2016-국가직-정보보호론-2형-해설-곽후근

1. 사용자 인증에 사용되는 기술이 아닌 것은?
① Snort
② OTP(One Time Password)
③ SSO(Single Sign On)
④ 스마트 카드
정답 체크 :
(1) Snort : 스노트(Snort)는 무료의 오픈 소스 네트워크 침입 차단 시스템(IPS)이자, 네트워크 침입 탐지 시스템(IDS)으로서, 마틴 로시가 1998년에 개발하였다. 실시간 트래픽 분석과 IP에서의 패킷 로깅을 수행하는 능력을 갖고, 프로토콜 분석, 내용 검색 그리고 매칭을 수행한다. 사용자 인증과는 무관하다.
오답 체크 :
(2) OTP : 고정된 비밀번호 대신 사용되는 매번 새롭게 바뀌는 일회용 비밀번호이다. S/KEY 방식, 시간 동기화 방식, 챌린지/응답 방식, 이벤트 동기화 방식 등이 있다. 소지 기반 인증에 사용된다.
(3) SSO : 모든 인증을 하나의 시스템에서 한다는 의미이다. 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면, 다른 시스템에 대한 접근 권한도 모두 얻는다. 이러한 접속 형태의 대표적인 인증 방법으로는 커버로스(Kerberos)를 이용한 윈도우의 액티브 디렉토리(Active Directory)가 있다. 지식 기반 인증에 사용된다.
(4) 스마트 카드 : 신용카드와 동일한 크기와 두께의 플라스틱 카드에 마이크로프로세서 칩과 메모리, 보안 알고리즘, 마이크로컴퓨터를 COB(chip on board) 형태로 내장된 전자식 카드이다. 기억소자를 탑재한 반도체 칩이 내장되어 있어 기존의 자기카드보다 저장용량이 월등하여 별도의 정보저장이 요구되는 다양한 부가기능을 수행할 수 있으며, 독특한 장비에 의해서만 해독될 수 있어 위조는 거의 불가능하다. 소지 기반 인증에 사용된다.

2. 보안 요소에 대한 설명과 용어가 바르게 짝지어진 것은?

ㄱ. 자산의 손실을 초래할 수 있는 원하지 않는 사건의 잠재적인 원인이나 행위자
ㄴ. 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성
ㄷ. 자산의 잠재적인 속성으로서 위협의 이용 대상이 되는 것

	ㄱ	ㄴ	ㄷ
①	위협	취약점	위험
②	위협	위험	취약점
③	취약점	위협	위험
④	위험	위협	취약점

정답 체크 :
(2)
위협(Threats) : 정보자산의 보안에 부정적 영향을 줄 수 있는 외부의 환경 또는 사건(이벤트)을 의미한다.
위험(Risk) : 자산의 취약한 부분에 위협요소가 발생하여 자산의 손실, 손상을 유발한 잠재성(가능성)을 의미한다.

취약점(Vulnerability) : 위협에 의해 보안에 부정적 영향을 줄 수 있는 정보자산의 속성이나 상태를 의미한다.

3. 공개키 암호 알고리즘에 대한 설명으로 옳은 것은?
① Diffie-Hellman 키 교환 방식은 중간자(man-in-the-middle) 공격에 강하고 실용적이다.
② RSA 암호 알고리즘은 적절한 시간 내에 인수가 큰 정수의 소인수분해가 어렵다는 점을 이용한 것이다.
③ 타원곡선 암호 알고리즘은 타원곡선 대수문제에 기초를 두고 있으며, RSA 알고리즘과 동일한 안전성을 제공하기 위해서 더 긴 길이의 키를 필요로 한다.
④ ElGamal 암호 알고리즘은 많은 큰 수들의 집합에서 선택된 수들의 합을 구하는 것은 쉽지만, 주어진 합으로부터 선택된 수들의 집합을 찾기 어렵다는 점을 이용한 것이다.
정답 체크 :
(2) RSA : 소인수 분해 문제의 어려움에 기초한다.
오답 체크 :
(1) Diffie-Hellman : 중간자 공격에 약하다(상대방의 난수가 진짜 상대방의 난수인지 알 방법이 없음).
(3) ECC : RSA에 비해 키의 비트 수가 적다.
(4) Elgamal : 해당 설명은 배낭 문제이고, Elgamal은 이산 대수를 구하는 것이 어렵다는 것을 이용한다.

4. ISO/IEC 27001의 보안 위험 관리를 위한 PDCA 모델에 대한 설명으로 옳지 않은 것은?
① IT기술과 위험 환경의 변화에 대응하기 위하여 반복되어야 하는 순환적 프로세스이다.
② Plan 단계에서는 보안 정책, 목적, 프로세스 및 절차를 수립한다.
③ Do 단계에서는 수립된 프로세스 및 절차를 구현하고 운영한다.
④ Act 단계에서는 성과를 측정하고 평가한다.
오답 체크 :
(4) Act : 해당 설명은 Check이고, Act는 지속적인 ISMS의 향상을 위해 내부 ISMS의 감사, 관리 리뷰, 다른 정보들에 기반하야 수정적, 예방적 행동을 수행한다.
정답 체크 :
(1) 순환적 프로세스 : PDCA 사이클 기반으로 실행된다.
(2) Plan : 조직 전체의 정책과 목적에 부합하도록 정보 보안을 개선하거나 위기를 관리하기 위한 ISMS 정책, 목적, 프로세스, 절차를 수립한다.
(3) Do : ISMS 정책, 컨트롤, 프로세스, 절차의 구현 및 운영을 수행한다.

5. 메시지의 무결성을 검증하는 데 사용되는 해시와 메시지 인증 코드(MAC)의 차이점에 대한 설명으로 옳은 것은?
① MAC는 메시지와 송·수신자만이 공유하는 비밀키를 입력받아 생성되는 반면에, 해시는 비밀키 없이 메시지로부터 만들어진다.
② 해시의 크기는 메시지 크기와 무관하게 일정하지만, MAC는 메시지와 크기가 같아야 한다.
③ 메시지 무결성 검증 시, 해시는 암호화되어 원본 메시지와 함께 수신자에게 전달되는 반면에, MAC의 경우에는 MAC 로부터 원본 메시지 복호화가 가능하므로 MAC만 전송하는 것이 일반적이

다.
④ 송·수신자만이 공유하는 비밀키가 있는 경우, MAC를 이용하여 메시지 무결성을 검증할 수 있으나 해시를 이용한 메시지 무결성 검증은 불가능하다.
정답 체크 :
(1) 비밀키 : MAC은 비밀키가 필요하고, 해시는 비밀키가 필요 없다.
오답 체크 :
(2) 메시지 크기 : 해시와 MAC 모두 메시지 크기와 무관하다.
(3) 전송 : 해시는 해시와 원본 메시지를 전달해야 하고, MAC은 MAC과 원본 메시지를 전달해야 한다.
(4) 무결성 : 해시는 무결성을 검증하고, MAC은 인증과 무결성을 검증한다.

6. DMZ(demilitarized zone)에 대한 설명으로 옳은 것만을 고른 것은?

ㄱ. 외부 네트워크에서는 DMZ에 접근할 수 없다. ㄴ. DMZ 내에는 웹 서버, DNS 서버, 메일 서버 등이 위치할 수 있다. ㄷ. 내부 사용자가 DMZ에 접속하기 위해서는 외부 방화벽을 거쳐야 한다. ㄹ. DMZ는 보안 조치가 취해진 네트워크 영역으로, 내부 방화벽과 외부 방화벽 사이에 위치할 수 있다.

① ㄱ, ㄷ
② ㄴ, ㄷ
③ ㄴ, ㄹ
④ ㄱ, ㄹ
정답 체크 :
(3)
(ㄴ) 서버 : DMZ에서는 외부에서 접근 가능한 서버들이 위치한다. 예를 들면, 웹 서버, DNS 서버, 메일 서버, FTP 서버 등이 위치할 수 있다.
(ㄹ) 방화벽 : 일반적으로 DMZ는 내부 방화벽과 외부 방화벽 사이에 위치한다.
오답 체크 :
(1), (2), (4)
(ㄱ) 접근 : 내부 네트워크에서 외부 네트워크에 공개하기 위한 서버들이 위치하므로 외부 네트워크에서 접근할 수 있다.
(ㄷ) 내부 사용자 : 내부 사용자가 DMZ에 접속하기 위해서는 내부 방화벽을 거쳐야 한다. 외부 사용자는 외부 방화벽을 거친다.

7. 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 상 정보통신 서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우 이용자들에게 알리고 동의를 받아야 하는 내용이 아닌 것은?
① 개인정보의 수집·이용 목적
② 수집하는 개인정보의 항 목
③ 개인정보의 보유·이용 기간
④ 개인정보 처리의 위탁 기관명
정답 체크 :
(4)

“정보통신망법” 제22조(개인정보의 수집 · 이용 동의 등) 상 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다. 1. 개인정보의 수집 · 이용 목적, 2. 수집하는 개인정보의 항목, 3. 개인정보의 보유 · 이용 기간

8. 임의접근제어(DAC)에 대한 설명으로 옳지 않은 것은?
① 사용자에게 주어진 역할에 따라 어떤 접근이 허용되는지를 말해주는 규칙들에 기반을 둔 다.
② 주체 또는 주체가 소속되어 있는 그룹의 식별자(ID)를 근거로 객체에 대한 접근을 승인하거나 제한한다.
③ 소유권을 가진 주체가 객체에 대한 권한의 일부 또는 전부를 자신의 의지에 따라 다른 주 체에게 부여한다.
④ 전통적인 UNIX 파일 접근제어에 적용되었다.
정답 체크 :
(1) 역할 : 해당 설명은 역할기반접근제어(RBAC)이다.
오답 체크 :
(2) 그룹의 식별자 : 시스템 객체에 대한 접근을 사용자 개인 또는 그룹의 식별자를 기반으로 한다.
(3) 권한 : 사용자가 자신이 소유한 자원의 접근 권한을 임의로 설정한다.
(4) UNIX : 유닉스의 파일 허가 등에 사용된다.

9. 식별된 위험에 대처하기 위한 정보보안 위험 관리의 위험 처리 방안 중, 불편이나 기능 저 하를 감수하고라도, 위험을 발생시키는 행위나 시스템 사용을 하지않도록 조치하는 방안은?
① 위험 회피
② 위험 감소
③ 위험 수용
④ 위험 전가
정답 체크 :
(1) 위험 회피 : 위험이 존재하는 사업, 프로세스를 진행하지 않는 것을 말한다. 그러므로 조직은 편리한 기능이나 유용한 기능 등을 상실할 수 있다.
오답 체크 :
(2) 위험 감소 : 위험을 감소시킬 대책을 마련하는 것. 비용이 많이 드니까 비용 분석을 실시한다.
(3) 위험 수용 : 위험의 잠재 손실 비용을 감수하는 것. 일정 수준 이하로 감소시키고 사업을 계속 진행한다.
(4) 위험 전가 : 보험이나 외주 등으로 잠재적 위험을 제 3자에게 전가하는 방법이다.

10. Bell-LaPadula 보안 모델의 *-속성(star property)이 규정하고 있는 것은?
① 자신과 같거나 낮은 보안 수준의 객체만 읽을 수 있다.
② 자신과 같거나 낮은 보안 수준의 객체에만 쓸 수 있다.
③ 자신과 같거나 높은 보안 수준의 객체만 읽을 수 있다.
④ 자신과 같거나 높은 보안 수준의 객체에만 쓸 수 있다.
정답 체크 :
(4) *-속성 : 자신과 같거나 높은 보안 수준의 객체에만 쓸 수 있다. 낮은 등급의 주체가 상위 등급

의 객체를 보지 않은 상태에서 수정하여 덮어쓰기가 가능하므로 문서가 비인가자로부터 변경될 가능성이 있다. (No Write-Down, NWD, Confinement property)
오답 체크 :
(1) 자신과 같거나 낮은 보안 수준의 객체만 읽을 수 있다 : BLP 속성(No Read-Up, NRU, Simple Security Rule = ss-속성)
(2) 자신과 같거나 낮은 보안 수준의 객체에만 쓸 수 있다 : Biba 속성(No Write-Up, NWU)
(3) 자신과 같거나 높은 보안 수준의 객체만 읽을 수 있다 : Biba 속성(No Read-Down, NRD)

11. 버퍼 오버플로우에 대한 설명으로 옳지 않은 것은?
① 프로세스 간의 자원 경쟁을 유발하여 권한을 획득하는 기법으로 활용된다.
② C 프로그래밍 언어에서 배열에 기록되는 입력 데이터의 크기를 검사하지 않으면 발생할 수 있다.
③ 버퍼에 할당된 메모리의 경계를 침범해서 데이터 오류가 발생하게 되는 상황이다.
④ 버퍼 오버플로우 공격의 대응책 중 하나는 스택이나 힙에 삽입된 코드가 실행되지 않도록 하는 것이다.
정답 체크 :
(1) 자원 경쟁 : 해당 설명은 레이스 컨디션 공격 기법이다.
오답 체크 :
(2) 배열 : 해당 방법으로 함수의 복귀 주소가 공격자가 원하는 주소로 바뀌게 된다.
(3) 버퍼 : 해당 방법으로 함수의 복귀 주소가 공격자가 원하는 주소로 바뀌게 된다.
(4) 실행 : 버퍼 오버플로우에 대한 방어책으로 Non-Executable 스택(NX-bit)에 해당한다.

12. 침입 탐지 시스템(IDS)에서 알려지지 않은 공격을 탐지하는 데 적합한 기법은?
① 규칙 기반의 오용 탐지
② 통계적 분석에 의한 이상(anomaly) 탐지
③ 전문가 시스템을 이용한 오용 탐지
④ 시그니처 기반(signature based) 탐지
정답 체크 :
(2) 이상 탐지 : 통계적 분석, 예측 가능 패턴 생성, 신경망 방식 등은 모두 이상 탐지에 해당된다.
오답 체크 :
(1), (3), (4) 오용 탐지 : 규칙 기반, 전문가 시스템, 키 모니터링, 상태 전이 분석, 시그니처 기반(패턴 매칭) 등은 모두 오용 탐지에 해당된다.

13. 전자서명법상 공인인증기관이 발급한 공인인증서의 효력 소멸 또는 폐지의 사유에 해당 하지 않는 것은?
① 공인인증서의 유효 기간이 경과한 경우
② 가입자의 전자서명검증정보가 유출된 경우
③ 공인인증기관이 가입자의 사망·실종 선고 또는 해산 사실을 인지한 경우
④ 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우
정답 체크 :
(2) 전자서명검증정보는 공개키이므로 유출되어도 무방하다. 전자서명생성정보(개인키)와 혼동하지 말아야 한다. 자주 출제되는 용어이므로 기억해두는 것이 좋다.

오답 체크 :
(1), (3), (4)
“전자서명법” 제16조(공인인증서의 효력의 소멸 등) 상 공인인증기관이 발급한 공인인증서는 다음 각호의 1에 해당하는 사유가 발생한 경우에는 그 사유가 발생한 때에 그 효력이 소멸된다. 1. 공인인증서의 유효기간이 경과한 경우, 2. 제12조제1항의 규정에 의하여 공인인증기관의 지정이 취소된 경우, 3. 제17조의 규정에 의하여 공인인증서의 효력이 정지된 경우, 4. 제18조의 규정에 의하여 공인인증서가 폐지된 경우
“전자서명법” 제18조(공인인증서의 폐지) 상 공인인증기관은 공인인증서에 관하여 다음 각호의 1에 해당하는 사유가 발생한 경우에는 당해 공인인증서를 폐지하여야 한다. 1. 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우, 2. 가입자가 사위 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우, 3. 가입자의 사망 · 실종선고 또는 해산 사실을 인지한 경우, 4. 가입자의 전자서명생성정보가 분실 · 훼손 또는 도난 · 유출된 사실을 인지한 경우

14. 가상사설망(VPN)에 대한 설명으로 옳지 않은 것은?
① 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 별도의 전용선을 사용하는 사설망에 비해 구축 비용이 저렴하다.
② 사용자들 간의 안전한 통신을 위하여 기밀성, 무결성, 사용자 인증의 보안 기능을 제공한다.
③ 네트워크 종단점 사이에 가상터널이 형성되도록 하는 터널링 기능은 SSH와 같은 OSI 모델 4계층의 보안 프로토콜로 구현해야 한다.
④ 인터넷과 같은 공공 네트워크를 통해서 기업의 재택근무자나 이동 중인 직원이 안전하게 회사 시스템에 접근할 수 있도록 해준다.
정답 체크 :
(3) 터널링 : L2F, PPTP, L2TP를 사용해서 2계층에서 구현한다.
오답 체크 :
(1) 공중망, 사설망 : VPN은 공중망을 이용해서 비용을 절감할 수 있고, 사설망을 구성해서 안전하게 사용할 수 있다.
(2) 기밀성, 무결성, 인증 : IPSec 혹은 SSL을 사용하면 VPN을 구성하면 기밀성, 무결성, 인증 등을 제공할 수 있다.
(4) 회사 시스템 : VPN은 회사 시스템(본사와 지사 연결)에 사용될 수 있다.

15. ISO/IEC 27002 보안 통제의 범주에 대한 설명으로 옳지 않은 것은?
① 보안 정책 : 비즈니스 요구사항, 관련 법률 및 규정을 준수하여 관리 방향 및 정보 보안 지원을 제공
② 인적 자원 보안 : 조직 내의 정보 보안 및 외부자에 의해 사용되는 정보 및 자원 관리
③ 자산 관리 : 조직의 자산에 대한 적절한 보호를 성취하고 관리하며, 정보가 적절히 분류될 수 있도록 보장
④ 비즈니스 연속성 관리 : 비즈니스 활동에 대한 방해에 대처하고, 중대한 비즈니스 프로세스를 정보 시스템 실패 또는 재난으로부터 보호하며, 정보 시스템의 시의 적절한 재개를 보 장
정답 체크 :
(2) 인적 자원 보안 : 해당 설명은 접근 통제에 해당되고, 인적 자원 보안은 고용 전, 고용 중, 고용의 종료 또는 변경을 포함한다.

오답 체크 :
(1) 보안 정책 : 정보보호 정책의 문서화와 검토를 포함한다.
(3) 자산 관리 : 자산에 대한 책임과 정보 분류를 포함한다.
(4) 비즈니스 연속성 관리 : 사업지속성관리의 정보보호 측면을 포함한다.

16. OWASP(The Open Web Application Security Project)에서 발표한 2013년도 10대 웹 애플리케이션 보안 위험 중 발생 빈도가 높은 상위 3개에 속하지 않는 것은?
① Injection
② Cross-Site Scripting
③ Unvalidated Redirects and Forwards
④ Broken Authentication and Session Management
정답 체크 :
(3) Unvalidated Redirects and Forwards(10위) : 웹 애플리케이션은 종종 사용자들을 다른 페이지로 리다이렉트 하거나 포워드하고, 대상 페이지를 결정하기 위해 신뢰할 수 없는 데이터를 사용한다. 적절한 검증 절차가 없으면 공격자는 피해자를 피싱 또는 악성코드 사이트로 리다이렉트 하거나 승인되지 않은 페이지에 접근하도록 전달할 수 있다.
오답 체크 :
(1) Injection(1위) : SQL, 운영체제, LDAP 인젝션 취약점은 신뢰할 수 없는 데이터가 명령어나 질의문의 일부분으로서 인터프리터로 보내질 때 발생한다. 공격자의 악의적인 데이터는 예상하지 못하는 명령을 실행하거나 적절한 권한 없이 데이터에 접근하도록 인터프리터를 속일 수 있다.
(2) Cross-Site Scripting(3위) : 애플리케이션이 신뢰할 수 없는 데이터를 가져와 적절한 검증이나 제한 없이 웹 브라우저로 보낼 때 발생한다. XSS는 공격자가 피해자의 브라우저에 스크립트를 실행하여 사용자 세션 탈취, 웹 사이트 변조, 악의적인 사이트로 이동할 수 있다.
(4) Broken Authentication and Session Management(2위) : 인증과 세션 관리와 관련된 애플리케이션 기능은 정확하게 구현되어 있지 않아서, 공격자가 패스워드, 키 또는 세션 토큰을 해킹하거나 다른 구현 취약점을 공격하여 다른 사용자 ID로 가장할 수 있다.
Tip! : 참고로 2017년 Top 3는 Injection(1위), Broken Authentication(2위), Sensitive Data Exposure(3위)이다.

17. 전자우편의 보안 강화를 위한 S/MIME(Secure/Multipurpose Internet Mail Ex tension)에 대한 설명으로 옳은 것은?
① 메시지 다이제스트를 수신자의 공개키로 암호화하여 서명한다.
② 메시지를 대칭키로 암호화하고 이 대칭키를 발신자의 개인키로 암호화한 후 암호화된 메시지와 함께 보냄으로써 전자우편의 기밀성을 보장한다.
③ S/MIME를 이용하면 메시지가 항상 암호화되기 때문에 S/MIME 처리 능력이 없는 수신자는 전자우편 내용을 볼 수 없다.
④ 국제 표준 X.509 형식의 공개키 인증서를 사용한다.
정답 체크 :
(4) X.509 : 사용자 인증을 위해 공인인증서를 사용한다.
오답 체크 :
(1) 서명 : 발신자의 개인키로 암호화하여 서명한다.

(2) 기밀성 : 대칭키를 수신자의 공개키로 암호화한다.
(3) S/MIME : 메시지는 서명된 데이터(서명과 내용을 부호화한다), 클리어 서명 데이터(서명만 부호화하기 때문에 S/MIME 기능이 없는 수신자도 메시지를 볼 수 있다), 봉인된 데이터(메시지를 암호화한다), 서명 및 봉인된 데이터(메시지를 암호화하고, 암호화된 메시지에 서명한다)가 존재한다.

18. 국내 정보보호관리체계(ISMS)의 관리 과정 5단계 중 위험 관리 단계의 통제 항목에 해 당 하지 않는 것은?
① 위험 관리 방법 및 계획 수립
② 정보보호 대책 선정 및 이행 계획 수립
③ 정보보호 대책의 효과적 구현
④ 위험 식별 및 평가
정답 체크 :
(3) 정보보호대책 구현(Do) : 정보보호대책의 효과적 구현, 내부 공유 및 교육
오답 체크 :
(1), (2), (4) 위험 관리(Plan) : 위험관리 방법 및 계획 수립, 위험식별 및 평가, 정보보호대책 선정 및 이행계획 수립

19. 공개키 기반 전자서명에서 메시지에 서명하지 않고 메시지의 해시값과 같은 메시지 다이제스트에 서명하는 이유는?
① 공개키 암호화에 따른 성능 저하를 극복하기 위한 것이다.
② 서명자의 공개키를 쉽게 찾을 수 있도록 하기 위한 것이다.
③ 서명 재사용을 위한 것이다.
④ 원본 메시지가 없어 도서명을 검증할 수 있도록 하기 위한 것이다.
정답 체크 :
(1) 성능 저하 : 공개키 암호는 두 키의 수학적 특성에 기반하기 때문에, 메시지를 암호화 및 복호화 하는 과정에 여러 단계의 산술 연산이 들어간다. 따라서 대칭키 암호에 비하여 속도가 매우 느리다는 단점을 지니고 있다. 그러므로 연산해야 하는 메시지의 양을 줄이기 위해 메시지의 해시 값(다이제스트)에 서명을 수행한다.

20. 윈도우즈에서 지원하는 네트워크 관련 명령어와 주요 기능에 대한 설명으로 옳지 않은 것은?
① route : 라우팅 테이블의 정보 확인
② netstat : 연결 포트 등의 네트워크 상태 정보 확인
③ tracert : 네트워크 목적지까지의 경로 정보 확인
④ nslookup : 사용자 계정 정보 확인
정답 체크 :
(4) nslookup : 해당 명령어는 net user이고, nslookup은 인터넷 서버 관리자나 사용자가 호스트 이름을 입력하면 그 IP 주소를 알려 주는 프로그램이고, 그 반대의 경우에도 가능하다.
오답 체크 :
(1) route : IP 라우팅 테이블을 출력하거나 조작한다.
(2) netstat : 사용 포트를 확인할 때 사용한다.
(3) tracert : 최종 목적지 컴퓨터(서버)까지 중간에 거치는 여러 개의 라우터에 대한 경로 및 응답

속도를 표시해 준다. 리눅스에서는 traceroute를 사용한다.