

1과목 : 정보보호개론

1. 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

2. 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.
③ 클라이언트의 공개키를 요구하지 않으므로 사용자 개인의 공개키를 선언해 놓지 않고 사전적인 트랜잭션을 시도할 수 있다.
④ S-HTTP를 탑재하지 않은 시스템과 통신이 어렵다.

3. 네트워크상의 부당한 피해라고 볼 수 없는 것은?

- ① 침입자가 부당한 방법으로 호스트의 패스워드 정보를 입수한 후 유용한 정보를 가져가는 경우
② 특정인이나 특정 단체가 고의로 호스트에 대량의 패킷을 흘려 보내 호스트를 마비시키거나 패킷 루프와 같은 상태가 되게 하는 경우
③ 특정인이나 특정 단체가 네트워크상의 흐르는 데이터 패킷을 가로채 내거나 다른 불법 패킷으로 바꾸어 보내는 경우
④ HTTP 프로토콜을 이용하여 호스트의 80번 포트로 접근하여 HTML 문서의 헤더 정보를 가져오는 경우

4. 암호 알고리즘 중 송, 수신자가 동일한 키에 의해 암호화 및 복호화 과정을 수행하는 암호 알고리즘은?

- ① 대칭키 암호 알고리즘 ② 공개키 암호 알고리즘
③ 이종키 암호 알고리즘 ④ 해시 암호 알고리즘

5. 응용계층 프로토콜로 옳지 않은 것은?

- ① SMTP ② FTP
③ Telnet ④ TCP

6. 암호 프로토콜 서비스에 대한 설명 중 옳지 않은 것은?

- ① 비밀성 : 자료 유출의 방지
② 접근제어 : 프로그램 상의 오류가 발생하지 않도록 방지
③ 무결성 : 메시지의 변조를 방지
④ 부인봉쇄 : 송수신 사실의 부정 방지

7. IPSec 프로토콜에 대한 설명으로 옳지 않은 것은?

- ① 네트워크 계층인 IP 계층에서 보안 서비스를 제공하기 위한 보안 프로토콜이다.
② 기밀성 기능은 AH(Authentication Header)에 의하여 제공되고, 인증 서비스는 ESP(Encapsulating Security Payload)에 의하여 제공된다.
③ 보안 연계(Security Association)는 사용된 인증 및 암호 알고리즘, 사용된 암호키, 알고리즘의 동작 모드 그리고 키의 생명 주기 등을 포함한다.
④ 키 관리는 수동으로 키를 입력하는 수동방법과 IKE 프로토콜을 이용한 자동방법이 존재한다.

8. 다음은 어떠한 바이러스에 대한 설명인가?

- UDP 1434 포트가 이용되었으며, 코드레드와 같이 메모리상에 상주하는 악성코드이다.
- ISP의 DNS 서버 장애로 인터넷 접속 장애 또는 지연이 발생하였다.

- ① Michelangelo ② Trojan Horse
③ Worm.SQL.Slammer ④ Nimda

9. 네트워크 또는 응용을 위한 보안 대책으로 옳지 않은 것은?

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

10. RSA 암호화 알고리즘에 대한 설명으로 옳지 않은 것은?

- ① 공개키 암호화 알고리즘 중 하나이다.
② Rivest 암호화, Adleman이 개발하였다.
③ 다른 암호화 방식에 비해 계산량이 적어, 저사양의 휴대 기기에 주로 사용된다.
④ 전자서명에 이용된다.

2과목 : 운영체제

11. Linux에서 특정한 파일을 찾고자 할 때 사용하는 명령어는?

- ① mv ② cp
③ find ④ file

12. 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.

13. Linux 시스템 파일의 설명으로 옳지 않은 것은?

- ① /etc/passwd - 사용자 정보 파일
② /etc/fstab - 시스템이 시작될 때 자동으로 마운트 되는 파일 시스템 목록
③ /etc/motd - 텔넷 로그인 전 나타낼 메시지
④ /etc/shadow - 패스워드 파일

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

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

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

- ① IP 기반의 네트워크에서만 사용가능하다.
- ② 헤드 압축을 지원한다.
- ③ 터널 인증을 지원한다.
- ④ IPsec 알고리즘을 이용하여 암호화 한다.

16. Linux 콘솔 상에서 네트워크 어댑터 'eth0'을 'ifconfig' 명령어로 '192.168.1.1' 이라는 주소로 사용하고 싶을 때 옳은 방법은?

- ① ifconfig eth0 192.168.1.1 activate
- ② ifconfig eth0 192.168.1.1 deactivate
- ③ ifconfig eth0 192.168.1.1 up
- ④ ifconfig eth0 192.168.1.1 down

17. Linux의 VI 편집기에서 수정하던 파일을 저장하지 않고 종료 시키는 명령어는?

- ① :q!
- ② :w!
- ③ :WQ!
- ④ :Wq!

18. 이미 내린 shutdown 명령을 취소하기 위한 명령어는?

- ① shutdown -r
- ② shutdown -h
- ③ cancel
- ④ shutdown -c

19. 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

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
- ③ root 유저의 home 디렉터리
- ④ 현재 디렉터리의 하위라는 의미

21. 현재 Linux 서버에 접속된 모든 사용자에게 메시지를 전송하는 명령어는?

- ① wall
- ② message
- ③ broadcast
- ④ bc

22. Linux에서 사용자의 'su' 명령어 시도 기록을 볼 수 있는 로그는?

- ① /var/log/secure
- ② /var/log/messages
- ③ /var/log/wtmp
- ④ /var/log/lastlog

23. 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 '!!'으로 채운다.
- ④ /etc/shadow 파일의 icqa의 네 번째 필드를 공백으로 만든다.

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

- ① /etc
- ② /lib
- ③ /root
- ④ /home

25. 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

26. 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

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

- ① ping
- ② traceroute
- ③ netstat
- ④ nslookup

28. 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

29. 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)

30. 커널의 대표적인 기능으로 옳지 않은 것은?

① 파일 관리

② 기억장치 관리

③ 명령어 처리

④ 프로세스 관리

3과목 : 네트워크

31. TCP/IP의 Transport Layer에 관한 설명으로 옳지 않은 것은?

① TCP는 흐름제어, 에러제어를 통하여 신뢰성 있는 통신을 보장한다.

② UDP는 신뢰성 제공은 못하지만, TCP에 비해 헤더 사이즈가 작다.

③ TCP는 3-way handshake를 이용하여 세션을 성립한 다음 데이터를 주고받는다.

④ UDP는 상위 계층을 식별하기 위하여 Protocol Field를 사용한다.

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

① DHCP는 DHCP서버가 존재하여, 요청하는 클라이언트들에게 IP Address, Gateway, DNS등의 정보를 일괄적으로 제공하는 기술이다.

② 클라이언트가 DHCP 서버에 DHCP Request를 보낼 때 브로드캐스트로 보낸다.

③ 192.168.10.2는 사설 IP Address이다.

④ 공인 IP Address를 다른 공인 IP로 변환하여 내보내는 기술이 NAT이다.

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

① 정지-대기 ARQ

② Go-back-N ARQ

③ Selective Repeat ARQ

④ 적응적 ARQ

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

① 물리 계층

② 세션 계층

③ 네트워크 계층

④ 트랜스포트 계층

35. 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

36. 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.

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

① 에러제어

② 순서제어

③ 흐름제어

④ 접속제어

38. 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

39. Distance Vector 알고리즘을 사용하는 프로토콜로 바르게 짝지어진 것은?

① OSPF, RIP

② RIP, EIGRP

③ IGRP, RIP

④ EIGRP, IGRP

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

① 255.255.228.0

② 255.255.240.0

③ 255.255.248.0

④ 255.255.255.248

41. TCP와 UDP의 차이점 설명으로 옳지 않은 것은?

① 데이터 전송형태로 TCP는 Connection Oriented방식이고 UDP는 Connectionless방식이다.

② TCP가 UDP보다 데이터 전송 속도가 빠르다.

③ TCP가 UDP보다 신뢰성이 높다.

④ TCP가 UDP에 비해 각종 제어를 담당하는 Header 부분이 커진다.

42. 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

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

① 23

② 21

③ 20

④ 25

44. 광섬유케이블의 구성요소로 옳지 않은 것은?

① 코어

② 클래드

③ 코팅

④ 스트레드

45. 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 메

시지에 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)

4과목 : 보안

46. 보안상의 문제가 있는 시스템 프로그램과 크래커(Cracker)의 Exploit Program이 서로 경쟁 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로 파일에 대한 접근을 가능하게 하는 방법은?

- ① Race Condition Problem
- ② Boundary Condition Problem
- ③ Input Validation Problem
- ④ Access Validation Problem

47. 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.

48. 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.
- ③ 공격이 진행되고 있는 상태에서 스위치와 연결된 정상적인 호스트가 통신할 때, 스위치의 MAC 정보에는 영향을 미치지 않는다.
- ④ MAC Flooding은 한 포트에서 수 천 개의 호스트가 스위치와 연결되어 있는 것으로 보이지만 실제로는 변조된 MAC 정보를 공격 호스트에서 발생시키는 것이다.

49. 방화벽의 주요 기능으로 옳지 않은 것은?

- ① 접근제어
- ② 사용자 인증
- ③ 로깅
- ④ 프라이버시 보호

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

- ① 메시지 인증
- ② 수신 부인방지
- ③ 사용자 인증
- ④ 송신 부인방지

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

- ① 스니핑
- ② IP 스푸핑
- ③ TCP wrapper
- ④ ipchain

52. 종단 간 보안 기능을 제공하기 위한 SSL 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

53. Windows 명령 프롬프트 창에서 'netstat -an' 을 실행한 결과이다. 옳지 않은 것은? (단, 로컬 IP Address는 211.116.233.104 이다.)

```
c:\w>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.

54. 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 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.

55. Linux 파일 시스템에 대한 사용자에 속하지 않는 것은?

- ① 소유자 : 파일이나 디렉터리를 처음 만든 사람
- ② 사용자 : 현재 로그인한 사용자
- ③ 그룹 : 사용자는 어느 특정 그룹에 속하며 이 그룹에 속한 다른 사람들을 포함
- ④ 다른 사용자 : 현재 사용자 계정을 가진 모든 사람

56. 다음에서 설명하는 것은?

%d, %f, %c, %s, %x, %p 등과 같이 정형화된 문자열은 printf(), sprintf(), vprintf() 등에 쓸 때 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 ④ **Format String Bug**

57. 사용자의 개인 정보를 보호하기 위한 바람직한 행동으로 보기 어려운 것은?

- ① 암호는 복잡성을 적용하여 사용한다.
② 로그인 한 상태에서 자리를 비우지 않는다.
③ 중요한 자료는 따로 백업을 받아 놓는다.
④ **좋은 자료의 공유를 위해 여러 디렉터리에 대한 공유를 설정해 둔다.**

58. Windows Server의 각종 보안 관리에 관한 설명이다. 그룹 정책의 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 **공개 키 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.

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

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

60. 침입 탐지 시스템을 비정상적인 침입탐지 기법과 오용탐지 기법으로 구분할 경우, 오용탐지기법은?

- ① 상태 전이 분석 ② 행위 측정 방식들의 결합
③ 통계적인 방법 ④ 특징 추출

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