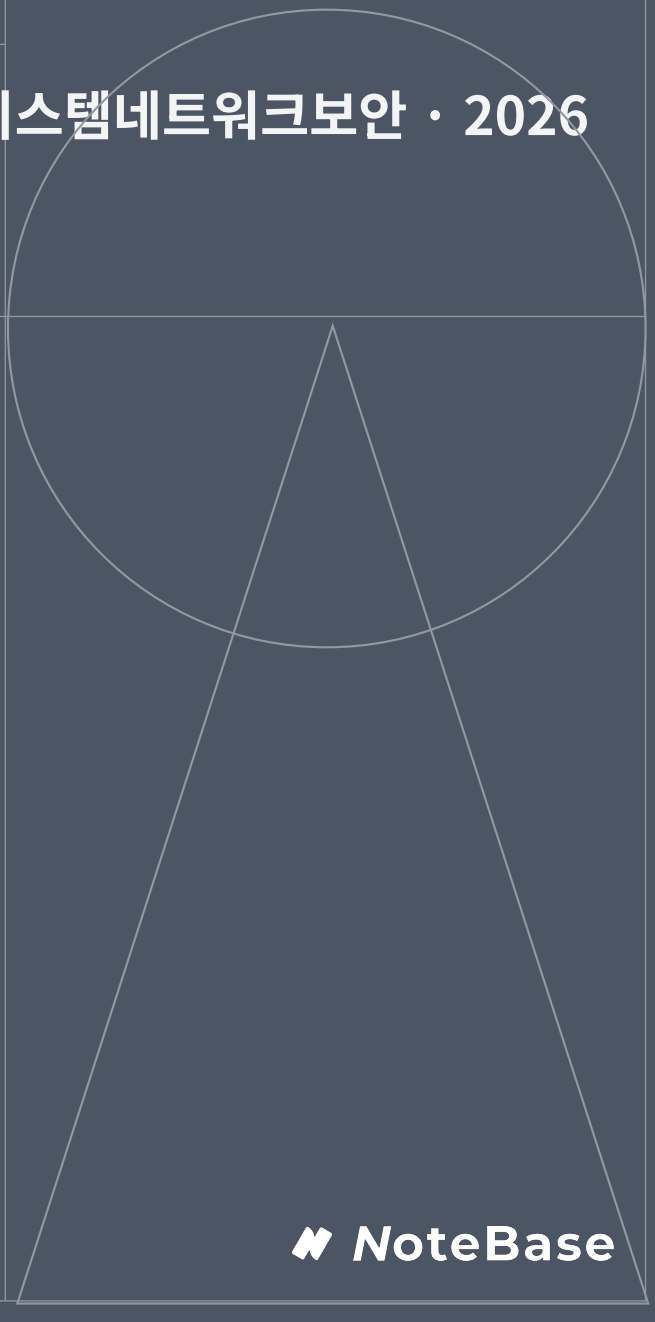
기출OX 해설집

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2026



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2026

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2026

문 1. OSI 참조모델의 각 계층에서 사용하는 프로토콜로 가장 적절하지 않은 것은?

① 데이터링크 계층 : X.25, DNS

② 네트워크 계층 : ARP, IGMP

③ 전송 계층 : TCP, UDP

④ 응용 계층 : HTTP, SNMP

정답 1번

간단한 해설

DNS는 이름과 주소 등의 정보를 조회하는 **응용 계층 프로토콜**이므로 데이터링크 계층으로 분류할 수 없다. X.25는 구성 프로토콜별 계층을 구분하고, ARP는 분류 체계에 따라 계층 표기가 달라질 수 있다는 점에 주의한다.

NoteBase

선지별 해설

① X: **DNS는 응용 계층 프로토콜**이므로 데이터링크 계층으로 묶을 수 없다. DNS는 도메인 이름과 IP 주소 등의 정보를 조회하는 데 사용된다. X.25는 하위 계층에 걸친 규격으로, 그중 패킷 계층 프로토콜인 PLP는 네트워크 계층, LAPB는 데이터링크 계층에 해당한다. 따라서 X.25 전체를 단일 계층과 무조건 동일시하기보다 구성 프로토콜을 구분해야 하며, 이 선지는 특히 DNS의 분류가 명백히 잘못되었다.

② O: 이 문항은 ARP를 네트워크 계층의 주소 해석을 지원하는 프로토콜로 묶는 분류를 따른다. ARP는 같은 링크에서 IP 주소에 대응하는 MAC 주소를 알아내고, IGMP는 IPv4 멀티캐스트 그룹의 가입 정보를 호스트와 인접 라우터 사이에서 관리한다. 다만 **ARP는 계층 경계에 걸친 기능**이 있어 TCP/IP 모델에서는 링크 계층으로 분류하기도 한다. 모든 분류 체계에서 ARP가 반드시 OSI 3계층에 속한다고 일반화해서는 안 된다.

③ O: TCP와 UDP는 **전송 계층**에서 응용 프로세스 사이의 통신을 지원한다. TCP는 연결 지향 방식으로 순서와 신뢰성 있는 전달을 제공하고, UDP는 비연결 데이터그램 방식으로 전달하며 자체적으로 재전송이나 순서 보장을 제공하지 않는다.

④ O: HTTP와 SNMP는 **응용 계층** 프로토콜이다. HTTP는 웹 자원 등에 관한 요청과 응답의 의미를 정의하고, SNMP는 네트워크 장비의 관리 정보를 조회·설정하거나 통지를 주고받는 데 사용된다.

NoteBase

문 2. 다음 빈칸 (㉠)~(㉣)에 들어갈 용어로 가장 적절한 것은?

가상 메모리 관리 기법에서 메모리의 크기를 고정 크기로 분할하여 관리하는 것은 (㉠)이고, 가변 크기로 관리하는 것은 (㉡)이다. (㉠)으로 가상 메모리를 관리하면 메모리 단편화 중에서 (㉢)가 발생하고, (㉡)으로 가상 메모리를 관리하면 (㉣)가 발생한다.

① (㉠): 페이징, (㉡): 세그먼테이션, (㉢): 내부단편화, (㉣): 외부단편화

② (㉠): 페이징, (㉡): 세그먼테이션, (㉢): 외부단편화, (㉣): 내부단편화

③ (㉠): 세그멘테이션, (㉡): 페이징, (㉢): 내부단편화, (㉣): 외부단편화

④ (㉠): 세그멘테이션, (㉡): 페이징, (㉢): 외부단편화, (㉣): 내부단편화

정답 1번

간단한 해설

페이징은 **고정 크기**로 나누므로 할당 공간 안에 남는 내부단편화가 발생할 수 있다. 세그먼테이션은 **가변 크기**로 나누므로 할당 영역 사이에 빈틈이 흩어지는 외부단편화가 발생할 수 있다.

빈칸별 해설

㉠ 페이징: 프로세스의 가상 주소 공간을 일정한 크기의 페이지로 나누고 물리 메모리도 같은 크기의 프레임으로 나누어 대응시킨다. 따라서 **고정 크기 단위**로 메모리를 관리한다는 조건에 해당한다.

㉡ 세그먼테이션: 프로그램을 코드·데이터·스택 등 논리적인 단위인 세그먼트로 구분한다. 세그먼트의 길이는 각각의 필요에 따라 달라지므로 **가변 크기 단위**로 관리한다는 조건에 해당한다.

㉢ 내부단편화: 페이징에서는 마지막 페이지에 담을 내용이 페이지 크기보다 작더라도 한 프레임을 할당한다. 그 결과 **할당된 공간 내부에 사용하지 않는 부분**이 생길 수 있다. 예를 들어 페이지 크기가 4 KB인데 마지막 페이지에 저장할 내용이 1 KB이면 그 프레임 안의 3 KB가 남는다. 이는 원문 수치가 아닌 설명용 예이다.

㉣ 외부단편화: 순수 세그먼테이션에서는 크기가 다른 세그먼트를 할당하고 해제하면서 **할당 영역 사이에 작은 빈 공간**이 흩어질 수 있다. 빈 공간의 총합이 충분해도 필요한 크기의 연속 영역이 없으면 새 세그먼트를 배치하기 어렵다. 고정 크기 프레임을 사용하는 페이징에서는 이러한 형태의 외부단편화를 피할 수 있다.

㉠부터 차례대로 페이징, 세그먼테이션, 내부단편화, 외부단편화가 들어가므로 ①과 일치한다.

NoteBase

문 3. 리눅스 시스템에서 슈퍼유저의 권한으로 명령을 실행하기 위한 sudo 명령의 기본 보안 정책이 저장된 파일로 가장 적절한 것은?

① /etc/passwd

② /etc/shadow

③ /etc/groups

④ /etc/sudoers

정답 4번

간단한 해설

sudo의 기본 파일 기반 보안 정책은 **/etc/sudoers**에 정의한다. 이 파일은 사용자·그룹별로 실행할 수 있는 명령과 사용할 권한 등을 정한다.

핵심 풀이

sudo는 허가된 사용자가 다른 사용자의 권한으로 명령을 실행하게 하는 도구이며, 일반적으로 root 권한 실행에 많이 사용된다. 기본 sudoers 정책을 파일로 관리할 때 사용하는 주 설정 파일은 /etc/sudoers이다.

/etc/sudoers에는 어떤 사용자나 그룹이 어느 호스트에서 어떤 사용자 권한으로 어떤 명령을 실행할 수 있는지 등의 정책을 지정한다. 계정 정보 자체를 저장하는 파일이 아니라 권한 위임과 실행 허용 범위를 정하는 파일이다.

/etc/passwd는 사용자 이름·사용자 ID·홈 디렉터리·로그인 셸 등 계정 정보를,

/etc/shadow는 비밀번호 해시와 만료 관련 정보 등을 다룬다.

일반적인 그룹 정보 파일명은 /etc/group이며, 선지의 /etc/groups와 다르다. 이들은 기본 sudo 실행 허용 정책 파일이 아니다.

따라서 /etc/sudoers인 ④에 해당한다. 환경에 따라 별도 포함 파일이나 다른 정책 저장방식을 사용할 수도 있지만, 문항이 묻는 기본 파일은 /etc/sudoers이다.

NoteBase

문 4. 다음에서 설명하는 작업 스케줄 관리 명령어로 가장 적절한 것은?

예약한 명령어를 정해진 시간에 한 번만 실행할 때 사용하는 명령어이다.

① at
② find
③ cron
④ lsattr

정답 1번

간단한 해설

at은 명령을 예약하여 **지정한 시각에 한 번 실행**하도록 하는 명령어이다. 지문의 '한 번만 실행'이 핵심 조건이다.

공통 해설

at은 실행할 명령과 시각을 지정하여 **일회성 작업을 예약**하는 명령어이다. 작업을 미리 등록하면 예약한 시각에 실행되므로, 사용자가 그때 직접 명령을 입력할 필요가 없다. 예를 들어 내일 오후 2시에 한 번 실행할 작업을 예약하는 경우에 해당한다.

지문은 정해진 시각에 한 번 실행하는 작업을 묻는다. 주기적인 반복 실행을 예약하는 cron과 구별되며, find와 lsattr도 이러한 일회성 작업 예약에 해당하는 명령어가 아니다. 따라서 지문의 설명은 at에 대응한다.

NoteBase

문 5. 다음에서 설명하는 ICMP 오류 보고 메시지로 가장 적절한 것은?

◯ 이 메시지는 IP의 흐름제어와 혼잡제어 기능과 유사한 기능을 추가하기 위하여 설계되었다.
◯ 라우터나 호스트가 혼잡으로 인해 데이터그램을 폐기하게 되면, 데이터그램의 송신자에게 이 메시지를 보내게 되고, 이 메시지를 받은 송신자는 전송을 잠시 중단하거나 전송률을 줄이는 등의 조치를 하여야 한다.

① Redirect 메시지
② Source Quench 메시지
③ Destination Unreachable 메시지
④ Time Exceeded 메시지

정답 2번

간단한 해설

혼잡으로 데이터그램을 폐기한 뒤 송신률을 줄이도록 알린다는 것은 Source Quench의 역사적 기능이다. 경로 변경이나 목적지 도달 실패, 시간 초과를 알리는 메시지와 구별한다.

대응 관계 해설

첫 번째 설명과의 대응: IP 자체는 신뢰성 있는 전달이나 송신률 조절을 보장하지 않는다. **Source Quench**는 혼잡을 알리고 송신 속도를 낮추도록 요청하기 위해 과거 ICMP에 마련된 메시지이다. 제시문의 흐름제어·혼잡제어와 유사한 기능이라는 설명은 이러한 보완 목적을 가리킨다.

두 번째 설명과의 대응: 라우터나 호스트의 처리 부담으로 데이터그램이 버려지면, 원래의 송신자에게 혼잡을 알리고 전송률을 줄이도록 한다는 것이 Source Quench의 역사적 동작이다. 핵심 단서는 **혼잡으로 인한 폐기 → 송신자에게 통보 → 송신률 감소**이다.

다른 메시지와의 구분: ① Redirect는 특정 목적지로 가는 더 적절한 다음 홉을 송신 호스트에 알려 주는 메시지이다.

③ Destination Unreachable은 네트워크·호스트·포트 등에 도달할 수 없는 사유를 알린다.

④ Time Exceeded는 TTL 소진이나 단편 재조립 시간 초과를 알린다. 이들은 혼잡을 이유로 송신률을 낮추도록 하는 Source Quench와 목적이 다르다.

두 설명이 함께 가리키는 메시지는 Source Quench이므로, 이에 해당하는 선택지는 ②이다.

NoteBase

관련 개념 정리

Source Quench는 현재 사용하는 혼잡 제어 방식으로 이해하면 안 된다. RFC 6633은 이 메시지에 반응하는 동작을 폐기했으며, 수신한 전송 프로토콜은 이를 무시하도록 규정한다. 이 문제는 **과거에 정의된 메시지의 기능**을 묻는 것으로 읽어야 한다.

NoteBase

문 6. 다음에서 설명하고 있는 HTTP 메소드로 가장 적절한 것은?

이 요청에 대한 응답은 원본 HTTP 요청의 사본을 포함하므로 클라이언트는 중간 서버로 변경된 내용을 확인할 수 있다. 일반적으로 웹 서버에서 이 요청은 보안 허점 역할을 할 수 있기 때문에 해제하는 것이 좋다.

① HEAD
② TRACE
③ OPTIONS
④ CONNECT

정답 2번

간단한 해설

TRACE는 서버가 받은 요청을 응답에 되돌려 보내는 **루프백 진단 메서드**이다. 클라이언트가 중간 전달 과정의 변경을 확인할 수 있지만, 민감한 정보의 반사·노출을 주의해야 한다.

대응 관계 해설

요청 사본을 되돌려 확인하는 기능은 TRACE에 대응한다. 최종 수신자가 받은 요청 메시지를 응답 내용으로 돌려보내는 루프백 방식이므로, 클라이언트는 보낸 내용과 비교하여 **중간 프록시 등을 거치며 달라진 부분**을 진단할 수 있다. 원본을 무조건 한 글자도 빠짐없이 돌려줘야 한다는 뜻은 아니다.

보안상 주의도 이 반사 기능과 연결된다. 요청에 민감한 정보가 들어 있으면 응답으로 노출될 우려가 있으므로 TRACE 요청에 인증정보나 쿠키 같은 민감한 필드를 넣지 않아야 하고, 수신자는 민감한 필드를 응답에서 제외해야 한다. 운영상 진단 용도가 없다면 불필요한 노출을 줄이기 위해 비활성화하는 취지이다.

HEAD는 GET과 같은 종류의 응답 메타데이터를 얻되 응답 내용을 보내지 않으며, OPTIONS는 대상에서 지원하는 통신 옵션을 확인한다. CONNECT는 대상 서버로의 터널을 설정한다. 어느 것도 받은 요청 메시지를 되돌려 경로상의 변경을 확인하는 기능 자체를 뜻하지 않는다.

따라서 제시된 기능과 보안상 주의에 대응하는 메서드는 ② TRACE이다.

NoteBase

문 7. 다음 RAID에 대한 설명으로 적절한 것은 모두 몇 개인가?

가. RAID 1은 디스크 미러링으로 여러 디스크에 데이터를 완전 이중화하여 저장하는 방식으로 비용이 많이 발생한다.
나. RAID 3은 패리티 정보를 별도 디스크에 저장하고 데이터는 블록 단위로 데이터 디스크에 분산 저장한다.
다. RAID 5는 분산 패리티를 구현하여 안정성을 향상하고 일반적으로 4개의 디스크로 구성된다.
라. RAID 6은 패리티를 다중화하여 저장하고 장애가 발생된 상황에서 추가적인 디스크 장애가 발생해도 정상 동작한다.

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

RAID 3은 전용 패리티 디스크를 사용하지만 데이터는 **바이트 단위**로 나눈다. 블록 단위와 전용 패리티의 조합은 RAID 4이며, RAID 5의 디스크 수는 반드시 4개로 고정되는 것은 아니다.

NoteBase

보기별 해설

RAID의 차이는 데이터 복제 여부, 스트라이핑 단위, 패리티의 위치와 개수로 구별한다. RAID의 디스크 장애 대비 기능은 파일 삭제나 악성코드 피해까지 막는 별도 백업과는 다르다.

가. O: RAID 1은 같은 데이터를 두 디스크 등에 미러링하여 저장한다. 한 디스크에 장애가 나도 다른 복제본을 사용할 수 있지만, 동일 용량 두 디스크의 일반적인 미러 구성에서는 저장용량의 절반만 실제 데이터에 사용하므로 용량 대비 비용이 크다.

나. X: RAID 3은 바이트 단위 스트라이핑과 전용 패리티 디스크를 사용하는 방식이다. 패리티를 별도 디스크에 둔다는 부분은 맞지만, 데이터를 블록 단위로 분산한다는 설명은 RAID 4의 특징과 혼동한 것이다.

다. O: RAID 5는 데이터와 단일 패리티를 여러 디스크에 분산하여 저장하며, 한 디스크의 장애를 견딜 수 있다. 4개 디스크로 구성할 수 있다는 설명을 최소 개수나 고정 개수로 이해해서는 안 된다. RAID 5의 일반적인 최소 디스크 수는 3개이고, 4개 구성은 그중 하나이다.

라. O: RAID 6은 서로 독립적인 두 패리티 정보를 사용하여 최대 두 디스크의 장애에도 데이터를 복구하며 동작할 수 있다. 즉 한 디스크가 고장 난 상태에서 다른 한 디스크가 추가로 고장 나도 견딜 수 있다는 뜻이다. 이 범위를 넘는 장애까지 보장하는 것은 아니다.

적절한 설명은 가·다·라의 3개이므로 ③에 해당한다.

NoteBase

문 8. ICMPv6에 추가된 기능으로 가장 적절하지 않은 것은?

① PMTUD(Path MTU Discovery)

② DSD(Duplicate Security Detection)

③ MLD(Multicast Listener Discovery)

④ NDP(Neighbor Discovery Protocol)

정답 2번

간단한 해설

IPv6의 중복 주소 검출 기능은 **DAD(Duplicate Address Detection)**이다. DSD는 해당 기능의 이름이 아니다.

선지별 해설

① O: PMTUD는 송신지와 목적지 사이 경로에서 처리할 수 있는 패킷 크기를 알아내는 절차이다. IPv6에서는 중간 라우터가 패킷을 단편화하지 않으므로, 너무 큰 패킷을 받으면 ICMPv6의 Packet Too Big 메시지로 송신자에게 알려 패킷 크기를 조정하게 한다. PMTUD라는 개념 자체가 IPv6에서 처음 생겼다는 뜻은 아니다.

② X: IPv6에서 주소를 사용하기 전에 중복 여부를 검사하는 기능은 **DAD(Duplicate Address Detection)**이다. 이웃 요청·응답 메시지를 활용하여 같은 링크에 해당 주소를 사용하는 노드가 있는지 확인한다. DSD(Duplicate Security Detection)는 이 중복 주소 검출 기능의 명칭이 아니다.

③ O: MLD는 링크에 어떤 IPv6 멀티캐스트 수신자가 있는지, 어떤 멀티캐스트 트래픽을 수신하려 하는지 라우터가 알아내기 위한 프로토콜이다. 질의와 보고 등에 ICMPv6 메시지를 사용하며 IPv4의 IGMP에 대응하는 역할을 한다.

④ O: NDP는 같은 링크의 이웃과 라우터를 발견하고 링크 계층 주소를 알아내거나 이웃의 도달 가능성을 확인하는 데 사용한다. 라우터 요청·광고, 이웃 요청·광고 등 ICMPv6 메시지를 이용하며 IPv4의 ARP 등이 담당하던 기능을 통합한다.

NoteBase

문 9. 다음 제로트러스트 네트워크에 대한 설명 중 빈칸 (㉠)에 들어갈 용어로 가장 적절한 것은?

(㉠)은 네트워크 트래픽을 기계적으로 관리하는 계층이다. 아주 빠른 속도로 트래픽을 처리하기 때문에 일반적으로 간단한 알고리즘을 사용하고, 경우에 따라 특별 제작된 하드웨어를 사용하여 알고리즘의 동작을 가속하기도 한다.

① 보안정책 엔진

② 트러스트 엔진

③ 컨트롤 플레인

④ 데이터 플레인

정답 4번

간단한 해설

실제 트래픽을 고속으로 처리하는 영역은 데이터 플레인이다. 접근 정책이나 처리 규칙을 결정하는 기능과, 정해진 규칙을 실제 데이터 흐름에 적용하는 기능을 구분한다.

빈칸별 해설

㉠ 데이터 플레인: **실제 트래픽을 처리하는 영역**이다. 정해진 전달·접근 제어 규칙을 적용하여 패킷을 전달하거나 차단하는 등 데이터 경로에서 동작한다. 많은 패킷을 빠르게 처리해야 하므로 규칙 조회와 반복 처리를 효율화하고, 필요하면 전용 하드웨어로 가속한다는 제시문의 설명과 맞는다.

컨트롤 플레인과의 구분: 컨트롤 플레인은 통신을 허용할지, 어떤 경로나 규칙을 적용할지 등을 결정하고 데이터 처리에 필요한 제어 정보를 제공한다. **결정·제어와 실제 트래픽 처리의 구분**이 핵심이며, 컨트롤 플레인이 모든 사용자 패킷을 직접 고속 전달하는 영역이라는 뜻은 아니다.

엔진과의 구분: 보안정책 엔진은 정책과 사용자·기기 등의 정보를 바탕으로 접근 허용·거부 등의 결정을 내리는 기능이다. 트러스트 엔진은 신원, 기기 상태, 상황 등의 신뢰 판단을 담당하는 의미로 사용된다. 이런 판단 기능을 나타내는 명칭은 제시문의 고속 트래픽 처리 영역 자체를 가리키는 데이터 플레인과 구별된다.

따라서 ㉠에는 데이터 플레인이 들어가며, 이에 해당하는 선택지는 ④이다.

NoteBase

문 10. 리눅스 로그파일에 대한 설명으로 가장 적절하지 않은 것은?

① 현재 로그인한 사용자 정보는 로그인을 수행할 때 utmp 로그 파일에 로그인 정보가 기록된다.

② wtmp 로그는 로그인과 로그아웃 정보를 가지고 있는 로그 파일로 접속정보를 계속 기록하는 파일이다.

③ btmp 로그는 리눅스 로그인시 실패한 정보를 가지고 있는 로그파일로 텍스트 형태로 저장되어 vi 에디터를 실행하여 확인할 수 있다.

④ pacct 로그는 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보를 저장하는 로그이다.

정답 3번

간단한 해설

btmp는 로그인 실패 정보를 **바이너리 형식**으로 저장한다. 일반 텍스트 파일처럼 vi로 읽는 것이 아니라 **lastb**처럼 해당 형식을 해석하는 명령으로 조회한다.

선지별 해설

① O: utmp는 **현재 로그인 세션의 상태**를 기록하는 파일이다. 로그인 처리 과정에서 사용자·터미널·접속 시각 등의 정보가 기록되며, who 같은 명령으로 현재 접속 사용자를 확인하는 데 활용된다. 과거 접속 이력을 계속 누적하는 wtmp와 목적이 다르다.

② O: wtmp는 로그인과 로그아웃의 이력을 누적하여 남기는 파일이다. 따라서 현재 접속 중인 사용자뿐 아니라 과거의 접속 내역과 세션 종료 정보도 확인할 수 있으며, 보통 last 명령으로 조회한다. 실제 기록 범위는 시스템 설정과 로그 보존 정책에 따른다.

③ X: btmp가 로그인 실패 정보를 기록한다는 부분은 맞지만, **일반 텍스트가 아니라 바이너리 형식**이라는 점이 중요하다. vi로 파일을 열 수 있다는 것과 구조화된 로그인 기록을 올바르게 해석할 수 있다는 것은 다르다. 실패한 로그인 내역은 보통 **lastb 명령**으로 확인한다.

④ O: pacct는 프로세스 회계 기능이 활성화된 시스템에서 사용자가 실행한 프로그램의 정보를 기록하는 파일이다. 프로세스가 종료될 때 실행 명령명·사용자·실행시간 등의 회계 정보가 남으며, lastcomm 등으로 확인한다. 모든 시스템에서 자동으로 기록되는 것은 아니며, 셸 입력문 전체를 그대로 저장하는 명령 이력 파일과도 구별된다.

NoteBase

문 11. 다음 빈칸 (㉠)에 들어갈 프로토콜로 가장 적절한 것은?

미국 국토안보부는 2013년 위협 정보를 전송하기 위한 위협 정보 표현 규격인 STIX와 위협 정보 전송 프로토콜인 (㉠)를 발표하였다. STIX는 사이버 위협 지능(CTI)을 교환하는데 사용되는 직렬화 형식의 언어이며, (㉠)는 이러한 사이버 위협 정보를 간단하게 확장할 수 있는 방식으로 통신하도록 해주는 프로토콜이다. (㉠)는 UTF-8로 인코딩된 JSON 형태로 데이터를 전송한다.

① BCP

② TAXII

③ PMS

④ SOAR

정답 2번

간단한 해설

STIX가 사이버 위협 정보의 표현 규격이라면, **TAXII는 그 정보를 교환하는 프로토콜**이다. TAXII 2.1은 UTF-8로 인코딩한 JSON을 사용한다.

빈칸별 해설

㉠: TAXII이다. STIX는 위협 지표·공격 기법 등 사이버 위협 정보를 공통된 구조로 표현하는 규격이고, TAXII는 그 정보를 시스템 사이에서 교환하기 위한 응용 계층 프로토콜이다. 즉 **정보 표현은 STIX, 정보 교환은 TAXII**로 구별한다. TAXII 2.1은 HTTPS를 이용하고 TAXII 자원을 UTF-8로 인코딩한 JSON으로 직렬화하므로 지문의 통신·데이터 형식 설명에 부합한다. 이 JSON 설명은 해당 버전의 규격이며, 최초 발표 당시의 모든 버전이 같은 형식을 사용했다는 뜻은 아니다.

다른 선택지의 BCP는 재난·장애에도 핵심 업무를 이어 가기 위한 업무연속성계획, PMS는 보안 패치의 배포·적용 등을 관리하는 패치관리시스템이다. SOAR는 보안 도구와 대응 절차를 연계하여 보안 운영을 자동화하는 체계로, 그 자체가 지문에서 묻는 위협 정보 교환 프로토콜의 명칭은 아니다.

따라서 반복된 빈칸 ㉠에는 모두 TAXII가 들어가며, 이에 해당하는 선택지는 ②이다.

NoteBase

문 12. 이메일(e-mail) 요소와 설명이 가장 적절하지 않은 것은?

① MUA - 사용자 역할이나 사용자 응용 프로그램을 대표하며 이들을 위해 동작한다.

② MDA - MHS로부터 MS로 메시지 전달을 책임지고 수행한다.

③ MTA - 응용 프로그램 수준의 한 홉(hop) 간에 메일을 중계한다.

④ MSA - 장기 메시지 저장소로 POP이나 IMAP을 이용해 원격서버에 있는 메시지를 검색한다.

정답 4번

간단한 해설

MSA는 사용자 측에서 제출한 메일을 받아 전송체계로 넘기는 **메일 제출 에이전트**이다. 장기간 메시지를 보관하고 POP·IMAP 등을 통한 접근의 대상이 되는 것은 메시지 저장소인 MS이다.

선지별 해설

메일 구조에서는 사용자의 작성·열람, 메일 제출, 전송 중계, 최종 배달, 저장의 기능을 구별한다. MHS는 메시지 처리체계이고 MS는 메시지 저장소로, 약어가 비슷해도 역할이 다르다.

① O: MUA는 Message User Agent로 사용자나 사용자 응용 프로그램을 대신하여 메일을 작성·제출하거나 수신 메시지를 표시·처리한다. 사용자가 메일 기능을 이용하는 접점에 해당한다.

② O: MDA는 Message Delivery Agent로 전송체계에서 도착한 메일을 수신자의 저장소 등 최종 수신 환경에 배달한다. 중간 중계가 아니라 목적지에서의 배달을 담당한다.

③ O: MTA는 Message Transfer Agent로 메일 전송경로상의 다음 메일 처리 주체로 메시지를 넘긴다. 여기서 한 홉은 응용 계층의 메일 중계 구간이며, IP 라우터 하나를 지나는 네트워크 홉과 같지 않다.

④ X: MSA는 Message Submission Agent로 MUA가 제출한 메시지를 받아 정책과 형식 요건 등을 확인하고 메일 전송체계에 넘기는 역할이다. 장기 저장 기능은 MS가 담당하며, MUA는 POP이나 IMAP 등을 통해 원격 MS의 메시지에 접근할 수 있다.

NoteBase

문 13. 다음 NTFS 디스크 구조에 대한 설명으로 옳은 것을 모두 고른 것으로 가장 적절한 것은?

가. MBR은 파티션 생성시 물리적 디스크의 첫 번째 섹터에 위치하는 512 Bytes 크기의 영역이다.
나. VBR은 윈도우 부팅을 위한 기계어 코드와 볼륨 및 클러스터의 크기, MFT의 시작주소 등 설정 정보를 담고 있다.
다. MFT는 볼륨/파일시스템에 존재하는 모든 파일과 디렉토리에 대한 정보를 담고 있는 테이블이다.

① 가, 나
② 나, 다
③ 가, 다
④ 가, 나, 다

정답 4번

간단한 해설

MBR은 **디스크 선두의 부팅·파티션 정보**, VBR은 해당 볼륨의 부팅·설정 정보, MFT는 파일과 디렉터리의 관리 정보를 담는다. 세 설명은 각각 다른 범위의 구조를 올바르게 설명한다.

보기별 해설

가. O: 전통적인 MBR 방식에서 MBR은 물리 디스크의 맨 앞, 즉 논리 블록 주소 0에 있는 512바이트 구조이다. 부트스트랩 코드와 파티션 테이블, 부트 서명을 담으며 디스크의 파티션 구성과 부팅에 필요한 정보를 제공한다. 특정 NTFS 볼륨의 시작 부분인 VBR과 위치를 구별해야 한다.

나. O: VBR은 해당 볼륨의 부트 레코드이다. NTFS 볼륨의 부팅 코드와 함께 섹터·클러스터 크기, 볼륨 크기, MFT의 시작 클러스터 위치 등 파일시스템을 해석하는 데 필요한 설정 정보를 담는다. MBR이 디스크의 파티션 구성을 다룬다면 VBR은 해당 볼륨의 구조를 설명한다.

다. O: MFT는 NTFS 볼륨에 있는 파일과 디렉터리를 관리하는 중심 테이블이다. 각 항목에 파일명·크기·시간 정보·데이터 위치 등 파일을 찾고 관리하는 데 필요한 속성을 기록한다. 작은 데이터는 MFT 레코드 안에 저장되기도 하지만, 모든 파일의 내용 전체가 MFT 안에 들어가는 것은 아니다.

따라서 가·나·다가 모두 옳으므로 ④에 해당한다.

NoteBase

문 14. 다음에서 설명하는 용어로 가장 적절한 것은?

◯ 인터넷 사용자들이 비밀번호를 제공하지 않고 다른 웹사이트 상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근권한을 부여할 수 있는 공통적인 수단으로 사용되는 접근 위임을 위한 개방형 표준이다.
◯ 애플리케이션(페이스북, 구글, 엑스 등)의 사용자 비밀번호를 Third Party 앱의 제공 없이 인증, 인가할 수 있는 오픈 표준 프로토콜이다.

① OAuth
② JWT
③ SPF
④ BOOTP

정답 1번

간단한 해설

다른 서비스의 비밀번호를 제3자 앱에 넘기지 않고 제한된 접근 권한을 위임하는 체계는 OAuth이다. 핵심은 사용자 인증 그 자체가 아니라 자원 접근에 대한 인가이다.

NoteBase

대응 관계 해설

접근 위임이라는 단서: **OAuth는 제3자 애플리케이션에 제한된 접근 권한을 부여하는 인가 체계**이다. 사용자가 다른 서비스에 보관한 자원에 접근하도록 허용하되, 해당 서비스의 비밀번호 자체를 제3자 앱에 넘기는 방식과 구별된다.

비밀번호를 제공하지 않는다는 단서: 대표적인 OAuth 흐름에서는 사용자가 원래 서비스의 인가 서버에서 동의 절차를 거치고, 제3자 앱은 발급받은 접근 토큰으로 허용된 자원에 접근한다. 토큰에는 접근 범위나 유효기간 같은 제한을 둘 수 있으므로 계정 비밀번호 전체를 공유하는 것과 다르다.

용어상 주의: 제시문은 인증·인가를 함께 언급하지만, **OAuth 자체의 핵심 목적은 인가**이다. 사용자가 누구인지 확인하는 인증과 무엇에 접근하도록 허용할지 결정하는 인가는 구별해야 한다. 소셜 로그인에 관련 기술이 쓰인다고 해서 OAuth 자체를 사용자 인증 프로토콜과 동일시해서는 안 된다.

다른 선택지와의 구분: ② JWT는 클레임을 JSON 기반으로 표현·전달하는 토큰 형식이다. OAuth에 쓰이는 토큰을 JWT로 구성할 수는 있지만, JWT 자체가 접근 위임 절차는 아니다. ③ SPF는 도메인에 대해 허용된 메일 송신 서버를 DNS 정보로 확인하는 체계이다. ④ BOOTP는 부팅하는 호스트가 IP 주소 등의 초기 설정 정보를 얻도록 하는 프로토콜이다.

따라서 두 설명의 핵심인 비밀번호 공유 없는 접근 권한 위임에 해당하는 것은 OAuth이며, 정답은 ①이다.

NoteBase

문 15. 다음에서 설명하고 있는 취약점 진단 도구로 가장 적절한 것은?

이 취약점 진단 도구는 웹 취약점 스캐너 계열로 GPLv2 라이선스를 따르고 있어, 톰캣, 아파치, PHP 등 다양한 플랫폼의 기본 설정 파일들이 설치된 이후에 삭제되지 않고 남겨져 웹상에서 노출되고 있는지 스캔을 수행한다.

① Nikto
② Nmap
③ Arachni
④ OpenVAS

정답 1번

간단한 해설

Nikto는 웹 서버에 남아 있는 기본 파일과 알려진 위험 경로, 설정상 문제를 점검하는 웹 취약점 스캐너이다. 설치 후 제거되지 않은 파일의 웹 노출 여부를 검사한다는 단서가 핵심이다.

구성 요소별 해설

웹 취약점 스캐너: Nikto는 웹 서버에서 위험한 파일, 알려진 취약점, 잘못된 설정 등을 점검하는 도구이다. 단순히 호스트와 열린 포트를 찾는 것보다 웹 서버의 노출 상태를 진단하는 데 초점이 있다.

GPLv2: 지문의 라이선스는 Nikto의 과거 배포 버전에 해당하는 설명이다. 라이선스는 버전에 따라 달라질 수 있으므로 모든 최신 버전에도 그대로 적용되는 고정 특성으로 보아서는 안 된다.

기본 설정 파일의 잔존·노출: 톰캣·아파치·PHP 등의 설치 후 불필요하게 남은 기본 파일이나 알려진 경로가 웹으로 접근 가능한지 검사하는 기능이 결정적인 단서이다. 이러한 파일은 환경 정보 노출이나 공격의 실마리가 될 수 있다.

다른 도구와의 구별: Nmap은 네트워크 탐색과 포트·서비스 조사에 널리 쓰인다. Arachni도 웹 애플리케이션 보안 점검 도구이고 OpenVAS는 폭넓은 취약점 평가 도구이지만, 이 지문처럼 기본 파일·설정 노출 검사와 과거 GPLv2 배포 특성을 함께 제시한 도구는 Nikto이다.

따라서 지문의 설명에 대응하는 도구는 ① Nikto이다.

NoteBase

문 16. 다음에 출력된 내용의 밑줄 친 ㉠에 대한 설명으로 가장 적절한 것은?

[root@localhost~]#crontab -l
- 생략 -
1 0 * * 2 root /home/clean.sh
㉠

① 매주 월요일 새벽 0시 1분에 /home/clean.sh 명령을 실행
② 매월 2일 새벽 0시 1분에 /home/clean.sh 명령을 실행
③ 매주 화요일 새벽 0시 1분에 /home/clean.sh 명령을 실행
④ 매일 새벽 0시 1분에 /home/clean.sh 명령을 실행

정답 3번

간단한 해설

crontab의 시간 필드는 '분 시 일 월 요일' 순서이다. '1 0 * * 2'에서 1과 0은 **0시 1분**, 마지막 2는 **화요일**을 뜻하므로 매주 화요일에 실행하는 일정이다.

출제 포인트

crontab의 다섯 시간 필드와 요일 번호를 읽어 반복 실행 일정을 해석하는 문제이다.

핵심 개념

cron은 정해진 일정에 명령을 반복 실행하는 작업 예약 기능이며, crontab은 그 일정을 등록하는 표이다.
시간 필드는 '분 시 일 월 요일' 순서이다. '1 0 * * 2'는 1분, 0시, 날짜 제한 없음, 월 제한 없음, 화요일을 뜻한다. 따라서 제시된 시간 조건은 매주 화요일 0시 1분이다.
요일 번호는 0 또는 7이 일요일, 1이 월요일, 2가 화요일이다. '*'는 해당 필드의 모든 값을 허용하지만, 다른 필드에 지정된 조건까지 없애지는 않는다.
시스템 crontab에서는 시간 필드 뒤의 'root'가 실행 사용자이다. 사용자별 crontab에는 별도 사용자 칸이 없으므로, 제시문은 출력 명령과 등록 줄의 형식이 섞여 있다. 이 문항은 앞의 다섯 시간 필드가 나타내는 일정을 묻는다.

NoteBase

선지별 해설

① X
'매주 월요일'이 틀리다. 요일 필드의 2는 화요일이므로 '매주 화요일 새벽 0시 1분'으로 고친다. 월요일 일정이라면 마지막 필드가 1이어야 한다.

② X
'매월 2일'이 틀리다. 2는 세 번째 날짜 필드가 아니라 다섯 번째 요일 필드에 있으므로 화요일을 뜻한다. 매월 2일 0시 1분이라면 시간 필드는 '1 0 2 * *'가 된다.

③ O
분 필드가 1이고 시 필드가 0이므로 0시 1분이다. 일과 월은 '*'로 제한하지 않고 요일을 2로 지정했으므로, 제시된 시간 조건은 매주 화요일 새벽 0시 1분에 /home/clean.sh를 실행하는 일정에 해당한다.

④ X
'매일'이 틀리다. 요일 필드가 2로 제한되어 있으므로 '매주 화요일'로 고친다. 매일 0시 1분 일정이라면 시간 필드는 '1 0 * * *'가 된다.

오답 포인트

마지막 2를 날짜로 읽으면 ②를 고르기 쉽다. 숫자의 의미는 값만이 아니라 필드 위치로 결정된다. 또 일과 월의 '*'만 보고 매일이라고 판단하면 요일 제한을 놓친다.

다시 나오면 이렇게 판단

왼쪽부터 '분 시 일 월 요일'을 대응시킨 뒤, 숫자로 지정된 조건과 '*'인 칸을 구분한다. 요일 번호는 일요일을 0으로 시작하므로 2를 화요일로 읽는다.

암기 포인트

분·시·일·월·요일 순서이며, 요일 0은 일요일, 1은 월요일, 2는 화요일이다.

NoteBase

문 17. 다음에서 설명하는 것으로 가장 적절한 것은?

◯ 원격 호스트에 로그온하거나 원격 호스트에서 명령을 실행하고, 다른 호스트로 파일을 조작할 수 있게 해주는 응용 프로그램 또는 프로토콜이다.
◯ 암호화 통신을 하므로 노출되더라도 안전하다.
◯ 버전 2에서 서버와 클라이언트는 Diffie-Hellman 키 교환 방식을 사용한다.

① rsh
② ssh
③ rlogin
④ telnet

정답 2번

간단한 해설

암호화된 원격 로그인·명령 실행과 버전 2의 키 교환을 함께 설명하는 것은 SSH이다. 단순히 원격 접속 기능이 있다는 점보다 통신 내용을 보호하는 보안 채널이라는 점이 결정적인 단서이다.

NoteBase

대응 관계 해설

원격 작업과의 대응: **SSH(Secure Shell)**는 안전하지 않은 네트워크에서도 원격 로그인과 명령 실행 등을 안전하게 수행하도록 하는 프로토콜이다. SSH 연결을 이용하는 파일 전송 기능을 통해 다른 호스트의 파일을 다룰 수도 있다.

암호화 통신과의 대응: SSH는 통신 내용을 암호화하여 도청자가 패킷을 보더라도 내용을 쉽게 읽지 못하도록 하고, 무결성 보호와 상대 인증을 제공한다. 제시문의 '노출되더라도 안전하다'는 것은 **전송 중인 암호문이 관찰되는 상황**에 대한 설명이지, 비밀키나 비밀번호 유출·취약한 설정까지 안전하다는 뜻은 아니다.

키 교환과의 대응: SSH 버전 2의 전송 계층 규격은 Diffie–Hellman 키 교환 방식을 정의한다. 이 과정에서 공유 비밀을 합의하고 이를 바탕으로 통신에 사용할 키를 만든다. SSH는 키 교환 알고리즘을 협상할 수 있으므로 모든 구현이 오직 하나의 고정된 Diffie–Hellman 방식만 사용한다고 해석하지 않는다.

다른 선택지와의 구분: ① rsh는 원격 명령 실행, ③ rlogin은 원격 로그인에 사용되는 전통적인 도구이다.

④ telnet도 원격 터미널 접속 기능을 제공한다. 그러나 이들 기본 방식은 SSH처럼 암호화된 보안 채널을 제공하지 않으므로, 원격 작업뿐 아니라 암호화와 SSH 버전 2의 키 교환까지 제시한 설명에는 맞지 않는다.

따라서 세 단서를 함께 만족하는 것은 SSH이며, 정답은 ②이다.

NoteBase

문 18. 다음 윈도우 레지스트리 루트키에 대한 설명으로 적절하지 않은 것은 모두 몇 개인가?

가. HKEY_CLASSES_ROOT(HKCR)는 시스템에 등록된 파일 확장자와 그것을 열 때 사용할 애플리케이션에 대한 맵핑 정보와 COM 오브젝트 등록 정보를 저장하고 있다.
나. HKEY_CURRENT_USER(HKCU)는 시스템에 있는 모든 계정과 그룹에 관한 정보를 저장하고 있다.
다. HKEY_LOCAL_MACHINE(HKLM)은 시스템이 시작할 때 사용하는 하드웨어 프로파일 정보를 저장하고 있다.

① 0개
② 1개
③ 2개
④ 3개

정답 3번

간단한 해설

HKCU는 모든 계정·그룹이 아니라 **현재 로그인한 사용자의 설정**을 다룬다. 시작 시 사용하는 하드웨어 프로파일에 대응하는 루트키는 **HKCC**이며 HKLM은 컴퓨터 전체의 설정을 다룬다.

출제 포인트

윈도우 레지스트리 루트키를 파일 연결, 현재 사용자 설정, 컴퓨터 전체 설정, 현재 하드웨어 프로파일로 구분하는 문제이다.

핵심 개념

레지스트리는 윈도우와 응용프로그램의 설정을 계층적으로 관리하는 데이터베이스이며, 루트키는 이 정보에 접근하는 최상위 진입점이다.
HKCR: 파일 확장자와 실행 프로그램의 연결 정보 및 COM 객체 등록 정보를 제공한다.
HKCU: 현재 로그인한 사용자의 환경과 응용프로그램 설정을 제공한다.
HKLM: 사용자에 공통으로 적용되는 컴퓨터의 하드웨어·소프트웨어·시스템 설정을 제공한다.
HKCC: 시스템 시작 시 사용하는 현재 하드웨어 프로파일 정보를 제공한다.

NoteBase

보기 판단

가 O: HKCR는 파일 형식과 이를 여는 프로그램의 연결 정보, COM 객체 등록 정보를 제공하므로 적절하다.
나 X: HKCU의 대상은 현재 로그인한 사용자이다. '시스템에 있는 모든 계정과 그룹'은 '현재 로그인한 사용자의 설정'으로 고친다. 모든 사용자의 설정과도 구분해야 하며, HKEY_USERS는 컴퓨터에 로드된 사용자 프로파일들을 제공한다.
다 X: 이 문항의 루트키별 대표 기능 구분에서 '시스템이 시작할 때 사용하는 하드웨어 프로파일'은 HKCC에 대응한다. 해당 기능을 설명하려면 'HKEY_LOCAL_MACHINE(HKLM)'을 'HKEY_CURRENT_CONFIG(HKCC)'로 고친다. HKLM은 컴퓨터 전체의 구성 정보를 다룬다. 다만 HKCC는 HKLM 내부의 현재 하드웨어 프로파일 경로를 가리키는 별칭이므로, HKLM에 하드웨어 프로파일 정보가 없다는 뜻은 아니다.

선지별 해설

① X: '0개'는 나와 다의 기능 연결 오류를 모두 놓친 값이다. 이 문항의 기능 구분에서는 나와 다를 포함한 2개로 고친다.
② X: '1개'는 나와 다 가운데 하나를 누락한 값이다. HKCU의 사용자 범위와 HKCC의 하드웨어 프로파일 기능을 함께 구분하면 2개이다.
③ O: 가는 적절하고, 나는 HKCU의 대상을 잘못 설명했으며, 다는 HKCC의 대표 기능을 HKLM에 연결했다. 이 문항에서 적절하지 않은 설명은 나와 다의 2개이다.
④ X: '3개'는 적절한 가까지 포함한 값이다. HKCR의 파일 연결·COM 등록 설명은 제외하므로 2개로 고친다.

오답 포인트

나의 '모든 계정과 그룹'을 현재 사용자 설정으로 오인하기 쉽다. 다에서는 HKLM도 하드웨어 정보를 다룬다는 이유로, 현재 하드웨어 프로파일에 대응하는 별도 루트키 HKCC를 놓치기 쉽다. 루트키의 대표 기능과 실제 하위 경로의 포함 관계는 구분한다.

다시 나오면 이렇게 판단

설명의 대상을 먼저 구분한다. 파일 형식·COM이면 HKCR, 현재 사용자 설정이면 HKCU, 컴퓨터 전체 설정이면 HKLM, 시작 시 사용하는 현재 하드웨어 프로파일이면 HKCC에 대응한다. 개수형 문항은 각 보기를 판단한 뒤 요구한 판단에 해당하는 보기만 센다.

암기 포인트

HKCR는 파일 연결·COM, HKCU는 현재 사용자, HKLM은 컴퓨터 전체, HKCC는 현재 하드웨어 프로파일이다.

NoteBase

문 19. FTP와 TFTP의 차이점에 대한 설명으로 가장 적절한 것은?

① TFTP는 FTP와 같이 TCP 포트 21번을 사용한다.

② TFTP는 자체 디스크가 없는 워크스테이션의 부팅 이미지 전달에 주로 사용한다.

③ TFTP는 사용자명/비밀번호 방식의 간단한 인증을 제공한다.

④ TFTP는 파일을 받고, 보내고, 삭제하기 등을 위한 다양한 명령을 지원한다.

정답 2번

간단한 해설

TFTP는 구현이 간단한 파일 전송 프로토콜이어서 **디스크 없는 장치의 부팅 이미지 전달**에 이용된다. FTP와 달리 UDP를 사용하며, 기본 규격에는 사용자 인증이나 파일 삭제 기능이 없다.

선지별 해설

① X: FTP는 TCP를 사용하며 제어 연결의 기본 서버 포트는 21번이다. 반면 TFTP는 **UDP를 사용하고 최초 요청을 서버의 69번 포트**로 보낸다. 이후 파일 데이터와 응답은 전송 양 끝에서 정한 포트 번호를 이용하므로 모든 TFTP 패킷이 69번 포트를 사용하는 것은 아니다.

② O: TFTP는 기능이 단순하고 구현 규모가 작아, 자체 디스크가 없는 워크스테이션이 네트워크를 통해 **부팅에 필요한 이미지 파일**을 내려받는 용도에 적합하다. 부팅 초기의 제한된 실행 환경에서도 비교적 간단한 파일 전송 기능을 구현할 수 있다는 점이 그 이유이다.

③ X: 기본 TFTP에는 **사용자명·비밀번호 인증 기능이 없다**. 사용자명과 비밀번호를 이용한 로그인은 FTP에서 지원하는 기능이다. 서버에서 접근 가능한 파일이나 통신 대상을 제한하는 것과 프로토콜 자체의 사용자 인증은 구별해야 한다.

④ X: TFTP는 파일 읽기·쓰기 전송을 중심으로 하는 단순한 프로토콜이며, **파일 삭제나 디렉터리 목록 조회 명령을 제공하지 않는다**. 파일 전송뿐 아니라 삭제와 디렉터리 관리 등 다양한 명령을 제공하는 것은 FTP이다.

NoteBase

문 20. 다음 빈칸 (㉠)에 들어갈 프로토콜로 가장 적절한 것은?

(㉠)는 MAC 주소를 기반으로 클라이언트에게 IP 주소를 할당하는데, 공격자는 이 점을 악용하여 MAC 주소를 랜덤하게 변경하여 새로운 IP 주소를 할당받는다. 결국 (㉠)가 할당할 IP 주소가 모두 고갈되어, 정상적인 클라이언트는 IP 주소를 할당받지 못하게 된다. 대응 방법으로는 특정 스위치 포트에 지정된 MAC 주소만 접속을 허용하고, 조건에 일치하지 않는 MAC 주소는 차단해야 한다.

① ARP

② RARP

③ DHCP

④ BOOTP

정답 3번

간단한 해설

여러 클라이언트처럼 보이는 요청으로 **IP 주소 임대 풀을 고갈**시키는 것은 DHCP 고갈 공격이다. 주소를 동적으로 임대하는 프로토콜은 DHCP이다.

빈칸별 해설

㉠은 DHCP이다. DHCP 서버는 관리하는 주소 풀에서 클라이언트에게 IP 주소와 네트워크 설정을 임대한다. 지문에서는 MAC 주소를 바꾼 여러 요청이 서로 다른 클라이언트의 요청처럼 처리되어 주소 풀이 소모되는 상황을 설명한다. 정상 클라이언트가 주소를 받지 못하게 되는 이 서비스 거부 유형을 DHCP 고갈 공격이라고 한다.

지문의 대응 방법은 스위치 포트에서 허용할 MAC 주소를 제한하는 포트 보안이다. 같은 포트에서 허용되지 않은 여러 출발지 MAC 주소를 사용하는 행위를 제한하여 제시된 고갈 방식을 완화한다. 다만 MAC 주소 제한만으로 모든 형태의 DHCP 공격을 막는다는 뜻은 아니다.

ARP는 IPv4 주소에 대응하는 링크 계층 주소를 찾는 기능이며 주소 풀을 임대하지 않는다.

RARP와 BOOTP도 주소·부팅 정보 제공과 관련이 있지만, 지문에서 설명하는 동적 주소 임대 풀의 고갈은 DHCP를 식별하는 단서이다.

따라서 반복된 두 빈칸 ㉠에 모두 들어가는 프로토콜은 DHCP이며 ③에 해당한다.

NoteBase

문 21. 다음에서 설명하는 스팸 메일 보안 대응을 위한 이메일 인증 기술로 가장 적절한 것은?

발신 메일 서버 정보를 사전에 발신 도메인 DNS 서버에 공개적으로 등록함으로써, 수신자가 수신한 메일의 발신자 IP 주소가 발신자 메일 주소 도메인의 실제 메일 서버 정보와 일치하는지 검사할 수 있도록 하는 이메일 인증 기술이다.

① DKIM(Domain Keys Identified Mail)

② DNSSEC(DNS Security Extensions)

③ S/MIME(Secure/Multipurpose Internet Mail Extension)

④ SPF(Sender Policy Framework)

정답 4번

간단한 해설

DNS에 허용된 메일 송신 서버 정보를 게시하고 실제 송신 IP를 대조하는 기술은 SPF이다. DNS 공개키로 메일의 전자서명을 검증하는 DKIM과 구별한다.

대응 관계 해설

DNS 등록과의 대응: **SPF는 해당 도메인을 사용해 메일을 보낼 수 있는 호스트를 DNS에 공개**하는 방식이다. 도메인 관리자는 허용할 송신 서버의 IP 주소나 관련 조건을 SPF 정책에 명시하며, 이 정책은 DNS TXT 레코드로 게시한다.

수신 시 검사와의 대응: 수신 서버는 자신에게 SMTP 연결을 한 송신 서버의 IP 주소를 SPF 정책과 대조하여, 그 서버가 해당 도메인을 사용해 메일을 보낼 권한이 있는지 확인한다. 정확히는 SMTP의 MAIL FROM 또는 HELO 식별자를 대상으로 하며, 메일 화면에 보이는 From 헤더 주소 자체를 언제나 직접 검증하는 것은 아니다.

DKIM과의 구분: ① DKIM도 DNS를 이용하지만, 핵심은 송신 IP 목록이 아니라 **메일에 붙은 전자서명의 검증**이다. 수신 측은 DNS에서 얻은 공개키로 서명을 검사하여 서명 도메인과 메시지의 관계 및 서명된 부분의 무결성을 확인한다.

나머지 선택지와의 구분: ② DNSSEC는 DNS 응답 데이터의 출처 인증과 무결성을 보호하는 확장이다.

③ S/MIME는 메일 내용의 전자서명과 암호화를 제공한다. 두 기술 모두 제시문의 ‘DNS에 공개한 허용 송신 서버 정보와 접속 IP를 대조’하는 SPF의 동작과 다르다.

따라서 제시된 설명에 해당하는 이메일 인증 기술은 SPF이며, 정답은 ④이다.

NoteBase

헷갈리는 개념

SPF 통과는 해당 도메인 정책상 송신 서버가 허용되었다는 뜻이다. 메일 내용이 안전하다거나 스팸이 아니라는 사실까지 보장하지 않으며, 보이는 발신자 주소의 도메인과 인증 도메인의 정렬 여부는 별도로 고려해야 한다.

NoteBase

문 22. 파일에 setuid와 setgid 모두가 부여된 것을 찾는 find 명령으로 가장 적절한 것은?

① find / -perm +6000

② find / -perm +4000

③ find / -mtime -1

④ find / -mtime -2

정답 1번

간단한 해설

setuid는 4000, setgid는 2000이므로 두 비트를 검색 대상으로 삼는 권한 마스크는 **6000**이다. 다만 옛 문법의 '+6000'은 둘 중 하나만 있어도 검색하므로 **두 비트가 모두 설정된 파일만** 찾는 정확한 조건은 '-perm -6000'이다.

출제 포인트

find의 권한 검색 옵션과 setuid·setgid의 8진수 값을 구별하는 문제이다.

핵심 개념

setuid와 setgid는 파일의 특수 권한 비트이다. 실행 파일에서 setuid는 소유자의 사용자 ID를, setgid는 소유 그룹의 그룹 ID를 유효 ID로 사용하도록 한다.
setuid는 8진수 4000, setgid는 8진수 2000이며, 두 비트를 합친 마스크는 6000이다.
'-perm'은 권한 비트를 검사하고, '-mtime'은 파일 내용의 마지막 수정 시점을 검사한다.
옛 '-perm +6000'은 두 비트 중 하나 이상이 설정되어 있으면 검색한다. '-perm -6000'은 두 비트가 모두 설정되어 있어야 검색한다. 예를 들어 권한이 4755인 파일은 전자에만, 6755인 파일은 두 조건 모두에 해당한다.

선지별 해설

① O: 'find / -perm +6000'은 제시된 선지 중 setuid와 setgid의 두 비트를 함께 검색 대상으로 삼는 명령이다. 권한 마스크 6000이 두 특수 권한을 포함하므로 시험에서 채택한 선택지이다. 다만 옛 '+6000' 조건은 한쪽만 설정된 파일도 검색한다. 문제의 '모두'를 엄밀하게 충족시키려면 'find / -perm -6000'으로 쓴다.
② X: 'find / -perm +4000'은 setuid 비트만 검사한다. setgid 비트의 설정 여부는 확인하지 않으므로 두 권한이 모두 있는 파일만 고를 수 없다. 두 비트를 모두 검사하는 조건은 '-perm -6000'이다.
③ X: 'find / -mtime -1'은 마지막 수정 후 24시간이 지나지 않은 파일을 찾는 시간 조건이다. 특수 권한의 유무와는 관계가 없다. 권한 검색에는 '-mtime -1' 대신 '-perm -6000'을 사용한다.
④ X: 'find / -mtime -2'는 마지막 수정 후 48시간이 지나지 않은 파일을 찾는 시간 조건이다. setuid나 setgid를 검사하지 않는다. 두 특수 권한이 모두 설정된 파일을 찾는 조건은 '-perm -6000'이다.

NoteBase

오답 포인트

4000만 보면 setuid만 검사하게 되고, '-mtime'을 고르면 권한 대신 수정 시점을 검사하게 된다. 또한 6000이라는 마스크와 그 앞의 기호를 따로 구별해야 한다. 옛 '+6000'은 '하나 이상', '-6000'은 '모두'라는 차이가 있다.

다시 나오면 이렇게 판단

권한을 묻는지 수정 시점을 묻는지 먼저 구분한다. 특수 권한 문제에서는 setuid의 4000과 setgid의 2000을 확인한 뒤, '모두'라는 조건이면 '-perm -6000'으로 판단한다. 제시된 옛 문법의 '+6000'을 두 비트가 모두 설정되어 있다는 뜻으로 해석하지 않는다.

암기 포인트

setuid 4000, setgid 2000, 두 비트의 마스크 6000. '-perm'은 권한, '-mtime'은 수정 시점. '-perm -6000'은 두 비트 모두이다.

NoteBase

문 23. 다음 접근제어목록(ACL) 규칙에 대한 설명으로 옳은 것을 모두 고른 것으로 가장 적절한 것은?

가. ACL의 위에서부터 아래로 수행된다.
나. 네트워크를 넓은 범위에서 좁은 범위로 설정해야 한다.
다. ACL의 마지막 줄은 ‘deny any’가 생략되어 있으므로, 마지막에 ‘permit any’가 없을 경우 모든 IP 주소는 차단된다.
라. Named ACL의 경우에는 중간 삽입, 삭제 및 추가가 가능하다.
마. 프로토콜, 방향, 인터페이스당 1개의 ACL만 적용 가능하다.

① 가, 나, 다, 라
② 가, 나, 다, 마
③ 가, 나, 라, 마
④ 가, 다, 라, 마

정답 4번

간단한 해설

ACL은 위에서부터 검사하여 **처음 일치한 규칙**으로 허용 여부를 결정한다. 따라서 범위가 겹치는 규칙은 **좁고 구체적인 범위를 먼저** 배치해야 하며 넓은 범위를 앞에 두면 뒤의 세부 규칙이 적용되지 않을 수 있다.

출제 포인트

ACL의 규칙 검사 순서, 묵시적 거부, Named ACL의 편집 기능과 인터페이스 적용 제한을 구분한다.

핵심 개념

ACL은 패킷의 주소나 프로토콜 등의 조건을 검사하여 통과를 허용하거나 차단하는 규칙 목록이다. 'permit'은 허용, 'deny'는 차단을 뜻한다.
위에서부터 검사하되 처음 일치한 규칙에서 판단을 끝내므로, 뒤의 규칙이 앞의 결정을 바꾸지 않는다. 예를 들어 한 호스트만 차단하고 그 호스트가 속한 네트워크의 나머지는 허용하려면, 해당 호스트의 차단 규칙을 네트워크 전체의 허용 규칙보다 앞에 둔다.

NoteBase

보기별 판단

가 O: ACL 규칙은 위에서 아래로 검사하며, 일치하는 규칙을 찾으면 그 규칙의 허용 또는 차단 결정을 적용한다.
나 X: '넓은 범위에서 좁은 범위로'가 잘못된 표현이다. 범위가 겹치는 규칙은 좁고 구체적인 범위를 먼저, 넓고 일반적인 범위를 나중에 배치한다. 넓은 범위를 먼저 처리하면 그 안에 포함되는 세부 규칙까지 검사하지 않기 때문이다.
다: 이 문항은 마지막의 묵시적 'deny any'를 설명한 항목으로 채택한다. 정확히는 앞의 어떤 규칙에도 일치하지 않아 끝까지 도달한 패킷이 차단된다. 마지막에 'permit any'가 없어도 앞의 'permit'에 일치한 패킷은 통과하므로, '모든 IP 주소는 차단된다'를 이미 허용된 패킷까지 차단한다는 뜻으로 읽으면 부정확하다. 허용 규칙이 전혀 없는 ACL이라면 모든 패킷이 차단된다.
라 O: Named ACL은 이름으로 식별하는 ACL이다. 개별 규칙을 삭제하거나 추가할 수 있고, 순서 번호를 이용하면 원하는 위치에 중간 삽입할 수 있다.
마 O: 같은 인터페이스에서 같은 프로토콜과 같은 방향에 적용하는 ACL은 하나이다. 수신 방향과 송신 방향은 별개이며, ACL 하나에는 여러 규칙을 넣을 수 있다.

선지별 해설

① X: 잘못된 나를 포함하고, 편집이 가능한 Named ACL을 설명한 라는 포함하지만 적용 제한을 설명한 마를 빠뜨렸다. 나를 빼고 마를 포함해야 한다.
② X: 잘못된 나를 포함하고, 옳은 라를 빠뜨렸다. 나를 빼고 라를 포함해야 한다.
③ X: 잘못된 나를 포함하고, 출제 취지상 묵시적 거부를 설명한 다를 빠뜨렸다. 나를 빼고 다를 포함해야 한다.
④ O: 최초 일치 규칙을 적용하는 가, 묵시적 거부를 설명한 다, Named ACL의 편집 기능을 설명한 라, 적용 단위별 제한을 설명한 마를 포함하고 나를 제외한 조합이다. 다는 위에서 설명한 적용 범위의 한정이 필요하다.

오답 포인트

나의 '넓은 범위에서 좁은 범위로'를 포괄적 규칙부터 처리한다는 이유로 옳다고 판단하기 쉽다. ACL에서는 먼저 일치한 규칙이 결정을 끝내므로 세부 예외를 앞에 둔다. 다의 묵시적 거부도 앞에서 허용된 패킷을 다시 차단하는 규칙은 아니다.

다시 나오면 이렇게 판단

규칙을 위에서부터 따라가며 최초 일치 위치를 찾는다. 범위가 겹치면 세부 규칙이 앞에 있는지 확인하고, 어느 규칙에도 일치하지 않은 패킷에는 마지막의 묵시적 거부를 적용한다. 적용 개수는 인터페이스·프로토콜·방향을 묶어서 판단한다.

암기 포인트

위에서 검사, 최초 일치로 결정, 구체적 범위 먼저, 미일치 패킷은 차단. 같은 인터페이스·프로토콜·방향에는 ACL 하나이다.

NoteBase

문 24. 인터넷 전자 메일의 표준 규약인 SMTP 프로토콜을 통해 메일 서비스를 하는 샌드메일(sendmail)의 주요 파일 중 스팸메일 및 Relay 차단을 위한 설정 파일로 가장 적절한 것은?

① /etc/spool/mail

② /etc/host.conf

③ /etc/mail/access

④ /usr/bin/sendmail

정답 3번

간단한 해설

sendmail의 **/etc/mail/access**는 호스트·도메인 등의 메일 접근과 릴레이 허용·거부 정책을 지정하는 파일이다. 스팸 발신지를 거부하거나 허가된 대상만 중계하도록 제어하는 데 사용된다.

핵심 풀이

메일 릴레이는 메일 서버가 다른 목적지의 메일 서버로 메시지를 중계하는 기능이다. 허가받지 않은 중계가 가능하면 스팸 발송에 악용될 수 있으므로, sendmail은 호스트·도메인·메일 주소 등에 대한 접근 정책으로 이를 제어한다. 이때 사용하는 텍스트 설정 파일이 **/etc/mail/access**이다. 이 파일에 REJECT와 같은 거부 정책이나 RELAY와 같은 중계 허용 정책을 지정하며, 데이터베이스를 사용하는 구성에서는 이를 조회용 access.db에 반영한다.

다른 선택지와 구별하면, /etc/host.conf는 호스트 이름 해석과 관련된 설정 파일이지 메일 중계 접근 정책 파일이 아니다.

메일 보관용 스풀 디렉터리는 설정 파일과 다르며, 일반적으로 /var/spool/mail 등의 경로를 사용한다. 따라서 ①의 /etc/spool/mail을 접근 제어 파일로 볼 수 없다.

④의 sendmail은 메일 전송 프로그램의 실행 파일을 가리키는 이름이며, 실행 파일의 설치 경로와 접근 정책 파일의 역할은 구별된다.

스팸메일과 릴레이의 허용·거부 정책을 지정하는 파일을 묻고 있으므로 ③ /etc/mail/access에 대응한다.

NoteBase

문 25. 시스템 취약점 분석 도구에 대한 설명으로 가장 적절하지 않은 것은?

① SATAN - 해커와 동일한 방식으로 시스템에 침입하여 보안상의 약점을 찾아 보완할 수 있는 네트워크 분석용 보안 관리 도구이다.

② SARA - SATAN을 기반으로 개발된 취약점 분석 도구로 유닉스 플랫폼에서도 동작하고, HTML 형식의 보고서 기능이 있다.

③ Snort - 시스템 내부에 존재하는 취약점 점검 도구로 유닉스 시스템에서 동작하고 취약한 패스워드를 검사한다.

④ Nessus - 클라이언트/서버 구조로 취약점 검사를 수행하고, GUI 형태의 취약점 점검 설정 및 결과를 확인할 수 있다.

정답 3번

간단한 해설

Snort는 네트워크 침입 탐지·방지 도구이지, 시스템 내부의 취약한 패스워드를 검사하는 도구로 분류하지 않는다. 취약점을 찾는 스캐너와 실제 트래픽에서 공격 징후를 탐지하는 도구의 역할을 구분한다.

선지별 해설

① O: SATAN은 **네트워크를 통해 드러나는 알려진 취약점을 점검**하고 관리자가 보완할 수 있도록 정보를 제공하는 도구이다. 공격자가 이용할 수 있는 서비스·설정의 약점을 외부 관점에서 조사한다는 취지로 이해한다. 다만 반드시 시스템 침입에 성공하거나 취약점을 자동으로 고치는 도구라는 뜻은 아니다.

② O: SARA는 SATAN 계열에서 발전한 네트워크 취약점 분석 도구이다. 유닉스 계열 환경에서 알려진 취약점을 점검하고, 하이퍼텍스트 기반 인터페이스로 검사와 결과 보고를 제공한다. 따라서 유닉스에서 동작하고 HTML 형식으로 결과를 확인한다는 설명이 맞다.

③ X: Snort의 핵심은 **네트워크 트래픽을 분석하는 침입 탐지·방지**이다. 패킷 내용과 규칙 등을 바탕으로 의심스러운 통신을 탐지하고 기록하며, 구성에 따라 차단한다. 시스템 내부의 설정과 취약한 패스워드를 점검하는 호스트 보안 감사 도구의 설명을 Snort에 잘못 붙인 것이다. 유닉스에서 실행될 수 있다는 사실만으로 도구의 주된 기능까지 맞는 설명이 되지는 않는다.

④ O: Nessus는 취약점 검사를 수행하는 스캐너와 이를 조작하는 사용자 인터페이스를 통해 검사 정책을 설정하고 결과를 확인한다. 클라이언트·서버 구조와 그래픽 인터페이스를 이용한 취약점 점검이라는 설명이 맞으며, 웹 기반 화면도 이러한 인터페이스에 해당한다.

NoteBase

문 26. 다음 중 ping이 제공하는 정보만을 모두 고른 것으로 가장 적절한 것은?

가. 호스트의 도메인 이름을 입력하면 호스트의 IP 주소를 반환
나. 경로상의 문제점이 있는 네트워크 정보
다. 각 구간에 대한 접근성 및 네트워크 속도
라. 패킷이 돌아오는데 걸리는 시간
마. 방화벽이나 라우터에서의 필터링 여부
바. 경유 라우터의 IP 주소 및 도착 시간

① 가, 라
② 가, 나, 라
③ 가, 다, 라, 마
④ 가, 나, 다, 마, 바

정답 1번

간단한 해설

ping은 도메인 이름의 이름 해석 결과인 **대상 IP 주소**와, 요청을 보낸 뒤 응답이 돌아오기까지의 **왕복 시간**을 보여 준다. 경유지별 경로·지연 정보를 나열하는 것은 일반적으로 tracert나 traceroute의 기능이며, ping의 특수 옵션과는 구별해야 한다.

NoteBase

보기별 해설

ping은 ICMP Echo Request와 Echo Reply를 이용하여 대상 호스트의 응답 여부와 왕복 시간을 확인하는 도구이다. 아래 판단은 일반적인 기본 출력과 경로 추적 도구의 기능을 구분한 것이며, 구현별 특수 옵션까지 불가능하다고 단정하는 것은 아니다.

가. O: 도메인 이름을 대상으로 ping을 실행하면 이름 해석으로 얻은 대상 호스트의 IP 주소가 표시된다. 주소를 알아내는 과정은 DNS 등 **이름 해석 기능**이 수행하며, ping은 그 결과를 이용하여 ICMP Echo Request를 보낸다.

나. X: ping은 대상까지의 응답 여부와 오류 메시지로 연결 문제의 단서를 제공하지만, 기본 출력만으로 **경로 중 어느 네트워크에 문제가 있는지 특정하지는 못한다**. 경로상의 문제 위치를 조사하려면 tracert·traceroute로 경유지를 확인하거나 pathping으로 경유지별 손실과 지연을 분석한다.

다. X: ping에 표시되는 시간은 대상까지 갔다가 돌아오는 지연 시간이다. 이것만으로 **각 구간의 접근성과 전송 속도를 모두 알 수는 없다**. 구간별 상태는 경유지별 진단이 필요하고, 실제 전송 속도는 처리량 측정 등으로 별도로 확인해야 한다.

라. O: ICMP Echo Request를 보낸 후 대응하는 Echo Reply를 받을 때까지의 **왕복 시간(RTT)**을 측정한다. 이는 송신 호스트에서 대상까지 갔다가 돌아오는 데 걸린 시간이며, 편도 시간이나 특정 구간만의 지연 시간이 아니다.

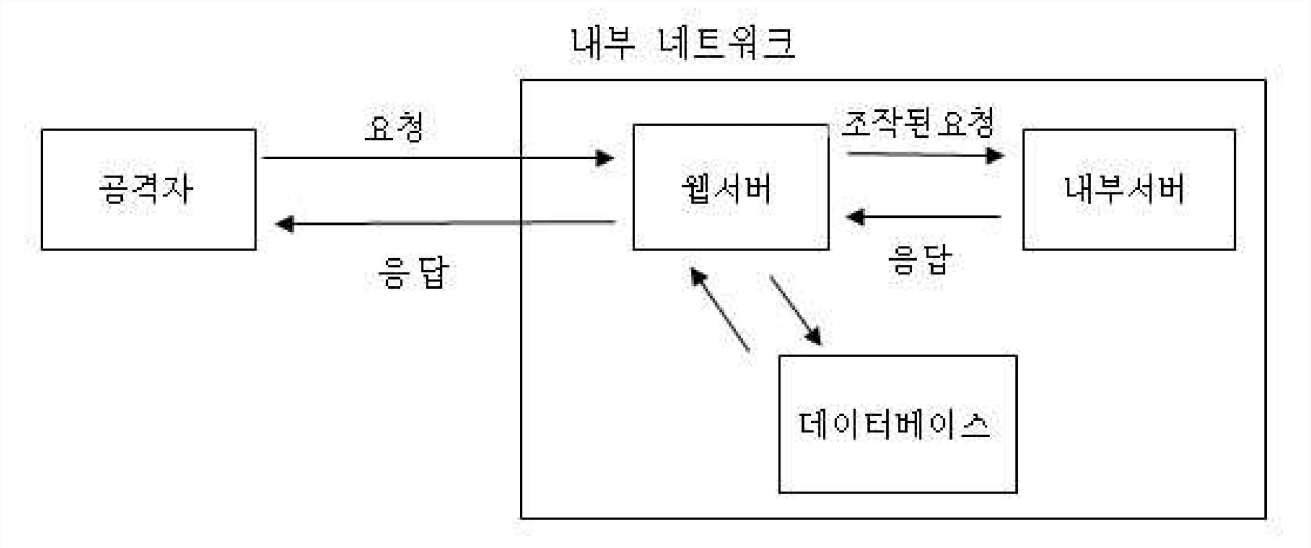
마. X: 응답이 없다는 사실만으로 **필터링 여부를 확정할 수는 없다**. 방화벽이나 라우터가 ICMP를 차단했을 수도 있지만, 대상의 중단이나 경로 장애 등도 원인이 될 수 있다. 필터링을 확인하려면 장비의 정책·로그 등 추가 근거가 필요하다.

바. X: 기본적인 ping 출력은 대상 호스트의 응답 정보를 보여 주며, 경유 라우터별 IP 주소와 응답 시간을 순서대로 나열하는 기능은 일반적으로 **tracert·traceroute**에 해당한다. 다만 Windows ping에는 경로를 기록하는 /r 옵션과 홉별 도착 시각을 기록하는 /s 옵션이 있으므로, ping으로 경유지 정보를 전혀 얻을 수 없다는 뜻은 아니다. 이 보기는 일반적인 기본 출력과 경로 추적 기능을 구분하는 범위에서 제외한다.

이와 같이 기본 기능을 구분하면 해당 보기는 가·라이며, ①의 조합에 해당한다.

NoteBase

문 27. 다음과 같이 공격자가 조작된 요청을 웹서버에 전송하여 내부 네트워크에 있는 다른 서버에 악의적인 요청을 보내는 공격으로 가장 적절한 것은?



① SQL Injection

② CSS(Cross Site Scripting)

③ CSRF(Cross Site Request Forgery)

④ SSRF(Server Side Request Forgery)

정답 4번

간단한 해설

웹서버가 공격자 대신 내부 서버로 요청을 보내도록 유도하는 것이 SSRF이다. 피해 사용자의 브라우저가 요청을 보내는 CSRF와 요청 주체가 다르다.

NoteBase

도식 해설

공격자 → 웹서버: 외부 공격자는 웹서버가 처리할 요청을 조작한다. 핵심은 공격자가 내부 서버에 직접 접속하는 것이 아니라 웹서버의 요청 전송 기능을 악용한다는 점이다.

웹서버 → 내부 서버: 조작된 요청을 받은 웹서버가 내부 네트워크의 다른 서버로 요청을 보낸다. 외부에서 직접 접근하기 어려운 자원에 웹서버의 접근 가능성을 이용해 도달하는 구조가 SSRF의 특징이다.

응답 경로와 데이터베이스: 그림의 내부 서버 응답은 웹서버를 거쳐 공격자에게 돌아간다. 웹서버와 데이터베이스의 연결도 표시되어 있지만, 데이터베이스가 있다는 사실만으로 SQL Injection이라고 판단할 수는 없다. 이 그림의 결정적 흐름은 서버가 공격자가 유도한 요청을 다른 서버로 보내는 것이다.

공격의 구별: SQL Injection은 입력으로 SQL 문의 의미를 바꾸는 공격이고, Cross Site Scripting은 웹 콘텐츠에 삽입된 스크립트가 사용자의 브라우저에서 실행되도록 하는 공격이다. CSRF는 사용자의 브라우저가 의도하지 않은 요청을 보내게 하는 반면, SSRF는 서버가 요청을 보내게 한다.

따라서 제시된 구조에 해당하는 공격은 ④ SSRF(Server Side Request Forgery)이다.

NoteBase

문 28. 다음에서 설명하는 웹 아티팩트 분석 대상으로 가장 적절한 것은?

다운로드 받은 이미지, 텍스트 파일, 아이콘 등을 가지고 있고, 다운로드 URL, 다운로드 시간, 데이터 크기 등의 정보를 가지고 있다.

① 웹 브라우저 캐시
② 히스토리 분석
③ 웹 브라우저 쿠키
④ 시스템 로그

정답 1번

간단한 해설

웹 브라우저 캐시는 **이미 받은 이미지·텍스트·아이콘 등의 웹 자원**을 재사용하기 위해 보관한다. 자원 자체와 URL·시각·크기 등의 관리 정보를 함께 분석할 수 있다는 점이 핵심이다.

NoteBase

대응 관계 해설

다운로드한 이미지·텍스트 파일·아이콘: 웹 브라우저 캐시는 이미 받은 웹 자원을 저장하여 재방문할 때 다시 활용하는 공간이다. 지문처럼 **웹 자원의 내용 자체를 보관한다**는 특징이 캐시를 가리킨다. 이를 재사용하면 같은 자원을 매번 다시 전송받는 부담을 줄일 수 있다.

다운로드 URL·다운로드 시간·데이터 크기: 캐시에는 자원 데이터뿐 아니라 그 자원의 주소, 저장·갱신과 관련된 시각, 크기 등의 관리 정보가 함께 남을 수 있다. 이러한 정보는 캐시 데이터가 어떤 웹 자원에 대응하는지, 언제 저장되었는지 등을 분석하는 단서가 된다. 구체적인 저장 항목과 시각의 의미는 브라우저와 캐시 형식에 따라 다르다.

히스토리 분석과의 구별: 방문 URL과 방문 시각 같은 **방문 이력**을 중심으로 확인한다. URL과 시각이 있다는 사실만으로 캐시라고 단정하지 않고, 지문에 이미지·텍스트·아이콘의 데이터 자체를 가지고 있다는 조건까지 함께 보아야 한다.

웹 브라우저 쿠키와의 구별: 쿠키는 사이트가 로그인 상태나 사용자 설정 등을 유지하기 위해 브라우저에 저장하는 작은 상태 정보이다. 웹 페이지를 구성하는 이미지와 아이콘 등의 자원을 재사용하려고 보관하는 캐시와 목적이 다르다.

시스템 로그와의 구별: 시스템 로그는 운영체제나 서비스에서 발생한 이벤트와 동작 상태 등을 기록한다. 웹 자원과 그 캐시 관리 정보를 저장하는 브라우저 캐시와는 분석 대상이 다르다.

웹 자원 자체와 URL·시각·크기 정보를 함께 가진다는 지문의 특징은 웹 브라우저 캐시에 대응하므로 ①과 일치한다.

NoteBase

문 29. LAND 공격 기법으로 가장 적절하지 않은 것은?

① 출발지와 목적지의 IP 주소를 동일하게 공격대상의 IP 주소로 변조하여 전송한다.

② 패킷의 시퀀스 넘버를 조작해 데이터 부분이 중첩되도록 전송함으로써, 재조립하는데 CPU 과부하를 유발한다.

③ 패킷을 수신한 시스템은 응답하기 위해 출발지 IP 주소를 참조하는데, 출발지 IP 주소가 자신의 IP 주소이기 때문에 자신에게 응답하게 되고 이 과정을 반복하게 하여 과부하를 유발한다.

④ 동시 사용자 수를 점유하고 루프 상태가 되도록 함으로써, 시스템 과부하를 유발한다.

정답 2번

간단한 해설

LAND 공격은 **출발지와 목적지를 피해 시스템 자신으로 위조**하는 공격이다. 데이터 조각을 겹치게 만들어 재조립 오류를 유발하는 것은 LAND가 아니라 Teardrop 계열의 방식이다.

선지별 해설

LAND는 위조된 패킷에 취약한 시스템이 자신에게 응답하거나 비정상 연결을 유지하도록 유도하는 서비스 거부 공격이다. 실제 장애 형태는 운영체제와 구현에 따라 달라진다.

① O: 출발지와 목적지 IP 주소를 모두 공격 대상의 주소로 설정하는 것이 LAND의 핵심이다. 전형적인 공격에서는 TCP SYN 패킷의 출발지·목적지 포트도 동일하게 설정한다.

② X: 데이터 조각이 겹치도록 만들어 재조립 과정의 오류를 유발하는 설명은 Teardrop 계열에 해당한다. 정확히는 IP 단편의 오프셋 등 단편화 정보를 조작하는 것이며, TCP 시퀀스 번호와 IP 단편 오프셋을 혼동해서는 안 된다. LAND의 핵심은 단편 중첩이 아니라 출발지와 목적지의 동일한 위조이다.

③ O: 출발지가 자신의 주소로 위조되어 있으므로 피해 시스템의 응답도 자신을 향한다. 취약한 구현에서는 이러한 자기 응답이나 비정상 연결 처리로 자원이 소모되어 서비스 거부가 발생할 수 있다. 모든 현대 시스템에서 무한 반복이 반드시 발생한다는 뜻은 아니다.

④ O: 자신과의 비정상 연결이 유지되거나 반복 처리되면 연결 상태와 처리 자원을 점유하여 정상 서비스에 지장을 줄 수 있다. 여기서 동시 사용자 수 점유는 실제 사용자가 늘어난다는 뜻이 아니라 가용 연결·세션 자원이 소모된다는 의미이며, 루프는 취약한 시스템의 자기 응답 처리와 관련된다.

문 30. 다음에서 OSI 참조 모델의 물리 계층부터 응용 계층 순서로 공격을 나열한 것으로 가장 적절한 것은?

가. ARP Spoofing 공격
나. ICMP Redirect 공격
다. SQL Injection 공격
라. SYN Flooding 공격

① 가 - 나 - 다 - 라
② 가 - 나 - 라 - 다
③ 나 - 가 - 라 - 다
④ 나 - 다 - 가 - 라

정답 2번

간단한 해설

공격이 악용하는 기능을 기준으로 ARP는 데이터 링크, ICMP는 네트워크, TCP SYN은 전송, SQL 질의 처리는 응용 계층에 대응한다. 따라서 **낮은 계층에서 높은 계층**으로 배치하면 된다.

올바른 순서

가 → 나 → 라 → 다

가. ARP Spoofing 공격은 IP 주소와 MAC 주소의 대응 정보를 속여 같은 링크에서 프레임이 잘못된 MAC 주소로 전달되게 하는 공격이다. **MAC 주소 기반 전달에 영향을 주는 데이터 링크 계층**의 공격으로 분류한다. 제시된 보기 중 가장 낮은 계층에 해당하며, 물리 계층의 신호 자체를 공격한다는 뜻은 아니다.

나. ICMP Redirect 공격은 경로 변경을 알리는 ICMP 메시지를 악용하여 호스트가 잘못된 게이트웨이·경로를 사용하게 하는 공격이다. **IP 패킷의 경로 선택**에 영향을 주므로 네트워크 계층에 대응하며 데이터 링크 계층보다 위에 놓인다.

라. SYN Flooding 공격은 TCP 연결 설정 요청을 다량 발생시켜, 연결 설정이 완료되지 않은 상태와 관련 자원을 소모시키는 서비스 거부 공격이다. TCP의 **연결 설정 과정**을 악용하므로 전송 계층에 대응한다.

다. SQL Injection 공격은 응용 프로그램이 외부 입력을 안전하게 처리하지 못할 때 입력이 데이터베이스 질의의 일부로 해석되어 의도하지 않은 질의가 실행되게 하는 공격이다. **응용 프로그램의 입력 처리와 질의 구성**을 대상으로 하므로 응용 계층에 대응한다.

NoteBase

문 31. 다음에서 설명하는 공격 방법으로 가장 적절한 것은?

◯ 공격대상에게 공격 트래픽을 전송할 때 라우터나 웹서버 같은 제 3자를 이용하여 출발지가 어디인지 알지 못하게 한다.
◯ 3 way-handshake 취약점 및 ICMP 프로토콜의 Echo Request/Echo Reply를 이용한다.
◯ 공격자의 IP 주소를 스푸핑하여 전송하기 때문에 대규모의 네트워크가 불필요하다.
◯ 경유지 서버 목록을 활용한다.

① Zero Day 공격
② Ransomware 공격
③ DRDoS 공격
④ APT 공격

정답 3번

간단한 해설

DRDoS는 요청의 출발지를 피해자의 주소로 위조하여 **제3자의 응답이 피해자에게 집중되게** 하는 공격이다. 반사 장비를 이용하므로 공격자가 직접 보낸 트래픽만으로 공격하는 방식과 구별된다.

NoteBase

구성 요소별 해설

제3자를 통한 트래픽 전송: DRDoS는 분산 반사 서비스 거부 공격으로, 여러 서버나 네트워크 장비가 보내는 응답을 피해 대상에 집중시킨다. 피해자에게 직접 보이는 출발지는 반사 장비이므로 최초 공격자의 추적이 어려워지지만, 추적이 절대 불가능하다는 뜻은 아니다.

TCP·ICMP 응답의 이용: TCP 연결 설정 과정에서 SYN에 대해 SYN-ACK을 보내는 동작이나 ICMP Echo Request에 대해 Echo Reply를 보내는 동작이 반사에 악용될 수 있다. 정상적인 요청·응답 기능 자체가 이용되는 것이며, 반드시 모든 핸드셰이크를 완료해야 하는 것은 아니다.

출발지 IP 스푸핑: 공격자는 요청의 출발지 IP 주소를 피해 대상의 주소로 위조한다. 그러면 제3자의 응답이 피해자에게 향한다. 지문의 대규모 네트워크가 불필요하다는 말은 공격자가 대규모 감염 호스트 집단을 직접 확보하지 않고도 외부 반사 장비를 이용할 수 있다는 취지이지, 공격에 네트워크 자원이나 트래픽이 필요 없다는 뜻은 아니다.

경유지 서버 목록: 응답을 반사시킬 수 있는 서버들을 대상으로 삼아 여러 출발지의 응답이 한 피해자에게 모이게 한다. 반사 서버는 공격자에게 감염되거나 장악된 장비일 필요가 없다.

Zero Day는 대응책이 마련되지 않은 취약점의 악용, Ransomware는 데이터·시스템 접근을 막고 대가를 요구하는 방식, APT는 특정 대상을 상대로 지속하는 침투 활동이라는 점이 중심이다. 이 지문의 출발지 위조·제3자 반사·응답 집중을 함께 설명하는 것은 ③ DRDoS 공격이다.

NoteBase

문 32. 위협 정보 표현 규격(STIX, Structured Threat Information Expression)의 구성 항목으로 가장 적절하지 않은 것은?

① SDO(STIX Domain Objects)

② SAO(STIX Attribute Objects)

③ SCO(STIX Cyber-observable Objects)

④ SRO(STIX Relationship Objects)

정답 2번

간단한 해설

STIX에서 객체를 설명하는 속성은 존재하지만, **SAO(STIX Attribute Objects)는 표준 객체 분류가 아니다**.

선지별 해설

① O: SDO는 사이버 위협에 관한 주요 개념을 표현하는 도메인 객체이다. 악성코드, 위협 행위자, 공격 패턴, 캠페인 등 위협 분석에서 의미를 갖는 대상을 구조화하여 나타낸다.

② X: STIX Attribute Objects라는 SAO는 STIX의 표준 객체 분류가 아니다. 각 객체를 설명하는 이름·유형·식별자 등의 **속성(property)**과 도메인 객체·관측 객체·관계 객체 같은 객체 분류를 혼동하면 안 된다.

③ O: SCO는 시스템이나 네트워크에서 관찰할 수 있는 기술적 대상을 표현한다. 파일, IP 주소, 도메인 이름, 네트워크 트래픽 등이 해당한다. 이런 관측 대상 자체와 그 대상이 나타내는 악성코드·공격 행위 등의 위협 개념을 구별한다.

④ O: SRO는 STIX 객체 사이의 관계나 목격 사실을 표현하는 관계 객체이다. 예를 들어 위협 행위자가 특정 악성코드를 사용한다는 관계를 연결하거나 특정 대상을 관찰했다는 사실을 나타낼 수 있다. 객체들을 연결하여 위협 정보의 맥락을 구성한다.

NoteBase

문 33. 취약점 점수 시스템 CVSS 3.1의 기본 측정 항목 중 공격 경로(Attack Vector)의 값으로 가장 적절하지 않은 것은?

① Local

② Network

③ Physical

④ System

정답 4번

간단한 해설

CVSS 3.1의 공격 경로 값은 **Network, Adjacent, Local, Physical**이다. System은 이 측정 항목에 정의된 값이 아니다.

선지별 해설

① O: Local(L)은 공식 공격 경로 값이다. 취약한 구성 요소의 악용이 네트워크 스택을 직접 통하기보다 파일 읽기·쓰기·실행 등의 로컬 기능을 통해 이루어지는 경우에 해당한다. 공격자가 로컬 환경을 사용하거나 사용자를 유도해 악성 파일을 열게 하는 경우 등이 포함될 수 있으며, 반드시 장치를 직접 만져야 한다는 뜻은 아니다.

② O: Network(N)은 공식 공격 경로 값이다. 취약한 구성 요소가 네트워크 스택에 연결되어 있고, 인접 네트워크에 한정되지 않은 네트워크 경로를 통해 공격할 수 있는 경우에 해당한다. 인터넷으로부터의 원격 공격이 대표적이지만, 반드시 공개 인터넷에 노출되어 있어야만 이 값이 되는 것은 아니다.

③ O: Physical(P)은 공식 공격 경로 값이다. 취약점을 악용하려면 공격자가 **장치에 물리적으로 접근하거나 직접 조작**해야 하는 경우를 나타낸다. 단순히 로컬 프로그램의 취약점을 이용한다는 의미의 Local과 구별한다.

④ X: System은 CVSS 3.1의 Attack Vector 값이 아니다. 공식 값은 **Network(N), Adjacent(A), Local(L), Physical(P)**의 네 가지이다. 선지에 제시되지 않은 Adjacent는 동일한 물리·논리 네트워크나 제한된 관리 영역 등 인접한 네트워크 접근을 요구하는 경우이다.

NoteBase

문 34. 다음에서 설명하는 윈도우 암호화 기능으로 가장 적절한 것은?

◯ 드라이브를 암호화하는 기능으로 디스크 전체 볼륨을 암호화한다.
◯ 윈도우 파티션, USB 플래시 드라이브 등 파티션 전체를 암호화한다.
◯ PC의 모든 사용자 계정을 암호화하고 TPM 하드웨어를 사용한다.

① VSS
② EFS
③ BitLocker
④ Quotas

정답 3번

간단한 해설

BitLocker는 볼륨 단위로 데이터를 암호화하는 기능이다. 파일 수준의 EFS와 달리 보호 볼륨 전체를 대상으로 하며, TPM을 활용해 키와 부팅 환경을 보호할 수 있다.

구성 요소별 해설

볼륨 단위 암호화: BitLocker는 개별 파일만 선택하는 방식이 아니라 드라이브의 볼륨을 암호화하여 분실·도난이나 디스크 분리 후의 오프라인 데이터 접근에 대비한다. 여기서 전체 볼륨이란 보호 대상으로 지정한 볼륨을 뜻하며, 모든 물리 디스크의 모든 파티션을 무조건 암호화한다는 의미는 아니다.

윈도우·USB 드라이브: 운영체제가 설치된 볼륨뿐 아니라 데이터 볼륨도 보호할 수 있다. USB 플래시 드라이브 같은 이동식 데이터 드라이브의 보호는 BitLocker To Go로 구분한다.

사용자 범위와 TPM: 지문의 모든 사용자 계정 암호화는 특정 사용자 파일만이 아니라 보호 볼륨에 저장된 여러 사용자의 데이터를 함께 보호한다는 취지이다. 계정 자체를 각각 암호화하는 기능이라는 뜻은 아니다. TPM은 키 보호와 부팅 환경의 무결성 확인에 이용되며, 조건에 따라 TPM 없이 시작 키 등을 사용하는 구성도 가능하므로 TPM이 모든 구성에서 절대 필수인 것은 아니다.

다른 기능과의 구별: VSS는 백업 등에 사용하는 볼륨 섀도 복사본을 만드는 서비스이다. EFS는 파일·폴더 수준의 암호화로 사용자 인증서·키와 연결된다. Quotas는 사용자의 디스크 사용량을 관리·제한하는 기능이다.

따라서 볼륨 단위 암호화와 TPM 활용이라는 핵심 단서를 만족하는 기능은 ③ BitLocker이다.

NoteBase

문 35. 다음에서 설명하는 것으로 가장 적절한 것은?

◯ 불특정 다수가 아닌 특정기관이나 기업의 내부직원을 목표로 삼아 집중적으로 공격하는 행위를 말한다.
◯ 정부기관이나 기업조직 등 특정목표의 내부 사용자를 은밀히 염탐하고 해당 조직의 기밀정보를 빼내기 위하여, 신뢰할 수 있는 내용처럼 위장한 악성 이메일(악성 링크나 악성 코드를 삽입)을 관련자들에게 전송하여 감염시킨다.
◯ 이후 원격제어 및 데이터 탈취 등을 시도하는 대표적인 지능형 공격이다.

① 랜섬웨어
② 애드웨어
③ 메신저 피싱
④ 스피어 피싱

정답 4번

간단한 해설

특정 조직·개인을 겨냥한 맞춤형 기만이 스피어 피싱의 핵심이다. 지문은 내부 직원이 신뢰할 만한 이메일로 위장하여 악성 링크·코드를 전달하는 표적형 공격을 설명한다.

NoteBase

대응 관계 해설

특정 내부 직원이라는 대상: 스피어 피싱은 불특정 다수에게 같은 메시지를 뿌리는 방식과 달리 **특정 개인·조직에 맞추어** 신뢰할 만한 메시지로 위장하는 표적형 피싱이다. 첫 번째 설명의 특정 기관·기업 내부 직원이라는 조건이 이에 대응한다.

신뢰를 위장한 이메일이라는 수단: 대상의 업무·관계 등에 맞춘 이메일로 악성 링크나 첨부파일을 신뢰하게 만들어 정보 입력이나 악성코드 실행 등을 유도한다. 두 번째 설명은 이러한 **맞춤형 기만과 이메일 전달**을 나타낸다.

원격제어·데이터 탈취라는 후속 행위: 악성코드 감염이 이루어지면 공격자가 원격제어나 기밀 탈취를 시도할 수 있다. 이는 스피어 피싱을 침투 수단으로 삼았을 때 이어질 수 있는 결과이며, 모든 스피어 피싱에 원격제어나 감염이 반드시 발생해야 하는 것은 아니다.

다른 명칭과의 구별: 랜섬웨어는 파일 암호화·시스템 사용 제한 등을 통해 대가를 요구하는 악성코드이고, 애드웨어는 광고 표시를 주요 기능으로 하는 소프트웨어이다. 메신저 피싱은 메신저에서 신뢰 관계를 사칭하는 등 기만을 하는 방식으로, 지문의 이메일 수단과 구별된다. 표적 선정 방식과 전달 매체는 서로 다른 분류 기준이므로 실제 공격에서 함께 나타날 수도 있다.

특정 조직의 내부 사용자를 겨냥하고 신뢰할 내용으로 위장한 이메일을 이용한다는 설명은 스피어 피싱에 대응하므로 ④에 해당한다.

NoteBase

문 36. HTTP 요청과 응답시 헤더정보에 공통으로 들어가는 항목으로 가장 적절한 것은?

① Authorization

② Referer

③ Connection

④ Location

정답 3번

간단한 해설

HTTP/1.x에서 **Connection은 요청과 응답 양쪽**에 연결 제어 옵션을 전달할 수 있다. Authorization과 Referer는 요청 헤더이고, Location은 응답 헤더이다.

선지별 해설

이 문항의 공통 헤더 분류는 HTTP/1.x를 기준으로 한다. 여기서 공통이라는 것은 요청과 응답 양쪽에 사용할 수 있다는 뜻이지, 모든 메시지에 반드시 포함된다는 뜻은 아니다.

① X: Authorization은 클라이언트가 원 서버에 자신을 인증하기 위한 자격 정보를 보내는 **요청 헤더**이다. 서버가 인증 방식을 요구할 때 응답에 사용하는 WWW-Authenticate와 구별된다.

② X: Referer는 현재 요청의 대상 URI를 얻게 된 이전 자원의 URI 정보를 서버에 전달하는 **요청 헤더**이다. 서버가 이동할 위치를 안내하는 응답 헤더와 다르며, 개인정보 보호 정책 등에 따라 생략되거나 정보가 제한될 수 있다.

③ O: Connection은 현재 연결에 적용할 제어 옵션을 나타내며 HTTP/1.x의 **요청과 응답 양쪽에 사용**된다. 예를 들어 'Connection: close'는 현재 요청·응답 이후 연결을 닫으려는 의사를 나타낸다. 인접한 통신 상대와의 연결에 관한 정보이지 최종 목적지까지 그대로 전달하는 정보가 아니다. HTTP/2에서는 Connection 필드를 허용하지 않으므로 모든 HTTP 버전에 공통이라고 확대해서는 안 된다.

④ X: Location은 리다이렉션할 자원의 위치나 새로 생성한 자원의 위치 등을 알리는 **응답 헤더**이다. 클라이언트가 요청을 보내게 된 이전 자원을 알리는 Referer와 구별된다.

NoteBase

문 37. /etc/shadow 파일 정보에 대한 설명으로 가장 적절하지 않은 것은?

```
root: $6$p4Hf~중략~T9g/: 14923: 0: 99999: 7: : :
                          ㉠   ㉡   ㉢   ㉣
```

① ㉠은 1970년 1월 1일부터 마지막으로 패스워드를 변경한 날까지의 일 수이다.

② ㉡은 패스워드를 변경하기 전에 최소 사용 기간의 일 수이다.

③ ㉢은 패스워드를 변경하지 않고 최대한 사용할 수 있는 기간의 일 수이다.

④ ㉣은 계정의 사용 제한을 결정하고 며칠 후에 완전히 사용을 정지할지 설정한다.

정답 4번

간단한 해설

㉣의 7은 계정 정지 유예기간이 아니라 **비밀번호 만료 전 경고 기간**이다. 비밀번호 만료 후의 비활성 기간과 계정 만료일은 별도 필드로 관리한다.

선지별 해설

/etc/shadow의 각 행은 콜론으로 구분한 필드를 갖는다. 그림에서 사용자 이름과 비밀번호 해시 뒤의 14923, 0, 99999, 7이 차례로 ㉠, ㉡, ㉢, ㉣에 대응한다.

① O: ㉠은 마지막 비밀번호 변경 날짜를 1970년 1월 1일을 기준으로 지난 일수로 저장한 필드이다. 14923은 변경 후 14923일이 지났다는 뜻이 아니라 기준일부터 변경일까지의 일수이다.

② O: ㉡은 비밀번호를 다시 바꾸기 전에 기다려야 하는 최소 일수이다. 값이 0이므로 최소 사용 기간의 제한 없이 다시 변경할 수 있다.

③ O: ㉢은 비밀번호 변경 후 최대 사용 기간이다. 그림의 99999는 최대 사용 기간을 99999일로 설정한 값이다. 기간이 지나면 비밀번호 갱신을 요구하는 것으로, 계정 자체의 만료 날짜와는 다르다.

④ X: ㉣은 비밀번호 만료 전 경고 기간이다. 값이 7이므로 만료 7일 전부터 변경 경고를 제공하는 기간을 뜻한다. 비밀번호 만료 후 얼마 동안 갱신을 허용하다가 사용을 제한할지는 다음의 비활성 기간 필드이며, 계정 자체의 만료일은 그다음 별도 필드이다.

NoteBase

문 38. 스위치 환경에서의 스니핑(Sniffing)과 관련된 공격으로 가장 적절하지 않은 것은?

① IP Spoofing

② Switch Jamming

③ ARP Spoofing

④ ICMP Redirect

정답 1번

간단한 해설

IP Spoofing은 **출발지 IP 주소를 위조**하는 기법이다. 주소 위조만으로 다른 호스트의 트래픽이 공격자에게 전달되는 것은 아니므로, 전달 경로나 주소 대응을 바꾸는 스니핑 기법과 구별된다.

선지별 해설

① X: IP Spoofing은 IP 패킷의 **출발지 IP 주소를 위조**하여 다른 호스트가 보낸 것처럼 가장하는 공격이다. 주소를 위조하는 것만으로 스위치의 전달 경로나 피해자의 수신 트래픽이 공격자 쪽으로 바뀌지는 않으므로, 스위치 환경에서 다른 호스트의 트래픽을 가로채는 기법으로는 가장 적절하지 않다.

② O: Switch Jamming은 다수의 위조된 출발지 MAC 주소를 보내 스위치의 MAC 주소 테이블을 소진시키는 공격이다. 목적지 MAC 주소를 학습하지 못한 프레임이 **같은 VLAN의 여러 포트로 플러딩**되면 공격자가 다른 호스트의 트래픽을 엿볼 수 있다. 모든 스위치가 반드시 허브처럼 동작한다는 뜻은 아니며, 동작과 방어 기능에 따라 공격 효과가 달라진다.

③ O: ARP Spoofing은 거짓 ARP 정보를 보내 피해자의 IP 주소와 MAC 주소 대응을 오염시키는 공격이다. 게이트웨이 등의 IP 주소에 **공격자의 MAC 주소를 대응**시키면 피해자가 보내는 프레임이 공격자에게 전달되어 스니핑이나 중간자 공격에 이용될 수 있다.

④ O: ICMP Redirect는 원래 호스트에게 더 적절한 다음 홉을 알려 주는 메시지이다. 이를 악용해 거짓 경로 정보를 수용하게 하면 **통신 경로를 공격자 쪽으로 유도**하여 트래픽을 가로챌 수 있다. 호스트가 위조된 리다이렉트 정보를 받아들이는 조건에서 성립하는 공격이다.

NoteBase

문 39. 다음에서 설명하는 SYN Flooding 대응 방법으로 옳은 것을 모두 고른 것으로 가장 적절한 것은?

가. IP당 SYN 요청에 대한 PPS(Packet per Second) 임계치를 단계적으로 조정한다.
나. SYN 패킷을 보낸 클라이언트의 존재 여부를 파악하여 차단한다.
다. 트래픽 유형별 임계치를 조정하여 TCP 세션 연결을 차단한다.
라. 임시적 방법으로 서버의 Queue 크기를 감소시킨다.

① 가, 나
② 가, 다
③ 가, 나, 다
④ 가, 나, 다, 라

정답 3번

간단한 해설

SYN Flooding은 연결을 완성하지 않은 요청을 쌓아 서버의 대기 자원을 소진시키는 공격이다. 요청량 제한과 클라이언트 검증이 대응 방법이며, 대기 큐를 조정한다면 임시로 **크기를 늘려야 하므로 '감소시킨다'는 표현은 잘못**이다.

NoteBase

보기별 해설

가. O: PPS는 초당 처리하는 패킷 수이다. IP별 SYN 요청량에 임계치를 두고 이를 정상 트래픽에 맞게 단계적으로 조정하면 특정 출발지의 과도한 연결 요청을 제한할 수 있다. 정상 접속까지 막지 않도록 **정상적인 요청량과 공격성 요청량을 구별**하는 기준이 필요하다.

나. O: SYN Flooding은 출발지 주소를 위조하거나 연결을 끝까지 완성하지 않는 요청으로 서버의 자원을 점유할 수 있다. 응답 확인이나 연결 검증으로 **실제로 응답하는 클라이언트인지 확인**하고, 검증되지 않는 요청을 차단하면 위조된 요청이 서버 자원을 소비하는 것을 줄일 수 있다.

다. O: 정상 트래픽의 특성에 맞추어 유형별 임계치를 설정하면 비정상적으로 많은 SYN 요청이나 불완전 연결을 탐지하여 해당 TCP 연결 시도를 제한할 수 있다. 모든 TCP 연결을 무조건 막는 것이 아니라 **임계치를 넘는 비정상 연결을 선별하여 차단**하는 대응이다.

라. X: SYN 요청을 받은 서버는 연결이 완성될 때까지 대기 정보를 큐에 보관한다. 이 큐의 크기를 줄이면 더 적은 요청으로 큐가 차므로 공격에 더 취약해질 수 있다. 임시 완화 방법은 **대기 큐의 크기를 늘리는 것**이며, 큐 확대만으로 지속적인 대량 공격을 근본적으로 해결할 수 있는 것은 아니다.

따라서 적절한 대응은 가, 나, 다이며, 이를 모두 포함한 ③과 일치한다.

NoteBase

문 40. 세션 하이재킹(Session Hijacking)의 탐지방법으로 가장 적절하지 않은 것은?

① 서버와 순서번호를 주기적으로 검사하여 비동기화 상태인지 탐지한다.

② 전송 중 윈도우 크기와 순서번호가 맞지 않는 상태가 되면 교정 패킷이 정상적으로 동작하지 못하게 되어, 무한루프에 빠지기 때문에 ACK 패킷의 비율이 감소하는지 탐지한다.

③ 공격자가 중간에 끼어있기 때문에 패킷의 유실과 재전송 발생, 서버와의 응답 시간이 증가하는지 탐지한다.

④ 접속 초기에 예상하지 못한 세션의 리셋이 발생하는지 탐지한다.

정답 2번

간단한 해설

비동기화된 TCP 연결에서 확인응답이 반복되는 'ACK 폭풍'이 발생하면 **ACK 패킷의 비율이 증가**한다. 감소 여부를 탐지한다는 설명은 방향이 반대이다.

선지별 해설

① O: TCP는 송신 순서번호와 수신 측이 기대하는 다음 순서번호를 이용하여 연결 상태를 유지한다. 양 끝의 순서번호와 확인응답번호를 대조하면 **정상적인 전송 흐름에서 벗어난 비동기화**를 탐지할 수 있다.

② X: 비동기화된 양 끝이 상대방의 패킷을 받아들이지 못하고 기대하는 번호를 담은 ACK를 되풀이하여 보내면 'ACK 폭풍'이 발생할 수 있다. 따라서 탐지할 현상은 **ACK 패킷 비율의 감소가 아니라 증가**이다. 모든 환경에서 무한히 지속되는 것은 아니며, 패킷 유실 등으로 반복이 끊길 수 있다.

③ O: 공격자의 개입과 비동기화로 패킷이 수용되지 않거나 유실되면 재전송이 늘고 정상 응답이 지연될 수 있다. **유실·재전송·응답 시간의 비정상적 증가**는 세션 하이재킹을 의심할 수 있는 징후이다. 다만 혼잡이나 장애도 같은 현상을 일으킬 수 있으므로 이것만으로 공격을 확정하지는 않는다.

④ O: 초기 연결을 끊고 다른 순서번호로 다시 연결하는 공격 방식에서는 **예상하지 못한 RST에 의한 연결 초기화**가 나타날 수 있다. 따라서 접속 초기의 비정상적인 세션 리셋을 감시하는 것도 탐지에 활용된다.

NoteBase