2019년 정보보안기사 필기 기출문제

전 회차 · 57문항 · 정답·해설 포함

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

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 자체는 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 계

열 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 공

유 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