

1과목 : 정보보호개론

1. 다음 중 유형이 다른 보안 알고리즘은?

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

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

- ① 1970년대 초 IBM이 개발한 알고리즘이다.
② 2048 비트까지의 가변 키 크기가 지원되고 있다.
③ NIST + NSA가 개발에 참여했다.
④ 암호화 방식의 전자 코드 복과 암호 피드백으로 이루어졌다.

3. 이산대수 문제에 바탕을 두며 인증메시지에 비밀 세션키를 포함하여 전달 할 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

4. 5명의 사용자가 대칭키(Symmetric Key)를 사용하여 주고받는 메시지를 암호화하기 위해서 필요한 키의 총 개수는?

- ① 2개 ② 5개
③ 7개 ④ 10개

5. 해킹 방법들에 대한 설명 중 옳지 않은 것은?

- ① 스니퍼(Sniffer) : 지나가는 패킷 흐름에서 로그인, 패스워드 등을 유출함
② 스푸핑(Spoofing) : 공격자가 다른 호스트 IP Address를 자신의 패킷에 부착하여 보내는 공격 방법
③ DOS(Denial of Service) : 특정 서버의 서비스 기능을 마비시켜 다른 정당한 클라이언트가 서비스를 제공받지 못하게 함
④ TCP Wrapper : 네트워크에 연결된 호스트의 이용 가능한 서비스와 포트를 조사함으로써 원격 공격자들이 공격에 이용할 수 있는 보안 취약점들을 조사함

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

- ① 불필요한 데몬을 제거한다.
② 불필요한 Setuid 프로그램을 제거한다.
③ 시스템의 무결성을 주기적으로 검사한다.
④ 무결성을 검사하기 위한 데이터베이스를 추후 액세스가 용이하게 하기 위하여 검사할 시스템에 저장하는게 좋다.

7. SEED(128 비트 블록 암호 알고리즘)의 특성으로 옳지 않은 것은?

- ① 데이터 처리단위는 8, 16, 32 비트 모두 가능하다.
② 암·복호화 방식은 공개키 암호화 방식이다.
③ 입출력의 크기는 128 비트이다.
④ 라운드의 수는 16 라운드이다.

8. 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.
③ 필터링은 클라이언트 컴퓨터에 대한 특정한 환경설정이나 사용자에게 대한 훈련이 요구되지 않는다.
④ 패킷 필터링이 실패하면 거부되어야 하는 패킷을 통과시키는 경우가 많다.

9. 암호화의 목적은?

- ① 정보의 보안 유지 ② 정보의 전송
③ 정보의 교류 ④ 정보의 전달

10. 공인인증서란 인터넷상에서 발생하는 모든 전자거래를 안심하고 사용할 수 있도록 해주는 사이버신분증이다. 공인인증서에 반드시 포함되어야 하는 사항으로 옳지 않은 것은?

- ① 가입자 이름 ② 유효 기간
③ 일련 번호 ④ 용도

2과목 : 운영체제

11. 로그를 기록해 주는 'syslogd'의 설정과 관련한 사항으로 옳지 않은 것은?

- ① LOG_AUTHPRIV : Security/Authorization관련 로그 기록
② LOG_CRON : Clock Daemon에 대한 로그 기록
③ LOG_DAEMON : 인터넷 슈퍼 Daemon에 대한 로그 기록
④ LOG_KERN : 커널 메시지에 대한 로그 기록

12. 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

13. 프락시 서버(Proxy Server)의 기능을 올바르게 설명한 것은?

- ① 데이터의 에러를 복구해 주는 기능을 가지고 있다.
② 전자우편에 대한 보안 서비스 기능을 제공한다.
③ HTTP에 대해서만 수행할 수 있다.
④ 데이터를 인증하며 부분적인 캐쉬 기능을 가지고 있다.

14. DHCP(Dynamic Host Configuration Protocol) Scope 범위 혹은 주소 풀(Address Pool)을 만드는데 주의할 점에 속하지 않는 것은?

- 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.
④ 하나의 서브넷에는 여러 개의 DHCP 범위가 사용될 수 있다.

15. 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.
③ /boot : LILO 설정 파일과 같은 부팅 관련 파일들이 들어있다.

④ /dev : 디바이스 장치 파일들이 위치한다.

16. ifconfig 명령으로 IP Address를 설정할 때 사용하는 값으로 가장 옳지 않은 것은?

- ① Subnet Mask ② Broadcast Address
③ Network Address ④ Unicast Address

17. 파일이 생성된 시간을 변경하기 위해 사용하는 Linux 명령어는?

- ① chown ② chgrp
③ touch ④ chmod

18. 다음 명령어 중에서 시스템의 메모리 상태를 보여주는 명령어는?

- ① mkfs ② free
③ ps ④ shutdown

19. Linux에서 'netstat -an' 명령으로 어떤 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]# 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      -           -         /dev/log
unix    2      [ ] DGRAM      -           -         -
unix    2      [ ] DGRAM      -           -         -
unix    2      [ ] DGRAM      -           -         -
unix    2      [ ] DGRAM      -           -         -
unix    2      [ ] STREAM    CONNECTED  537      -

```

- ① MySQL ② DHCP
③ Samba ④ Backdoor

20. 커널의 대표적인 기능으로 옳지 않은 것은?

- ① 파일 관리 ② 기억장치 관리
③ 명령어 처리 ④ 프로세스 관리

21. 삼바 데몬을 Linux에 설치하여 가동하였을 때 열리는 포트 로 알맞게 나열한 것은?

- ① UDP 137, 139 ② TCP 137, 139
③ TCP 80, 25 ④ UDP 80, 25

22. 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?

- ① 701 ② 777
③ 755 ④ 705

23. Linux 시스템에서 현재 사용자가 수행되는 백그라운드 작업을 출력하는 명령어는?

- ① jobs ② kill
③ ps ④ top

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

- ① ping ② traceroute

③ netstat

④ nslookup

25. Linux에서 현재 사용하고 있는 셸(Shell)을 확인해 보기 위한 명령어는?

- ① echo \$SHELL ② vi \$SHELL
③ echo &SHELL ④ vi &SHELL

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

- ① lpd ② netfs
③ nscd ④ named

27. 이메일에서 주로 사용하는 프로토콜로 옳지 않은 것은?

- ① SMTP ② POP3
③ IMAP ④ SNMP

28. Linux 파일 시스템의 마운팅과 논리적 계층 구조에 관련된 내용이라 할 수 없는 것은?

- ① Linux는 모든 블록 장치에 존재하는 파일 시스템들을 마운트 하여 사용한다.
② 파일 시스템이 존재하는 논리적인 파티션을 소스(Source)하고, 논리적 파일계층 구조에서 위치할 경로를 대상으로 마운트 시킨다.
③ 마운트의 기본 디렉터리는 '/var'이다.
④ 제한된 디스크 공간을 여러 사용자가 공유하는 경우에 쿼터의 사용이 필요하다.

29. Linux에 등록된 사용자들 중 특정 사용자의 Telnet 로그인만 중지시키려면 어떤 방법으로 중지해야 하는가?

- ① Telnet 포트를 막는다.
② /etc/hosts.deny 파일을 편집한다.
③ Telnet 로그인을 막고자 하는 사람의 셸을 false로 바꾼다.
④ /etc/passwd 파일을 열어서 암호부분을 * 표시로 바꾼다.

30. Linux 파일 시스템의 기본 구조 중 파일에 관한 중요한 정보를 실는 곳은?

- ① 부트 블록 ② i-node 테이블
③ 슈퍼 블록 ④ 실린더 그룹 블록

3과목 : 네트워크

31. 라우터 명령어 중 NVRAM에서 RAM으로 configuration file을 copy하는 명령어는?

- ① copy flash start
② copy running-config startup-config
③ copy startup-config running-config
④ wr mem

32. 통신 에러제어는 수신측이 에러를 탐지하여 송신자에게 재전송을 요구하는 ARQ(Automatic Repeat Request)를 이용하게 된다. ARQ 전략으로 옳지 않은 것은?

- ① Windowed Wait and Back ARQ
② Stop and Wait ARQ
③ Go Back N ARQ

④ Selective Repeat ARQ

33. 전화망에 일반적으로 Twisted-Pair Cable을 많이 사용한다. Twisted-Pair Cable을 꼬아 놓은 가장 큰 이유는?

- ① 수신기에서 잡음을 감소하기 위하여
- ② 관리가 용이하게 하기 위하여
- ③ 꼬인 선의 인장 강도를 크게 하기 위하여
- ④ 구분을 용이하게 하기 위하여

34. 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 ④ CSMA/CD

35. IPv6 프로토콜의 구조는?

- ① 32bit ② 64bit
- ③ 128bit ④ 256bit

36. 네트워크 아키텍처에 관한 설명으로 옳지 않은 것은?

- ① Ethernet은 가장 광범위하게 설치된 근거리 통신이다.
- ② 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 목적으로 사용하는 장치이다.

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

- ① Transport Layer ② Datalink Layer
- ③ Presentation Layer ④ Application Layer

38. '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.
- ③ 같은 네트워크 내에 있는 모든 컴퓨터들이 응답패킷을 보낸다.
- ④ 자기 자신에게 'ICMP_ECHO_REQUEST' 패킷을 보낸다.

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

- ① 물리 계층 ② 세션 계층
- ③ 네트워크 계층 ④ 트랜스포트 계층

40. X.25 프로토콜에서 회선 설정, 데이터 교환, 회선 종단 단계

를 가지며, 패킷의 종단 간(End-to-End) 패킷 전송을 위해 사용되는 방식은?

- ① 데이터그램 방식 ② 회선 교환 방식
- ③ 메시지 교환 방식 ④ 가상 회선 방식

41. HDLC 프레임 구조의 순서가 올바른 것은?(단, 'F'는 플래그 시퀀스, 'C'는 제어부, 'A'는 어드레스부, 'I'는 정보부, 'FCS'는 프레임 검사 시퀀스이다.)

- ① F - A - C - I - FCS - F
- ② F - A - I - C - FCS - F
- ③ F - I - C - A - FCS - F
- ④ C - I - A - C - FCS - F

42. 서브넷 마스크에 대한 설명으로 올바른 것은?

- ① DNS 데이터베이스를 관리하고 IP Address를 DNS의 이름과 연결한다.
- ② IP Address에 대한 네트워크를 분류 또는 구분한다.
- ③ TCP/IP의 자동설정에서 사용되는 프로토콜로서 정적, 동적 IP Address를 지정하고 관리한다.
- ④ 서로 다른 네트워크를 연결할 때 네트워크 사이를 연결하는 장치이다.

43. TCP의 Header 구성은?

- ① 각 32비트로 구성된 6개의 단어
- ② 각 6비트로 구성된 32개의 단어
- ③ 각 16비트로 구성된 7개의 단어
- ④ 각 7비트로 구성된 16개의 단어

44. 패킷(Packet)에 있는 정보로 옳지 않은 것은?

- ① 출발지 IP Address ② TCP 프로토콜 종류
- ③ 전송 데이터 ④ 목적지 IP Address

45. OSI 7 Layer 구조에서 계층 7에서 계층 4를 차례대로 나열한 것은?

- ① 응용 - 세션 - 표현 - 전송
- ② 응용 - 표현 - 세션 - 전송
- ③ 응용 - 표현 - 세션 - 네트워크
- ④ 응용 - 네트워크 - 세션 - 표현

4과목 : 보안

46. 해킹에 성공한 후 해커들이 하는 행동의 유형으로 옳지 않은 것은?

- ① 추후에 침입이 용이하게 하기 위하여 트로이 목마 프로그램을 설치한다.
- ② 서비스 거부 공격 프로그램을 설치한다.
- ③ 접속 기록을 추후의 침입을 위하여 그대로 둔다.
- ④ 다른 서버들을 스캔 프로그램으로 스캔하여 취약점을 알아낸다.

47. SSH(Secure Shell)에 대한 설명으로 옳지 않은 것은?

- ① 안전하지 못한 네트워크에서 안전하게 통신할 수 있는 기능과 강력한 인증방법을 제공한다.
- ② 문자를 암호화하여 IP Spoofing, DNS Spoofing으로부터 보호할 수 있다.
- ③ 쌍방 간 인증을 위해 Skipjack 알고리즘이 이용된다.

- ④ 네트워크의 외부 컴퓨터에 로그인 할 수 있고 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해주는 프로그램이다.
48. IIS를 통하여 Web 서비스를 하던 중 '.asp' 코드가 외부 사용자에게 의하여 소스코드가 유출되는 버그가 발생하였다. 기본적으로 취해야 할 사항으로 옳지 않은 것은?
- ① 중요 파일(global.asa 등)의 퍼미션을 변경 혹은 파일 수정을 통하여 외부로부터의 정보유출 가능성을 제거한다.
 - ② '.asp'의 권한을 실행권한만 부여한다.
 - ③ 'C:\WINDOWS\System32\Winetsrv\Wasp.dll'에 매칭되어 있는 '.asp'를 제거한다.
 - ④ '.asp'가 위치한 디렉터리와 파일에서 Read 권한을 제거한다.
49. 현재 Linux 시스템 상에서 침입자의 침입여부나 사용자의 사용여부를 확인하고자 한다. 적합한 명령어로 옳지 않은 것은?
- ① [root@icqa /bin]#w
 - ② [root@icqa /bin]#netstat -t
 - ③ [root@icqa /bin]#nuser -a
 - ④ [root@icqa /bin]#who
50. 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
 - ④ 웹 서버의 서비스를 중단 시키고, 공격자가 서버에 도착하는 모든 패킷을 가로채는 방법
51. Linux에서 Nmap의 옵션 중 상대방의 OS를 알아내는 옵션은?
- ① [root@icqa bin]#./nmap -O www.target.com
 - ② [root@icqa bin]#./nmap -l www.target.com
 - ③ [root@icqa bin]#./nmap -sS www.target.com
 - ④ [root@icqa bin]#./nmap -sP www.target.com
52. 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.
 - ③ 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.
53. 다음 중 파일 보호 방식에서 사용되는 보호 기법으로 옳지 않은 것은?
- ① 파일 감춤법
 - ② 접근 리스트법
 - ③ 암호법
 - ④ 파일의 명명법

54. Tripwire의 특징으로 옳지 않은 것은?

- ① 어셈블리어로 작성되어 거의 모든 플랫폼에서 정상적으로 컴파일 된다.
- ② 설치 전에 네트워크를 위한 전자서명 값의 데이터베이스를 구축할 수 있다.
- ③ 데이터베이스의 승인되지 않은 변경으로부터 보호를 한다.
- ④ 매크로 처리언어로 특정작업을 자동으로 수행할 수 있다.

55. SYN 플러딩 공격에 대한 설명으로 옳바른 것은?

- ① TCP 프로토콜의 3-way handshaking 방식을 이용한 접속의 문제점을 이용하는 방식으로, IP 스푸핑 공격을 위한 사전 준비 단계에서 이용되는 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.

56. TCPdump 가 동작하기 위해 필요한 라이브러리는?

- ① ncurses
- ② libpcap
- ③ libmod
- ④ modperl

57. IP Spoofing 공격을 예방하는 방법으로 옳지 않은 것은?

- ① IP Spoofing은 DoS(Denial of Service) 공격을 막는 것이 곧 IP Spoofing을 막는 방법이다.
- ② IP 패킷의 순서 번호 생성을 무작위로 한다.
- ③ 보안화된 패킷전송을 위한 DNS를 설정한다.
- ④ 외부에서 들어오는 패킷 중에서 출발지 IP Address에 내부 망 IP Address를 가지고 있는 패킷을 라우터 등에서 패킷 필터링을 사용하여야 한다.

58. DDoS(Distributed Denial of Service) 공격용 기법이나 도구로 알려진 것이 아닌 것은?

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

59. PGP(Pretty Good Privacy)에 대한 설명으로 잘못된 것은?

- ① 1991년 미국의 Phil Zimmerman 에 의해 개발된 전자우편 보안도구이다.
- ② MAC에서는 활용할 수 없다.
- ③ 구현이 용이하고 사용된 알고리즘의 안전성이 높다.
- ④ 메시지 기밀성, 전자서명, 압축, 전자우편 호환성 등의 기능을 제공한다.

60. Linux 시스템에서 Rootkit의 역할로 옳지 않은 것은?

- ① 불법적인 권한을 다시 획득하는 역할을 수행한다.
- ② 시스템 상에서 침입자의 흔적을 지워주는 역할을 수행한다.
- ③ 정상적인 프로그램처럼 보이지만 내부에 악의적인 코드가 내장되어있다.
- ④ 자가 복제를 통해 자신의 존재를 숨기면서 다른 시스템과의 접속을 시도한다.

전자문제집 CBT PC 버전 : www.comcbt.com
 전자문제집 CBT 모바일 버전 : m.comcbt.com
 기출문제 및 해설집 다운로드 : www.comcbt.com/x

전자문제집 CBT란?

종이 문제집이 아닌 인터넷으로 문제를 풀고 자동으로 채점하며 모의고사, 오답 노트, 해설까지 제공하는 무료 기출문제 학습 프로그램으로 실제 시험에서 사용하는 OMR 형식의 CBT를 제공합니다.

PC 버전 및 모바일 버전 완벽 연동
 교사용/학생용 관리기능도 제공합니다.

오답 및 오탈자가 수정된 최신 자료와 해설은 전자문제집 CBT에서 확인하세요.

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