2020년 정보보안기사 필기 기출문제

전 회차 · 54문항 · 정답·해설 포함

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

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 감지하면 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 로그인 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 ◆