2022년 정보보안기사 필기 기출문제

전 회차 · 51문항 · 정답·해설 포함

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

2022년 정보보안기사 필기

제1회 · 27문항

[1번] 다음 중 취약점 점검 도구에 대한 설명으로 틀린 것은?

1COPS/COPE : 네트워크 기반의 취약점 분석도구로 컴퓨터, 서버, N/W IDS의 보안 취약점을 분석한다.
2Nessus : 네트워크 취약점 점검도구로써 클라이언트-서버 구조로 클라이언트의 취약점을 점검하는 기능이 있다.
3nmap : 시스템 내부에 존재하는 취약성을 점검하는 도구로써 취약한 패스워드 점검 기능 등이 있다.
4SAINT : 네트워크 취약점 분석도구로써 HTML 형식의 보고서 기능이 있으며 원격으로 취약점을 점검하는 기능을 가지고 있다.

▸ 이 문항은 확정답안에서 복수정답으로 처리된 문항입니다. 「COPS/COPE : 네트워크 기반의 취약점 분석도구로 컴퓨터, 서버, N/W IDS의 보안 취약점을 분석한다.」와 「nmap : 시스템 내부에 존재하는 취약성을 점검하는 도구로써 취약한 패스워드 점검 기능 등이 있다.」가 모두 정답으로 인정되었습니다. 여기서는 채점을 위해 한 선택지만 정답으로 두었으니, 다른 것을 고르셨더라도 틀린 판단이 아닙니다. COPS(Computer Oracle and Password System)는 한 대의 호스트에 설치되어 파일 권한이나 설정값 등을 점검하는 호스트 기반 취약점 점검 도구다. 컴퓨터·서버·네트워크 IDS까지 아우르는 네트워크 기반 분석 도구로 설명한 부분이 실제 동작 범위와 어긋난다. 나머지 보기는

[2번] 다음은 passwd 파일 구조를 나타내는 그림이다. “A”는 무엇인가?

1패스워드
2UID 값
3계정명
4설명

▸ 그림에서 A가 가리키는 자리는 Test, 곧 /etc/passwd 한 줄의 첫 번째 필드인 계정명(로그인 ID)이다. passwd 항목은 콜론으로 나뉘어 계정명:패스워드:UID:GID:설명:홈 디렉터리:로그인 셸 순서를 갖는다. 그림의 Test : x : 500 : 500 : Gen-User : /home/test : /usr/bin/bash 에 대입하면 B의 x는 암호화된 패스워드가 /etc/shadow 로 분리되어 있음을 뜻하는 표시, C는 UID 500, D는 GID 500, E는 설명(Gen-User), F는 홈 디렉터리, G는 로그인 셸이다. 따라서 A 자리에 오는 것은 계정명이며, 패스워드·UID 값·설명은 각각 두 번째·세 번째·다섯 번째 필드여서 위치가 다르다.

[3번] 버퍼오버플로우 공격을 완화할 수 있는 방법으로 스택과 힙 영역에 쉘코드 등을 실행하지 못하도록 하는 메모리 보호기법에 해당하는 것은?

1ASLR
2DEP/NX bit
3Format String
4Stack Canary

▸ DEP/NX bit는 스택·힙과 같은 데이터 영역을 실행 불가능(Non-eXecutable)으로 표시해 그 안에 주입된 쉘코드가 실행되지 못하도록 막는 메모리 보호 기법이다. ASLR은 주소 공간을 무작위화해 특정 주소를 예측하지 못하게 하는 기법이고, Stack Canary는 함수가 반환하기 직전에 카나리 값이 변조되었는지 검사해 스택 훼손을 탐지하는 기법이라 데이터 영역의 실행 자체를 막는 방식과는 다르다. Format String은 방어 기법이 아니라 취약점을 이용한 공격 기법 자체다.

[4번] 도구의 기능과 도구명이 짝지어진 것 중 틀린 것은?

1운영체제별 로그 변조 탐지도구 - Chklastlog
2운영체제별 감사로그 관리도구 - Natas
3취약점 진단도구 - SATAN
4접근통제관련 로깅 도구 – Syslogd

▸ 변조 탐지용 Chklastlog, 진단 도구 SATAN, 로깅 데몬 Syslogd는 각각 제시된 기능과 정확히 짝지어져 있다. 반면 운영체제별 감사로그 관리도구로 짝지어진 Natas는 그런 용도의 관리 도구로 알려진 이름이 아니어서, 기능과 도구명의 짝짓기가 어긋난다.

[5번] 다음 윈도우(Windows)의 Administrators 그룹에 대한 설명으로 틀린 것은?

1대표적인 관리자 그룹으로 윈도우 시스템의 모든 권한을 가지고 있다.
2사용자 계정을 만들거나 없앨 수 있다.
3윈도우가 사용 가능한 모든 자원에 대한 권한을 설정할 수 있다.
4해당 컴퓨터 밖의 네트워크에서도 일반 사용자보다 특별한 권한을 행사할 수 있다.

▸ 로컬 Administrators 그룹의 권한은 해당 컴퓨터 안에서만 유효하며, 네트워크상의 다른 컴퓨터에 대해서는 일반 사용자와 동일하게 취급된다. 계정 생성·삭제, 시스템 자원에 대한 권한 설정 등 로컬 시스템 전반에 대한 통제권을 가진다는 설명은 맞지만, 그 권한이 컴퓨터 밖 네트워크까지 자동으로 확장되지는 않는다.

[6번] 사용자 PC가 언제 부팅되었는지를 확인하기 위해 입력해야 하는 명령어는?

1net statistics workstation
2net computer boot time
3net reboot time
4net time boot

▸ net statistics workstation 명령은 워크스테이션 서비스가 시작된 시점부터의 통계를 보여주며, 이를 통해 시스템이 언제 부팅되었는지 확인할 수 있다. 나머지 보기는 실제로 존재하는 net 명령 옵션이 아니다.

[7번] 리눅스 proc 파일 시스템에서 ASLR(Address Space Layout Randomization) 설정값을 확인할 수 있는 파일은 무엇인가?

1/proc/sys/kernel/randomize_va_space
2/proc/sys/kernel/watchdog
3/proc/sys/kernel/panic
4/proc/sys/kernel/random

▸ 리눅스에서 ASLR 활성화 수준은 /proc/sys/kernel/randomize_va_space 파일 값으로 확인·설정한다. 값이 0이면 비활성화, 1이면 스택·라이브러리 등 일부 영역만, 2이면 힙까지 포함한 전면적인 무작위화가 적용된다.

[8번] 다음 중 무결성(Integrity) 검사를 위한 도구가 아닌 것은?

1tripwire
2Fcheck
3Samhain
4prstat

▸ tripwire, Fcheck, Samhain은 파일의 해시값을 기준 스냅샷과 비교해 변조 여부를 검사하는 대표적인 무결성 점검 도구다. 반면 prstat는 Solaris 계열에서 프로세스의 CPU·메모리 사용 현황을 실시간으로 보여주는 모니터링 명령으로, 파일 무결성 검사와는 목적이 다르다.

[9번] 다음 문장에서 설명하고 있는 내용의 괄호 안에 들어갈 올바른 항목은?

▸ 파일과 디렉터리는 물론 메타 정보까지 전부 파일 형태로 관리하는 파일 시스템은 NTFS다. NTFS는 볼륨의 모든 객체를 MFT(Master File Table)의 레코드로 관리하고, $MFT·$LogFile·$Bitmap 같은 메타데이터조차 파일로 존재한다. 그래서 포렌식에서는 MFT만 확보해도 파일명·타임스탬프·크기·삭제 흔적을 되짚어 정보를 알아낼 수 있다. * FAT은 클러스터 연결 정보를 담은 할당표와 디렉터리 엔트리 수준만 제공해 메타데이터가 빈약하다. * MBR은 디스크 첫 섹터의 부트코드와 파티션 테이블로, 파일 시스템 자체가 아니다. * BIOS는 부팅을 담당하는 펌웨어여서 파일 관리와 무관하다.

[10번] 다음 중 프로세스 스케줄링과 관계가 가장 먼 것은?

1페이징(Paging)
2스와핑(Swapping)
3레이스컨디션(Race condition)
4환형대기(Circular wait)

▸ 페이징(Paging)은 가상 메모리를 고정 크기 페이지 단위로 관리하는 메모리 관리 기법으로, 어떤 프로세스를 언제 CPU에 배정할지를 다루는 프로세스 스케줄링과는 성격이 다르다. 스와핑은 스케줄링 정책에 따라 프로세스를 메모리에 올리고 내리는 동작이고, 레이스컨디션과 환형대기는 여러 프로세스가 자원과 실행 순서를 다투는 과정에서 발생하는 스케줄링 관련 현상이라는 점에서 페이징과 구분된다.

[11번] 다음 문장이 설명한 공격 위협은 무엇인가?

1운영체제 명령 실행
2XPath 인젝션
3디렉터리 인덱싱
4정보 누출

▸ 파이프·앰퍼샌드·세미콜론·백틱처럼 셸이 명령 구분과 명령 치환에 쓰는 메타문자를 걸러내라는 요구는 운영체제 명령 실행(OS Command Injection) 대응책이다. 웹 애플리케이션이 사용자 입력을 시스템 명령의 인자로 넘길 때 | & ; ` 를 그대로 통과시키면 공격자가 뒤에 임의 명령을 이어 붙여 웹서버 권한으로 실행할 수 있다. 지문이 권한 변경과 시스템 운영 악영향을 함께 말하는 이유가 여기에 있다. * XPath 인젝션은 XML 질의문을 조작하는 공격이라 작은따옴표·대괄호 같은 질의 구문 문자가 문제가 된다. * 디렉터리 인덱싱은 파일 목록이 노출되는 서버 설정 문제로 입력값 필터링과 무관하다. * 정보 누출은 에러 메시지나 주석에 내부 정보가 드러나는 취약점이다.

[12번] 웹 쿠키(Cookies)에 대한 설명 중 올바른 것은?

1쿠키는 서버가 아닌 클라이언트에 저장된다.
2쿠키는 웹 서버에 저장되므로 클라이언트에서 제어할 수 없다.
3쿠키는 실행가능한 파일로 바이러스로 동작할 수 있다.
4쿠키는 강력한 인증 기능을 제공한다.

▸ 쿠키는 웹 서버가 아니라 클라이언트(브라우저) 측에 저장되는 작은 텍스트 데이터다. * 서버에 저장되어 클라이언트가 제어할 수 없다는 설명은 저장 위치 자체가 반대다. * 쿠키는 단순 텍스트 데이터로 스스로 실행되는 파일이 아니므로 바이러스처럼 동작할 수 없다. * 쿠키만으로는 신원을 강하게 증명할 수 없어 강력한 인증 수단으로 보기 어렵다.

[13번] Syslog와 같은 시스템 로그를 주기적으로 스캔하여 어떠한 행위가 발생했는지를 분석하는 시스템 로깅 도구는?

1Nikto
2X-scan
3N-stealth
4Swatch(Simple WATCHer)

▸ Swatch(Simple WATCHer)는 syslog 등 시스템 로그를 주기적으로 스캔해 미리 정의한 패턴이 나타나면 관리자에게 알리는 로그 모니터링 도구다. Nikto, X-scan, N-stealth는 웹 서버나 네트워크의 취약점을 원격에서 스캔하는 도구로, 로그를 분석하는 도구와는 목적이 다르다.

[14번] 다음 문장에서 설명한 공격 위협은 무엇인가?

1SSI 인젝션
2XPath 인젝션
3크로스사이트 스크립팅
4악성 콘텐츠

▸ 입력값 필터링이 부실한 게시판·URL에 악성 스크립트를 심어 글을 읽는 다른 사용자의 쿠키(세션)를 탈취하고 악성코드 유포지로 리다이렉트시키는 것은 크로스사이트 스크립팅(XSS)이다. 핵심은 공격 코드가 서버가 아니라 피해자의 브라우저에서 실행된다는 점이다. 지문에 나열된 JavaScript·VBScript·ActiveX·Flash가 모두 클라이언트 측에서 동작하는 실행 요소라는 사실이 이를 뒷받침한다. * SSI 인젝션은 서버가 해석하는 지시어를 삽입해 서버 쪽에서 명령·파일 읽기가 일어나게 한다. * XPath 인젝션은 XML 데이터 질의문을 조작해 인증 우회나 정보 탈취를 노린다. * 악성 콘텐츠는 악성 파일을 올려 유포하는 유형으로, 열람자 세션 탈취를 목적으로 한 스크립트 삽입과 구분된다.

[15번] 다음 중 트로이목마 프로그램인 루트킷에 대한 설명으로 가장 부적절한 것은?

1루트킷의 목적은 자신과 다른 소프트웨어를 보이지 않게 숨기고 사용자가 공격자의 소프트웨어를 인지하고 제거할 가능성을 피한다.

2윈도우용 루트킷에는 FU-Rootkit, Hxdef100, NTRRootkit 등이 있다.
3리눅스용 루트킷에는 Suckit, lrk4, lrk5, adore 등이 있다.
4자기 복제를 하여 다른 컴퓨터에 루트킷을 설치함으로써 그 피해가 커질 수 있다.

▸ 루트킷은 이미 침입에 성공한 시스템에서 자신과 다른 악성 흔적을 숨기는 데 목적이 있는 도구로, 바이러스나 웜처럼 스스로를 복제해 다른 컴퓨터로 전파하는 기능은 루트킷의 본질적 특징이 아니다. 윈도우용 FU-Rootkit·Hxdef100·NTRootkit, 리눅스용 Suckit·lrk 계열·adore 등이 실제 존재하는 루트킷이라는 설명과, 은폐가 목적이라는 설명은 타당하다.

[16번] 관리자 A는 개별그룹으로 신규 사용자 등록(kim, jang) 작업을 어느날 수행한 후 1주일 후에 아래와 같은 시스템 내용을 보고 판단하였다. 올바른 판단은?

1패스워드 파일(/etc/passwd)은 누구든지 직접 수정 가능하다.
2사용자 jang은 /etc/passwd 파일의 권한을 설정할 수 있다.
3사용자 kim은 사용자 계정에 jang 디렉토리에 들어가서 읽을 수도 없고 실행을 못 시킬 것이다.
4jang은 kim의 패스워드를 바꿀 수 있다.

▸ /home/jang 의 권한이 drwxr-x--- 이므로, 개별 그룹으로 만들어진 kim 은 jang 디렉터리를 읽을 수도 진입·실행할 수도 없다. 디렉터리에서 r은 목록 조회 권한, x는 진입(cd)과 내부 접근 권한이다. drwxr-x--- 의 마지막 세 자리가 --- 이라 소유자 jang 과 jang 그룹을 뺀 나머지 사용자에게는 두 권한이 모두 없다. 사용자마다 개별 그룹이 만들어졌으므로 kim 은 jang 그룹에 속하지 않는다. * /etc/passwd 는 -rw-r--r-- root root 여서 소유자 root 만 쓰기가 가능하고 일반 사용자는 읽기만 된다. * 파일 권한 변경은 소유자나 root 만 할 수 있으므로 jang 이 root 소유 파일의 권한을 설정할 수 없다. * 다른

[17번] 소유권 없는 파일을 찾는 명령어 및 옵션이 아닌 것은?

1find / -ls 2 > /dev/null
2find / −nouser–o–nogroup-nouser –o –nogroup -xdev –exec ls –al{}
3find / -nouser -print
4find / -nogroup –print

▸ find / -ls는 -nouser나 -nogroup 같은 조건 없이 시스템의 모든 파일 목록을 출력하는 명령으로, 소유자·소유그룹이 없는 파일만 골라내는 기능은 없다. 나머지 보기들은 모두 -nouser 또는 -nogroup 옵션을 사용해 소유권이 없는 파일을 찾는다는 공통점이 있다.

[18번] 다음 문장의 괄호 안에 해당하는 것은 무엇인가?

1버퍼오버플로우
2루팅
3인젝션
4접근 제어

▸ 루트 액세스 권한을 얻어 안드로이드 장치를 완전히 제어하고 제조·판매 단계에서 걸어 둔 제약을 푸는 행위는 루팅(rooting)이다. 안드로이드는 리눅스 커널 기반이어서 계정이 일반 사용자와 루트로 나뉘고, 운영체제 변경·특정 명령 실행·도구 설치에는 루트 권한이 필요하다. 루팅하면 이 제한이 풀리는 대신 애플리케이션 샌드박스와 정식 업데이트 체계가 함께 무력화되어 악성코드에 크게 취약해진다. * 버퍼오버플로우는 경계 검사 없는 메모리 복사로 생기는 취약점으로, 루팅의 수단이 될 수는 있어도 권한 획득 상태 자체를 가리키는 용어가 아니다. * 인젝션은 입력값에 악의적 구문을 끼워 넣어 질의나 명령을 조작하는 공격이다. * 접근 제어는 주체의 권한에 따라 자원 사용을 통제하는 보안 기능이다.

[19번] 다음 중 은폐형 바이러스에 대한 설명으로 가장 적합한 것은?

1파일이 감염될 경우 그 파일의 내용을 확인할 수 없다.
2감염된 파일의 길이가 증가하지 않은 것처럼 보이게 하고, 감염전의 내용을 보여주어 바이러스가 없는 것처럼 백신과 사용자를 속인다.
3바이러스 분석가에게 분석을 어렵게 하고 백신 개발을 지연시키도록 여러 단계의 기법을 사용한다.
4백신으로 진단이 어렵도록 바이러스 프로그램의 일부 또는 전체를 암호화한다.

▸ 은폐형(Stealth) 바이러스는 감염된 파일의 크기가 늘어나지 않은 것처럼 보이게 하거나 감염 전 원본 내용을 그대로 보여주는 방식으로 백신과 사용자의 탐지를 피한다. 파일 내용을 아예 확인할 수 없게 만드는 것은 파괴형에 가깝고, 분

석을 어렵게 하려고 여러 단계 기법을 쓰는 것은 갑옷형(armored), 프로그램 전체나 일부를 암호화하는 것은 암호화형 바이러스의 특징이라 은폐형과는 구분된다.

[20번] 다음 문장에서 리눅스 시스템에 침해 흔적을 조사하기 위해 루트 권한을 가진 setuid를 찾는 명령어로 괄호안에 들어갈 적합한 것은?

1-perm –06000 \
2-perm –00100 \
3-perm –00400 \
4-perm –00200 \

▸ 루트 소유 파일 가운데 setuid·setgid 비트가 설정된 것을 찾아야 하므로 괄호에는 -perm -06000 조건이 들어간다. 유닉스 권한의 맨 앞자리 특수 비트는 setuid=4000, setgid=2000, sticky=1000 이다. 두 비트를 합한 6000 앞에 빼기 기호를 붙이면 '그 비트를 포함하는 모든 파일'이 검색된다. 완성된 명령은 find / -user root -type f \(-perm -06000 \) -exec ls -al {} \; 이며, 백슬래시로 감싼 괄호가 검색 조건식을 하나로 묶고 뒤에 오는 -exec 가 찾은 파일마다 상세 목록을 출력한다. * 00100은 소유자 실행 비트여서 일반 실행 파일이면 모두 걸려 침해 흔적 조사에 쓸 수 없다. * 00400(

[21번] 다음 중 VPN에 대한 설명으로 가장 옳지 않은 것은?

1SSL VPN은 웹브라우저만 있으면 언제 어디서나 사용이 가능하다.
2IPsec VPN은 네트워크 계층에서 안전하게 정보를 전송하는 방법이다.
3IPsec VPN은 운영방식에 따라 트랜스포트 모드만 지원하고 암호화 여부에 따라 ESP, AH 프로토콜을 사용한다.
4기본적으로 SSL VPN과 IPsec VPN은 데이터의 기밀성과 무결성은 동일하며, 단지 데이터의 암호화 구현 방식에 차이가 있다.

▸ IPsec VPN은 운영 방식에 따라 트랜스포트 모드와 터널 모드를 모두 지원하며, 트랜스포트 모드만 지원한다는 설명은 사실과 다르다. 암호화 여부에 따라 인증만 제공하는 AH와 기밀성까지 제공하는 ESP를 선택적으로 사용한다는 점은 맞는 설명이다. SSL VPN이 별도 클라이언트 없이 웹브라우저만으로 접속 가능하다는 점, IPsec VPN이 네트워크 계층에서 동작한다는 점은 모두 타당한 설명이다.

[22번] 다음 스크린드 서브넷 구조에 대한 설명으로 가장 옳지 않은 것은?

1외부 인터넷 환경에서 접속이 되어야 한다.
2스크리닝 라우터 사이에 듀얼 홈드 게이트웨이가 위치하는 구조이다.
3다른 방화벽에 비해 설치 및 관리가 쉽다.
4서비스 속도가 낮다.

▸ 스크린드 서브넷 구조는 두 대의 스크리닝 라우터 사이에 배스천 호스트(듀얼 홈드 게이트웨이 성격의 서브넷)를 두는 다계층 방화벽 구조로, 보안성은 높지만 구성 요소가 많아 설치와 관리가 오히려 복잡하고 까다롭다. 여러 단계를 거치는 구조 특성상 서비스 속도가 낮아질 수 있다는 설명은 타당하다.

[23번] 다음 중 Window 계열의 시스템에 대한 포트 스캐닝을 할 수 없는 것은?

1TCP SYN Scan
2TCP FIN Scan
3TCP Connect Scan
4UDP Scan

▸ TCP FIN Scan은 열린 포트든 닫힌 포트든 윈도우 계열 TCP/IP 스택이 RFC 표준과 달리 RST로 응답하는 경향이 있어 응답만으로 포트 상태를 구분하기 어렵고, 그 결과 윈도우 시스템에는 사실상 적용되지 않는다. TCP SYN Scan, TCP Connect Scan, UDP Scan은 연결 수립 과정이나 UDP 응답 유무를 직접 확인하는 방식이라 운영체제 종류와 무관하게 포트 상태를 판별할 수 있다.

[24번] 바이러스 및 공격으로부터 IoT(Internet of Thing) 기기를 보호할 수 있는 접근제어, 기기 인증, 통신 암호화, 가용성 등과 같은 보안 요구 사항을 알기 쉽게 나타내도록 IoT용 SoA(Service oriented Architecture)는 4계층으로 구성된다. 다음 중 IoT용 SoA 4 계층에 포함되지 않는 것은 어떤 계층인가?

1센싱 계층
2네트워크 계층
3트랜스포트 계층

4서비스 계층

▸ 사물인터넷용 SoA 4계층은 일반적으로 센싱 계층, 네트워크 계층, 서비스 계층, 응용(인터페이스) 계층으로 구성된다. 트랜스포트 계층은 OSI·TCP/IP 참조 모델에서 종단 간 전송을 담당하는 계층 이름으로, 이 IoT 4계층 구조에서 별도로 정의하는 계층 명칭은 아니다.

[25번] 다음 문장의 괄호 안에 들어갈 알맞은 용어는?

1PLC
2SCADA
3Stuxnet
4Modbus

▸ 산업제어시스템의 공정과 설비를 중앙에서 감시하고 제어하는 컴퓨터 시스템은 SCADA(Supervisory Control And Data Acquisition)다. SCADA는 현장의 센서·제어기에서 데이터를 수집해 감시 화면에 보여 주고 제어 명령을 내려보내는 상위 계층으로, 전력·상하수도·가스처럼 사회기반시설 운영의 중추를 이루기 때문에 사이버 공격의 표적이 된다. * PLC는 현장 기기를 직접 구동하는 제어 장치로, 감시·제어 체계 전체가 아니라 그 하부 구성 요소다. * Stuxnet은 원심분리기 제어 설비를 노린 악성코드이므로 시스템이 아니라 공격 수단이다. * Modbus는 산업 제어 기기 사이에서 데이터를 주고받는 통신 프로토콜이다.

[26번] 네트워크에서 큰 크기의 파일을 전송할 때, 정상적인 경우에 전송가능한 최대 사이즈로 조각화 되어 전송되며, 이때 Fragment Number를 붙여 수신측에서 재조합을 하게 된다. Fragmentation Offset을 위조하여 중복하게 하거나 공간을 두어 재조합을 방해하는 공격은 OSI 7계층 중 어느 계층에서 발생하는 것인가?

1OSI 2 계층
2OSI 3 계층
3OSI 4 계층
4OSI 5 계층

▸ 정답은 OSI 3계층(네트워크 계층)이다. Fragmentation Offset을 조작해 조각을 중복시키거나 빈틈을 만드는 공격은 IP 계층에서의 단편화·재조합 과정을 악용하는 것이며, IP가 이 계층에서 동작하기 때문이다.

[27번] 다음 문장은 모바일 악성코드에 관한 설명이다. 어떤 악성코드에 관한 설명인가?

1Card trap. A
2CommWarrior
3Hobbles. A
4Brader

▸ 휴대전화 통신망을 타고 번지면서 단말에 저장된 전화번호로 스스로 자신을 퍼뜨린 모바일 악 </partial_content> <instructions> Document is too large (84918 tokens). Only showing first 10000 tokens. For complete analysis, run `gsk summarize "https://www.moducbt.com/exam/pdf/28432" --question "<your specific question>"` — it analyzes the full document (PDFs, academic papers, reports, web content) and returns a targeted answer. </instruct

제2회 · 24문항

[1번] 서버 시스템의 접근통제 관리에 대한 설명으로 틀린 것은?

1윈도우 시스템 이벤트에는 시스템, 어플리케이션, 보안 이벤트가 있으며 감사로그는 제어판-관리도구-로컬보안설정-감사정책에서 각각 설정할 수 있다.
2윈도우 시스템은 도메인 환경에서 사용자 인증을 위하여 레지스트리가 익명의 사용자에 의해 접근할 수 있도록 설정하여야 한다.
3iptables, tcp wrapper 도구를 사용하면 서버 시스템의 네트워크 접근통제 기능을 설정할 수 있다.
4Unix 서버 시스템에서 불필요한 파일에 설정된 SUID와 SGID 비트를 제거하여 실행 권한이 없는 프로그램의 비인가된 실행을 차단하여야 한다.

▸ 레지스트리를 익명 사용자가 접근할 수 있도록 설정하는 것은 접근통제 관점에서 틀린 설명이다. 도메인 환경이라도 사용자 인증을 위해 레지스트리를 익명으로 열어 둘 필요는 없으며, 오히려 익명 접근을 허용하면 시스템 설정과 계정 정보가 노출되는 취약점이 된다. * 윈도우 이벤트 로그(시스템·어플리케이션·보안)는 로컬 보안 설정의 감사 정책에서

설정할 수 있다. * iptables·tcp wrapper는 서버의 네트워크 접근통제 도구로 쓰인다. * 불필요한 파일의 SUID·SGID 비트를 제거해 비인가 실행을 막아야 한다.

[2번] 다음은 passwd 파일 구조를 나타내는 그림이다. “G”가 의미하는 것은?

1홈디렉터리 위치
2지정된 셸(Shell)
3패스워드
4설명

▸ 맨 뒤 필드 /usr/bin/bash를 가리키는 G는 그 계정이 로그인할 때 실행되는 지정된 셸(Shell)이다. 그림의 한 줄은 Test : x : 500 : 500 : Gen-User : /home/test : /usr/bin/bash 로, /etc/passwd 는 콜론으로 구분된 7개 필드다. 차례로 사용자명(Test) → 패스워드 자리(x) → UID(500) → GID(500) → 설명(Gen-User) → 홈 디렉터리(/home/test) → 셸(/usr/bin/bash) 이며 화살표 A·B·C·D·E·F·G가 이 순서대로 각 필드를 가리킨다. * 홈디렉터리 위치는 여섯 번째 필드 /home/test 로, 그림에서는 F가 가리킨다. * 패스워드는 두 번째 필드 x 로, 실제 해시는 /etc

[3번] 안드로이드 adb를 통해 접속 후 쓰기 가능한 디렉터리는?

1/system/
2/data/app
3/data/local/tmp/
4/bin/

▸ /data/local/tmp/는 안드로이드 adb 접속 시 일반(shell) 권한으로도 쓰기가 가능한 대표적인 디렉터리다. 루팅되지 않은 기기에서 /system은 읽기 전용으로 마운트된 시스템 영역이고, 앱 설치 영역인 /data/app 과 /bin 같은 시스템 실행 경로도 shell 사용자에게 쓰기 권한이 없다. 반면 /data/local/tmp/는 임시 파일 전송·테스트 용도로 shell 계정에 쓰기가 허용되어 adb push 등으로 파일을 올릴 수 있다.

[4번] 다음 문장에서 설명하는 공격 위협은?

1XPath 인젝션
2디렉터리 인덱싱
3운영체제 명령 실행
4정보 누출

▸ 중요정보나 과도한 에러 메시지가 그대로 드러나 공격자에게 단서를 주는 취약점은 정보 누출이다. 개인정보·계정정보·금융정보가 화면이나 응답에 노출되고, 예외 발생 시 DB 오류 메시지·웹 서버 구성 정보·개발 단계의 주석까지 보이면 공격자는 이를 모아 2차 공격의 정찰 자료로 쓴다. 대응은 사용자에게 표준화된 오류 페이지만 보여주고 상세 내용은 서버 로그에만 남기는 것이다. * XPath 인젝션 — XML 문서를 조회하는 XPath 질의에 악의적 구문을 끼워 넣어 인증을 우회하거나 데이터를 빼내는 주입 공격이다. * 디렉터리 인덱싱 — 기본 문서가 없을 때 웹 서버가 디렉터리 내 파일 목록을 그대로 보여주는 설정상의 취약점이다. * 운영체제 명령 실행 — 웹 애플리케이션 입력값이 시스템 명령으로 전달

[5번] 인증 장치에 대한 설명으로 옳은 것은?

1USB 메모리에 디지털 증명서를 넣어 인증 디바이스로 하는 경우 그 USB 메모리를 접속하는 PC의 MAC 어드레스가 필요하다.
2성인의 홍채는 변화가 없고 홍채 인증에서는 인증 장치에서의 패턴 갱신이 불필요하다.
3정전용량 방식의 지문인증 디바이스 LED 조명을 설치한 실내에서는 정상적으로 인증할 수 없게 될 가능성이 높다.
4인증에 이용되는 접촉형 IC 카드는 카드 내의 코일의 유도 기전력을 이용하고 있다.

▸ 성인의 홍채 패턴은 시간이 지나도 변하지 않으므로, 홍채 인증은 한번 등록하면 이후 패턴을 다시 갱신할 필요가 없다. * USB 메모리에 담긴 디지털 증명서로 인증하는 방식은 증명서 자체의 검증으로 이뤄지며 접속 PC의 MAC 주소를 요구하지 않는다. * 정전용량 방식 지문 센서는 피부의 전기적 특성을 감지하므로 조명 때문에 인증이 어려워지는 일은 드물다(빛에 민감한 쪽은 광학 방식이다). * 접촉형 IC카드는 단자를 통한 직접 전기 접촉으로 동작하며, 코일의 유도 기전력을 쓰는 것은 비접촉형 IC카드다.

[6번] 컴퓨터 시스템에 대한 하드닝(Hardening) 활동으로 틀린 것은?

1사용하지 않는 PDF 소프트웨어를 제거하였다.

2시스템 침해에 대비하여 전체 시스템에 대한 백업을 받아두었다.
3운영체제의 감사 기능과 로깅 기능을 활성화하였다.
4운영체제 보안 업데이트를 수행하였다.

▸ 전체 시스템 백업은 장애·침해 이후의 복구를 위한 대비책이지, 시스템의 공격 표면을 줄이는 하드닝 활동은 아니다. 하드닝은 불필요한 서비스·소프트웨어 제거, 보안 패치 적용, 감사·로깅 활성화처럼 침해 가능성 자체를 낮추는 사전 조치를 말한다. * 사용하지 않는 PDF 소프트웨어 제거는 공격 표면을 줄이는 하드닝이다. * 감사·로깅 기능 활성화는 하드닝에 해당한다. * 보안 업데이트 적용은 하드닝에 해당한다.

[7번] 다음 문장에서 설명하는 기억 장치의 메모리 반입 정책은?

1최초 적합(First fit)
2최상 적합(Best fit)
3최악 적합(Worst fit)
4다음 적합(Next fit)

▸ 수용 가능한 공간 가운데 가장 큰 공간을 골라 배치하는 방식은 최악 적합(Worst fit)이다. 최악 적합은 큰 빈 공간을 먼저 쪼개므로 할당 후 남는 조각도 커서 다음 요청에 재활용될 여지가 있지만, 큰 공간을 빠르게 소모한다는 단점이 있다. * 최초 적합 — 앞에서부터 훑어 처음 만나는 충분한 공간에 배치하므로 탐색이 가장 빠르다. * 최상 적합 — 수용 가능한 공간 중 가장 작은 공간을 선택해 낭비를 줄이지만, 쓰기 어려운 작은 조각이 많이 남는다. * 다음 적합 — 직전에 할당했던 위치부터 이어서 탐색하는 최초 적합의 변형이다.

[8번] 악성프로그램에 대한 설명으로 틀린 것은?

1바이러스 : 한 시스템에서 다른 시스템으로 전파하기 위해서 사람이나 도구의 도움이 필요한 악성프로그램이다.
2웜 : 한 시스템에서 다른 시스템으로 전파하는데 있어서 외부의 도움이 필요하지 않은 악성프로그램이다.
3백도어 : 사용자의 동의없이 설치되어 컴퓨터 정보 및 사용자 개인정보를 수집하고 전송하는 악성프로그램이다.
4논리 폭탄 : 합법적 프로그램 안에 내장된 코드로서 특정한 조건이 만족되었을 때 작동하는 악성 코드이다.

▸ 백도어는 인증 절차를 우회해 공격자가 시스템에 원격으로 재접근할 수 있도록 열어두는 통로이며, 사용자 정보를 몰래 수집·전송하는 것은 백도어가 아니라 스파이웨어의 특징이다. * 바이러스는 전파를 위해 사람이나 매개체의 도움이 필요하다. * 웜은 외부 도움 없이 스스로 전파된다. * 논리 폭탄은 정상 프로그램에 내장돼 특정 조건에서 작동한다.

[9번] 다음은 SUID 프로그램이 일반 권한에서 관리자 권한으로 상승하여 처리하는 정상적인 과정을 나타내고 있다. 심볼릭 링크를 이용한 레이스 컨디션 공격이 실행되는 단계는?

11단계
22단계
33단계
44단계

▸ 임시 파일이 만들어진 뒤 프로그램이 그 파일을 실제로 열어 처리하기 직전인 3단계에서 공격이 성립한다. 그림의 흐름은 일반 권한에서 '프로그램 실행 → SetUID로 인한 프로세스 권한 상승'을 거쳐, 관리자 권한 영역에서 '임시 파일 생성 → 프로그램 동작 및 임시 파일 처리 → 프로그램 종료'로 이어지며, 각 구간 경계가 ①~④단계로 표시되어 있다. ③단계 경계선이 바로 임시 파일 생성과 임시 파일 처리 사이에 놓여 있다. 공격자는 임시 파일이 생성된 시점과 그 파일을 사용하는 시점 사이의 빈틈을 노려, 생성된 임시 파일을 지우고 같은 이름으로 /etc/passwd 같은 중요 파일을 가리키는 심볼릭 링크를 걸어 둔다. 그러면 관리자 권한으로 동작 중인 프로그램이 링크를 따라가 엉뚱한 파일을 덮어쓰게

[10번] 다음은 IDS Snort Rule이다. Rule이 10~11번째 2바이트의 값이 0xFFFF인지를 검사하는 Rule이라 할 때 ㉠~㉢의 올바른 키워드는 무엇인가?

1㉠ : value, ㉡ : offset, ㉢ : content
2㉠ : value, ㉡ : content, ㉢ : offset
3㉠ : content, ㉡ : depth, ㉢ : offset
4㉠ : content, ㉡ : offset, ㉢ : depth

▸ 탐지할 값을 적는 content, 검사 시작 위치를 정하는 offset, 검사 범위를 제한하는 depth 순서가 맞다 — ㉠ content, ㉡ offset, ㉢ depth 이다. content는 페이로드에서 찾을 패턴을 적는 키워드이고, 파이프로 감싼 |FF FF| 는 16진수 바이트 0xFF 0xFF를 뜻한다. offset은 페이로드 맨 앞에서 몇 바이트를 건너뛴 뒤부터 찾을지를 정한다. offset:9 는 앞의 9

바이트를 건너뛰고 10번째 바이트부터 검사한다는 뜻이다. depth는 offset 지점부터 검사할 길이로, depth:2 는 2바이트만 본다는 뜻이다. 둘을 합치면 10~11번째 2바이트가 0xFFFF인지 검사하는 규칙이 된다. value는 Snort 규칙 옵션에 없는 이름이고, 위치(

[11번] 매크로 바이러스에 대한 설명으로 틀린 것은?

1플랫폼과 무관하에 실행된다.
2주로 이메일을 통해 감염된다.
3문서 파일의 기능을 악용한다.
4EXE 형태의 자동화된 기능을 포함한다.

▸ 매크로 바이러스는 워드·엑셀 같은 문서 파일의 매크로 기능을 악용하는 것이지, EXE 실행 파일 형태로 존재하는 것이 아니다. * 매크로는 해당 응용프로그램만 있으면 운영체제 종류와 무관하게 실행된다. * 문서를 이메일로 주고받는 과정에서 주로 감염된다. * 문서 파일에 내장된 매크로 기능을 악용한다.

[12번] Window에서 파일이 삭제된 직후 일정 시간(기본 15초)안에 동일한 이름의 파일이 생성되는 경우 방금 삭제된 파일의 테이블 레코드를 재사용하는 경우가 있다. 이러한 특징을 갖는 기능은?

1파일시스템 터널링(File system tunneling)
2Shellbags
3윈도우 파일 프로텍션
4타임스톰핑

▸ 삭제 직후 짧은 시간 안에 같은 이름의 파일이 다시 생성되면 방금 지워진 레코드를 재사용하는 현상을 파일시스템 터널링이라 부른다. 이는 파일 삭제·재생성을 반복하는 프로그램의 성능을 높이기 위한 캐시성 동작으로, 삭제된 파일의 원래 생성 시각 등 메타데이터가 새 파일에 그대로 이어질 수 있어 포렌식 분석에서 주의가 필요하다.

[13번] 리눅스 Capabilities에서 실행 바이너리에 커널 모듈을 올리거나 내릴 수 있는 권한을 할당할 수 있는 Capability는 무엇인가?

1CAP_CHOWN
2CAP_AUDIT_CONTROL
3CAP_SYS_MODULE
4CAP_MAC_ADMIN

▸ 실행 바이너리에 커널 모듈을 적재·제거할 수 있는 권한을 부여하는 리눅스 Capability는 CAP_SYS_MODULE이다. CAP_CHOWN은 파일 소유자 변경, CAP_AUDIT_CONTROL은 감사 설정 제어, CAP_MAC_ADMIN은 강제접근제어(MAC) 정책 관리에 관련된 권한으로 커널 모듈 적재와는 무관하다.

[14번] 다음 중 로그의 성격이 다른 것은?

1데이터베이스 로그
2웹서버 로그
3메일서버 로그
4유닉스 계열의 syslog

▸ 유닉스 계열의 syslog는 운영체제가 제공하는 표준 로깅 체계로, 여러 프로그램의 로그를 통합해 수집하는 시스템 로그라는 점에서 성격이 다르다. 데이터베이스 로그, 웹서버 로그, 메일서버 로그는 각각 해당 응용 서비스 자체가 자신의 형식으로 남기는 어플리케이션 로그다.

[15번] 윈도우 운영체제의 레지스트리에 대한 설명으로 틀린 것은?

1시스템 구성정보를 저장하는 데이터베이스로 SYSTEM.DAT, USER.DAT 파일을 말한다.
2레지스트리는 regedit.exe 전용 편집기에 의해서만 편집이 가능하다.
3윈도우 레지스트리 키는 HKEY_CLASS_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG 등이 있다.
4레지스트리 백업 및 복구는 shell.exe를 구동하여 행한다.

▸ 이 문항은 등록된 정답의 근거를 확정하지 못한 문항입니다. 출제 당시 기준으로 두 개 이상의 보기가 성립하거나 원문 확인이 필요한 경우이니, 표시된 정답을 그대로 외우지 마시고 개념 확인용으로만 활용하시기 바랍니다.

[16번] 대부분의 응용 프로그램에서 생성된 파일은 그 응용 프로그램이 생성한 파일임을 인식할 수 있도록 항상 동일한 몇 바이트를 파일 내부의 특정 위치에 가지고 있다. 특정위치의 고정값이 의미하는 것은?

1시그니처(Signature)
2확장자(Extensions)
3메타데이터(Metadata)
4레코드(Record)

▸ 파일 내부 고정된 위치에 각 응용프로그램마다 동일하게 들어가는 식별용 바이트 값을 시그니처(Signature)라 한다. 이를 매직 넘버라고도 부르며, 파일 확장자가 조작되어도 이 값을 통해 실제 파일 형식을 판별할 수 있어 포렌식에서 파일 카빙·형식 식별에 활용된다. * 확장자는 파일명 뒤에 붙는 표시일 뿐 파일 내부 고정 위치의 값이 아니다. * 메타데이터는 파일 자체가 아니라 파일에 대한 부가 정보를 가리키는 포괄적 용어다. * 레코드는 데이터베이스 등에서 쓰이는 자료 단위 용어로 이 상황과 맞지 않다.

[17번] 다음 그림은 a.a.a.a 시스템에서 UDP 패킷을 TTL=1부터 하나씩 늘려가면서 b.b.b.b로 전송하고, TTL=4일 때 b.b.b.b 시스템에 UDP 패킷이 도달하고 ICMP Port Unreachable(Type 3) 패킷이 a.a.a.a 시스템으로 돌아왔다. 무엇을 하기 위한 과정인가?

1ICMP scan
2traceroute
3ping
4UDP scan

▸ TTL을 1부터 하나씩 늘려 가며 UDP 패킷을 보내 경로상의 라우터를 차례로 드러내는 과정은 traceroute다. TTL은 라우터를 지날 때마다 1씩 줄고 0이 되면 그 라우터가 ICMP Time Exceeded를 보내온다. 그 응답의 출발지 주소가 곧 해당 홉의 주소이므로, TTL을 1, 2, 3 … 으로 올려 가면 a.a.a.a 에서 b.b.b.b 까지의 경로가 한 홉씩 밝혀진다. 그림은 그 마지막 시도를 그린 것이다. TTL=4로 내보낸 패킷이 라우터를 지날 때마다 TTL:4 → TTL:3 → TTL:2 → TTL:1 로 줄어들며 마침내 b.b.b.b 에 도달했고, 목적지의 해당 UDP 포트가 닫혀 있어 ICMP Port Unreachable(Type 3)이 a.a.a.a 로 되돌아왔다. 이

[18번] 다음 문장에서 설명하는 Window 시스템의 인증 구성 요소는?

1LSA(Local Security Authority)
2LAM(Local Authentication Manager)
3SAM(Security Account Manager)
4SRM(Security Reference Monitor)

▸ SID를 부여하고 그 SID로 자원 접근 허용 여부를 판정하며 감사 기록까지 남기는 구성 요소는 SRM(Security Reference Monitor)이다. 윈도우 인증은 입력받은 로그온 정보를 LSA가 받아 SAM의 계정 데이터베이스와 대조해 검증하고, 검증이 끝나면 SRM이 그 사용자에게 SID를 부여해 이후 파일·디렉터리 등 객체 접근을 통제하는 순서로 이루어진다. * LSA(Local Security Authority) — 로그온 검증 요청과 보안 정책 적용, 감사 로그 기록을 총괄하는 중앙 통제 부분으로, 파일 접근 허용 판정 자체를 수행하지는 않는다. * SAM(Security Account Manager) — 사용자 계정과 패스워드 해시를 보관하는 데이터베이스 역할이다. * LAM(L

[19번] BIOS에 대한 설명으로 틀린 것은?

1하드디스키의 구성, 종류, 용량을 확인할 수 있다.
2전원이 공급되지 않으면 정보가 유지되지 않는다.
3운영체제와 하드웨어 사이의 입출력을 담당하는 펌웨어이다.
4BIOS에 저장된 시스템 시간은 포렌식 관점에서 중요하다.

▸ BIOS 설정값은 메인 전원이 꺼져도 CMOS의 작은 배터리 전원으로 유지되므로, 전원이 공급되지 않으면 정보가 사라진다는 설명은 틀렸다. * 하드디스크의 구성·종류·용량 확인 기능은 BIOS 설정에서 제공된다. * 운영체제와 하드웨어 사이의 입출력을 담당하는 펌웨어라는 설명은 맞다. * BIOS에 저장된 시스템 시간은 파일 생성·수정 시각과 비교하는 등 포렌식 관점에서 중요한 근거가 된다.

[20번] 다음 중 인증의 방법이 아닌 것은?

1당신이 알고 있는 것(Something You Know)

2당신이 위치를 알고 있는 곳(Somewhere You Know)
3당신이 가지고 있는 것(Something You Have)
4당신 모습 자체(Something You Are)

▸ 인증 요소는 통상 아는 것(Something You Know)·가진 것(Something You Have)·본인 자체(Something You Are)·있는 곳(Somewhere You Are)의 네 가지로 분류되며, "위치를 알고 있는 곳"이라는 표현 자체는 표준적인 인증 방법 분류에 쓰이지 않는다. 나머지 세 가지는 표준적인 인증 요소 분류와 일치한다.

[21번] 패킷 필터링을 위한 규칙에 대한 설명으로 틀린 것은? (단, 서비스에 사용되는 포트는 기본값이며, Internal은 내부, External은 외부 네트워크를 의미한다.)

1 Internal External 80/TCP Allow
2 Any 169.168.2.25 21/TCP Allow
3 Internal 169.168.10.10 53/TCP Allow
4 Any Any Any Duny
1내부에서 외부로 나가는 웹 서비스에 대해서 허용한다.
2서버(169.168.2.25)로 FTP 서비스 연결은 어디에서나 가능하나 데이터 전송은 원활하게 이루어지지 않을 수 있다.
3필터링 규칙에 명시하지 않은 모든 프로토콜에 대해서는 거부한다.
4서버(169.168.10.10)로 DNS 서비스는 내부에서 이용이 가능하나 Message 정보가 512 바이트보다 클 경우에는 허용하지 않는다.

▸ DNS 서버로 가는 규칙이 53/TCP 허용이므로, 512바이트를 넘어 TCP로 전달되는 DNS 메시지야말로 통과되는 쪽이어서 '크면 허용하지 않는다'는 설명이 사실과 반대다. DNS는 메시지가 512바이트 이하일 때 UDP를, 그보다 클 때 TCP를 사용한다. 표의 3행은 Internal → 169.168.10.10 / 53/TCP / Allow 이므로 큰 메시지(TCP)는 열리고 오히려 평상시 UDP 질의가 막히는 구성이다. 나머지 설명은 규칙표와 그대로 맞아떨어진다. * 1행 Internal → External 80/TCP Allow — 내부에서 외부로 나가는 웹 접속을 허용한다. * 2행 Any → 169.168.2.25 21/TCP Allow — FTP 제어 연결(21)만 열려 있고 데이터

[22번] UDP Flooding의 대응 방안으로 틀린 것은?

1미사용 프로토콜 필터링
2도착지 IP별 임계치 기반 차단
3패킷 크기 기반 차단
4Anycast를 이용한 대응

▸ UDP Flooding 공격은 다수의 출발지에서 대량의 트래픽이 동일한 목적지(피해 서버)로 몰리는 형태이므로, 목적지 IP 기준의 임계치 차단은 정상·공격 트래픽을 구분하지 못해 효과적인 대응이 되지 못한다. 실제로는 트래픽을 보내는 출발지 IP별 임계치로 차단하거나 미사용 프로토콜 필터링, 패킷 크기 기반 차단, Anycast 분산 등을 함께 활용해야 한다.

[23번] 클라우드 시스템 및 서비스와 관련한 보안 측면의 설명으로 틀린 것은?

1클라우드 서비스를 구동하기 위해 필수적인 가상화 시스템 내 하이퍼바이저가 취약할 경우 이를 활용하는 여러개의 가상머신(VM)이 동시에 피해를 입을 가능성을 고려해야 한다.
2기존 네트워크 보안기술(방화벽, IPS/IDS)로는 가상화 내부 영역에 대한 침입탐지가 어렵다.
3사용자의 가상머신들의 상호 연결되어 내부의 가상머신에서 다른 가상 머신으로서 패킷스니핑, 해킹, DDoS 공격, 악성코드전파 등의 공격 경로가 존재한다.
4가상화 기술 중 스토리지 가상화와 네트워크 가상화에 보안 위협이 존재하나 메모리 가상화에는 보안 위협이 존재하지 않는다.

▸ 가상화 기술 중 메모리 가상화에도 보안 위협은 존재하므로, 메모리 가상화에는 위협이 없다는 설명은 틀렸다. 가상머신 간에 메모리 영역이 적절히 격리되지 않으면 한 가상머신이 다른 가상머신의 메모리 정보를 들여다보거나 유출시킬 수 있는 위협이 발생할 수 있다. * 하이퍼바이저 취약점은 여러 가상머신에 동시에 영향을 줄 수 있다는 설명은 맞다. * 기존 방화벽·IPS/IDS로는 가상화 내부 트래픽 탐지가 어렵다는 설명은 맞다. * 가상머신 간 스니핑·해킹·DDoS·악성코드 전파 경로가 존재한다는 설명은 맞다.

[24번] 다음 중 원격지 서버의 스니핑 모니터링 프로그램인 sentinal을 이용하여 스니퍼를 탐지하는 예시와 그에 대한 의미로 틀린 것은?

1./sentinel –a –t 211.47.65.4 : ARP 테스트
2./sentinel –d –f 1.1.1.1 –t 211.47.65.4 : DNS 테스트
3./sentinel–e –t 211.47.65.4 : Etherping 테스트
4./sentinel–t 211.47.65.4 –f 1.1.1.1 –d –a - : 3개의 테스트 중 하나만 테스트

▸ sentinel은 -a(ARP)·-d(DNS)·-e(Etherping) 가운데 명령행에 지정한 테스트를 모두 수행한다. 여러 테스트 옵션을 한꺼번에 붙였다고 해서 그중 하나만 골라 수행하는 것이 아니므로 이 설명은 틀렸다. 나머지는 각각 ARP 테스트, 위조 출발지(-f)를 지정한 DNS 테스트, Etherping 테스트를 실행하는 예로 옵션과 의미가 서로 맞다.