2021-해경1차-네트워크보안-해설-곽후근

1. 다음 〈보기〉의 ㉠, ㉡, ㉢에 가장 적합한 것으로 짝지어진 것은?

〈 보기 〉
○ 이더넷은 네트워크 인터페이스 카드에 설정된 ㉠ 물리적 주소를 사용한다.
○ 네트워크 계층의 주소는 ㉡ 논리 주소를 사용한다.
○ 전송계층의 주소는 ㉢ 포트 주소를 사용한다.

① ㉠ 8Byte ㉡ 2Byte ㉢ 1Byte
② ㉠ 8Byte ㉡ 4Byte ㉢ 2Byte
③ ㉠ 6Byte ㉡ 2Byte ㉢ 1Byte
④ ㉠ 6Byte ㉡ 4Byte ㉢ 2Byte

정답 체크
(4) ㉠ 6Byte : MAC 주소는 6바이트이다.
㉡ 4Byte : IP 주소는 4바이트이다(IPv4의 경우).
㉢ 2Byte : 포트 주소는 2바이트이다.

2. 다음 〈보기〉는 라우터를 이용한 네트워크 보안 설정에 관련된 내용이다. 가장 옳은 내용을 모두 고르시오.

〈 보기 〉
㉠ egress 필터링은 라우터 내부에서 외부로 나가는 패킷의 소스 IP를 체크하여 필터링하는 것이다.
㉡ ingress 필터링은 standard 또는 extended access-list를 활용하여 라우터 내부로 유입되는 패킷의 소스 IP나 목적지 포트 등을 체크하여 허용하거나 거부하도록 필터링하는 것이다.
㉢ blackhole 필터링이란 인터페이스를 통해 들어오는 패킷의 소스 IP에 대해 라우팅 테이블을 확인하여 들어온 인터페이스로 다시 나가는지 확인하는 것이다.
㉣ unicast RPF는 access-list나 blackhole 필터링을 이용하여 일일이 IP나, IP대역을 지정하지 않고도 비정상 트래픽을 효율적으로 필터링할 수 있다.

① ㉠, ㉡, ㉢ ② ㉠, ㉣
③ ㉠, ㉡, ㉣ ④ ㉠, ㉡, ㉢, ㉣

정답 체크
(3) ㄱ : 라우터 외부에서 라우터 내부로 유입되는 패킷을 필터링하는 것이다. 패킷의 소스 IP 나 목적지 포트 등을 체크하여 허용하거나 거부하도록 필터링 하는 것을 뜻한다.
ㄴ : 라우터 외부로 나가는 패킷의 소스 IP만을 검사하여 필터링하는 것으로, 라우터 내부의 네트워크에서 소스 IP를 위조하여 다른 네트워크를 공격하는 형태의 공격을 차단하는 필터링 기법이다.
ㄹ : 인터페이스를 통해 들어오는 패킷의 소스 ip 에 대해 라우팅 테이블을 확인하여 들어온 인터페이스로 다시 나가는지 확인한다(악의적인 트래픽 공격을 막기 위해 사용).
오답 체크
(1) ㄹ이 없다.
(2) ㄴ이 없다.
(4) ㄷ : unicast RPF에 대한 설명이고, blackhole 필터링이란 특정한 ip 대역에 대해서 Null 이라는 가상의 쓰레기 인터페이스로 보내도록 함으로써 패킷의 통신이 되지 않도록 하도록 하는 필터

링 기법으로 null routing을 활용한 필터링이라고도 한다.

3. TCP는 흐름 제어를 다루기 위하여 슬라이딩 윈도우 (Sliding Window)를 사용한다. 수신자 호스트 B는 8500 바이트의 버퍼를 갖고 있으며, 현재 버퍼에 3150 바이트의 처리되지 않은 데이터를 갖고 있다고 가정했을 때, 호스트 A를 위한 수신자 윈도우(rwnd) 값은?
① 3150 ② 5350
③ 8500 ④ 11650
정답 체크
(2) 수신자 윈도우는 자신이 받을 수 있는 크기이므로 8500(총 크기)에서 3150(처리되지 않은 크기)을 빼주면 된다.

4. 다음 중 DDoS(Distributed Denial of Service) 공격과 툴에 대한 설명으로 가장 옳지 않은 것은?
① Teardrop은 두 번째 패킷의 Fragment Offset을 위조하여, 첫 번째 패킷 다음에 두 번째 패킷을 추가하지 않고 첫 번째 패킷의 TCP 헤더와 데이터 부분을 덮어쓰게 한다.
② Trinoo는 UDP Flood 서비스 거부 공격에 사용되는 툴이다.
③ Ghost Call은 IP Scan 이후 프리픽스로 호를 시도하여, Digest 인증을 해킹하는 공격을 의미하는 것이 아니라, 단순한 INVITE를 보내는 패턴 공격이다.
④ NetBot Attacker는 발신지와 수신지 IP를 동일하게 설정하여 라우터 및 서버의 성능장애나 시스템 다운을 유발시킨다.
정답 체크
(4) land 공격에 대한 설명이고, NetBot Attacker는 DDoS 공격 툴이다.
오답 체크
(1) 데이터의 송수신과정에서 데이터의 송신한계를 넘으면 MTU(1500byte) 조각으로 나누어 fragment number를 붙여 송신하고, 수신측에는 fragment 넘버로 재조합하여 분석한다. fragment 내의 나누어진 byte 정보인 fragmentation offset을 위조하여 offset을 중복되게 하거나 공간을 두면 수신측에서 재조합이 안 되어 다운이 되게 하는 공격이다. UDP인 경우는 fragment offset이 중첩되고, TCP인 경우 순서 번호가 중첩된다.
(2) 1999년 6월 말부터 7월 사이에 퍼지기 시작한 것으로, 미네소타 대학 사고의 주범이다(원래 이름은 Trin00). 솔라리스 2.x(유닉스) 시스템에서 처음 발견되었으며, 최소 227개 시스템이 공격에 쓰인 것으로 알려져 있다. UDP를 기본으로 공격을 시행하며 'statd, cmsd, ttdbserverd' 데몬이 주된 공격 대상으로 한다.
(3) 통화 수신자가 응답 할 때 통화의 다른 쪽 끝에 아무도없는 전화 통화이다. 이 용어는 IP PBX 시스템 관리에도 사용된다.

5. ICMP(Internet Control Message Protocol) 프로토콜은 문제를 해결하는 기능과 전달할 수 없는 패킷에 대한 에러 정보를 알리기 위해 사용된다. 아래 대표적인 ICMP 메시지의 기능을 설명한 것 중 가장 옳지 않은 것은?
① Echo Request 메시지는 원하는 호스트로의 IP 연결을 확인하기 위해 사용된다.
② Destination Unreachable은 라우터나 목적호스트에 의해 보내지며 데이터그램이 전달되지 못한다는 것을 데이터를 보낸 호스트에 알려준다.

③ Source Quench는 데이터를 보내는 호스트에게 IP 데이터그램이 라우터의 집중현상에 의해 손실되고 있음을 알리기 위해 라우터가 보내는 메시지이다.
④ Echo Reply는 데이터를 보내는 호스트에게 목적 IP 주소에 대한 좀 더 적합한 경로가 있음을 알리기 위해 라우터가 보내는 메시지이다.
정답 체크
(4) Echo Request의 응답으로 보내는 메시지이다.
오답 체크
(1) Echo Request 메시지는 송신측의 전송 패킷이 목적지 노드나 라우터에 도착했는지를 확인하는데 사용한다(주로 ping에서 사용).
(2) 라우터가 특정 노드의 패킷을 목적지에 보내지 못할 경우 보내는 메시지이다. 목적지까지 전송되지 못한 이유를 나타내는 정보가 포함된다.
(3) IP 라우터의 WAN 쪽에 집중이 발생하여 송신 불능 상태가 되면 보내는 메시지이다(보내는 양을 줄여달라는 메시지).

6. 다음 TCP(Transport Control Protocol) 프로토콜의 타이머에 대한 설명 중 가장 옳지 않은 것은?
① RTO 값은 해당 시간까지 Acknowledge가 전송되어 오지 않는 경우, 재전송하기 위한 설정값이다.
② RTO 값은 초기 RTT값을 기준으로 항상 고정되어 있다.
③ RTO 시간이 너무 클 경우 수신측의 중복 ACK에 대한 손실 세그먼트를 재전송 하는 Fast retransmission 현상이 발생한다.
④ TCP 세그먼트가 유실되어, 해당 세그먼트를 요구하는 Acknowledge가 계속 도착하더라도 RTO 시간이 Time-out되어야 재전송이 가능하다.
정답 체크
(2) RTT를 기반으로 동적으로 생성된다.
오답 체크
(1) 재전송을 위해 타이머가 작동하는 시간을 의미한다.
(3) 중복 ACK가 3번 도착하면 RTO를 기다리지 않고 재전송을 수행한다.
(4) Fast retransmission을 제외하고, RTO의 타이머가 타임아웃이 되어야 재전송이 가능하다.

7. 다음 〈보기〉는 TCP Session Hijacking의 공격 순서를 나열한 것이다. 순서가 가장 옳은 것은?

〈 보기 〉
㉠ 공격 목표를 정하고 공격 대상을 설정한다.
㉡ 시퀀스 넘버의 난이도 검사를 한다.
㉢ TCP/IP 스택 구현이나 원리를 예측하고, 이를 통하여 얻어진 데이터로부터 시퀀스 넘버를 추측한다.
㉣ 공격자가 세션을 설정하고자 하는 컴퓨터로부터 시퀀스 넘버의 추측이 끝나면 그 서버와 연결되어 있는 컴퓨터에게 DoS 공격 등을 통하여 사용자를 제거한다.
㉤ 공격 대상에 세션을 설정하여 현재 공격 목표와 연결되어있는 공격 대상의 세션을 설정한다.
㉥ 제거된 사용자로부터 추측한 시퀀스 넘버를 이용하여 Session Hijacking을 실시한다.

① ㉠-㉡-㉢-㉣-㉤-㉥ ② ㉠-㉤-㉡-㉣-㉢-㉥ ③ ㉠-㉢-㉣-㉡-㉤-㉥ ④ ㉠-㉡-㉤-㉢-㉣-㉥

정답 체크
(3) ㄱ : 첫단계는 공격 목표를 설정하는 것이다.
ㄷ : 공격자가 서버와 통신하기 위한 순서 번호를 추측한다.
ㄹ : 사용자(클라이언트)를 제거한다. 앞으로 공격자와 서버가 통신한다.
ㄴ : 사용자를 대신해 보낼 순서 번호의 난이도를 검사한다(얼마나 어려운지?).
ㅁ : 공격자가 RST과 3-way handshaking을 이용하여 서버와 세션을 설정한다.
ㅂ : 마지막 단계는 설정된 세션에 추측한 순서 번호를 이용하여 세션 하이재킹을 실시한다.

8. 다음 중 침입 방지 시스템에 대한 설명으로 가장 옳지 않은 것은?
① 침입 방지 시스템의 검사영역은 네트워크 계층과 전송계층의 IP/Port 정보를 기반으로 동작한다.
② 침입 방지 시스템의 검사영역은 방화벽이 검사할 수 없는 전송계층 상단의 어플리케이션 계층의 데이터까지도 검사가 가능하다.
③ 침입 경고 이전에 상대의 공격을 중단시키는데 목적을 두고 있다.
④ 안티 바이러스와 같은 시그니처 기반의 기술과 방화벽과 같은 네트워크 차단기능이 결합된 방식을 침입 방지 시스템이라 한다.
정답 체크
(1) 방화벽에 대한 설명이다.
오답 체크
(2) 7계층(payload) 데이터를 검사한다(패킷의 내용과 시그너처를 비교).
(3) 능동적 보안 장비이다. 참고로 IDS는 수동적 보안 장비이다.
(4) 방화벽(IP/Port 기반)과 IDS(시그너처 기반)의 장점을 결합한 장비이다.

9. 다음 중 무선 보안 강화 방안을 설명한 것 중 가장 옳지 않은 것은?
① SSID를 브로드캐스트 불가로 접속하면 누구도 접속할 수 없다.
② TKIP은 WEP을 적용할 수 있도록 구성된 무선랜 장비 펌웨어 업그레이드나 소프트웨어 업그레이드를 통해 사용자 레벨의 보안을 강화하기 위한 방법을 제공하고 있다.
③ WEP는 RC4 스트림 암호화 기법을 사용하고 키 스트림을 정적 키를 사용한다.
④ IEEE 802.11i는 AES 암호화 기법을 사용한다.
정답 체크
(1) 브로드캐스트를 하지 않을 때 직접 SSID 이름을 입력하여 접속할 수 있다.
오답 체크
(2) WEP의 취약성을 보완하기 위해 RC4 암호 알고리즘의 입력 키 길이를 128 비트로 늘리고 패킷당 키 할당, 키값 재설정 등 키 관리 방식을 개선하였다. 네트워크에 접근하는 사람을 제한할 수 있는 기능도 있다.
(3) WEP는 RC4(스트림 키)를 사용하고 키가 고정이다.
(4) WPA2는 CCMP와 AES를 사용한다.

10. 다음 중 가상사설망(VPN) 구현에 사용되는 터널링 프로토콜(Tunneling Protocol)로 가장 옳은 것은?
① PPTP, IPSEC, MPLS
② PPTP, L2TF, WAP

③ IPSEC, SET, SSL
④ L2TF, WAP, IPSEC
정답 체크
(1) PPTP : 2계층 터널링 프로토콜이다.
IPSEC : 3계층 터널링 프로토콜이다.
MPLS : 기존 2계층, 3계층 터널링 프로토콜을 지원한다.
오답 체크
(2), (4) WAP : 휴대 전화 등의 장비에서 인터넷을 하는 것과 같은, 무선 통신을 사용하는 응용 프로그램의 국제 표준이다. WAP은 매우 작은 이동 장비에 웹 브라우저와 같은 서비스를 제공하기 위해 설계되었다. WAP의 구조는 네트워크, 전송, 보안(기존 유선 구조에서는 없음), 세션, 응용 계층 등으로 구성된다.
(3) SET : 전자상거래를 위한 프로토콜이다.
SSL : 4계층 터널링 프로토콜이다.

11. 다음 〈보기〉는 오용탐지(Misuse Detection)와 이상탐지 (Anomaly Detection)에 대한 설명이다. 이상탐지에 해당되는 것을 모두 고른 것은?

〈 보기 〉
㉠ 통계적 분석방법 등을 활용하여 급격한 변화를 발견하면 침입으로 판단한다.
㉡ 미리 축적한 시그니처와 일치하면 침입으로 판단한다.
㉢ 제로데이 공격탐지에 적합하다.
㉣ 임계값을 설정하기 쉽기 때문에 오탐률이 낮다.

① ㉠, ㉢ ② ㉠, ㉣ ③ ㉡, ㉢ ④ ㉡, ㉣
정답 체크
(1) ㄱ. 통계적 분석 방법 등을 활용하여 급격한 변화를 발견하면 침입으로 판단한다: 이상탐지
ㄷ. 제로데이 공격을 탐지하기에 적합하다: 이상탐지
오답 체크
(2), (3), (4)
ㄴ. 미리 축적한 시그너처와 일치하면 침입으로 판단한다: 오용탐지
ㄹ. 임계값을 설정하기 쉽기 때문에 오탐률이 낮다: 오용탐지

12. 다음 중 가상 사설망(VPN)에 대한 설명으로 가장 옳지 않은 것은?
① 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 별도의 전용선을 사용하는 사설망에 비해 구축비용이 저렴하다.
② 사용자들 간의 안전한 통신을 위하여 기밀성, 무결성, 사용자인증의 보안 기능을 제공한다.
③ 네크워크 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: SSH와 같은 OSI 모델 7계층의 보안 프로토콜로 구현해야 한다.
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 사용하여 VPN을 구성하면 기밀성, 무결성, 인증 등을 제공할 수 있다.
④ 회사 시스템: VPN은 다음과 같이 회사 시스템에 사용될 수 있다.

13. 다음 중 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec에 대한 설명으로 가장 옳지 않은 것은?
① DES-CBC, RC5, Blowfish 등을 이용한 메시지 암호화를 지원한다.
② 방화벽이나 게이트웨이 등에 구현한다.
③ IP 기반의 네트워크에서만 동작한다.
④ 암호화/인증방식이 지정되어 있어 신규 알고리즘 적용이 불가능하다.
정답 체크
④ IKE(Internet Key Exchange)를 통해 신규 알고리즘을 적용할 수 있다.
오답 체크
① 메시지 암호화에 DES-CBC, 3DES, CAST-128, IDEA, RC5, Blowfish 등을 사용할 수 있다.
② 방화벽, 게이트웨이, 라우터 등에 구현할 수 있다.
③ IP 기반의 네트워크에서만 동작하기 때문에 IPSec(IP Security)이다.

14. 다음 〈보기〉에서 설명하는 보안 시스템은?

〈 보기 〉 ○ 패킷을 버리거나 또는 의심이 가는 트래픽을 감지함으로써, 공격 트래픽을 방어하는 기능을 가지고 있다. ○ 모든 트래픽을 수신하는 스위치의 포트를 모니터 하고, 특정 트래픽을 막기 위하여 적합한 명령어를 라우터(Router)나 침입차단시스템(Firewall)에 전송할 수 있다. ○ 호스트(Host) 기반의 이 보안 시스템은 공격을 감지하기 위하여 서명이나 비정상 감지기술을 사용한다.

① IDS ② IPS ③ DNS ④ VPN
정답 체크
(2) 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
(1) passive(수동적) 보안 장비로, 네트워크상의 패킷을 7계층(payload or content) 레벨에서 분석하여 침입을 탐지한다.
(3) 도메인 이름과 IP 주소 간 변환 서비스를 제공한다.
(4) 인터넷망(public network)을 전용선(private network)처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 서비스로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용한다.

15. 다음 중 네트워크 기반 공격기법에 대한 설명으로 가장 옳지 않은 것은?

① SYN Flooding 공격은 TCP 연결설정 과정의 취약점을 악용한 서비스 거부 공격이다.
② Zero Day 공격은 시그니처(Signature) 기반의 침입탐지시스템으로 방어하는 것이 일반적이다.
③ APT 공격은 공격대상을 지정하여 시스템의 특성을 파악한 후 지속적으로 공격한다.
④ Buffer Overflow 공격은 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.
정답 체크
② Zero Day: 프로그램에 문제가 알려지고 난 후 보안패치가 나올 때까지 시간차를 이용해 공격하는 기법을 말한다. 알려지지 않은 공격이므로 보안 장비로 막을 수 없으나 IDS를 이용하고자 한다면 시그너처 기반의 오용 탐지가 아니라 이상 탐지로 방어를 해야 한다.
오답 체크
① SYN Flooding: 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고(메모리를 할당한 상태), 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다(더 이상 SYN을 위한 메모리가 없음).
③ APT: 특정 기업 또는 기관의 핵심 정보통신 설비에 대한 중단 또는 핵심정보의 획득을 목적으로 공격자는 장기간 동안 공격 대상에 대해 IT인프라, 업무환경, 임직원 정보 등 다양한 정보를 수집하고, 이를 바탕으로 제로 데이 공격, 사회공학적 기법 등을 이용하여 공격 대상이 보유한 취약점을 수집·악용해 공격을 실행하는 것을 말한다.
④ Buffer Overflow: 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다.

16. 다음 〈보기〉는 보안 공격 유형을 나열한 것이다. 소극적 공격을 모두 고른 것은?

〈 보기 〉
㉠ 신분위장 (Masquerade) ㉡ 재전송(Replay)
㉢ 패킷 분석(Analysis of Packet)
㉣ 메시지 수정(Modification of Message) ㉤ 스니핑 (Sniffing)
㉥ 서비스 거부(Denial of Service)

① ㉠, ㉢, ㉤
② ㉠, ㉣
③ ㉢, ㉤
④ ㉢, ㉣, ㉥
정답 체크
(3) 패킷 분석과 스니핑은 기밀성 공격이다.
오답 체크
(1), (2), (4) 신분위장, 재전송, 메시지 수정은 무결성 공격이다.
서비스 거부는 가용성 공격이다.

17. 다음 중 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보로 가장 옳은 것은?
① 수신 시스템이 처리할 수 있는 윈도우 크기
② 패킷을 송신하고 수신하는 프로세스의 포트 번호

③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호
④ 송신 시스템의 TCP 패킷의 생성 시간
정답 체크
④ 생성 시간: 패킷의 헤더에는 통신을 위해 필요한 필수 정보가 들어가야 한다. 보기의 TCP 패킷의 생성 시간은 어디에도 사용할 수 없는 의미 없는 정보이다.
오답 체크
①, ②, ③ TCP 패킷의 헤더는 다음과 같다.

필드	크기(비트)	설명
송신측의 포트 번호	16	데이터를 보내는 애플리케이션의 포트 번호
수신측의 포트 번호	16	데이터를 받을 애플리케이션의 포트 번호
순서번호	32	송신하는 데이터의 일련번호로 선두 위치를 나타냄
인정(ACK) 번호	32	수신된 데이터의 순서 번호에 수신된 데이터 크기를 더한 값
데이터 오프셋	4	데이터가 시작되는 위치
예약 필드	6	사용하지 않음
제어 비트	6	SYN, ACK, FIN 등의 제어 번호
윈도위 크기	16	수신측에서 수신할 수 있는 데이터의 크기
체크섬	16	데이터 오류 검사에 필요한 정보
긴급 위치	16	긴급하게 처리할 데이터의 위치
옵션	가변길이	기타 정보를 위한 부분

18. 다음 중 ACL 적용 규칙에 해당하지 않는 것으로 가장 옳은 것은?
① Named ACL은 순서대로 입력되므로 중간에 삽입이나 삭제가 불가능하다.
② ACL의 마지막에는 deny any가 생략되어 있다.
③ ACL은 먼저 입력한 순서대로 수행된다.
④ Numbered ACL은 순서대로 입력되므로 중간에 삽입이나 삭제가 불가능하다.
정답 체크
(1) 임의로 입력되므로 중간에 삽입이나 삭제가 가능하다.
오답 체크
(2) 조건에 맞지 않는 패킷들은 모두 deny되어야 한다.
(3) ACL은 순서를 가지고, 해당 순서대로 실행된다.
(4) 순서대로 입력되어 중간에 삽입이나 삭제가 불가능하다.

19. 다음 〈보기〉의 VPN에 대한 설명 중 가장 옳은 것을 모두 고른 것은?

〈 보기 〉
㉠ 터널링 기술은 VPN의 기본이 되는 기술로서 터미널이 형성되는 양 호스트 사이에 전송되는 패킷을 추가 헤더 값으로 캡슐화하는 기술이다.
㉡ 데이터 암호화 기술은 터널이 형성된 한 쪽 호스트에서 데이터를 암호화해서 보내면 반대편 호스트에서 암호화 데이터를 복호화하여 원본 데이터를 확인하게 된다.
㉢ VPN은 데이터의 출처 즉, 출발지 IP가 확실 한지에 대한 인증기술을 제공하고, 내부 자원에

대해서 허가 받지 않은 사용자의 접속을 차단하는 접근제어 기능을 제공한다.
㉣ VPN 구현에 가장 널리 사용되는 터널링 프로토콜에는 PPP, SSL, SSH 등이 있다.

① ㉠
② ㉠, ㉡
③ ㉠, ㉡, ㉢
④ ㉠, ㉡, ㉢, ㉣

정답 체크
(3) ㄱ : 터널링 기술을 이용한다.
ㄴ : IPSec, SSL/TLS, SSH 등을 이용한다.
ㄷ : 인증, 무결성, 기밀성, 재전송 방지, 접근제어 등의 기능을 제공한다.
오답 체크
(4) ㄹ : PPP가 아닌 PPTP이다.

20. 다음 중 무선랜 구축 시 보안을 위한 고려사항으로 가장 옳지 않은 것은?
① SSID(Service Set IDentifier)를 숨김 모드로 사용
② 무선 단말기의 MAC(Media Access Control)주소 인증 수행
③ 관리자용 초기 ID/Password 변경
④ 보안성이 우수한 WEP(Wired Equivalent Privacy) 사용

정답 체크
(4) WEP(보안이 약함)가 아닌 WPA2(WPA3)를 사용해야 한다.
오답 체크
(1) 공개된 SSID를 통해 접근할 수 없도록 한다.
(2) MAC filtering 기술을 이용한다(WPA, WPA2에서 사용).
(3) 초기 ID/PW를 변경하고, 주기적으로 PW를 변경한다.