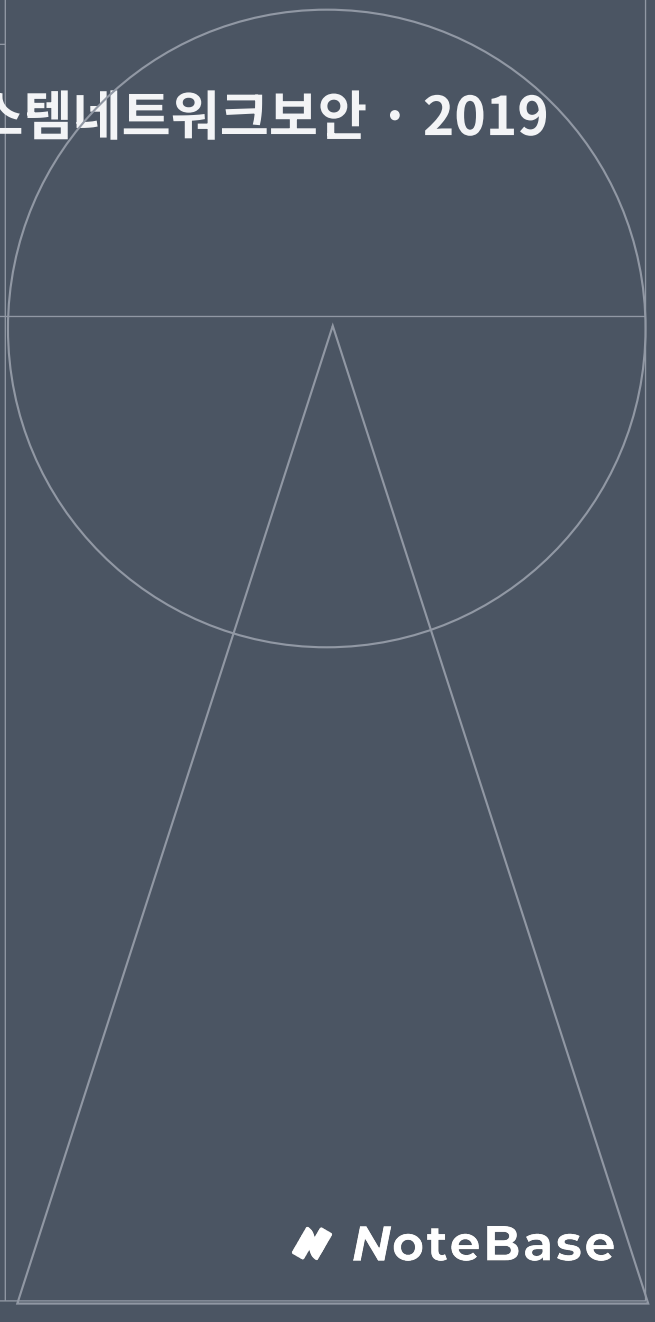
기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2019



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2019

공무원/경찰/경력채용 · 시스템네트워크보안 · 2019

문 1. 보안에 취약한 인터넷 응용 프로토콜/프로그램과 보안이 강화된 프로토콜/프로그램을 짝지은 것으로 가장 적절하지 않은 것은?

① TELNET — SSH

② SMTP — PGP

③ HTTP — HTTPS

④ FTP — TFTP

정답 4번

간단한 해설

TFTP는 단순한 파일 전송 프로토콜로, **FTP에 인증·암호화를 추가한 보안 강화판이 아니다**. SSH 기반 SFTP나 TLS를 적용한 FTPS와 구별해야 한다.

선지별 해설

① O: 기본 TELNET은 원격 접속 과정의 계정 정보와 통신 내용을 암호화하지 않아 도청에 취약하다. SSH는 원격 접속에 **암호화·인증·무결성 보호**를 제공하므로 보안이 강화된 대안으로 연결된다.

② O: 기본 SMTP는 메일 전송 절차를 제공하지만 그 자체로 메일 본문의 종단 간 암호화와 전자서명을 제공하지 않는다. PGP는 메일 내용을 암호화하고 전자서명으로 발신자 및 내용의 무결성을 확인할 수 있게 한다. 따라서 **메일 내용의 보안을 보완하는 프로그램**이라는 연결은 적절하다. PGP가 SMTP를 대체하는 전송 프로토콜이라는 뜻은 아니다.

③ O: 기본 HTTP의 통신은 평문으로 전달된다. HTTPS는 **HTTP 통신에 TLS 보호**를 적용하여 전송 내용의 기밀성·무결성과 서버 인증을 제공하므로 적절한 연결이다.

④ X: TFTP는 간단한 파일 전송을 위한 프로토콜이며 **FTP의 보안 강화판이 아니다**. 기본 TFTP에는 로그인·접근통제 및 암호화 기능이 없다. 보안 파일 전송에는 SSH 기반 SFTP나 TLS를 사용하는 FTPS 등을 구별하여 사용한다.

NoteBase

문 2. 대표적인 스마트폰 운영체제는 iOS와 Android이다. iOS가 Android에 비해 상대적으로 안전하다고 알려져 있다. <보기> 중 그 이유로 적절한 것을 모두 고른 것은?

<보기>
㉠ iOS는 샌드박스(sandbox)를 활용하나 Android는 그렇지 않다.
㉡ 애플은 자신의 CA(Certification Authority)를 통해 응용 프로그램을 서명하여 배포한다.
㉢ iOS는 커널 무결성 확인 후, 이상이 없으면 정상 부팅된다.
㉣ iOS는 리눅스 커널을 기반으로 만들어진 운영체제이다.

① ㉠㉡
② ㉡㉢
③ ㉡㉣
④ ㉠㉣

정답 2번

간단한 해설

Apple의 인증서에 기반한 **앱 코드 서명**과 부팅 단계의 **커널 무결성 검증**이 iOS의 보안 장치이다. Android도 샌드박스를 사용하며, iOS의 커널은 리눅스가 아니다.

보기별 해설

㉠ X: 샌드박스는 앱이 다른 앱의 데이터나 시스템 자원에 함부로 접근하지 못하도록 실행 범위를 제한하는 격리 장치이다. **Android도 앱별 사용자 식별자와 프로세스 등을 이용한 샌드박스**를 제공하므로 iOS만 활용한다는 설명은 성립하지 않는다.

㉡ O: iOS 앱은 **Apple이 발급한 인증서를 이용한 코드 서명** 체계의 통제를 받는다. 개발자의 신원과 코드 서명을 확인하여 승인된 출처의 앱인지, 배포된 코드가 변조되지 않았는지 검사한다. 이 보기는 Apple의 인증기관을 신뢰의 기반으로 하는 앱 서명·배포 체계를 뜻한다.

㉢ O: iOS는 부팅 단계마다 다음 단계의 서명을 검증하는 신뢰 사슬을 사용한다. 부트로더가 **커널의 서명과 무결성을 확인한 후 실행**하므로 변조된 운영체제 코드가 정상 부팅 과정에 끼어드는 것을 막는 데 기여한다.

㉣ X: iOS는 리눅스 커널이 아니라 **Mach와 BSD 구성 요소를 결합한 XNU 커널**을 사용한다. 리눅스 커널을 기반으로 하는 스마트폰 운영체제는 Android이다.

따라서 제시된 보기에서 적절한 설명은 ㉡과 ㉢이며, 이를 묶은 ②에 해당한다.

NoteBase

문 3. 패스워드에 관한 설명 중 가장 적절하지 않은 것은?

① 사용자에게 부여된 권한(authorization)을 결정한다.

② 보안 강화를 위해 주기적인 패스워드 변경이 권장된다.

③ 패스워드 보안을 위해 패스워드와 솔트(salt)를 결합한 후, 그 해시 값을 저장하는 방법이 일반적으로 사용된다.

④ 사용자는 공격자의 패스워드 추측을 어렵게 하기 위해 컴퓨터 생성 패스워드를 이용할 수 있다.

정답 1번

간단한 해설

패스워드는 본인임을 확인하는 **인증** 수단이다. 어떤 자원에 접근하거나 어떤 작업을 할 수 있는지 정하는 **인가**와는 다르다.

선지별 해설

① X: 패스워드는 제시한 사용자가 본인인지 확인하는 **인증(authentication)** 수단이다. 인증된 사용자에게 어떤 자원과 작업을 허용할지 결정하는 것은 **인가(authorization)**이며, 계정·역할·접근통제 정책 등에 따라 정해진다.

② O: 이 문항은 주기적인 변경으로 동일 패스워드가 장기간 사용되는 것을 줄이려는 **전통적인 관리정책의 관점**을 전제로 한다. 국내 보안관리 안내에서도 이러한 변경 정책을 권고해 왔다. 다만 무조건 자주 바꾸면 항상 안전하다는 뜻은 아니다. 현재 NIST 지침은 정기 변경을 일률적으로 강제하지 않고 유출 증거가 있으면 변경하도록 하므로, 시험의 관점과 모든 환경에 적용되는 보안 원칙을 구분한다.

③ O: 패스워드마다 다른 솔트를 함께 사용하여 해시하면 **같은 패스워드도 서로 다른 저장값**을 갖게 할 수 있고, 미리 계산한 해시 목록의 재사용을 어렵게 한다. 솔트와 해시를 저장하고 로그인 시 같은 방식으로 계산해 비교하며, 안전한 패스워드 전용 해시 방식과 적절한 계산 비용을 사용한다.

④ O: 사람이 이름·생일·사전 단어 등을 바탕으로 고른 패스워드는 추측되기 쉽다. 컴퓨터가 **충분한 길이로 예측하기 어렵게 무작위 생성**한 패스워드를 이용하면 이러한 예측 가능성을 낮출 수 있다. 컴퓨터로 만들었다는 사실만으로 약한 생성 방식까지 안전해지는 것은 아니다.

NoteBase

문 4. ARP(Address Resolution Protocol)에 관한 설명 중 가장 적절한 것은?

① ARP는 MAC 주소에 대응되는 IP 주소를 구할 때 사용되는 프로토콜이다.

② ARP 요청 메시지와 ARP 응답 메시지는 LAN 상으로 브로드캐스트 된다.

③ 호스트의 ARP 테이블을 정적(static)으로 유지하면 ARP 스푸핑 공격을 막을 수 있다.

④ ARP 패킷은 IP 데이터그램의 페이로드(payload)로 전달된다.

정답 3번

간단한 해설

신뢰할 수 있는 IP–MAC 대응을 **정적 ARP 항목으로 고정**하면 거짓 ARP 응답에 의해 그 대응 정보가 바뀌는 것을 막을 수 있다. ARP 스푸핑의 핵심인 캐시 오염을 방지하는 방법이다.

선지별 해설

① X: ARP는 같은 링크에서 통신할 상대의 **IP 주소에 대응하는 MAC 주소**를 알아내는 프로토콜이다. MAC 주소를 바탕으로 IP 주소를 구하는 방향은 RARP의 설명이다.

② X: 일반적인 주소 확인에서 ARP 요청은 대상을 찾기 위해 브로드캐스트하지만, 응답은 요청에 담긴 발신자의 MAC 주소를 이용하여 **요청 호스트로 유니캐스트**한다. 요청과 응답을 모두 브로드캐스트한다고 설명한 부분이 잘못되었다.

③ O: ARP 스푸핑은 거짓 주소 대응 정보를 보내 상대의 ARP 캐시를 오염시키는 공격이다. 신뢰할 수 있는 IP–MAC 대응을 **정적 항목으로 고정**하여 동적 응답으로 바뀌지 않도록 하면 해당 항목의 변조를 막을 수 있다. 이는 올바르게 설정한 대응 관계를 보호하는 방법이며, 모든 네트워크 공격을 막는다는 뜻은 아니다.

④ X: 이더넷에서 ARP 메시지는 IP 데이터그램 안이 아니라 **이더넷 프레임에 직접 실려** 전달된다. 프레임의 유형 필드로 ARP를 구분하므로 IP 페이로드라는 설명은 맞지 않는다.

NoteBase

문 5. <보기>에서 TCP를 이용하는 네트워크 공격에 해당하는 것들을 모두 고른 것은?

<보기>
㉠ SYN flooding 공격 ㉡ Ping of Death 공격
㉢ Telnet Session Hijacking 공격
㉣ HTTP GET flooding 공격
㉤ Smurf 공격 ㉥ ICMP Redirecting 공격

① ㉠㉡㉢
② ㉠㉢㉣
③ ㉢㉣㉤
④ ㉢㉤㉥

정답 2번

간단한 해설

SYN flooding은 TCP 연결 수립을, Telnet 세션 가로채기는 TCP 세션을 이용한다. HTTP GET flooding도 이 시험의 **TCP 기반 HTTP**를 전제로 하며, 나머지 세 항목은 ICMP와 관련된다.

NoteBase

보기별 해설

㉠ TCP: SYN flooding은 TCP 연결 수립 과정의 SYN과 미완료 연결 상태를 악용하는 서비스 거부 공격이다. **TCP의 연결 설정 절차**를 대상으로 하므로 TCP를 이용한다.

㉡ ICMP: 이 문항의 Ping of Death는 비정상적으로 큰 ping 패킷의 처리·재조립 취약점을 이용하는 공격을 가리킨다. ping은 **ICMP Echo 메시지**를 사용하므로 여기서는 TCP 공격으로 분류하지 않는다.

㉢ TCP: Telnet은 TCP 연결 위에서 원격 터미널 통신을 한다. Telnet Session Hijacking은 이미 성립한 **TCP 기반 세션을 가로채는** 공격이므로 TCP를 이용한다.

㉣ TCP: HTTP GET flooding은 많은 HTTP GET 요청으로 웹 서버의 처리 자원을 소모시키는 공격이다. 이 시험에서 전제한 **TCP 기반 HTTP 통신**을 이용하므로 TCP 공격에 포함한다.

㉤ ICMP: Smurf 공격은 출발지 주소 위조와 브로드캐스트 응답을 결합한 증폭형 서비스 거부 공격으로, **ICMP Echo 요청·응답**을 이용한다. 따라서 이 문항에서는 TCP가 아니라 ICMP에 해당한다.

㉥ ICMP: ICMP Redirecting은 경로 변경을 알리는 **ICMP Redirect 메시지**를 악용하여 통신 경로를 바꾸는 공격이다. 메시지의 프로토콜 자체가 ICMP이므로 TCP 공격으로 분류하지 않는다.

TCP를 이용하는 항목은 ㉠·㉢·㉣이므로 ②와 일치한다.

NoteBase

문 6. <보기>의 주소들이 속해 있는 주소 블록들의 네트워크 주소와 브로드캐스트 주소가 올바르게 짝지어진 것은?

<보기>
㉠ 14.12.62.8/24 ㉡ 200.107.26.17/18

① ㉠ 네트워크주소: 14.12.62.0/24, ㉠ 브로드캐스트 주소: 14.12.62.255/24, ㉡ 네트워크주소: 200.107.0.0/18, ㉡ 브로드캐스트 주소: 200.107.63.255/18

② ㉠ 네트워크주소: 14.12.62.1/24, ㉠ 브로드캐스트 주소: 14.12.62.255/24, ㉡ 네트워크주소: 200.107.1.0/18, ㉡ 브로드캐스트 주소: 200.107.1.255/18

③ ㉠ 네트워크주소: 14.12.62.0/24, ㉠ 브로드캐스트 주소: 14.12.62.255/24, ㉡ 네트워크주소: 200.107.26.0/18, ㉡ 브로드캐스트 주소: 200.107.26.255/18

④ ㉠ 네트워크주소: 14.12.62.1/24, ㉠ 브로드캐스트 주소: 14.12.62.255/24, ㉡ 네트워크주소: 200.107.192.0/18, ㉡ 브로드캐스트 주소: 200.107.192.255/18

정답 1번

간단한 해설

/24에서는 마지막 옥텟만 호스트 부분이지만, /18에서는 세 번째 옥텟의 하위 6비트도 호스트 부분이다. 따라서 ㉡의 세 번째 옥텟 26이 속하는 **블록 범위는 0~63**이다.

NoteBase

계산 과정

주소 경계의 기준: 접두사 길이만큼은 네트워크 비트이고 나머지는 호스트 비트이다. 네트워크 주소는 **호스트 비트를 모두 0**으로, 브로드캐스트 주소는 **호스트 비트를 모두 1**로 만든 주소이다. 첫 사용 가능 호스트 주소와 네트워크 주소를 혼동하지 않는다.

㉠ 14.12.62.8/24: 서브넷 마스크는 255.255.255.0이다. 앞 세 옥텟이 네트워크 부분이고 마지막 옥텟 전체가 호스트 부분이므로 네트워크 주소는 **14.12.62.0/24**, 브로드캐스트 주소는 **14.12.62.255/24**이다. 14.12.62.1은 이 블록의 첫 사용 가능 호스트 주소이지 네트워크 주소가 아니다.

㉡ 200.107.26.17/18: 마스크는 255.255.192.0이고, 세 번째 옥텟의 블록 간격은 256 − 192 = 64이다. 세 번째 옥텟 26은 **0~63 범위**에 속한다. 따라서 호스트 비트를 모두 0으로 하면 200.107.0.0/18, 모두 1로 하면 200.107.63.255/18이 된다. /18은 세 번째 옥텟의 하위 6비트와 마지막 옥텟의 8비트까지 호스트 부분이므로 세 번째 옥텟 26을 그대로 고정하지 않는다.

두 결과를 함께 대조하면 ㉠은 14.12.62.0/24~14.12.62.255/24, ㉡은 200.107.0.0/18~200.107.63.255/18이며 ①과 일치한다.

NoteBase

문 7. <보기 1>의 용어와 <보기 2>의 설명을 연결한 것으로 가장 적절한 것은?

<보기 1>
(가) Footprinting
(나) APT(Advanced Persistent Threat) 공격
(다) Promiscuous 모드
(라) Zero Day 공격
<보기 2>
㉠ 특정 기업 또는 기관의 시스템을 목표로 한 장기적이고 정교한 공격
㉡ 컴퓨터 소프트웨어의 취약점에 대한 패치가 나오지 않은 시점에 이루어지는 공격
㉢ 해킹하기 전에 공격 대상에 대한 정보를 모으는 사전 준비 작업
㉣ 스니핑을 위해 랜카드의 필터링 기능을 해제

① (가): ㉠, (나): ㉡, (다): ㉢, (라): ㉣
② (가): ㉡, (나): ㉠, (다): ㉣, (라): ㉢
③ (가): ㉢, (나): ㉠, (다): ㉣, (라): ㉡
④ (가): ㉣, (나): ㉡, (다): ㉢, (라): ㉠

정답 3번

간단한 해설

Footprinting은 **사전 정보 수집**, APT는 **특정 목표에 대한 지속적 공격**이다. Promiscuous 모드는 수신 주소 필터링 해제, Zero Day 공격은 패치 제공 전 취약점 악용과 연결된다.

NoteBase

대응 관계 해설

(가) Footprinting → ㉣: 공격 대상의 조직, 도메인, 네트워크 구성 등 **대상에 관한 정보를 미리 수집**하는 사전 조사 활동이다. 실제 침투에 앞서 대상의 특징과 공격 경로를 파악하는 준비 작업이라는 설명과 연결된다.

(나) APT 공격 → ㉠: 특정 기업이나 기관 같은 목표를 정하고 여러 수단을 결합하여 **장기간 지속적으로 목적을 추구**하는 정교한 공격이다. 한 번의 무차별 시도보다 특정 대상에 대한 지속성과 조직성이 핵심이다.

(다) Promiscuous 모드 → ㉡: 네트워크 인터페이스가 수신한 프레임 중 자신의 주소를 목적지로 하지 않은 것도 운영체제에 전달하도록 **수신 주소에 따른 필터링을 해제**하는 모드이다. 패킷 관찰에 이용되지만, 스위치가 해당 포트에 보내지 않은 트래픽까지 자동으로 수신하게 하는 기능은 아니다.

(라) Zero Day 공격 → ㉢: 취약점을 해결할 **보안 패치가 제공되기 전에 그 취약점을 악용**하는 공격이다. 패치가 이미 배포되었는데 사용자가 적용하지 않은 상태를 노리는 공격과 구별한다.

따라서 (가) ㉣, (나) ㉠, (다) ㉡, (라) ㉢의 대응이며 ③과 일치한다.

NoteBase

문 8. 다음 표는 패킷 필터링 방화벽에 적용된 필터링 규칙의 예이다. 표에 대한 설명 중 가장 적절하지 않은 것은? (방화벽은 내부 네트워크와 외부 네트워크의 경계에 위치하는 것으로 가정함)

규칙	방향	발신지 IP주소	목적지 IP주소	프로토콜	목적지 포트번호	동작
A	안으로	외부	내부	TCP	25	허용
B	밖으로	내부	외부	TCP	25	허용
C	안으로	외부	내부	TCP	80	허용
D	양방향	전부	전부	TCP/UDP	전부	거절

① 방화벽 내부의 사용자들은 외부로 전자메일을 전송할 수 있다.

② 방화벽 내부의 사용자들은 외부의 FTP 서버에 접속할 수 없다.

③ 방화벽 내부의 사용자들은 외부의 웹 서버에 접속할 수 있다.

④ 방화벽 내부의 사용자들은 외부의 텔넷 서버에 접속할 수 없다.

정답 3번

간단한 해설

규칙 C가 허용하는 것은 **외부→내부의 목적지 TCP 80번**이다. 내부에서 외부 웹 서버로 향하는 요청은 허용 목록에 없으므로 마지막 거절 규칙 D에 해당한다.

NoteBase

선지별 해설

표는 A~C의 명시적 허용을 먼저 적용하고 나머지를 D로 거절하는 서비스 접근 정책으로 읽는다. '안으로'는 외부→내부, '밖으로'는 내부→외부이며, 열에 적힌 번호는 출발지 포트가 아니라 목적지 포트이다. 다만 응답 패킷·상태 추적 규칙은 표에 제시되지 않아 실제 연결의 완전한 왕복 허용까지 확인한 것은 아니다.

① O: 규칙 B는 내부에서 외부로 향하는 TCP 목적지 포트 25번을 허용한다. 25번은 SMTP에 사용하는 포트이므로, 문항의 서비스 접근 정책상 **외부로 보내는 전자메일 요청이 허용**된다. 규칙 A는 반대 방향인 외부에서 내부의 25번으로 향하는 요청을 허용한다.

② O: FTP 제어 연결의 일반적인 목적지 포트는 TCP 21번이다. 표에 내부에서 외부의 21번으로 향하는 허용 규칙이 없으므로 **나머지 트래픽을 거절하는 D**에 해당한다. 따라서 표의 정책상 외부 FTP 서버로의 접속은 차단된다.

③ X: 규칙 C는 **외부에서 내부**로 향하는 TCP 목적지 포트 80번을 허용한다. 내부 사용자가 외부 웹 서버로 요청하려면 내부에서 외부의 80번으로 향하는 규칙이 필요하지만 표에는 없다. 해당 요청은 D로 거절되므로, 표는 외부 사용자의 내부 웹 서비스 접근을 허용하는 것이지 내부 사용자의 외부 웹 접속을 허용하는 것이 아니다.

④ O: Telnet의 일반적인 목적지 포트는 TCP 23번이다. 내부에서 외부의 23번으로 향하는 허용 규칙이 없으므로 **D에 의해 거절**되어 외부 Telnet 서버에 접속할 수 없다.

따라서 규칙 C의 방향을 반대로 해석한 ③이 가장 적절하지 않다.

NoteBase

문 9. <보기>의 NAT(Network Address Translation) 라우터에 대한 설명으로 옳은 것을 모두 고른 것은?

<보기>
㉠ 사설 IP주소와 공인 IP주소의 매핑을 제공한다.
㉡ NAT 라우터는 일반적으로 IP주소와 포트 번호를 조합하여 매핑한다.
㉢ IPv4 주소 고갈 문제를 완화할 수 있으며 보안 상 이점을 갖는다.
㉣ 사설망 내부에서 웹 서버 운영 시 port forwarding을 통해 접속을 허용할 수 있다.

① ㉠㉢
② ㉠㉡㉢
③ ㉠㉢㉣
④ ㉠㉡㉢㉣

정답 4번

간단한 해설

NAT는 사설·공인 주소를 변환하고, 일반적인 NAPT는 **주소와 포트의 조합으로 공인 주소를 공유**한다. 내부 주소 노출을 줄이는 이점이 있으며, 포트 포워딩으로 외부 요청을 내부 웹 서버에 전달할 수 있다.

NoteBase

보기별 해설

㉠ O: NAT는 내부에서 사용하는 사설 IP주소와 외부 통신에 사용하는 공인 IP주소 사이의 **주소 변환 관계**를 제공한다. 외부로 나가는 패킷과 돌아오는 응답의 주소를 변환하여 사설망 호스트가 공인망과 통신할 수 있게 한다.

㉡ O: 일반적인 공유기 등은 IP주소뿐 아니라 TCP·UDP의 포트 번호도 변환하는 NAPT 또는 PAT를 사용한다. **주소와 포트의 조합**으로 각 통신을 구분하므로 여러 내부 호스트가 하나의 공인 IP주소를 공유할 수 있다. 주소만 변환하는 기본 NAT와 구별되는 방식이지만, 문항의 일반적인 NAT 라우터 설명에는 해당한다.

㉢ O: 여러 내부 호스트가 소수의 공인 IP주소를 공유하면 필요한 공인 IPv4 주소 수를 줄여 주소 고갈을 완화한다. 또한 **내부 주소를 외부에 직접 노출하지 않는** 효과가 있어 보안상 이점이 있다. 다만 NAT 자체가 암호화나 완전한 접근통제·침입차단을 제공하는 것은 아니므로 방화벽을 대체하지는 않는다.

㉣ O: 포트 포워딩은 공인 IP주소의 특정 포트로 들어온 요청을 **지정한 내부 서버의 주소·포트로 전달**하도록 매핑한다. 이를 통해 사설망의 웹 서버에 외부에서 접속할 수 있게 하며, 별도로 적용되는 방화벽 정책도 해당 통신을 허용해야 한다.

따라서 네 보기 ㉠·㉡·㉢·㉣이 모두 옳으며, 이들을 빠짐없이 포함한 조합은 ④이다.

NoteBase

문 10. 리눅스 시스템의 사용자 계정 관련 파일로 가장 적절하지 않은 것은?

① /etc/passwd

② /etc/shadow

③ /etc/permission

④ /etc/group

정답 3번

간단한 해설

/etc/permission은 표준 계정 관리 파일이 아니다. 사용자 기본 정보는 /etc/passwd, 패스워드 관련 정보는 /etc/shadow, 그룹 정보는 /etc/group에서 관리한다.

개념 구분

/etc/passwd는 **사용자 계정의 기본 정보**를 저장한다. 사용자명, UID, 기본 GID, 홈 디렉터리, 로그인 셸 등이 포함된다. 섀도 패스워드를 사용하는 시스템에서는 패스워드 필드에 보통 x가 표시되고 실제 패스워드 해시는 별도 파일에 둔다.

/etc/shadow는 **패스워드 해시와 유효기간 관련 정보**를 저장한다. 일반 사용자에게 읽기 접근을 제한하여 계정 인증 정보를 보호한다.

/etc/group은 그룹 이름, GID 및 그룹 구성원 목록 등 **그룹 계정 정보**를 저장한다. 사용자의 그룹 소속은 자원 접근 권한 판단과 연결된다.

/etc/permission은 리눅스의 표준 사용자 계정 관리 파일이 아니다. 파일 접근 권한은 파일시스템의 소유자·그룹·모드와 필요시 ACL 등의 메타데이터로 관리하므로, 이름에 permission이 들어간다는 이유로 계정 관리 파일로 볼 수 없다.

따라서 계정 관련 표준 파일로 적절하지 않은 것은 ③ /etc/permission이다.

NoteBase

문 11. 네트워크 진단 프로그램에 대한 설명으로 가장 적절하지 않은 것은?

① traceroute - 지정한 호스트까지의 경로를 조사하는 프로그램

② nslookup - DNS 서버에 도메인 네임에 관한 질의를 하는 프로그램

③ metasploit - 네트워크 토폴로지를 매핑시키는 프로그램

④ tcpdump - 네트워크 패킷 캡처 프로그램

정답 3번

간단한 해설

Metasploit의 핵심 용도는 네트워크 연결 구조를 그리는 것이 아니라, **취약점을 검증하는 침투 테스트**이다.

선지별 해설

① O: traceroute는 탐사 패킷의 TTL 등을 단계적으로 조절하고 중간 장비의 응답을 이용해 목적지까지 거치는 **홉과 경로**를 조사한다. 응답을 차단하는 장비가 있으면 일부 구간이 표시되지 않을 수 있다.

② O: nslookup은 DNS 서버에 도메인 이름과 관련된 레코드를 질의하는 도구이다. 예를 들어 이름에 대응하는 IP 주소 등을 확인하여 **이름 해석 문제**를 진단할 수 있다.

③ X: Metasploit은 취약점의 공격 가능성을 시험하고 검증하는 **침투 테스트 프레임워크**이다. 네트워크 장비의 연결 구조를 지도처럼 나타내는 토폴로지 매핑을 대표 용도로 하는 프로그램이라는 설명은 부적절하다. 일부 탐색·스캔 기능을 포함할 수 있다는 점과 도구의 핵심 목적을 구별해야 한다.

④ O: tcpdump는 네트워크 인터페이스에서 패킷을 캡처하고 내용을 표시하거나 파일로 저장하는 도구이다. 주소·포트·프로토콜 등의 조건으로 필요한 통신을 골라 **패킷 수준의 동작**을 분석할 수 있다.

NoteBase

문 12. 네트워크 보안 프로토콜에 대한 설명 중 가장 적절하지 않은 것은?

① EAP(Extensible Authentication Protocol)는 다양한 인증 방법을 지원하는 네트워크 접근 제어 프로토콜이다.

② IPsec(IP Security)은 AH(Authentication Header)를 통해 인증, 무결성, 기밀성을 제공한다.

③ TLS(Transport Layer Security)는 최근 버전 1.3으로 표준화되었으며, 핸드셰이크(handshake) 과정을 통해 암호화에 필요한 알고리즘 및 관련 매개변수를 교환한다.

④ DNSSEC(DNS Security)은 DNS 데이터 인증과 무결성을 보장하지만, DNS 서버에 대한 DoS(Denial of Service) 공격은 막지 못한다.

정답 2번

간단한 해설

IPsec의 AH는 인증과 무결성을 제공하지만 **암호화에 의한 기밀성은 제공하지 않는다**. 기밀성 보호는 암호화 기능을 사용하는 ESP와 구별해야 한다.

선지별 해설

① O: EAP는 하나의 인증 방식만 고정하지 않고 **여러 인증 방법을 수용하는 인증 프레임워크**이다. 네트워크 접근 인증에서 인증 메시지를 주고받는 공통 틀을 제공하고 실제 인증 방식은 선택한 EAP 방법에 따라 정해진다.

② X: IPsec의 AH는 데이터 출처 인증과 무결성 검증, 재전송 공격 방지에 사용되지만 **데이터를 암호화하여 기밀성을 제공하지는 않는다**. IPsec에서 기밀성이 필요하면 암호화 기능을 사용하는 ESP를 적용해야 한다. 인증·무결성과 암호화에 의한 기밀성을 구분해야 한다.

③ O: TLS 1.3은 **2018년 8월 RFC 8446**으로 표준화되어 2019년 시험 당시의 '최근 버전'이라는 설명에 부합한다. 핸드셰이크에서는 통신 상대의 인증, 암호 알고리즘·매개변수 협상과 공유 키 재료의 확립을 수행하여 이후 데이터를 보호할 준비를 한다.

④ O: DNSSEC는 DNS 응답 데이터의 **출처 인증과 무결성**을 검증하여 위조·변조를 탐지하도록 한다. 그러나 서버나 네트워크의 자원을 소모시키는 서비스 거부 공격까지 막아 가용성을 보장하는 수단은 아니므로 DoS 방어와 구별된다.

따라서 AH가 기밀성까지 제공한다고 한 ②가 가장 적절하지 않다.

NoteBase

문 13. IEEE 802.11i에 관한 설명으로 가장 적절하지 않은 것은?

① IEEE 802.11 무선랜의 보안 표준으로 인증, 데이터 무결성, 데이터 기밀성, 키 관리에 관한 내용을 포함한다.

② 무선단말(station)과 무선접속점(access point) 간의 안전한 통신을 제공한다.

③ 인증서버(authentication server)는 무선단말을 인증한다.

④ 무선단말과 무선접속점은 RADIUS(Remote Authentication Dial In User Service) 프로토콜을 통해 인증 정보를 교환한다.

정답 4번

간단한 해설

무선단말과 무선접속점 사이에서는 **EAPOL**로 인증 메시지를 주고받는다. RADIUS는 무선접속점과 인증서버 사이에서 인증 정보를 전달하는 데 사용된다.

선지별 해설

① O: IEEE 802.11i는 기존 무선랜의 보안을 강화하는 표준이다. 접근하려는 단말의 인증, 데이터의 기밀성·무결성 보호, 이를 위한 키 관리 등을 다룬다.

② O: 무선단말과 무선접속점 사이의 무선 구간에 암호화와 무결성 검증을 적용하여 도청이나 데이터 변조에 대응한다. 이때 보호하는 구간은 **단말과 접속점 사이**이며, 인터넷상의 모든 종단 구간을 자동으로 보호한다는 뜻은 아니다.

③ O: 인증서버를 사용하는 802.1X 기반 구성에서는 무선접속점이 단말의 인증 메시지를 중계하고, **인증서버가 단말의 인증 여부를 판단**한다. 모든 802.11i 구성에 별도 인증서버가 필수인 것은 아니며 사전 공유 키를 사용하는 방식도 있다.

④ X: RADIUS를 사용하는 통신 구간을 잘못 설명했다. 단말과 접속점은 EAPOL로 인증 메시지를 교환하며, 접속점은 그 안의 EAP 메시지를 RADIUS에 담아 인증서버로 전달한다. 따라서 RADIUS가 사용되는 구간은 **무선접속점과 인증서버 사이**이다.

NoteBase

문 14. C 언어로 개발된 소프트웨어의 메모리 오염(memory corruption)에 대한 설명으로 가장 적절하지 않은 것은?

① Heap Buffer Overflow – malloc() 함수를 통해 힙(heap) 영역에 할당한 변수의 메모리 경계를 검사하지 않고 사용할 때 발생할 수 있음

② Integer Overflow – 변수의 자료형보다 큰 수를 저장할 때 발생할 수 있음

③ Use-After-Free – free() 함수를 통해 이미 해제된 포인터를 사용할 때 발생할 수 있음

④ Double Free – free() 함수를 통해 포인터 해제 후, 같은 이름의 포인터를 생성하고 free() 함수로 해제할 때 발생할 수 있음

정답 4번

간단한 해설

Double Free는 **이미 해제한 동일한 할당 메모리를 다시 해제**하는 오류이다. 포인터 변수 이름이 같은지가 아니라 어떤 메모리 할당을 해제하는지가 기준이다.

선지별 해설

① O: 힙 버퍼 오버플로는 malloc() 등으로 할당한 힙 버퍼의 **할당 경계를 넘어 데이터를 쓸 때** 발생한다. 할당 크기보다 많은 데이터를 복사하거나 잘못된 인덱스로 접근하면 주변 데이터나 메모리 관리 정보를 손상시킬 수 있다. 경계를 검사하지 않는 사용이 원인이 될 수 있다는 설명이다.

② O: 정수형이 **표현할 수 있는 수의 범위를 초과**하는 계산·저장 과정에서는 의도한 값을 유지하지 못하는 정수 오버플로 관련 문제가 생길 수 있다. 자료형 자체보다 수가 크다는 표현은 그 자료형의 표현 범위를 넘는다는 뜻으로 이해한다. 잘못 계산된 길이로 작은 버퍼를 할당하면 버퍼 오버플로로 이어질 수도 있으나, 정수 범위 오류와 메모리 경계 초과는 구별한다.

③ O: free()가 해제하는 것은 포인터 변수가 아니라 그 포인터가 가리키던 동적 할당 메모리이다. 그 뒤 남아 있는 포인터를 통해 **이미 해제된 메모리에 다시 접근**하면 Use-After-Free가 된다. 해당 영역이 다른 용도로 재할당되면 다른 데이터를 읽거나 손상시킬 수 있다.

④ X: Double Free의 기준은 포인터의 이름이 아니라 **동일한 할당 메모리를 중복 해제**했는지이다. 이미 해제한 메모리를 가리키는 포인터나 별칭 포인터로 다시 free()를 호출하면 문제가 된다. 같은 이름의 변수를 다시 쓰거나 새 메모리를 할당받아 그 새 할당을 한 번 해제하는 행위 자체는 Double Free가 아니다.

NoteBase

문 15. DEP(Data Execution Prevention)에 대한 설명으로 가장 적절하지 않은 것은?

① 실행 권한이 없는 메모리 영역에서 코드가 실행되지 않도록 하는 기법을 말한다.

② CPU에서 지원하는 하드웨어 기반 DEP과 운영체제가 지원하는 소프트웨어 기반 DEP으로 구분할 수 있다.

③ ROP(Return Oriented Programming) 기법에 의해 우회가 가능하다.

④ RTL(Return To Library) 공격을 막기 위해 개발되었다.

정답 4번

간단한 해설

DEP는 **비실행 영역에 주입된 코드의 실행**을 막는다. RTL은 이미 실행 가능한 라이브러리 코드를 재사용하므로 DEP만으로 차단되지 않는다.

선지별 해설

① O: DEP는 실행 가능으로 지정되지 않은 메모리에서 코드를 실행하려는 시도를 막는 보호 기법이다. 스택·힙 등에 주입된 코드를 실행하는 공격을 줄이지만, **메모리 내용이 덮어써지는 것 자체**를 모두 막는 기법은 아니다.

② O: DEP라는 보호 기능은 하드웨어 기반과 소프트웨어 기반으로 구분하여 설명한다. 하드웨어 기반은 CPU의 NX/XD 같은 실행 금지 지원을 이용한다. Windows에서 소프트웨어 DEP라고 부르는 기능은 예외 처리의 안전성 검사와 관련되며, **하드웨어의 페이지 실행 금지와 같은 보호는 아니다**.

③ O: ROP는 이미 실행 가능한 메모리에 있는 짧은 코드 조각을 재사용하여 제어 흐름을 구성한다. 따라서 **새 코드를 비실행 영역에서 실행하지 않고도** DEP의 제한을 우회할 수 있다. DEP만으로 모든 코드 재사용 공격을 차단하지는 못한다.

④ X: RTL은 기존 라이브러리 함수를 재사용하는 공격이다. DEP는 주로 **비실행 영역에 주입된 코드의 실행**을 막기 위한 것이므로, 이미 실행 가능한 라이브러리 코드를 이용하는 RTL을 막기 위해 개발되었다고 볼 수 없다. 이러한 코드 재사용을 어렵게 하려면 주소 무작위화나 제어 흐름 보호 등을 함께 고려한다.

NoteBase

문 16. 32비트 인텔 CPU 아키텍처에서 윈도우 운영체제를 사용한다고 가정할 때, 어셈블리어 명령어들에 대한 설명이다. 가장 적절하지 않은 것은?

① ADD ECX, 10 - 카운터 레지스터 ECX에 10을 더한 후 데이터 레지스터 EDX에 저장

② MOV ECX, 4 - 카운터 레지스터 ECX에 4를 저장

③ INC EAX - 누산기 레지스터 EAX에 저장된 값을 1만큼 증가

④ CALL EBX - 베이스 레지스터 EBX에 저장된 주소로 이동 및 실행

정답 1번

간단한 해설

ADD ECX, 10의 목적지는 첫 번째 피연산자인 ECX이다. 덧셈 결과는 **EDX가 아니라 ECX에 저장**된다.

선지별 해설

① X: Intel 문법의 두 피연산자 명령에서는 앞쪽이 목적지이다. ADD ECX, 10은 기존 ECX 값에 10을 더한 결과를 **ECX 자신에 저장**한다. EDX는 이 명령의 피연산자가 아니므로 결과 저장 대상이 아니다.

② O: MOV ECX, 4는 즉시값 4를 **목적지 ECX에 복사**한다. 기존 ECX 값에 4를 더하는 연산이 아니라 ECX의 값을 4로 바꾸는 명령이다.

③ O: INC EAX는 EAX의 현재 값을 **1만큼 증가**시키고 결과를 EAX에 저장한다. 32비트 레지스터 연산이므로 저장되는 결과는 32비트 범위에 따른다.

④ O: CALL EBX는 EBX가 가리키는 주소로 제어를 옮기는 간접 호출이다. 단순 점프와 달리 **호출 다음 명령의 복귀 주소를 스택에 저장**한 뒤 대상 코드의 실행을 시작하므로, 이후 반환 명령으로 돌아올 수 있다.

따라서 ADD의 결과 저장 레지스터를 EDX로 설명한 ①이 가장 적절하지 않다.

NoteBase

문 17. 백도어(backdoor)에 관한 설명으로 가장 적절하지 않은 것은?

① 백도어는 공격자에 의해 시스템 관리자 권한이 탈취된 후 설치되거나, 백도어가 이미 탑재된 악의적인 소프트웨어 설치를 통해 시스템에 설치될 수 있다.

② 하드웨어 펌웨어에 탑재된 백도어는 디스크 포맷 후, 정상적인 운영체제 재설치를 통해 삭제될 수 있다.

③ 운영체제 레벨의 백도어(예를 들어, 악의적인 코드가 탑재된 kernel32.dll)는 디스크 포맷 후, 정상적인 운영체제 재설치를 통해 삭제될 수 있다.

④ 응용 레벨의 백도어는 현재 동작 중인 프로세스 확인, 포트 검사, 바이러스 탐지 툴, 시스템 무결성 검사 등으로 탐지가 가능하다.

정답 2번

간단한 해설

펌웨어의 백도어는 운영체제 파일과 저장 위치가 다르므로 **디스크 포맷과 운영체제 재설치만으로 제거되지 않는다**.

선지별 해설

① O: 백도어는 정상적인 인증·접근 통제를 우회하여 시스템에 접근하게 하는 숨겨진 통로이다. 공격자가 **관리자 권한을 확보한 뒤 설치**할 수도 있고, 백도어 기능을 포함한 악성 소프트웨어가 설치되면서 함께 들어올 수도 있다.

② X: 하드웨어 펌웨어는 보통 운영체제가 설치된 디스크와 별도의 비휘발성 저장 영역에 존재한다. 따라서 **디스크 포맷과 운영체제 재설치만으로는 펌웨어의 백도어를 제거하지 못한다**. 감염된 펌웨어 자체의 신뢰할 수 있는 복구·재기록이나 장치 수준의 조치가 필요하므로, 가장 적절하지 않은 설명은 ②이다.

③ O: 변조된 kernel32.dll처럼 **디스크의 운영체제 파일에 존재하는 백도어**는 해당 디스크를 포맷하고 신뢰할 수 있는 정상 운영체제를 새로 설치하면 제거할 수 있다. 이는 오염이 그 파일 영역에 한정되고, 펌웨어나 감염된 복원 자료에서 다시 유입되지 않는 경우의 설명이다.

④ O: 응용 레벨의 백도어는 실행 프로세스나 통신 포트의 이상, 악성코드 탐지 결과, 정상 파일과의 차이 등을 통해 발견할 수 있다. 여러 검사 방법을 함께 사용하면 **실행·통신·파일 변조 흔적**을 확인할 수 있지만, 어느 한 검사만으로 모든 백도어의 탐지를 보장하는 것은 아니다.

NoteBase

문 18. 암호 알고리즘에 대한 설명 중 가장 적절하지 않은 것은?

① AES는 기존 DES, 3DES의 취약한 암호 강도를 극복하고자 미국 NIST에서 전세계 암호학자들에게 공모를 통해 선정한 비대칭 암호 알고리즘으로 데이터에 대한 기밀성 제공 및 부인 방지 기능을 제공한다.

② RC5는 미국 RSA 연구소에서 개발한 입출력, 키, 라운드 수가 가변적인 블록 암호 알고리즘으로 DES에 비해 빠른 연산 속도를 제공한다.

③ SEED는 한국인터넷진흥원과 국내 암호 전문가들이 순수 국내 기술로 개발한 블록 암호 알고리즘이며, 국제표준화기구인 ISO/IEC와 IETF로부터 암호 표준 알고리즘으로 인정받았다.

④ ARIA는 국가보안기술연구소와 국내 암호 전문가들이 경량 환경을 위해 개발한 블록 암호 알고리즘이다.

정답 1번

간단한 해설

AES는 **대칭키 블록 암호**로 기밀성을 제공하지만, 그 자체로 부인 방지 기능을 제공하지는 않는다.

선지별 해설

① X: AES는 NIST의 공개 공모로 선정된 **대칭키 블록 암호**이지 비대칭키 암호가 아니다. 비밀키를 이용한 암호화로 기밀성을 제공하지만, 같은 키를 공유하는 당사자 중 누가 데이터를 만들었는지 입증하는 부인 방지를 AES 자체가 제공하지는 않는다. 부인 방지에는 전자서명 등 별도의 수단이 필요하다.

② O: RC5는 RSA 연구소의 Rivest가 설계한 블록 암호로, **블록 크기·키 길이·라운드 수**를 매개변수로 정할 수 있다. 단순한 연산을 이용하여 빠른 소프트웨어 구현을 지향한다. DES와의 속도 비교는 구현 환경과 매개변수에 따라 달라지므로 모든 조건에서 항상 빠르다는 뜻은 아니다.

③ O: SEED는 한국인터넷진흥원과 국내 전문가들이 개발한 **국산 블록 암호**이다. ISO/IEC 국제표준에 포함되었으며, IETF에서도 알고리즘과 활용을 다루는 RFC 문서로 규정되어 국제적으로 활용된다.

④ O: ARIA는 국가보안기술연구소를 중심으로 국내 전문가들이 개발한 블록 암호이다. **경량 환경과 하드웨어 구현**을 고려해 설계된 범용 블록 암호라는 점이 설명과 부합한다.

NoteBase

문 19. 다음 설명 중 가장 적절하지 않은 것은?

① 워터마크(watermark)는 저작권 보호를 위해 이미지나 동영상 파일에 저작권 정보를 삽입하는 기법을 말한다.

② DRM(Digital Right Management)은 문서나 동영상 파일에 보안성을 제공하기 위해 암호화 하고 인가된 사용자에 한해서 해당 파일에 접근할 수 있는 권한을 부여한다.

③ 백신 프로그램은 문서나 동영상에 접근할 수 없는 사용자로부터 해당 파일의 저작권을 보호한다.

④ 방화벽은 워터마크나 DRM이 적용된 파일을 탐지하지 못한다.

정답 3번

간단한 해설

백신 프로그램은 **악성코드를 탐지·차단·제거**하는 수단이지 콘텐츠의 저작권이나 이용권한을 관리하는 수단이 아니다. 비인가자의 파일 이용을 통제하는 기능은 DRM과 구별해야 한다.

선지별 해설

① O: 디지털 워터마크는 이미지·동영상 등 콘텐츠에 **저작권자나 소유권을 식별하는 정보**를 삽입하는 기법이다. 소유권 확인이나 불법 유통 추적에 활용할 수 있지만, 정보 삽입 자체가 모든 복사·열람을 차단하는 것은 아니다.

② O: DRM은 콘텐츠를 암호화하고 사용권한을 관리하여 **인가된 사용자에게 허용된 이용만** 가능하도록 통제하는 기술이다. 권한에 따라 열람·복사·인쇄 등을 제한할 수 있으며, 단순히 저작권 정보를 표시하는 워터마크와 구별한다.

③ X: 백신 프로그램의 기본 역할은 **악성코드의 탐지·차단·제거**이다. 파일에 대한 저작권이나 사용권한을 관리하는 기능으로 설명한 것은 부적절하다. 비인가자의 콘텐츠 이용을 제한하는 역할은 DRM 등 권한관리 기술과 연결해야 한다.

④ O: 이 문항은 각 기술의 기본 역할을 구별하는 맥락이다. 기본적인 방화벽의 접근 제어 기능만으로 **워터마크·DRM의 권리 정보를 판별·관리하는 것은 아니다**. 다만 원문의 '탐지하지 못한다'는 표현을, 콘텐츠 검사 기능을 결합한 제품까지 해당 파일의 식별이 절대 불가능하다는 뜻으로 일반화해서는 안 된다. 가장 명확하게 기능을 잘못 연결한 설명은 백신을 저작권 보호 수단으로 본 ③이다.

NoteBase

문 20. 다음 설명 중 가장 적절하지 않은 것은?

① 비트코인(Bitcoin)은 블록체인(blockchain) 기반 암호화폐(cryptocurrency)이다.

② 비트코인은 공개키 기반 주소를 사용하고 트랜잭션(transaction)을 암호화하여 전송하기 때문에 익명성이 보장된다.

③ 비트코인 블록체인의 작업증명(Proof-of-Work)은 단방향 해시 함수의 특성을 이용한다.

④ 비트코인 블록체인은 누구나 참여할 수 있는 공개형 블록체인이다.

정답 2번

간단한 해설

비트코인 거래 내역은 **공개적으로 기록**되며, 전자서명은 거래 내용을 숨기는 암호화와 다르다. 주소를 사용해도 거래의 연결 관계가 드러날 수 있으므로 **완전한 익명성은 보장되지 않는다**.

선지별 해설

① O: 비트코인은 거래 내역을 블록에 모으고 앞 블록의 해시로 연결하는 **블록체인 기반 암호화폐**이다. 네트워크 참여자들이 거래와 블록의 규칙 준수를 검증하며 원장을 유지한다.

② X: 비트코인의 거래는 내용을 숨기기 위해 암호화한 채 원장에 기록하는 것이 아니라 **블록체인에 공개적으로 기록**된다. 전자서명은 지출 권한을 검증하는 수단이지 거래 내용을 비밀로 만드는 암호화가 아니다. 실명 대신 주소를 사용하더라도 주소 간 거래가 추적·연결될 수 있으므로 완전한 익명성이 보장되지 않는다.

③ O: 작업증명은 블록 헤더의 해시값이 정해진 목표 이하가 되도록 입력을 바꾸어 반복 계산하는 방식이다. 원하는 해시 결과를 만드는 입력을 곧바로 역산하기 어렵지만 **제시된 결과의 검증은 쉽게** 할 수 있는 해시 함수의 성질을 이용한다.

④ O: 비트코인은 특정 관리자의 사전 참여 허가를 요구하는 폐쇄형 시스템이 아니라 **누구나 참여할 수 있는 공개형 네트워크**이다. 다만 누구나 임의 거래나 블록을 승인받는다는 뜻은 아니며, 참여자가 제시한 데이터는 합의·검증 규칙을 충족해야 한다.

따라서 거래 암호화와 완전한 익명성 보장을 주장한 ②가 가장 적절하지 않다.

NoteBase