2022-해경1차-네트워크보안-해설-곽후근

1. 다음 중 SSL(Secure Socket Layer) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?
① ChangeCipherSpec - Handshake 프로토콜에 의해 협상된 암호규격과 암호키를 이용하여 추후의 레코드 계층의 메시지를 보호할 것을 지시한다.
② Handshake - 서버와 클라이언트 간 상호인증 기능을 수행하고, 암호화 알고리즘과 이에 따른 키 교환 시 사용된다.
③ Alert - 내부적 및 외부적 보안 연관을 생성하기 위해 설계된 프로토콜이며, Peer가 IP 패킷을 송신할 필요가 있을 때, 트래픽의 유형에 해당하는 SA가 있는지를 알아보기 위해 보안 정책 데이터베이스를 조회한다.
④ Record - 상위계층으로부터(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용계층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택적으로 압축된다.

정답 체크
③ Alert: 해당 설명은 VPN에서 사용하는 IKE 프로토콜에 대한 설명이고, Alert는 뭔가 에러가 발생했다는 것을 통신 상대에게 전달한다.
오답 체크
① ChangeCipherSpec: 암호 방법을 변경하는 신호를 통신 상대에게 전달한다.
② Handshake: 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유 키를 결정한다. 인증서를 이용한 인증을 수행한다.
④ Record: 대칭 암호를 사용해서 메시지를 암호화하고 통신하는 부분이다. 대칭 암호와 메시지 인증 코드를 이용한다. 알고리즘과 공유 키는 핸드쉐이크 프로토콜을 사용해서 서버와 클라이언트가 상담하여 결정한다.

2. 다음 중 망 내 교환 장비들이 오류 상황에 대한 보고를 할 수 있게 하고, 예상하지 못한 상황이 발생한 경우 이를 알릴 수 있도록 지원하는 프로토콜은 무엇인가?
① ICMP ② ARP ③ RARP ④ IGMP

정답 체크
(1) 인터넷 제어 메시지 프로토콜은 RFC 792에서 정의한 인터넷 프로토콜 모음 중의 하나이다. ICMP 메시지들은 일반적으로 IP 동작에서 진단이나 제어로 사용되거나 오류에 대한 응답으로 만들어진다. 예를 들어, 핑(ping) 유틸리티는 ICMP "에코 요청(Echo request)"과 "에코 응답(Echo reply)" 메시지를 사용해 구현할 수 있다.
오답 체크
(2) IP 주소(논리 주소)에 대한 MAC 주소(물리 주소)를 제공한다.
(3) MAC 주소에 대한 IP 주소를 제공한다.
(4) 인터넷 그룹 관리 프로토콜은 호스트 컴퓨터와 인접 라우터가 멀티캐스트 그룹 멤버십을 구성하는 데 사용하는 통신 프로토콜이다. 특히 IPTV와 같은 곳에서 호스트가 특정 그룹에 가입하거나 탈퇴하는데 사용하는 프로토콜을 가리킨다.

3. 다음 〈보기〉 중 제시된 Well Known Port 번호에 해당하는 프로토콜을 순서대로 가장 적합하게 제시한 것은?

〈 보 기 〉
㉠ 22번 포트 ㉡ 53번 포트 ㉢ 161번 포트

① ㉠ SSH ㉡ Gopher ㉢ NetBIOS
② ㉠ SSH ㉡ DNS ㉢ SNMP
③ ㉠ FTP ㉡ Gopher ㉢ SNMP
④ ㉠ FTP ㉡ DNS ㉢ NetBIOS

정답 체크

(2) 주요 서버스와 포트 번호는 다음과 같다.

포트 번호	서비스	설명
20	FTP	• File Transfer Protocol (Data) • FTP 연결 시 실제로 데이터를 전송한다.
21	FTP	• File Transfer Protocol (Control) • FTP 연결 시 인증과 제어를 한다.
23, 22	Telnet, SSH	• 텔넷 서비스로, 원격지 서버의 실행창을 얻어낸다.
25	SMTP	• Simple Message Transfer Protocol • 메일을 보낼 때 사용한다.
53	DNS	• Domain Name Service • 이름을 해석하는 데 사용한다.
69	TFTP	• Trivial File Transfer Protocol • 인증이 존재하지 않는 단순한 파일 전송에 사용한다.
80	HTTP	• Hyper Text Transfer Protocol • 웹서비스를 제공한다.
110	POP3	• Post Office Protocol • 메일 서버로 전송된 메일을 읽을 때 사용한다.
111	RPC	• Sun의 Remote Procedure Call • 원격에서 서버의 프로세스를 실행할 수 있게 한다.
138	NetBIOS	• Network Basic Input Output Service • 윈도우에서 파일을 공유할 수 있게 한다.
143	IMAP	• Internet Message Access Protocol • POP3와 기본적으로 같으나, 메일이 확인된 후에도 서버에 남는다는 것이 다르다.
161, 162	SNMP	• Simple Network Management Protocol • 네트워크 관리와 모니터링을 위해 사용한다.

오답 체크

(1), (3), (4) FTP, NetBIOS는 위의 표를 참고한다.

Gopher은 70번 포트를 사용한다.

4. 다음 중 OSI 7계층 모델에서 동작하는 계층이 가장 다른 것은?
① L2TP ② PPTP
③ SYN 플러딩 ④ ARP 스푸핑

정답 체크
(3) 4계층: SYN 플러딩 → 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다. (syn cookie를 이용해서 막을 수 있다.)
오답 체크
(1), (2) 2계층: L2TP(PPTP+L2F), PPTP(1:1 연결) → VPN에서 사용하는 터널링 프로토콜, L2F(1:N 연결)도 존재한다.
(4) 2계층: ARP 스푸핑 → 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다. (3계층과 경계가 애매하나 가장 틀린 답은 아님)

5. 다음 중 SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 옳지 않은 것은?
① MIB는 객체의 이름을 붙이고 객체의 유형을 정의하며, 객체와 값을 부호화하는 등의 일반적인 규칙을 정의한다.
② 관리자는 GetRequest와 같은 메시지를 에이전트에 보내서 에이전트의 정보를 요구한다.
③ 에이전트는 비정상적인 상황을 관리자에게 경고하기 위하여 Trap 메시지를 관리자에 보냄으로써 관리 과정에 기여할 수 있다.
④ TCP/IP 프로토콜을 사용하는 네트워크에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.

정답 체크
(1) SMI를 의미하고, MIB는 관리자가 조회하거나 설정할 수 있는 개체들의 데이터베이스이다.
오답 체크
(2) Get Request, Get Next Request, Set Request, Get Response 등을 이용한다.
(3) Trap 메시지에는 Cold Start, Warm Start, Link Down, Link Up 등이 존재한다.
(4) Get Request를 위해 161번 포트를 사용하고, Trap을 위해 162번 포트를 사용한다.

6. 취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은 무엇인가?
① DoS 공격 ② 취약한 인증 및 세션 공격 ③ SQL 삽입 공격 ④ CSRF 공격

정답 체크
④ CSRF: 웹 사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행

위(수정, 삭제, 등록 등)를 특정 웹 사이트에 요청하게 하는 공격
오답 체크
① DoS: flooding 공격 등을 통해 서버를 무력화시킨다.
② 취약한 인증 및 세션 공격:
• URL에 세션 정보가 노출 되도록 코딩하는 경우이다.
• 공공장소의 컴퓨터에서 사용되는 어플리케이션에서 세션 타임아웃이 없고, 로그아웃을 하지 않고 단순히 브라우저만 닫아서 세션이 유지되는 경우이다.
• 쿠키 변조: 쿠키를 사용하는 웹페이지의 경우 쿠키를 암호화할 때 취약한 암호를 사용하는 경우이다.
③ SQL 삽입: 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이 있다.

7. 다음 중 SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는데 악용될 수 있는 명령어는 무엇인가?
① HELO ② MAIL FROM
③ RCPT TO ④ VRFY

정답 체크
④ VRFY: 수신자의 주소를 조회하려고 사용한다.
오답 체크
① HELO: SMTP 세션을 시작하며, 송신자의 호스트 이름을 전송하여 서버에 자신의 신분을 알려준다.
② MAIL FROM: 송신자의 메일 주소를 통지한다.
③ RCPT TO: 수신자의 메일 주소를 통지한다.

8. 다음 중 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 가장 옳지 않은 것은?
① 물리적 망분리와 논리적 망분리 기법이 존재한다.
② 물리적 망분리가 되었다 하더라도 USB와 같은 저장 매체를 통한 악성 코드 침입이 가능하다.
③ 논리적 망분리 기법으로 SBC 및 CBC 기반의 망분리 기법이 존재한다.
④ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.

정답 체크
④ 애플리케이션 가상화 및 데스크톱 가상화는 물리적 망분리가 아니라 논리적 망분리이다.
오답 체크
① 물리적 망분리는 물리적으로 2대의 PC를 사용하고, 논리적 망분리는 SBC, CBC를 이용하여 논리적으로 1대의 PC를 사용한다.
② 물리적으로 2대의 PC를 사용한다고 하더라도 USB와 같은 저장 매체를 통해 악성 코드 침입이 가능하다(사회공학기법: 누군가 회사앞에 USB를 떨어뜨려놓고 회사 사람이 그것을 주워 자신의 회사 PC에 꽂아봄).
③ 논리적 망분리에서는 SBC(서버 기반 가상화)와 CBC(클라이언트 기반 가상화) 기법이 존재한다.

9. 다음 중 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직으로 가장 옳은 것은?
① CISO ② CERT ③ CPPG ④ CPO

정답 체크
② CERT: 1988년 11월 22일 저녁, 미국 전역의 컴퓨터가 모리스 웜에 의해 멎어버린 사건 이후 미 정부가 적극적으로 적절한 침해 사고의 대응책을 마련했다. DARPA(The Defense Advanced Research Projects Agency)은 컴퓨터와 관련한 침해 사고에 적절히 대응하고자, 피치버그의 카네기 멜론 대학 내의 소프트웨어공학 연구소에 CERT(Computer Emergency Response Team) 팀을 만들었다.
오답 체크
① CISO: 최고정보보안임원(Chief Information Security Officer)은 조직의 정보 및 데이터 보안을 책임지는 임원이다. (CSO와 비슷한 개념이다.)
③ CPPG: 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 갖춘 인력 또는 향후 기업 또는 기관의 개인정보 관리를 희망하는 자가 취득하는 비공인 민간 자격이다(Certified Privacy Protection General).
④ CPO: 개인정보 보호책임자(Chief Privacy Officer)로서, 홈페이지에 공개한다.

10. 다음 중 HTTP 응답 메시지 상태 코드의 의미가 가장 옳지 않은 것은?
① 201 - Created ② 301 - Moved Permanently
③ 401 - Unauthorized ④ 501 - Bad Request

정답 체크
(4) 501은 Not Implemented이고, Bad Request는 400이다.
오답 체크
(1) 요청이 성공적으로 처리되었고, 자원이 생성되었음을 나타낸다.
(2) 요구한 데이터를 변경된 임시 URL에서 찾았음을 나타낸다(주어진 URL로 완전히 옮겨짐).
(3) 특정 웹 사이트에 접속하기 위해 정확한 사용자 아이디와 암호를 입력하여야 하는데, 잘못된 정보를 입력하였을 경우이다.

11. 다음 중 IP Spoofing 공격 활동으로 가장 옳지 않은 것은?
① SYN Flooding 공격
② slowloris 공격
③ RST를 이용한 접속 끊기
④ 순서번호 추측(Sequence number guessing)

정답 체크
(2) 느리게 공격하는 DoS 공격에 해당한다.
오답 체크
(1) 서버에 접속된 클라이언트를 해당 공격으로 제거한다.

(3) 서버와 클라이언트의 접속을 끊는다.
(4) 공격자가 순서번호를 추측하여 서버와 연결을 맺는다.

12. 다음 중 ESM(통합보안솔루션)의 구성요소에 대한 설명으로 가장 옳지 않은 것은?
① 보안패치 : 최근 보안취약점이 발생한 시스템에 대해서 자동으로 패치를 수행한다.
② Manager : 수집된 로그정보를 통합하고 분석한다.
③ Console : 관리자는 ESM Console을 사용해서 모니터링하고 명령어를 실행한다.
④ Agent : 시스템에 설치되어서 각종 로그정보를 수집한다.

정답 체크
(1) 보안패치는 ESM의 구성요소가 아니다.
오답 체크
(2) 로그를 데이터베이스에 저장하고 분석한다.
(3) 보안 정보를 모니터링하여 침입 발생 시 명령을 전달한다.
(4) 각종 보안 솔루션의 로그를 수집한다.

13. 다음 중 〈보기〉의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

〈 보 기 〉
(㉠)는 웹 페이지에 입력되는 입력 값 검증 및 필터링 등을 수행하는 방화벽이다.
(㉡)는 모바일 단말에 대해서 소프트웨어 및 펌웨어를 관리하는 솔루션이다.
(㉢)는 네트워크 패킷을 탐지하고 대응 까 지 수행한다.

① ㉠ WAF(Web Application Firewall) ㉡ MDM ㉢ IPS
② ㉠ WAF(Web Application Firewall) ㉡ MAM ㉢ IDS
③ ㉠ Firewall ㉡ MDM ㉢ IDS
④ ㉠ Firewall ㉡ MAM ㉢ IPS

정답 체크
(1) WAF : 방화벽 기능이 웹에 특화되었다.
MDM : MDM은 통상 IT 부서가 기기를 완전히 제어할 수 있도록, 직원의 스마트패드와 스마트폰에 잠금·제어·암호화·보안 정책 실행을 할 수 있는 기능을 제공한다.
IPS : 수동적인 방어 개념의 침입 차단 시스템(Firewall)이나 침입 탐지 시스템(IDS)과 달리 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다.
오답 체크
(2), (3), (4) MAM : 스마트 기기 전체가 아니라, 기기에 설치된 업무 관련 앱만 보안 및 관리 기능을 적용한다.
IDS : 네트워크나 시스템의 미심쩍은 점을 조사 및 감시하고, 필요한 조치를 취하는 시스템이다. 사용자 시스템의 행동을 분석 및 관찰하고, 설정된 시스템에 대한 보안 상태를 테스트한다. 탐지만 수행하고 적극적 방어를 수행하지 않는다(수동적 장비).
Firewall : 인터넷과 같은 외부 네트워크로부터 기업의 내부 네트워크를 보호하는 보안 장치로, 외부 네트워크와 내부 네트워크 사이의 유일한 연결점에 위치해 트래픽(Traffic)을 제어하는 시스템을 말

한다(port와 ip를 이용하여 접근 제어).

14. 다음 중 Spoofing의 종류로 가장 옳지 않은 것은?
① ARP Spoofing ② IP Spoofing
③ DNS Spoofing ④ ULU Spoofing

정답 체크
(4) 통상적으로 사용하는 spoofing이 아니다.
오답 체크
(1) 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다. 상대방의 MAC을 고정해서 방어한다.
(2) 서버와 트러스트(Trust)로 관계를 맺고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어진다.
(3) 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다.

15. 다음 〈보기〉는 VPN에 대한 설명이다. ( )에 들어갈 설명으로 가장 옳은 것은?

〈 보 기 〉
· IPSEC VPN은 (㉠) 단위로 데이터를 암호화 한다.
· SSL VPN은 (㉡) 단위로 데이터를 암호화 한다.

① ㉠ 프레임 ㉡ 데이터 ② ㉠ 데이터 ㉡ 프레임
③ ㉠ 패킷 ㉡ 메시지 ④ ㉠ 메시지 ㉡ 메시지

정답 체크
(3) IPSEC : 3계층 PDU인 패킷을 암호화한다.
SSL : 5, 6, 7계층 PDU인 메시지를 암호호한다.
오답 체크
(1), (2), (4) 데이터 : 5, 6, 7계층 PDU이다.
프레임 : 2계층 PDU이다.

16. 다음 〈보기〉는 VLAN(Virtual Local Area Network)에 대한 설명이다. 다음 중 ( )에 들어갈 설명으로 가장 옳은 것은?

〈 보 기 〉
VLAN은 여러 개의 구별되는 (㉠) 도메인을 만들기 위해서 단일 2 계층 네트워크를 (㉡)으로 분할하고 한 포트에서 보이는 모든 네트워크 패킷 혹은 전체 VLAN의 모든 패킷들을 다른 모니터링 포트로 복제하는 (㉢) 기능을 제공한다.

① ㉠ 유니캐스트 ㉡ 물리적 ㉢ 허브 미러링
② ㉠ 브로드캐스트 ㉡ 논리적 ㉢ 포트 미러링
③ ㉠ 유니캐스트 ㉡ 논리적 ㉢ 포트 미러링

④ ㉠ 브로드캐스트 ㉡ 물리적 ㉢ 허브 미러링

정답 체크
(2) 브로드캐스트 : 브로드캐스트 도메인을 분리한다(나의 브로드캐스트가 어디까지 전송될 것인가?).
논리적 : 물리적으로 분리(아래 내용 참고)하지 않고 논리적으로 분리한다.
포트 미러링 : 포트로 오고가는 패킷을 다른 포트로 복사한다.
오답 체크
(1), (3), (4) 유니캐스트 : 유니캐스트 도메인은 따로 분리할 필요가 없다.
물리적 : 2개의 이상의 랜카드를 사용한다.
허브 미러링 : 통상적으로 사용하는 용어가 아니다.

17. 다음 중 〈보기〉의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

〈 보 기 〉
ANTI APT 솔루션에서 악성코드를 동적으로 분석하기 위해서 악성코드를 실행한 후에 행위 로그를 분석한다. 이 때 악성코드 분석은 ( ) 환경에서 수행되어야 한다.

① SCADA ② Sandbox
③ Cloud ④ CRM

정답 체크
(2) 외부로부터 받은 파일을 바로 실행하지 않고 보호된 영역에서 실행시켜 봄으로써 외부로부터 들어오는 파일과 프로그램이 내부 시스템에 악영향을 주는 것을 미연에 방지하는 기술이다.
오답 체크
(1) 국가 및 산업의 중요 기반 시설을 제어하는 시스템이다(Stuxnet의 공격 대상).
(3) 인터넷 기술을 활용하여 'IT 자원을 서비스'로 제공하는 것으로 IT 자원(소프트웨어, 스토리지, 서버, 네트워크 등)을 필요한 만큼 사용하고 서비스 부하에 따라서 실시간 확장이 가능하며 사용한 만큼 비용을 지불하는 서비스이다.
(4) 소비자들을 자신의 고객으로 만들고, 이를 장기간 유지하고자 하는 경영방식이며 기업들이 고객과의 관계를 관리, 고객 확보, 그리고 고객, 판매인, 협력자와 내부 정보를 분석하고 저장하는데 사용하는 광대한 분야를 아우르는 방법이다.

18. 다음 중 〈보기〉의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

〈 보 기 〉
Tcpdump는 네트워크에서 전송되는 패킷을 스니핑하는 도구이다. 전송되는 패킷을 특정 포트로 (㉠), 스니핑 모드를 (㉡)(으)로 설정해야 한다.

① ㉠ 포트 미러링 ㉡ 정규 모드
② ㉠ 무차별 모드 ㉡ 포트 미러링
③ ㉠ 포트 미러링 ㉡ 무차별 모드
④ ㉠ 무차별 모드 ㉡ 정규 모드

정답 체크

(3) 포트 미러링 : 포트로 오고가는 패킷을 다른 포트로 복사한다.
무차별 모드 : promiscuous 모드를 의미한다(모든 패킷을 받아들임).
오답 체크
(1), (2), (4) 정규 모드 : non-promiscuous 모드를 의미한다(IP와 MAC을 기준으로 패킷을 차단).

19. 다음 중 〈보기〉의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

〈 보 기 〉
IPv6는 (㉠)비트의 주소 공간을 가지며 헤더는 총 (㉡)개의 필드를 가지고 있다. 그리고 암호화와 (㉢)기능을 지원한다.

① ㉠ 128 ㉡ 8 ㉢ 인증 ② ㉠ 32 ㉡ 4 ㉢ 인증
③ ㉠ 32 ㉡ 8 ㉢ 인가 ④ ㉠ 128 ㉡ 4 ㉢ 인가

정답 체크
(1) 128 : IPv6의 주소는 128비트이다.
8 : Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop limit, Source Address, Destination Address의 필드를 가진다.
인증 : 사용자의 신원을 증명한다.
오답 체크
(2), (3), (4) 32 : IPv4의 주소 길이이다.
4 : IPv6는 8개의 필드를 가진다.
인가 : 특정 리소스에 접근할 수 있는 권한을 부여한 것이다.

20. 다음 중 리눅스 시스템의 네트워크 관리 도구 및 서비스에 대한 설명으로 가장 옳지 않은 것은?
① ifconfig - 네트워크 인터페이스의 IP 주소 설정
② traceroute - 최종 목적지 컴퓨터까지 중간에 걸치는 여러 개의 라우터에 대한 경로 및 응답 속도를 표시
③ fping - 네트워크 연결 상태, 라우팅 테이블, 인터페이스 관련 통계 정보 출력
④ tcpdump - 네트워크 모니터링 및 패킷 분석을 위해 사용되는 도구로, 패킷 필터 기능을 통해서, 특정 침입자의 침입 경로에 따라 원하는 트래픽만을 감시

정답 체크
(3) netstat에 대한 설명이고, fping은 ping sweep(여러 개의 서버나 네트워크 전체를 대상으로 ping)를 한다.
오답 체크
(1) 유닉스 혹은 리눅스에서 일반적으로 네트워크 인터페이스의 IP 주소와 넷마스크의 설정 및 인터페이스의 활성화/비활성화 등을 위해 사용된다.
(2) 리눅스에서 최종 목적지 컴퓨터(서버)까지 중간에 거치는 여러 개의 라우터에 대한 경로 및 응답속도를 표시해 준다. 윈도우에서는 tracert를 사용한다.
(4) 명령 줄에서 실행하는 일반적인 패킷 가로채기 소프트웨어이다.