2018년 정보보안기사 필기 기출문제

전 회차 · 32문항 · 정답·해설 포함

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

2018년 정보보안기사 필기

제2회 · 32문항

[1번] 어떤 공격을 방지하기 위한 것인가?

1XSS 공격
2힙 스프레이 공격
3CSRF 공격
4SQL 인젝션 공격

▸ DEP와 NX 비트는 힙 스프레이 공격처럼 메모리에 올려둔 데이터를 코드로 실행시키는 공격을 막기 위한 보호기법이다. 힙 스프레이는 힙 영역에 NOP 슬레드와 셸코드를 대량으로 뿌려 두고 실행 흐름이 그 영역으로 넘어가게 만드는 기법이다. DEP·NX는 힙·스택처럼 데이터용으로 할당된 페이지에 실행 권한을 주지 않아 흐름이 그리로 튀어도 셸코드가 실행되지 못하게 한다. 나머지는 메모리 실행 권한과 무관한 웹 애플리케이션 계층의 공격이라 DEP·NX로 막을 수 없다. 스크립트 삽입은 입력 검증과 출력 인코딩, 요청 위조는 토큰·Referer 검증, 질의문 삽입은 파라미터 바인딩으로 대응해야 한다.

[2번] 다음 중 옳지 않은 것은?

1리눅스 시스템에서는 계정 목록을 /etc/passwd 파일에 저장하고 있다.
2일반 사용자의 사용자 번호(UID, User ID)는0번으로 부여받게 된다.
3디렉토리의 권한은 특수권한, 파일 소유자 권한, 그룹 권한, 일반(Others) 권한으로 구분된다.
4접근 권한이 rwxr-xr-x인 경우 고유한 숫자로 표기하면 755가 된다.

▸ 리눅스에서 UID 0번은 관리자 계정인 root에게 부여되는 번호이며, 일반 사용자는 배포판에 따라 보통 500번 또는 1000번 이상의 UID를 순차적으로 부여받는다. 계정 목록이 /etc/passwd 파일에 저장되는 것, 디렉토리 권한이 특수권한·소유자권한·그룹권한·일반권한으로 구성되는 것, rwxr-xr-x가 숫자로 755에 대응하는 것은 모두 올바른 설명이다.

[3번] 적절하게 고른 것은?

1가 /usr 나/temp 다/dev
2가 /usr 나/tmp 다/var
3가 /etc 나/temp 다/var
4가 /etc 나/tmp 다/dev

▸ 차례대로 /etc, /tmp, /dev가 들어간다. 시스템 환경 설정과 주요 설정 파일(passwd, shadow, hosts, services 등)은 /etc에 모여 있고, 프로그램 실행 중 만들어지는 임시 파일은 누구나 쓸 수 있도록 스티키 비트가 걸린 /tmp에 놓인다. 프린터·터미널·디스크 같은 물리 장치를 다루는 장치 파일은 /dev에 있다. /usr는 사용자 명령과 라이브러리가 들어가는 디렉터리, /var는 로그·메일·스풀처럼 크기가 변하는 데이터가 쌓이는 디렉터리이며, /temp는 유닉스 표준 디렉터리가 아니다.

[4번] 인적자원 관리자가 특정 부서 사용자들에게 같은 직무를 수행할 수 있는 접근 권한을 할당하고 있다. 이것은 다음 중 어느 것의 예인가?

1역할기반 접근 통제
2규칙기반 접근 통제
3중앙집중식 접근 통제
4강제적 접근 통제

▸ 특정 부서의 사용자들에게 동일한 직무 수행에 필요한 접근 권한을 일괄로 할당하는 방식은 사용자 개인이 아니라 직무(역할) 단위로 권한을 부여하는 역할기반 접근 통제(RBAC)의 전형적인 예이다. 역할에 권한을 먼저 매핑해 두고 사용

자를 해당 역할에 배정하면, 같은 역할을 가진 사용자 모두가 동일한 접근 권한을 갖게 되어 인적자원 관리 관점에서 부서별·직무별 권한 관리가 용이해진다.

[5번] 윈도우 레지스트리 하이브 파일이 아닌 것은?

1HKEY-CLASSES-ROOT
2HKEY LOCAL-MACHINE
3HKEY-CURRENT-SAM
4HKEY-CURRENT-USER

▸ 윈도우 레지스트리의 최상위 하이브는 HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG이며, HKEY-CURRENT-SAM이라는 명칭의 하이브는 존재하지 않는다. SAM에 관한 정보는 HKEY_LOCAL_MACHINE 하위의 SAM 키에 저장될 뿐, 그 자체가 별도의 최상위 하이브로 존재하는 것은 아니다.

[6번] 윈도우 NTFS에서 모든 파일들과 디렉터리에 대한 정보를 포함하고 있는 것은?

1MFT(Master File Table)
2FAT(File Allocation Table)
3$Attr Def
4$LogFile

▸ NTFS에서 볼륨 내 모든 파일과 디렉터리에 대한 정보(위치, 속성, 크기 등)를 담고 있는 핵심 메타데이터 구조는 MFT(Master File Table)이다. FAT는 FAT 파일시스템의 할당 테이블이고, $Attr Def와 $LogFile은 NTFS의 부속 메타파일이지 파일·디렉터리 정보 전체를 아우르는 테이블은 아니다.

[7번] 리눅스/유닉스 시스템에서 로그를 확인하는 명령어나 로그파일과 가장 거리가 먼 것은?

▸ find는 조건에 맞는 파일을 검색하는 명령어일 뿐, 로그를 확인하거나 로그파일 자체를 가리키는 용도로 쓰이지 않는다. wtmp는 로그인 기록 로그파일, history는 명령어 실행 이력 로그, pacct는 프로세스 계정(실행 명령) 로그로 모두 로그 확인과 직접 관련된 항목이다.

[8번] 다음 지문이 설명하는 데이터베이스 보안 유형은 무엇인가?

1Access Control
2Encryption
3Views
4Authorization Rules

▸ 허가받은 범위만 보이도록 전체 데이터베이스를 잘라 보여주는 보안 유형은 뷰(View)다. 뷰는 기본 테이블에서 필요한 행과 열만 뽑아 정의한 가상 테이블이어서, 사용자는 자신에게 허용된 부분 집합만 조회하게 된다. 보여줄 범위 자체를 한정한다는 점이 지문의 표현과 정확히 맞는다. 나머지 유형은 통제 방식이 다르다. * 접근 제어(Access Control): 계정·주체 단위로 데이터베이스 접근 자체를 허용하거나 차단한다. * 권한 부여 규칙(Authorization Rules): 어떤 주체가 어떤 객체에 어떤 연산을 할 수 있는지 규칙으로 정한다. * 암호화(Encryption): 저장·전송 중인 데이터를 읽을 수 없는 형태로 변환해 유출 시 내용을 보호한다.

[9번] 패스워드와 함께 일방향 해시함수에 입력되는 12비트 난수값은?

1세션키
2메시지
3솔트(salt)
4멜로리

▸ 패스워드와 함께 일방향 해시함수에 입력되어 동일한 패스워드라도 서로 다른 해시값이 나오도록 만드는 난수값은 솔트(salt)이다. 세션키는 통신 세션의 암호화에 쓰이는 값이고 메시지는 해시 입력의 원본 데이터 자체를 가리키므로, 패스워드에 덧붙는 난수값이라는 역할과는 구분된다.

[10번] 아이노드(i-node)가 가지고 있지 않은 정보는?

1파일의 이름
2파일의 링크 수

3파일 수정시각
4파일 유형

▸ 아이노드(i-node)는 파일의 소유자, 권한, 크기, 링크 수, 수정시각, 데이터 블록 위치 등 메타데이터를 담고 있지만 파일의 이름은 저장하지 않는다. 파일 이름은 디렉터리 엔트리에서 아이노드 번호와 매핑되어 관리되므로, 같은 아이노드를 여러 이름(하드링크)이 가리킬 수 있는 구조가 성립한다.

[11번] 다음 악성코드에 대한 설명 중 옳지 않은 것은?

1루트킷(Rootkit)은 단일 컴퓨터 또는 일련의 컴퓨터 네트워크에 대해 관리자 레벨의 접근을 가능하도록 하는 도구의 집합이다.
2웜(Worm)은 네트워크 등의 연결을 통하여 자신의 복제품을 전파한다.
3트로이목마(Trojan Horse)는 정상적인 프로그램으로 가장한 악성 프로그램으로 보통 복제 과정을 통해 스스로 전파된다.
4트랩도어(Trapdoor)는 정상적인 인증 과정을 거치지 않고 프로그램에 접근하는 일종의 통로이다.

▸ 트로이목마(Trojan Horse)는 정상 프로그램으로 위장해 사용자가 직접 실행하도록 유도하는 악성코드로, 스스로 복제되어 전파되는 자기복제 기능은 갖고 있지 않다. 자신을 복제해 네트워크 등을 통해 스스로 전파되는 것은 웜(Worm)의 특징이며, 루트킷의 관리자 권한 은폐 기능이나 트랩도어의 정상 인증 우회 통로라는 설명은 옳다.

[12번] 디스크 공간 할당의 논리적 단위는?

1Volume
2Page
3Cluster
4Stream

▸ 디스크 공간을 할당할 때 사용하는 논리적 최소 단위는 클러스터(Cluster)이며, 여러 섹터를 묶어 하나의 클러스터로 구성해 파일에 공간을 배정한다. Volume은 파일시스템이 놓이는 저장영역 전체, Page는 메모리 관리 단위, Stream은 NTFS의 대체 데이터 스트림 개념으로 디스크 공간 할당의 논리적 단위와는 성격이 다르다.

[13번] 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

▸ 파일시스템 무결성 점검은 소유자·소유그룹, 파일 크기, 접근·수정 시각, 하드링크 수 등의 변경 여부를 비교하는 방식으로 이루어지며, 파일에 걸린 심볼릭 링크의 개수 자체는 표준적인 점검 항목으로 다루지 않는다. 소유자·소유그룹 변경, 파일 크기 변경, 접근 시각 변경을 추적하는 것은 무결성 점검 도구가 실제로 비교하는 대표적인 속성들이다.

[14번] 다음 파일시스템(FAT, NTFS)에 대한 설명 중 옳지 않은 것은?

1FAT 뒤의 숫자는 표현 가능한 최대 클러스터 개수와 관련되어 있다.
2NTFS 파일시스템은 대용량 볼륨, 보안 및 암호화를 지원한다.
3NTFS 파일시스템은 타 운영체제 호환이 용이하다.
4저용량 볼륨에서는 FAT가 NTFS보다 속도가 빠르다.

▸ NTFS는 대용량 볼륨과 보안·암호화 기능을 지원하지만, 오래된 운영체제나 일부 비윈도우 환경에서는 제한적으로만 지원되어 타 운영체제와의 호환성이 오히려 떨어지는 편이다. FAT 뒤에 붙는 숫자가 표현 가능한 클러스터 수와 관련된다는 것, NTFS가 대용량·보안 기능을 지원한다는 것, 저용량 볼륨에서는 구조가 단순한 FAT가 NTFS보다 빠른 경향이 있다는 것은 모두 맞는 설명이다.

[15번] 다음 중 SECaaS에 대한 설명으로 적합하지 않은 것은?

1클라우드 컴퓨팅 환경 하에서 인터넷을 통하여 보안서비스를 제공하는 것을 두고 SECaaS(Security as a Service)라고 한다.
2SECaaS는 Standalone으로 클라우드 기반 보안서비스를 제공하는 형태와 클라우드 서비스 제공업체가 자사의 고객에게 보안기능을 제공하는 형태로 나뉠 수 있다
3SECaaS는 보안서비스를 ASP 형태로 공급한다는 측면에서 넓은 의미의 PaaS(Platform as a Service) 로 볼 수 있다.

4SECaaS는 인증, 안티바이러스, 침입탐지, 모의침투, 보안이벤트 관리 등의 다양한 보안 기능을 제공할 수 있다.

▸ SECaaS(Security as a Service)는 보안 서비스를 인터넷을 통해 제공한다는 점에서 소프트웨어를 서비스 형태로 제공하는 넓은 의미의 SaaS로 분류되며, 플랫폼을 제공하는 PaaS로 보는 것은 적절하지 않다. 클라우드 환경에서 인터넷으로 보안 서비스를 제공한다는 정의, Standalone형과 클라우드 제공업체 결합형으로 구분된다는 것, 인증·안티바이러스·침입탐지·모의침투 등을 제공한다는 설명은 모두 SECaaS에 대한 올바른 설명이다.

[16번] SAM에 대한 설명으로 옳지 않은 것은?

1사용자 패스워드는 해시된 상태로 저장된다.
2SID를 사용하여 각 자원에 대한 접근권한을 명시한다.
3SAM 파일은 사용자, 그룹 계정 및 암호화된 패스워드 정보를 저장하고 있는 데이터베이스이다.
4사용자 로그인 정보와 SAM 파일에 저장된 사용자 패스워드 정보를 비교해 인증 여부가 결정된다.

▸ 각 자원에 대한 접근권한은 자원의 ACL(접근제어목록)이 SID를 참조하여 명시하는 것이며, SAM 자체가 자원별 접근권한을 직접 명시하는 것은 아니다. SAM은 사용자·그룹 계정과 해시된 패스워드 정보를 저장하는 데이터베이스로, 로그인 시 입력된 패스워드와 SAM에 저장된 해시값을 비교해 인증 여부를 판단하는 역할을 한다.

[17번] 로그분석에 사용되며 문자열을 처리하는 Unix 명령어와 가장 거리가 먼 것은?

▸ nohup은 터미널 연결이 끊겨도 프로세스가 계속 실행되도록 하는 작업 제어 명령어일 뿐, 텍스트나 로그의 문자열을 처리하는 명령어가 아니다. awk, wc, grep은 각각 필드 추출·가공, 줄·단어·문자 수 계산, 패턴 검색을 수행하는 문자열 처리 명령어로 로그 분석에 자주 쓰인다.

[18번] 다음 지문에서 설명하고 있는 침입탐지 기술이 무엇인지 고르시오.

1IDS(Instrusion Detection System)
2IPS(Instrusion Prevention System)
3UTM(Unified Threat Management)
4Honeypot

▸ 공격자의 동작 정보를 모으고 오래 머물도록 유도하는 기술은 허니팟(Honeypot)이다. 허니팟은 일부러 취약하게 꾸며 놓은 미끼 시스템으로, 공격자를 끌어들여 공격 기법·도구·경로를 관찰하고 관리자가 대응할 시간을 버는 것이 목적이다. 탐지나 차단이 아니라 유인과 정보 수집이 핵심이라는 점이 지문의 두 조건과 맞는다. 나머지는 목적이 다르다. * 침입탐지 시스템: 침입 징후를 탐지해 경보를 울리는 데 그친다. * 침입방지 시스템: 탐지에 더해 해당 트래픽을 실시간 차단한다. * 통합 위협 관리: 방화벽·침입탐지/방지·안티바이러스 등을 한 장비에 통합한 제품이다.

[19번] 다음 중 Unix 시스템에서 secure.txt 파일의 소유자에게는 읽기와 실행권한을 부여하고 다른 사용자에게는 읽기 권한을 제거하라는 권한 변경 명령으로 알맞은 것은?

1#chmod306 secure.txt
2#chmod504 secure.txt
3#chmodotrx, a-r secure.txt
4#chmodu=rx, o-r secure.txt

▸ 요구사항은 소유자에게 읽기·실행(r-x) 권한을 부여하고 다른 사용자에게서는 읽기 권한만 제거하는 것이므로, 심볼릭 모드로 u=rx와 o-r을 함께 지정하는 명령이 정확히 대응한다. 숫자 모드 306은 소유자 권한이 쓰기·실행(-wx)이 되어 읽기가 빠지고 다른 사용자에게는 오히려 읽기·쓰기(rw-)를 부여하며, 504는 소유자 권한(r-x)은 맞지만 다른 사용자에게 읽기(r--)를 부여해 읽기 권한을 제거하라는 요구와 정반대가 된다.

[20번] 리눅스에서 관리하는 주요 로그파일에 대한 설명으로 옳지 않은 것은?

1/var/log/cron : 시스템의 정기적인 작업에 대한 로그
2/var/log/messages : 커널에서 보내주는 실시간 메시지
3/var/log/secure : 시스템의 접속에 관한 로그로 언제/누가/어디의 정보를 포함
4/var/log/xferlog : 메일 송수신에 관한 로그

▸ /var/log/xferlog는 FTP를 통한 파일 전송 기록을 남기는 로그이며, 메일 송수신에 관한 로그가 아니다. /var/log/cron은 정기 작업 실행 기록, /var/log/messages는 커널을 비롯한 시스템의 실시간 메시지, /var/log/secure는 로그인·접속 등 인증 관련 기록을 남기는 로그로 각각의 설명이 올바르다.

[21번] 다음은 PORT 스캔 공격에 관한 설명이다. 설명 중 맞는 것을 모두 고른 것은?

1가, 나
2가, 나, 다.
3가, 나, 라
4가, 나, 다, 라

[22번] 다음의 포트 스캔 중 플래그 (SYN, RST, ACK, AN, PS URG)을 모두 off하여 스캔하는 것은?

1TCP SYN 스캔
2Fin 스캔
3Null 스캔
4Xmas 스캔

▸ SYN, RST, ACK, FIN, PSH, URG 등 TCP 플래그를 모두 off한 상태로 패킷을 보내 대상의 포트 상태를 탐지하는 기법은 Null 스캔이다. TCP SYN 스캔은 SYN 플래그만 사용하고, FIN 스캔은 FIN 플래그만 사용하며, Xmas 스캔은 FIN·PSH·URG 플래그를 모두 켜서 보낸다는 점에서 플래그를 전부 끄는 방식과 구분된다.

[23번] 오용탐지 방법으로 적당하지 않은 것은?

1시그니처 분석
2페트리넷(Petri-net)
3상태전이 분석
4데이터마이닝

▸ 오용탐지(Misuse Detection)는 이미 알려진 공격의 패턴을 시그니처, 상태전이, 페트리넷 등으로 정의해 비교하는 방식이며, 대량의 데이터에서 통계적 패턴이나 이상치를 찾아내는 데이터마이닝 기법은 주로 이상(비정상) 탐지에서 활용된다. 시그니처 분석, 페트리넷, 상태전이 분석은 모두 알려진 공격 패턴을 정의하고 매칭하는 오용탐지 기법에 해당한다.

[24번] 공격 대상이 방문할 가능성이 있는 합법적인 웹 사이트를 미리 감염시킨 뒤, 잠복하고 있다가 공격 대상이 방문하면 대상의 컴퓨터에 악성코드를 설치하는 공격 방법은?

1악성 봇(Malicious Bot) 공격
2워터링 홀(Watering Hole) 공격
3스피어 피싱(Spear Phishing) 공격
4피싱(Phishing) 공격

▸ 공격 대상이 자주 방문할 만한 합법적 웹사이트를 미리 감염시켜 놓고 방문을 기다리는 공격 방식은 워터링 홀(Watering Hole) 공격이다. 피싱과 스피어 피싱은 이메일 등으로 사용자를 속여 직접 정보를 입력하게 유도하는 방식이고, 악성 봇 공격은 감염된 시스템을 원격 제어하는 데 초점을 두므로, 신뢰하는 사이트 자체를 감염시켜 잠복한다는 특징과는 구분된다.

[25번] 다음 중 패킷의 출발지와 목적지 모두를 반영하여 주소 변환을 수행하는 NAT(Network Address Translation)는?

1동적 NAT
2정적 NAT
3바이패스 NAT
4폴리시 NAT

▸ 패킷의 출발지와 목적지 주소를 함께 고려해 어떤 규칙으로 주소를 변환할지 결정하는 방식은 폴리시(정책기반) NAT이다. 동적 NAT와 정적 NAT는 출발지 주소를 기준으로 매핑을 정하는 방식이고, 바이패스 NAT는 주소 변환을 건너뛰는 개념이어서 출발지·목적지를 함께 반영해 변환 여부와 방식을 결정하는 정책기반 방식과는 다르다.

[26번] 도메인을 탈취하거나 도메인 네임 시스템 또는 프록시 서버의 주소를 변조함으로써 사용자들로 하여금 진짜 사이트로 오인해 접속하도록 유도한 뒤, 개인 정보를 탈취하는 해킹 기법은?

1피싱
2파밍
3스미싱

4봇넷

▸ 도메인을 탈취하거나 DNS·프록시 서버의 주소를 변조해 사용자가 진짜 사이트로 오인하고 접속하도록 유도한 뒤 개인정보를 탈취하는 수법은 파밍(Pharming)이다. 피싱은 가짜 메일이나 사이트로 정보를 직접 입력하게 속이는 방식이고, 스미싱은 문자메시지를 이용하며, 봇넷은 다수의 감염 시스템을 원격 제어하는 네트워크를 가리켜 도메인·서버 주소 자체를 변조한다는 특징과는 구분된다.

[27번] 다음 용어 중 개념상 나머지와 가장 거리가 먼 것은?

1sniffing
2eavesdropping
3tapping
4spoofing

▸ 스니핑, 이브스드로핑(eavesdropping), 태핑(tapping)은 모두 통신 내용을 몰래 엿듣거나 가로채는 수동적 도청 계열의 개념이다. 반면 스푸핑(spoofing)은 출발지 주소나 신원 정보를 위조해 상대를 속이는 능동적 공격 개념이므로, 나머지 세 용어와는 성격이 다르다.

[28번] 다음 중 end point에 설치되어 다양한 보안 기능을 통합적으로 수행하는 보안 시스템을 지칭하는 것은?

▸ NAC(Network Access Control)은 단말에 설치된 에이전트를 통해 접속 전 보안 상태를 점검하고, 백신 연동, 패치관리, 매체제어, 자산관리 등 다양한 보안 기능을 통합적으로 수행하는 엔드포인트 보안 시스템이다. IPS나 방화벽은 네트워크 구간에서 트래픽을 검사·차단하는 장비이고, UTM은 여러 보안 기능을 하나로 묶은 네트워크 게이트웨이형 장비여서 단말에 직접 설치되는 통합 보안 에이전트라는 설명과는 성격이 다르다.

[29번] 다음 중 전문가 시스템(Expert System)을 이용한 IDS에서 사용되는 침입 탐지기법은?

1Behavior Detection
2State Transition Detection
3Knowledge Based Detection
4Statistical Detection

▸ 사람의 지식과 규칙을 축적해 판단하는 전문가 시스템(Expert System)을 이용한 침입탐지 기법은 규칙 기반의 지식기반탐지(Knowledge Based Detection)이다. 행위기반탐지는 통계·행동 패턴에 의존하고, 상태전이탐지는 공격 단계를 상태 흐름으로 모델링하며, 통계적 탐지는 수치적 이상 여부를 판단하는 방식이어서 전문가 시스템의 규칙 기반 추론과는 구분된다.

[30번] Snort의 각 규칙은 고정된 헤더와 옵션을 가지고 있다. 패킷의 payload 데이터를 검사할 때 사용되는 옵션에 포함되지 않는 필드는?

1ttl
2content
3depth
4offset

▸ Snort 규칙에서 패킷의 payload(내용) 데이터를 검사하는 옵션에는 content, depth, offset처럼 문자열의 존재 여부와 위치를 지정하는 필드가 쓰이며, ttl은 IP 헤더의 생존시간 값을 검사하는 옵션으로 payload 검사와는 무관하다. content는 찾을 문자열, depth는 검사할 최대 깊이, offset은 검사를 시작할 위치를 지정하는 옵션으로 모두 payload 내용을 대상으로 한다.

[31번] 이래 지문 빈칸에 들어갈 용어를 바르게 짝지은 것은?

1가 : 포트 미러링(Port Mirroring) 나: 수집 모드(Acquisition Mode)
2가 : 포트 미러링(Port Mirroring) 나 : 무차별 모드(Promiscuous Mode)
3가 : 패킷 포워딩(Packet Forwarding) 나 : 수집 모드(Acquisition Mode)
4가 : 패킷 포워딩(Packet Forwarding) 나 : 무차별 모드(Promiscuous Mode)

▸ 빈칸은 각각 포트 미러링(Port Mirroring)과 무차별 모드(Promiscuous Mode)다. 스위치는 목적지 MAC 주소를 보고 해당 포트로만 프레임을 내보내므로, 남의 트래픽까지 받으려면 지정한 포트로 트래픽 사본을 복제해 주는 포트 미러링(SPAN) 설정이 필요하다. 랜카드는 기본적으로 자기 MAC 주소가 아닌 프레임을 버리기 때문에, 무차별 모드로 바꿔야 수신한 모든 프레임을 운영체제로 올려 Tcpdump가 볼 수 있다. 패킷 포워딩은 장비가 프레임을 전달하는 일반 동작일

뿐이고, 수집 모드는 랜카드 동작 모드 명칭이 아니다.

[32번] 다음 중 VoIP 서비스에 대한 공격과 가장 거리가 먼 것은?

1Register 플러딩 공격
2GET 플러딩 공격
3INVITE 플러딩 공격
4RTP 플러딩 공격

▸ GET 플러딩 공격은 HTTP 웹 서버를 대상으로 하는 공격이며 VoIP 서비스와는 직접 관련이 없다. * Register 플러딩은 SIP 세션 등록 메시지를 대량으로 보내 서버 자원을 고갈시키는 VoIP 공격이다. * INVITE 플러딩은 SIP 세션 개시 메시지를 대량 전송해 통화 처리 자원을 소진시키는 VoIP 공격이다. * RTP 플러딩은 실제 음성 데이터가 오가는 RTP 스트림을 겨냥한 VoIP 공격이다. 즉 SIP·RTP를 이용한 세 공격과 달리 GET 플러딩은 VoIP와 무관한 웹 계층 공격이다.