정보보안기사 필기 기출문제 합본 (2018–2023)

전 6개년 277문항 · 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.

2019년 정보보안기사 필기

제1회 · 28문항

[1번] 다음 중 주로 카메라, DVR 등 인터넷에 연결된 기기들을 감염시켜 봇넷을 만든 후 디도스(DDoS) 공격을 수행하는 악성코드는?

1백오리피스(BackOrifice) 악성코드
2다이어(Dyre) 악성코드
3미라이(Mirai) 악성코드
4워너크라이(Wannacry) 악성코드

▸ 카메라, DVR 등 인터넷에 연결된 IoT 기기를 감염시켜 봇넷을 구성한 뒤 디도스 공격에 활용하는 대표적인 악성코드는 미라이(Mirai)다. 미라이는 기본 계정과 취약한 패스워드가 설정된 IoT 장치를 스캔해 감염시키고, 확보한 대규모 봇넷으로 대상 서버에 대량 트래픽을 전송하는 디도스 공격을 수행한 것으로 알려져 있다.

[2번] 계정의 패스워드를 암호화된 형태로 저장하고 있는 파일은?

1/etc/security
2/etc/shadow
3/etc/profile
4/etc/login.defs

▸ 리눅스 시스템에서 계정의 패스워드를 암호화된 형태로 저장하는 파일은 /etc/shadow다. 초기 유닉스 체계에서는 /etc/passwd에 암호화된 패스워드를 함께 저장했으나, 일반 사용자도 읽을 수 있어 오프라인 크래킹에 취약했기 때문에 이후 root만 읽을 수 있는 shadow 파일로 패스워드 정보를 분리했다.

[3번] Internet Explorer의 검색 히스토리는 어느에 저장되는가?

1config.sys
2command.com
3index.dat
4sys.bak

▸ 인터넷 익스플로러의 검색 및 방문 히스토리는 index.dat 파일에 저장된다. index.dat은 사용자가 직접 열지 않아도 브라우저 종료 이후에도 남아 있어, 포렌식 조사에서 웹 사용 기록을 복원하는 핵심 증거 파일로 다뤄진다.

[4번] ftp 접근 여부를 검토할 수 있는 로그는?

▸ FTP 접속 및 파일 송수신 내역을 검토할 수 있는 로그 파일은 xferlog다. xferlog는 파일 전송이 이루어질 때마다 전송 시각, 접속 계정, 전송 파일명 등을 기록해 FTP 접근 여부를 확인하는 근거가 된다.

[5번] Null Session 공유 취약점을 가지고 있는 것은?

▸ 인증 없이 세션을 맺을 수 있는 Null Session 취약점과 관련된 윈도우 공유는 IPC$다. IPC$는 프로세스 간 통신을 위한 특수 공유로, 과거 윈도우 환경에서는 익명 사용자도 이 공유를 통해 계정·공유 목록 등의 정보를 열람할 수 있는 취약점이 있었다.

[6번] root 계정과 동일한 권한을 가진 계정은?

1chalie 계정 uid: 0 gid: 200
2sally 계정 uid: 100 gid: 0
3johny 계정 uid: 10 gid: 10
4sara 계정 uid: 10 gid: 200

▸ 유닉스/리눅스 시스템에서 root 계정과 동일한 권한을 갖는지는 UID(사용자 식별번호) 값으로 결정되며, UID가 0이면 계정 이름과 무관하게 root 권한을 갖는다. chalie 계정은 GID가 200이라도 UID가 0이므로 파일 소유권이나 프로세스 실행 권한 면에서 root와 동일하게 취급된다. * UID 100인 sally 계정은 GID가 0이어도 사용자 권한 자체는 root가 아니다. * UID 10인 johny, sara 계정도 마찬가지로 root 권한을 갖지 않는다.

[7번] 다음 지문에서 설명하는 크래킹 방법은?

1Rainbow Table Attack
2Dictionary Attack
3Brute Force Attack
4Hash Attack

▸ 가능한 문자 집합에서 만들 수 있는 모든 조합을 빠짐없이 생성해 하나씩 대입하는 방식은 Brute Force Attack(전수조사 공격)이다. 지문의 "사용될 수 있는 문자열의 범위를 정하고, 그 범위 내에서 생성 가능한 모든 패스워드를 생성"이 결정적 단서로, 시간만 충분하면 반드시 성공하지만 자릿수와 문자 종류가 늘수록 경우의 수가 기하급수로 커진다. * 미리 만들어 둔 사전 파일의 단어와 그 변형만 시도하는 방식은 Dictionary Attack이다. * 평문과 해시값 쌍을 미리 계산해 표로 저장해 두고 조회하는 방식은 Rainbow Table Attack이다. * Hash Attack은 패스워드 크래킹 기법으로 따로 정의된 명칭이 아니다.

[8번] 리눅스 서버 관리자 A씨는 피해 시스템을 점검하던 중 다음과 같은 시스템 바이너리 파일들이 변조된 것을 확인하였다. 공격자의 입장에서 파일을 변조한 이유가 잘못 연결된 것은?

1ps, top: 특정 프로세스 정보를 숨김
2ls, du: 특정 파일이나 디렉터리를 숨김
3w, who: 특정 사용자의 정보를 숨김
4ifconfig: 특정 IP에서의 접속을 숨김

▸ 공격자가 ifconfig를 변조하는 목적은 특정 IP의 접속을 숨기기 위해서가 아니라, 네트워크 카드가 프로미스큐어스(PROMISC) 모드로 동작 중임을 나타내는 표시를 감추어 스니퍼 실행 사실을 은폐하기 위한 것이다. 특정 IP에서의 접속 내역을 숨기는 작업은 보통 연결 상태를 보여주는 netstat과 같은 도구를 변조해 이루어진다. * ps, top 변조는 특정 프로세스를 목록에서 감추기 위한 것이다. * ls, du 변조는 특정 파일이나 디렉터리를 감추기 위한 것이다. * w, who 변조는 특정 사용자의 접속 정보를 감추기 위한 것이다.

[9번] 소유자에게만 읽기와 쓰기 권한이 있는 경우는?

1rwxr--r-- 1 root root 312 Nov 30 13:05 listner.ora
2r-xrw-r-- 1 root root 312 Nov 30 13:05 listner.ora
3rwxrw-rw- 1 root root 312 Nov 30 13:05 listner.ora
4rwxr—rw- 1 root root 312 Nov 30 13:05 listner.ora

▸ 소유자에게만 읽기와 쓰기 권한이 있으려면 그룹과 기타 사용자에게는 쓰기 권한이 없어야 하며, 소유자에게는 쓰기 권한이 주어져야 한다. 소유자가 rwx, 그룹과 기타 사용자가 각각 r--로 설정된 권한은 오직 소유자만 파일을 수정할 수 있고 그룹과 기타 사용자는 읽기만 가능한 상태를 나타낸다. 나머지 보기들은 소유자가 쓰기 권한을 갖지 못하거나 그룹 또는 기타 사용자에게도 쓰기 권한이 함께 부여되어 있어 조건을 충족하지 못한다.

[10번] 다음 빈 칸 들어갈 서비스명으로 적절한 것은?

▸ 다른 주소 공간의 함수·프로시저를 마치 로컬 호출처럼 실행하게 해 주는 프로세스 간 통신 프로토콜은 RPC(Remote Procedure Call)이다. 빈칸을 그대로 대입하면 두 번째 문단이 XML-RPC가 되는 것이 결정적 단서로, RPC 호출의 매개변수와 리턴값을 XML로 인코딩해 주고받는 분산 통신 방식이다. 유닉스에서는 portmapper(111번)가 RPC 서비스의 포트를 중개한다. * SSHD는 암호화된 원격 접속 셸을 제공하는 데몬으로 함수 단위 원격 호출과는 성격이 다르다. * Bluetooth는 근거리 무선 통신 규격이다. * NFS는 원격 파일시스템 공유 서비스로, 내부적으로 RPC를 이용할 뿐 RPC 자

체는 아니며 XML을 앞에 붙인 서비스명도 존재하지 않는다.

[11번] 다음 지문에서 설명은?

▸ MINIX 파일시스템의 한계를 보완해 만든 리눅스 최초의 파일시스템은 EXT(Extended File System)이다. 볼륨 크기를 2GB까지, 파일명을 255byte까지 늘렸지만 접근제어·inode 수정·타임스탬프 수정을 지원하지 못했고, 연결 리스트로 빈 블록을 관리해 쓸수록 단편화가 심해지는 결함 때문에 곧 ext2로 대체됐다. * FAT16과 FAT32는 MS-DOS·Windows 계열 파일시스템이라 MINIX 보완과 무관하고 inode라는 개념 자체가 없다. * NTFS는 저널링과 ACL 기반 접근제어, 압축·암호화까지 갖춘 Windows NT 계열 파일시스템이므로 "접근제어가 불가능하다"는 설명과 정면으로 어긋난다.

[12번] 다음 중 윈도우 로그 종류와 설명이 가장 바르게 짝지어진 것은?

1계정 관리 감사 - 사용자 권한 할당 정책, 감사 정책, 신뢰 정책의 변경과 관련된 사항을 로깅한다.
2정책 변경 감사 - 권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.
3개체 액세스 감사 - 특정 파일이나 디렉터리, 레지스트리 키 등과 같은 객체에 대한 접근을 시도하거나 속성 변경 등을 탐지한다.
4로그인 이벤트 감사 - 시스템의 시작과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.

▸ 개체 액세스 감사는 특정 파일, 디렉터리, 레지스트리 키 같은 객체에 대한 접근 시도나 속성 변경을 탐지하는 기능이 맞다. 나머지 보기는 로그 종류와 설명이 서로 뒤바뀌어 있다. * 사용자 권한 할당·감사·신뢰 정책의 변경을 기록하는 것은 계정 관리 감사가 아니라 정책 변경 감사의 역할이다. * 권한 설정 변경이나 관리자 권한이 필요한 작업을 로깅하는 것은 정책 변경 감사가 아니라 권한 사용 감사의 역할이다. * 시스템의 시작·종료나 보안 로그 삭제 등을 기록하는 것은 로그인 이벤트 감사가 아니라 시스템 이벤트 감사의 역할이다.

[13번] tcpwrapper의 설정파일의 내용이 다음과 같을 때, 어떤 현상이 발생하는가?

1모든 접속이 허용된다.
2모든 접속이 차단된다.
3일부 서비스는 모두 허용되고 일부 서비스는 모두 차단된다.
4알 수 없다.

▸ TCP Wrapper는 hosts.allow를 먼저 읽어 일치하면 그 자리에서 허용으로 판정을 끝내므로, 두 파일에 똑같이 "All: All"이 들어 있으면 결과는 모든 접속 허용이다. 판정 순서는 hosts.allow 일치 시 허용 → 불일치면 hosts.deny 일치 시 차단 → 양쪽 모두 불일치면 허용이다. 따라서 hosts.deny의 "All: All"은 앞 단계에서 이미 허용 결론이 났기 때문에 아예 평가되지 않는다. 차단을 의도했다면 hosts.deny에만 전체 거부를 두고 hosts.allow에는 허용할 대상만 한정해 적어야 하며, 지금처럼 양쪽을 모두 전체 허용으로 두면 거부 규칙이 무력화된다.

[14번] wtmp 로그 파일에 대한 설명 중 옳지 않은 것은?

1사용자의 로그인 및 로그아웃 정보 포함
2로그인 실패 정보 포함
3바이너리 형태로 저장
4시스템 종료 및 부팅 정보 포함

▸ 로그인 실패 정보는 wtmp가 아니라 btmp 파일에 기록되므로, 이를 wtmp의 특징으로 설명한 것은 옳지 않다. wtmp는 성공한 로그인·로그아웃 기록과 시스템의 부팅·종료 이력을 바이너리 형태로 담고 있는 로그 파일이다. * 사용자의 로그인·로그아웃 정보를 포함한다는 설명은 wtmp의 특징이 맞다. * 바이너리 형태로 저장된다는 설명도 wtmp의 특징이 맞다. * 시스템 종료 및 부팅 정보를 포함한다는 설명도 wtmp의 특징이 맞다.

[15번] 다음 지문에서 설명하고 있는 것은?

1sudo
2PAM
3Shell script
4Batch file

▸ 인증 로직을 응용프로그램에서 분리해 끼워 넣을 수 있는 공유 라이브러리 모듈로 제공하는 구조는 PAM(Pluggable Authentication Modules)이다. login·su·sshd 같은 프로그램은 PAM API만 호출하고, 실제 인증 방식은 /etc/pam.d/ 아래 설정에서 pam_unix·pam_cracklib 등 모듈을 갈아 끼워 결정한다. 그래서 프로그램을 다시 컴파일하지 않고도 인증 방법을 교체할 수 있다. * sudo는 일반 사용자가 지정된 명령을 관리자 권한으로 실행하게 해 주는 권한 위임 도구다. *

Shell script와 Batch file은 명령을 모아 실행하는 스크립트 파일일 뿐, 인증 프레임워크가 아니며 공유 라이브러리도 아니다.

[16번] 리눅스 운영체제 특수 권한에 대한 설명으로 틀린 것은?

1SetGID가 부여된 파일은 소유 그룹의 실행 권한이 x에서 s로 변경
2SetUID가 부여된 파일은 소유자의 실행 권한이 x에서 s로 변경
3Sticky bit가 부여된 디렉터리는 그 외 사용자의 실행 권한이 x에서 s로 변경
4Sticky bit는 /tmp와 같은 777 권한의 공용 디렉터리에서 파일 삭제 문제를 해결

▸ Sticky bit가 부여된 디렉터리에서 기타 사용자의 실행 권한 표시는 x에서 t(또는 실행 권한이 없을 때 T)로 바뀌는 것이지 s로 바뀌는 것이 아니다. s는 SetUID·SetGID에서 사용하는 표시이며, Sticky bit는 이와 구분되는 별도의 특수 권한 표시를 사용한다. * SetGID가 부여된 파일에서 소유 그룹의 실행 권한이 x에서 s로 바뀐다는 설명은 옳다. * SetUID가 부여된 파일에서 소유자의 실행 권한이 x에서 s로 바뀐다는 설명도 옳다. * Sticky bit가 /tmp처럼 누구나 쓸 수 있는 디렉터리에서 다른 사용자의 파일이 함부로 삭제되는 문제를 막는다는 설명도 옳다.

[17번] 각 파일확장자에 대한 정보와 관련 응용프로그램 간의 연결에 대한 정보를 포함하고 있는 윈도우 레지스트리 키는?

1HKEY_CLASSES_ROOT
2HKEY_LOCAL_MACHINE
3HKEY_CURRENT_CONFIG
4HKEY_USERS

▸ 파일 확장자와 이를 열 응용프로그램 간의 연결 정보를 담고 있는 윈도우 레지스트리 키는 HKEY_CLASSES_ROOT다. 이 키에는 확장자별 파일 형식(ProgID)과 그 형식을 실행할 프로그램 경로, 아이콘 등의 연결 정보가 저장되어 있어 파일을 더블클릭했을 때 어떤 프로그램으로 열릴지를 결정한다.

[18번] 다음 지문에서 설명하는 것은?

1wireshark
2tripwire
3snort
4iptables

▸ "가벼운(Lightweight) 네트워크 침입탐지시스템"이라는 표현은 Snort의 공식 소개 문구를 그대로 옮긴 것이다. Snort는 룰(rule) 기반으로 패킷 헤더와 페이로드를 검사해 버퍼 오버플로우·Stealth 포트스캔·CGI 공격·SMB 탐색·OS 핑거프린팅 시도를 탐지하며, 스니퍼·패킷 로거·네트워크 침입탐지 세 가지 모드로 동작한다. * wireshark는 캡처한 패킷을 사람이 분석하도록 보여 주는 프로토콜 분석기로, 공격 시그니처 룰 매칭 기능이 없다. * tripwire는 파일의 해시를 기준선과 대조하는 호스트 기반 무결성 점검 도구다. * iptables는 리눅스 커널의 패킷 필터링 방화벽으로 접근 차단이 목적이며 침입 탐지 기능은 수행하지 않는다.

[19번] 빈칸 ㉠, ㉡에 들어갈 용어를 바르게 짝지은 것은?

1㉠ Web Shell ㉡ Fuzzing
2㉠ Spear Phishing ㉡ Fuzzing
3㉠ File Upload ㉡ Exploit
4㉠ Drive By Download ㉡ Exploit

▸ 웹사이트에 악성 스크립트를 숨겨 두고 방문만 해도 악성코드가 내려받아지게 하는 기법이 Drive By Download이며, 그 스크립트가 브라우저·플러그인의 취약점을 파고드는 코드가 Exploit 코드다. 클릭이나 설치 같은 행위를 전혀 하지 않아도 페이지 접속만으로 감염된다는 지문의 마지막 문장이 이 기법의 정의 그 자체다. * Web Shell은 침해한 서버에 올려 두고 공격자가 원격으로 명령을 내리는 스크립트로, 방문자를 감염시키는 수단이 아니다. * Spear Phishing은 특정 대상에게 맞춤 메일을 보내 첨부파일이나 링크를 열게 하는 공격이라 "사용자의 개입 없이"와 맞지 않는다. * File Upload 공격은 서버에 악성 파일을 직접 올려 실행시키는 서버 침해 기법으로, 홈페이지 방

[20번] UNIX 또는 리눅스 시스템에서 똑같은 작업을 사용자가 지정된 시간에 반복 작업하기 위해서 cron 테이블을 작성한다. 사용자가 매주 토요일 오전 10시 정각에 'mytest' 라는 프로그램을 주기적으로 수행시키기 위해 작성한 cron 테이블 내용으로 맞는 것은?

10 10 6 * * mytest
20 10 * * 6 mytest
30 10 * 6 * mytest
40 * * 10 6 mytest

▸ cron 테이블은 분 시 일 월 요일 순서로 실행 시각을 지정하며, 토요일은 요일 필드에서 6으로 표기한다. 매주 토요일 오전 10시 정각에 실행하려면 일과 월 필드는 특정 값을 지정하지 않는 * 로 두고, 분 필드에 0, 시 필드에 10, 요일 필드에 6을 넣어야 한다.

[21번] 다음 지문에서 설명하고 있는 보안 기술은?

▸ USB·하드디스크 같은 매체 제어와 블루투스·LTE 같은 통신 규격 제어로 내부 자료의 반출 경로를 차단하는 솔루션은 DLP(Data Loss Prevention)다. DLP는 저장·전송되는 문서의 내용을 검사해 기밀로 판정되면 복사·전송·출력 자체를 막는, 유출 방지 관점의 기술이다. * DRM은 문서를 암호화해 배포한 뒤 권한 있는 사용자만 열람·편집하도록 사용 권한을 통제하는 기술로, 반출 경로 차단이 아니라 파일 자체의 이용 통제가 목적이다. * IPS는 외부에서 유입되는 공격 트래픽을 탐지·차단하는 침입방지시스템이다. * Firewall은 IP·포트 단위의 접근통제 장비로 내부 자료의 내용을 판별하지 못한다.

[22번] DDoS(Distributed Denial of Service) 공격에 대한 공격유형을 파악하려고 한다. 이때 유입 트래픽을 확보하기 위해 사용될 수 있는 도구로는?

1argus
2ngrep
3tcpdstat
4tcpdump

▸ 디도스 공격의 유입 트래픽 자체를 확보하기 위해 사용하는 도구는 tcpdump다. tcpdump는 네트워크 인터페이스를 지나는 패킷을 그대로 캡처해 저장하는 도구이며, argus나 tcpdstat 같은 도구는 이렇게 확보된 트래픽 데이터를 가공해 흐름 통계를 뽑아내는 분석 도구에 가깝다.

[23번] NAC의 주요 기능으로 옳지 않은 것은?

1PC 및 네트워크 장치 통제
2접근제어 및 인증
3폭탄 메일이나 스팸 메일 차단
4해킹, 웜, 유해 트래픽 탐지 및 차단

▸ 폭탄 메일이나 스팸 메일 차단은 NAC(Network Access Control)의 주요 기능에 해당하지 않는다. NAC는 PC 및 네트워크 장치를 통제하고 접근제어·인증을 수행하며, 해킹·웜 등 유해 트래픽을 탐지·차단해 내부 네트워크 접근 자체를 관리하는 솔루션이다. 스팸이나 폭탄 메일을 걸러내는 기능은 메일 보안(스팸 필터링) 솔루션의 영역이지 네트워크 접근 통제의 영역이 아니다.

[24번] 스머프 공격에서 echo request 패킷을 수신 서브넷 전체에 전달하기 위해 라우터의 해당 인터페이스에서 활성화해야 하는 것은?

1ip direct broadcast
2ICMP Redirect
3ARP Spoofing
4Switch Jamming

▸ 스머프 공격은 위조된 발신지 주소로 보낸 ICMP echo request를 서브넷 전체 호스트에 전달해 다수의 응답이 피해자에게 몰리게 하는 공격으로, 이때 라우터가 브로드캐스트 주소로 향하는 패킷을 서브넷 내부로 전달하도록 하는 설정이 바로 IP Directed Broadcast다. 라우터 인터페이스에서 이 기능이 켜져 있으면 외부에서 보낸 브로드캐스트 주소행 패킷이 해당 서브넷의 모든 호스트에 전달되어 증폭 공격이 가능해진다.

[25번] 다음 중 침입탐지시스템 및 침입방지시스템에 대한 설명으로 틀린 것은?

1침입탐지시스템에서 문자열을 비교하여 네트워크 패킷을 검사하는 방법은 Signature-based Detection의 일종이다.
2Anomaly Detection은 정상 행위를 규정하여 공격을 탐지하는 방법이다.
3알려지지 않은 공격을 Signature-based Detection 방법으로 탐지할 수 있다.

4침입방지시스템은 침입자에게 시스템이나 네트워크를 사용하지 못하게 하는 등 능동적인 기능을 수행할 수 있다.

▸ Signature-based Detection은 이미 알려진 공격 패턴(시그니처)과 일치하는지를 비교하는 방식이므로, 알려지지 않은 새로운 공격은 이 방식으로 탐지할 수 없다는 점이 옳지 않은 설명이다. 알려지지 않은 공격을 탐지하려면 정상 행위를 기준으로 삼아 벗어난 행위를 잡아내는 Anomaly Detection 방식이 필요하다. * 문자열 비교로 패킷을 검사하는 방식이 Signature-based Detection의 일종이라는 설명은 옳다. * Anomaly Detection이 정상 행위를 규정해 공격을 탐지한다는 설명도 옳다. * 침입방지시스템이 침입자의 시스템·네트워크 사용을 능동적으로 차단할 수 있다는 설명도 옳다.

[26번] 다음 중 방화벽의 기능과 가장 거리가 먼 것은?

1접근제어
2데이터 필터링과 축약
3로깅과 감사추적
4인증

▸ 데이터 필터링과 축약은 방화벽의 핵심 기능과는 거리가 멀다. 방화벽은 정해진 규칙에 따라 트래픽을 허용·차단하는 접근제어, 통신 기록을 남기는 로깅과 감사추적, 사용자나 시스템을 확인하는 인증 기능을 수행하는 장비다. 대량의 데이터를 걸러내고 축약해 분석에 활용하는 작업은 로그 분석이나 침입탐지 체계의 영역에 가깝다.

[27번] 다음 빈칸 ㉠에 들어갈 알맞은 용어는?

1PLC
2SCADA
3Modbus
4Stuxnet

▸ 산업제어시스템의 공정과 설비를 원격에서 감시하고 제어하는 상위 컴퓨터 시스템은 SCADA(Supervisory Control And Data Acquisition)다. 현장의 센서·제어기에서 데이터를 수집해 중앙 HMI에 표시하고 제어 명령을 내려보내는 계층으로, 전력·상하수도·가스 같은 사회기반시설 운영의 핵심이라 사이버 공격의 표적이 된다. * PLC는 현장 설비를 직접 구동하는 제어기로, 감시·수집을 총괄하는 시스템이 아니라 관리 대상이 되는 하위 장치다. * Modbus는 제어기 사이에서 쓰이는 통신 프로토콜이다. * Stuxnet은 이란 원심분리기 제어 설비를 노렸던 악성코드의 이름으로, 시스템이 아니라 공격 도구다.

[28번] 다음 보기 중 서비스 이름과 잘 알려진 포트(well-known port) 번호가 잘못된 것은?

1IMAP - 134
2HTTPS - 443
3SMTP - 25
4FTP – 20, 21

▸ IMAP의 잘 알려진 포트 번호는 134가 아니라 143이다. 134번 포트로 표기된 것은 실제 IMAP 서비스와 맞지 않는 잘못된 정보다. * HTTPS가 443번 포트를 사용한다는 설명은 옳다. * SMTP가 25번 포트를 사용한다는 설명도 옳다. * FTP가 20, 21번 포트를 사용한다는 설명도 옳다.

제2회 · 29문항

[1번] 다음 윈도우 운영체제의 기능은?

1Privileged Access Management
2Privileged Account Management
3User Access Control
4User Account Control

▸ 설명은 윈도우의 사용자 계정 컨트롤(User Account Control) 기능이다. 관리자 계정으로 로그인했더라도 평소에는 표준 사용자 권한으로 동작시키다가, 시스템 설정 변경이나 소프트웨어 설치처럼 관리자 권한이 필요한 순간에만 동의 창을 띄워 암호를 요구하는 방식으로 강제적 접근제어를 구현한다. 이름이 비슷한 특권 접근 관리·특권 계정 관리(Privileged Access/Account Management)는 운영체제 내장 기능이 아니라 관리자 계정을 중앙에서 통제·감사하는 솔루션 분야를 가리키며, 윈도우가 쓰는 정식 명칭도 접근(Access)이 아니라 계정(Account) 쪽이다.

[2번] 보기의 취약점 또는 사이버 공격 중 그 원인이 하드웨어에 기반하는 것은?

1Heartbleed
2Shellshock
3Spectre
4WannaCry

▸ Spectre는 CPU의 추측 실행(speculative execution) 기능이라는 하드웨어 설계 특성에서 비롯된 취약점으로, 소프트웨어 패치만으로는 근본 해결이 어렵다. * Heartbleed는 OpenSSL 라이브러리 코드 결함에서 비롯된 소프트웨어 취약점이다. * Shellshock는 Bash 셸의 환경변수 처리 결함에서 비롯된 소프트웨어 취약점이다. * WannaCry는 SMB 취약점을 악용해 퍼지는 랜섬웨어로, 소프트웨어 취약점을 이용한 공격이다.

[3번] 리눅스 설정 파일의 일부이다. 이 설정 파일로 알맞은 것은?

1/etc/services
2/etc/ports
3/etc/protocols
4/etc/resolv.conf

▸ 주어진 내용은 /etc/services 파일의 일부다. 이 파일은 서비스명 포트번호/프로토콜 [별칭] 형식으로 잘 알려진 포트와 서비스 이름의 대응을 담는데, 지문의 systat 11/tcp users, daytime 13/tcp, ftp-data 20/tcp, ftp 21/tcp가 정확히 그 형식이다. * /etc/protocols는 tcp 6, udp 17처럼 프로토콜 이름과 번호를 담고, /etc/resolv.conf는 nameserver 항목 등 DNS 질의 설정을 담는다. * /etc/ports라는 표준 파일은 리눅스에 존재하지 않는다.

[4번] 좀비 프로세스의 존재를 확인하기 위한 명령어들로 올바르게 짝지어진 것은?

1(가), (다)
2(나), (라)
3(가), (나)
4(다), (라)

▸ 좀비 프로세스를 확인할 수 있는 것은 top -b -n 1 | grep zombie와 ps -ef | grep defunct 조합이다. top의 요약 줄에는 “Tasks: … 0 zombie”처럼 zombie라는 단어가 그대로 출력되므로, 배치 모드(-b)로 한 번만(-n 1) 찍어 zombie를 걸러내면 좀비 개수를 확인할 수 있다. 반면 ps의 출력에서 좀비는 명령어 자리에 <defunct>로 표시되고 zombie라는 문자열은 나타나지 않는다. 그래서 ps는 defunct로, top은 zombie로 걸러야 서로 맞는 짝이 된다.

[5번] 홈페이지 회원 계정 및 패스워드 보안 강화를 위해 홈페이지 서버 관리자가 수행할 내용과 가장 거리가 먼 것은?

1패스워드 무작위 대입 공격에 대응하기 위해 서버를 이중화 하였다.
2초기 설정한 암호는 반드시 바꾸도록 설정하였다.
3/etc/shadow 파일에서 사용기간 및 만료일을 설정하였다.
45회 연속 암호 실패 시, 일정시간이 경과한 후 재 로그인 하도록 계정 Lock을 설정하였다.

▸ 서버를 이중화하는 것은 장애에 대비한 가용성 확보 조치로, 패스워드 무작위 대입 공격을 막는 것과는 직접 관련이 없다. 초기 비밀번호 변경 강제, 계정 유효기간·만료일 설정, 로그인 5회 실패 시 계정 잠금은 모두 계정·패스워드 탈취 시도에 직접 대응하는 조치다.

[6번] Null Session 취약점을 갖는 것은?

▸ 윈도우의 IPC$ 공유는 자격증명 없이 연결할 수 있는 널 세션(Null Session) 취약점의 대표적인 통로로, 이를 통해 계정이나 공유 목록이 열거될 수 있다. Admin$, C$, D$는 관리자 인증이 필요한 관리용 숨김 공유로, 널 세션만으로 접근되는 대상은 아니다.

[7번] 리눅스/유닉스 시스템에서 최상위 디렉터리를 올바르게 짝지은 것은?

1㉠ /usr ㉡ /tmp ㉢ /var
2㉠ /usr ㉡ /temp ㉢ /dev
3㉠ /etc ㉡ /temp ㉢ /var
4㉠ /etc ㉡ /tmp ㉢ /dev

▸ 빈칸은 순서대로 /etc, /tmp, /dev다. /etc는 passwd·hosts·services 같은 시스템 환경 설정 파일을 모아 두는 디렉터리이고, /tmp는 프로그램이 실행 중 만들어 내는 임시 파일이 놓이는 곳이라 보통 모든 사용자에게 쓰기 권한이 열려 있다.

/dev는 프린터·터미널·디스크 같은 물리 장치를 파일처럼 다루기 위한 장치 특수 파일을 담는다. /usr는 응용 프로그램과 라이브러리를, /var는 로그·메일처럼 내용이 자주 변하는 데이터를 담아 지문과 맞지 않으며 /temp라는 표준 디렉터리는 존재하지 않는다.

[8번] Black Hacker인 X는 리눅스 서버의 보안 취약점을 이용하여 root 권한을 획득하는데 우연히 성공했다. X는 이후 시스템이 시작될 때마다 자신이 만들어 놓은 해킹 툴을 자동으로 구동시키기 위하여 관련된 파일을 변조하였다.

1/etc/crontab
2/etc/resolv.conf
3/etc/sysconfig/network
4/etc/rc.d/rc.local

▸ 시스템이 시작될 때마다 해킹 툴이 자동 실행되게 하려면 부팅 마지막 단계에서 읽히는 /etc/rc.d/rc.local에 실행 명령을 끼워 넣는 것이 전형적인 수법이다. rc.local은 런레벨별 초기화 스크립트가 모두 끝난 뒤 root 권한으로 한 번 실행되므로, 한 줄만 추가해도 재부팅할 때마다 백도어가 되살아난다. 나머지 위치는 부팅 시 자동 실행과 거리가 있다: * /etc/crontab은 정해진 주기·시각에 작업을 돌리는 파일로, 트리거가 '시스템 시작'이 아니다. * /etc/resolv.conf(DNS 서버 주소)와 /etc/sysconfig/network(호스트명·네트워크 사용 여부)는 네트워크 설정값만 담고 있어 프로그램을 실행시키지 못한다.

[9번] ftp 접근 여부를 검토할 수 있는 로그는?

▸ xferlog는 FTP 서버를 통해 이뤄진 파일 송수신 기록을 남기는 로그로, ftp 접근 여부와 전송 내역을 확인하는 데 쓰인다. wtmp·utmp는 로그인 이력, sulog는 su 명령 사용 이력을 기록하는 로그로 ftp 접근 확인과는 목적이 다르다.

[10번] 트로이목마의 기능과 가장 거리가 먼 것은?

1패스워드 가로채기
2원격 조정
3시스템 파일 파괴
4악성코드 전파

▸ 트로이목마는 정상 프로그램으로 위장해 자리 잡은 뒤 원격 조정, 정보 탈취, 파일 파괴 등을 수행하는 것이 주된 기능이며, 스스로 복제해 다른 시스템으로 퍼지는 전파 기능은 웜(worm)의 특징에 가깝다. 패스워드 가로채기, 원격 조정, 시스템 파일 파괴는 트로이목마가 침투한 시스템 내부에서 수행하는 전형적인 악성 행위다.

[11번] 로그인 실패 시 로그가 저장되는 파일은?

▸ btmp는 로그인 실패 기록을 저장하는 로그 파일로, lastb 명령으로 조회할 수 있다. utmp는 현재 로그인 사용자 정보, wtmp는 로그인·로그아웃 성공 이력, pacct는 실행 명령 이력을 기록해 로그인 실패 확인과는 목적이 다르다.

[12번] 유닉스 또는 리눅스에서 실행 파일 a.out의 소유자가 root, 그룹은 staff이라고 할 때, chmod 4755 a.out 명령을 수행한 후의 a.out의 특성에 대해 올바르게 설명하고 있는 것은?

1그룹이 staff인 모든 사용자에 한해 a.out을 읽고 실행시킬 수 있다.
2root만이 a.out을 읽고 실행시킬 수 있다.
3실행하는 사용자에 관계없이 a.out은 root의 권한으로 실행된다.
4실행하는 사용자에 관계없이 a.out은 staff의 권한으로 실행된다

▸ 4755의 4000은 setuid 비트를 의미하므로, 이 실행파일은 누가 실행하더라도 파일 소유자인 root 권한으로 프로세스가 동작한다. 나머지 755는 소유자에게 읽기·쓰기·실행, 그룹과 기타 사용자에게는 읽기·실행 권한을 부여하는 부분으로, setuid 여부와 무관하게 실행 자체는 root 외 사용자에게도 열려 있다.

[13번] 리눅스 사용자 'test_user'에게 60일 마다 패스워드의 교체를 의무화시키기 위한 보안정책을 반영하기 위한 명령어에 해당하는 것은?

1passwd –x 60 test_user
2useradd –e 60 test_user
3passwd +x 60 test_user
4usermod –f 60 test_user

▸ passwd -x 옵션은 지정한 계정의 패스워드 최대 사용 기간(maximum age)을 일 단위로 설정하는 명령으로, 60을 지정하면 60일마다 교체가 강제된다. useradd -e는 계정 자체의 만료일을 지정하는 옵션이고, usermod -f는 계정 잠금까지의 유예 기간을 지정하는 옵션이라 패스워드 교체 주기 설정과는 용도가 다르다.

[14번] 아래 지문이 설명하는 평가인증 제도는 무엇인가?

▸ 보안기능 요구사항을 FAU·FCO·FCS·FDP·FMT·FIA·FPR·FPT·FRU·FTA·FTP 11개 클래스로 나누고 보증등급을 EAL1~EAL7로 두는 체계는 국제 공통평가기준인 CC(Common Criteria, ISO/IEC 15408)다. CC는 평가대상(TOE)을 정해 보호프로파일(PP)과 보안목표명세서(ST)를 작성하고, 등급이 올라갈수록 설계·시험·형상관리 등 보증요구사항이 강해지는 구조이며 인증 결과가 회원국 간 상호인정된다. 나머지는 등급 체계부터 다르다: * TCSEC(오렌지북)은 미국 국방부 기준으로 D~A1 등급을 쓰고 기밀성 위주다. * ITSEC은 유럽 기준으로 기능성과 보증(E0~E6)을 분리해 평가했고, KTSEC처럼 CC 이전 세대의 국가별 기준들은 11개 기능 클

[15번] 윈도우 레지스트리 중 등록된 응용 프로그램과 확장자 사이의 관계 정보를 담고 있는 곳은?

1HKEY_CLASSES_ROOT
2HKEY_LOCAL_MACHINE SYSTEM
3HKEY_CURRENT_CONFIG
4HKEY_USERS

▸ HKEY_CLASSES_ROOT는 파일 확장자와 이를 처리할 응용 프로그램 간의 연결 정보 및 각 프로그램의 등록 정보를 담고 있는 레지스트리 루트 키다. HKEY_LOCAL_MACHINE\SYSTEM은 시스템 하드웨어·드라이버 설정, HKEY_CURRENT_CONFIG는 현재 하드웨어 프로필, HKEY_USERS는 사용자별 프로필 정보를 담아 확장자 연결 정보와는 성격이 다르다.

[16번] rlogin은 원격 시스템에 접속할 때 사용하는 서비스로 사전에 서버의 특정 파일에 호스트를 등록하여 클라이언트가 패스워드를 입력할 필요 없이 로그인이 가능하게 하는 서비스이다. 다음 중 호스트를 등록하는 파일은?

1/etc/hosts
2/etc/hosts.equiv
3/etc/resolv.conf
4/etc/syslog.conf

▸ /etc/hosts.equiv는 rlogin·rsh 등에서 패스워드 없이 접속을 허용할 신뢰 호스트 목록을 등록해 두는 파일이다. /etc/hosts는 단순 호스트명-IP 매핑, /etc/resolv.conf는 DNS 서버 설정, /etc/syslog.conf는 로그 수집 설정 파일로 rlogin 신뢰 호스트 등록과는 무관하다.

[17번] 다음 지문에서 설명하는 파일시스템으로 옳은 것은?

▸ 초창기 리눅스 전용으로 개발돼 최대 2GB 크기와 256byte 파일명만 지원하고, 접근제어·inode·타임스탬프 수정이 불가능하며 쓸수록 단편화가 심해지는 것은 리눅스의 첫 파일시스템인 EXT다. EXT는 MINIX 파일시스템의 한계를 넘기 위해 만들어졌지만 위 제약 탓에 곧 ext2로 대체됐고, 이후 저널링을 갖춘 ext3·ext4로 발전했다. 보기의 윈도우 계열 파일시스템은 설명과 맞지 않는다: * FAT16·FAT32는 리눅스 전용으로 개발된 것이 아니며 파일명 처리 방식도 8.3 또는 롱 네임이라 지문과 다르다. * NTFS는 ACL 기반 접근제어와 저널링·암호화를 제공하므로 '접근제어가 불가능하다'는 설명과 정반대다.

[18번] 리눅스용 패킷 필터 기반 시스템 접근통제 도구와 거리가 먼 것은?

1iptables
2ipfwadm
3ipchains
4modsecurity

▸ modsecurity는 웹 애플리케이션 방화벽(WAF) 모듈로 HTTP 요청 내용을 검사하는 도구라서, 네트워크 계층에서 패킷 헤더를 거르는 패킷 필터링과는 동작 계층이 다르다. iptables, ipchains, ipfwadm은 모두 리눅스 커널 레벨에서 패킷 단위로 접근을 통제하는 패킷 필터 기반 도구다.

[19번] 한정된 자원을 동시에 이용하려는 여러 프로세스가 자원의 이용을 위해 경쟁을 벌이는 현상을 의미하는 것으로, 취약 프로그램이 생성하는 임시 파일과 같은 이름의 파일을 생성한 후 생성한 임시 파일에 대한 심볼릭 링크를 설정한다.

1Format String
2Heap Spray
3Race Condition
4Buffer Overflow

▸ 한정된 자원을 동시에 쓰려는 프로세스들의 경쟁 상황을 노려, 취약 프로그램이 만들 임시 파일과 같은 이름의 파일을 먼저 만들고 심볼릭 링크를 걸어 두는 공격은 레이스 컨디션(Race Condition)이다. 임시 파일을 확인하는 시점과 사용하는 시점 사이의 짧은 틈(TOCTOU)에 링크가 바꿔치기되면, root 권한으로 도는 프로그램이 공격자가 지정한 파일에 쓰게 되어 권한 상승이 일어난다. 대응은 사용 전 심볼릭 링크 여부 확인과 O_EXCL 같은 배타적 생성이다. 나머지는 메모리 조작 계열이라 임시 파일·심볼릭 링크와 무관하다: * 포맷 스트링과 버퍼 오버플로는 입력값으로 스택·힙 영역을 덮어써 제어 흐름을 바꾸는 공격이다. * 힙 스프레이는 힙에 셸코드를 대량으로 뿌려 실행 확률을 높이는 보조

[20번] 윈도우에서는 사용자 계정을 추가하면 일반 사용자 그룹인 Users 그룹에 자동으로 포함된다. NTFS로 포맷된 볼륨에서는 이 그룹의 구성원이 운영체제 및 설치된 프로그램의 무결성을 손상시킬 수 없도록 새로 설치된 시스템의 기본 보안 설정이 지정된다.

1Users 그룹의 구성원은 워크스테이션을 종료할 수 있고, 서버도 종료할 수 있다.
2Users 그룹의 구성원은 관리자가 설치하거나 배포한 인증된 프로그램을 실행할 수 있다.
3Users 그룹의 구성원은 로컬 그룹을 만들 수는 있지만 자신이 만든 로컬 그룹만 관리할 수 있다.
4Users 그룹의 구성원은 자신의 모든 데이터 파일(%userprofile%) 및 레지스트리에서 자신에 속하는 부분(HKEY_CURRENT_USER)을 완전하게 제어할 수 있다.

▸ Users 그룹 구성원은 워크스테이션은 종료할 수 있지만 서버는 종료할 수 없다. 서버 종료 권한은 Administrators 등 관리 권한 그룹에만 기본 부여되므로 '서버도 종료할 수 있다'는 설명이 잘못됐다. Users 그룹은 계정을 만들면 자동으로 들어가는 일반 사용자 그룹으로, NTFS 볼륨에서 운영체제와 설치된 프로그램의 무결성을 훼손하지 못하도록 제한된 권한만 갖는다. 나머지 설명은 모두 맞다. 관리자가 설치·배포한 인증된 프로그램 실행, 로컬 그룹을 만들되 자신이 만든 그룹만 관리, %userprofile%과 HKEY_CURRENT_USER에 대한 완전한 제어가 허용된다.

[21번] * 이더넷은 네트워크 인터페이스 카드에 설정된 (㉠) 물리 주소를 사용한다.

18Byte, 2Byte, 1Byte
28Byte, 4Byte, 2Byte
36Byte, 4Byte, 2Byte
46Byte, 2Byte, 1Byte

▸ 이더넷 NIC의 MAC 물리 주소는 6Byte, 인터넷 계층의 IPv4 논리 주소는 4Byte, 전송 계층의 포트 주소는 2Byte다. MAC 주소는 48비트로 앞 3바이트가 제조사 식별자(OUI), 뒤 3바이트가 일련번호다. IPv4 주소는 32비트여서 4바이트, 포트 번호는 16비트여서 0~65535 범위의 2바이트로 표현된다. 계층이 올라갈수록 주소 길이가 짧아지는 6 → 4 → 2 흐름으로 묶어 두면 헷갈리지 않는다.

[22번] 분산서비스 거부공격(DDoS)의 구성요소가 아닌 것은?

1마스터(Master)
2포트 미러링(Port Mirroring)
3에이전트(Agent)
4공격자(Attacker)

▸ 포트 미러링은 스위치의 특정 포트로 흐르는 트래픽을 다른 포트로 복사해 모니터링·분석하는 네트워크 관리 기법으로, 공격을 수행하는 구성요소가 아니다. 공격자, 공격 명령을 중계하는 마스터, 실제 트래픽을 발생시키는 에이전트(좀비)는 분산서비스 거부공격을 이루는 전형적인 구성요소다.

[23번] SSL Handshake 프로토콜에 대한 설명으로 옳지 않은 것은?

1Cipher Suite은 공개키 암호 시스템, 대칭키 암호 시스템, 해시 알고리즘 등 3개의 정보로 구성된다.

2SSL Handshake 프로토콜 동작과정을 통해 SSL 클라이언트와 서버가 공유하는 암호 알고리즘들과 키 값들이 생성된다.
3SSL 클라이언트는 통신 상대인 서버의 신원확인을 위해 전자인증서 기반의 인증을 수행한다.
4SSL 클라이언트와 서버의 전자인증서는 대칭키 암호 시스템을 이용한다.

▸ SSL/TLS에서 사용하는 전자인증서는 공개키(비대칭키) 암호 시스템을 기반으로 발급·검증되며, 대칭키 암호 시스템을 이용한다는 설명은 옳지 않다. Cipher Suite가 공개키·대칭키·해시 알고리즘 정보로 구성된다는 점, 핸드셰이크로 공유 암호 알고리즘과 키 값이 생성된다는 점, 서버 인증서로 신원을 확인한다는 점은 SSL Handshake의 일반적 동작과 일치한다.

[24번] VLAN이란 (㉠) 트래픽을 제한하며 불필요한 트래픽을 차단하기 위한 (㉡) LAN이다. 스위치는 허브처럼 한 포트에서 발생한 데이터를 모든 포트에 전달하지 않기 때문에 스위치에 흐르는 데이터를 분석하려면 허브와는 달리 (㉢) 기능을 사용해야 한다.

1㉠ 멀티캐스팅 ㉡ 논리적인 ㉢ Port Mirroring
2㉠ 브로드캐스팅 ㉡ 논리적인 ㉢ Port Mirroring
3㉠ 브로드캐스팅 ㉡ 물리적인 ㉢ Port Filtering
4㉠ 멀티캐스팅 ㉡ 물리적인 ㉢ Port Filtering

▸ VLAN은 브로드캐스팅 트래픽을 제한하기 위해 스위치 포트를 논리적인 LAN으로 나눈 것이고, 스위치 구간의 트래픽을 분석하려면 Port Mirroring이 필요하다. 스위치는 MAC 주소를 보고 목적지 포트로만 프레임을 보내므로 다른 포트에 붙인 장비에서는 패킷이 보이지 않는다. 그래서 감시 대상 포트의 트래픽을 특정 포트로 복사해 주는 미러링(SPAN)을 걸어야 한다. 케이블을 다시 깔지 않고 설정만으로 분할하므로 '물리적인 LAN'은 성립하지 않고, Port Filtering은 특정 포트를 차단·허용하는 접근통제 기능이라 트래픽 분석 용도가 아니다.

[25번] C:\>ping 127.0.0.1

127.0.0.1의 응답 바이트=32 시간 <1ms TTL=128
127.0.0.1의 응답 바이트=32 시간 <1ms TTL=128
127.0.0.1에 대한 Ping 통계
1Echo Reply 패킷 크기
2Reply 패킷을 받기까지의 시간
3라우팅 정보가 잘못되어 발생하는 패킷 무한 반복을 제어하기 위한 값
4손실된 패킷의 수

▸ ping 출력의 TTL=128은 패킷이 거칠 수 있는 라우터 수의 한계값으로, 라우팅 정보 오류로 패킷이 무한히 순환하는 것을 막기 위한 값이다. 패킷이 라우터를 하나 지날 때마다 TTL이 1씩 줄고 0이 되면 폐기되며 ICMP Time Exceeded가 돌아온다. tracert가 경로를 알아내는 원리도 이 값을 1부터 늘려 가며 보내는 것이다. 같은 출력의 다른 항목과 혼동하면 안 된다. 바이트=32는 패킷 크기, 시간 <1ms는 응답까지 걸린 왕복 시간, 손실 = 0은 손실된 패킷 수로 각각 따로 표시되고 있다.

[26번] TCP 플래그 값을 모두 off(비활성화)한 패킷들을 이용하여 스캔하는 기법은?

1FIN 스캔
2TCP SYN 스캔
3Null 스캔
4XMAS 스캔

▸ TCP 플래그를 모두 비활성화(off)한 패킷을 보내 포트 상태를 확인하는 기법은 Null 스캔이다. FIN 스캔은 FIN 플래그만, XMAS 스캔은 FIN·PSH·URG 플래그를 설정해 보내며, SYN 스캔은 SYN 플래그를 설정한 패킷으로 연결을 시도해 플래그 구성이 서로 다르다.

[27번] 웹서버 OS의 TCP 스택(Stack) 자원을 소모하는 특징을 갖는 웹서버 자원 소모 공격으로 사용될 수 있으며, 그 대응방법으로 Anti-DDoS 장비에서 소스 IP별로 PPS 임계치를 설정하거나 패킷 헤더 검사를 통해 정상적인 옵션 필드값을 갖지 않는 비정상 패킷을 차단할 수 있다.

1UDP Flooding
2SYN Flooding
3GET Flooding

4ICMP Flooding

▸ 웹서버 OS의 TCP 스택 자원을 소모시키고, 소스 IP별 PPS 임계치와 패킷 헤더의 옵션 필드 검사로 막는 공격은 SYN Flooding이다. 3-way 핸드셰이크에서 SYN만 보내고 ACK를 주지 않아 백로그 큐를 연결 대기(SYN_RECEIVED) 상태로 채우므로, 응용 계층이 아니라 TCP 연결 테이블이 먼저 고갈된다. 정상 클라이언트의 SYN에는 MSS·SACK·윈도 스케일 같은 옵션이 붙지만 공격 도구가 만든 패킷은 옵션이 비어 있어 헤더 검사로 걸러낼 수 있다. 나머지는 소모 대상이 다르다: * UDP·ICMP Flooding은 대량 트래픽으로 회선 대역폭을 채우는 공격이다. * GET Flooding은 정상적으로 연결을 맺은 뒤 HTTP 요청을 반복해 웹 애플리케이션과 DB를 소모시

[28번] 수동적 공격과 가장 거리가 먼 것은?

1도청
2메세지 수정
3감시
4메시지 내용 절취

▸ 메시지 수정(변조)은 전송 중인 데이터를 가로채 내용을 바꾸는 행위로, 데이터나 시스템에 직접 개입하는 능동적 공격에 해당한다. 도청, 감시, 메시지 내용 절취는 통신 내용을 몰래 엿보기만 할 뿐 데이터나 시스템 상태를 바꾸지 않는 수동적 공격의 전형적인 예다.

[29번] 3계층 터널링 프로토콜은?

1PPTP VPN
2L2TP VPN
3IPSec VPN
4SSL VPN

▸ IPSec VPN은 네트워크 계층(3계층)에서 IP 패킷 단위로 터널링과 암호화를 수행하는 프로토콜이다. PPTP VPN과 L2TP VPN은 데이터링크 계층(2계층)에서 동작하는 터널링 프로토콜이고, SSL VPN은 전송·응용 계층 수준에서 동작해 </partial_content> <instructions> Document is too large (72873 tokens). Only showing first 10000 tokens. For complete analysis, run `gsk summarize "https://www.moducbt.com/exam/pdf/28437" --question "<your specific question>"` — it analyzes the full documen

2020년 정보보안기사 필기

제1회 · 28문항

[1번] 리눅스 서버에서 xinetd 데몬을 이용한 접근 제어 시 지정된 원격지 IP 주소 대역에 대해 접근을 허락할 때 xinetd.conf 파일에서 사용하는 옵션은?

1enable
2allow
3enable_access
4only_from

▸ xinetd.conf에서 특정 원격지 IP 주소 대역의 접근을 허용할 때 사용하는 옵션은 only_from이다. 반대로 특정 대역의 접근을 차단할 때는 no_access를 사용하고, allow나 enable_access는 xinetd가 지원하지 않는 이름이다. enable(enabled)은 접근 대역이 아니라 서비스의 활성화 여부를 지정하는 항목이다.

[2번] i-node가 가지고 있지 않은 정보는?

1파일 이름
2파일의 링크 수
3파일 크기
4마지막으로 수정된 시간

▸ 파일 이름은 i-node가 아니라 디렉터리 엔트리에 저장되며, 디렉터리는 파일 이름과 그에 대응하는 i-node 번호를 연결하는 역할만 한다. i-node에는 파일의 링크 수, 파일 크기, 최종 수정 시간처럼 파일의 속성 정보와 데이터 블록 위치 정보가 저장된다.

[3번] /etc/shadow 파일의 일부분이다. 이를 통해 알 수 있는 내용이 아닌 것은?

1sec_admin 사용자는 비밀번호 변경 후 최대 30일간 이를 사용할 수 있다.
2sys_admin 사용자의 비밀번호는 아직 부여되지 않은 상태이며, 계정은 막혀 있다.
3prog_user 사용자는 비밀번호 유효기간이 만료되기 7일 전부터 비밀번호 만료에 관한 경고메시지를 받는다.
4prog_user 사용자는 비밀번호를 변경한 후 3일 이내에 자신의 비밀번호를 변경할 수 있다.

▸ 옳지 않은 설명은 prog_user가 비밀번호 변경 후 3일 이내에 다시 변경할 수 있다는 내용이다. /etc/shadow의 필드는 계정:암호:최종변경일:최소변경일수:최대사용일수:경고일수:비활성일수:만료일 순이다. prog_user 행에서 최종변경일 15711 바로 다음 값인 3이 최소변경일수이므로, 마지막 변경일로부터 3일이 지나야 비밀번호를 다시 바꿀 수 있고 그 전에는 변경이 거부된다. * sec_admin 행은 최종변경일 15860 뒤가 0:30:10 이라 최대사용일수가 30이다. 따라서 변경 후 최대 30일간 그 비밀번호를 쓸 수 있다. * sys_admin의 암호 필드가 !! 이므로 비밀번호가 부여되지 않아 로그인이 잠긴 상태다. * prog_user의 경고일수가 7이므로 만료 7일 전부

[4번] 파일 시스템이란 운영체제가 파일을 시스템의 디스크 상에 구성하는 방식을 말한다. 운영체제는 시스템의 디스크 파티션 상에 파일들을 일정한 규칙을 가지고 저장하는데 파일 시스템은 이러한 규칙들의 방식을 제시하는 역할을 한다. 다음 중 윈도우 운영체제에서 사용하는 파일 시스템이 아닌 것은?

▸ EXT3는 리눅스 계열 운영체제에서 사용하는 파일 시스템으로, 윈도우 운영체제가 사용하는 파일 시스템이 아니다. FAT16, FAT32, NTFS는 모두 윈도우 운영체제에서 지원하는 파일 시스템이다.

[5번] 좀비 프로세스를 확인하고 중지시키기 위한 UNIX 명령어에 대한 설명으로 올바른 것은?

1ps 명령어 실행 후 STAT 값이 Z로 표시되는 프로세스가 좀비 프로세스이며, kill 명령어 사용
2ss 명령어 실행 후 STAT 값이 B로 표시되는 프로세스가 좀비 프로세스이며, kill 명령어 사용
3ps 명령어 실행 후 STAT 값이 B로 표시되는 프로세스가 좀비 프로세스이며, halt 명령어 사용
4zs 명령어 실행 후 STAT 값이 Z로 표시되는 프로세스가 좀비 프로세스이며, halt 명령어 사용

▸ ps 명령어로 프로세스 상태를 확인했을 때 STAT 값이 Z(Zombie)로 표시되는 프로세스가 좀비 프로세스이며, 이를 정리할 때는 kill 명령어를 사용한다. ss나 zs 같은 명령어, B 상태 표기, halt 명령어는 좀비 프로세스 확인·종료와 관련이 없다.

[6번] 매일 오전 8시 40분에 /usr/logreport.sh 스크립트가 실행되도록 하기 위해 contab에 넣을 설정 내용으로서 적절한 것은?

1* 40 08 * * -exec {/usr/logreport.sh}
240 08 * * * /usr/logreport.sh
3* * * 08 40 /usr/logreport.sh
4* * * 08 40 –exec {/usr/logreport.sh}

▸ crontab의 각 필드는 분·시·일·월·요일 순서로 구성되므로, 매일 오전 8시 40분에 실행하려면 40 08 * * * 뒤에 실행할 스크립트 경로를 적어야 한다. 일·월 자리에 08과 40을 넣거나 -exec 옵션을 붙이는 방식은 crontab 문법에 맞지 않는다.

[7번] 다음 지문에서 설명하는 유닉스 시스템 관리자용 명령어는?

▸ 지문이 설명하는 명령어는 df다. df는 마운트된 파일시스템의 슈퍼블록 정보를 읽어 전체·사용·사용 가능한 디스크 블록 수와 여유 i-node 수를 보여 준다. 지문의 "사용 가능한 디스크 블록과 free node 수를 알려 줌"이 그대로 이 명령의 기능이다. * ps는 현재 실행 중인 프로세스 목록과 상태를 출력한다. * file은 지정한 파일의 종류·형식을 판별해 알려 준다. * find는 디렉터리 트리에서 조건에 맞는 파일을 검색한다.

[8번] 다음 중 버퍼 오버플로우(Buffer Overflow)에 대한 대책으로 옳지 않은 것은?

1경계 검사를 하는 컴파일러 및 링크를 사용한다.
2경계를 검사하는 함수를 사용한다.
3운영체제 커널 패치를 실시한다.
4최대 권한으로 프로그램을 실행한다.

▸ 버퍼 오버플로우 대책은 프로그램이 필요한 최소 권한으로만 실행되도록 제한해 공격 성공 시 피해 범위를 줄이는 것이며, 최대 권한으로 실행하는 것은 대책이 아니라 위험을 키우는 방식이다. 경계 검사를 지원하는 컴파일러·링크 사용, 경계 검사 함수 사용, 운영체제 커널 패치는 모두 정당한 대응책이다.

[9번] 하이퍼바이저에 대한 내용으로 옳지 않은 것은?

1가상머신과 하드웨어 사이에 위치하여 다수의 가상머신들이 각각의 운영체제가 구동될 수 있도록 논리적으로 독립된 가상머신 환경을 제공한다.
2주 기능은 CPU, 메모리 등 하드웨어 자원을 각 가상머신에 논리적으로 분할 할당・스케줄링하는 것이다.
3하이퍼바이저는 bare-metal 타입, hosted 타입으로 나누어지며, bare-metal 타입은 하드웨어 상에서 동작하는 것이 아니라 호스트 운영체제 위에서 동작한다.
4hosted 타입은 VMware Workstation, Parallels Desktop 등이 대표적이다.

▸ bare-metal 타입 하이퍼바이저는 호스트 운영체제 없이 하드웨어 위에서 직접 동작하며, 호스트 운영체제 위에서 동작하는 것은 hosted 타입이다. 가상머신과 하드웨어 사이에서 논리적으로 독립된 가상 환경을 제공하는 점, CPU·메모리를 각 가상머신에 분할·스케줄링하는 점, VMware Workstation이나 Parallels Desktop이 hosted 타입의 대표적 사례라는 점은 모두 옳은 설명이다.

[10번] 다음 중 리눅스에서 Process ID(PID) 1번을 가지고 있는 프로세스는 무엇인가?

1init
2부트로더
3OS 커널
4BIOS

▸ 리눅스에서 부팅 후 커널이 가장 먼저 실행하는 사용자 프로세스가 init이며, PID 1번을 부여받아 이후 모든 프로세스의 최상위 조상 역할을 한다. 최근 배포판에서는 systemd가 그 자리를 대신한다. 부트로더, OS 커널, BIOS는 프로세스로 취급되지 않는 부팅 이전 또는 커널 자체의 구성 요소다.

[11번] 다음 지문이 설명하는 것은?

1Kerberos
2OAuth
3EAP
4RADIUS

▸ 지문이 설명하는 것은 OAuth다. OAuth는 사용자의 비밀번호를 넘기지 않고 접근 토큰(Access Token)으로 제3의 애플리케이션에 권한을 위임하는 공개 API 기반 표준이다. 트위터·페이스북 계정으로 다른 앱이나 다른 기기에서 사용자 정보에 접근하게 해 준다는 지문 설명이 정확히 이 방식이다. * Kerberos는 KDC가 발급한 티켓과 대칭키로 인증하는 폐쇄망용 프로토콜로 공개 API 방식이 아니다. * EAP는 PPP·무선랜 구간에서 여러 인증 방식을 실어 나르는 인증 프레임워크다. * RADIUS는 원격 접속 사용자를 중앙에서 인증·인가·과금하는 서버 프로토콜이다.

[12번] 윈도우 NTFS에서 모든 파일들과 디렉터리에 대한 정보를 포함하고 있는 것은?

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

▸ NTFS에서 모든 파일과 디렉터리에 대한 정보를 담고 있는 것은 MFT(Master File Table)이다. FAT는 FAT 파일 시스템에서 쓰이는 별개의 구조이고, $AttrDef와 $LogFile은 MFT를 보조하는 메타파일로 전체 정보를 총괄하는 역할은 아니다.

[13번] 리눅스 시스템의 /etc/logrotate/conf 파일에서 로그순환 설정을 하려고 한다. 최소 6개월분의 로그를 저장하기 위해 빈칸 ㉠에 들어갈 용어로 적절한 것은?

1save
2rotate
3cycle
4minimum

▸ 빈칸에 들어갈 용어는 rotate다. 설정의 monthly 는 로그를 한 달에 한 번 순환시키고, rotate 6은 순환된 로그 파일을 6개까지 보관한다는 뜻이다. 따라서 월 1회 순환 × 보관 6개 = 6개월분의 로그가 남는다. logrotate 설정에서 보관 개수를 지정하는 지시어는 rotate 뿐이며 save·cycle·minimum 은 인식되지 않는다. 함께 쓰인 create는 순환 직후 빈 로그

파일을 새로 만들고, compress는 순환된 파일을 압축해 보관한다.

[14번] FTP 접속기록을 확인할 수 있는 파일은?

1xferlog
2ftplog
3error log
4pacct

▸ 유닉스 계열 시스템에서 FTP 접속 기록을 확인할 수 있는 파일은 xferlog이다. ftplog나 error log는 FTP 접속기록을 남기는 파일이 아니며, pacct는 프로세스 계정(accounting) 로그로 FTP 접속기록과는 다르다.

[15번] 다음 지문에서 설명하고 있는 것은?

1S/Key 인증
2RADIUS
3Challenge Response
4Kerberos

▸ 지문이 설명하는 것은 RADIUS다. RADIUS는 리빙스턴사가 개발해 표준화된 AAA(인증·인가·과금) 프로토콜로, ISP의 전화 접속 같은 원격 접속 사용자를 중앙 서버에서 인증한다. 접속장비가 클라이언트가 되고 계정은 중앙집중 관리되며 인증 방식으로 PAP·CHAP를 지원한다는 점이 지문과 그대로 맞는다. * S/Key 인증은 해시를 반복 적용해 만든 일회용 비밀번호 방식이지 원격 접속 인증 서버가 아니다. * Challenge Response는 난수를 주고받아 검증하는 인증 기법의 총칭으로 특정 서버·제품을 가리키지 않는다. * Kerberos는 KDC가 티켓을 발급하는 대칭키 기반 인증 프로토콜로 개발 주체와 용도가 다르다.

[16번] 다음은 윈도우 부팅 순서이다. 올바르게 나열된 것은?

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

▸ 올바른 순서는 POST → CMOS → MBR → NTLDR → NTDETECT.COM → NTOSKRNL.EXE, 즉 나-바-가-다-라-마 이다. 전원이 들어오면 먼저 POST가 하드웨어 이상 유무를 점검하고, 이어서 CMOS에 저장된 사용자 설정(부팅 순서 등)을 읽어 적용한다. 그 다음 지정된 부팅 매체의 MBR을 읽어 기본 파일시스템 정보를 얻는다. 이후 부팅 파티션의 NTLDR이 간단한 파일시스템을 구동해 BOOT.INI를 읽고, NTDETECT.COM이 설치된 하드웨어를 검사한 뒤, 마지막으로 NTOSKRNL.EXE가 HAL.dll을 로드하면서 커널이 올라온다.

[17번] Cyber Kill Chain의 단계 중 빈칸 ⓐ, ⓑ에 들어갈 절차로 알맞은 것은?

1ⓐ 악성코드 제작(Develop) ⓑ 명령 및 제어(Command & Control)
2ⓐ 명령 및 제어(Command & Control) ⓑ 전달(Delivery)
3ⓐ 전달(Delivery) ⓑ 명령 및 제어(Command & Control)
4ⓐ 전달(Delivery) ⓑ 악성코드 제작(Develop)

▸ 빈칸에 들어갈 절차는 ⓐ 전달(Delivery), ⓑ 명령 및 제어(Command & Control)다. 사이버 킬 체인 7단계는 정찰 → 무기화 → 전달 → 취약점 악용 → 설치 → 명령 및 제어 → 목표 실행 순이다. 무기화로 만든 악성코드를 메일·웹 등으로 표적에 보내는 단계가 전달이고, 설치된 악성코드가 공격자 서버와 통신 채널을 열어 원격 조종을 받는 단계가 명령 및 제어다. 악성코드 제작은 별도의 단계가 아니라 이미 무기화에 포함되며, 명령 및 제어는 설치 이후에 오는 단계이므로 세 번째 자리에는 올 수 없다.

[18번] 다음 지문이 설명하는 것은?

1CryptoCurrency Hijacking
2CryptoCurrency Jacking
3Currency Hijacking
4CryptoJacking

▸ 지문이 설명하는 공격은 크립토재킹(CryptoJacking)이다. 감염된 시스템의 CPU·GPU 자원을 몰래 빼앗아 가상화폐를 채굴하고 그 결과를 공격자에게 보내는 공격으로, Cryptocurrency와 Hijacking을 합쳐 만든 용어다. 피해 시스템에서는

자원 점유율 급등과 성능 저하, 발열·전력 소모 증가가 나타난다. 나머지 보기는 이 용어를 풀어 쓰거나 일부만 떼어낸 변형 표기일 뿐, 보안 분야에서 통용되는 정식 명칭은 크립토재킹 하나다.

[19번] 실행 레벨은 0부터 6까지 있는데 다음 지문의 빈칸 ㉠, ㉡, ㉢에 해당되는 실행 레벨로 알맞게 짝지어진 것은?

1㉠ 실행레벨 0 ㉡ 실행레벨 5 ㉢ 실행레벨 4
2㉠ 실행레벨 1 ㉡ 실행레벨 6 ㉢ 실행레벨 3
3㉠ 실행레벨 0 ㉡ 실행레벨 5 ㉢ 실행레벨 3
4㉠ 실행레벨 1 ㉡ 실행레벨 6 ㉢ 실행레벨 2

▸ 단일 사용자 모드는 실행레벨 1, 재부팅은 실행레벨 6, 전체 서비스를 지원하는 다중 사용자 모드는 실행레벨 3이다. 실행레벨 1은 네트워크와 다중 사용자 서비스를 올리지 않고 관리자만 접속시키는 복구·점검용 모드이고, 6은 시스템을 정지한 뒤 다시 올리는 재시작 전용 레벨이다. 나머지 레벨은 지문의 세 항목과 맞지 않는다. * 0: 시스템 종료(halt) * 2: 네트워크 파일 공유(NFS) 없이 동작하는 다중 사용자 모드 * 5: X 윈도우 기반 그래픽 로그인 모드

[20번] 유닉스 또는 리눅스 시스템에서 SetUID와 SetGID가 설정된 모든 파일을 찾으려고 한다. 명령어가 바르게 기술된 것은?

1find / -type f \(-perm –1000 –o –perm -2000 \) -print
2find / -type f \(-perm -2000 –o –perm -4000 \) -print
3find / -type f \(-perm -100 –o –perm -200 \) -print
4find / -type f \(-perm -200 –o –perm -400 \) -print

▸ setuid 비트는 4000, setgid 비트는 2000으로 표현되므로, 두 권한이 설정된 파일을 모두 찾으려면 -perm -4000과 -perm -2000 조건을 -o(또는)로 묶어 find로 검색해야 한다. -1000은 sticky bit이고, -100이나 -200, -400은 소유자의 실행·쓰기·읽기 권한 비트이므로 setuid·setgid 탐색 조건이 될 수 없다.

[21번] Smurf 공격을 방지하기 위하여 라우터에서 차단되어야 하는 기능은?

1Directed Broadcast
2Ingress Filtering
3HTTP GET Flooding
4ICMP Ping Request

▸ Smurf 공격은 브로드캐스트 주소로 대량의 ICMP 요청을 보내 다수의 호스트가 동시에 응답하도록 유도하는 방식이므로, 라우터에서 Directed Broadcast를 차단하면 공격 트래픽의 증폭을 막을 수 있다. Ingress Filtering은 출발지 IP 위조 트래픽 차단에 쓰이고, ICMP Ping Request 자체나 HTTP GET Flooding 차단은 다른 유형의 공격 대응에 쓰이는 개념이라는 점에서 구분된다.

[22번] IPv4의 IP 주소 고갈 및 라우팅 테이블 대형화에 대한 해소책으로 기존의 클래스 기반 IP 주소 체계를 벗어나 서브넷 마스크 정보를 IP 주소와 함께 라우팅 정보로 사용할 수 있게 만든 IP 주소 지정 방식은?

1FLSM
2CIDR
3VLSM
4Static Routing

▸ 클래스 기반 주소 체계에서 벗어나 서브넷 마스크 정보를 IP 주소와 함께 라우팅 정보로 사용하는 방식이 CIDR(Classless Inter-Domain Routing)이다. VLSM은 하나의 네트워크 안에서 가변 길이로 서브넷을 나누는 기법이고, FLSM은 고정 길이로 나누는 기법이라는 점에서 CIDR과 구분된다.

[23번] 다음 지문에서 설명하는 네트워크 기술은?

1Bypass
2LLCF
3Failover
4DPDK

▸ 이중화된 장비의 링크 상태를 감시하다가 장애가 나면 예비 경로로 절체하는 기능은 Failover다. 지문은 링크 상태를 모니터링해 링크가 다운되면 경로정보를 변경한다고 했다. 평소에는 주 방화벽으로 트래픽을 보내다가 장애를 감지하

면 대기 장비 쪽으로 경로를 바꿔 서비스 중단을 막는 가용성 확보 기술이다. 나머지 용어는 장애 시 경로 자체를 전환하는 기능이 아니다. * Bypass: 보안장비가 죽었을 때 트래픽을 장비를 거치지 않고 그대로 통과시키는 회로 * LLCF: 한쪽 구간의 링크 장애를 반대편 포트까지 강제로 내려 상대 장비가 장애를 인지하게 하는 전달 기능 * DPDK: 커널을 우회해 패킷 처리 성능을 높이는 고속 패킷 처리 라이브러리

[24번] 스니핑 할 수 있는 공격방법과 거리가 먼 것은?

1ARP Redirect
2Switch Jamming
3ARP Spoofing
4IP Spoofing

▸ IP Spoofing은 출발지 IP 주소를 위조해 신원을 속이는 공격 기법으로, 스위치 환경에서 트래픽을 가로채는 스니핑 기법과는 직접적인 관련이 없다. ARP Redirect, Switch Jamming, ARP Spoofing은 모두 스위치의 트래픽 분리 기능을 무력화해 스니핑을 가능하게 하는 대표적 기법이다.

[25번] 다음 지문에서 설명하고 있는 공격 특징 및 대응방안과 관련성이 가장 높은 것은?

1UDP Flooding
2SYN Flooding
3ICMP Flooding
4GET Flooding

▸ OS의 TCP 스택 자원을 고갈시키는 공격은 SYN Flooding이다. 연결 요청(SYN)만 대량으로 보내고 세 단계 핸드셰이크를 끝내지 않으면 서버는 half-open 연결을 백로그 큐에 쌓아 두게 되고, 큐가 차면 정상 사용자의 접속까지 거부된다. 지문의 대응방안도 TCP 계층 대응이다. 소스 IP별 PPS 임계치로 과다한 연결 요청을 끊고, TCP 헤더의 옵션 필드(MSS·윈도우 스케일 등)가 정상 클라이언트와 다른 조작 패킷을 헤더 검사로 걸러낸다. UDP·ICMP Flooding은 TCP 스택이 아니라 회선 대역폭을 소모하는 공격이고, GET Flooding은 연결을 정상적으로 맺은 뒤 HTTP 요청을 반복하는 응용계층 공격이라 스택 고갈과 성격이 다르다.

[26번] 컴퓨터 및 네트워크에서 서비스가 더 이상 진행되지 못하도록 하는 경우로써 < 보기 > 에서 설명하고 있는 공격 방법으로 가장 옳은 것은?

1스머프(smurf) 공격
2중간자(man-in-the-middle) 공격
3포맷 스트링(format string) 공격
4포맷 스트링(format string) 공격

▸ 이 문항은 원본 출처에서 문제 또는 보기 내용이 정확하지 않다고 밝힌 문항입니다. 지문이 원래 시험 문제와 다를 수 있으니 개념 확인용으로만 활용하시기 바랍니다. 출발지 주소를 피해자 IP로 위장한 ICMP 요청을 뿌려 다수의 응답이 피해자에게 몰리게 하는 공격은 스머프(smurf) 공격이다. 지문처럼 발신주소를 목적지 IP로 위장(spoofing)하면 살아 있는 노드들이 보내는 ICMP 에코 응답이 전부 피해 시스템으로 쏟아져 증폭된 트래픽으로 과부하가 발생한다. 나머지 공격은 ICMP 응답을 증폭시키는 방식이 아니다. * 중간자 공격: 통신 경로 사이에 끼어들어 내용을 도청·변조하는 공격 * 포맷 스트링 공격: printf 계열 함수의 서식 문자열 취약점으로 메모리를 읽거나 덮어쓰는 공격

[27번] 다음 네트워크 공격은 무엇인가?

1Ping of death
2LAND attack
3Teardrop
4Smurf attack

▸ 단편 오프셋(offset)을 겹치거나 비도록 조작해 재조립을 방해하는 공격은 Teardrop이다. IP는 MTU보다 큰 패킷을 잘라 보내고 수신 측이 오프셋 값을 보고 원래 순서대로 이어 붙이는데, 오프셋이 중첩되거나 비어 있으면 재조립 루틴이 비정상 동작해 자원을 낭비하거나 시스템이 멈춘다. 나머지는 단편 오프셋 조작이 아닌 다른 방식이다. * Ping of death: 허용 크기를 넘는 거대한 ICMP 패킷을 보내 처리 과정에서 오류를 일으키는 공격 * LAND attack: 출발지와 목적지 주소를 같게 만들어 시스템이 자기 자신과 통신하게 하는 공격 * Smurf attack: 위장한 ICMP 요청을 뿌려 응답을 피해자에게 집중시키는 공격

[28번] 다음 보기의 내용은 어떤 공격에 대한 특징인가?

1Land Attack
2Bonk
3Boink
4Teardrop

▸ 정상적인 순서로 보내다가 중간중간에만 시퀀스 번호를 어긋나게 보내는 공격은 Boink다. 지문은 1번·100번·200번까지 규칙적으로 보내다가 20번째부터 2002, 100, 다시 2002처럼 일부 패킷의 순서 정보만 틀어 ⟨/partial_content> <instructions> Document is too large (72895 tokens). Only showing first 10000 tokens. For complete analysis, run `gsk summarize "https://www.moducbt.com/exam/pdf/28436" --question "<your specific question>"` — it analyzes the full document (PDFs, aca

제2회 · 26문항

[1번] 리눅스 운영체제 특수 권한에 대한 설명으로 틀린 것은?

1SetGID가 부여된 파일은 소유 그룹의 실행 권한이 x에서 s로 변경된다.
2SetUID가 부여된 파일은 소유자의 실행 권한이 x에서 s로 변경된다.
3Sticky bit이 부여된 디렉터리는 기타 사용자의 실행 권한이 x에서 s로 변경된다.
4Sticky bit는 /tmp와 같은 777 권한의 공용 디렉터리에서 파일 삭제 통제에 이용된다.

▸ Sticky bit가 부여된 디렉터리는 기타 사용자의 실행 권한이 x에서 t로 표시되며, s로 표시된다는 설명은 틀렸다. SetUID는 소유자 실행 권한이 x에서 s로, SetGID는 소유 그룹 실행 권한이 x에서 s로 바뀌지만, Sticky bit는 별도로 t(또는 실행 권한이 없을 때 T)로 표시된다. /tmp처럼 777 권한의 공용 디렉터리에서 다른 사용자가 만든 파일을 함부로 삭제하지 못하도록 통제하는 용도라는 설명은 옳다.

[2번] 악성코드 유형은 무엇인가?

1루트킷
2트로이 목마
3스파이웨어
4파일리스

▸ 디스크에 실행 파일을 남기지 않고 메모리에서만 동작하는 파일리스(Fileless) 악성코드에 대한 설명이다. 하드디스크에 파일을 설치하지 않고 시스템 메모리에 곧바로 로드되며, OS에 내장된 PowerShell·WMI 같은 정상 도구를 빌려 실행되므로 백신이 정상 실행으로 오인한다. E-Mail 첨부파일·PDF·JPEG 문서에 삽입되어 유포된다는 점도 실행 파일 형태로 배포되지 않는 이 유형의 특징이다. * 루트킷 — 시스템 파일·커널 모듈을 교체해 침입 흔적을 숨기는 도구 모음으로 디스크에 실체가 남는다 * 트로이 목마 — 정상 프로그램으로 위장해 디스크에 설치되는 실행 파일이다 * 스파이웨어 — 몰래 설치되어 사용자 정보를 수집·전송하는 프로그램이다

[3번] 최근 기관이나 단체를 사칭하는 것부터 이력서나 발주서 등을 사칭해 무의식 중에 열어보도록 하는 방법을 사용하여 이메일에 첨부파일이나 URL을 삽입한 후, 이를 클릭해 악성코드를 실행하도록 하는 등의 공격이 성행하고 있다. 이러한 공격의 차단을 목적으로 하는 가장 적합한 솔루션은?

1WAF(Web Application Firewall)
2CDR(Content Disarm & Reconstruction)
3TMS(Threat Management System)
4DLP(Data Loss Prevention)

▸ CDR(Content Disarm & Reconstruction)이 가장 적합한 솔루션이다. CDR은 첨부파일에서 매크로·스크립트 등 잠재적으로 악성일 수 있는 활성 콘텐츠를 제거하고 문서를 재구성해 전달하는 기술로, 사칭 이메일에 숨겨진 악성코드 실행을 원천적으로 차단하는 데 특화되어 있다. WAF는 웹 애플리케이션 공격 방어, TMS·DLP는 위협 통합관리·정보유출 방지에 초점이 맞춰져 있어 이메일 첨부파일 자체의 무해화 목적과는 거리가 있다.

[4번] 다음 지문이 설명하는 파일 시스템은?

1exFAT(Extended File Allocation Table)
2ext4(extended file system)

3HFS(Hierarchical File System)
4ReFS(Resilient File System)

▸ 마이크로소프트가 플래시 저장매체를 겨냥해 만든 exFAT(Extended File Allocation Table)에 대한 설명이다. 윈도우 CE 6.0에서 처음 도입되어 윈도우 비스타·7·서버 2008로 확대되었고, FAT32의 4GB 파일 크기 한계와 디렉터리 엔트리 제약을 풀면서도 NTFS보다 자료구조 오버헤드가 작다. 나머지는 지문의 개발사·도입 시점과 맞지 않는다. * ext4 — 리눅스의 저널링 파일 시스템으로 마이크로소프트 제품이 아니다 * HFS — 애플 매킨토시의 계층적 파일 시스템이다 * ReFS — 마이크로소프트가 만들었으나 윈도우 서버 2012에서 NTFS를 대체할 목적으로 나온 것이라 윈도우 CE·비스타 도입이라는 설명과 어긋난다

[5번] 다음 중 윈도우 운영체제에서 시스템에 대한 비인가 변경을 통제하기 위한 기술에 해당하는 것은?

1커널 모드
2윈도우 디펜더
3보안 업데이트
4사용자 계정 컨트롤

▸ 사용자 계정 컨트롤(UAC)이 시스템에 대한 비인가 변경을 통제하는 기술이다. UAC는 관리자 권한이 필요한 작업이 수행될 때 사용자에게 동의나 자격 증명 입력을 요구해 악성코드나 사용자의 실수로 인한 무단 시스템 변경을 막는다. 커널 모드는 운영체제 실행 권한 수준, 윈도우 디펜더는 악성코드 탐지, 보안 업데이트는 취약점 패치 기능으로 비인가 변경 통제 자체를 목적으로 하는 기능은 아니다.

[6번] OTP(One-Time Password) 사용자 인증방식에 대한 설명으로 틀린 것은?

1OTP는 해시함수 등 암호학적 알고리즘에 의해 패스워드를 생성하기 때문에 다음 생성될 암호를 예측하는 것은 계산상 불가능하다.
2OTP에 의해 생성된 패스워드는 재사용이 불가능한 특징을 보인다.
3OTP 단말기와 서버는 사전에 공유한 비밀값을 암호학적 알고리즘에 적용하여 패스워드를 생성한다.
4시간 동기화 방식을 사용하는 OTP 시스템에서 OTP 서버와 단말기에 적용되는 시간은 정확한 패스워드 생성을 위해 시간 오차를 전혀 허용하지 않는다.

▸ 시간 동기화 방식 OTP가 시간 오차를 전혀 허용하지 않는다는 설명은 틀렸다. 실제 시간 동기화 방식 OTP 시스템은 서버와 단말 간 시계 오차를 감안해 일정한 허용 오차 범위(윈도)를 두고 그 범위 내의 패스워드를 유효한 것으로 인정한다. 해시함수 기반 예측 불가능성, 생성된 패스워드의 재사용 불가, 사전에 공유한 비밀값을 이용한 패스워드 생성이라는 나머지 설명은 옳다.

[7번] 다음 지문에서 설명하는 파일은?

1mediarun.msc
2activerun.inf
3autorun.inf
4execute.inf

▸ 이동식 미디어의 루트에 놓여 자동 실행을 지시하는 autorun.inf다. 윈도우는 CD/DVD나 USB가 연결되면 루트 디렉터리의 autorun.inf를 읽어 그 안에 지정된 프로그램을 자동 실행하는데, 이 동작이 그대로 이동식 매체를 통한 악성코드 전파 통로가 된다. 그래서 자동실행 기능을 끄고 매체 연결 시 백신 검사를 강제하는 것이 기본 대응이다. 보기의 나머지 이름들은 윈도우가 실제로 참조하는 자동실행 설정 파일이 아니다.

[8번] secure.txt 파일의 소유자에게는 읽기와 실행권한을 부여하고 다른 사용자에게는 읽기 권한을 제거하는 권한 변경 명령으로 알맞은 것은?

1chmod 401 secure.txt
2chmod o+rx, a-r secure.txt
3chmod 504 secure.txt
4chmod u=rx, o-r secure.txt

▸ chmod u=rx, o-r secure.txt가 요구사항에 맞는 명령이다. 소유자 권한을 정확히 읽기·실행(rx)으로 지정(u=rx)하고, 다른 사용자의 읽기 권한만 제거(o-r)해 그 외 기존 권한은 그대로 유지하는 방식이라 조건을 정확히 충족한다. chmod 401은 소유자에게 실행 권한을 주지 못하고, chmod o+rx, a-r은 오히려 다른 사용자에게 실행 권한을 부여하면서 소유자의 읽기 권한까지 없애며, chmod 504는 다른 사용자의 읽기 권한이 그대로 남아 요구사항과 맞지 않는다.

[9번] 다음 중 빈칸 ㉠에 들어갈 알맞은 용어는?

1클라우드
2저장소
3젠킨스
4빌드

▸ GitHub·GitLab·Bitbucket을 한데 묶어 부르는 말이므로 빈칸에는 저장소(Repository)가 들어간다. 이들은 소스코드를 보관하고 버전을 관리하는 온라인 소스코드 저장소 서비스로, 접근 권한을 공개로 잘못 설정하면 프로젝트 전체와 하드코딩된 인증정보까지 노출되어 공급망 공격의 출발점이 된다. * 클라우드 — 인프라 제공 형태를 가리키는 말이라 세 서비스를 묶는 이름이 되지 못한다 * 젠킨스 — 빌드·배포를 자동화하는 CI 도구로 코드를 보관하는 곳이 아니다 * 빌드 — 소스를 실행 가능한 산출물로 만드는 공정 자체를 뜻한다

[10번] 윈도우 시스템 인증 구성요소에서 모든 계정의 로그인에 대한 검증을 하고, 비밀번호 변경을 처리하며 자원 접근 토큰을 생성하는 것은?

1LSA(Local Security Authority)
2SAM(Security Account Manager)
3SRM(Security Reference Monitor)
4NTLM(NT LAN Manager)

▸ LSA(Local Security Authority)가 모든 계정의 로그인 검증, 비밀번호 변경 처리, 자원 접근 토큰 생성을 담당한다. SAM은 로컬 계정 정보를 저장하는 데이터베이스, SRM은 접근 권한 검사를 수행하는 구성요소, NTLM은 인증 프로토콜로 각각 LSA와 역할이 구분된다.

[11번] 도메인 계정에 대한 로그인 성공, 실패 관련 이벤트 로그를 기록하기 위해 보안설정이 필요한 감사 항목은?

1계정 관리 감사
2계정 로그인 이벤트 감사
3개체 액세스 감사
4시스템 이벤트 감사

▸ 계정 로그인 이벤트 감사를 활성화해야 도메인 계정의 로그인 성공·실패 이벤트가 기록된다. 계정 관리 감사는 계정 생성·변경 등 관리 작업을, 개체 액세스 감사는 파일·폴더 등 개체에 대한 접근을, 시스템 이벤트 감사는 시스템 재시작·종료 등을 기록 대상으로 하여 로그인 이벤트와는 목적이 다르다.

[12번] 레지스트리에 대한 설명으로 틀린 것은?

1시스템 구성정보를 저장하는 데이터베이스로 저장되는 위치는 윈도우 운영체제 버전에 따라 다르다.
2레지스트리의 편집을 위해 사용되는 도구는 regedit.exe이다.
3레지스트리 키는 HKEY_CLASSES_ROOT, HKEY_USERS, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_CURRENT_CONFIG 등을 포함한다.
4레지스트리 백업 및 복구는 shell.exe를 구동하여 수행한다.

▸ 레지스트리 백업 및 복구를 shell.exe로 수행한다는 설명은 틀렸다. 레지스트리 편집과 백업·복구는 일반적으로 regedit.exe의 내보내기·가져오기 기능이나 시스템 복원 기능을 이용하며, shell.exe라는 도구는 존재하지 않는다. 레지스트리가 시스템 구성정보를 저장하는 데이터베이스이고 버전에 따라 저장 위치가 다르다는 점, HKEY_CLASSES_ROOT 등의 주요 키 구성은 실제와 일치한다.

[13번] ㉠, ㉡, ㉢에 들어갈 내용이 올바르게 짝지어진 것은?

1㉠ 패스워드 무차별 대입 ㉡ disable ㉢ 10
2㉠ 패스워드 무차별 대입 ㉡ deny ㉢ 600
3㉠ 부채널 ㉡ disable ㉢ 10
4㉠ 부채널 ㉡ deny ㉢ 600

▸ 3회 실패 시 계정을 잠그는 정책이므로 ㉠은 패스워드 무차별 대입, ㉡은 deny, ㉢은 600이다. pam_tally2 모듈에서 로그인 실패 허용 횟수를 지정하는 옵션 이름이 deny이며, disable이라는 옵션은 존재하지 않는다. unlock_time은 초 단위이므로 10분 = 10 × 60 = 600이 들어간다. 부채널 공격은 전력·시간 등 물리적 부수정보를 분석하는 기법이라 로그

인 실패 횟수 제한으로 막을 수 있는 공격이 아니다.

[14번] 쿠키(Cookie)에 대한 설명 중 옳지 않은 것은?

1웹사이트에 마지막으로 방문한 시간, 페이지 등 다양한 정보를 기록할 수 있다.
2웹서버가 웹브라우저에게 보내어 저장했다가 서버의 부가적인 요청이 있을 때 다시 서버로 보내준다.
3일정한 기간 동안만 유효하게 할 수 있고, 유효(만료) 기한이 설정되지 않을 경우 웹브라우저 종료 시에 자동 삭제된다.
4웹서버에 저장된 쿠키값은 개인정보보호를 위해 정기적으로 삭제해야 한다.

▸ 쿠키값이 웹서버에 저장된다는 전제 자체가 옳지 않다. 쿠키는 웹서버가 발급해 웹브라우저(클라이언트) 측에 저장되었다가 이후 요청 시 서버로 다시 전송되는 정보이므로, 웹서버에 저장된 쿠키값을 정기적으로 삭제한다는 서술은 저장 주체를 잘못 지칭한 것이다. 방문 이력 등 다양한 정보 기록, 서버 요청 시 재전송되는 동작, 만료기한이 없으면 브라우저 종료 시 삭제된다는 나머지 설명은 옳다.

[15번] 다음 중 AD(Active Directory) 시스템을 안전하게 관리하기 위한 방안을 잘못 설명한 것은?

1전용 계정을 별도로 관리하여 일반 업무용 AD 계정과 는 분리하여 사용한다.
2관리자 계정은 특수성이 있으므로 비밀번호 갱신주기에 대해서는 예외적용을 하도록 한다.
3비밀번호 갱신 정책에는 최근에 사용한 비밀번호들을 재사용하지 못하게 하는 제약조건도 고려되어야 한다.
4관리자용 단말은 인터넷과 격리된 망분리 환경으로 구성되어야 한다.

▸ 관리자 계정의 비밀번호 갱신주기에 예외를 적용한다는 설명이 잘못되었다. 관리자 계정은 권한이 크기 때문에 오히려 일반 계정보다 더 엄격한 비밀번호 정책과 갱신 주기를 적용해야 하며, 갱신주기 예외를 두는 것은 보안상 바람직하지 않다. 전용 계정 분리 운영, 비밀번호 재사용 제한, 관리자 단말의 망분리 운영이라는 나머지 설명은 안전한 AD 관리 방안에 해당한다.

[16번] 스택상에서 특정 코드 실행을 막기 위해 수정해야 하는 파일은?

1/etc/system
2/etc/getty
3/etc/fsck
4/etc/conf

▸ 솔라리스 계열에서 스택 영역의 코드 실행을 막으려면 /etc/system 파일을 수정한다. 이 파일에 스택 비실행(non-executable stack) 관련 설정을 추가하면 스택에 삽입된 공격 코드가 실행되는 것을 차단할 수 있어, 스택 기반 버퍼 오버플로 공격에 대한 대응책으로 활용된다.

[17번] 시스템 오류를 공격하는 Heap Overflow 공격의 특징 및 원리에 대한 설명으로 틀린 것은?

1프로그램이 실행되면서 메모리를 동적으로 할당하는 영역을 이용한다.
2프로그래머가 malloc과 같은 메모리 할당 함수를 이용한다.
3힙 영역을 오버플로우 시켜서 특정 코드를 실행하여 공격하는 기술이다.
4버스를 통해 전달되는 중요 정보를 엿보고 가로채는 공격 기술이다.

▸ 버스를 통해 전달되는 정보를 엿보고 가로채는 공격이라는 설명은 Heap Overflow와 무관하다. Heap Overflow는 동적으로 할당되는 메모리 영역(힙)을 대상으로, malloc 등 메모리 할당 함수로 확보한 공간을 오버플로우시켜 임의 코드를 실행하는 공격 기법이다. 버스를 통한 정보 가로채기는 하드웨어 도청·스니핑 계열의 공격에 해당하며, 힙 영역의 동적 메모리 오남용과는 성격이 다르다.

[18번] 다음 지문의 설정사항이 의미하는 것은?

1root 계정의 패스워드 임계치를 설정하고 있다.
2모든 계정에 대한 패스워드 임계치를 설정하고 있다.
3모든 계정에 대한 암호화 접속을 활성화하기 위한 설정이다.
4root 계정의 원격접속을 제한하는 설정이다.

▸ root 계정의 원격 접속을 제한하는 설정이다. /etc/securetty는 root 로그인이 허용되는 터미널 목록인데, 여기에 pts/0~pts/x 같은 가상 터미널이 남아 있으면 원격 접속으로도 root 직접 로그인이 가능하다. 그래서 해당 줄을 지우거나 주석 처리한다. HP-UX 쪽은 반대로 console 줄의 주석을 풀어 콘솔에서만 root 로그인을 허용하게 만든다. 이 파일은 로그인 허용 단말을 통제할 뿐이어서 패스워드 임계치 설정이나 암호화 접속 활성화와는 관련이 없다.

[19번] 윈도우 시스템에 포함된 원격 접속 프로그램인 터미널 서비스 기능을 이용할 때 사용되는 명령어는?

1vnc
2mstsc
3teamviewer
4realvnc

▸ 윈도우 터미널 서비스(원격 데스크톱)를 이용할 때 사용하는 명령어는 mstsc이다. vnc·realvnc·teamviewer는 윈도우에 기본 내장된 명령어가 아니라 별도로 설치해야 하는 원격제어 프로그램으로, 운영체제에 포함된 터미널 서비스 클라이언트와는 구분된다.

[20번] 가상사설망(VPN)의 터널링에 사용되는 프로토콜이 아닌 것은?

▸ RSVP는 VPN 터널링 프로토콜이 아니다. RSVP는 네트워크 경로상의 대역폭 등 자원을 예약해 QoS(서비스 품질)를 보장하기 위한 프로토콜로, 가상사설망 터널을 구성하는 용도가 아니다. PPTP·L2F·IPSec은 모두 VPN 구간의 데이터를 캡슐화·보호하는 터널링 프로토콜에 해당한다.

[21번] 아래 지문에서 강조(밑줄)된 프로토콜의 기능과 가장 거리가 먼 것은?

1네트워크 장치의 동적 상황 검사
2Routing Table 변경 요청
3IP 통신을 위한 진단 데이터 전송
4Multi-casting 제어

▸ 밑줄 친 프로토콜은 ICMP이고, 멀티캐스트 그룹의 가입·탈퇴를 제어하는 일은 IGMP의 역할이므로 ICMP의 기능과 가장 거리가 멀다. ICMP는 IP 통신 중 발생한 오류와 상태를 알리는 프로토콜이다. Echo Request/Reply로 장치의 동적 상태를 점검하고, Destination Unreachable·Time Exceeded 같은 진단 데이터를 전달한다. 지문처럼 ICMP Redirect 메시지로 라우팅 테이블 변경을 요청하는 것도 ICMP의 기능이며, DoubleDirect는 바로 이 기능을 악용한 중간자 공격이다.

[22번] 다음 보기 중 빅데이터의 방대한 정보 속에서 단순한 로그 수집 및 분석이 아닌 사후에 추적 등이 가능하도록 상관분석과 포렌식 기능을 제공해주는 지능적 위협에 대한 조기 경고 모니터링 체계를 의미하는 것은?

▸ 단순 로그 수집·분석을 넘어 상관분석과 포렌식 기능까지 제공하는 조기경보 체계는 SIEM(Security Information and Event Management)이다. SIEM은 방대한 로그를 통합 수집한 뒤 이벤트 간 상관관계를 분석해 위협을 조기에 탐지하고, 사후 추적조사에 필요한 근거 자료를 남기는 데 특화되어 있다. IPS는 실시간 공격 차단, TMS는 위협 통합관리, UTM은 다양한 보안 기능의 통합 장비로 각각 SIEM과 목적이 다르다.

[23번] 다음 지문은 네트워크 공격기술에 대한 설명이다. 적절하지 못한 것으로 짝지어진 것은?

1㉠, ㉡
2㉠, ㉢
3㉡, ㉣
4㉢, ㉣

▸ SYN 플러딩과 스머프의 설명이 서로 뒤바뀌어 있어 이 두 항목이 잘못된 설명이다. ICMP 패킷을 브로드캐스트로 증폭해 서비스 거부를 일으키는 것은 스머프(Smurf) 공격이고, 동시 사용자 수 제한을 노려 존재하지 않는 클라이언트의 연결로 백로그 큐를 채우는 것은 SYN 플러딩이다. 나머지 두 항목은 설명이 맞다. Boink는 오프셋이 어긋난 IP 단편을 보내 재조합 로직을 망가뜨리고, 랜드(LAND) 공격은 출발지와 목적지 IP를 동일하게 만들어 대상이 자기 자신에게 응답하도록 유도한다.

[24번] 다음 지문은 라우팅에 관한 설명이다. 빈칸에 들어갈 내용을 순서대로 나열한 것은?

1(가) 라우터 (나) 라우팅 테이블 (다) Static Route
2(가) 라우터 (나) 라우팅 테이블 (다) Default route
3(가) 스위치 (나) 목적지 테이블 (다) Static Route
4(가) 스위치 (나) 목적지 테이블 (다) Default Route

▸ (가)는 라우터, (나)는 라우팅 테이블, (다)는 Default route다. 목적지 IP를 보고 라우팅 테이블에서 서브넷이 일치하는 레코드를 찾아 인터페이스와 게이트웨이를 결정하는 장비는 3계층 장비인 라우터다. 스위치는 MAC 주소로 전달하는

2계층 장비라 목적지 IP 기반 경로 결정을 하지 않는다. 테이블에 등록되어 있지 않은 목적지 전부를 한 경로로 흘려보내는 설정은 Default route(0.0.0.0/0)다. Static route는 관리자가 특정 목적지의 경로를 수동으로 지정하는 것이라 미등록 주소 전체를 처리하지 못한다.

[25번] 스위칭 환경에서 시도할 수 있는 스니핑 공격 유형과 거리가 먼 것은?

1SYN Flooding
2Switch jamming
3ICMP Redirect
4ARP Spoofing

▸ SYN Flooding은 스위칭 환경의 스니핑 공격과는 거리가 멀다. SYN Flooding은 TCP 연결 요청을 대량으로 보내 시스템 자원을 고갈시키는 서비스 거부(DoS) 공격으로, 트래픽을 도청하는 스니핑과는 목적과 방식이 다르다. Switch jamming, ICMP Redirect, ARP Spoofing은 모두 스위치의 정상 동작을 교란하거나 속여 트래픽을 자신에게 우회시켜 도청하는 스니핑 기법에 해당한다.

[26번] 지문에서 설명한 공격의 대응 방안으로 옳지 않은 것은?

1위조된 패킷이 인터넷망으로 인입되지 않도록 ISP의 네트워크 단에서 직접 차단한다.
2사전 공격에 악용될 소지가 있는 취약한 DNS 서버 등에 대해 보완 조치한다.
3악의적으로 이용되지 않기 위해 ICMP 프로토콜을 사용할 필요가 없는 시스템인 경우에는 스위치 또는 서버에서 해당 프로토콜을 차단한다.
4외부 인터넷 서버의 접속이 잦을 경우 클라이언트의 보호를 위해 HTTP 프로토콜을

2021년 정보보안기사 필기

제1회 · 28문항

[1번] 내부 정보 유출 차단을 위한 보안 제품은 무엇인가?

▸ 단말에 에이전트를 설치해 메일·SNS·웹 등 유출 경로를 감시하고 막는 제품은 DLP(Data Loss Prevention)다. DLP는 오가는 데이터의 내용을 키워드·패턴·문서지문으로 검사해 반출 행위 자체를 통제한다. 그래서 메일 전송, 웹 업로드, 출력, 이동식 매체 복사 같은 채널이 모두 감시 대상이 된다. * DRM — 문서를 암호화하고 사용자별 열람·편집 권한을 부여해 유출되더라도 열지 못하게 하는 방식으로, 유출 경로를 탐지·차단하는 것이 목적이 아니다. * VDI — 업무 환경을 중앙 서버의 가상 데스크톱으로 옮겨 자료가 단말에 남지 않게 하는 인프라 방식이다. * EDMS — 전자문서를 등록·결재·보관·검색하는 문서관리 시스템으로 유출 차단 솔루션이 아니다.

[2번] 다음 중 Windows에서 사용하는 일반사용자 그룹인 Users 그룹에 대한 설명 중 적합하지 않은 것은?

1User는 시스템 크기의 레지스트리 설정, 운영체제 파일 또는 프로그램 파일을 수정할 수 없다.
2User는 워크스테이션을 종료할 수는 있지만 서버는 종료할 수 없다.
3Users가 로컬 그룹을 만들 수는 있지만 자신이 만든 로컬 그룹만 관리할 수 있다.
4Users 그룹의 구성원은 다른 Users 그룹에서 실행할 수 있는 프로그램을 설치할 수 있다.

▸ Windows의 Users 그룹은 시스템 전반에 영향을 주는 프로그램의 설치나 시스템 파일·레지스트리 변경이 제한되어 있어, 다른 Users가 실행할 수 있는 프로그램이라도 임의로 설치할 수는 없다. 워크스테이션은 종료할 수 있지만 서버는 종료할 수 없다는 점, 자신이 만든 로컬 그룹만 관리할 수 있다는 점은 Users 그룹의 실제 권한 범위와 일치한다.

[3번] 파일 무결성 점검 도구에 해당하는 것은?

1John the Ripper
2Tripwire
3Snort
4Nmap

▸ Tripwire는 파일의 해시값을 주기적으로 비교해 무단 변경 여부를 탐지하는 대표적인 파일 무결성 점검 도구이다. John the Ripper는 패스워드 크래킹 도구, Snort는 침입 탐지 시스템(IDS), Nmap은 포트·서비스 스캐너로 각각 목적이 다르다.

[4번] 주체가 주도적으로 자신이 소유한 객체(파일 등)에 대한 접근권한(Read, Write, Execution, Append 등)을 다른 주체(사용자)에게 양도하는 등의 행위가 가능한 접근통제 정책은?

▸ DAC(임의적 접근통제)는 객체의 소유자가 자신의 판단으로 다른 사용자에게 읽기·쓰기·실행 등의 접근 권한을 부여하거나 양도할 수 있는 방식이다. MAC은 시스템이 정한 보안등급에 따라 강제로 통제되고, RBAC은 역할에 따라, CBAC은 접속 상황(문맥) 조건에 따라 권한이 결정되어 소유자가 임의로 양도할 수 있는 구조가 아니다.

[5번] 다음 지문이 설명하는 파일 시스템은?

1exFAT(Extended File Allocation Table)
2ext4(extended file system)
3HFS(Hierarchical File System)
4ReFS(Resilient File System)

▸ FAT32의 파일 크기·디렉터리 제약을 풀기 위해 마이크로소프트가 만든 파일 시스템은 exFAT이다. exFAT은 윈도우 CE 6.0과 비스타 이후 데스크톱·서버에 도입됐고, 저널링과 보안 기술자 같은 무거운 기능을 덜어내 자료구조 오버헤드를 줄인 구조라 플래시 메모리·SD 카드 등 이동식 대용량 매체에 주로 쓰인다. * ext4 — 리눅스 계열에서 쓰는 파일 시스템으로 마이크로소프트가 만든 것이 아니다. * HFS — 애플 매킨토시에서 쓰던 계층적 파일 시스템이다. * ReFS — 마이크로소프트 제품이지만 윈도우 서버 2012에서 NTFS를 대체할 복원력 중심으로 도입됐고, 지문이 말하는 도입 시점·대상 제품과 맞지 않는다.

[6번] 다음은 윈도우 부팅 순서이다. 올바르게 나열된 것은?

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

▸ 전원을 켠 뒤 진행 순서는 POST → CMOS → MBR → NTLDR → NTDETECT.com → ntoskrnl.exe다. 먼저 펌웨어가 하드웨어 이상 유무를 점검하고(POST), 사용자가 저장해 둔 설정값을 CMOS에서 읽어 적용한다. 그다음 부팅 매체의 첫 섹터인 MBR을 읽어 부팅 파티션의 위치를 알아낸다. 이어 부팅 파티션의 NTLDR이 boot.ini를 읽어 올릴 운영체제를 정하고, NTDETECT.com이 설치된 하드웨어를 조사한 뒤, 마지막으로 커널인 ntoskrnl.exe가 HAL.dll과 함께 적재된다. 하드웨어 점검보다 MBR 읽기가 앞서거나 커널 적재가 하드웨어 검사보다 먼저인 배열은 성립하지 않는다.

[7번] 소유자 외에는 읽기, 쓰기, 실행 등 일체의 접근을 불허하기 위한 umask 설정값으로 알맞은 것은?

1umask 077
2umask 020
3umask 022
4umask 066

▸ umask 077은 소유자 권한을 제외한 그룹과 기타 사용자의 읽기·쓰기·실행 권한을 모두 차단한다. 077은 그룹과 기타 사용자 권한 비트를 모두 마스크하므로 소유자만 접근할 수 있으며, 020·022·066은 일부 권한이 허용될 수 있다.

[8번] 'last' 명령을 사용하여 정보를 확인할 수 있는 로그파일은?

▸ wtmp 파일은 사용자의 로그인·로그아웃 이력을 누적 기록하며, last 명령은 이 파일을 읽어 로그인 기록을 출력한다. utmp는 현재 로그인 중인 세션 정보, pacct는 실행된 명령의 프로세스 회계 정보, lastlog는 사용자별 마지막 로그인 시각을 담고 있어 각각 다른 명령으로 조회한다.

[9번] 다음 지문에서 설명하는 파일은 무엇인가?

1hosts.equiv
2hosts
3inetd.conf
4shadow

▸ IP 주소와 호스트 이름을 직접 대응시켜 두는 /etc/hosts에 대한 설명이다. 이름 해석은 일반적으로 hosts 파일을 DNS보다 먼저 참조하므로, 공격자가 이 파일에 한 줄만 추가해도 정상 도메인이 악성 IP로 연결되는 파밍이 성립한다. 그래서 소유자를 root로 두고 일반 사용자에게 쓰기 권한을 주지 않는 것이 기본 대응이다. * hosts.equiv — 신뢰할 호스트

와 사용자를 등록해 r 계열 명령의 인증을 생략시키는 파일로, 이름과 IP를 매핑하지 않는다. * inetd.conf — 슈퍼데몬이 어떤 포트에 어떤 서비스를 띄울지 정의하는 설정 파일이다. * shadow — 계정의 암호화된 패스워드와 만료 정책을 담는 파일이다.

[10번] 다음 지문에서 설명하는 것은?

1Session
2Web Beacon
3Super Cookie
4History Stealing

▸ 지문이 설명하는 것은 웹 비콘(Web Beacon)이다. 쿠키와 결합해 웹사이트 이용·이메일 열람 행동을 추적하려고 페이지나 메일 본문에 심어 두는 1픽셀*1픽셀 크기의 눈에 띄지 않는 임베딩 이미지이며, Web bug·pixel tag·e-mail 트래킹이라는 별칭이 붙는다는 점이 결정적 단서다. * 세션은 서버가 접속 상태를 유지하려고 관리하는 연결 단위일 뿐 추적용 이미지가 아니다. * 슈퍼 쿠키는 일반 쿠키를 지워도 되살아나는 영속형 추적 저장 방식이고, 히스토리 스틸링은 방문 기록 링크의 렌더링 차이를 이용해 방문 사이트 목록을 캐내는 공격 기법이다.

[11번] access log에는 referer라는 필드가 존재한다. 이 필드가 의미하는 것은?

1서비스에서 발생하는 이벤트 서버와 글로벌 카달로그 사이의 연결문제를 기록한다.
2사이트를 방문한 사용자가 어떤 경로를 통해 사이트를 방문했는지 알 수 있게 해준다.
3시스템 구성요소가 기록하는 이벤트로 시스템 부팅 시 드라이버가 로드되지 않는 경우와 같이 구성요소의 오류를 기록한다.
4응용프로그램이 기록한 다양한 이벤트가 저장되며, 저장되는 부분은 소프트웨어 개발자에 의해 결정된다.

▸ 웹 access log의 referer 필드는 사용자가 현재 페이지에 접근하기 직전에 머물렀던 이전 페이지(유입 경로)의 주소를 기록한다. 이를 통해 방문자가 어떤 링크나 검색을 거쳐 사이트로 들어왔는지 추적할 수 있으며, 시스템 이벤트나 드라이버 오류, 애플리케이션 이벤트 로그와는 성격이 다르다.

[12번] 루트 사용자 소유로 SUID 권한을 부여한 경우, 이러한 파일로 의심되는 파일을 검색하는 명령어로 알맞은 것은?

1find / -user –perm –1000 -print
2find / -user –perm –2000 -print
3find / -user –perm –3000 -print
4find / -user –perm –4000 -print

▸ SUID(Set User ID) 권한은 8진수 특수 권한 비트 4000으로 표현되며, find 명령에서 -perm -4000 조건으로 루트 소유 SUID 파일을 검색할 수 있다. 1000은 sticky bit, 2000은 SGID, 3000은 SGID와 sticky bit가 함께 설정된 값을 의미해 SUID 검색 목적과는 맞지 않는다.

[13번] Unix 명령($ ls -l)의 실행 결과에 대한 설명으로 가장 옳은 것은?

1파일 aaa에 대한 소유자는 bbb이다.
2파일 bbb에 대한 소유자는 aaa이다.
3파일 ccc에 대한 소유자는 aaa이다.
4파일 aaa에 대한 소유자는 ccc이다.

▸ 출력된 줄에서 파일 이름은 맨 끝의 ccc이고 그 소유자는 aaa이므로, 파일 ccc의 소유자가 aaa라는 설명이 옳다. 표시된 결과는 -rwxr--r-- aaa bbb 98 Aug 7 19:16 ccc 이며, 왼쪽부터 권한 → 소유자 → 그룹 → 크기 → 수정시각 → 파일명 순이다(실제 ls -l 은 권한과 소유자 사이에 링크 수가 한 칸 더 붙는다). 따라서 aaa는 소유자, bbb는 그룹, 98은 파일 크기, ccc는 파일명이다. aaa·bbb·ccc 가 모두 이름처럼 보이지만 파일명은 줄의 마지막 하나뿐이므로, aaa나 bbb를 파일로 보는 설명은 성립하지 않는다.

[14번] Crontab을 이용해 정기적으로 매일 오전 1시에 아파치 웹 서버 로그를 백업하고자 한다. 백업 경로는 /backup/logs/ 이며, 파일 이름은 “log-년월일시분” 형식을 따른다. 정상적으로 작동시키기 위해 Crontab에 등록해야할 값으로 올바른 것은? (파일이름 예시: log-201903210019)

1* * * 1 0 cp /etc/httpd/logs/access_log /backup/logs/log-'date + %Y %m %d %H %M'
20 1 * * * cp /etc/httpd/logs/access_log /backup/logs/log-'date + %Y %m %d %H %M'

3* * * 0 1 cp /etc/httpd/logs/access_log /backup/logs/log-'date + %Y %m %d %H %M'
40 1 * * 0 cp /etc/httpd/logs/access_log /backup/logs/log-'date + %Y %m %d %H %M'

▸ crontab 필드는 분 시 일 월 요일 순서이며, 매일 오전 1시에 실행하려면 일·월·요일 자리를 모두 *로 두고 분과 시만 지정한 0 1 * * * 형태로 작성해야 한다. 요일 자리에 0이나 1을 넣으면 특정 요일에만 실행되고, 분·시 자리를 별표로 두면 매분 실행되어 매일 오전 1시 실행이라는 요건을 만족하지 못한다.

[15번] 하드웨어 및 소프트웨어를 탑재한 시스템 요소를 의미하는 것은?

▸ TCB(Trusted Computing Base)는 하드웨어 및 소프트웨어를 포함해 시스템의 보안 정책을 구현하는 모든 보호 메커니즘의 총체를 의미한다. 시스템 내에서 접근통제 등 보안 기능이 실제로 수행되는 신뢰 기반 요소들을 통칭하는 개념으로, EGID(유효 그룹 ID)·PCB(프로세스 제어 블록)·CC(공통평가기준)와는 성격이 다르다.

[16번] 다음 지문에서 설명하고 있는 공격은 무엇인가?

1스펙터
2캐시 포이즈닝
3멜트다운
4미라이

▸ 지문이 가리키는 것은 멜트다운(Meltdown)이다. 멜트다운은 비순차 명령 실행에서 권한 검사가 끝나기 전에 미리 수행된 결과가 CPU 캐시에 흔적으로 남는 점을 악용해, 일반 프로그램이 커널 영역의 데이터를 간접적으로 읽어내게 만드는 취약점이다. * 스펙터는 같은 시기에 공개된 부채널 취약점이지만 분기 예측을 속여 다른 프로세스 영역을 읽는 방식이라 지문의 비순차 실행 검사 우회와 구분된다. * 캐시 포이즈닝은 DNS 등 서버 캐시에 거짓 정보를 주입하는 네트워크 공격이고, 미라이는 IoT 기기를 감염시켜 대규모 DDoS를 일으킨 악성코드다.

[17번] 윈도우 로그는 무엇인가?

1응용 프로그램 로그
2시스템 로그
3보안 로그
4설정 로그

▸ 운영체제 구성요소가 남기는 기록, 즉 시스템 로그에 대한 설명이다. 윈도우 이벤트 뷰어의 시스템 로그에는 운영체제 시작 시점의 이벤트와 장치 드라이버의 로드 성공·실패처럼 OS 자체 구성요소가 발생시킨 항목이 쌓인다. * 응용 프로그램 로그는 OS가 아니라 설치된 프로그램이 남기는 기록이다. * 보안 로그는 로그온 성공·실패와 개체 접근 감사 등 감사 정책에 따른 기록이며, 윈도우 이벤트 로그에 '설정 로그'라는 기본 분류는 없다.

[18번] 파일 공유와 관련된 서비스 포트에 대한 내용으로 적절하지 않은 것은?

1445(TCP/UDP, Direct Host)
2139(TCP, NetBIOS Session)
3137(UDP, NetBIOS Name)
4335(UDP, NetBIOS Datagram)

▸ NetBIOS Datagram Service는 138번 UDP 포트를 사용하므로, 335번이라는 설명은 옳지 않다. 파일 공유(SMB) 환경에서는 445(TCP/UDP), NetBIOS Name(137, UDP), NetBIOS Datagram(138, UDP), NetBIOS Session(139, TCP) 포트가 함께 쓰인다.

[19번] 유닉스 시스템에서 계정과 패스워드에 관련된 설명으로 틀린 것은?

1유닉스 시스템에서 사용자들은 각각 고유의 아이디를 갖고 있으며, 그 아이디에 대한 정보는 /etc/passwd에 저장된다.
2유닉스 시스템에서는 각각의 사용자만이 접근 가능한 파일과 디렉터리가 존재할 수 있다.
3사용자 패스워드는 /etc/passwd 또는 /etc/shadow 파일에서 관리한다.
4/etc/shadow 파일에는 사용자의 패스워드가 AES-256 알고리즘에 의해 암호화되어 저장된다.

▸ 유닉스의 패스워드는 AES-256 같은 대칭키 암호화가 아니라 단방향 해시(crypt, MD5, SHA-512 등)로 변환되어 저장된다. 해시는 복호화가 불가능한 일방향 함수이므로, 암호화되어 저장된다는 설명은 옳지 않다.

[20번] 접근권한을 확인하였더니 'rwSr- -r- -'이었다. 권한 내의 대문자 S에 대한 설명으로 옳은 것은?

1SetUID를 실행 권한이 없는 파일에 설정할 경우 대문자 S로 표기된다.

2SetGID를 실행 권한이 없는 파일에 설정할 경우 대문자 S로 표기된다.
3디렉터리에 스티키 비트가 설정되어 대문자 S로 표기하였다.
4SetGID를 설정하여 대문자 S로 표기하였다.

▸ SetUID 비트가 설정된 파일에 소유자 실행 권한(x)이 없는 경우 소문자 s 대신 대문자 S로 표기된다. 실행 권한이 있으면 소문자 s로 표기되어, S와 s는 실행 권한 유무를 함께 나타내는 표기 방식이다.

[21번] 다음은 WEP에 대한 설명이다. 빈칸 ㉠에 들어갈 내용으로 적절한 것은?

1Encryption Key
2Initial Key
3Initial Vector
4Encryption Vector

▸ 빈칸에 들어갈 것은 Initial Vector(초기화 벡터, IV)이다. WEP은 RC4 스트림 암호를 쓰기 때문에 같은 비밀키로 같은 키스트림이 반복되면 안 된다. 그래서 프레임마다 랜덤한 24비트 IV를 만들어 비밀키 앞에 붙여 키스트림을 생성하고, 그 IV는 상대가 복호할 수 있도록 평문으로 단말에 함께 전송한다. 지문의 '키 생성 순서 예측 방지를 위해 랜덤하게 생성해 무선 단말기에 보낸다'가 바로 IV의 역할이다. 실제 암·복호에 쓰는 비밀키 자체는 전송되지 않으므로 Encryption Key·Initial Key 처럼 키를 뜻하는 용어는 빈칸에 들어갈 수 없고, Encryption Vector 는 WEP 규격에 없는 용어다.

[22번] 무선랜의 전송 패킷에 덧붙여지는 32bytes 길이의 고유 식별자로서, 무선장치들이 BSS(Basic Service Set)에 접속할 때 패스워드같이 사용되는 코드는 무엇인가?

1무선 네트워크 아이디(SSID)
2WEP(Wired Equivalent Privacy)
3MAC(Message Authentication Code)
4RFID 태그

▸ 무선 패킷에 덧붙는 32바이트 이하의 고유 식별자로 BSS 접속 시 패스워드처럼 쓰이는 것은 SSID(무선 네트워크 식별자)이다. WEP은 암호화 방식, MAC(Message Authentication Code)은 무결성·인증용 코드, RFID 태그는 별도의 무선 식별 기술로 이 설명과는 무관하다.

[23번] 지문에서 설명하고 있는 것은?

1NFV(Network Function Virtualization)
2MDR(Managed Detection & Response)
3EDR(Endpoint Detection & Response)
4SDN(Software Defined Networking)

▸ 지문이 설명하는 것은 SDN(Software Defined Networking)이다. SDN은 네트워크 장비의 제어 평면과 데이터 평면을 분리해 폐쇄적이던 장비를 개방형 인터페이스로 열고, 컨트롤러 소프트웨어가 트래픽 흐름을 직접 제어하게 한다. 그 덕분에 지문처럼 미세흐름 조정, QoS 보장, 손쉬운 장비 관리가 가능해진다. * NFV는 방화벽·로드밸런서 같은 네트워크 기능을 가상 소프트웨어로 구현하는 기술이어서 장비 제어 구조를 개방한다는 설명과 초점이 다르다. * EDR과 MDR은 단말 위협 탐지·대응과 그 관제 서비스여서 네트워크 구조의 패러다임과는 무관하다.

[24번] 다음 중 지능형 지속 위협에 대한 설명으로 옳은 것은?

1공격의 설계부터 침투까지 매우 빠른 시간 내에 이루어진다.
2다른 형태의 공격들에 비해 대체로 공격자의 비용이 적게 든다.
3시스템관리자는 가능한 모든 공격을 고려해야 되기 때문에 방어가 매우 어렵다.
4하나의 타깃에 대해서 같은 방법으로 지속적으로 뚫을 때까지 공격하는 것이다.

▸ 지능형 지속 위협(APT)은 특정 대상을 겨냥해 다양한 침투 경로를 장기간 시도하므로, 방어자는 가능한 모든 공격 경로를 대비해야 해 방어가 매우 어렵다. 공격 설계부터 침투까지 오랜 시간과 많은 비용이 들고, 하나의 방법만 반복하기보다 여러 기법을 병행한다는 점에서 다른 설명들과 구분된다.

[25번] 다음 지문의 빈칸 ㉠, ㉡에 들어갈 용어로 올바르게 짝지어진 것은?

1㉠ MAC ㉡ 암호화
2㉠ MAC ㉡ 인증
3㉠ 스위치 ㉡ 인증

4㉠ 스위치 ㉡ 암호화

▸ ㉠에는 MAC, ㉡에는 암호화가 들어간다. 랜카드를 무차별 모드(promiscuous mode)로 두면 목적지 MAC 주소가 자기 것이 아닌 프레임도 버리지 않고 상위 계층으로 올려 스니핑이 가능해진다. 랜카드가 프레임을 걸러내는 기준이 MAC 주소이기 때문이다. 스니핑은 엿듣는 행위 자체를 막기 어려우므로, 가로채더라도 내용을 알아볼 수 없게 만드는 통신 구간 암호화가 가장 효과적인 대응이다. 스위치 환경은 ARP 스푸핑 등으로 우회되고, 인증은 접속 자격만 확인할 뿐 오가는 내용을 보호하지 못한다.

[26번] OSI 7 Layer 중 어느 계층에 대한 설명인가?

1Transport Layer
2Network Layer
3Session Layer
4Physical Layer

▸ 데이터 유실 없이 End-to-End 신뢰성을 보장하고 오류가 있으면 재전송을 요구하는 계층은 전송 계층(Transport Layer)이다. 전송 계층은 종단 프로세스 사이에서 순서 제어·흐름 제어·오류 제어와 재전송을 담당하며, TCP가 바로 이 기능을 수행한다. * 네트워크 계층은 라우팅과 논리 주소 지정을 맡을 뿐 전달을 보장하지 않는다. * 세션 계층은 통신 연결의 설정·유지·동기점 관리를, 물리 계층은 비트의 전기적 전송을 담당한다.

[27번] 1출발지 211.1.99.1 / 목적지주소 32.15.1.1인 패킷은 규칙 1에 의해 거부된다.

2출발지 211.1.99.1 / 목적지주소 32.15.6.15인 패킷은 규칙 2에 의해 허용된다.
3출발지 211.1.37.15 / 목적지주소 32.15.6.15인 패킷은 규칙 2에 의해 허용된다.
4출발지 211.1.37.15 / 목적지주소 32.15.1.1인 패킷은 규칙 3에 의해 차단된다.

▸ 이 문항은 원본 출처에서 문제 또는 보기 내용이 정확하지 않다고 밝힌 문항입니다. 지문이 원래 시험 문제와 다를 수 있으니 개념 확인용으로만 활용하시기 바랍니다.

[28번] TCP의 3-Way Handshaking을 통한 서버와의 연결 설정 과정에서, 연결에 성공한 클라이언트 측의 연결 상태 천이 다이어그램상의 상태 변화의 순서를 바르게 나열한 것은?

1CLOSED→SYN_RCVD→ESTABLISHED
2CLOSED→SYN_SENT→ESTABLISHED
3LISTEN→SYN_RCVD→ESTABLISHED
4LISTEN→SYN_SENT→ESTABLISHED

▸ 클라이언트는 연결을 시작할 때 CLOSED 상태에서 SYN을 보내 SYN_SENT로 전이하고, 서버의 SYN+ACK에 ACK로 응답한 뒤 ESTABLISHED 상태가 된다. SYN_RCVD와 LISTEN은 서 </partial_content> <instructions> Document is too large (77409 tokens). Only showing first 10000 tokens. For complete analysis, run `gsk summarize "https://www.moducbt.com/exam/pdf/28434" --question "<your specific question>"` — it analyzes the full document (PDFs, academic pape

제2회 · 26문항

[1번] NTFS 파일 시스템의 메타 데이터 해당하지 않는 것은?

1$MFT
2$Logfile
3$Volume
4$Bios

▸ $Bios는 NTFS의 메타데이터 파일이 아니다. NTFS는 $MFT, $LogFile, $Volume 외에도 $Bitmap, $Boot, $Secure 등 $로 시작하는 시스템 파일들로 메타데이터를 관리하는데, 이 중 $Bios라는 항목은 존재하지 않는다.

[2번] 다음 지문에서 설명하는 공격은 무엇인가?

1힙 오버플로우 공격
2레이스 컨디션 공격
3스택 오버플로우 공격
4코드 기반 공격

▸ 두 프로세스가 같은 자원을 두고 경쟁 상태(Race Condition)에 놓이는 순간을 노려 SetUID 프로그램의 권한을 가로채는 공격이다. SetUID가 걸린 프로그램이 파일 존재를 확인한 뒤 실제로 그 파일을 여는 사이의 짧은 시간 틈에 공격자가 해당 경로를 심볼릭 링크로 바꿔치기하면, 프로그램은 root 권한으로 공격자가 지정한 파일을 열거나 덮어쓰게 된다. * 스택 오버플로우: 지역변수 버퍼를 넘치게 해 스택의 복귀주소를 덮는 공격 * 힙 오버플로우: 동적 할당 영역을 넘치게 해 관리 구조나 함수 포인터를 조작하는 공격 이 둘은 모두 버퍼 경계 검사 부재를 노린 메모리 손상 공격이어서, 두 프로세스의 실행 순서 차이를 이용하는 지문의 설명과 다르다.

[3번] 리눅스에서 새로 생성되는 사용자 계정의 홈 디렉터리는 .bashrc 등과 같이 모든 사용자가 필요로 하는 파일들을 만들어줄 필요가 있다. 이러한 공통 파일들을 미리 만들어 특정 디렉터리에 넣어두면 사용자 계정 생성 시 자동복사 되도록 설정할 수 있는데, 이러한 용도의 디렉터리는 무엇인가?

1/etc/init
2/etc/services
3/etc/login.defs
4/etc/skel

▸ 리눅스에서 신규 사용자 계정 생성 시 홈 디렉터리에 기본으로 복사되는 공통 파일들을 모아두는 곳은 /etc/skel이다. useradd로 계정을 만들면 /etc/skel 안의 .bashrc, .profile 등의 파일이 새 홈 디렉터리로 자동 복사된다. * /etc/init은 시스템 초기화 스크립트 디렉터리다. * /etc/services는 포트와 서비스명 매핑 파일이다. * /etc/login.defs는 계정 정책(UID 범위, 비밀번호 만료 등) 설정 파일이다.

[4번] 2016년에 처음 발견되었으며 IP 카메라나 가정용 라우터와 같은 IoT 장치를 주요 공격 대상으로 삼는 DDoS 공격용 봇넷 악성코드는 무엇인가?

1님다
2미라이
3스턱스넷
4SQL 슬래머

▸ 2016년 처음 발견되어 IP 카메라·홈라우터 등 IoT 장치를 감염시켜 대규모 DDoS에 악용된 봇넷은 미라이(Mirai)다. 미라이는 기본 계정·비밀번호가 바뀌지 않은 IoT 장치를 스캔해 감염시키고, 감염된 다수의 장치로 봇넷을 구성해 목표 서버에 트래픽을 집중시키는 방식으로 동작한다.

[5번] 다음 지문에서 설명하는 내용은 스푸핑 공격 중 어떤 공격에 해당하는가?

32bit IP 주소를 48bit의 네트워크 카드 주소(MAC Address)로 대응시켜 주는 프로토콜이고 실제로 IP 주소를 통해 네트워크 연결을 시도하면 TCP/IP에서는 해당 IP주소 해당하는 네트워크 카드 주소를 찾아 연결하게 된다. 이더넷 환경에서 공격대상자의 cache 테이블에 공격자가 원하는 IP에 대한 하드웨어 주소(MAC Address)를 거짓으로 지정하여 업데이트함으로써 공격대상자의 패킷 흐름을 공격자가 원하는 방향으로 조절하여 공격하는 기술이다.
1DHCP 스푸핑
2IP 스푸핑
3DNS 스푸핑
4ARP 스푸핑

▸ 32비트 IP 주소를 48비트 MAC 주소로 대응시키는 프로토콜의 캐시를 거짓 정보로 갱신하는 공격이므로 ARP 스푸핑이다. ARP는 요청을 보낸 적이 있는지조차 검증하지 않고 받은 응답으로 캐시를 갱신하기 때문에, 공격자가 위조 ARP 응답을 지속적으로 보내면 피해자의 ARP 캐시에 공격자 MAC이 등록되어 같은 이더넷 세그먼트의 트래픽이 공격자를 거쳐 흐르게 된다. * IP 스푸핑: 패킷의 출발지 IP를 위조해 신뢰관계를 악용하는 공격으로 MAC 캐시와 무관하다 * DNS 스푸핑: 도메인 질의에 가짜 응답을 먼저 보내 다른 IP로 유도하는 공격이다 * DHCP 스푸핑: 가짜 DHCP 서버를 띄워 IP·게이트웨이·DNS 정보를 잘못 할당하는 공격이다

[6번] 디지털저장매체 중 하드디스크 구조에서 물리적으로는 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 무엇이라고 하는가?

1슬랙
2CHS
3클러스터
4확장 공간

▸ 디스크에서 물리적으로는 클러스터가 할당되어 있지만 실제 파일 크기가 그보다 작아 논리적으로 사용할 수 없는 여유 공간을 슬랙(Slack) 공간이라 한다. 이 영역은 이전에 저장되어 있던 데이터의 잔재가 남아 있을 수 있어 디지털 포렌식에서 중요한 증거 수집 대상이 된다.

[7번] 윈도우 레지스트리 키 중에서 파일의 각 확장자에 대한 정보와 프로그램의 맵핑 정보가 저장된 키로 옳은 것은?

1HKEY_CLASSES_ROOT
2HKEY_CURRENT_USER
3HKEY_FILE_EXT
4HKEY_LOCAL_MACHINE

▸ 파일 확장자별 프로그램 연결 정보(파일 형식-프로그램 매핑, COM 등록 정보)가 저장되는 레지스트리 키는 HKEY_CLASSES_ROOT다. HKEY_CURRENT_USER는 로그인한 사용자별 설정, HKEY_LOCAL_MACHINE은 시스템 전역 설정을 담고 있어 확장자 연결 정보와는 다르며, HKEY_FILE_EXT라는 키는 존재하지 않는다.

[8번] 다음 지문에서 설명하고 있는 시스템 보안은?

▸ 민감한 암호 연산을 전용 하드웨어 칩으로 옮겨 안전한 부팅과 키 보관을 제공하는 것은 TPM(Trusted Platform Module)이다. TPM은 메인보드에 탑재되는 암호 프로세서로, 부팅 단계마다 무결성 측정값을 저장해 인증된 부트를 보장하고 암호키를 칩 내부에 봉인해 소프트웨어 공격으로 유출되지 않게 한다. * SRM: 윈도우 커널에서 객체 접근 권한을 판단하는 보안 참조 모니터로 소프트웨어 구성요소다 * SAM: 윈도우 계정과 패스워드 해시를 저장하는 데이터베이스다 * SID: 사용자·그룹을 구분하기 위한 보안 식별자 값이다

[9번] 아래 지문의 척도들과 가장 관련성이 높은 보안 서비스는?

1기밀성
2무결성
3가용성
4유지보수성

▸ 가동시간과 정지시간, MTTF·MTTR은 시스템을 필요할 때 쓸 수 있는 정도를 재는 지표이므로 가용성과 직결된다. 가용성은 보통 가동시간 ÷ (가동시간 + 정지시간)으로 계산하며, 장애 발생까지의 평균 시간(MTTF)이 길고 복구에 걸리는 평균 시간(MTTR)이 짧을수록 높아진다. * 기밀성: 인가되지 않은 대상에게 정보가 노출되지 않는 성질로 암호화·접근통제로 확보한다 * 무결성: 정보가 위·변조되지 않은 성질로 해시·전자서명으로 확인한다 * 유지보수성: 고치기 쉬운 정도를 뜻하는 품질 속성이며 정보보호의 3대 요소에 들지 않는다

[10번] IoT 위협 및 보안에 대한 설명으로 올바르지 않은 것은?

1홈가전 IoT 제품의 보안 요구사항에는 시큐어 코딩, 알려진 보안약점 및 취약점 제거, 최신 제3자(3rd party) 소프트웨어 사용 등이 있다.
2홈캠, 네트워크 카메라 등의 네트워크 제품에 대한 주요 보안 위협에는 사진 및 동영상을 공격자의 서버 및 이메일로 전송하는 것이 있다. 이에 대한 원인으로는 접근통제 및 전송 데이터 보호의 부재가 있다.
3시큐어 코딩이 적용되지 않은 스마트 홈가전 제품의 경우 입력 데이터 검증 및 표현, 보안 기능, 시간 및 상태, 에러처리 등에서 보안 취약점이 발생할 수 있다.
4스마트 홈가전 제품의 데이터 기밀성 및 무결성을 위해 안전한 암호인 MD5, SHA-1 등의 사용이 권장된다.

▸ 스마트 홈가전의 데이터 기밀성·무결성을 위해 MD5, SHA-1 사용을 권장한다는 설명이 옳지 않다. MD5와 SHA-1은 이미 충돌 공격이 실증되어 취약성이 드러난 알고리즘으로, 오늘날에는 SHA-256 이상의 안전한 해시 알고리즘 사용이 권장된다. 나머지 보기는 시큐어 코딩·접근통제·전송데이터 보호 등 IoT 보안 위협과 대응에 대한 올바른 설명이다.

[11번] 기존 파일 시스템에 새로운 파일 시스템을 하위 디렉터리로 연결하기 위해 사용하는 명령어는 무엇인가?

▸ 기존 파일 시스템에 새 파일 시스템을 특정 디렉터리에 연결해 사용할 수 있게 하는 명령어는 mount다. * mkfs는 새 파일 시스템을 생성(포맷)하는 명령어다. * fsck는 파일 시스템의 무결성을 점검·복구하는 명령어다. * mknod는 특수 파일(장치 파일 등)을 생성하는 명령어다.

[12번] 유닉스에서는 패스워드 보호를 위해 암호 처리된 패스워드 정보를 공격자가 접근하기 어렵게 일반 사용자 권한으로 접근할 수 없는 (㉠)를 사용하고 있다.

1해시 암호화 패스워드 파일
2섀도(Shadow) 패스워드 파일
3익명(Anonymity) 패스워드 파일
4PAM(Pluggable Authentication Module) 패스워드 파일

▸ 암호화된 패스워드를 일반 사용자가 읽지 못하도록 따로 떼어 둔 것은 섀도(Shadow) 패스워드 파일이다. 원래 /etc/passwd는 모든 사용자가 읽을 수 있어 해시가 그대로 노출됐는데, 해시를 /etc/shadow로 옮기고 root만 읽을 수 있게 권한을 제한해 사전 공격이나 무차별 크래킹 시도를 차단한다. * 해시 암호화 자체는 passwd 파일에서도 이미 쓰이던 방식이라 접근 권한을 제한한다는 설명과 맞지 않는다 * PAM은 인증 방식을 모듈로 끼워 넣는 인증 프레임워크이지 패스워드를 저장하는 파일이 아니다

[13번] [그림1]은 어떤 리눅스 시스템에 존재하는 특정 /home 디렉터리와 그 아래에 존재하는 디렉터리 및 파일들의 속성 중 name, permission, user, group 등에 대한 정보만 요약한 것이며, [그림2]는 이 시스템에 존재하는 /etc/group 파일의 일부분이다. 이를 통하여 확인할 수 있는 파일 및 디렉터리의 permission에 관한 설명 중 올바르지 않은 것은?

1user1이란 사용자는 /home/user1 디렉터리로 이동할 수 있다
2user2란 사용자는 exam.txt란 파일의 내용을 읽을 수 있다.
3user3란 사용자는 exam.txt란 파일을 삭제할 수 있다.
4시스템 내에 존재하는 user4란 사용자는 /home/user1 디렉터리로 이동할 수 없다.

▸ 파일을 지우려면 그 파일이 들어 있는 디렉터리에 쓰기(w) 권한이 있어야 하는데, security 그룹인 user3에게 /home/user1은 drwxr-x---로 r와 x만 허용되므로 exam.txt를 삭제할 수 없다. 삭제는 파일 자체의 rw- 권한이 아니라 디렉터리 안의 파일 목록을 고치는 작업이라는 점이 판단의 기준이다. * user1은 /home/user1의 소유자로 rwx를 가지므로 그 디렉터리로 이동할 수 있다 * user2는 /etc/group에서 security 그룹원이므로 /home/user1에 x가 있어 들어갈 수 있고, exam.txt의 그룹 권한 rw로 내용을 읽을 수 있다 * user4는 security 그룹에 없어 기타 사용자 권한(---)만 적용되므로 /home/user

[14번] 다른 로그파일에 비해 많은 정보를 포함하고 있는 로그파일로 동작 중인 서비스에 대한 버퍼 오버플로우 공격의 경우와 같이 시스템 장애에 대한 정보를 로그파일로 저장한다.

1btmp
2wtmp
3syslog
4messages

▸ 시스템 전반의 장애·오류 메시지가 가장 폭넓게 남는 로그는 messages 로그다. 커널과 각종 데몬이 syslog 체계를 통해 보낸 메시지가 이곳에 모이므로, 서비스 비정상 종료나 버퍼 오버플로우로 인한 세그먼테이션 폴트 같은 장애 흔적을 여기서 확인한다. * btmp: 로그인 실패 기록만 남기는 바이너리 로그다 * wtmp: 로그인·로그아웃과 재부팅 이력을 남기는 바이너리 로그다 * syslog: 로그를 수집·분배하는 로깅 체계를 가리키는 이름으로, 시스템 장애 정보를 폭넓게 담는 텍스트 로그의 대표로는 보지 않는다

[15번] 랜섬웨어에 해당하지 않는 것은?

1페트야(Petya)
2크립토월(CryptoWall)
3워너크라이(WannaCry)
4크립토재커(CryptoJacker)

▸ 크립토재커(CryptoJacker)는 시스템 자원을 몰래 이용해 암호화폐를 채굴하는 크립토재킹(가상화폐 무단 채굴) 악성코드로, 파일을 암호화해 금전을 요구하는 랜섬웨어와는 목적과 동작 방식이 다르다. 페트야, 크립토월, 워너크라이는 모두 파일을 암호화한 뒤 복호화 대가로 금전을 요구하는 대표적인 랜섬웨어다.

[16번] 서버의 파일 시스템에 대한 시간 속성이 잘못 기술된 것은?

1mtime: 파일을 생성하거나 내용을 수정한 시간
2atime: 최근 파일을 읽거나 실행시킨 시간
3ctime: 파일 속성이 변경된 시간

4rtime: 파일을 실시간 실행시킨 시간

▸ rtime이라는 파일 시간 속성은 존재하지 않으므로 이 설명이 옳지 않다. 일반적으로 파일 시스템은 mtime(수정시간), atime(접근시간), ctime(속성 변경시간)의 세 가지를 기본으로 관리하며, 이를 흔히 MAC 타임이라 부른다.

[17번] 다음에서 설명하고 있는 것은 무엇인가?

1sudo
2PAM
3Batch file
4Shell script

▸ 설명하는 것은 PAM(Pluggable Authentication Module)이다. 인증 절차를 응용프로그램 본체에서 떼어내 공유 라이브러리 묶음으로 제공하는 리눅스의 인증 프레임워크다. 덕분에 login·su·ftp 같은 프로그램을 재컴파일하지 않고 /etc/pam.d 의 설정 파일만 바꿔 비밀번호·LDAP·생체인증 등으로 인증방식을 갈아끼울 수 있다. * sudo: 일반 사용자가 관리자 권한으로 명령을 실행하도록 하는 권한 위임 도구로, 인증 방식 자체를 교체하는 라이브러리가 아니다. * Batch file·Shell script: 명령을 모아 실행하는 스크립트 파일일 뿐 인증 모듈 구조와 무관하다.

[18번] 윈도우 NTFS 파일 시스템의 특징으로 옳지 않은 것은?

1파일과 폴더에 개별 권한을 설정할 수 있어 강력한 보안정책 설정이 가능하다.
2이벤트 뷰어를 사용하여 MFT(Master File Table)의 내용을 확인할 수 있다.
3FAT 파일 시스템에 없는 보안 속성(사용자 접근제어) 정보를 내장하고 있다.
4파일 압축 및 암호화를 위한 구조를 갖는다.

▸ 윈도우의 이벤트 뷰어는 응용 프로그램·보안·시스템 등의 이벤트 로그를 확인하는 도구일 뿐, MFT(Master File Table) 내용을 확인하는 용도가 아니므로 이 설명이 옳지 않다. MFT는 NTFS가 각 파일·폴더의 메타데이터를 기록해 두는 구조로, 그 내용을 보려면 포렌식 도구 등 별도의 분석 도구가 필요하다. 나머지 보기는 개별 권한 설정, 사용자 접근제어 속성, 압축·암호화 구조 등 NTFS의 실제 특징을 올바르게 설명하고 있다.

[19번] rlogin 접속을 허용하는 설정 파일들로 올바르게 짝지어진 것은?

1/etc/hosts.allow, /etc/exports
2/etc/hosts.allow, /.rhosts
3/etc/hosts.equiv, /etc/exports
4/etc/hosts.equiv, /.rhosts

▸ rlogin 접속을 신뢰 관계로 허용하는 설정 파일은 시스템 전체 신뢰 목록인 /etc/hosts.equiv와 사용자별 신뢰 목록인 /.rhosts다. 두 파일에 등록된 호스트·사용자는 비밀번호 없이 rlogin/rsh 접속이 허용되므로 관리가 소홀하면 심각한 보안 위협이 된다. /etc/hosts.allow는 TCP 래퍼 접근제어용, /etc/exports는 NFS 공유 설정용 파일로 rlogin 신뢰 관계와는 무관하다.

[20번] 다음 지문에서 설명하고 있는 안전한 보안 인증 방식은?

1SSH(Secure Shell)
2SAM(Secure Access Module)
3SSO(Single Sign On)
4PAM(Pluggable Authentication Module)

▸ 지문이 가리키는 것은 PAM(Pluggable Authentication Module)이다. 인증 기능을 끼워 넣을 수 있는(pluggable) 모듈로 분리해 공유 라이브러리 형태로 제공한다. 응용 프로그램은 인증 코드를 직접 갖지 않고 이 라이브러리를 호출하므로, 시스템 환경에 맞춰 설정만 바꾸면 여러 인증 방식을 부가적으로 조합할 수 있다. * SSH(Secure Shell): 원격 접속 구간을 암호화하는 통신 프로토콜이지 인증 모듈 라이브러리가 아니다. * SAM(Secure Access Module): 단말에 탑재해 키를 보관·연산하는 보안 모듈로, OS 의 인증 프레임워크와 성격이 다르다. * SSO(Single Sign On): 한 번 인증으로 여러 서비스를 이용하는 통합 인증 개념이라

[21번] ㉠에 들어갈 용어로 적절한 것은?

1Duplex Mode
2MAC 변조
3Promiscuous Mode

4ARP

▸ ㉠ 에 들어갈 말은 Promiscuous Mode(무차별 모드)다. NIC 는 평소 자기 MAC 주소 앞으로 온 프레임과 브로드캐스트만 상위로 올리는데, 스니핑을 하려면 목적지가 자신이 아닌 프레임까지 전부 받아들이는 무차별 모드로 바꿔야 한다. 그래서 탐지 도구는 각 호스트 NIC 가 이 모드인지를 검사한다. * Duplex Mode: 송수신을 동시에 할지(전이중/반이중)를 정하는 통신 방식 설정으로 패킷 수집 여부와 무관하다. * MAC 변조: 주소를 속이는 공격 기법이지 NIC 의 수신 모드 상태를 가리키지 않는다. * ARP: IP 주소를 MAC 주소로 변환하는 프로토콜로, 스푸핑에 악용될 뿐 NIC 모드가 아니다.

[22번] 다음 지문에서 설명하는 공격 대응 방법은 무엇인가?

1DNS 라우팅
2DNS 스푸핑
3DNS 웜홀
4DNS 싱크홀

▸ 설명하는 대응 방법은 DNS 싱크홀(DNS Sinkhole)이다. 악성봇이 명령·제어(C&C) 서버 도메인을 질의하면 DNS 가 진짜 IP 대신 싱크홀 서버 주소를 응답해 연결을 돌려버린다. 그 결과 감염 PC 는 해커의 악의적인 명령을 전달받지 못하고, 관리자는 싱크홀에 접속해 온 IP 로 감염 단말을 찾아낼 수 있다. * DNS 스푸핑: 거짓 응답을 보내 사용자를 악성 사이트로 유도하는 공격 기법이므로 대응 방법이 될 수 없다. * DNS 라우팅·DNS 웜홀: 악성봇 차단 대응책으로 통용되는 기술 용어가 아니다.

[23번] Firewall, IDS, IPS의 비교 중 올바른 것으로 짝지어진 것은?

1㉠, ㉢
2㉡, ㉢
3㉠, ㉣, ㉤
4㉠, ㉢, ㉣

▸ 표에서 바르게 적힌 줄은 패킷 차단·이상 탐지·장점 세 항목이다. 패킷 차단은 방화벽과 IPS 가 수행하고 IDS 는 탐지·경보만 하므로 표의 ○×가 맞고, 이상 탐지는 IDS 와 IPS 가 함께 갖는 기능이라 역시 맞다. 장점도 방화벽은 엄격한 접근 통제, IDS 는 실시간 탐지, IPS 는 세션 기반 탐지로 통용되는 설명이다. * 오용 탐지 줄: 시그니처로 알려진 공격을 잡는 오용 탐지는 IDS 의 대표 방식인데 표에는 ×로 되어 있어 틀렸다. * 단점 줄: 방화벽의 약점은 허용 정책을 통과한 트래픽과 내부에서 발생하는 공격에 취약하다는 점이므로 "외부 공격에 취약"은 맞지 않다.

[24번] 다음 지문에서 설명하는 용어는 무엇인가?

1HSM
2비트라커
3OTP
4TCB

▸ 설명하는 장치는 HSM(Hardware Security Module)이다. 암호화·복호화·전자서명 연산을 전용 칩으로 고속 처리하고, 암호키를 장치 내부에서 생성해 외부로 추출되지 않게 보관하는 것이 핵심이다. 물리적 변조를 감지하면 키를 스스로 파기하는 내변조성도 갖춘다. * 비트라커: 윈도우의 디스크 전체 암호화 소프트웨어 기능으로, 연산 가속과 키 보관을 담당하는 하드웨어 장치가 아니다. * OTP: 일회용 비밀번호를 생성해 사용자를 인증하는 수단이라 역할이 다르다. * TCB: 보안 정책을 집행하는 하드웨어·소프트웨어·펌웨어 전체를 가리키는 신뢰 컴퓨팅 기반 개념이다.

[25번] 침입차단시스템에 대한 설명으로 옳지 않은 것은?

1패킷 필터링 방화벽은 패킷의 통과여부를 결정하기 위해 프로토콜 종류, 출발지 또는 목적지 IP 주소, TCP/UDP 포트 번호 등을 이용한다.
2응용 게이트웨이 방식 방화벽은 내부망으로 패킷이 전송되는 것을 방지할 수 있으며 사용자 인증 기능도 제공할 수 있다.
3상태 기반 패킷 검사(SPI) 방식 방화벽은 프로토콜 종류, 출발지 또는 목적지 IP 주소, TCP/UDP 포트 번호 외에 패킷의 데이터 부분에 대한 점검도 수행하지만, nmap 도구에 의해 ACK 스캔을 차단하지 못하는 단점이 있다.
4심층 패킷 분석(DPI) 방식 방화벽은 패킷의 데이터 부분에 포함된 바이러스 등 악성코드를 검사할 수 있다.

▸ 상태 기반 패킷 검사(SPI) 방식 방화벽에 대한 설명이 옳지 않다. SPI는 연결의 상태(세션) 정보를 추적해 패킷 통과 여부를 판단하는 방식으로, 패킷의 데이터 부분(payload)까지 검사하는 것은 SPI가 아니라 심층 패킷 분석(DPI)의 역할이다. 또한 SPI는 세션 상태를 추적하기 때문에 정상 연결 없이 들어오는 ACK 패킷(예: nmap의 ACK 스캔)을 비정상으로

판단해 차단할 수 있어, 차단하지 못한다는 설명도 사실과 다르다.

[26번] 서비스의 가용성과 성능뿐만 아니라 DDoS 공격 대응에도 효과적이서 최근 Anycast DNS가 많이 도입되어 있다. 다음 중 이 기술에 대해 잘못 설명한 것은?

1사용자가 접속에 사용하는 IP 주소의 패킷은 해당 주소를 갖는 가장 가까운 호스트로 라우팅된다.
2주요 라우팅 프로토콜로 OSPF가 사용된다.
3IPv4/IPv6 anycast 모두 적용 가능하다.
41.1.1.1이나 8.8.8.8

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, 분석을 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 9바이트를 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.

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 원형 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 시스템에 자신을 복제하는 방식으로 원형 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,