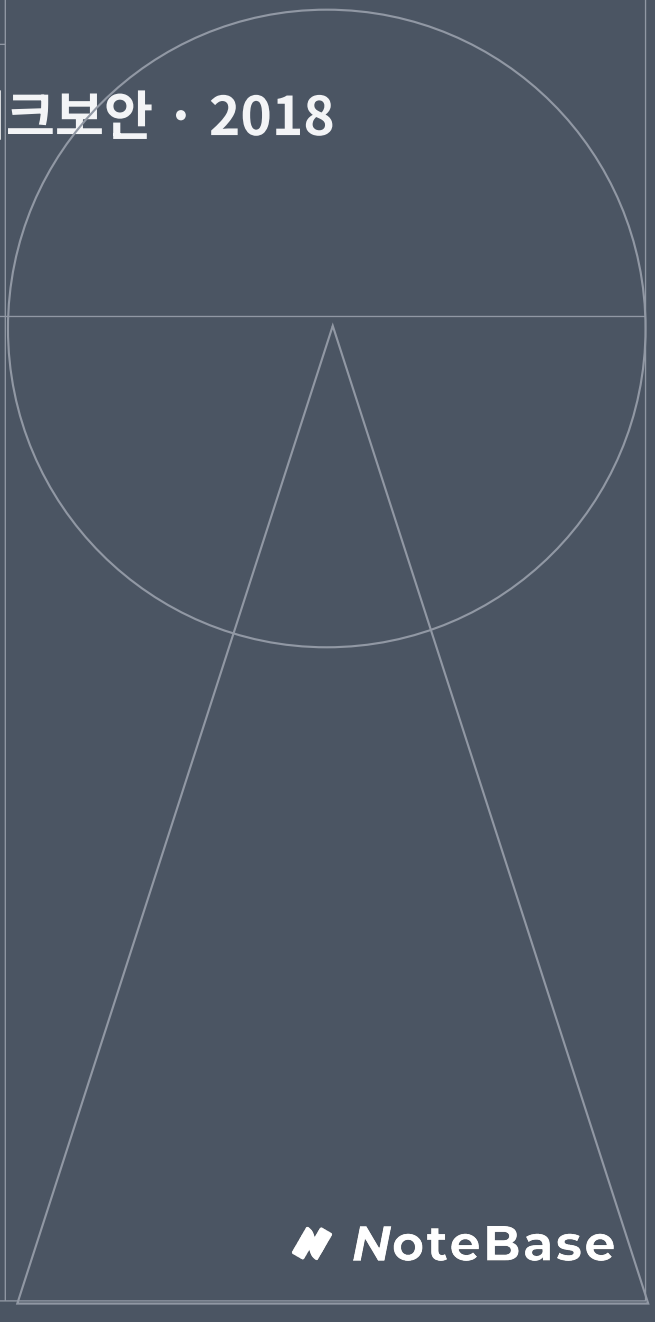
# 기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2018



NoteBase

# 기출OX 해설집

## 공무원/국가직/9급 · 네트워크보안 · 2018

**공무원/국가직/9급 · 네트워크보안 · 2018**

**문 1. ICMP(Internet Control Message Protocol)의 기능으로 옳지 않은 것은?**

① 네트워크 데이터 전송 오류 보고

② 멀티캐스트 그룹 멤버십 보고

③ 네트워크 혼잡 보고

④ Timeout 보고

**정답 2번**

**간단한 해설**

멀티캐스트 그룹 멤버십 보고는 호스트가 자신이 속한 멀티캐스트 그룹을 인접 라우터에 알리는 기능으로, ICMP가 아니라 **IGMP**가 담당한다.

**선지별 해설**

① O: ICMP는 IP 데이터그램 처리 중 발생한 오류를 송신 측에 알린다. 예를 들어 목적지에 도달할 수 없으면 **Destination Unreachable** 메시지로 그 사유를 보고한다. 오류를 알리는 기능이며, ICMP 자체가 손실된 데이터를 재전송하여 전달을 보장하는 것은 아니다.

② X: IPv4에서 멀티캐스트 그룹 멤버십 보고를 담당하는 프로토콜은 **IGMP**이다. 호스트는 Membership Report 메시지로 자신이 해당 그룹의 데이터를 받으려 한다는 사실을 인접 멀티캐스트 라우터에 알린다. 따라서 이 기능을 ICMP의 기능으로 제시한 부분은 IGMP의 기능으로 고쳐야 한다.

③ O: 초기 ICMP 규격에는 혼잡을 알리고 송신 속도를 줄이도록 요청하는 **Source Quench** 메시지가 있었다. 라우터의 버퍼가 부족하거나 수신 호스트의 처리 능력을 넘는 속도로 데이터가 들어오는 경우에 사용하는 것으로 정의되었다. 이 문항은 이러한 전통적인 기능 분류를 기준으로 한다. 다만 현재 표준에서는 Source Quench가 폐기되어, 이를 이용한 혼잡 제어를 사용해서는 안 된다.

④ O: ICMP의 **Time Exceeded** 메시지는 전송 중 패킷의 TTL이 소진되거나, 목적지에서 분할된 데이터그램을 제한 시간 안에 재조립하지 못한 상황을 보고한다. 여기서 Timeout 보고는 이러한 시간 초과를 뜻하며, 응용 프로그램의 모든 응답 대기 시간 초과를 ICMP가 보고한다는 의미는 아니다.

NoteBase

**문 2. 다음에서 설명하는 방화벽 구성 방법은?**

네트워크로 들어오는 트래픽에 대해서 스크리닝 라우터는 패킷 필터링으로 1차 방어를 하고, 베스천 호스트로 단일 홈 게이트웨이에서 프록시 등으로 2차 방어를 한다. 또한, 베스천 호스트는 스크리닝 라우터를 거치지 않은 모든 접속을 거부하며, 스크리닝 라우터도 베스천 호스트를 거치지 않은 모든 접속을 거부하도록 설정한다.

① 스크린된 호스트 게이트웨이

② 스크리닝 라우터

③ 단일 홈 게이트웨이

④ 이중 홈 게이트웨이

**정답 1번**

**간단한 해설**

**스크리닝 라우터와 베스천 호스트를 결합**하여 패킷 필터링과 프록시로 두 단계의 방어를 수행하는 구성이 스크린된 호스트 게이트웨이이다. 두 장치의 접근 규칙으로 베스천 호스트를 우회한 접속도 차단한다.

**공통 해설**

스크린된 호스트 게이트웨이는 **패킷 필터링을 하는 스크리닝 라우터와 응용 서비스를 중계하는 베스천 호스트를 결합**한 방화벽 구성이다. 베스천 호스트는 외부 접근을 통제하도록 보안을 강화한 호스트이며, 프록시는 클라이언트의 요청을 대신 전달하여 응용 서비스 이용을 중계한다.

지문에서는 스크리닝 라우터가 들어오는 패킷을 먼저 걸러 1차 방어를 하고, 단일 홈 베스천 호스트가 프록시 등으로 2차 방어를 한다. 라우터와 호스트의 접근 규칙을 함께 설정하여 **정해진 방어 경로를 우회하는 접속을 거부**한다. 따라서 설명의 대상은 라우터나 단일 홈 게이트웨이 각각의 장치가 아니라, 이들을 연계한 전체 방화벽 구성이다.

여기서 단일 홈은 호스트의 네트워크 인터페이스가 하나라는 뜻이다. 이중 홈 게이트웨이는 두 네트워크 인터페이스로 내부망과 외부망에 각각 연결되는 호스트를 이용하므로, 지문의 **단일 홈 호스트와 별도의 스크리닝 라우터를 결합**한 구성과 구별된다.

NoteBase

**문 3. OSI 7계층과 각 계층에서 송수신되는 프로토콜 데이터 단위(PDU)를 바르게 연결한 것은?**

ㄱ. 전송 계층 ㄴ. 네트워크 계층 ㄷ. 데이터링크 계층

① ㄱ: 프레임, ㄴ: 세그먼트, ㄷ: 패킷
② ㄱ: 프레임, ㄴ: 패킷, ㄷ: 세그먼트
③ ㄱ: 세그먼트, ㄴ: 프레임, ㄷ: 패킷
④ ㄱ: 세그먼트, ㄴ: 패킷, ㄷ: 프레임

**정답 4번**

**간단한 해설**

계층별 PDU는 전송 계층의 **세그먼트**, 네트워크 계층의 **패킷**, 데이터링크 계층의 **프레임**으로 연결된다. 송신 측에서는 하위 계층으로 내려가면서 각 계층의 제어 정보를 덧붙인다.

**대응 관계 해설**

PDU는 각 계층의 프로토콜이 송수신하는 데이터 단위이다. 같은 응용 데이터라도 어느 계층에서 처리하는지에 따라 제어 정보와 단위의 명칭이 달라진다.

ㄱ. 전송 계층 → 세그먼트: 전송 계층은 종단의 응용 프로세스 사이에서 데이터를 전달한다. 대표적으로 TCP는 데이터를 나누고 포트 번호, 순서 번호 등의 제어 정보를 담은 헤더를 붙여 **세그먼트**를 만든다.

ㄴ. 네트워크 계층 → 패킷: 네트워크 계층은 목적지까지 데이터를 전달하기 위한 주소 지정과 경로 선택을 담당한다. IP에서는 상위 계층의 데이터에 출발지·목적지 IP 주소 등을 담은 헤더를 붙여 **패킷**을 만든다.

ㄷ. 데이터링크 계층 → 프레임: 데이터링크 계층은 직접 연결된 구간에서 데이터를 전달한다. 네트워크 계층의 패킷에 해당 링크에서 사용하는 제어 정보를 붙여 **프레임**을 만든다. 예를 들어 이더넷 프레임에는 출발지·목적지 MAC 주소와 오류 검출을 위한 정보가 포함된다.

따라서 ㄱ은 세그먼트, ㄴ은 패킷, ㄷ은 프레임으로 연결되며, 이는 ④의 대응과 일치한다.

NoteBase

**문 4. ㉠~㉣에 들어갈 윈도우 명령어를 바르게 연결한 것은?**

○ (㉠)은(는) 도메인 네임을 얻거나 IP주소 매핑을 확인하기 위해 DNS에 질의할 때 사용하는 명령
○ (㉡)은(는) 지정한 IP주소의 통신 장비 접속성을 확인하기 위한 명령
○ (㉢)은(는) 패킷이 목적지까지 도달하는 동안 거쳐 가는 라우터의 IP주소를 확인하는 명령
○ (㉣)은(는) 전송 프로토콜, 라우팅 테이블, 네트워크 인터페이스, 네트워크 프로토콜 통계를 위한 네트워크 연결 상태를 보여주는 명령

① ㉠: ping, ㉡: tracert, ㉢: netstat, ㉣: nslookup
② ㉠: nslookup, ㉡: ping, ㉢: netstat, ㉣: tracert
③ ㉠: ping, ㉡: nslookup, ㉢: tracert, ㉣: netstat
④ ㉠: nslookup, ㉡: ping, ㉢: tracert, ㉣: netstat

**정답 4번**

**간단한 해설**

DNS에 이름·주소 정보를 질의하는 명령은 **nslookup**이다. 목적지의 접속 가능성을 확인하는 ping과 달리, **tracert는 경유 라우터를 추적**한다.

**빈칸별 해설**

㉠ nslookup: **DNS 서버에 질의**하여 도메인 이름에 대응하는 IP주소 등을 조회한다. 역방향 조회를 지원하는 DNS 정보가 있으면 IP주소에 대응하는 도메인 이름도 확인할 수 있다.

㉡ ping: 대상에 ICMP 에코 요청을 보내고 에코 응답이 돌아오는지 확인하여 **IP 수준의 접속 가능성**을 점검한다. 응답 시간과 패킷 손실도 확인할 수 있지만, 목적지까지 거치는 라우터 목록을 보여주는 명령은 아니다.

㉢ tracert: 패킷의 TTL 값을 점차 늘려 보내면서 중간 라우터의 응답을 이용해 **목적지까지의 경로**를 추적한다. 응답한 각 홉의 IP주소와 응답 시간을 표시하므로 경유 라우터를 확인하는 설명에 해당한다.

㉣ netstat: **네트워크 연결 상태와 통계**를 표시한다. 기본적으로 활성 연결을 확인하며, 옵션에 따라 라우팅 테이블(-r), 네트워크 인터페이스의 이더넷 통계(-e), 프로토콜별 통계(-s) 등을 확인할 수 있다.

㉠~㉣에 들어갈 명령은 각각 nslookup, ping, tracert, netstat이며, ④의 연결과 일치한다.

NoteBase

**문 5. IPsec에 대한 설명으로 옳지 않은 것은?**

① AH(Authentication Header)－IP 패킷에 대한 인증과 무결성을 제공하지만, 기밀성은 제공하지 않는다.

② ESP(Encapsulating Security Payload)－IP 패킷에 대한 기밀성, 인증, 무결성을 제공하며 IPsec의 전송 모드와 터널 모드에서 모두 동작 가능하다.

③ IKE(Internet Key Exchange)－IPsec의 보안 연관(security association)을 수립하고 필요한 보안키 교환 기능을 제공하지만, 인증서를 통한 개체 인증은 제공하지 않는다.

④ MIB(Management Information Base)－IPsec의 보안 정책이나 관리 정보를 저장하는 데 사용될 수 있는 자료구조이다.

**정답 3번**

**간단한 해설**

IKE는 보안 연관을 수립하고 키 교환을 수행할 뿐 아니라, **인증서와 전자서명을 이용한 개체 인증도 지원**한다. 따라서 '인증서를 통한 개체 인증은 제공하지 않는다'는 설명이 잘못되었다.

**선지별 해설**

① O: AH는 수신한 데이터가 전송 중 변조되지 않았는지 확인하는 무결성과 데이터 출처 인증을 제공한다. 그러나 **데이터를 암호화하지 않으므로 기밀성은 제공하지 않는다**. 즉, 변조 여부를 확인하는 기능과 내용을 숨기는 기능은 구별해야 한다.

② O: ESP는 암호화를 통한 기밀성과 데이터 출처 인증·무결성을 제공할 수 있다. 실제 제공되는 보안 서비스는 보안 연관을 수립할 때 선택한 알고리즘과 설정에 따라 달라진다. **전송 모드와 터널 모드를 모두 지원**하며, 전송 모드는 주로 원래 IP 패킷의 상위 계층 데이터를 보호하고 터널 모드는 원래 IP 패킷 전체를 새 IP 패킷 안에 넣어 보호한다.

③ X: IKE는 IPsec 통신에 사용할 보안 연관(SA)을 협상하고 필요한 키 교환을 수행한다. 보안 연관은 사용할 보안 알고리즘·키 등 보안 처리에 필요한 매개변수를 정한 것이다. IKE는 **인증서 기반 개체 인증도 지원**한다. 인증서의 유효성을 확인하고 그 인증서에 담긴 공개키로 상대방의 전자서명을 검증하여, 상대방이 해당 개인키를 보유한 통신 주체인지 확인할 수 있다. 따라서 '인증서를 통한 개체 인증은 제공하지 않는다'를 '인증서를 통한 개체 인증도 지원한다'로 고쳐야 한다.

④ O: MIB는 장비의 관리 대상 정보를 체계적으로 정의한 관리 객체들의 집합으로, 논리적인 관리 정보 저장소이다. IPsec의 보안 정책 데이터베이스(SPD)를 설정·관리하는 MIB도 정의되어 있으므로, **IPsec의 보안 정책이나 관리 정보를 표현·관리하는 데 사용**할 수 있다. 관리 시스템은 SNMP 등을 통해 이러한 관리 객체에 접근한다.

NoteBase

**문 6. 다음에서 설명하는 스위치 패킷 전송 방식은?**

수신한 프레임의 목적지 주소를 확인하고 목적지 주소의 포트로 프레임을 즉시 전송하는 방식으로 지연 시간이 최소화되나 수신한 프레임에 오류가 발생할 때는 목적지 장치에서 폐기하는 방식이다.

① 컷스루 방식(cut-through)
② 저장 후 전송 방식
③ 반이중 방식
④ 전이중 방식

**정답 1번**

**간단한 해설**

컷스루 방식은 **목적지 주소를 확인하면 프레임 전체를 받기 전에 전송을 시작**하여 지연을 줄인다. 전송 전에 프레임 전체의 오류를 검사하지 않으므로 오류 프레임도 전달될 수 있다.

**공통 해설**

컷스루 방식(cut-through)은 수신 중인 프레임의 목적지 MAC 주소를 읽어 출력 포트를 결정하면, **프레임 전체의 수신이 끝나기 전에 전달을 시작**하는 방식이다. 나머지 부분을 받는 동안 앞부분을 내보낼 수 있어, 프레임 전체를 받은 뒤 전달하는 저장 후 전송 방식보다 대기 시간이 짧다.

프레임의 오류를 검사하는 FCS는 프레임 끝에 있으므로, 컷스루 방식에서는 오류 검사 결과를 확인하기 전에 전송이 시작될 수 있다. 이 때문에 오류 프레임도 전달될 수 있으며, 이를 받은 목적지 장치가 오류를 검사하여 폐기한다. 지문의 즉시 전송, 짧은 지연 시간, 오류 프레임의 전달은 모두 이러한 **수신 완료 전 전달**이라는 작동 원리에서 나온다.

NoteBase

**문 7. 네트워크 접근 제어(NAC) 시스템에 대한 설명으로 옳지 않은 것은?**

① 네트워크에 접근하는 단말기의 보안정책 준수 여부를 검사하여 네트워크 접속을 통제할 수 있다.

② 보안정책에서 필요에 따라 특정 단말기에 보안 소프트웨어 설치를 유도할 수 있다.

③ DHCP를 이용한 방식은 공인인증서 기반으로 단말기에 URL을 할당하여 네트워크 접속을 통제한다.

④ 네트워크 접근 시 인증을 위해 Active Directory, Kerberos, LDAP 등을 사용한다.

**정답 3번**

**간단한 해설**

DHCP 기반 NAC는 단말기의 보안정책 준수 여부에 따라 **IP 주소와 네트워크 설정**을 할당하여 접근을 통제한다. '공인인증서 기반으로 URL을 할당한다'는 설명은 DHCP 기반 통제의 원리가 아니다.

**선지별 해설**

① O: NAC는 네트워크에 접속하려는 단말기가 조직의 보안정책을 충족하는지 검사한다. 백신 설치 여부나 보안 업데이트 상태 등을 확인하고, **검사 결과에 따라 접속을 허용하거나 제한**할 수 있다.

② O: NAC는 정책에 미달한 단말기가 필요한 보안조치를 수행하도록 유도할 수 있다. 예를 들어 백신이 설치되지 않은 단말기의 접근을 제한하면서 **백신 설치 안내나 설치 페이지**를 제공하고, 설치 후 정책 준수 여부를 다시 확인할 수 있다.

③ X: DHCP는 단말기에 IP 주소와 필요한 네트워크 설정을 자동으로 제공하는 프로토콜이다. DHCP 기반 NAC는 보안상태 검사 결과에 따라 정상적인 접근이 가능한 설정 또는 접근이 제한되는 설정을 제공한다. 정책을 충족하지 못한 단말기는 보안조치를 위한 서버에만 접근하도록 제한할 수 있다. 따라서 선지의 설명은 **공인인증서 기반 URL 할당이 아니라 IP 주소 및 네트워크 설정을 통한 접근 통제**로 고쳐야 한다.

④ O: NAC는 **기존 계정·인증 체계와 연동**하여 사용자나 단말기의 신원을 확인할 수 있다. Active Directory는 계정 정보를 관리하는 디렉터리 서비스이고, Kerberos는 티켓을 이용하는 인증 프로토콜이다. LDAP는 디렉터리 정보에 접근하는 프로토콜로, 계정 조회와 인증 연동에 활용할 수 있다. 이들은 단말기의 보안상태 검사와 함께 네트워크 접근 여부를 결정하는 데 사용될 수 있다.

NoteBase

**문 8. 안전한 해시함수(SHA)에 대한 설명으로 옳은 것은?**

① 한 블록을 처리할 때 SHA-512는 SHA-384보다 많은 라운드(round)를 거친다.

② SHA-1의 메시지 다이제스트(message digest) 길이는 160 bits이다.

③ SHA-256의 입력메시지 최대 길이는 $2^{128}$ bits이다.

④ SHA-512의 입력메시지 최대 길이는 $2^{512}$ bits이다.

**정답 2번**

**간단한 해설**

메시지 다이제스트는 해시함수가 입력 메시지를 처리해 만든 고정 길이의 출력값이다. SHA-1은 입력 메시지의 길이와 관계없이 **160비트**의 다이제스트를 생성한다.

**선지별 해설**

① X: SHA-512와 SHA-384는 한 블록을 처리할 때 **모두 80라운드**를 거친다. 두 알고리즘은 같은 블록 처리 구조를 사용하며, 초기 해시값과 최종 출력 방식이 다르다. 출력 길이가 각각 512비트와 384비트라는 차이를 라운드 수의 차이로 해석해서는 안 된다.

② O: SHA-1의 메시지 다이제스트 길이는 **160비트로 고정**된다. 다이제스트는 입력 메시지 자체가 아니라 해시 연산의 결과이므로, 입력 메시지가 길어져도 출력 길이는 늘어나지 않는다.

③ X: SHA-256이 처리하는 원래 입력 메시지의 길이는 $2^{64}$비트 미만이며, 비트 단위 최대 길이는 $2^{64}-1$ 비트이다. 메시지에 패딩을 붙일 때 **원래 메시지의 길이를 64비트로 기록**하므로 이 범위를 갖는다. $2^{128}$비트 미만이라는 입력 길이 범위는 SHA-384와 SHA-512에 해당한다.

④ X: SHA-512의 원래 입력 메시지 길이는 $2^{128}$비트 미만이며, 비트 단위 최대 길이는 $2^{128}-1$비트이다. 패딩 과정에서 원래 메시지의 길이를 128비트로 기록한다. 이름의 **512는 다이제스트의 비트 수**이며, 입력 메시지 길이의 지수를 뜻하지 않는다.

NoteBase

**문 9. TCP 헤더의 제어용 플래그(control flags, 1: on, 0: off) 6 bits에 할당된 값 010001이 의미하는 것은?**

① SYN(synchronization)과 RST(reset) 값이 1이다.

② ACK(acknowledgment)와 FIN(finish) 값이 1이다.

③ URG(urgent)와 PSH(push) 값이 1이다.

④ SYN(synchronization)과 PSH(push) 값이 1이다.

**정답 2번**

**간단한 해설**

TCP의 6비트 제어 플래그는 왼쪽부터 URG·ACK·PSH·RST·SYN·FIN 순서이다. 010001에서 1인 두 번째와 여섯 번째 비트는 각각 **ACK와 FIN**에 해당한다.

**공통 해설**

문제에서 제시한 6비트 제어 플래그는 왼쪽부터 **URG·ACK·PSH·RST·SYN·FIN** 순서로 배치된다. 각 비트는 해당 플래그의 상태를 나타내며, 1이면 켜지고 0이면 꺼진다.

010001을 이 순서에 맞추면 URG = 0, ACK = 1, PSH = 0, RST = 0, SYN = 0, FIN = 1이다. 따라서 ACK와 FIN만 켜져 있으며, 나머지 후보에 제시된 SYN·RST·URG·PSH는 모두 꺼져 있다.

ACK가 1이면 **확인응답 번호 필드가 유효**하다는 뜻이고, FIN이 1이면 **송신자가 더 보낼 데이터가 없음**을 뜻한다. 즉, 확인응답 번호가 유효하면서 송신 방향의 데이터 전송 종료를 알리는 세그먼트이다.

NoteBase

**문 10. 무선랜 보안에 대한 설명으로 옳은 것만을 모두 고른 것은?**

ㄱ. 802.11b에서 사용된 WEP는 RC4 암호화 알고리즘을 기본으로 사용한다.
ㄴ. WEP는 사전에 공유된 비밀키를 인증에 사용한다.
ㄷ. RADIUS 프로토콜은 엑세스 포인트(access point)와 무선 단말기 사이에 사용되는 프로토콜이다.
ㄹ. 802.1X는 포트 기반 접근제어 기능을 제공하며 인증자(authenticator)는 RADIUS 서버이다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

**정답 1번**

**간단한 해설**

RADIUS는 무선 단말기와 AP 사이가 아니라 **AP와 인증 서버 사이**에서 사용된다. 802.1X에서 AP는 접속을 통제하는 **인증자**이고, RADIUS 서버는 인증을 처리하는 인증 서버이다.

**보기별 해설**

ㄱ. O: 802.11b에서 사용된 WEP는 **RC4 스트림 암호**를 사용한다. 공유 비밀키와 초기화 벡터(IV)를 바탕으로 키 스트림을 생성하고, 이를 평문과 XOR하여 데이터를 암호화한다.

ㄴ. O: WEP의 **공유키 인증 방식**에서는 AP와 무선 단말기에 미리 설정한 동일한 비밀키를 인증에 사용한다. AP가 보낸 도전 문자열을 단말기가 공유키로 암호화하여 돌려주면 AP가 이를 검증한다. 다만 WEP를 사용하는 환경에서도 개방형 인증을 선택할 수 있으므로, 모든 인증 방식에서 비밀키 소유 여부를 확인한다는 뜻은 아니다.

ㄷ. X: RADIUS는 일반적인 802.1X 무선랜 구성에서 **AP와 RADIUS 인증 서버 사이**에 사용된다. 무선 단말기와 AP 사이에서는 EAPOL로 인증 메시지를 주고받으며, AP가 그 안의 EAP 메시지를 RADIUS 메시지에 담아 인증 서버로 전달한다.

ㄹ. X: 802.1X가 포트 기반 접근제어를 제공한다는 부분은 맞지만, 인증자를 RADIUS 서버라고 한 부분이 틀렸다. 무선 단말기는 인증 요청자(supplicant), **AP는 인증자(authenticator)**, RADIUS 서버는 인증 서버(authentication server)에 해당한다. AP는 인증 서버의 인증 결과에 따라 단말기의 네트워크 접근을 허용하거나 차단한다.

따라서 옳은 보기는 ㄱ, ㄴ이며, ①의 조합에 해당한다.

NoteBase

**문 11. 포트 스캔 공격에 대한 설명으로 옳지 않은 것은?**

① TCP Full Open 스캔에서 대상 시스템의 포트가 열린 경우 공격자는 TCP Three-way handshaking의 모든 과정을 거친다.

② TCP Half Open 스캔에서 대상 시스템의 포트가 열린 경우 공격자가 SYN 세그먼트를 보내면 대상 시스템이 SYN + ACK 세그먼트로 응답하고 공격자는 즉시 RST 세그먼트를 보내 연결을 끊는다.

③ NULL, FIN, XMAS 스캔에서 대상 시스템의 포트가 열린 경우에만 공격자에게 RST 세그먼트가 되돌아오고, 닫힌 경우에는 아무런 응답이 없다.

④ UDP 스캔에서 대상 시스템의 포트가 닫힌 경우 대상 시스템은 공격자에게 ICMP unreachable 패킷을 보내지만, 열린 경우에는 아무런 응답이 없다.

**정답 3번**

**간단한 해설**

③은 포트 상태에 따른 응답을 반대로 설명했다. 표준 TCP 동작을 따르는 NULL·FIN·XMAS 스캔에서는 **닫힌 포트가 RST로 응답**하고, 열린 포트는 응답하지 않는다.

**선지별 해설**

① O: TCP Full Open 스캔은 열린 포트에 대해 **3방향 핸드셰이크를 완료**한다. 공격자의 SYN → 대상의 SYN + ACK → 공격자의 ACK 순서로 TCP 연결을 수립하여 포트가 열려 있음을 확인한다.

② O: TCP Half Open 스캔은 SYN에 대한 SYN + ACK를 받으면 포트가 열려 있다고 판단한다. 이때 마지막 ACK 대신 **RST를 보내 연결 수립을 중단**하므로, 3방향 핸드셰이크를 완료하는 Full Open 스캔과 구별된다.

③ X: NULL은 TCP 플래그를 모두 끄고, FIN은 FIN만, XMAS는 FIN·PSH·URG를 설정하여 보낸다. 표준 TCP 동작을 따르는 대상은 **열린 포트에서는 응답하지 않고, 닫힌 포트에서는 RST로 응답**한다. 선지는 이 관계를 뒤바꾸었다. 다만 TCP 구현에 따라 반응이 다를 수 있으며, 필터링으로도 응답이 사라질 수 있어 무응답만으로 열린 포트라고 확정하지는 못한다.

④ O: 일반적인 UDP 탐침에서는 닫힌 포트가 **ICMP Port Unreachable** 메시지로 응답하고, 열린 포트는 빈 데이터나 유효하지 않은 요청을 받은 응용 프로그램이 이를 버려 응답하지 않는 경우가 많다. 선지는 이러한 기본 반응을 설명한다. 다만 유효한 서비스 요청에는 열린 포트도 UDP로 응답할 수 있고, 필터링도 무응답을 만들 수 있으므로 '열리면 항상 무응답'이라는 뜻으로 일반화하지 않는다.

NoteBase

**문 12. DoS(Denial of Service) 공격 유형에 해당하는 것은?**

① Eavesdropping 공격

② Man-In-The-Middle 공격

③ Smurf 공격

④ Stealth Scan 공격

**정답 3번**

**간단한 해설**

Smurf 공격은 피해자의 IP 주소를 출발지로 위조하여 보낸 요청에 대한 **다수의 응답을 피해자에게 집중**시킨다. 이 트래픽으로 정상적인 서비스 이용을 방해하므로 DoS 공격에 해당한다.

**공통 해설**

DoS는 정상적인 사용자가 시스템이나 네트워크 서비스를 이용하지 못하게 하여 **가용성을 침해**하는 공격이다. 통신 내용을 알아내는지보다 정상적인 서비스 제공을 방해하는 공격인지가 분류 기준이다.

Smurf 공격은 출발지 IP 주소를 피해자의 주소로 위조한 ICMP Echo Request를 다른 네트워크의 브로드캐스트 주소로 보낸다. 이 요청에 응답하는 여러 호스트의 ICMP Echo Reply가 피해자에게 몰리면서 트래픽이 증폭된다. 그 결과 피해자의 네트워크 대역폭이나 처리 자원이 소모되어 정상적인 통신이 어려워지므로 **서비스 거부 공격**에 해당한다.

Eavesdropping은 통신 내용을 엿듣는 방식이고, Man-In-The-Middle은 통신 당사자 사이에 끼어들어 통신을 가로채거나 조작하는 방식이다. Stealth Scan은 탐지를 피하면서 포트 등의 상태를 조사하는 방식이다. 이들은 각각 도청·통신 개입·정보 수집을 나타내며, 그 자체가 서비스 이용을 마비시키는 DoS 유형을 뜻하지 않는다.

NoteBase

**문 13. 보안 솔루션에 대한 설명으로 옳지 않은 것만을 모두 고른 것은?**

ㄱ. SSO(Single Sign On)는 하나의 인증 시스템을 통해 인증 시스템과 연결된 다른 시스템에 추가적인 인증 과정 없이 로그인하는 기능을 제공한다.
ㄴ. PKI(Public Key Infrastructure)는 네트워크 보안을 제공하기 위해 패킷을 분석하고 정상적인 패턴이 아닌 경우 차단 등의 기능을 제공한다.
ㄷ. FDS(Fraud Detection System)는 다양한 네트워크 기기의 인증을 통합 제어하는 기능을 제공한다.
ㄹ. DRM(Digital Rights Management)은 문서 열람, 편집, 출력 등에 관한 접근 권한을 설정하는 기능을 제공한다.

① ㄱ, ㄷ
② ㄴ, ㄷ
③ ㄴ, ㄹ
④ ㄷ, ㄹ

**정답 2번**

**간단한 해설**

ㄴ의 패킷 분석·차단은 **침입방지시스템(IPS)**의 기능이며, PKI는 공개키와 인증서를 관리하는 기반 구조이다.
ㄷ의 FDS는 기기 인증을 통합 제어하는 것이 아니라 **이상금융거래를 탐지**하는 시스템이다.

NoteBase

**보기별 해설**

ㄱ. O: SSO는 한 번의 로그인으로 얻은 인증 결과를 연계된 여러 시스템에서 활용하는 기능이다. 따라서 사용자는 시스템을 옮길 때마다 **로그인 정보를 다시 입력할 필요가 없다**. 이는 각 시스템이 인증 결과를 확인하지 않는다는 뜻이 아니라, 기존 인증 결과를 공유하여 반복 로그인을 줄인다는 뜻이다.

ㄴ. X: PKI는 **공개키와 인증서의 발급·관리·검증을 위한 기반 구조**이다. 인증서를 통해 공개키와 그 소유자의 신원을 연결하여 신뢰할 수 있는 인증과 통신을 뒷받침한다. 패킷을 분석하여 비정상적인 트래픽을 탐지하고 차단하는 설명은 침입방지시스템(IPS)에 해당한다.

ㄷ. X: FDS는 거래 정보와 이용 패턴 등을 분석하여 **금융사기로 의심되는 이상거래를 탐지**하는 시스템이다. 따라서 '다양한 네트워크 기기의 인증을 통합 제어'한다는 부분을 '이상금융거래를 탐지'하는 기능으로 고쳐야 한다.

ㄹ. O: DRM은 디지털 콘텐츠의 이용 권한을 관리하는 기술이다. 문서에 적용하면 사용자별로 **열람·편집·출력 권한을 구분**하여 설정할 수 있다. 예를 들어 문서를 읽는 것은 허용하면서 편집이나 출력은 제한할 수 있다.

옳지 않은 보기는 ㄴ과 ㄷ이므로, 두 보기를 묶은 ②에 해당한다.

NoteBase

**문 14. 다음에서 설명하는 보안 프로토콜의 특성은?**

공격자에게 비밀키 혹은 패스워드가 노출되더라도 그 후에 키분배 과정을 거쳐 새롭게 생성되는 세션키(session key)를 알 수 없다.

① Inverse Cipher
② Zero-Knowledge Authentication
③ Perfect Forward Secrecy
④ Second Preimage Resistance

**정답 3번**

**간단한 해설**

완전 순방향 비밀성(PFS)은 **장기 비밀정보의 노출이 세션키 노출로 이어지지 않도록** 하는 성질이다. 지문의 새 세션키 보호는 공격자가 키교환에 직접 개입하지 않고 교환 정보를 도청하는 경우를 전제로 이해한다.

**공통 해설**

완전 순방향 비밀성(Perfect Forward Secrecy, PFS)은 장기 비밀키가 나중에 노출되더라도 이전에 안전하게 합의한 세션키를 복원할 수 없게 하는 키 합의 프로토콜의 성질이다. 세션키는 한 통신 세션의 데이터를 보호하는 데 쓰는 키이다. 핵심은 **장기 비밀정보만으로 세션키를 재구성할 수 없게 하는 것**이다.

대표적인 구현 방법은 매 세션마다 새로운 임시 비밀값을 사용하는 디피–헬먼 키교환이다. 양측은 각자의 임시 비밀값과 상대가 보낸 공개값을 이용해 같은 공유 비밀을 계산하고, 여기서 세션키를 도출한다. 공격자는 장기 비밀키나 패스워드를 알아도 임시 비밀값까지 알게 되는 것은 아니므로, 도청한 공개값만으로 세션키를 계산할 수 없다. 사용이 끝난 임시 비밀값과 세션키를 삭제하면 이후 장기 비밀키가 노출되어도 과거 통신을 보호할 수 있다.

지문의 '그 후에 키분배 과정을 거쳐 새롭게 생성되는 세션키를 알 수 없다'는 설명도 이러한 키교환에서 **공격자가 도청만 하는 경우**에 적용할 수 있다. 새 세션에 별도의 임시 비밀값을 사용하므로 노출된 장기 비밀정보만으로는 그 세션키를 알아낼 수 없다는 뜻이다. 다만 장기 인증정보를 얻은 공격자가 상대방을 사칭하여 새 키교환에 직접 개입하는 공격까지 PFS만으로 막는다는 의미는 아니다.

NoteBase

**문 15. 블록암호 운영모드 중 암호화 알고리즘과 복호화 알고리즘이 둘 다 필요한 것은?**

① Cipher Block Chaining

② Cipher Feedback

③ Output Feedback

④ Counter

**정답 1번**

**간단한 해설**

CBC는 평문에 블록암호의 암호화 함수를 적용하여 암호문을 만들고, 이를 되돌릴 때 **복호화 함수**를 사용한다. 따라서 암호화·복호화 두 방향의 함수가 모두 필요하다.

**공통 해설**

이 문제의 암호화·복호화 알고리즘은 운영모드 내부에서 사용하는 블록암호의 순방향 암호화 함수와 그 역함수인 복호화 함수를 뜻한다. 판단 기준은 **평문을 복원할 때 블록암호의 역함수가 필요한가**이다.

CBC(Cipher Block Chaining)는 평문 블록과 직전 암호문 블록을 XOR한 뒤 암호화 함수를 적용한다. 복원할 때는 먼저 해당 암호문 블록에 **복호화 함수를 적용**하고, 그 결과와 직전 암호문 블록을 XOR하여 평문을 얻는다. 첫 블록에서는 직전 암호문 대신 초기화 벡터(IV)를 사용한다. 이처럼 CBC는 암호화 과정과 복호화 과정에서 각각 순방향 함수와 역함수를 사용한다.

CFB(Cipher Feedback), OFB(Output Feedback), CTR(Counter)은 블록암호의 암호화 함수로 XOR에 사용할 비트열을 만든다. 평문과 그 비트열을 XOR하면 암호문이 되고, 암호문에 같은 비트열을 다시 XOR하면 평문이 복원된다. XOR은 같은 비트열로 두 번 적용하면 원래 값으로 돌아오므로, 세 모드에서는 **복호화할 때도 암호화 함수**로 필요한 비트열을 생성하며 블록암호의 복호화 함수는 사용하지 않는다.

NoteBase

**문 16. DNS 서버로부터 얻을 수 있는 레코드 종류와 그 내용이 옳지 않은 것은?**

① NS(Name Server) - 각 도메인에 한 개 이상 있어야 하며, DNS 서버를 가리킨다.

② MX(Mail Exchanger) - 도메인 이름으로 보낸 메일을 받는 호스트 목록을 지정한다.

③ PTR(Pointer) - 도메인 이름에 IP주소를 매핑하는 역할을 한다.

④ CNAME(Canonical Name) - 호스트의 다른 이름을 정의하는 데 사용된다.

**정답 3번**

**간단한 해설**

③은 PTR의 조회 방향을 반대로 설명했다. PTR은 **IP 주소에 대응하는 도메인 이름**을 찾는 역방향 조회에 사용하며, 도메인 이름을 IPv4 주소에 연결하는 것은 A 레코드이다.

**선지별 해설**

① O: NS는 해당 도메인의 DNS 정보를 관리하는 **권한 있는 DNS 서버**를 지정한다. 독립된 DNS 관리 영역인 존(zone)에는 한 개 이상의 NS 레코드가 필요하다. 모든 하위 호스트 이름마다 NS 레코드를 따로 두어야 한다는 뜻은 아니다.

② O: MX는 해당 도메인으로 보내는 메일을 **받아 처리할 메일 서버**를 지정한다. 여러 MX 레코드를 등록하여 수신 서버 목록을 구성할 수 있으며, 각 레코드에는 서버 이름과 우선순위 값이 들어간다. 우선순위 값이 작을수록 먼저 시도한다.

③ X: PTR은 **IP 주소에서 도메인 이름을 찾는 역방향 조회**에 사용한다. 따라서 '도메인 이름에 IP주소를 매핑'한다는 설명은 'IP 주소에 대응하는 도메인 이름을 매핑'하는 것으로 고쳐야 한다. 반대로 도메인 이름에서 IPv4 주소를 찾는 정방향 조회에는 A 레코드를 사용한다.

④ O: CNAME은 호스트의 **별칭을 정식 도메인 이름에 연결**한다. 별칭으로 조회하면 연결된 정식 이름을 따라 필요한 주소 정보를 찾을 수 있다. CNAME 자체가 IP 주소를 직접 저장하는 것은 아니다.

NoteBase

**문 17. TCP 세션 하이재킹(session hijacking) 공격의 보안 대책으로 옳지 않은 것은?**

① Inverse DNS Lookup 탐지

② ACK Storm 탐지

③ 패킷 유실과 재전송 증가 탐지

④ TCP 순서 번호(sequence number) 비동기 상태 탐지

**정답 1번**

**간단한 해설**

Inverse DNS Lookup 탐지는 수집한 패킷의 IP 주소를 이름으로 바꾸려는 DNS 질의를 관찰하여 **스니퍼를 탐지**하는 기법이다. TCP 세션 탈취로 생기는 순서 번호의 비동기 상태를 직접 탐지하는 방법과 구별한다.

**선지별 해설**

TCP 세션 하이재킹은 공격자가 이미 성립한 TCP 연결의 통신 당사자를 가장하여 데이터를 주입하거나 세션을 가로채는 공격이다. 여기서 보안 대책은 공격에 따른 이상 징후를 탐지하는 방법을 포함한다.

① X: Inverse DNS Lookup 탐지는 스니퍼가 수집한 패킷 속 IP 주소의 호스트 이름을 알아내려고 역방향 DNS 질의를 보내는 특성을 이용한다. 따라서 **스니핑 탐지 기법**에 해당하며, TCP 세션 하이재킹 자체의 탐지 방법으로 분류하는 것은 적절하지 않다. 세션 하이재킹은 순서 번호의 비동기 상태나 그에 따른 ACK 이상 등을 감시하여 탐지할 수 있다.

② O: 공격자가 기존 연결에 데이터를 끼워 넣으면 정상 통신 양단이 기억하는 송수신 상태가 어긋날 수 있다. 이때 서로 자신이 기대하는 순서 번호를 알리는 ACK를 반복해서 보내는 **ACK Storm**이 발생할 수 있으므로, 비정상적인 ACK 반복을 탐지하는 것은 세션 하이재킹의 징후를 찾는 방법이다.

③ O: 세션 하이재킹으로 송수신 상태가 어긋나면 정상 패킷이 수신 측에서 폐기되거나 확인 응답을 받지 못할 수 있다. 송신 측은 확인되지 않은 데이터를 다시 보내므로 **패킷 유실과 재전송 증가**를 감시하여 공격 징후를 찾을 수 있다. 다만 이러한 현상은 혼잡이나 통신 장애로도 생길 수 있어 이것만으로 공격을 확정하지는 않는다.

④ O: TCP는 순서 번호로 데이터의 바이트 위치를 구분하고, 확인 응답 번호로 다음에 받을 위치를 알린다. 공격자가 한쪽에 데이터를 주입하면 다른 쪽이 모르는 만큼 순서 번호가 진행하여 **양단의 송수신 상태가 어긋날 수 있다**. 따라서 기존 연결의 순서 번호와 확인 응답 번호가 정상적인 진행 관계를 유지하는지 검사하는 것은 세션 하이재킹 탐지에 적절하다.

NoteBase

**문 18. 인터넷 보안 위협에 대한 설명으로 옳지 않은 것은?**

① 이블 트윈 공격(evil twin attack)은 사회관계망에서 공격 대상의 지인 또는 특정 유명인으로 위장해 공격 대상으로부터 중요한 정보를 획득하는 데 사용된다.

② Man-In-The-Browser 공격은 웹브라우저 내에 악성코드를 설치하여 웹브라우저에서 표시되는 웹페이지 내용을 도청하거나 위·변조하는 공격으로 SSL/TLS 등을 통해 통신구간을 암호화하지 않으면 대응하기 힘들다.

③ 피싱(phishing)이란 진짜 웹사이트와 거의 동일하게 꾸며진 가짜 웹사이트를 통해 개인정보를 탈취하는 것이다.

④ 파밍(pharming)이란 도메인을 탈취하거나 악성코드를 통해 DNS의 이름을 속여 사용자가 진짜 웹사이트로 오인하게 만들어 개인정보를 탈취하는 것이다.

**정답 2번**

**간단한 해설**

Man-In-The-Browser 공격은 **브라우저 내부의 악성코드**가 데이터를 가로채거나 바꾸므로, **SSL/TLS로 통신 구간을 암호화해도 막기 어렵다**. 암호화 전이나 복호화 후의 데이터에 접근할 수 있기 때문이다.

**선지별 해설**

① O: 사회관계망에서의 이블 트윈 공격은 **실제 인물을 사칭하는 가짜 계정**으로 신뢰를 얻어 정보를 수집하는 방식이다. 지인이나 유명인의 이름·사진 등을 흉내 내면 피해자가 진짜 계정으로 믿고 중요한 정보를 제공할 수 있다. 이 문항은 무선 접속점을 사칭하는 경우가 아니라 사회관계망의 계정 사칭을 설명한다.

② X: Man-In-The-Browser 공격은 브라우저에 침투한 악성코드가 웹페이지나 입력·전송 데이터를 가로채거나 변조하는 공격이다. SSL/TLS는 브라우저와 서버 사이의 통신 구간을 보호하지만, 악성코드는 브라우저 안에서 **암호화 전 또는 복호화 후의 데이터**에 접근할 수 있다. 따라서 '암호화하지 않으면 대응하기 힘들다'는 부분은 '통신 구간을 암호화하더라도 대응하기 힘들다'로 고쳐야 한다. 감염된 브라우저의 악성코드를 탐지·제거하는 등 단말 자체를 보호해야 한다.

③ O: 피싱은 신뢰할 수 있는 기관이나 사이트를 사칭하여 사용자가 민감한 정보를 제공하도록 속이는 공격이다. 정상 사이트와 비슷한 **가짜 웹사이트에 정보를 입력하도록 유도**하여 아이디·비밀번호 등을 탈취하는 것은 대표적인 피싱 방식이다.

④ O: 파밍은 도메인이나 DNS의 이름 해석 과정 등을 조작하여 사용자를 가짜 사이트로 연결하는 공격이다. DNS는 도메인 이름에 대응하는 IP 주소를 알려 주므로, 그 결과를 속이면 사용자가 **정상 주소를 입력해도 가짜 사이트로 연결**될 수 있다. 피해자는 해당 사이트를 진짜로 믿고 개인정보를 입력하게 된다.

NoteBase

**문 19. 침입탐지 시스템에 대한 설명으로 옳은 것만을 모두 고른 것은?**

ㄱ. 호스트 기반 침입탐지 시스템은 내부 호스트에서 동작하는 악성코드의 스택 오버플로(stack overflow) 공격을 막기 위해 스택 영역을 실행 불가능하게 만든다.
ㄴ. 오용 탐지(misuse detection)는 정립된 공격패턴을 활용해 제로데이(zero day)와 같은 새로운 형태의 공격을 탐지하는 데 사용된다.
ㄷ. 이상 탐지(anomaly detection)는 호스트 기반과 네트워크 기반 침입탐지 시스템에 모두 적용될 수 있는 탐지 방법으로 오랜 기간 수집된 올바른 사용자 행동패턴을 활용해 통계적으로 공격을 탐지하는 데 사용된다.
ㄹ. False Negative는 실제 공격임에도 공격을 탐지하지 못하는 것을 의미한다.

① ㄱ, ㄴ

② ㄱ, ㄷ

③ ㄴ, ㄷ

④ ㄷ, ㄹ

**정답 4번**

**간단한 해설**

이상 탐지는 **정상 행동 기준에서 벗어나는 활동**을 찾아내는 방식으로, 호스트와 네트워크 양쪽에서 활용할 수 있다. **False Negative는 실제 공격을 놓치는 미탐**을 뜻한다.

NoteBase

**보기별 해설**

ㄱ. X: 호스트 기반 침입탐지 시스템은 호스트의 로그, 파일 변경, 프로세스 활동 등을 감시하여 침입 징후를 탐지한다. 스택 영역을 실행 불가능하게 만드는 것은 **운영체제와 프로세서의 메모리 보호 기능**이며, DEP나 NX가 이에 해당한다. 이는 스택에 삽입된 코드의 실행을 막는 대책으로, 호스트 기반 침입탐지 자체의 기능과 구별해야 한다.

ㄴ. X: 오용 탐지는 관찰된 활동을 **이미 알려진 공격패턴**과 대조하는 방식이므로, 알려진 공격을 탐지하는 데 효과적이다. 반면 제로데이처럼 대응 패턴이 아직 마련되지 않은 새로운 공격은 탐지하기 어렵다. 정상 행동 기준에서 벗어나는지를 살펴 새로운 공격의 징후를 탐지하는 방식은 이상 탐지이다.

ㄷ. O: 이상 탐지는 일정 기간 수집한 정상 활동으로 행동 기준을 만들고, 현재 활동이 그 기준에서 통계적으로 크게 벗어나면 공격 가능성을 판단한다. 호스트의 로그인·프로세스 활동과 네트워크의 트래픽 특성 모두에 적용할 수 있다. **호스트 기반·네트워크 기반은 관찰 대상에 따른 구분**이고, 이상 탐지는 탐지 방법에 따른 구분이므로 서로 배타적인 분류가 아니다.

ㄹ. O: False Negative는 실제로 공격이 발생했는데도 탐지 시스템이 이를 공격으로 식별하지 못한 **미탐**이다. 반대로 정상 활동을 공격으로 잘못 판단하는 것은 False Positive, 즉 오탐이다.

옳은 보기는 ㄷ과 ㄹ이며, 이를 모두 묶은 선택지는 ④이다.

NoteBase

**문 20. 다음에서 설명하는 웹 보안 취약점은?**

악성 스크립트가 포함된 웹사이트에 방문한 사용자가 악성 스크립트에 의해 공격자가 의도한 행위를 수행하는 것이다. 이러한 악성 스크립트는 사용자의 웹브라우저에서 실행되지 않고 웹사이트에서 실행된다.

① SQL 명령 삽입
② 안전하지 않은 직접 객체 참조
③ 취약한 인증 및 세션 관리
④ 크로스 사이트 요청 변조

**정답 4번**

**간단한 해설**

크로스 사이트 요청 변조(CSRF)는 **사용자의 인증 상태를 악용**하여 의도하지 않은 요청을 보내게 하고, 웹사이트가 이를 정상 요청으로 받아들여 처리하게 하는 공격이다.

**공통 해설**

크로스 사이트 요청 변조(CSRF)는 사용자가 로그인한 웹사이트에 본인이 의도하지 않은 요청을 보내도록 유도하는 공격이다. 세션 쿠키가 자동으로 첨부되는 요청에서는 공격자가 쿠키 값을 몰라도 사용자의 브라우저를 통해 인증된 요청을 보낼 수 있다. 웹사이트가 요청의 진위를 별도로 확인하지 않으면 이를 사용자가 직접 보낸 요청으로 받아들인다. 따라서 판단 기준은 **인증된 사용자의 권한을 이용해 원치 않는 요청을 처리하게 하는가**이다.

예를 들어 사용자가 어떤 서비스에 로그인한 상태에서 악성 페이지를 열었을 때, 그 페이지가 해당 서비스로 이메일 주소 변경 요청을 보내도록 유도할 수 있다. 이 요청에 사용자의 세션 쿠키가 첨부되고 서비스가 위조 요청을 걸러 내지 못하면, 사용자가 의도하지 않은 이메일 주소 변경이 이루어진다. 지문의 '공격자가 의도한 행위를 수행'한다는 설명은 이러한 CSRF의 작동 방식에 해당한다.

다만 지문의 '웹브라우저에서 실행되지 않고 웹사이트에서 실행된다'는 표현은 엄밀한 스크립트 실행 위치 설명으로 받아들이면 부정확하다. CSRF에서는 브라우저가 위조 요청을 보내고 서버가 그 요청에 따른 동작을 처리한다. **악성 스크립트가 서버에서 실행되어야 하는 것은 아니다**.

NoteBase