2017년04월09일년 인터넷보안전문가 2급 필기시험 기출문제 답안

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

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

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

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

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. 안전한 전자지불을 위하여 수립된 보안 대책과 사용 용도에 대한 연결이 옳지 않은 것은?

① PGP(Pretty Good Privacy) - 메일 보안 시스템

② PEM(Privacy-enhanced Electronic Mail) - 보안 메일의 IETF 표준

③ Kerberos - 사용자 인증

❹ SNMPv2 - Web 문서 관리

2. 보안과 관련된 용어의 정의나 설명으로 옳지 않은 것은?

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

❷ 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

3. 안전한 Linux Server를 구축하기 위한 방법으로 옳지 않은 것은?

① 불필요한 데몬을 제거한다.

② 불필요한 Setuid 프로그램을 제거한다.

③ 시스템의 무결성을 주기적으로 검사한다.

❹ 무결성을 검사하기 위한 데이터베이스를 추후 액세스가 용이하게 하기 위하여 검사할 시스템에 저장하는게 좋다.

4. 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

5. 금융기관이나 인터넷 상에서 많은 사람들로부터 적은 금액을 조금씩 빼내고 피해자는 사건이 알려지기 전까지 전혀 눈치 채지 못하는 컴퓨터 사기수법은?

① Scavenging

② 논리 폭탄(Logic Bomb)

❸ 살라미(Salami) 기법

④ 자료의 부정변개(Data Diddling)

Download on the App Store 전자문제집 CBT(App Store) :[다운로드]

GET IT ON Google Play 전자문제집 CBT(Google Play) :[다운로드]

6. 개인 홈페이지 서버가 크래킹(Cracking) 당하였을 때 취해야할 행동으로 올바른 것은?

① 로그분석을 통해 크래킹을 한 사람의 신원을 밝혀내어 접속한 서버를 크래킹 한다.

❷ 네트워크 분리 후 로그 분석을 통해 크래킹을 한 시점과 방법을 알아내 차후 동일수법에 의한 사고를 방지한다.

③ 백업된 자료를 이용하여 그대로 복구하여 놓는다.

④ 백도어의 염려가 있으므로 시스템을 포맷한다.

7. 암호의 목적에 대한 설명 중 옳지 않은 것은?

① 비밀성(Confidentiality) : 허가된 사용자 이외 암호문 해독 불가

② 무결성(Integrity) : 메시지 변조 방지

❸ 접근 제어(Access Control) : 프로토콜 데이터 부분의 접근제어

④ 부인봉쇄(Non-Repudiation) : 송수신 사실 부정방지

8. 공개키 암호와 관용 암호를 비교한 설명 중 옳지 않은 것은?

① 관용 암호에서는 암호화와 복호화에 동일한 알고리즘이 이용되지만, 공개키 암호에서는 하나의 키는 암호화, 다른 하나는 복호화에 이용하는 알고리즘을 이용한다.

② 관용 암호에서는 키가 절대적으로 비밀이 유지가 되어야 하나, 공개키 암호에서는 두 개의 키 중에서 개인 비밀키의 보안이 유지되면 된다.

③ 관용 암호의 대표적인 예로 DES, IDEA 등을 들 수 있으며, 공개키 암호의 대표적인 예로 RSA, RC4 등을 들 수 있다.

❹ 관용 암호의 가장 큰 단점은 계산 시간이 많이 소요된다는 사실이고, 공개키 암호의 가장 큰 단점은 사용이 불편하다는 점이다.

9. 인증 서비스를 제공하기 위한 공개키 인증서(Public-key Certificate)에 포함되어 있지 않은 내용은?

① 가입자의 이름

② 가입자의 전자서명 검증키(공개키)

③ 인증서의 유효기간

❹ 가입자의 거주 주소, 전화번호 등의 개인정보

10. 다음 중 방화벽의 유형으로 옳지 않은 것은?

① Packet Filtering Gateway

② Circuit Level Gateway

❸ Screened Host

④ Proxy서버/응용 Gateway

【2과목】 운영체제 (20문제)

11. Linux 콘솔 상에서 네트워크 어댑터 'eth0'을 '192.168.1.1' 이라는 주소로 사용하고 싶을 때 올바른 명령은?

① ifconfig eth0 192.168.1.1 activate

② ifconfig eth0 192.168.1.1 deactivate

❸ ifconfig eth0 192.168.1.1 up

④ ifconfig eth0 192.168.1.1 down

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

① tar -tvf mt.tar

② tar -cvf mt.tar

③ tar -cvvf mt.tar

❹ tar –xvf mt.tar

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

```
Root:$1$szfVKcHi$dEFUonrDJZ2ZGOPuqq9yK0:11
458:0:99999:7:::
adm:*:11458:0:99999:7:::
lp:*:11458:0:99999:7:::
named:!!:11458:0:99999:7:::
gdm:!!:11458:0:99999:7:::
```

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

❷ gdm에서 '!!'은 로그인 쉘을 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

14. 아파치 웹서버에 대한 설명으로 잘못된 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 디렉터리, 에러 로그가 기록될 파일 경로 등을 포함한다.

❹ 설정 파일에서 웹 서버가 사용할 사용자와 그룹을 나타내는 설정 변수인 User와 Group은 'root' 로 설정해야 한다.

15. Linux 서버 내에 로그인 해 있는 사람들과 실시간 채팅을 할 수 있는 Perl 스크립트를 만들어 'chat.pl' 이라는 파일로 저장하였다. 하지만 저작권 문제 때문에 소스를 보이지 않고 사람들이 오직 이 스크립트 파일을 실행만 하게하고 싶다. 이때 올바른 파일 퍼미션은?

❶ 701

② 777

③ 755

④ 705

16. Linux에서 현재 위치한 디렉터리를 표시해 주는 명령어는?

① mkdir

❷ pwd

③ du

④ df

17. 프로토콜을 POP3 대신에 IMAP를 쓰는 환경에서 vi편집기를 이용해서 POP 프로토콜을 주석처리 하고, IMAP 프로토콜의 주석을 제거 하였지만 서비스가 정상적으로 이루어지지 않고 있다면 그 원인에 해당하는 것은?

① IMAP 프로토콜은 POP3를 대신할 수 없기 때문이다.

② Sendmail과 IMAP는 근본적으로 상관이 없기 때문이다.

❸ 데몬 설정 파일을 변경한 후 데몬을 재실행 해주지 않았기 때문이다.

④ 해당 포트가 열렸기 때문이다.

18. 삼바 데몬을 Linux에 설치하여 가동하였을 때 열리는 포트들로 알맞게 나열된 것은?

❶ UDP 137, 139

② TCP 137, 139

③ TCP 80, 25

④ UDP 80, 25

19. 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.

❸ 이 디렉터리에는 커널로 로딩 가능한 커널 모듈들이 저장되어 있다.

④ 대표적으로 하드디스크 드라이브, USB, CD-ROM 그리고 루프 백 장치 등이 존재한다.

20. 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

21. Linux 네트워크 서비스에 관련된 설정을 하는 설정 파일은?

❶ /etc/inetd.conf

② /etc/fstab

③ /etc/ld.so.conf

④ /etc/profile

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

① mount

② showexports

❸ showmount

④ export

23. Telnet과 같은 원격 터미널 세션에서 통신을 암호화하여 중간에서 스니핑과 같은 도청을 하더라도 해석을 할 수 없도록 해주는 프로그램으로 옳지 않은 것은?

① sshd

② sshd2

③ stelnet

❹ tftp

24. Linux에서 호스트 이름을 IP Address로 변환시켜 주는 DNS 데몬은?

① lpd

② netfs

③ nscd

❹ named

25. 파일이 생성된 시간을 변경하기 위해 사용하는 Linux 명령어는?

① chmod

② chgrp

❸ touch

④ chown

26. 화면상에서 File 안의 내용을 보기 위한 Linux 명령어는?

① touch

② ls

❸ more

④ mkdir

27. Linux에서 'netstat -an' 명령으로 시스템을 확인한 결과 다음과 같은 결과가 나왔다. 아래 '3306'번 포트는 어떤 데몬이 가동될 때 열리는 포트인가?(단, 시스템의 기본 포트는 Well-Known 포트를 사용한다.)

```
root@db:~
[root@db root]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:588             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     863    /tmp/mysql.sock
unix  5      [ ]         DGRAM                    761    /dev/log
unix  2      [ ]         DGRAM                    830
unix  2      [ ]         DGRAM                    812
unix  2      [ ]         DGRAM                    770
unix  2      [ ]         STREAM     CONNECTED     537
[root@db root]#
```

❶ MySQL

② DHCP

③ Samba

④ Backdoor

28. 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
```

❶ Primary 서버와 Secondary 서버가 동기화 하게 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.

29. NTFS의 주요 기능에 대한 설명 중 옳지 않은 것은?

① 파일 클러스터를 추적하기 위해 B-Tree 디렉터리 개념을 사용한다.

② 서버 관리자가 ACL을 이용하여 누가 어떤 파일만 액세스 할 수 있는지 등을 통제할 수 있다.

③ 교체용 디스크와 고정 디스크 모두에 대해 데이터 보안을 지원한다.

❹ FAT 보다 대체적으로 빠른 속도를 지원한다.

30. Windows Server에서 FTP 서비스에 대한 설명으로 옳지 않은 것은?

❶ 웹 사이트가 가지고 있는 도메인을 IP Address로 바꾸어 주는 서비스를 말한다.

② IIS에서 기본적으로 제공하는 서비스이다.

③ 기본 FTP 사이트는 마우스 오른쪽 버튼을 눌러 등록정보를 수정할 수 있다.

④ FTP 서비스는 네트워크를 통하여 파일을 업로드 및 다운로드 할 수 있는 서비스를 말한다.

【3과목】 네트워크 (15문제)

31. IP Address '172.16.0.0'인 경우에 이를 14개의 서브넷으로 나누어 사용하고자 할 경우 서브넷 마스크는?

① 255.255.228.0

❷ 255.255.240.0

③ 255.255.248.0

④ 255.255.255.248

32. 다음 중 디지털 변조로 옳지 않은 것은?

① ASK

② FSK

❸ PM

④ QAM

33. TCP와 UDP의 차이점을 설명한 것 중 옳지 않은 것은?

① TCP는 전달된 패킷에 대한 수신측의 인증이 필요하지만 UDP는 필요하지 않다.

② TCP는 대용량의 데이터나 중요한 데이터 전송에 이용 되지만 UDP는 단순한 메시지 전달에 주로 사용된다.

③ UDP는 네트워크가 혼잡하거나 라우팅이 복잡할 경우에는 패킷이 유실될 우려가 있다.

❹ UDP는 데이터 전송 전에 반드시 송수신 간의 세션이 먼저 수립되어야 한다.

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

❶ SYN

② RST

③ FIN

④ URG

35. '192.168.0.0/255.255.255.0' 네트워크에서 '192.168.0.3/255.255.255.0' 컴퓨터가 'ping 192.168.0.255' 라는 명령을 내렸을 때 예상되는 동작은?

① 네트워크 주소이므로 ping 프로그램은 아무런 메시지도 출력하지 않고 종료한다.

② 패킷이 내부망을 떠돌아다니다가 TTL이 만료되어 에러 메시지를 출력한다.

❸ 같은 네트워크 내에 있는 모든 컴퓨터들이 응답패킷을 보낸다.

④ 자기 자신에게 'ICMP_ECHO_REQUEST' 패킷을 보낸다.

36. 네트워크를 관리 모니터링 하는데 사용되는 프로토콜로, 'get', 'get-next', 'set', 'trap' 과 같은 메시지를 사용하여 작업을 수행하는 것은?

① FTP

② HTTP

③ IP

❹ SNMP

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. TCP 포트 중 25번 포트가 하는 일반적인 역할은?

① Telnet

② FTP

❸ SMTP

④ SNMP

39. LAN에서 사용하는 전송매체 접근 방식으로 일반적으로 Ethernet 이라고 불리는 것은?

① Token Ring

② Token Bus

❸ CSMA/CD

④ Slotted Ring

40. IPv4에 비하여 IPv6이 개선된 설명으로 잘못된 것은?

① 128bit 구조를 가지기 때문에 기존의 IPv4 보다 더 많은 노드를 가질 수 있다.

❷ 전역방송(Broad Cast)이 가능하다.

③ IPv6에서는 확장이 자유로운 가변길이 변수로 이루어진 옵션 필드 부분 때문에 융통성이 발휘된다.

④ IPv6에서는 Loose Routing과 Strict Routing의 두 가지 옵션을 가지고 있다.

41. 라우팅 되지 않는 프로토콜(Non-Routable Protocol)은?

① TCP/IP, DLC

② NetBEUI, TCP/IP

③ IPX/SPX, NetBEUI

❹ NetBEUI, DLC

42. 패킷(Packet)에 있는 정보로 옳지 않은 것은?

① 출발지 IP Address

❷ TCP 프로토콜 종류

③ 전송 데이터

④ 목적지 IP Address

43. 다음 TCP/IP에 관한 설명으로 옳지 않은 것은?

① Application 계층에는 Telnet, FTP, HTTP, SMTP 등의 프로토콜이 존재한다.

② Transport계층에는 대표적으로 TCP와 UDP가 존재한다.

③ 미국에서 연구된 후로 실용적으로 발전된 프로토콜이다.

❹ Reference적인 성격을 가지고 있으며 7 계층으로 layer를 구성한다.

44. TCP 헤더 필드의 내용으로 옳지 않은 것은?

❶ TTL(Time To Live)

② 발신지 포트번호

③ 윈도우 크기

④ Checksum

45. 네트워크 주소에 대한 설명 중 옳지 않은 것은?

① X.121 : X.25 공중네트워크에서의 주소지정 방식

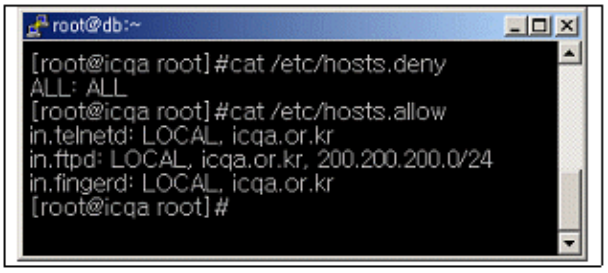
❷ D Class 주소 : 맨 앞의 네트워크 주소가 '1111' 로서 멀티캐스트 그룹을 위한 주소이다.

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 '10'이 되어야 한다.

【4과목】 보안 (15문제)

46. 아래 TCP_Wrapper 설정 내용으로 올바른 것은?



㉠ 모든 호스트가 이 서버에 접근 불가능하다.
㉡ Telnet으로 LOCAL과 icqa.or.kr만이 접근 가능하다.
㉢ FTP로 LOCAL과 icqa.or.kr 200.200.200.0번 호스트인 경우에만 접근 가능하다.
㉣ Finger로 LOCAL과 icqa.or.kr만 접근 가능하다.

① ㉠, ㉢

❷ ㉡, ㉣

③ ㉠, ㉡, ㉢

④ ㉡, ㉢, ㉣

47. 통신을 암호화하여 중간에서 스니핑과 같은 도청을 하더라도 해석을 할 수 없도록 해 주는 프로그램으로 옳지 않은 것은?

① sshd

② sshd2

③ stelnet

❹ tftp

48. PGP(Pretty Good Privacy)에서 사용되는 알고리즘이 아닌 것은?

① RSA

❷ DES

③ MD5

④ IDEA

49. 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.

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

① DoS

② Trojan Horse

③ Worm Virus Backdoor

❹ Buffer Overflow

52. 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

53. 현재 Linux 시스템 상에서 침입자의 침입여부나 사용자의 사용 여부를 확인하고자 한다. 적합한 명령어로 옳지 않은 것은?

① [root@icqa /bin]#w

② [root@icqa /bin]#netstat -t

❸ [root@icqa /bin]#nuser -a

④ [root@icqa /bin]#who

54. DoS(Denial of Service) 공격의 특징으로 옳지 않은 것은?

① 공격의 원인이나 공격자를 추적하기 힘들다.

❷ 루트 권한을 획득하여 시스템을 장악한다.

③ 공격시 이를 해결하기 힘들다.

④ 사용자의 실수로 발생할 수도 있다.

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

```
[root@linux /root]# rm a -rf
 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.

❹ chattr 명령으로 쓰기금지를 해제한다.

56. 'tcpdump' 라는 프로그램을 이용해서 '192.168.1.1' 호스트로부터 '192.168.1.10' 이라는 호스트로 가는 패킷을 보고자 한다. 올바른 명령은?

① tcpdump src host 192.168.1.10 dst host 192.168.1.1

② tcpdump src host 192.168.1.1 dst host 192.168.1.10

❸ tcpdump src host 192.168.1.1 and dst host 192.168.1.10

④ tcpdump src host 192.168.1.10 and dst host 192.168.1.1

57. Linux 로그인 파일에 대한 설명이 옳지 않은 것은?

① 커널 에러, 부팅 메시지, 로긴 실패, 그리고 su 로그 등의 기록을 남기는 파일은 '/var/log/messages' 파일이다.

② FTP와 관련된 로그 파일은 'xferlog' 파일이다.

③ TCP Wrapper와 같은 보안 관련 로그 파일은 'secure' 파일이다.

❹ 현재 로그인 되어 있는 사용자의 리스트를 저장하는 파일은 '/var/log/lastlog' 파일이다.

58. 네트워크 취약성 공격으로 옳지 않은 것은?

① Scan 공격

② IP Spoofing 공격

③ UDP 공격

❹ Tripwire 공격

59. 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.

60. 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