

	㉠	㉡
①	웜	애드웨어
②	트로이 목마	애드웨어
③	애드웨어	바이러스
④	바이러스	트로이 목마
⑤	웜	트로이 목마

정답 체크

(1) 웜 : 인터넷 또는 네트워크를 통해서 컴퓨터에서 컴퓨터로 전파되는 악성 프로그램이다.

애드웨어 : 특정 소프트웨어를 실행할 때 또는 설치 후 자동적으로 광고가 표시되는 프로그램을 말한다.

오답 체크

(2), (3), (4), (5) 트로이 목마 : 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 형태이다.

바이러스 : 사용자 컴퓨터(네트워크로 공유된 컴퓨터 포함) 내에서 사용자 몰래 프로그램이나 실행 가능한 부분을 변형해 자신 또는 자신의 변형을 복사하는 프로그램이다.

4. 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

- ① Adaptive Chosen-plaintext Attack은 Ciphertext-only Attack보다 공격자 입장에서 더 높은 자유도를 갖는다.
- ② Differential Cryptanalysis는 평문과 암호문 간의 차분 정보를 사용하는 암호 공격 기법이다.
- ③ Side-channel Attack은 소비 전력이나 실행 시간 등 암호의 구현상 특성을 활용하는 공격 기법이다.
- ④ Birthday Attack은 공개키 암호 알고리즘의 암호 안전도를 측정하는 데 사용된다.
- ⑤ 해시함수는 Collision Resistance를 가져야 한다.

정답 체크

(4) 해시 알고리즘의 안전도를 측정하는데 사용된다.

오답 체크

(1) 공격자는 이전의 암호화 결과를 보고 다음 평문을 선택할 수 있다.

(2) 평문의 일부를 변경할 때 암호문이 어떻게 변화하는지 관찰하여 조사한다.

(3) 알고리즘의 약점을 찾거나(암호 해독과는 다름) 무차별 공격을 하는 대신에 암호 체계의 물리적인 구현 과정의 정보를 기반으로 하는 공격 방법이다. 예를 들어, 소요 시간 정보, 소비 전력, 방출하는 전자기파, 심지어는 소리를 통해서 시스템 파괴를 위해 악용할 수 있는 추가 정보를 얻을 수 있다.

(5) 약한 충돌 내성과 강한 충돌 내성을 가져야 한다.

5. 양자내성암호(Post-Quantum Cryptography)에 대한 설명으로 옳지 않은 것은?

- ① 양자컴퓨터의 실현 가능성이 높아짐에 따라 기존 대칭키 암호를 대체하는 목적으로 만들어지고 있다.
- ② RSA는 양자내성암호로 볼 수 없다.
- ③ 양자내성암호의 종류로는 격자 기반 암호, 코드 기반 암호, 해시기반 암호 등이 있다.
- ④ 양자내성암호는 알고리즘의 종류에 따라 키 교환 목적, 전자서명 목적으로 사용된다.
- ⑤ 양자내성암호는 NIST에 의해 표준화가 진행되고 있다.

정답 체크

(1) 기존의 공개키 암호가 가지고 있던 문제를 해결하고 대체할 수 있는 암호이다.

오답 체크

(2) RSA는 기존의 공개키 암호이다.

- (3) 다변수 기반, 코드 기반, 격자 기반, 아이소제니, 해시 기반 암호 등이 있다.
- (4) 암호화, 키교환 및 전자서명 목적으로 사용된다.
- (5) 미 NSA(National Security Agency)는 2015.8월 양자내성암호의 필요성을 밝히고 2016년부터 NIST를 통해 양자내성 알고리즘 표준공모전을 진행중이다.

6. 다음에서 설명하는 DoS 공격 유형은?

패킷을 전송할 때 출발지 IP주소와 목적지 IP주소의 값을 똑같이 만들어서 공격대 상에게 보낸다. 이때 조작된 목적지 IP주소는 공격대상의 IP주소이다. 이렇게 목적지 주소가 조작된 패킷을 공격대상에게 보내면 시스템은 공격자가 보낸 SYN패킷의 출발지 주소를 참조하여 응답패킷을 보내는데, 이때 패킷이 네트워크 밖으로 나가지 않고 자신에게 다시 되돌아오며, 돌아온 패킷의 출발지 IP주소에는 또다시 자신의 IP주소가 기록되어 시스템을 마비시키는 공격의 종류이다.

- ① Ping of Death
- ② Land Attack
- ③ SYN Flooding Attack
- ④ Smurf Attack
- ⑤ Mail Bomb

정답 체크

(2) 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어서 공격 대상에게 보내는 공격이다.

오답 체크

(1) 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).

(3) 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.

(4) 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부(DDoS) 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.

(5) 흔히 폭탄 메일이라고 하고 스팸 메일도 여기에 해당한다. 메일 서버는 각 사용자에게 일정한 양의 디스크 공간을 할당하는데, 메일이 폭주하여 디스크 공간을 가득 채우면 정작 받아야 하는 메일을 받을 수 없다. 즉 스팸 메일도 서비스 거부 공격이 될 수 있다. DoS 공격이지 스니핑(sniffing)과는 무관하다.

7. OSI 7 Layer 중 계층별 프로토콜의 연결이 옳지 않은 것은?

	OSI 모델	프로토콜
①	응용계층	HTTP, FTP
②	표현계층	MPEG, Telnet
③	전송계층	TCP, UDP
④	네트워크계층	IP, ICMP
⑤	데이터링크계층	Ethernet

정답 체크

(2) MPEG은 표현 계층이지만, Telnet은 응용계층이다.

오답 체크

(1) HTTP, SMTP, SNMP, FTP 등이 존재한다.

(3) TCP, UDP, RTP, RSVP 등이 존재한다.

(4) IP, ICMP, IGMP 등이 존재한다.

(5) Ethernet, HDLC, PPP 등이 존재한다.

8. IP주소에 대한 설명으로 옳지 않은 것은?

① IP주소는 TCP/IP 프로토콜로 접속된 네트워크에서 각 컴퓨터를 식별하는 데 사용하는 숫자이다.

② InterNIC에서 관리하는 IP주소는 네트워크와 호스트(노드)로 구성되어 있다.

③ IPv6는 IP주소 공간의 부족, 12개 필드로 구성된 IPv4 헤더 영역의 비효율적인 사용, 네트워크 프래그멘테이션 증가로 인한 스위칭의 비효율성 문제를 해결하기 위해 개발되었다.

④ IPv4 주소는 상위 4비트 값을 기초로 다섯 개의 클래스로 분류된다.

⑤ 클래스 D는 멀티캐스트용 주소이다.

정답 체크

(3) IPv4는 13개의 필드로 구성된다.

오답 체크

(1) IPv4와 IPv6가 존재한다.

(2) 네트워크는 대표 주소를 의미하고, 호스트를 개별 주소를 의미한다.

(4) A(0), B(10), C(110), D(1110), E(1111) 클래스로 구분된다.

(5) 네트워크 주소가 1110으로 시작하고 멀티캐스트용으로 사용된다.

9. RSA 암호 시스템에서 오일러 Totient 함수는 $\varphi(n) = \{n\text{보다 작은 양의 정수 중에서 } n\text{과 서로소인 양의 정수의 개수}\}$ 로 정의할 수 있다. p 와 q 가 각각 서로 다른 소수(Prime Number)라고 가정할 때, 옳지 않은 것은?

① $\varphi(p) = p - 1$

② $\varphi(p \cdot q) = \varphi(p)\varphi(q)$

③ $a^{\varphi(2 \cdot p)} \not\equiv a^{\varphi(p)} \pmod{p}$: 만일 p 가 2보다 큰 소수이고, a 는 p 에 의하여 나누어지지 않는 양의 정수일 때

④ $a^{\varphi(n)} \equiv 1 \pmod{n}$: 서로소인 a 와 n 에 대하여

⑤ $\varphi(35) = 24$

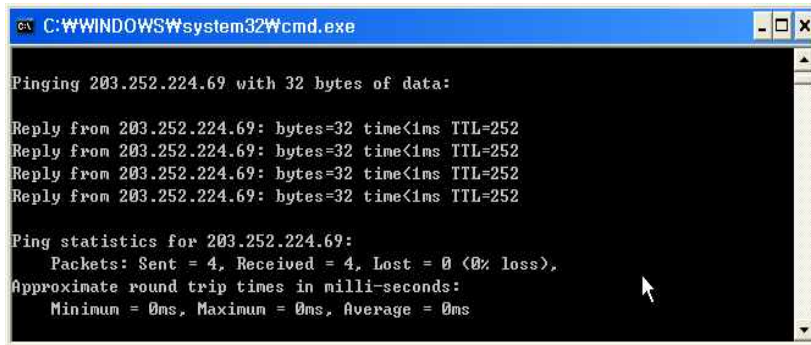
정답 체크

(3) 실제로 값을 대입하면 합동식이 성립함을 알 수 있다($p = 3, a = 2$). $2^{\varphi(2 \cdot 3)} \not\equiv 2^{\varphi(3)} \pmod{3} \rightarrow 2^2 \not\equiv 2^1 \pmod{3}$

오답 체크

- (1) $\varnothing (p^k) = p^{k-1}(p-1)$ 에 기반한다.
- (2) 곱셈적 함수이다.
- (4) 오일러의 정리라고 한다.
- (5) 서로소가 아닌 5, 7, 10, 14, 15, 20, 21, 25, 28, 30을 제외한다.

10. 다음은 ping 명령을 실행한 것이다. TTL이 의미하는 것은?



```
C:\WINDOWS\system32\cmd.exe

Pinging 203.252.224.69 with 32 bytes of data:

Reply from 203.252.224.69: bytes=32 time<1ms TTL=252
Reply from 203.252.224.69: bytes=32 time<1ms TTL=252
Reply from 203.252.224.69: bytes=32 time<1ms TTL=252
Reply from 203.252.224.69: bytes=32 time<1ms TTL=252

Ping statistics for 203.252.224.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- ① 해당 IP주소 서브넷의 대표 주소이다.
- ② 전송 속도를 보여주며, 단위는 ms이다.
- ③ 전송된 패킷의 바이트 크기이다.
- ④ 해당 패킷의 생명주기이다.
- ⑤ 발신 패킷과 수신 패킷 간의 손실률을 보여준다.

정답 체크

- (4) TTL은 라우터 등을 통과할 때마다 1씩 감소한다.

오답 체크

- (1) 203.252.224.69를 의미한다.
- (2) time을 의미한다.
- (3) bytes를 의미한다.
- (5) Lost를 의미한다.

11. 「개인정보보호법」상 민감정보에 해당하지 않는 것은?

- ① 건강 및 성생활에 관한 정보
- ② 사상, 신념 및 정치적 견해
- ③ 유전정보
- ④ 인종, 민족에 관한 정보
- ⑤ 사번, 학번, 법인등록번호, 사업자등록번호에 관한 정보

정답 체크

(5) 개인정보 보호법 제23조(민감정보의 처리 제한) 상 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다.

12. 다음과 관련된 디지털 포렌식의 기본 원칙은?

- 적절한 절차를 따르지 않고 수집한 증거는 위법수집 증거에 해당되기 때문에 이를 사용할 수 없다.
- 독수독과이론(Fruit of the Poisonous Tree) 또는 독과수이론

- ① 기밀성의 원칙
- ② 무결성의 원칙
- ③ 정당성의 원칙
- ④ 가용성의 원칙
- ⑤ 연계보관성의 원칙

정답 체크

(3) 모든 증거는 적절한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.

오답 체크

- (1) 해당 원칙은 존재하지 않는다.
- (2) 수집된 정보는 연계 보관성을 만족시켜야 하고, 각 단계를 거치는 과정에서 위조 및 변조되어서는 안 되며, 이러한 사항을 매번 확인해야 함을 의미한다.
- (4) 해당 원칙은 존재하지 않는다.
- (5) 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.

13. SSL Record 프로토콜의 처리 순서가 올바른 것은?

- ① 압축 → 단편화 → 암호화 → MAC → 전송
- ② 압축 → 단편화 → MAC → 암호화 → 전송
- ③ MAC → 암호화 → 압축 → 단편화 → 전송
- ④ 암호화 → MAC → 단편화 → 압축 → 전송
- ⑤ 단편화 → 압축 → MAC → 암호화 → 전송

정답 체크

(5) 메시지가 여러 개의 짧은 단편(fragment)으로 분할되고, 단편 단위로 압축된다. 압축에 사용하는 알고리즘은 상대와 합의한 것을 이용하고, 압축한 단편에 메시지 인증 코드(MAC)를 부가한다. 압축한 단편과 메시지 인증 코드를 합치고 그것을 대칭 암호로 암호화를 수행하고, 암호화에는 CBC 모드를 이용한다. 이후에 전송을 수행한다.

14. 인터넷 환경에서 많이 사용 중인 보안 프로토콜에 대한 설명으로 옳지 않은 것은?

- ① ISAKMP 프로토콜은 IPsec에서 보안 연관을 생성하기 위해 사용된다.
- ② IPsec은 IPv4와 IPv6에서 사용할 수 있는 보안 프로토콜이므로 상위계층 보안이 필요한 VPN을 제공하지 못한다.
- ③ IPsec에서 제공하는 Transport 모드는 두 엔드포인트 장치 간에 Point-to-point 연결을 제공한다.
- ④ IPsec은 데이터 보호를 위해 AH와 ESP 보안 프로토콜을 제공한다.
- ⑤ IPsec은 상호간 안전한 키 분배를 위해 Diffie-Hellman 키 분배 프로토콜을 사용할 수 있다.

정답 체크

(2) IPsec은 VPN에서 암호화를 위해 사용된다.

오답 체크

(1) IKE(Internet Key Exchange)는 SA(AH와 ESP를 위한 파라미터 제공)를 협상하고 ISAKMP(인증, 키 교환)를 제공한다.

(3) Transport 모드는 호스트 대 호스트 간에 주로 사용하고, Tunnel 모드는 두 라우터 간에, 호스트와 라우터 간에 또는 두 게이트웨이 간에 주로 사용한다.

(4) AH는 인증, 무결성을 제공하고, ESP는 인증, 무결성, 기밀성을 제공한다.

(5) Diffie-Hellman은 IPsec에서 사용된다.

15. Kerberos 보안 프로토콜에 대한 설명으로 옳지 않은 것은?

① 발급 받은 TGT(Ticket Granting Ticket)는 일회성으로 재사용이 불가능하다.

② Kerberos의 정상적인 동작을 위해서는 관련된 호스트의 시간 동기화가 필요하다.

③ Kerberos는 SSO(Single Sign On)와 상호 인증 기능을 제공한다.

④ Kerberos에 참여하는 인증서버는 클라이언트에 TGT(Ticket Granting Ticket)를 발급한다.

⑤ Kerberos는 대칭키 암호 기반의 인증 프로토콜로 신뢰할 수 있는 제3자를 필요로 한다.

정답 체크

(1) TGT는 로그인 시 한번 발생되며, 유효 기간 내 재사용이 가능하다.

오답 체크

(2) 타임 스탬프 등이 전송되므로 시간 동기화가 필요하다.

(3) SSO에는 Kerberos와 Active Directory가 사용된다.

(4) AS는 TGT를 발급하고, TGS는 Ticket를 발급한다.

(5) 제3자로서 AS와 TGS를 사용한다.

16. <보기>에 해당하는 계층별 보안 프로토콜과 세부 프로토콜은?

〈 보 기 〉

이 프로토콜의 각 메시지는 2바이트로 되어 있으며, 첫 바이트는 발생한 메시지 오류의 심각성을 알려주기 위해 경고(warning) 또는 치명적(fatal) 값을 가진다. 만약 레벨이 치명적이라면, 계층 보안 프로토콜은 즉시 연결을 종결시킨다. 동일 세션상의 다른 연결들은 지속될 수 있지만, 이 세션에서 새로운 연결이 만들어질 수는 없다. 두 번째 바이트에는 구체적인 경보를 나타내는 코드가 들어있다.

① IPsec에서의 경고 프로토콜(Alert Protocol)

② SSL에서의 경고 프로토콜(Alert Protocol)

③ SSH에서의 경고 프로토콜(Alert Protocol)

④ S/MIME에서의 경고 프로토콜(Alert Protocol)

⑤ SSH에서의 연결 프로토콜(Connection Protocol)

정답 체크

(2) SSL에서 뭔가 에러가 발생했다는 것을 통신 상대방에게 전달한다.

오답 체크

(1), (3), (4) 해당 프로토콜에서 경보는 존재하지 않는다.

(5) 연결 관련 프로토콜이 존재하나 경보와는 무관하다.

17. 다음 네트워크 기반과 호스트 기반 IDS(침입탐지시스템)의 특징 중 옳지 않은 것만을 모두 고르면?

〈네트워크 기반(Network-based)〉

- ㄱ. 전체 네트워크에 대한 침입탐지가 가능하다.
- ㄴ. 탐지된 침입의 실제 공격 성공 여부를 네트워크단에서는 알지 못한다.
- ㄷ. 기존 네트워크 환경을 크게 변경하여야만 설치가 가능하다.

〈호스트 기반(Host-based)〉

- ㄹ. 네트워크 기반 IDS가 탐지 불가능한 로컬 시스템에 대한 공격을 탐지할 수 있다.
- ㅁ. 모든 개별 호스트에 대한 설치 및 관리를 하기 때문에 네트워크 기반 IDS 보다 설치 및 관리가 쉽다.
- ㅂ. 고부하·스위치 네트워크에서도 적용이 가능하며, 우회 가능성이 거의 없다.

- ① ㄱ, ㄹ
- ② ㄴ, ㅁ
- ③ ㄴ, ㅂ
- ④ ㄷ, ㅁ
- ⑤ ㄷ, ㅂ

정답 체크

(4) ㄷ : 기존 네트워크 환경을 크게 변경하지 않고 설치가 가능하다.

ㅁ : 네트워크 기반 IDS 보다 설치 및 관리가 어렵다.

오답 체크

(1), (2), (3), (5) ㄱ : 네트워크 중간에 설치되므로 전체 네트워크에 대한 탐지가 가능하다.

ㄴ : 실제 공격 성공 여부는 호스트 단에서 알 수 있다.

ㄹ : 로컬 시스템(호스트)에 대한 공격을 탐지할 수 있다.

ㅂ : 호스트에 설치하므로 고부하/스위치 네트워크에서도 적용이 가능하고, 우회 가능성이 거의 없다.

18. 재해복구시스템의 복구 수준별 유형을 비교한 설명으로 옳지 않은 것은?

- ① Mirror Site는 주센터와 동일한 수준의 정보 기술 자원을 원격지에 구축하고 Active-Active 상태로 운영한다.
- ② Hot Site는 주센터와 동일한 수준의 정보 기술 자원을 원격지에 구축하여 대기(Standby) 상태로 유지한다.
- ③ Warm Site는 중요성이 높은 정보기술 자원만 부분적으로 재해복구센터에 보유한다.
- ④ Cold Site는 데이터만 원격지에 보관하고 이의 서비스를 위한 정보자원을 확보하지 않거나 장소 등 최소한으로만 확보한다.
- ⑤ 재해발생시 RTO(Recovery Time Objective)가 빠른 것은 Hot Site → Mirror Site → Warm Site → Cold Site 순서이다.

정답 체크

(5) 목표 복구 시간(얼마나 빨리 복구할 수 있는가?)이 빠른 것은 Mirror Site → Hot Site → Warm Site → Cold Site 순이다.

오답 체크

- (1) Mirror Site는 주센터와 동일 환경이므로 Active-Active 상태로 운영한다.
- (2) Hot Site는 주센터와 동일 환경에서 인원이 없으므로 Standby 상태로 운영한다.
- (3) Warm Site는 주센터와 동일 환경에서 소프트웨어와 인원이 없다.
- (4) Cold Site는 장소와 HVAC(Heating, Ventilation, Air Conditioning)만 존재한다.

19. 악성코드에 대한 설명으로 옳지 않은 것은?

- ① Backdoor는 비인가된 접근을 허용하는 것으로 공격자가 사용자 인증 과정 등의 정상 절차를 거치지 않고 프로그램이나 시스템에 접근하도록 지원한다.
- ② Rootkit은 보안 관리자나 보안 시스템의 탐지를 피하면서 시스템을 제어하기 위해 공격자가 설치하는 악성파일이다.
- ③ Ransomware는 사용자의 파일을 암호화하여 사용자가 실행하거나 읽을 수 없도록 한 뒤 자료복구 대가로 돈을 요구한다.
- ④ Launcher는 Downloader나 Dropper 등으로 생성된 파일을 실행하는 기능을 가지고 있다.
- ⑤ Exploit은 악성코드에 감염되지 않았는데도 악성코드를 탐지했다고 겁을 주어 자사의 안티바이러스 제품으로 제거해야 한다는 식으로 구매를 유도한다.

정답 체크

- (5) 해당 설명은 Scareware이고, Exploit는 컴퓨터 소프트웨어와 하드웨어의 버그나 취약점 등을 이용하여 공격자가 원하는 악의적 동작을 하도록 하는 공격 방법이다.

오답 체크

- (1) 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 토큰이다.
- (2) 트로이목마 설치, 원격 접근, 내부 사용 흔적 삭제, 관리자 권한 획득 등 주로 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램의 모음이다.
- (3) 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.
- (4) 추가적인 악성 행위를 하기 위해서 새로운 파일을 실행하기 위한 기능을 수행한다.

20. NAT(Network Address Translation)에 대한 설명으로 옳지 않은 것은?

- ① 사용자에게 투명성을 제공함으로써 처리 속도가 빠르다.
- ② 한정된 공인 IP주소 부족 문제의 해결이 가능하다.
- ③ 주소 변환 기능을 제공한다.
- ④ 외부 컴퓨터에서 사설 IP를 사용하는 호스트에 대한 접근이 어려워 보안 측면에서 장점을 제공한다.
- ⑤ 외부 컴퓨터에 네트워크 구조를 노출하지 않는 보안상의 이점을 제공한다.

정답 체크

- (1) 주소 변환이 수행되므로 투명성을 제공하지 않고, 빠른 속도를 제공하지 않는다.

오답 체크

- (2) 사설 IP주소를 사용한다.
- (3) 사설 IP와 공인 IP 간의 주소 변환을 제공한다.
- (4) 일반적으로 외부 컴퓨터에서 내부 컴퓨터로 접근하기 어렵다.
- (5) 내부 컴퓨터의 사설 IP는 외부로 노출되지 않는다.