

# 2017년 경찰간부후보생 정보보호론 풀이

by 호이호이꿀떡

※ 빠른 정답 체크는 마지막 페이지 우측 하단으로!

## 1. 다음 지문에서 설명하는 기법은 무엇인가?

가. 그림 또는 문장 속에 비밀자료를 숨겨서 전달하는 방법  
 나. 그림의 픽셀 중 일부를 저장하고 싶은 데이터로 대체하여 저장하는 방법  
 다. 원본 그림과 대체된 그림을 육안으로 봐서는 구별할 수 없다.

- ① 전자서명(Digital Signature)
- ② 인증서(Certificate)
- ③ 스테가노그래피(Steganography)
- ④ 제로데이 공격(Zero-Day Attack)

답 ③

- ③ 스테가노그래피(steganography)는 보통의 데이터에 또 다른 정보나 데이터를 보이지 않게 삽입하는 기술이다.
- ① 전자서명(Digital Signature)은 디지털 문서를 작성하거나 전송할 때 서명함으로써, 누가 서명을 하였고 누가 그 문서를 전송하였는지 확인하기 위한 장치이다.  
『전자서명법』 제 2 조 2 항  
"전자서명"이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
- ② 인증서(Certificate)는 전자 서명의 검증에 필요한 공개키가 위변조되지 않았다는 것을 인증해주는 전자문서이다.
- ④ 제로데이 공격(Zero-Day Attack)은 운영체제나 소프트웨어의 보안 취약점에 대한 업데이트 패치가 나오기 전에, 그 취약점을 이용하여 공격하는 방법이다.

## 2. Diffie-Hellman 알고리즘은 비밀키를 공유하는 과정에서 특정 공격에 취약할 가능성이 존재한다. 이러한 취약점을 이용하여 공격하는 방법은 무엇인가?

- ① DDoS(Distributed Denial of Service) 공격
- ② 중간자 개입(Man-In-The-Middle) 공격
- ③ 세션 하이재킹(Session Hijacking) 공격
- ④ 강제지연(Forced-Delay) 공격

답 ②

- ② 중간자 개입(Man-In-The-Middle, MITM) 공격은 연결하는 두 송수신자 사이에 중간자가 침입하여 한쪽에서 전달된 정보를 도청한 뒤 이를 다른 쪽에 전달하는 공격이다. 두 송수신자는 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며, 중간자는 해당 정보를 도청한 한 뒤 그대로 보낼 수도 있고, 조작하여 보낼 수도 있다.  
디피 헬만 키 교환은 중간자 공격에 취약하다는 단점이 있다.
- ① 디피 헬만은 키를 교환하기 위한 알고리즘으로, 서버의 가용성을 침해하는 DoS와는 상관이 없다.  
DoS(Denial of Service, 서비스 거부 공격)은 해당 시스템의 자원을 고갈시켜 제대로 사용하지 못하게 하는 공격이다. DDoS(Distributed DoS, 분산 서비스 거부 공격)은 다수의 시스템을 이용해 DoS 공격을 하는 것이다.  
DRDoS(Distributed Reflect DoS, 분산 반사 서비스 거부 공격)은 패킷의 출발지 IP 주소를 공격 대상의 IP 주소로 스푸핑한 TCP-SYN 패킷을 브로드캐스트로 다수의 시스템에 전송하여, 패킷을 받은 단말들이 보내는 응답 패킷을 공격 대상으로 물리게 만들어 공격 대상의 시스템 자원을 고갈시켜 서비스를 마비시키는 공격이다.
- ③ 세션 하이재킹(Session Hijacking) 공격 시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채기 하는 공격이다.
- ④ 강제지연(Forced-Delay) 공격  
공격자가 통신을 주고 받는 두 송수신자 사이에 개입하여, 그들이 보내는 통신 정보를 가로채 두었다가 일정 시간이 흐른 뒤 전송하는 공격이다.  
강제지연 공격은 빠른 메시지 전송이 중요한 전자상거래 등 e-비즈니스 사업에 큰 손해를 끼칠 가능성이 있다.

3. 다음 중 암호화 키와 복호화 키가 서로 다른 암호화 알고리즘은 무엇인가?

- ① DES 알고리즘
- ② IDEA 알고리즘
- ③ AES 알고리즘
- ④ RSA 알고리즘

답 ④

- ④ 암호화 키와 복호화 키가 다른 것은 공개키 암호 알고리즘이다.  
RSA 알고리즘은 소인수분해의 어려움에 기반한 공개키 암호 알고리즘이다.
- 대칭키 암호 알고리즘  
DES, 3-DES, IDEA, AES, RC5, Skipjack, Blowfish  
(국산 대칭키) SEED, HIGHT, ARIA, LEA, LSH
- 비대칭키 암호(공개키 암호) 알고리즘  
RSA : 소인수분해  
Rabin : 소인수분해  
ElGamal : 이산대수  
ECC : 타원곡선 상의 이산대수  
Schnorr : 이산대수, ElGamal 에 기반, 짧은 키 길이  
DSA : 이산대수, Schnorr 의 응용  
DSS : 이산대수, 전자서명 전용  
ECDSA : 내부적으로 타원곡선  
Knapsack : 부분집합의 합을 구하는 문제(NP-complete 문제)  
KCDSA : 국산, 국내표준  
ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

4. AES 알고리즘에 관한 설명 중 옳지 않은 것은 무엇인가?

- ① AES 는 128, 192, 256 비트 키를 사용하고 키 크기에 따라 각각 10, 12, 14 라운드를 갖는다.
- ② 마스터 키의 크기가 달라도 라운드 키는 모두 128 비트이다.
- ③ AES 는 바이트 기반 암호이다.
- ④ 안전성을 보장하기 위하여 AES 는 모든 라운드에 대치, 치환, 뒤섞음, 키덧셈의 네 종류 변환을 사용한다.

답 ④

- ④ AES 는 각 단계에서 바이트 치환(SubBytes), 행 이동(ShiftRows), 열 혼합(MixColumns), 키 덧셈(AddRoundKey)의 4 단계를 거친다.  
단, 마지막 단계에서는 열 혼합을 제외한 3 단계만 수행한다. 그러므로 모든 라운드에서 네 종류 변환을 사용한다는 말이 틀렸다.

※ 문제에는 대치, 치환, 뒤섞음, 키덧셈의 네 종류라고 나와있는데, 대치와 치환(Substitution)은 같은 의미다.  
치환(혹은 대치), 전치, 뒤섞음, 키덧셈이라고 쓰였어야 한다.

AES(Advanced Encryption Standard)

- SPN 구조
- 블록 128 비트(16 바이트)
- 키 길이 128 비트 - 10 라운드
- 키 길이 192 비트 - 12 라운드
- 키 길이 256 비트 - 14 라운드

5. 다음 중 공개키 암호 시스템의 장점이 아닌 것은 무엇인가?

- ① 키의 분배가 용이하다.
- ② 사용자의 증가에 따라 관리할 키의 개수가 상대적으로 적다.
- ③ 암호화 및 복호화가 빠르다.
- ④ 키 변화의 빈도가 적다.

답 ③

- ③ 공개키는 대칭키보다 키의 길이도 길며, 암호화 복호화 속도도 느리다.
- ① 대칭키는 송수신자가 같은 키를 사용해야 하기 때문에 안전하게 키를 주고 받는 과정이 필요한 반면, 공개키는 암호화 키와 복호화 키가 다르기 때문에 암호화 키를 중간에도 전달해도 큰 문제가 없어 키를 분배하기에 용이하다.
- ② 대칭키는 각 통신 상대방마다 다른 키를 사용하기 때문에 사용자 수가 늘어날 경우 관리해야 할 키가 매우 늘어나지만, 공개키는 상대방이 몇 명이든 상관없이 개인별로 개인 키와 공개키 2 개씩만 가지고 있으면 된다.
- ④ 공개키 알고리즘에서 개인키는 소유자 본인만이 아는 키이기 때문에 상대적으로 키를 오래 사용할 수 있다.

6. 다음 중 전자서명(Digital Signature)에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

- ① 인증(Authentication) 기능을 제공하며 개인키로 암호화된 메시지를 제 3 자의 공개키로 복호화 할 경우 메시지를 읽을 수 없다.
- ② 비밀성(Confidentiality) 기능을 제공하며 대칭키 암호화 알고리즘을 이용하여 전자서명을 생성할 수 있다.
- ③ 무결성(Integrity) 기능을 제공하며 메시지의 부분 또는 전체를 바꿀 경우 복호화된 메시지를 통해 변경 여부를 확인할 수 있다.
- ④ 부인방지(Non-Repudiation) 기능을 제공하며 송신자의 개인키와 공개키를 가지고 암호화와 복호화하여 저장된 메시지를 생성할 수 있다.

답 ②

- ② 전자서명(Digital Signature)은 누가 그 문서를 전송하였는지 확인하기 위한 기술로, 전자서명을 생성할 때 개인키를, 전자서명을 검증할 때 공개키를 사용한다. 전자서명을 검증할 때 누구나 확인할 수 있도록 공개키를 사용하기 때문에 비밀성(기밀성)은 보장할 수 없다. 또한 전자서명은 대칭키 알고리즘이 아닌 공개키 알고리즘을 사용한다.

7. 다음 중 로봇프로그램과 사람을 구분하는 방법의 하나로 사람이 인식할 수 있는 문자나 그림을 활용하여 자동 회원가입 및 게시글 포스팅을 방지하는데 사용하는 방법은 무엇인가?

- ① 해시함수(Hash Function)
- ② 인증서(Certificate)
- ③ 전자서명(Digital Signature)
- ④ 캡차(CAPTCHA)

답 ④

④ 캡차(CAPTCHA, Completely Automated Public Turing test to tell Computers and Humans Apart)

어떠한 사용자가 실제 사람인지 컴퓨터 프로그램인지를 구별하기 위해 사용되는 방법이다.

의도적으로 일그러뜨린 텍스트나 이미지를 주고 그에 대한 내용을 물어보는 방법이 자주 사용하는데, 이것은 실제 사람은 쉽게 인식할 수 있지만, 컴퓨터 프로그램은 변형된 텍스트나 이미지를 인식하지 못하므로 사람이 아니라는 걸 확인할 수 있다.

웹사이트에 회원가입이나 게시글을 작성할 때 자동가입 프로그램을 걸러내기 위해 사용된다.

8. 다음 중 공인인증서의 설명으로 옳지 않은 것은 무엇인가?

- ① 공인인증서는 사용자의 공개키와 사용자의 ID 정보를 결합하여 인증기관의 전자서명을 포함한 문서이다.
- ② 공인인증서에는 버전, 발행자, 유효기간, 알고리즘 식별자, 사용자의 개인키 등이 포함되어 있다.
- ③ 인증기관이 자신의 키를 이용하여 전자서명을 생성 후, 인증서에 첨부하고, 인증기관 키를 사용하여 인증서의 유효성을 확인한다.
- ④ 공인인증서 관련한 표준으로 X.509 가 있으며 대부분의 인증서는 이 표준을 따르고 있다.

답 ②

인증서(Certificate)는 전자 서명의 검증에 필요한 공개키가 위변조되지 않았다는 것을 인증해주는 전자문서이다.

- ② 개인키는 사용자 본인만 가지고 있어야 한다. 인증서에는 공개키가 포함된다.
- ③ 인증서에는 인증기관의 개인키로 생성한 서명이 첨부되어 있다. 인증서 이용자는 인증기관의 공개키로 이 서명을 검증하여, 인증서가 위변조되지 않았다는 것을 확인할 수 있다.

9. 디스크 스케줄링 정책 중 큐의 항목을 순차적으로 처리하는 것은 무엇인가?

- ① SSTF(Shortest Service Time First)
- ② FIFO(First-In-First-Out)
- ③ SCAN
- ④ C-SCAN(Circular SCAN)

답 ②

(: 정보보호론 과목인데, 컴퓨터일반과 자료구조에 대한 내용이 출제되었다.)

② 큐(queue)는 먼저 집어 넣은 데이터가 먼저 나오는 FIFO (First In First Out) 형식으로 저장하는 자료 구조이다.  
rear 에서 자료의 삽입이 이루어지고, front 에서 자료의 삭제 이루어진다.  
먼저 집어 넣은 데이터를 먼저 처리하는 디스크 스케줄링 방식은 FCFS(=FIFO) 스케줄링이다.

※ 디스크 스케줄링 기법

- FCFS 스케줄링(First Come First Served)=FIFO  
요청이 들어온 순서대로 처리
- SSTF 스케줄링(Shortest Seek Time First)  
현재 디스크의 헤드 위치에서 가장 가까운 실린더에 대한 요청을 우선적으로 처리
- SCAN 스케줄링  
디스크의 한 쪽 끝에서 반대쪽 끝으로 이동하면서 처리하며, 마지막 실린더에 도착하면 반대 방향으로 스캔을 진행 양방향으로 진행
- C-SCAN(Circular SCAN) 스케줄링  
디스크의 한 쪽 끝에서 반대쪽 끝으로 이동하면서 처리하며, 마지막 실린더에 도착하면 시작점으로 되돌아간 후 다시 스캔을 진행  
항상 바깥쪽에서 안쪽으로만 진행
- LOOK 스케줄링  
SCAN 기법과 같이 한 쪽 끝에서 반대쪽 끝으로 이동하면서 처리하되, 진행방향의 마지막 요청까지 서비스를 완료하면, 반대쪽 끝에 요청이 없을 경우 굳이 끝까지 이용하지 않고 바로 방향을 바꿔서 진행
- C-LOOK(Circular LOOK) 스케줄링  
C-SCAN 기법과 같이 한 쪽 방향으로만 이동하면서 처리하되, 끝까지 이동하지 않고 마지막 요청을 처리한 후 바로 제일 처음으로 이동한 후 다시 스캔을 진행
- N 단계 SCAN 스케줄링  
SCAN 기법과 같이 진행 방향 상의 요청을 서비스하지만, 진행 중에 새로이 추가된 요청은 서비스하지 않고 다음 진행 시에 서비스하는 기법

10. 컴퓨터의 메모리는 사용되는 방식에 따라 여러 개의 영역으로 나누어 생각할 수 있는데 프로그램 실행 중 malloc()등의 system call 로 할당되어 사용되다가 free()등의 system call 로 해제되는 영역은 무엇인가?

- ① Text 영역
- ② Data 영역
- ③ Stack 영역
- ④ Heap 영역

답 ④

프로그램 실행 중 메모리를 malloc()으로 할당하여 사용하다가 free()로 반납하는 것은 동적 메모리 할당(dynamic memory allocation)을 의미한다.

- ④ Heap(힙) 영역  
필요에 의해 동적으로 메모리를 할당 할 때 사용  
쓰기 가능, 크기 가변
- ① Text(텍스트) 영역 = Code(코드) 영역  
소스 코드 자체를 기계어로 변환하여 저장되는 영역으로, 변수가 아닌 순수 코드만 있는 공간이다.  
쓰기 금지, 크기 고정
- ② Data(데이터) 영역  
전역 변수와 정적(static) 변수가 할당되는 영역  
프로그램의 시작과 동시에 할당되고, 프로그램이 종료되어야 메모리에서 소멸됨  
쓰기 가능, 크기 고정  
(좀 더 세분화하면 데이터 영역에는 초기화된 전역 변수와 정적 변수가 저장되고, 초기화되지 않은 전역 변수와 정적 변수는 BSS (Block Stated Symbol) 영역에 저장된다.)
- ③ Stack(스택) 영역  
함수 호출 시 생성되는 지역 변수와 매개 변수가 저장되는 영역  
함수 호출이 완료되면 사라짐  
쓰기 가능, 크기 가변

11. 유닉스(Unix) 운영체제에서 파일에 대한 권한을 모두 허용(-rwxrwxrwx)하는 모드(명령어)는 무엇인가?

- ① chmod 777
- ② chmod a-rwx
- ③ chmod 666
- ④ chmod ug+rw

답 ①

chmod(change mode)는 파일이나 디렉터리에 대한 권한을 변경하는 명령어다.

- ① rwx 에서 각각 r(읽기)은 4, w(쓰기)는 2, x(실행)는 1로 계산된다.  
 $r + w + x = 4 + 2 + 1 = 7$
- ② a-는 모두(all)에게서 권한을 제거(-)한다.  
a-rwx 는 모든 사용자들의 읽기, 쓰기, 실행 권한을 모두 제거
- ③ 666 은 읽기(r)과 쓰기(w)의 권한이 부여된다. 신라 지증왕)
- ④ ug+는 소유자(user)와 그룹(group)에게 권한을 부여(+).  
ug+rw 는 소유자와 그룹에게 읽기와 쓰기 권한을 부여

12. 리눅스(Linux) 사용자의 패스워드를 암호화하여 저장하고 있는 파일은 무엇인가?

- ① /etc/shadow
- ② /etc/passwd
- ③ /etc/skel
- ④ /etc/group

답 ①

- ① 패스워드 부분만 암호화해 따로 저장한 것이 shadow 파일로, shadow 파일은 관리자만이 접근할 수 있다.
- ② passwd 파일에는 사용자의 ID 와 패스워드를 비롯한 정보가 저장되어 있는데, 이 파일은 누구나 열람할 수 있어 보안에 취약하다.
- ③ skel 디렉터리에는 사용자를 처음 생성했을 때 해당 계정의 홈디렉터리에 기본으로 들어가는 파일을 저장된다. 사용자 생성시 skel 디렉터리 안에 있는 파일을 계정 홈디렉토리로 복사한다.
- ④ group 파일에는 그룹의 기본 정보가 들어있다.



15. 다음은 윈도우 7 운영체제의 명령어 창에서 어떤 명령어를 실행한 출력 결과의 일부이다. 실행한 명령어는 무엇인가?

| 이미지 이름       | PID   | 세션 이름    | 세션#   | 메모리 사용   |
|--------------|-------|----------|-------|----------|
| =====        | ===== | =====    | ===== | =====    |
| System Idle  | 0     | Services | 0     | 12 K     |
| Process      | 4     | Services | 0     | 284 K    |
| System       | 472   | Services | 0     | 844 K    |
| smss.exe     | 592   | Services | 0     | 4,672 K  |
| csrss.exe    | 648   | Console  | 1     | 16,528 K |
| csrss.exe    | 656   | Services | 0     | 4,288 K  |
| wininit.exe  | 708   | Services | 0     | 9,260 K  |
| services.exe | 732   | Services | 0     | 8,900 K  |
| lsass.exe    | 740   | Console  | 1     | 6,244 K  |
| winlogon.exe | 768   | Services | 0     | 4,580 K  |
| lsm.exe      | 868   | Services | 0     | 7,340 K  |
| svchost.exe  | 928   | Services | 0     | 5,780 K  |
| nvsvcs.exe   | 960   | Services | 0     | 6,564 K  |
| svchost.exe  | 1048  | Services | 0     | 3,228 K  |

- ① netstat -an                      ② ipconfig /all
- ③ tasklist                          ④ arp -a

답 ③

- ③ 현재 실행되고 있는 프로세스 목록을 표시한 것으로 tasklist 명령어에 해당한다.
- ① netstat 는 네트워크의 연결상태, 네트워크 인터페이스 상태를 확인하는 명령어이다.
  - a 옵션은 연결되지 않은 소켓의 정보까지 모두 표시하고,
  - n 옵션은 호스트나 포트명을 숫자로 표시해준다.
- ② ipconfig 는 물리적, 논리적으로 연결된 네트워크 장치들과 해당 장치에 연결된 IP 주소 정보를 표시해주는 명령어이다.
  - /all 옵션은 보다 자세한 내용을 표시해준다.
- ④ arp 는 시스템이 가지고 있는 ARP 테이블의 목록을 확인, 추가, 삭제하는 명령어이다.
  - a 옵션은 ARP 테이블 보기
  - d 옵션은 ARP 테이블에서 해당 IP 삭제
  - s 옵션은 ARP 테이블에 해당 IP 와 MAC 주소 추가

16. 유닉스(Unix) 운영체제의 로그파일과 그 로그파일에 기록되는 내용을 바르게 짝지은 것은 무엇인가?

- 가. history - 각 사용자별 수행한 명령을 기록
- 나. sulog - su 명령어의 로그를 기록
- 다. xferlog - 실패한 로그인 시도를 기록
- 라. loginlog - FTP 파일 전송 내역을 기록

- ① 가, 나                              ② 가, 다
- ③ 나, 다                              ④ 다, 라

답 ①

- 다와 라의 설명이 바뀌었다.
- 다. xferlog: FTP 파일 전송 내역을 기록
- 라. loginlog: 로그인할 때 5 번 이상 실패할 경우의 기록

17. 다음 지문에서 설명하는 공격은 무엇인가?

가. 두 프로세스 간 자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능하게 하는 공격 기법  
 나. 공격 조건으로 프로그램에 root 권한의 SetUID 가 설정되어야 함  
 다. 대응 방법으로는 임시파일 사용 시 링크상태, 파일의 종류, 파일의 소유자, 파일의 변경여부 등을 점검

- ① 힙 오버플로우(Heap Overflow) 공격
- ② 레이스 컨디션(Race Condition) 공격
- ③ 스택 오버플로우(Stack Overflow) 공격
- ④ 코드(Code) 기반 공격

답 ②

- ② 레이스 컨디션(Race Condition)에 대한 설명이다.
- ①③ 버퍼 오버플로우(buffer overflow) 공격은 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다. 오버 플로우가 발생하는 데이터 영역에 따라, 힙 오버플로우(heap overflow) 공격과 스택 기반 오버플로우(stack overflow)로 나뉜다.
- ④ 코드 기반 공격은 공격자가 악성 코드를 작성해 공격 대상이나 봇넷을 감염시키는 방법으로 이루어지는 공격이다.

18. OSI 7 계층 중 다음 내용을 수행하는 계층은 무엇인가?

가. 메시지 분할 및 조립, 순서화  
 나. 포트주소 지정  
 다. 연결제어  
 라. 다중화와 역다중화

- ① 전송층(Transport Layer)
- ② 링크층(Link Layer)
- ③ 네트워크층(Network Layer)
- ④ 세션층(Session Layer)

답 ①

- ① 전송 계층(Transport Layer)에 대한 설명이다.
- ② 데이터 링크 계층(Data Link Layer)  
인접한 노드 간 통신, 흐름제어, 오류제어, 순서제어(프레임 동기화)
- ③ 네트워크 계층(Network Layer)  
경로 설정, 주소 변환, 논리 주소 지정, 흐름제어, 오류제어
- ④ 세션 계층(Session Layer)  
프로세스 간 연결을 확립, 논리적 연결(동기화), 대화 관리, 동기점을 이용한 오류 복구

19. 다음은 TCP 제어 플래그에 대한 설명이다. 옳지 않은 것은 무엇인가?

- ① TCP 제어 플래그는 TCP 연결제어나 전송 데이터를 관리 하기 위해 사용된다.
- ② URG 패킷은 순서에 상관없이 우선적으로 전송된다.
- ③ SYN 패킷은 TCP 통신에서 세션 확립을 위해 가장 먼저 전송된다.
- ④ RST 패킷은 송신측에서 더 이상 보낼 데이터가 없을 때 전송된다.

답 ④

- ④ 더 이상 보낼 데이터가 없을 경우, FIN 패킷을 전송한다.  
RST 패킷은 갑작스러운 비정상적인 연결 해제 및 재설정  
에 사용
- TCP 제어 플래그  
TCP 헤더에는 6 개의 제어 플래그 필드가 있으며, 이들은 논  
리적인 TCP 연결회선 제어 및 데이터 관리를 위해 사용
- URG(Urgent) 패킷  
긴급 데이터로, 순서에 상관없이 먼저 송신됨
- ACK(Acknowledgement) 패킷  
응답 확인
- PSH(Push) 패킷  
TELNET 과 같은 상호작용이 중요한 프로토콜의 경우 빠른  
응답이 중요한데, 이렇게 버퍼링된 데이터를 가능한 한 빨  
리 상위 계층 응용프로그램에 즉시 전달할 때 사용  
때로는, 서버측에서 더이상 전송할 데이터가 없음을 사용  
하기도 함
- RST(Reset) 패킷  
연결확립(ESTABLISHED)된 회선에 강제 리셋 요청, 비정상  
적인 세션 종료  
연결 재설정을 하기 위해 사용  
LISTEN, SYN\_RCVD 상태에서 RST 수신한 경우에는 LISTEN  
상태로 들어감  
그밖의 상태에서 RST 수신한 경우에는 연결을 끊고  
CLOSED 상태로 들어감
- SYN(Synchronize) 패킷  
연결 시작, 회선 개설, 세션 확립 시 가장 먼저 전송  
TCP 연결설정 초기화를 위한 순서번호의 동기화
- FIN(Finish) 패킷  
세션 연결 해제, 회선 종결  
더 이상 전송할 데이터가 없음을 의미

20. 다음 중 프로토콜과 포트번호의 연결이 옳지 않은 것은 무엇인가?

- ① HTTP - 80
- ② SMTP - 25
- ③ DNS - 53
- ④ TELNET - 20

답 ④

- ④ 20 번 - FTP 데이터  
23 번 - telnet

※ 주요 포트 목록

- 20 - FTP 실제 데이터 전송
- 21 - FTP 연결 시 인증 제어 정보 전송
- 22 - SSH(Secure Shell)
- 23 - telnet
- 25 - SMTP
- 53 - DNS
- 80 - HTTP
- 88 - 커beros(Kerberos)
- 109 - POP2
- 110 - POP3
- 143 - IMAP4
- 161 - SNMP
- 220 - IMAP3
- 443 - HTTPS

21. 다음 지문에서 설명하는 것은 무엇인가?

가. 침입탐지시스템(IDS, Intrusion Detection System)의 일종이다.  
 나. Rule 을 이용한 침입탐지 분석 기능을 가지고 있다.  
 다. 네트워크상에서 실시간 트래픽 분석, 프로토콜 분석이 가능 하다.

- ① Snort
- ② Sniffer
- ③ Strings
- ④ Encase

답 ①

- ① snort(스노트)는 오픈 소스이며, 실시간으로 트래픽을 분석하고 패킷을 기록하는 침입 탐지 시스템(IDS) 또는 침입 방지 시스템(IPS)이다.
- ② sniffer(스니퍼)는 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷을 엿듣는 도구나 공격자를 말하거나, 또는 네트워크 상의 트래픽 데이터를 분석하여 문제점을 제시함으로써 효율적인 네트워크 운영을 돕는 고장수리 도구를 말한다.
- ③ strings 는 유닉스 계열 운영 체제에서 실행 파일 같은 바이너리 파일에 삽입된 텍스트 문자열들을 찾고 보여주는 프로그램이다.
- ④ encase 는 포렌식(forensic)에 사용하는 디지털 증거 조사 및 분석 소프트웨어이다. 포렌식적으로 무결성을 검증 할 수 있는 방식으로 데이터를 수집하고 분석 업무를 수행하며, 미국 법원에서 증거물로 인정받았다.

22. 데이터 통신에서 사용되는 통신방식에 대한 설명 중 옳은 것은 무엇인가?

- ① Half-duplex 방식은 한쪽에서 데이터를 보내고 난 이후, 다른 한쪽에서 데이터 전송이 가능하다.
- ② Full-duplex 방식은 수신측에서는 송신측으로 응답할 수 없다.
- ③ Half-duplex 방식은 키보드(입력)와 모니터(출력) 사이의 전송이다.
- ④ Full-duplex 방식은 양방향으로 송수신이 가능하나, 한 순간 에는 반드시 한쪽 방향으로만 전송 가능하다.

답 ①

- ① 반이중(Half-duplex) 방식은 양쪽 방향으로 모두 전송할 수 있으나, 동시에 전송할 수는 없는 통신 방식이다. 그러므로 반드시 한쪽의 전송이 끝난 이후에 다른 쪽에서 전송이 가능하다. ON-OFF 무전기가 이에 해당한다.
- ② 전이중(Full-duplex) 방식은 송수신 쌍방이 동시에 통신이 가능한 통신 방식이다. 일반적인 전화기나 인터넷이 전이중 방식에 해당한다.
- ③ 키보드(입력)와 모니터(출력)은 한쪽 방향으로만 전송이 가능한 단방향(Simplex) 통신 방식이다. 키보드는 입력만 가능하고, 모니터는 출력만 가능하다.
- ④ 반이중(Half-duplex) 방식에 대한 설명이다. 전이중(Full-duplex) 방식은 동시에 송수신이 가능하다.



25. 컴퓨터의 네트워크 연결 상태를 점검하기 위해 netstat 명령을 사용하였다. 다음 중 옳지 않은 것은 무엇인가?

- ① LISTENING - 연결을 위하여 접속을 대기하고 있는 상태
- ② CLOSED\_WAIT - 완전히 종료된 상태
- ③ ESTABLISHED - 서로 연결된 상태
- ④ TIME\_WAIT - 연결이 종료되었거나 다음 연결을 위해 대기하고 있는 상태

답 ②

② CLOSED\_WAIT는 연결을 종료하기 위해 사용중인 프로세스를 종료하고 대기하고 있는 상태이다. 완전히 종료된 상태는 CLOSED이다.

26. 다음 중 지문에서 설명하는 공격 방식과 바르게 짝지어진 것은 무엇인가?

- 가. 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 동일하게 만들어 전송하는 공격
- 나. TCP 3-way handshake 과정 중 Listen 상태에서 SYN 을 받은 서버가 SYN/ACK 를 전달한 후 ACK 를 무한정 기다리게 하는 공격
- 다. 공격자가 다량의 ICMP Echo Request 의 출발지 IP 주소를 피해시스템의 IP 주소로, 목적지 IP 주소를 Direct Broadcast IP 주소로 Spoofing 하여 공격

|   | 가                   | 나                   | 다            |
|---|---------------------|---------------------|--------------|
| ① | Smurf Attack        | SYN Flooding Attack | Land Attack  |
| ② | SYN Flooding Attack | Land Attack         | Smurf Attack |
| ③ | Land Attack         | SYN Flooding Attack | Smurf Attack |
| ④ | SYN Flooding Attack | Smurf Attack        | Land Attack  |

답 ③

- 가. 출발지 IP 주소와 목적지 IP 주소를 동일하게  
-> Land Attack
- 나. 서버가 SYN/ACK 를 전달한 후 ACK 를 무한정 기다리게  
-> SYN Flooding Attack
- 다. 다량의 ICMP Echo Request 의 출발지 IP 주소를 피해시스템의 IP 주소로  
-> Smurf Attack(=ICMP Flooding Attack)

27. 다음 중 쿠키 세션 위조 공격과 그 방지방법에 대한 설명으로 옳지 않은 것은 무엇인가?

- ① SSO(Single-Sign-On)를 사용하는 응용프로그램의 경우 공격자는 쿠키를 알아냄으로써 공격을 수행할 수 있다.
- ② 사용자 PC 에 저장되는 쿠키정보는 불안전하므로 암호화하여 변조를 방지할 수 있다.
- ③ 세션이 비활성 상태인 동안에도 발생 가능하다.
- ④ 세션관리 정보를 서버 측에 저장하고 서버 측 세션을 사용 하도록 구현함으로써 쿠키 세션 위조 공격을 방지할 수 있다.

답 ③

- ③ 세션 쿠키는 사용자가 서버와 활성 연결 상태일 때만 유효한 쿠키이다. 사용자가 브라우저를 종료하거나 연결을 종료할 때 세션 쿠키의 내용은 지워지며, 따라서 비활성 상태에서는 세션 쿠키를 이용해 정당한 요청을 할 수 없다.

쿠키(Cookie)는 사용자가 방문하는 웹 사이트에 대한 설정 정보와 인증 정보를 사용자의 PC 에 저장해두는 것이다.

쿠키에는 Persistent Cookie 와 Session Cookie(세션 쿠키)가 있다.

Persistent Cookie 는 사용자가 웹 사이트 방문했을 때 설정한 정보(팝업창 표시 등)와 인증 정보(ID, Password 등)를 기억해두었다가, 나중에 재방문 시에 빠른 서비스를 제공하기 위한 것으로, 사용자의 하드 디스크에 저장해둔다.

Session Cookie(세션 쿠키)는 브라우저 프로세스가 실행되고 있을 때까지만 유효한 쿠키로, 현재 연결중인 웹 사이트의 인증 정보를 유지하기 위한 것이다.

메모리 공간에 상주해있다가, 사용자가 브라우저를 종료하면 쿠키는 삭제된다.

28. 다음은 웹서버 로그에서 볼 수 있는 상태코드(응답 코드)로 HTTP/1.1 에서 정의한 것이다. 옳지 않은 것은 무엇인가? (상태코드 : 설명)

- ① 200 : OK
- ② 400 : Access Denied
- ③ 404 : Not Found
- ④ 500 : Internal Server Error

답 ②

- ② 400 은 Bad Request(잘못된 요청): 서버가 요청사항을 이해하지 못한다.  
정확히 'Access Denied'는 없고, 접근을 제한하는 에러코드로는 인증에 실패했을 때 401(Unauthorized, 권한없음), 인가에 실패했을 때 403(Forbidden, 금지됨)이 있다.

※ 주요 HTTP 응답코드

- 100 Continue(계속)
- 101 Switching Protocol(프로토콜 전환)
- 200 OK(성공): 에러 없이 전송 성공
- 400 Bad Request(잘못된 요청): 요청사항 인식 불가
- 401 Unauthorized(권한 없음): 인증 실패
- 403 Forbidden(금지됨): 인가 실패
- 404 Not Found(찾을 수 없음): 요청 페이지 찾을 수 없음
- 408 Request timeout(요청 시간초과)
- 500 Internal Server Error(내부 서버 오류)
- 502 Bad Gateway(불량 게이트웨이): 게이트웨이 상태 나쁨
- 503 Service Unavailable(서비스 사용 불가): 일시적인 다운
- 504 Gateway timeout(게이트웨이 시간초과)

29. 다음 지문에서 설명하는 공격 방법은 무엇인가?

가. 웹 서버에 명령을 실행하여 관리자 권한을 획득하는 공격 방법이다.

나. 웹 어플리케이션의 첨부파일에 대한 부적절한 신뢰와 불충분한 점검으로 인해 악의적인 공격 코드가 웹 서버로 전송, 실행되는 방법이다.

다. 파일 업로드 취약점을 이용하며, 이것의 종류로는 서버 명령을 실행할 수 있는 asp, cgi, php, jsp 파일 등이 있다.

- ① 웹셸(Web Shell)
- ② 워터링홀(Watering Hole)
- ③ APT(Advanced Persistent Threats)
- ④ Encase

답 ①

- ① 웹셸(Web Shell)
 

공격자가 공격 대상 서버에 악의적으로 제작한 스크립트 파일을 업로드하여 관리자 권한을 획득하는 해킹법이다. 주로 asp, php, jsp, cgi 등 웹스크립트 파일을 통해 이루어진다.
- ② 워터링홀(Watering Hole)
 

열대지방의 맹수들이 물 웅덩이(waterhole) 주변에 잠복해 기다리다가 물을 마시러 오는 동물을 사냥하는 것에 비유한 공격으로, 특정 웹사이트에 알려지지 않은 취약점을 이용해 악성코드를 심어두고 사용자가 해당 사이트를 방문하는 사용자들을 악성코드에 감염시키는 방식이다. 특정 목표 대상 그룹(표적)을 선택하여 그들이 자주 이용하는 웹사이트를 악성코드를 감염시키는 방식으로, 해당 웹사이트를 신뢰하는 사용자의 심리를 이용한 공격이다.
- ③ APT(Advanced Persistent Threats, 지능형 지속 공격)
 

개인이나 단체, 국가, 또는 사업체나 정치 단체를 표적으로 삼아, 목적을 달성하기 위해 오랜 시간 동안 정보를 수집하고 다각도로 연구하여 고급 기술을 동원해 공격하는 기법을 말한다.
- ④ Encase
 

포렌식(forensic)에 사용하는 디지털 증거 조사 및 분석 소프트웨어이다. 포렌식적으로 무결성을 검증 할 수 있는 방식으로 데이터를 수집하고 분석 업무를 수행하며, 미국 법원에서 증거물로 인정받았다.

30. OWASP 는 주로 웹에 관한 정보노출, 악성파일 및 스크립트, 보안 취약점을 연구하고 있다. '10 대 웹 어플리케이션 취약점' 2013 년 에디션에 속하지 않는 것은 무엇인가?

- ① Buffer Overflow(버퍼 오버플로우)
- ② Broken Authentication and Session Management (인증 및 세션 관리 취약점)
- ③ Cross Site Scripting(크로스 사이트 스크립팅)
- ④ Injection(인젝션)

답 ①

OWASP TOP 10 2013

- A1 인젝션(Injection)
- A2 인증 및 세션 관리 취약점 (Broken Authentication and Session Management)
- A3 크로스 사이트 스크립팅(XSS, Cross Site Scripting)
- A4 안전하지 않은 객체 참조 (Insecure Direct Object Reference)
- A5 보안상 잘못된 구성(Security Misconfiguration)
- A6 민감한 데이터 노출(Sensitive Data Exposure)
- A7 기능 수준 접근 통제 누락 (Missing Function Level Access Control)
- A8 크로스 사이트 요청 변조 (CSRF, Cross Site Request Forgery)
- A9 알려진 취약점이 있는 컴포넌트 사용 (Using Components with Known Vulnerabilities)
- A10 검증되지 않은 리다이렉트 및 포워드 (Unvalidated Redirects and Forwards)

31. 웹과 DB 를 연동한 어플리케이션에서 SQL Injection 공격을 방어하기 위한 방법으로 옳지 않은 것은 무엇인가?

- ① DB 어플리케이션을 최소권한으로 구동한다.
- ② DB 에 내장된 프로시저를 사용한다.
- ③ 원시 ODBC 에러를 사용자가 볼 수 있도록 코딩한다.
- ④ DB 테이블 이름, 컬럼 이름, SQL 구조 등이 외부 HTML 에 포함되어 나타나지 않도록 한다.

답 ③

③ 공격자가 에러 메시지를 분석하여 DB 의 구조를 파악하고 공격에 활용할 수 있기 때문에, 에러 메시지 또한 이용자에게 보이지 않도록 설정해야 한다.

SQL 삽입(SQL 인젝션, SQL injection)

클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격하는 것이다.

SQL 삽입에 대한 대책

- 스크립트의 모든 파라미터들을 점검하여 사용자의 입력 값이 SQL injection 을 발생시키지 않도록 수정
- 입력 시 특수문자가 포함되어 있는지 검사하여 허용되지 않은 문자열이나 문자가 포함된 경우에는 에러로 처리
- SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정  
공격자는 에러 메시지를 분석하여 공격법을 찾는 데 활용하기 때문이다.

32. 다음 지문에서 설명하는 DB 보안 요구 사항은 무엇인가?

가. 기밀이 아닌 데이터로부터 기밀 정보를 얻어내는 가능성을 의미한다.  
 나. DB 데이터는 상호연관 가능성이 있어, 데이터에 직접 접근하지 않고도 가용한 데이터 값을 이용할 수 있다.  
 다. 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 하는 것을 의미한다.

- ① 추론 방지
- ② 데이터 무결성
- ③ 감사 기능
- ④ 사용자 인증

답 ①

- ① 추론 방지(inference control)  
사용자가 겉에 보이는 일반적 데이터로부터 숨겨둔 비밀정보를 획득하는 추론이 불가능하도록 보호하는 것
- ② 데이터 무결성(integrity)  
허가받지 않은 사용자에 의해 데이터가 위조나 변조되지 않도록 하는 것
- ③ 감사 기능(audit)  
어떤 상황의 실태를 조사하여 문제점을 찾아내고 수정하도록 권고하는 것
- ④ 사용자 인증(authentication)  
정당한 상대방인지, 진짜인지 가짜인지를 확인하는 것

33. 다음 지문에서 설명하는 시스템은 무엇인가?

가. 공격성향이 있는 자들을 중요한 시스템으로부터 다른 곳으로 끌어내도록 설계된 유도시스템이다.  
 나. 공격자의 동작에 관한 정보를 수집한다.  
 다. 관리자가 반응할 수 있도록 공격자로 하여금 시스템에 충분히 오랜 시간동안 머무르도록 유도한다.

- ① 라디어스(RADIUS)
- ② 허니팟(Honeypot)
- ③ 방화벽(Firewall)
- ④ AAA(Authentication Authorization Accounting)

답 ②

- ② 허니 팟(honeypot)  
 비정상적인 접근을 탐지하기 위해 의도적으로 설치해 둔 시스템  
 컴퓨터에 중요한 정보가 있는 것처럼 꾸며 공격자가 해당 컴퓨터를 공격하도록 한 뒤, 이를 통해 취약점과 공격 방법, 공격자의 패턴 등을 탐지할 수 있다
- ① 라디어스(RADIUS, Remote Authentication Dial In User Service)  
 사용자가 네트워크에 접속하고 서비스를 받기 위한 중앙 집중화된 인증, 인가, 회계(AAA) 관리를 제공하는 프로토콜 중 하나
- ③ 방화벽(Firewall, 침입 차단 시스템)  
 네트워크 트래픽을 모니터링하고 정해진 보안 규칙을 기반으로 특정 트래픽의 허용 또는 차단을 결정하는 네트워크 보안 디바이스
- ④ AAA(Authentication Authorization Accounting)  
 서버에 접근하는 사용자에게 대해 인증(Authentication)을 하고 주어진 권한 레벨을 검증(Authorization)한 뒤,사용자의 사용량(UDR)을 기록하여 사용요금 부과(Accounting) 기능을 수행하는 기반 구조 서비스 또는 프로토콜

34. 다음 중 공격 명칭과 공격에 대한 설명이 바르게 짝지어진 것은 무엇인가?

가. ARP Spoofing - IP 주소를 위·변조하는 공격  
 나. XSS(Cross Site Scripting) - 게시물에 실행코드와 태그의 업로드가 규제되지 않는 경우 이를 악용하여 열람한 타 사용자의 PC로부터 정보를 유출할 수 있는 공격  
 다. MITM(Man-In-The-Middle) 공격 - 통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 정보를 자기 것과 바꾸어 버림으로써 들리지 않고 도청을 하거나 통신 내용을 바꾸는 공격

- ① 가, 나
- ② 가, 다
- ③ 나, 다
- ④ 가, 나, 다

답 ③

- 가. ARP Spoofing(ARP 스푸핑) 공격은 ARP 테이블 내의 공격 대상자의 MAC 주소를 공격자의 MAC 주소로 바꾸어, 공격자가 공격 대상자 행세를 하는 것이다.  
 IP 주소를 위·변조하는 것은 IP 스푸핑으로, 단말 사이가 IP 주소 기반의 트러스트 관계일 경우 인증 절차를 생략한다는 취약점을 이용하여 IP 를 속여 다른 사람 행세를 하는 공격이다.
- 나. 크로스 사이트 스크립팅(XSS, Cross-site Scripting)  
 웹 사이트에 악성 스크립트를 삽입하여, 다른 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격

35. 다음 중 공격기법과 그에 대한 설명으로 옳은 것은 무엇인가?

- ① Smurf Attack : IP Broadcast Address 로 전송된 ICMP 패킷에 대해 응답하지 않도록 시스템을 설정하여 방어할 수 있다.
- ② Heap Spraying : 아이디와 패스워드 같이 사용자의 입력이 요구되는 정보를 프로그램 소스에 기록하여 고정시키는 방식이다.
- ③ Backdoor : 조직 내에 신뢰할 만한 발신인으로 위장해 ID 및 패스워드 정보를 요구하는 공격이다.
- ④ CSRF : 다른 사람의 세션 상태를 훔치거나 도용하여 액세스 하는 해킹 기법을 말한다.

답 ①

- ① **Smurf(ICMP flooding) 공격**은 공격대상 호스트의 IP 주소로 위장된 소스 IP 주소의 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상이 많은 양의 ICMP Echo 응답 패킷을 받아 시스템의 자원을 고갈시키는 공격이다. 브로드캐스팅을 이용하는 공격이기 때문에 라우터의 브로드캐스트를 막는 것으로 예방할 수 있다.
- ② **하드 코딩(Hard-Coding)**에 대한 설명이다. 하드 코딩은 설정사항이나 코드 등 시스템적으로 사용하는 데이터에 변수를 지정하지 않고, 직접 값을 넣어서 사용하는 방식을 말한다. 유연성이 없고 유지보수에 어려움이 있지만, 직관적이고 유효성 검사 등을 할 필요가 없어 프로그램 실행 속도가 올라간다. **Heap Spraying(힙 스프레이) 공격**은 메모리의 힙 영역에 악성코드를 깔아놓는 공격으로, 코드 삽입을 위한 사전 단계로 많이 사용된다.
- ③ 스피어피싱(Spear Phishing)에 대한 설명이다. **Backdoor(백도어)**는 인증절차 없이 시스템에 접근하기 위한 통로 이다.
- ④ 세션 하이재킹(Session Hijacking)에 대한 설명이다. **CSRF(Cross-site request forgery, 크로스사이트 요청 위조)**는 로그인 된 사용자의 세션 쿠키에 기타 다른 인증정보를 포함하여 위조된 HTTP 요청(수정, 삭제, 등록 등)을 강제로 보내도록 하는 공격이다.

36. 최근 사이버범죄자들은 인터넷 접속 시 추적을 피하기 위해 VPN(Virtual Private Network)서비스를 이용하고 있다. 다음 중 VPN 에서 사용하는 프로토콜이 아닌 것은 무엇인가?

- ① PPTP(Point-to-Point Tunneling Protocol)
- ② L2TP(Layer 2 Tunneling Protocol)
- ③ PGP(Pretty Good Privacy)
- ④ IPSec(Internet Protocol Security)

답 ③

- ③ PGP(Pretty Good Privacy)는 전자우편 서비스에 대한 보안 기술로, 인증기관을 사용하지 않고, 개개인의 신뢰 관계를 이용하여 인증한다.

계층별 보안 프로토콜

- PPTP - 2 계층
- L2F - 2 계층
- L2TP - 2 계층
- IPSec - 3 계층
- SSL/TLS - 4 계층
- SOCKSv5 - 5 계층
- SSH(Secure Shell) - 7 계층(telnet 이나 FTP 를 암호화)

37. 다음 지문에서 설명하는 공간은 무엇인가? ① 클러스터(Cluster) ② 파티션(Partition) ③ 섹터(Sector) ④ 슬랙(Slack)

저장매체의 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간으로, 물리적으로 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 말한다. 램, 드라이브, 파일시스템, 볼륨 등에 나타난다.

- ① 클러스터(Cluster)
- ② 파티션(Partition)
- ③ 섹터(Sector)
- ④ 슬랙(Slack)

답 ④

- ④ 슬랙(Slack) 공간이란 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간을 말한다. 물리적으로는 파일에 할당된 공간이지만 논리적으로는 사용할 수 없는 공간으로, 슬랙 공간에 정보를 은닉할 수 있고, 파일의 복구 및 삭제된 파일의 파편조사 시 유용하게 사용할 수 있다.
- ① 클러스터(cluster)는 컴퓨터 하드디스크에서 사용하는 논리적 단위로, 파일은 클러스터 여러 개로 이루어진다.
  - ② 파티션(Partition)은 하나의 디스크 드라이브를 논리적으로 여러 부분으로 분할하는 것이다.
  - ③ 섹터(Sector)은 디스크의 저장공간을 나누는 단위들 중 최소단위이다.

38. 다음 지문에서 설명하는 포렌식 도구는 무엇인가?

가. Guidance Software Inc.가 사법기관 요구사항에 바탕을 두고 개발한 컴퓨터 증거분석용 소프트웨어이다.

나. 컴퓨터 관련 수사에서 디지털 증거의 획득과 분석 기능을 제공하며, 미국에서 1990년대 후반부터 600여개 사법기관에서 컴퓨터 관련 범죄수사에 활용되고 있으며, 미국 법원이 증거능력을 인정하는 독립적인 솔루션이다.

다. Windows 환경에서 증거원본 미디어에 어떠한 영향을 미치지 않으면서도 '미리보기', '증거사본작성', '분석', '결과보고'에 이르는 전자증거조사의 모든 과정을 수행할 수 있다.

- ① Wireshark
- ② Encase
- ③ KICS
- ④ IDA

답 ②

- ② 지문은 Encase에 대한 설명이다.
- ① Wireshark(와이어샤크)는 자유 및 오픈 소스 패킷 분석 프로그램으로, 네트워크의 문제, 분석, 소프트웨어 및 통신 프로토콜 개발, 교육에 쓰인다.
  - ③ KICS(korea information system of criminal-justice services)란 법원·법무부·검찰·경찰·해양경비안전본부가 표준화된 정보기술 시스템을 통해 수사, 기소, 재판, 형 집행의 형사사법 절차를 신속하게 진행하고, 그 결과의 피드백을 통해 업무 효율성과 투명성을 높이는 시스템이다.
  - ④ IDA(Interactive DisAssembler)는 기계어 코드로부터 어셈블리어 소스 코드를 생성해주는 디스어셈블러 프로그램이다.

39. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 71 조(벌칙) 제 1 항의 각 호 내용 중 일부를 나열한 것이다. 실제 내용과 다른 것은 무엇인가?

- ① 이용자의 동의를 받지 아니하고 개인정보를 수집한 자
- ② 정보통신망에 침입한 자
- ③ 정보통신망에 장애가 발생하게 한 자
- ④ 타인의 정보를 훼손하거나 타인의 비밀을 판매 또는 도용한 자

답 ④

- ④ '타인의 비밀을 판매 또는 도용한 자'가 아니라, '타인의 비밀을 침해·도용 또는 누설한 자'이다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 71 조(벌칙)

- ① 다음 각 호의 어느 하나에 해당하는 자는 5 년 이하의 징역 또는 5 천만원 이하의 벌금에 처한다.
  1. 이용자의 동의를 받지 아니하고 개인정보를 수집한 자
  2. 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 자
  3. 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
  4. 이용자의 동의를 받지 아니하고 개인정보 처리위탁을 한 자
  5. 이용자의 개인정보를 훼손·침해 또는 누설한 자
  6. 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
  7. 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 자
  8. 법정대리인의 동의를 받지 아니하고 만 14 세 미만인 아동의 개인정보를 수집한 자
  9. 정보통신망에 침입한 자
  10. 정보통신망에 장애가 발생하게 한 자
  11. 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자
- ② 제 1 항제 9 호의 미수범은 처벌한다.

40. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 상 정보통신망에 유통되어서는 안 되는 불법정보 관련 조항을 나열한 것이다. 실제 내용과 다른 것은 무엇인가?

- ① 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
- ② 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
- ③ 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인을 모욕하는 내용의 정보
- ④ 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보

답 ③

- ③ '타인을 모욕하는 내용의 정보'가 아니라, '타인의 명예를 훼손하는 내용의 정보'이다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 44 조의 7(불법정보의 유통금지 등)

- ① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.
  1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
  2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보
  3. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보
  4. 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
  5. 「청소년 보호법」에 따른 청소년유해매체물로서 상대방의 연령 확인, 표시의무 등 법령에 따른 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
  6. 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
- 6의 2. 이 법 또는 개인정보 보호에 관한 법령을 위반하여 개인정보를 거래하는 내용의 정보
- 7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
- 8. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
- 9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보

**정답 체크**

|           |           |           |           |           |           |           |           |           |           |
|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| <b>01</b> | <b>02</b> | <b>03</b> | <b>04</b> | <b>05</b> | <b>06</b> | <b>07</b> | <b>08</b> | <b>09</b> | <b>10</b> |
| ③         | ②         | ④         | ④         | ③         | ②         | ④         | ②         | ②         | ④         |
| <b>11</b> | <b>12</b> | <b>13</b> | <b>14</b> | <b>15</b> | <b>16</b> | <b>17</b> | <b>18</b> | <b>19</b> | <b>20</b> |
| ①         | ①         | ②         | ②         | ③         | ①         | ②         | ①         | ④         | ④         |
| <b>21</b> | <b>22</b> | <b>23</b> | <b>24</b> | <b>25</b> | <b>26</b> | <b>27</b> | <b>28</b> | <b>29</b> | <b>30</b> |
| ①         | ①         | ③         | ④         | ②         | ③         | ③         | ②         | ①         | ①         |
| <b>31</b> | <b>32</b> | <b>33</b> | <b>34</b> | <b>35</b> | <b>36</b> | <b>37</b> | <b>38</b> | <b>39</b> | <b>40</b> |
| ③         | ①         | ②         | ③         | ①         | ③         | ④         | ②         | ④         | ③         |