2023년 정보보안기사 필기 기출문제

전 회차 · 29문항 · 정답·해설 포함

출처: 모두CBT(moducbt.com) 공개 기출문제를 연도별·회차별로 정리한 자료입니다.

2023년 정보보안기사 필기

제1회 · 29문항

[1번] 윈도우 시스템의 사용자 계정 및 패스워드를 암호화하여 보관하고 있는 SAM(Security Account Manager)에 대한 설명으로 틀린 것은?

1HKEY_LOCAL_MACHINE\SAM에 저장된 키는 일반계정도 확인할 수 있다.
2크래킹을 통해 패스워드를 얻을 수 있다.
3운영체제가 작동하는 한 접근할 수 없도록 잠겨져 있다.
4레지스트리 HKEY_LOCAL_MACHINE\SAM에 구체화된 자료들을 실제로 저장한다.

▸ SAM은 운영체제가 동작하는 동안 잠겨 있어 일반 계정이 레지스트리 경로로 직접 열람할 수 없다. SAM은 사용자 계정과 해시화된 패스워드를 HKEY_LOCAL_MACHINE\SAM 레지스트리에 실제로 저장하며, 오프라인 부팅이나 크래킹 도구로 해시를 추출해 패스워드를 얻는 공격이 가능하다. 따라서 SAM 값을 일반 계정도 확인할 수 있다는 설명은 사실과 다르다.

[2번] 디스크 스케줄링 알고리즘 중 엘리베이터 알고리즘이라고 불리는 기법은?

▸ 디스크 스케줄링에서 엘리베이터 알고리즘이라 불리는 기법은 SCAN이다. 헤드가 디스크의 한쪽 끝에서 반대쪽 끝까지 이동하며 경로상의 요청을 순차 처리하고, 끝에 도달하면 방향을 바꿔 다시 처리하는 방식이 엘리베이터가 오르내리며 각 층에 서는 동작과 비슷해 이 이름이 붙었다. SSTF는 탐색거리가 가장 짧은 요청을 우선 처리하고, C-SCAN은 항상 한쪽 방향으로만 이동하며, FCFS는 요청 순서 그대로 처리한다는 점에서 SCAN과 구분된다.

[3번] 윈도우에서 제공하는 BitLocker에 대한 설명으로 틀린 것은?

1윈도우 7에서도 가능하다.
2exFAT 파일 시스템은 지원하지 않는다.
3USB 저장매체도 지원 가능하다.
4텍스트 파일 형태의 복구키를 제공한다.

▸ BitLocker는 NTFS뿐 아니라 exFAT, FAT32 등 다양한 파일 시스템의 볼륨도 암호화할 수 있어, exFAT을 지원하지 않는다는 설명은 사실과 다르다. 윈도우 7부터 제공되기 시작했고 USB 등 이동식 저장매체 암호화(BitLocker To Go)도 지원하며, 복구 시 사용할 복구 키를 텍스트 파일 형태로 출력해 보관할 수 있다.

[4번] EDR(Endpoint Detection Response) 솔루션의 주요 기능으로 옳지 않은 것은?

1보안사고 탐지 영역
2보안사고 통제 영역
3보안사고 확산 영역
4보안사고 치료 영역

▸ EDR은 엔드포인트에서 발생하는 위협을 탐지하고 대응(통제·치료)하는 데 초점을 둔 솔루션으로, 침해 지표를 수집·분석해 이상행위를 찾아내고 격리·차단·복구 조치를 수행한다. 보안사고가 확산되는 것은 EDR이 막아야 할 결과이지, 솔루션이 다루는 기능 영역으로 분류되는 범주가 아니다.

[5번] Window 서버의 보안 옵션 설정 중 보안 강화를 위한 설정으로 옳지 않은 것은?

1 “로그온 하지 않고 시스템 종료 허용” 을 “사용 안함” 으로 설정하였다.
2원격 관리를 위해 “원격 시스템에서 강제로 종료” 정책의 “Administrators” 외 서버에 등록된 계정을 모두 등록하였다.
3 “이동식 미디어 포맷 및 꺼내기 허용” 정책이 “Administrators” 로 되어 있다.
4 “SAM 계정과 공유의 익명 열거 허용 안함” 정책을 설정하였다.

▸ 서버 보안 강화 관점에서는 원격에서 강제 종료할 수 있는 권한을 Administrators로 한정해야 하며, 필요 이상의 계정에 이 권한을 부여하는 것은 오히려 보안을 약화시키는 설정이다. * 로그온 없이 시스템 종료를 허용하지 않도록 설정하는 것은 물리적 접근 통제를 강화하는 조치다. * 이동식 미디어 포맷·꺼내기 권한을 관리자로 제한하는 것도 권장 설정이다. * SAM 계정 및 공유의 익명 열거를 막는 것도 정보 노출을 줄이는 강화 조치다.

[6번] 웹사이트의 쿠키(cookie)에 대한 설명으로 틀린 것은?

1Set-Cookie 헤더를 통해 쿠키를 설정
2여러개의 값을 추가시 “/” 특수문자를 사용
3쿠키의 구조는 이름=값 형태로 구성
4사용자 PC에 저장

▸ 쿠키에서 하나의 헤더에 여러 값을 추가할 때는 세미콜론(;)으로 구분하며, 슬래시(/)는 쿠키가 유효한 경로(Path 속성)를 지정할 때 쓰인다. 쿠키는 Set-Cookie 응답 헤더로 서버가 설정하고 이름=값 형태의 구조로 사용자 PC(브라우저)에 저장된다.

[7번] 다음 문장에서 설명하는 공격으로 올바르게 짝지어진 것은?

1㉠ : Warwalking, ㉡ : Evil Twin
2㉠ : 사전 공격, ㉡ : 무차별 공격
3㉠ : 무차별 공격, ㉡ : 사전 공격
4㉠ : Evil Twin, ㉡ : Wardriving

▸ ㉠은 무차별 공격(Brute Force), ㉡은 사전 공격(Dictionary Attack)이다. ㉠은 "도구를 이용하여 ID, 패스워드를 자동 조합하여 크랙"한다고 했다. 가능한 문자 조합을 기계적으로 전수 대입하는 방식이므로 무차별 공격이다. ㉡은 "ID와 패스워드가 될 가능성이 있는 단어를 사전파일로 만들어놓고 사전파일의 단어를 대입"한다고 했다. 미리 준비한 단어 목록만 순서대로 시도하므로 사전 공격이다. 나머지 용어는 유선 계정 크랙이 아니라 무선랜 관련 기법이다. * Wardriving·Warwalking: 차량이나 도보로 이동하며 무선 AP의 위치와 보안 설정을 탐색하는 행위 * Evil Twin: 정상 AP와 같은 SSID의 가짜 AP를 띄워 단말의 접속을 유도하는 공격

[8번] 내부 정보 유출 차단용 보안솔루션에 대한 설명으로 틀린 것은?

1문서암호화 솔루션 : PC에 저장되는 파일을 암호화하고 외부로 유출시 복호화 기능
2내부정보 유출 방지 솔루션 : 메일, 메신저, 웹 등을 통해 발생할 수 있는 중요정보 유출을 탐지, 차단
3문서중앙화 시스템 : 문서 작업의 결과가 원천적으로 PC에 남지 않으므로 파일 유출을 차단
4네트워크 방화벽 : PC 메신저나 웹 메일 등 내부정보유출 수단으로 쓰이는 프로그램을 네트워크 방화벽에서 도메인 기준으로 차단

▸ 문서암호화 솔루션(DRM)은 PC 내 파일을 암호화해 두었다가 조직 외부로 반출되면 복호화되지 않도록 막는 것이 핵심 기능이며, 외부 유출 시 복호화를 지원한다는 설명은 목적과 반대된다. 내부정보 유출 방지 솔루션(DLP)은 메일·메신저·웹 등을 통한 중요정보 유출을 탐지·차단하고, 문서중앙화 시스템은 문서를 PC에 남기지 않아 유출 경로 자체를 차단하며, 네트워크 방화벽도 도메인 기준으로 유출 경로를 차단하는 데 활용될 수 있다.

[9번] 리눅스 환경에서 로그에 대한 설명으로 틀린 것은?

1secure 로그 : 사용자의 원격 로그인 정보를 저장
2dmesg 로그 : 시스템 부팅 관련 시스템 메시지 저장
3lastlog 로그 : 사용자가 로그인한 마지막 로그를 저장
4wtmp 로그 : 사용자의 루트 접속 기록 저장

▸ wtmp 로그는 루트 계정에 국한되지 않고 모든 사용자의 로그인·로그아웃 이력을 기록하므로, 루트 접속 기록만 저장한다는 설명은 옳지 않다. secure 로그는 원격 로그인 등 인증 관련 정보를, dmesg 로그는 부팅 시 커널 메시지를, lastlog 로그는 각 사용자의 가장 최근 로그인 기록을 저장한다.

[10번] 윈도우 시스템 암호화에 대한 설명으로 틀린 것은?

1BitLocker는 윈도우 운영체제에서 제공하는 볼륨 단위와 암호화 기능이다.
2BitLocker는 컴퓨터를 시작하는데 필요한 시스템 파티션 부분도 암호화한다.
3EFS(Encrypted File Service)는 사용자 단위 데이터 암호화 기능을 제공한다.
4EFS(Encrypted File Service)는 컴퓨터 단일 또는 복수 사용자에게 대한 파일 및 폴더 단위 암호화를 지원한다.

▸ BitLocker는 볼륨 단위 암호화 기능이지만, 컴퓨터 부팅에 필요한 시스템(부트) 파티션 자체는 암호화 대상에서 제외되어 별도의 암호화되지 않은 영역으로 남는다. EFS는 사용자 단위로 동작해 파일·폴더 단위 암호화를 제공하며, 하나의 컴퓨터에서 단일 또는 여러 사용자에게 각각 적용될 수 있다.

[11번] AI나 머신러닝의 이미지 인식에 있어서 이미지 속에 인간이 감지할 수 없는 노이즈나 작은 변화를 주어 AI 알고리즘의 특성을 악용하여 잘못된 판단을 유도하는 공격은?

1Membership inversion 공격
2Adversarial 공격
3Poisoning 공격
4Model inversion 공격

▸ 이미지에 사람이 인지하기 어려운 미세한 노이즈를 추가해 AI 모델이 잘못된 분류·판단을 내리도록 유도하는 공격은 Adversarial(적대적) 공격이다. Model inversion 공격은 모델 출력으로부터 학습 데이터를 역으로 추정하는 공격이고, Membership inversion 공격은 특정 데이터가 학습에 사용되었는지를 추정하는 공격이며, Poisoning 공격은 학습 단계에 악의적 데이터를 주입해 모델을 오염시키는 공격이라는 점에서 서로 다르다.

[12번] 다음은 포맷스트링의 종류를 설명하고 있다. 형식에 대한 매개변수는?

1㉠ : %s, ㉡ : %o, ㉢ : %lf
2㉠ : %s, ㉡ : %x, ㉢ : %hn
3㉠ : %c, ㉡ : %o, ㉢ : %lf
4㉠ : %c, ㉡ : %x, ㉢ : %hn

▸ ㉠은 %s, ㉡은 %x, ㉢은 %hn이다. 표에서 ㉠의 형식은 "문자스트링"이므로 문자열 포인터를 받아 출력하는 %s가 들어간다. ㉡은 "16진수 양의 정수"이므로 부호 없는 값을 16진수로 출력하는 %x이다. ㉢은 "%n의 반인 2바이트 단위"라고 했다. %n은 그때까지 출력된 바이트 수를 4바이트 정수 단위로 메모리에 써 넣는데, short를 뜻하는 h를 붙인 %hn은 절반인 2바이트 단위로 기록한다. 포맷스트링 공격에서 주소를 상·하위로 쪼개 덮어쓸 때 쓰이는 지시자다. %c는 문자 하나, %o는 8진수, %lf는 double 실수를 출력하므로 표의 설명과 맞지 않는다.

[13번] netstat 명령어를 통해 확인할 수 없는 정보는?

1소켓을 열고 있는 프로세스 ID, 프로세스 이름
2라우팅 테이블 정보
3열린 포트 정보
4데이터 패킷

▸ netstat 명령어는 열린 포트와 소켓을 사용 중인 프로세스의 PID·이름, 라우팅 테이블 정보까지 확인할 수 있지만, 오가는 데이터 패킷 자체의 내용은 보여주지 않는다. 패킷 내용을 확인하려면 tcpdump나 Wireshark 같은 패킷 캡처 도구가 필요하다.

[14번] 리눅스에서 제공하는 Cron 기능에 대한 설명으로 틀린 것은?

1crontab –r 명령어로 등록된 데이터를 삭제할 수 있다.
2루트 권한으로 실행은 불가능하다.
3특정 시간에 작업해야 하는 명령어 실행이 가능하다.
4파이썬, 펄 등의 스크립트 언어도 실행이 가능하다.

▸ cron은 루트 계정으로도 실행할 수 있어, root의 crontab에 등록된 작업은 시스템 전반에 강력한 권한으로 동작하므로 오히려 더 엄격히 관리해야 한다. crontab -r로 등록된 작업을 삭제할 수 있고, 특정 시각에 명령을 실행하도록 예약할 수 있으며, 셸 스크립트뿐 아니라 파이썬·펄 등 스크립트 언어로 작성된 작업도 실행 가능하다.

[15번] Visual Basic 스크립트를 이용한 악성코드에 대한 설명으로 옳은 것은?

1웹브라우저에서 실행될 경우 스크립트가 브라우저에 내장되므로 파일의 내용을 확인하기 어렵다.
2독립형으로 개발할 경우 파일 생성에 제한을 받아 웜형 악성코드를 만들지 못한다.
3확장자는 VBA 이다.
4러브버그라고 불리는 이메일에 첨부되어 전파된 바이러스가 Visual Basic 스크립트로 개발되었다.

▸ 이메일에 첨부되어 전 세계적으로 퍼진 러브버그(ILOVEYOU) 웜은 Visual Basic 스크립트로 작성된 대표적 사례다. 이런 스크립트는 브라우저에 내장되어 실행되더라도 텍스트로 저장되므로 내용을 비교적 쉽게 확인할 수 있고, 파일 시스

템에 자신을 복제하는 방식으로 웜형 악성코드 제작도 가능하며, 확장자는 VBS이지 VBA가 아니다.

[16번] 다음은 sudo 설정파일(/etc/sudoers)의 내용이다. sudo를 통한 명령 사용이 불가능한 사용자는?

1uid=(10)guest1, gid(10)guest1, groups=(10)guest1,3(admin)
2uid=(11)guest2, gid(11)guest2, groups=(11)guest2,4(sudo)
3uid=(12)guest3, gid(12)guest3, groups=(12)guest3,5(adm)
4uid=(13)guest4, gid(13)guest4, groups=(13)guest4,5(adm)

▸ 보조그룹이 adm뿐이고 사용자 이름도 등록돼 있지 않은 guest4가 sudo를 쓸 수 없다. 설정 파일에는 그룹 규칙 두 줄(%admin, %sudo)과 사용자 규칙 두 줄(root, guest3)만 있다. %로 시작하는 줄은 그룹, %가 없는 줄은 개별 사용자 이름을 가리킨다. 그래서 나머지 세 사용자는 모두 권한을 얻는다. * 보조그룹에 3(admin)이 있는 guest1 → %admin 규칙으로 허용 * 보조그룹에 4(sudo)가 있는 guest2 → %sudo 규칙으로 허용 * guest3 → 사용자 이름이 직접 등록돼 허용 guest4의 보조그룹 5(adm)에 해당하는 %adm 줄이 파일에 없으므로 이 사용자만 sudo 실행이 거부된다.

[17번] 랜섬웨어에 대한 설명으로 틀린 것은?

1단방향 암호화 방식을 주로 사용한다.
2파일 확장자를 임의 변경한다.
3안티바이러스 프로그램을 강제 종료한다.
4윈도우 복원 시점을 제거한다.

▸ 랜섬웨어는 피해자가 금전을 지불하면 파일을 복구해 주어야 하므로, 되돌릴 수 없는 단방향(해시) 암호화가 아니라 복호화가 가능한 대칭·비대칭 키 기반 암호화를 사용한다. 파일 확장자를 임의로 변경하고, 탐지를 피하기 위해 백신 프로그램을 강제 종료하며, 복구를 막기 위해 윈도우의 복원 시점(볼륨 섀도 복사본)을 제거하는 것이 랜섬웨어의 전형적 행동이다.

[18번] 리버스엔지니어링 분석 방법 중 소스코드를 이해하고 분석하는 방법으로 소프트웨어의 프로그래밍 오류와 구현 오류를 찾을 때 유용한 분석 방법은?

1블랙박스 분석
2화이트박스 분석
3그레이박스 분석
4그린박스 분석

▸ 소스코드를 직접 확인하며 프로그래밍·구현상의 오류를 찾아내는 리버스엔지니어링 분석 방법은 화이트박스 분석이다. 블랙박스 분석은 소스코드 없이 입출력만으로 동작을 파악하는 방식이고, 그레이박스 분석은 제한된 내부 정보만 활용해 두 방식을 절충한 방법이라는 점에서 구분된다.

[19번] 침해 당한 리눅스 서버의 하드 디스크를 umount 명령을 통해 분리하는 과정에서 “Device is busy”라는 문구 때문에 분리하지 못하고 있는 상황이다. 디바이스를 사용 중인 프로세스를 찾기 위해 사용할 수 있는 명령어로 옳은 것은?

▸ 특정 디바이스나 파일을 사용 중인 프로세스를 확인할 때는 lsof(list open files) 명령을 사용하며, 마운트 해제 시 나타나는 “Device is busy” 문제의 원인 프로세스를 찾아 종료한 뒤 언마운트를 진행할 수 있다. mount는 마운트 상태 확인, ps는 프로세스 목록 확인, netstat은 네트워크 연결 확인에 쓰이는 명령이라 이 상황에 직접적인 해답을 주지 않는다.

[20번] 다음 중 파일 시스템의 무결성 보장을 위해 점검해야 할 사항으로 옳지 않은 것은?

1파일의 소유자, 소유그룹 등의 변경 여부 점검
2파일의 크기 변경 점검
3최근에 파일에 접근한 시간 점검
4파일의 symbolic link의 수 점검

▸ 파일 무결성 점검은 소유자·소유그룹 변경 여부, 파일 크기 변경, 접근·수정 시각(atime·mtime), 그리고 하드링크 개수 같은 항목을 대조해 변조 흔적을 찾는 방식으로 이뤄진다. 심볼릭 링크의 개수는 무결성 검사에서 통상적으로 점검하는 항목이 아니어서, 이를 점검 대상으로 제시한 설명은 적절하지 않다.

[21번] 다음 문장에서 설명하는 보안시스템은?

▸ IP 관리 시스템에서 발전했고 MAC 주소를 기반으로 접근 제어·인증을 수행하는 것은 NAC(Network Access Control)이다. NAC는 단말이 네트워크에 붙는 시점에 MAC 주소로 등록 자산인지 확인하고, 백신·패치 등 보안 상태가 기준에 못 미치면 격리하거나 차단한다. 지문의 "IP 관리 시스템에 네트워크에 대한 통제를 강화"가 바로 이 발전 과정을 가리킨다. 나머지는 목적이 다르다. * DRM: 문서·콘텐츠를 암호화해 허가된 권한 범위에서만 열람·편집하게 하는 기술 * SSO: 한 번의 인증으로 여러 서비스를 이용하게 하는 통합 인증 * IDS: 트래픽과 로그를 분석해 침입 시도를 탐지·경보하는 시스템으로, 접속 자체를 막는 접근 통제 장비가 아니다

[22번] 봇넷(Botnet) 또는 C&C(Command & Control)에 많이 사용되는 프로토콜로 IRC(Internet Relay Chat) 프로토콜이 있다. 다음 중 IRC의 기능이 아닌 것은?

1다수의 사용자들과 텍스트 메시지를 공유
2사용자들 간의 파일 전송
3한 클라이언트의 사용자가 다른 클라이언트 상에서 실행 가능한 메시지 전송
4바이러스 프로그램의 제작

▸ IRC는 다수 사용자와의 텍스트 메시지 공유, 사용자 간 파일 전송, 그리고 원격 클라이언트에서 실행 가능한 명령 전송 기능을 제공하며 이 때문에 봇넷의 C&C 채널로 자주 악용된다. 다만 바이러스 프로그램을 직접 제작하는 기능은 IRC 프로토콜 자체가 제공하는 기능이 아니다.

[23번] 어느 회사의 메일 서버가 스팸 메일 발송 경유지로 악용하는 사례가 발생하였다. 이 때 보안관리자는 pcap 파일을 통해 패킷 분석을 진행하고자 보기와 같은 필터링을 실행하였다. 다음 필터링 결과에 대한 설명으로 옳은 것은?

1이메일 서비스 확장 지원 세션을 시작한 것을 필터링
2SMTP 세션을 시작한 것을 필터링
3서버에 인증을 시작한 것을 필터링
4메일 데이터 전송을 한 것을 필터링

▸ 이 필터는 확장 SMTP(ESMTP) 세션을 여는 인사 명령만 골라낸다. SMTP 세션의 첫 인사 명령은 HELO이고, AUTH 인증·8비트 전송·SIZE 제한 같은 확장 기능을 쓰려는 클라이언트는 EHLO로 세션을 시작한다. 따라서 SMTP.req.command=="EHLO"로 걸러내면 이메일 서비스 확장을 지원하는 세션의 시작 지점만 추려진다. 단순히 SMTP 세션 시작 전체를 보려면 HELO도 함께 잡아야 하는데 이 필터는 EHLO만 지정하고 있다. 서버 인증 시작은 AUTH, 실제 메일 본문 전송은 DATA 명령이라 이 조건에 걸리지 않는다.

[24번] 리버싱을 하기 위해서는 여러 가지 도구가 필요하다. 제시된 도구들과 그 역할이 올바르게 짝지어진 것은?

1㉠-ⓐ, ㉡-ⓑ, ㉢-ⓒ
2㉠-ⓐ, ㉡-ⓒ, ㉢-ⓑ
3㉠-ⓒ, ㉡-ⓑ, ㉢-ⓐ
4㉠-ⓒ, ㉡-ⓐ, ㉢-ⓑ

▸ OllyDbg는 PE 파일의 구조와 동작 확인, Procexp는 프로세스 동작 정보 확인, Filemonitor는 파일 이벤트 정보 확인에 쓰인다. OllyDbg는 윈도우용 디버거다. 실행파일(PE)을 올려 어셈블리 코드·메모리·레지스터를 단계별로 추적하므로 파일의 내부 구조와 실행 흐름을 파악하는 데 쓴다. Procexp(Process Explorer)는 실행 중인 프로세스의 부모·자식 관계, 로드된 DLL, 열려 있는 핸들을 보여 주는 도구라 프로세스 동작 관찰용이다. Filemonitor는 파일 생성·읽기·쓰기·삭제 같은 파일 접근 이벤트를 실시간으로 기록한다.

[25번] 스니핑(sniffing) 기법으로 틀린 것은?

1Switch Jamming
2SYN Flooding
3ARP Redirect
4ICMP Redirect

▸ Switch Jamming, ARP Redirect, ICMP Redirect는 모두 스위치 환경에서 트래픽을 자신에게 우회시켜 패킷을 가로채는 스니핑 기법에 해당한다. 반면 SYN Flooding은 TCP 연결 요청을 대량으로 보내 자원을 고갈시키는 서비스 거부(DoS) 공격이지, 트래픽을 도청하는 스니핑 기법이 아니다.

[26번] 2016년에 처음 발견되었으며, IP 카메라나 가정용 라우터와 같은 IoT 장치를 주요 공격 대상으로 삼는 DDoS 공격용 봇넷은?

1님다(Nimda)
2미라이(Mirai)
3스턱스넷(Stuxnet)
4SQL슬래머(Slammer)

▸ 2016년 처음 발견되어 IP 카메라·가정용 라우터 등 IoT 기기를 감염시켜 대규모 DDoS 공격에 동원한 봇넷은 미라이(Mirai)다. 님다는 2001년 웜, 스턱스넷은 산업제어시스템을 겨냥한 웜, SQL슬래머는 MS-SQL 취약점을 이용한 웜으로 각각 다른 시기·대상을 겨냥한 악성코드다.

[27번] ARP 스푸핑(Spoofing)은 LAN(Local Area Network) 상에서 MAC 주소를 조작하는 공격기법이다. 이에 대한 설명으로 옳은 것은?

1시스템의 ARP 테이블을 동적(Dynamic)으로 관리한다.
2ping [ip주소] 명령을 사용하여 시스템을 모니터링한다.
3arp –s [ip주소] [mac 주소] 명령을 통해 ARP 테이블을 관리한다.
4nslookup [mac 주소] 명령을 사용해 통신경로를 절대경로로 설정한다.

▸ arp -s [IP주소] [MAC주소] 명령은 특정 IP-MAC 매핑을 정적(static)으로 고정해 ARP 테이블을 관리하는 방법으로, ARP 스푸핑을 예방하는 대응책으로도 활용된다. * ARP 테이블이 동적으로 갱신된다는 사실 자체는 스푸핑 공격이 가능한 전제이지, 시스템이 이를 안전하게 관리한다는 의미가 아니다. * ping 명령은 단순 통신 확인용으로 ARP 테이블을 모니터링하는 수단이 아니다. * nslookup은 도메인 이름을 IP로 변환하는 명령으로 MAC 주소나 통신 경로 설정과는 무관하다.

[28번] Tcpdump 를 사용한 패킷 스니핑에 관한 설명이다. 괄호 안에 들어갈 적당한 말은?

1㉠ : 포트 스캐닝, ㉡ : 단일 모드
2㉠ : 포트 미러링, ㉡ : 무차별 모드
3㉠ : 포트 미러링, ㉡ : 단일 모드
4㉠ : 포트 스캐닝, ㉡ : 무차별 모드

▸ ㉠은 포트 미러링, ㉡은 무차별 모드(Promiscuous Mode)다. 스위치 환경에서는 자기 포트로 향하는 프레임만 보이므로, 같은 세그먼트의 트래픽을 수집하려면 스위치에서 해당 트래픽을 분석 포트로 복제해 주는 포트 미러링(SPAN)을 설정해야 한다. NIC는 기본적으로 목적지 MAC 주소가 자신과 다르면 프레임을 버린다. 인터페이스를 무차별 모드로 전환하면 주소가 달라도 폐기하지 않고 모두 올려 보내므로 tcpdump가 그 패킷을 볼 수 있다. 포트 스캐닝은 대상 호스트의 열린 포트를 찾는 정찰 기법이고, 단일 모드는 이런 수신 정책을 가리키는 용어가 아니다.

[29번] 네트워크 침입탐지와 방지를 위해 ModSecurity를 설치 운용하고자 한다. ModSecurity 정책 설정을 위해 SecAuditEngine에서 설정할 수 없는 것은?

1DetectionOnly
2On
3Off
4RelevantOnly

▸ SecAuditEngine 지시자에 설정할 수 있는 값은 On, Off, RelevantOnly이며, 감사 로그 기록 여부와 범위를 제어한다. DetectionOnly는 규칙 위반을 </partial_content> <instructions> Document is too large (73571 tokens). Only showing first 10000 tokens. For complete analysis, run `gsk summarize " https://www.moducbt.com/exam/pdf/28430" --question "<your specific question>"` — it analyzes the full document (PDFs, academic papers, reports,