

## 2023년04월09일년 인터넷보안전문가 2급 필기시험 기출문제 답안

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

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!



**【1과목】 정보보호개론 (10문제)**

1. IPSec 프로토콜에 대한 설명으로 옳지 않은 것은?

- ① 네트워크 계층인 IP 계층에서 보안 서비스를 제공하기 위한 보안 프로토콜이다.

기밀성 기능은 AH(Authentication Header)에 의하여  
② 제공되고, 인증 서비스는 ESP(Encapsulating Security Payload)에 의하여 제공된다.

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.

2. 공격 유형 중 마치 다른 송신자로부터 정보가 수신된 것처럼 꾸미는 것으로, 시스템에 불법적으로 접근하여 오류의 정보를 정확한 정보인 것처럼 속이는 행위를 뜻하는 것은?

① 차단(Interruption)

② 위조(Fabrication)

③ 변조(Modification)

④ 가로채기(Interception)

3. 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

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. 전자 상거래의 보안이 중요시되고 있는 현시점에서 은행 카드 사용자에게 안전한 상거래를 할 수 있도록 보장해 주는 보안 프로토콜은?

① SSL

② SET

③ PEM

④ PGP

6. 대칭형 암호화 방식의 특징으로 옳지 않은 것은?

① 처리 속도가 빠르다.

② RSA와 같은 키 교환 방식을 사용한다.

③ 키의 교환 문제가 발생한다.

④ SSL과 같은 키 교환 방식을 사용한다.

7. 다음 중 유형이 다른 보안 알고리즘은?

① SEED 알고리즘

② RSA 알고리즘

③ Rabin 알고리즘

④ ECC 알고리즘

8. 다음 중 악성 프로그램/코드의 종류가 아닌 것은?

① Iosf

② Stacheldraft

③ Salami

④ Convert Channel

9. 서버를 안전하게 유지하는 방법으로 옳지 않은 것은?

① 운영체제를 정기적으로 패치하고, 데몬을 최신 버전으로 갱신하여 설치한다.

② 불필요한 SUID 프로그램을 제거한다.

③ 침입차단시스템의 정책을 적절하게 적용하여 내부 자원을 보호한다.

④ 사용자의 편리성과 가용성을 위하여 시스템이 제공하는 모든 데몬들을 설치하여 사용한다.

10. 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

**【2과목】 운영체제 (20문제)**

11. Linux에서 프로세스 실행 우선순위를 바꿀 수 있는 명령어는?

- ① chps
- ② reserv
- ③ nice
- ④ top

12. 다음은 어떤 명령어에 대한 설명인가?

이 명령어는 모든 프로세스의 부모 프로세스로서 시스템 부팅 과정의 제일 마지막에 불러져서 `/etc/inittab`을 읽고 시스템의 실행레벨을 결정한다.

- ① runlevel
- ② init
- ③ nice
- ④ halt

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

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

14. 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, USB, CD-ROM 그리고 루프 백 장치 등이 존재한다.

15. 커널의 대표적인 기능으로 옳지 않은 것은?

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

16. IIS 웹 서버를 설치한 다음에는 기본 웹사이트 등록정보를 수정하여야 한다. 웹사이트에 접속하는 동시 접속자수를 제한하려고 할 때 어느 부분을 수정해야 하는가?

- ① 성능 탭
- ② 연결 수 제한
- ③ 연결 시간 제한
- ④ 문서 탭

17. Linux 파일 시스템의 기본 구조 중 파일에 관한 중요한 정보를 싹는 곳은?

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

18. 다음 명령어 중에서 시스템의 메모리 상태를 보여주는 명령어는?

- ① mkfs
- ② free
- ③ ps
- ④ shutdown

19. Windows Server에서 자동으로 호스트의 네트워크 환경을 설정할 수 있는 서비스는?

- ① IIS(Internet Information Server)
- ② FTP(File Transfer Protocol)
- ③ DHCP(Dynamic Host Configuration Protocol)
- ④ DNS(Domain Name System)

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. Linux 시스템의 shadow 파일 내용에 대한 설명으로 올바른 것은?

```
Root:$1$szfVKcHi$dEFUonrDJZ2ZGOPuqq9yK
0:11458:0:99999:7:::
adm:!:11458:0:99999:7:::
lp:!:11458:0:99999:7:::
named:!:11458:0:99999:7:::
gdm:!:11458:0:99999:7:::
```

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

② gdm에서 '!'은 로그인 셸을 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.

22. 디스크의 용량을 확인하는 Linux 명령어는?

① df

② free

③ cp

④ mount

23. 파일의 허가 모드가 '-rwxr---w-'이다. 다음 설명 중 옳지 않은 것은?

① 소유자는 읽기 권한, 쓰기 권한, 실행 권한을 갖는다.

② 동일한 그룹에 속한 사용자는 읽기 권한만을 갖는다.

③ 다른 모든 사용자는 쓰기 권한 만을 갖는다.

④ 동일한 그룹에 속한 사용자는 실행 권한을 갖는다.



전자문제집 CBT(App Store) : [다운로드](#)



전자문제집 CBT(Google Play) : [다운로드](#)

24. Linux에서 'ls -al' 명령에 의하여 출력되는 정보로 옳지 않은 것은?

① 파일의 접근허가 모드

② 파일 이름

③ 소유자명, 그룹명

④ 파일의 소유권이 변경된 시간

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

① ping

② traceroute

③ netstat

④ nslookup

26. Windows Server의 DNS 서비스 설정에 관한 설명으로 옳지 않은 것은?

① 정방향 조회 영역 설정 후 반드시 역방향 조회 영역을 설정해 주어야 한다.

② Windows Server는 고정 IP Address를 가져야 한다.

③ Administrator 권한으로 설정해야 한다.

④ 책임자 이메일 주소의 at(@)은 마침표(.)로 대체된다.

27. 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)

28. Linux 시스템이 부팅될 때 나오는 메시지가 저장된 로그 파일의 경로와 명칭으로 올바른 것은?

① /var/log/xferlog

② /var/log/dmesg

③ /var/log/message

④ /var/log/secure

29. VI(Visual Interface) 에디터에서 편집행의 줄번호를 출력해주는 명령은?

① :set nobu

② :set nu

③ :set nonu

④ :set showno

30. '/data' 라는 디렉터리는 40개의 텍스트 파일과 2개의 디렉터리가 들어있는 상태이다. root 유저로 로그인 한 후 alias 목록을 확인한 결과 alias rm='rm -i' 라고 지정되어 있었다. root 유저가 이 'data'라는 디렉터리를 확인 메시지 없이 한번에 지우려면 다음 중 어떤 명령을 내려야 하는가?

- ① rm data
- ② rm -r data
- ③ rm -f data
- ④ rm -rf data

**【3과목】 네트워크 (15문제)**

31. IP Address '129.120.120.88'가 속하는 Class는?

- ① A Class
- ② B Class
- ③ C Class
- ④ D Class

32. 데이터 전송 운영 방법에서 수신측에 n개의 데이터 블록을 수신할 수 있는 버퍼 저장 공간을 확보하고 송신측은 확인신호 없이 n개의 데이터 블록을 전송하는 흐름 제어는?

- ① 블록
- ② 모듈러
- ③ Xon/Xoff
- ④ Window

33. 오류검사 방법 중에서 문자 단위로 오류를 검사하는 것으로서, 각 전송 비트 내에 1의 개수가 홀수 또는 짝수로 계산되거나 하나의 비트를 추가하여 오류 여부를 검출하고 만약 오류 비트가 짝수 개 발생하면 오류 사실을 검출하지 못하는 오류 검사 방식은?

- ① 해밍 코드
- ② 블록합 검사
- ③ 순환중복 검사
- ④ 패리티 검사

34. 다음 중 디지털 변조로 옳지 않은 것은?

- ① ASK
- ② FSK
- ③ PM
- ④ QAM

35. Internet Layer를 구성하는 프로토콜들에 대한 설명으로 옳지 않은 것은?

① IP는 TCP와 같이 신뢰성 있는 통신을 제공한다.

② ARP는 상대방의 IP Address는 알고 있으나, 상대방의 MAC Address를 모를 경우에 사용되는 프로토콜이다.

RARP는 Disk가 없는 터미널에서 자신의 랜카드 상의  
③ MAC은 알고 있으나 자신의 IP를 모를 경우에 사용되는 프로토콜이다.

ICMP는 Ping 등을 지원할 수 있는 프로토콜이며, 또한  
④ IP 데이터그램의 전달과정 중에 발생할 수 있는 에러에 대한 보고용으로 사용된다.

36. 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.

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

④ UDP는 상위 계층을 식별하기 위하여 Protocol Field를 사용한다.

37. 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.

④ Reference적인 성격을 가지고 있으며 7 계층으로 layer를 구성한다.

38. Distance Vector 알고리즘을 사용하는 프로토콜로 바르게 짝지어진 것은?

① OSPF, RIP

② RIP, EIGRP

③ IGRP, RIP

④ EIGRP, IGRP

39. RIP의 동작 설명으로 옳지 않은 것은?

- ① 라우팅 테이블은 데이터그램 패킷을 통하여 모든 라우터에 방송된다.
- ② RIP에서는 최대 Hop를 16으로 제한하므로 16이상의 경우는 도달할 수 없는 네트워크를 의미한다.
- ③ 매 60초 마다 라우팅 정보를 방송한다.
- ④ 만약 180초 이내에 새로운 라우팅 정보가 수신되지 않으면 해당 경로를 이상 상태로 간주한다.

40. 다음 중 OSI 7 Layer 중에서 응용프로그램이 네트워크 자원을 사용할 수 있는 통로를 제공해주는 역할을 담당하는 Layer는?

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

41. '서비스' - 'Well-Known 포트' - '프로토콜'의 연결이 옳지 않은 것은?

- ① FTP - 21 - TCP
- ② SMTP - 25 - TCP
- ③ DNS - 53 - TCP
- ④ SNMP - 191 - TCP

42. IP Address의 부족과 Mobile IP Address 구현문제로 IP Address인 IPv6가 있다. IPv6는 몇 비트의 Address 필드를 가지고 있는가?

- ① 32 비트
- ② 64 비트
- ③ 128 비트
- ④ 256 비트

43. OSI 7 Layer 중 아래와 같은 기능을 제공하는 계층은?

- 코드변환(Code Conversion)
- 데이터의 암호화(Data Encryption)
- 텍스트 압축(Text Compression)
- 가상 터미널 프로토콜(Virtual Terminal Protocol)
- 파일 전송 프로토콜(File Transfer Protocol)

- ① Data Link Layer
- ② Network Layer
- ③ Presentation Layer
- ④ Transport Layer

44. 프로토콜의 기능 중 전송을 받는 개체에서 발송지로부터 오는 데이터의 양이나 속도를 제한하는 기능은?

- ① 흐름 제어
- ② 에러 제어
- ③ 순서 제어
- ④ 접속 제어

45. TCP 포트 중 25번 포트가 하는 일반적인 역할은?

- ① Telnet
- ② FTP
- ③ SMTP
- ④ SNMP

#### 【4과목】 보안 (15문제)

46. IP Spoofing의 과정 중 포함되지 않는 것은?

- ① 공격자의 호스트로부터 신뢰받는 호스트에 SYN-Flooding 공격으로 상대방 호스트를 무력화 시킨다.
- ② 신뢰받는 호스트와 공격하려는 타겟호스트간의 패킷교환 순서를 알아본다.
- ③ 신뢰받는 호스트에서 타겟호스트로 가는 패킷을 차단하기 위해 타겟호스트에 Flooding 과 같은 공격을 시도한다.
- ④ 패킷교환 패턴을 파악한 후 신뢰받는 호스트에서 보낸 패킷처럼 위장하여 타겟호스트에 패킷을 보낸다.

47. 버퍼 오버플로우(Buffer Overflow) 개념으로 옳지 않은 것은?

- ① 스택의 일정부분에 익스플로러 코드(Explorer Code)를 삽입하고 어떤 프로그램의 리턴 어드레스(Return Address)를 익스플로러 코드가 위치한 곳으로 돌린다.
- ② 대체적으로 문자열에 대한 검사를 하지 않아서 일어나는 경우가 많다.
- ③ 소유자가 root인 Setuid가 걸린 응용프로그램인 경우 익스플로러 코드를 이용 root의 권한을 획득할 수 있다.
- ④ Main 프로그램과 Sub 프로그램의 경쟁관계와 Setuid를 이용하여 공격하는 패턴이 존재한다.

48. SYN 플러딩 공격에 대한 설명으로 올바른 것은?

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.

네트워크에 연결된 호스트들의 이용 가능한 서비스와 포트를 조사하여 보안 취약점을 조사하기 위한 공격방법이다.

④ 패킷을 전송할 때 암호화하여 전송하는 보안 도구이다.

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

① 메시지 인증

② 수신 부인방지

③ 사용자 인증

④ 송신 부인방지

50. 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.

데이터 암호화를 위한 비밀키를 Hand Shake 프로토콜 ④ 단계에서 정한 후에 키를 사용하여 암호화된 메시지로 상대방의 신원을 증명할 수 있다.

51. 대형 응용 프로그램을 개발하면서 전체 시험실행을 할 때 발견되는 오류를 쉽게 해결하거나 처음부터 중간에 내용을 볼 수 있는 부팅루틴을 삽입해 컴퓨터의 정비나 유지 보수를 핑계 삼아 컴퓨터 내부의 자료를 훔아가는 해킹 행위는?

① Trap Door

② Asynchronous Attacks

③ Super Zapping

④ Salami Techniques

52. DoS(Denial of Service)의 개념으로 옳지 않은 것은?

① 다량의 패킷을 목적지 서버로 전송하여 서비스를 불가능하게 하는 행위

② 로컬 호스트의 프로세스를 과도하게 fork 함으로서 서버에 장애를 주는 행위

③ 서비스 대기 중인 포트에 특정 메시지를 다량으로 보내 서비스를 불가능하게 하는 행위

④ 익스플로러를 사용하여 특정권한을 취득하는 행위

53. 아래와 같이 초기설정이 되어있는 '/bin/su' 명령어가 있다. Linux 서버의 내부 보안을 위해 '/bin/su' 명령어를 root에게는 모든 권한을, 'wheel'이라는 그룹에게는 실행권한만을 부여하려고 한다. 이 과정 중에 올바르지 않은 사항은?

```
[rroot@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

54. '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

③ 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

55. 다음은 어떤 보안 도구를 의미하는가?

회사의 사설 네트워크와 외부의 공중 네트워크 사이의 중립 지역으로써 삽입된 컴퓨터 호스트 또는 소형 네트워크를 말한다.

① IDS

② DMZ

③ Firewall

④ VPN

56. 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

57. Linux의 침입차단시스템 설정 중, 임의의 외부 호스트에서 '210.119.227.226'으로 telnet 접속을 막는 규칙을 삽입하기 위한 iptables 명령어로 올바른 것은?

- ① `/sbin/iptables -A INPUT -i eth0 -s 0/0 -d 210.119.227.226 -p tcp --dport telnet -j drop`
- ② `/sbin/iptables -A OUTPUT -i eth0 -s 0/0 -d 210.119.227.226 -p tcp --dport telnet -j drop`
- ③ `/sbin/iptables -A INPUT -i eth0 -s 0/0 -d 210.119.227.226 -p tcp --dport telnet -j accept`
- ④ `/sbin/iptables -A OUTPUT -i eth0 -s 0/0 -d 210.119.227.226 -p tcp --dport telnet -j accept`

58. Linux 시스템에서 'chmod 4771 a.txt' 명령어를 수행한 후 변경된 사용 권한으로 올바른 것은?

- ① -rwsrwx-x
- ② -rwxrws-x
- ③ -rwxrwx-s
- ④ -rwxrwx-x

59. 웹 해킹의 한 종류인 SQL Injection 공격은 조작된 SQL 질의를 통하여 공격자가 원하는 SQL구문을 실행하는 기법이다. 이를 예방하기 위한 방법으로 옳지 않은 것은?

- ① 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. 스머프 공격(Smurf Attack)에 대한 설명으로 올바른 것은?

- ① 두 개의 IP 프래그먼트를 하나의 데이터그램인 것처럼 하여 공격 대상의 컴퓨터에 보내면, 대상 컴퓨터가 받은 두 개의 프래그먼트를 하나의 데이터그램으로 합치는 과정에서 혼란에 빠지게 만드는 공격이다.
- ② 서버의 버그가 있는 특정 서비스의 접근 포트로 대량의 문자를 입력하여 전송하면, 서버의 수신 버퍼가 넘쳐서 서버가 혼란에 빠지게 만드는 공격이다.
- ③ 내고, 서버가 그것을 처리하지 못하게 만들어 시스템을 혼란에 빠지게 하는 공격이다.

- ④ 출발지 주소를 공격하고자 하는 컴퓨터의 IP Address로 지정한 후, 패킷신호를 네트워크 상의 컴퓨터에 보내게 되면, 패킷을 받은 컴퓨터들이 반송 패킷을 다시 보내게 되는데, 이러한 원리를 이용하여 대상 컴퓨터에 갑자기 많은 양의 패킷을 처리하게 함으로써 시스템을 혼란에 빠지게 하는 공격이다.