목은?

- ① 로그인 할 수 있는 컴퓨터의 IP Address
- ② 로그인 시간 제한
- ③ 계정 만료 날짜
- ④ 암호 사용 기간 무제한

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

- ① who
- ② w
- ③ finger
- ④ ping

15. Linux에서 특정한 파일을 찾고자 할 때 사용하는 명령어는?

- ① mv
- ② cp
- ③ find
- ④ file

16. Windows Server 환경에서 기본 그룹계정의 설명 중 옳지 않은 것은?

- ① Users - 시스템 관련 사항을 변경할 수 없는 일반 사용자
- ② Administrators - 컴퓨터/도메인에 모든 액세스 권한을 가진 관리자
- ③ Guest - 파일을 백업하거나 복원하기 위해 보안 제한을 변경할 수 있는 관리자
- ④ Power Users - 일부 권한을 제외한 관리자 권한을 가진 고급 사용자

17. DNS(Domain Name System) 서버를 처음 설치하고 가장 먼저 만들어야 하는 데이터베이스 레코드는?

- ① CNAME(Canonical Name)
- ② HINFO(Host Information)
- ③ PTR(Pointer)
- ④ SOA(Start Of Authority)

18. 다음은 ssh의 클라이언트 설정 파일이다. '/etc/ssh_config' 옵션 내용 중 옳지 않은 것은?

- ① BatchMode no: SSH 연결 시 비대화형 모드로 설정하지 않음 (비밀번호 입력을 요구함)
- ② PasswordAuthentication no: 패스워드 기반 인증을 허용함
- ③ PubkeyAuthentication yes: 공개키 기반 인증을 허용함
- ④ StrictHostKeyChecking yes: 호스트 키를 엄격히 확인하여 미리 신뢰하지 않는 호스트에 연결하지 않음

19. Windows Server 부팅 시 로컬 로그인 단계에서 직접적으로 사용되지 않는 파일은?

- ① Winlogon.exe
- ② Lsass.exe
- ③ Svchost.exe
- ④ LogonUI.exe

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

- ① 파일 폴더에 대한 액세스
- ② 사용자의 로그인과 로그오프
- ③ 메모리에 상주된 프로세스의 사용 빈도
- ④ 액티브 디렉터리에 대한 변경 시도

21. 파일 시스템의 기능으로 옳지 않은 것은?

- ① 여러 종류의 접근 제어 방법을 제공
- ② 파일의 생성, 변경, 제거
- ③ 파일의 무결성과 보안을 유지할 수 있는 방안 제공
- ④ 네트워크 제어

22. SSL/TLS 레코드 계층의 서비스를 사용하는 세 개의 특정 SSL/TLS프로토콜 중의 하나이며 메시지 값이 '1'인 단일 바이트로 구성되는 것은?

- ① Handshake 프로토콜
- ② Change cipher spec 프로토콜
- ③ Alert 프로토콜
- ④ Record 프로토콜

23. Linux의 기본 디렉터리에 해당하지 않는 것은?

- ① /etc
- ② /root
- ③ /grep
- ④ /home

24. Linux 시스템에서 '-rwxr-xr-x' 퍼미션을 나타내는 숫자는?

- ① 755
- ② 777
- ③ 766
- ④ 764

25. Linux에서 VI(Visual Interface) 명령어 중 변경된 내용을 저장한 후 종료하고자 할 때 사용해야 할 명령어는?

- ① :wq
- ② :q!
- ③ :e!
- ④ \$

26. 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

27. 현재 Linux 서버는 Shadow Password System을 사용하고 있고, '/etc/passwd'에서 'icqa'의 부분은 아래와 같다. 'icqa' 계정을 비밀번호 없이 로그인 되도록 하는 방법은?

```
icqa:x:500:500:/home/icqa:/bin/bash
```

- ① /etc/passwd 파일의 icqa의 세 번째 필드를 공백으로 만든다.
- ② /etc/shadow 파일의 icqa의 두 번째 필드를 공백으로 만든다.
- ③ /etc/passwd 파일의 icqa의 다섯 번째 필드를 '!!'로 채운다.
- ④ /etc/shadow 파일의 icqa의 네 번째 필드를 공백으로 만든다.

28. Windows Server에서 기본적으로 인식하지 못하는 파일 시스템은?

- ① NTFS
- ② EXT4
- ③ FAT32
- ④ ReFS

29. Linux 시스템이 부팅될 때 나오는 메시지가 저장된 로그 파일의 경로와 명칭으로 옳바른 것은?

- ① /var/log/xferlog
- ② /var/log/dmesg
- ③ /var/log/message
- ④ /var/log/secure

30. 아래는 DNS Zone 파일의 SOA 레코드 내용이다. SOA 레코드의 내용을 보면 5 개의 숫자 값을 갖는데, 그 중 두 번째 값인 Refresh 값의 역할은?

```
@ IN SOA localhost. root.localhost.(
    1997022700 ; Serial
    28800      ; Refresh
    14400      ; Retry
    3600000    ; Expire
    86400 ) ; Minimum
```

① Primary 서버와 Secondary 서버가 동기화하게 되는 기간이다.

② Zone 내용이 다른 DNS 서버의 Cache 안에서 살아남을 기간이다.

③ Zone 내용이 다른 DNS 서버 안에서 Refresh 될 기간이다.

④ Zone 내용이 Zone 파일을 갖고 있는 서버 내에서 자동 Refresh 되는 기간이다.

[3과목] 네트워크 (15문제)

31. 주파수분할다중화의 특징으로 옳지 않은 것은?

① 전송매체를 통해 전송되는 신호는 아날로그이다.

② 다중화되는 입력신호는 아날로그 신호와 디지털 신호 모두 가능하다.

③ 각 신호를 고유한 주파수 대역으로 할당하여 동시에 전송할 수 있도록 하여, 여러 통신을 동시에 가능하게 한다.

④ 전송매체를 부채널로 분리하여 사용하므로 대역폭 낭비가 적다.

32. IP Address '129.120.120.88'가 속하는 Class는?

① A Class

② B Class

③ C Class

④ D Class

33. 다음 중 데이터 링크 계층의 기능에 해당하지 않는 것은?

① 데이터 링크 커넥션의 설정과 해제

② 전송 데이터의 프레임화

③ 물리 매체에 비트 열 전송

④ 전송 확인 및 흐름 제어

34. 다음 중 데이터 전송과정에서 먼저 전송된 패킷이 나중에 도착되어도 착신측 노드에서 패킷의 순서를 바르게 제어하는 것은?

① 순서제어

② 흐름제어

③ 오류제어

④ 연결제어

35. 다음 중 프로토콜의 기본 구성요소로 옳지 않은 것은?

① 구문

② 의미

③ 타이밍

④ 부호화

36. 오류검출 방식인 ARQ 방식 중에서 일정한 크기 단위로 연속해서 프레임을 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

37. 시간을 매체로 데이터를 다중화하여 전송하는 통신 방식은?

① FDM

② TDM

③ WDM

④ CDM

38. 광섬유케이블의 구성요소로 옳지 않은 것은?

① 코어(Core)

② 클래딩(Cladding)

③ 코팅(Coating)

④ 스레드(Thread)

39. OSPF에서 Neighbor의 상태를 확인할 수 있는 명령어는?

① show ip ospf interface

② show ip ospf database

③ show ip ospf neighbor

④ show ip ospf border-router

40. Distance Vector 프로토콜에서 루핑 방지를 위해 사용되는 기술로 옳지 않은 것은?

① SPF(Shortest Path First)

② Split-Horizon

③ Poison & Poison-Reverse

④ Holddown Timer

41. 라우터 명령어 중 NVRAM에서 RAM으로 configuration file 을 copy하는 명령어는?

① copy flash start

② copy running-config startup-config

③ copy startup-config running-config

④ wr mem

42. 다음 203.214.3.0/26 Subnet의 호스트에 사용할 수 있는 IP Address로 맞는 것은?

① 203.214.3.0

② 203.214.3.64

③ 203.214.3.63

④ 203.214.3.1

43. ICMP의 메시지 유형으로 옳지 않은 것은?

① Destination Unreachable

② Time Exceeded

③ Echo Reply

④ Echo Research

44. IP Address는 알고 MAC Address를 모를 경우 데이터 전송을 위해 Datalink 계층인 MAC Address를 알아내는 Protocol 은?

① ARP

② RARP

③ ICMP

④ IP

45. TCP와 UDP의 차이점 설명으로 옳지 않은 것은?

① 데이터 전송형태로 TCP는 Connection Oriented방식 이고 UDP는 Connectionless방식이다.

② TCP가 UDP보다 데이터 전송 속도가 빠르다.

③ TCP가 UDP보다 신뢰성이 높다.

④ TCP가 UDP에 비해 각종 제어를 담당하는 Header 부분이 커진다.

【4과목】 보안 (15문제)

46. Linux에서 root만 로그인하고 나머지 사용자 계정은 로그인이 불가능하게 하는 설정 파일은?

① /etc/nologin

② /etc/hosts.allow

③ /etc/hosts.deny

④ /bin/more

47. 침입차단시스템에 대한 설명 중 옳지 않은 것은?

① 침입차단시스템은 내부 사설망을 외부의 인터넷으로부터 보호하기 위한 장치이다.

패킷 필터링 침입차단시스템은 주로 발신지와 목적지 IP
② Address와 발신지와 목적지 포트 번호를 바탕으로 IP 패킷을 필터링한다.

침입차단시스템의 유형은 패킷 필터링 라우터, 응용 레벨
③ 게이트웨이, 그리고 회선 레벨 게이트웨이 방법 등이 있다.

④ 침입차단시스템은 네트워크 사용에 대한 로깅과 통계자료를 제공할 수 없다.

48. 네트워크 취약성 공격으로 옳지 않은 것은?

① Scan 공격

② IP Spoofing 공격

③ UDP 공격

④ Tripwire 공격

49. IP 스푸핑 공격에 대한 설명으로 옳지 않은 것은?

- ① 공격자가 자신으로부터 전송되는 패킷에 다른 호스트의 IP 주소를 담아서 전송하는 공격 방법이다.
- 이 공격은 TCP 세그먼트의 일련번호를 예측 여부에 따라
- ② 서 Non-Blinding IP 스푸핑 공격과 Blinding IP 스푸핑 공격으로 분류될 수 있다.
- IP 스푸핑 공격의 주요 요소는 공격 호스트, 공격에 이용
- ③ 되는 호스트, 그리고 공격당하는 호스트로 이루어진다.
- 모든 운영체제는 64K 법칙을 이용하여 순서번호를 생성
- ④ 하므로 이 공격에 매우 취약하다.

50. 패스워드 보안을 위해서 취하는 행동 중 적절하지 못한 것은?

- ① ID와 같거나 사전에 등록된 단어를 패스워드로 사용하지 않도록 한다.
- ② 패스워드는 숫자, 영문, 특수기호를 포함하여 8자리 이상 조합하여 사용한다.
- ③ Secure Shell (SSH) 클라이언트 및 Secure File Transfer Protocol (SFTP)을 사용한다.
- ④ Telnet을 사용할 때는 패스워드 노출을 막기 위해서 패스워드를 해쉬(Hash)해서 전송한다.

51. TCP 프로토콜의 연결 설정을 위하여 3-Way Handshaking의 취약점을 이용하여 실현되는 서비스 거부 공격은?

- ① Ping of Death
- ② 스푸핑(Spoofing)
- ③ 패킷 스니핑(Packet Sniffing)
- ④ SYN Flooding

52. L2 스위칭 공격에 대한 설명으로 옳지 않은 것은?

- ① 하드웨어에 대한 공격과 트래픽 흐름을 변경하는 네트워크 공격으로 분류할 수 있다.
- ② MAC Flooding, ARP Spoofing, Spanning Tree Attack 등이 있다.
- 공격이 진행되고 있는 상태에서 스위치와 연결된 정상적
- ③ 인 호스트가 통신할 때, 스위치의 MAC 정보에는 영향을 미치지 않는다.
- MAC Flooding은 한 포트에서 수 천 개의 호스트가 스위
- ④ 치와 연결되어 있는 것으로 보이지만 실제로는 변조된 MAC 정보를 공격 호스트에서 발생시키는 것이다.

53. 다음에서 설명하는 현상은?

프로그램이 메모리에 할당된 버퍼의 크기를 초과하여 데이터를 기록함으로써, 인접한 메모리 공간을 덮어쓰게 되는 현상이다. 이로 인해 시스템의 안정성에 영향을 미치거나 악성 코드를 실행할 수 있는 취약점이 발생할 수 있다.

- ① Race Condition
- ② Buffer Overflow
- ③ IP Spoofing
- ④ Password Attack

54. 종단 간 보안 기능을 제공하기 위한 TLS(Transport Layer Security) 프로토콜에서 제공되는 보안 서비스로 옳지 않은 것은?

- ① 통신 응용간의 기밀성 서비스
- ② 인증서를 이용한 클라이언트와 서버의 인증
- ③ 메시지 무결성 서비스
- ④ 클라이언트에 의한 서버 인증서를 이용한 서버 메시지의 부인방지 서비스

55. Snort가 사전에 정의된 패턴과 일치하는 경우 취하는 특성의 행동으로 옳지 않은 것은?

- ① 특정데이터에 대한 경고
- ② 특정데이터에 대한 로깅
- ③ 특정데이터에 대한 무시
- ④ 특정데이터에 대한 지연

56. DDoS(Distrivuted Denial of Service) 공격용 기법이나 도구로 알려진 것이 아닌 것은?

- ① Trinoo
- ② TFN
- ③ Stacheldraft
- ④ Sasser

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

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

58. 아래와 같이 초기설정이 되어있는 '/bin/su' 명령어가 있다.

Linux 서버의 내부 보안을 위해 '/bin/su' 명령어를 root에게는 모든 권한을, 'wheel'이라는 그룹에게는 실행권만만을 부여하려고 한다. 이 과정 중에 올바르지 않은 사항은?

```
[root@icqa/bin]# ls -alF su
-rwsr-xr-x 1 root root 14188 3월 7 2017 su*
```

- ① [root@icqa /bin]#chmod 4710 /bin/su
- ② [root@icqa /bin]#chown root /bin/su
- ③ [root@icqa /bin]#chgrp wheel /bin/su
- ④ [root@icqa /bin]#chown -u root -g wheel /bin/su

59. Linux에서 root 권한 계정이 'a' 라는 파일을 지우려 했을때 나타난 결과이다. 이 파일을 지울 수 있는 방법은?

```
[root@linux /root]# rm -rf a
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' 바이트이기 때문에 지워지지 않으므로, 파일에 내용을 넣은 후 지운다.
- ② 현재 로그인 한 사람이 root가 아니므로 root로 로그인 한다.
- ③ chmod 명령으로 쓰기금지를 해제한다.
- ④ chattr 명령으로 쓰기금지를 해제한다.

60. Linux에서 Nmap의 옵션 중 상대방의 OS를 알아내는 옵션은?

- ① [root@icqa bin]#./nmap -O www.target.com
- ② [root@icqa bin]#./nmap -I www.target.com
- ③ [root@icqa bin]#./nmap -sS www.target.com
- ④ [root@icqa bin]#./nmap -sP www.target.com