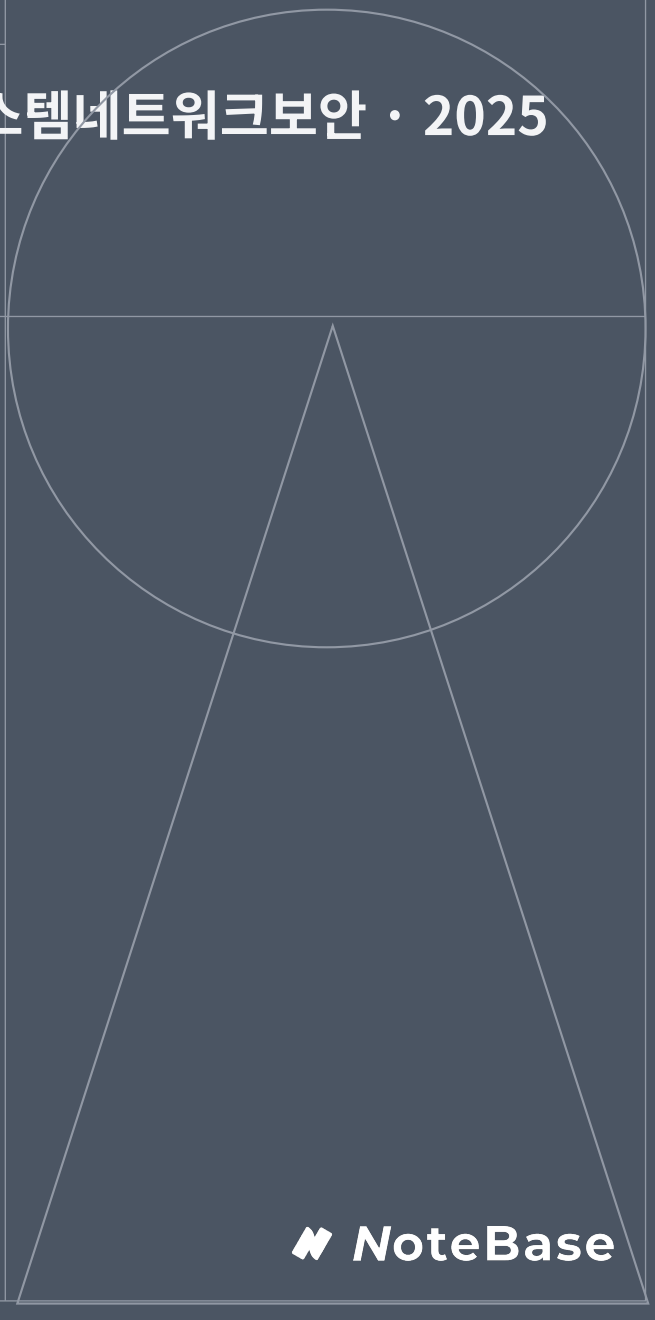
기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2025



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2025

공무원/경찰/경력채용 · 시스템네트워크보안 · 2025

문 1. ext4 파일 시스템의 슈퍼블록에 저장되는 파일 시스템 관련 정보로 가장 적절하지 않은 것은?

① 블록의 크기

② 디렉터리의 개수

③ 파일시스템 상태

④ 전체 inode의 개수

정답 2번

간단한 해설

ext4의 **디렉터리 개수는 블록 그룹 디스크립터**에 기록된다. 슈퍼블록에는 블록 크기, 파일 시스템 상태, 전체 inode 개수 등 파일 시스템 전반의 정보가 저장된다.

선지별 해설

① O: 슈퍼블록에는 **블록 크기를 결정하는 정보**가 저장된다. ext4의 s_log_block_size 필드가 이에 해당하며, 파일 시스템의 블록을 해석하는 데 사용된다.

② X: **디렉터리 개수는 블록 그룹 디스크립터**에서 그룹별로 관리하는 정보이다. bg_used_dirs_count_lo와 필요한 경우 bg_used_dirs_count_hi에 기록되며, 디스크에 저장되는 ext4 슈퍼블록의 전체 디렉터리 개수 필드는 아니다.

③ O: 슈퍼블록의 **s_state는 파일 시스템 상태**를 나타낸다. 파일 시스템이 정상적으로 정리되었는지 또는 오류가 있는지 등을 표시하는 상태 정보이다.

④ O: 슈퍼블록의 **s_inodes_count는 전체 inode 개수**를 나타낸다. 파일 시스템 전체 규모를 설명하는 메타데이터로, 각 블록 그룹의 디렉터리 개수와 구별된다.

NoteBase

문 2. 유닉스/리눅스 시스템에서 기록되는 로그에 관한 설명으로 가장 적절하지 않은 것은?

① lastlog - 가장 최근에 실행한 명령어 및 작업

② pacct - 시스템에 로그인한 사용자의 명령어 실행 여부 및 작업에 대한 사용 내역

③ btmp - 로그인 실패에 대한 내역

④ utmp - 시스템에 현재 로그인한 사용자에 대한 상태정보

정답 1번

간단한 해설

lastlog는 **사용자별 마지막 로그인**에 관한 기록이다. 최근 실행한 명령어와 작업 내역을 기록하는 로그로 설명한 부분이 잘못되었다.

선지별 해설

① X: lastlog는 사용자별 **마지막 로그인 정보**를 기록한다. 최근 로그인 시각이나 접속 터미널 등을 확인하는 자료이며, 가장 최근에 실행한 명령어나 작업을 기록하는 로그가 아니다. 명령 실행 및 프로세스 사용 내역은 프로세스 회계 기록과 구별해야 한다.

② O: pacct는 프로세스 회계 기능이 활성화된 경우 명령 실행과 프로세스의 자원 사용 내역 등을 기록하는 파일이다. 일반적으로 프로세스가 종료될 때 명령 이름, 실행 사용자, 사용 시간 등의 회계 정보가 남는다. 사용자가 입력한 모든 셸 명령문을 원문 그대로 저장하는 명령 이력과는 다르다.

③ O: btmp는 **실패한 로그인 시도**의 내역을 기록한다. 정상 로그인 이력이나 현재 접속자 상태와 구별되는 실패 기록이다. 실제 기록 여부와 위치는 로그인 프로그램 및 시스템 설정에 영향을 받는다.

④ O: utmp는 **현재 로그인한 사용자와 세션의 상태**를 나타내는 기록이다. 과거 로그인·로그아웃 이력을 누적하는 wtmp와 구별하며, 현재 접속자 확인에 이용한다.

NoteBase

문 3. 물리적 망 분리에 관한 설명으로 가장 적절하지 않은 것은?

① 업무용과 인터넷용 네트워크 분리 구성

② 업무자료 유출의 근본적 방지

③ 사용자가 2대의 PC를 사용하고 네트워크도 2개로 분리하는 방식

④ CBC(Client Based Computing) 방식과 SBC(Server Based Computing) 방식으로 구분

정답 4번

간단한 해설

물리적 망 분리는 업무용과 인터넷용 **단말·네트워크를 물리적으로 나누는 방식**이다. CBC와 SBC는 **논리적 망 분리**의 구분에 해당한다.

선지별 해설

① O. 물리적 망 분리는 **업무용 네트워크와 인터넷용 네트워크를 물리적으로 분리**하여 직접적인 통신 경로를 차단하는 구성이다. 단순히 같은 망에서 계정이나 프로그램만 구별하는 것과 다르다.

② O. 문항의 '근본적 방지'는 **인터넷과 업무망 사이의 직접 연결 경로를 제거하여 업무자료 유출 위험을 줄이는 목적**을 뜻한다. 모든 유출을 완전히 방지한다는 보장은 아니며, 이동식 매체·내부자·망간 자료전송 경로에는 별도의 통제가 필요하다.

③ O. 사용자가 **업무용 PC와 인터넷용 PC를 각각 두고 네트워크도 별도로 구성**하는 방식은 대표적인 물리적 망 분리이다. 두 환경의 단말과 접속망을 함께 분리한다는 점이 핵심이다.

④ X. **CBC와 SBC는 논리적 망 분리**의 대표적인 구분이다. CBC는 클라이언트 측에서 실행 환경을 분리하고, SBC는 서버 측에서 제공되는 분리된 실행 환경에 접속하는 방식이다. 별도의 물리적 PC·망을 두는 물리적 망 분리의 분류로 제시한 점이 잘못이다.

따라서 물리적 망 분리의 설명으로 가장 적절하지 않은 것은 ④이다.

NoteBase

문 4. 신뢰 플랫폼 모듈(TPM)에 관한 특징으로 가장 적절하지 않은 것은?

① 훼손 방지(Tamper Protection) 제공

② 하드웨어 TPM은 소프트웨어 방식의 공격과 물리적인 도난에 안전

③ 설정정보를 암호화하여 강화된 보안 제공

④ 암호화 키의 생성/저장, 패스워드 저장, 무결성 검증 값 저장

정답 3번

간단한 해설

TPM의 대표적인 설정정보 보호 원리는 설정을 암호문으로 바꾸는 것이 아니라 **해시 측정값을 기록하여 무결성을 확인**하는 것이다. 이를 비밀정보의 암호화·봉인 기능과 구별해야 한다.

선지별 해설

① O: 하드웨어 TPM은 내부의 키와 보안 기능을 보호하기 위해 **변조·훼손에 대한 저항성**을 제공한다. 이는 공격을 어렵게 하는 보안 특성이며 모든 물리 공격을 완전히 막는다는 의미는 아니다.

② O: 키와 중요한 보안 연산을 일반 소프트웨어 실행 환경에서 분리하므로 악성코드에 의한 키 추출을 어렵게 한다. 장치나 저장장치를 도난당한 경우에도 TPM에 결합된 키와 접근 조건이 비밀정보 보호에 기여한다. 여기서 '안전'은 하드웨어 기반 보호를 제공한다는 취지이며 장치 도난 자체를 방지하거나 모든 물리 공격에 절대 안전하다는 뜻은 아니다.

③ X: 플랫폼 설정정보의 무결성 보호 기능을 설명한 것으로 보면, '설정정보를 암호화'한다는 표현은 핵심 원리와 다르다. 소프트웨어와 설정정보의 **해시 측정값을 PCR에 기록**하고 예상 상태와의 일치 여부에 따라 키 사용 등을 통제한다. 암호화가 내용을 숨기는 데 초점을 두는 것과 달리 이 기능은 설정이 바뀌었는지를 확인하는 데 초점을 둔다. TPM이 별도로 키 암호화나 데이터 봉인 기능을 지원하지 않는다는 뜻은 아니다.

④ O: TPM은 암호키를 생성·보호하고, 암호나 인증에 필요한 비밀정보를 보호하는 데 사용되며, 플랫폼 무결성 검증에 필요한 측정값을 보관한다. 패스워드 저장은 모든 응용프로그램의 암호를 평문으로 모아 두는 기능이 아니라 인증용 비밀정보의 보호라는 의미로 이해한다.

NoteBase

문 6. 다음에서 설명하는 공격으로 가장 적절한 것은?

· Smurfing Attack이라고도 함
· 전체 대역폭을 점유하여 네트워크를 마비시킴
· 위조된 IP 패킷과 브로드캐스트 IP 주소를 이용하여 네트워크나 시스템에 과부하를 일으키는 공격

① Tear Drop
② Land Attack
③ TCP SYN Flooding
④ ICMP Flooding

정답 4번

간단한 해설

Smurf 공격은 **위조된 출발지 주소와 브로드캐스트**를 이용해 다수의 ICMP 응답을 피해자에게 집중시킨다. 제시된 선택지 중에서는 ICMP Flooding으로 분류할 수 있다.

핵심 풀이

제시문은 **출발지 IP 위조와 브로드캐스트**를 이용하는 Smurf 공격을 설명한다. 피해자의 IP 주소를 출발지로 가장한 ICMP Echo Request가 브로드캐스트로 전달되면, 여러 호스트의 응답이 피해자에게 집중되어 대역폭과 처리 자원을 소모한다. 따라서 제시된 선택지에서는 ④ ICMP Flooding에 해당한다.

Smurf는 **ICMP를 이용한 반사·증폭형 공격**의 한 형태이다. 모든 ICMP Flooding이 반드시 Smurf처럼 브로드캐스트를 사용하는 것은 아니므로, 제시문의 표현은 이 공격 유형을 가리키는 맥락으로 이해해야 한다. Tear Drop은 IP 단편 재조립, Land Attack은 출발지와 목적지 주소·포트를 같게 한 패킷, TCP SYN Flooding은 연결 설정 대기 상태의 자원 소모와 관련되어 핵심 기법이 다르다.

NoteBase

문 7. ESM(Enterprise Security Management)의 주요 업무로 가장 적절하지 않은 것은?

① 정보보안 정책을 등록하고 자산 및 자원을 관리한다.

② 실시간 종합 관제 지원으로 침입 발생 시 탐지가 가능하다.

③ 침입 경고 전에 공격 중단 기능이 주요 목적이다.

④ 실시간 보안감사, 위험도 추론 침입탐지, 상관성 분석을 지원한다.

정답 3번

간단한 해설

ESM의 핵심은 보안 장비·정책·이벤트를 모아 **통합 관리하고 관제·분석**하는 것이다. 직접적인 공격 차단을 주된 목적으로 하는 IPS와 구별해야 한다.

선지별 해설

① O. ESM은 여러 보안 시스템을 **통합 관리**하기 위한 체계이다. 정보보안 정책을 등록·관리하고 관리 대상 자산과 보안 자원을 파악하는 업무가 그 범위에 포함된다.

② O. 여러 장비에서 발생하는 보안 이벤트를 모아 **실시간 종합 관제**를 지원한다. 개별 장비의 탐지 결과와 상태를 함께 확인하므로 침입 발생 징후를 통합적으로 파악할 수 있다.

③ X. 공격 트래픽을 즉시 차단하여 **침입을 방지하는 것**을 주된 목적으로 하는 것은 IPS의 역할에 가깝다. ESM의 중심은 보안 장비·정책·이벤트의 통합 관리와 관제·분석이다. ESM이 다른 장비와 연계하여 대응을 지시할 수 있다는 사실과, 직접적인 공격 중단을 주요 목적으로 한다는 설명은 구별해야 한다.

④ O. ESM은 보안 로그와 이벤트를 활용한 **보안감사, 위험도 평가, 침입 징후 분석 및 상관성 분석**을 지원할 수 있다. 서로 다른 장비에서 나온 정보를 연관 지어 분석하면 개별 이벤트만 보았을 때 놓칠 수 있는 위협을 파악하는 데 도움이 된다.

따라서 ESM의 주요 업무로 가장 적절하지 않은 것은 ③이다.

NoteBase

문 8. VPN(Virtual Private Network)에서 동일한 OSI 계층을 사용하는 터널링(tunneling) 프로토콜을 연결한 것으로 가장 적절한 것은?

① PPTP - IPSec

② L2TP - IPSec

③ PPTP - L2TP

④ L2TP - SOCKS

정답 3번

간단한 해설

PPTP와 L2TP는 모두 **데이터 링크 계층(2계층) 터널링** 프로토콜이다. 터널을 운반할 때 사용하는 하위 네트워크나 전송 프로토콜이 아니라, 터널링 대상 계층을 기준으로 구분한다.

선지별 해설

① X: PPTP는 PPP 프레임을 터널링하는 **데이터 링크 계층(2계층)** 방식이고, IPSec은 IP 패킷을 보호하는 **네트워크 계층(3계층)** 보안 방식이다. 두 프로토콜은 같은 계층으로 분류되지 않는다.

② X: L2TP는 **2계층 터널링** 프로토콜이고 IPSec은 **3계층** 보안 프로토콜이다. L2TP의 통신을 IPSec으로 보호하는 결합 방식이 존재하더라도, 두 프로토콜 자체의 계층이 같다는 뜻은 아니다.

③ O: PPTP와 L2TP는 모두 **PPP 기반의 2계층 터널링** 프로토콜이다. 다른 네트워크 위로 PPP 트래픽을 운반하므로, VPN의 터널링 대상 계층을 기준으로 동일한 계층에 분류된다.

④ X: L2TP는 **데이터 링크 계층**의 터널링 방식이다. SOCKS는 응용 계층과 전송 계층 사이에서 통신을 중계하는 프록시 프로토콜로, L2TP와 같은 2계층 터널링 방식이 아니다.

NoteBase

문 9. 다음에서 설명하고 있는 버퍼 오버플로우(Buffer Overflow) 방지기술로 가장 적절한 것은?

메모리 공격을 방어하려고 주소 공간 배치를 난수화하는 기법으로, 스택, 힙, 라이브러리 등의 데이터 영역 주소 등을 난수화하여 프로세스의 주소 공간에 배치한다.

① rtl(return to libc)
② 스택 실드
③ 스택 가드
④ ASLR

정답 4번

간단한 해설

스택·힙·라이브러리 등의 배치 주소를 무작위화하는 기법은 **ASLR**이다. 공격자가 사용할 메모리 주소를 예측하기 어렵게 하여 메모리 취약점 악용을 방해한다.

핵심 풀이

ASLR은 주소 공간 배치 난수화 기법이다. 스택·힙·라이브러리 등의 배치 주소를 예측하기 어렵게 바꾸어, 공격자가 목표 코드나 데이터의 정확한 주소를 알아야 하는 메모리 공격의 성공을 어렵게 한다. 제시문의 **주소 공간 배치를 난수화**한다는 표현이 결정적인 단서이다.

스택 가드는 스택에 카나리라는 검사용 값을 두고 함수가 반환될 때 값이 바뀌었는지 검사하는 방식이다.

스택 실드는 반환 주소를 별도로 보호·보관하여 반환 주소 변조를 막는 계열의 기법이다. 둘 다 스택 보호와 관련되지만 주소 공간 전체의 배치를 난수화한다는 설명과는 다르다.

rtl(return to libc)은 이미 존재하는 라이브러리 코드를 이용하도록 제어 흐름을 바꾸는 코드 재사용 공격 기법이다. 주소 난수화를 수행하는 방어 기술이 아니다.

ASLR은 메모리의 범위를 벗어나는 쓰기 자체를 제거하는 것은 아니므로, 버퍼 오버플로우 취약점의 수정과는 구별된다. 제시된 주소 예측 방해 기법에 해당하는 선택지는 ④ ASLR이다.

NoteBase

문 10. 리눅스 디렉터리 구조와 설명이 올바르지 않은 것은?

① /bin : 기본적인 실행 명령 모음

② /sbin : 장치 파일 모음

③ /lib : 라이브러리 모음

④ /etc : 시스템 설정파일 모음

정답 2번

간단한 해설

/sbin은 시스템 관리 명령을 두는 곳이고, **장치 파일은 /dev**에 둔다. /bin은 기본 실행 명령, /lib는 필수 라이브러리, /etc는 시스템 설정 파일에 대응한다.

선지별 해설

① O. /bin은 사용자가 이용하는 **필수 실행 명령**을 두는 디렉터리이다. 기본 명령 모음이라는 설명이 맞다.

② X. /sbin은 부팅·복구·관리 등에 필요한 **시스템 관리 명령**을 두는 디렉터리이다. 장치 파일을 모아 두는 디렉터리는 **/dev**이므로 제시된 연결은 틀리다.

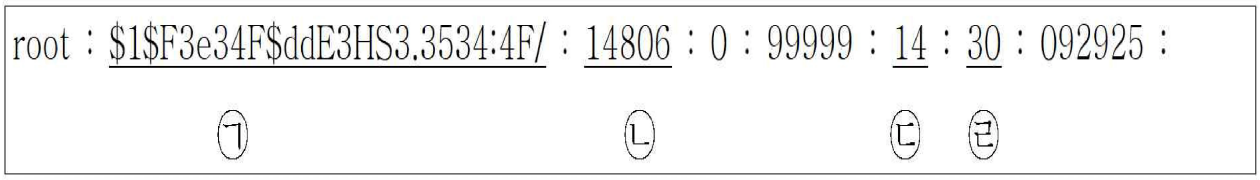
③ O. /lib는 시스템 부팅과 기본 명령 실행에 필요한 **공유 라이브러리** 등을 두는 디렉터리이다. 라이브러리 모음이라는 설명이 맞다.

④ O. /etc는 해당 시스템의 **설정 파일**을 두는 디렉터리이다. 시스템 설정파일 모음이라는 설명이 맞다.

따라서 디렉터리와 설명의 연결이 올바르지 않은 것은 ②이다.

NoteBase

문 11. 다음은 유닉스에서 /etc/shadow 파일의 구성을 나타낸 것이다. ㉠~㉣에 관한 설명으로 가장 적절한 것은?



① ㉠ - 패스워드 서명 값

② ㉡ - 패스워드 변경 전 최대 사용기간

③ ㉢ - 패스워드 사용 만료일 전에 경고 메시지 제공 일수

④ ㉣ - 로그인 계정 만료일

정답 3번

간단한 해설

/etc/shadow에서 여섯 번째 필드는 **패스워드 만료 전 경고 기간**이다. 그림의 ㉢에 있는 14는 만료 14일 전부터 경고한다는 뜻이다.

선지별 해설

/etc/shadow는 콜론으로 필드를 구분한다. 그림의 표시를 필드 순서와 대응시키면 해시 저장 문자열, 마지막 변경일, 경고 기간, 만료 후 비활성화 유예기간을 구별할 수 있다.

① X: 그림의 ㉠은 두 번째 필드로, 패스워드를 검증하기 위한 **해시 기반 저장 문자열**이다. 패스워드 원문이나 공개키 방식의 전자서명 값을 저장하는 필드가 아니다.

② X: ㉡의 14806은 세 번째 필드로, **마지막 패스워드 변경일**을 1970년 1월 1일부터 지난 일수로 나타낸 값이다. 최대 사용기간은 다섯 번째 필드에 있는 99999이다. 그 앞의 0은 최소 사용기간이다.

③ O: ㉢의 14는 여섯 번째 필드인 경고 기간이다. 패스워드가 만료되기 **14일 전부터 경고**를 제공한다는 의미이다. 마지막 변경일이나 최대 사용기간과 달리 만료 전 경고를 시작하는 시점을 정한다.

④ X: ㉣의 30은 일곱 번째 필드로, 패스워드 만료 후 적용되는 비활성화 유예기간을 일수로 나타낸다. 만료 후 이 기간까지 지나면 계정의 로그인이 제한되는 기준으로 쓰인다. 계정 자체의 만료일은 그 다음 여덟 번째 필드이며, 그림에서는 092925가 들어 있는 자리이다.

NoteBase

문 12. Nmap을 이용한 포트 스캔 방법 중 TCP Xmas Scan에서 사용하는 TCP 플래그(flag)로 가장 적절하지 않은 것은?

① URG

② PSH

③ FIN

④ SYN

정답 4번

간단한 해설

Nmap의 TCP Xmas Scan은 **FIN · PSH · URG**를 동시에 설정한다. SYN은 이 조합에 포함되지 않는다.

핵심 풀이

Nmap의 TCP Xmas Scan은 **FIN · PSH · URG** 플래그를 동시에 설정한 탐색 패킷을 사용한다. 따라서 URG, PSH, FIN은 모두 이 스캔의 플래그 조합에 포함된다.

SYN은 Xmas Scan의 조합에 포함되지 않는다. SYN은 TCP 연결 수립 시 시퀀스 번호를 동기화하는 데 쓰이며, SYN Scan의 탐색 패킷에서 사용하는 플래그와 구별해야 한다.

따라서 Nmap의 TCP Xmas Scan에서 사용하는 플래그로 가장 적절하지 않은 것은 ④ SYN이다.

NoteBase

문 13. 다음 아파치 웹서버의 설정파일 설명으로 가장 적절하지 않은 것은?

<Directory />
Options Indexes FollowSymLinks
AllowOverride All
Order allow, deny
Allow from all
Deny from all
</Directory>

① 심볼릭 링크를 사용하도록 설정했다.

② 디렉터리에 인증을 통한 접근을 하기 위해 .htaccess 파일을 사용하도록 설정했다.

③ 모든 클라이언트로부터 요청을 허용하도록 설정했다.

④ DirectoryIndex에서 지정한 파일이 없으면 디렉터리에 존재하는 하위 디렉터리 및 파일의 목록을 보여주도록 설정했다.

정답 3번

간단한 해설

문항이 의도한 **Allow,Deny 평가 순서**에서는 Deny from all이 최종 적용되어 모든 접근이 거부되므로 ③이 적절하지 않다. 원문의 쉼표 뒤 공백은 실제 Apache 지시어 문법에 맞지 않는 별도 표기 문제이다.

NoteBase

선지별 해설

원문에는 Order allow, deny처럼 쉼표 뒤 공백이 있으나, 실제 지시어 문법은 **Order allow,deny**처럼 공백 없이 써야 한다. 아래는 원문을 정상 실행 가능한 설정으로 단정하는 것이 아니라, 제시된 허용→거부 순서의 구식 접근제어 규칙이 뜻하는 바를 풀이한 것이다. Apache 2.4에서는 이 구식 지시어에 mod_access_compat가 필요하다.

① O: Options의 **FollowSymLinks**는 해당 디렉터리 범위에서 심볼릭 링크를 따라가도록 허용하는 옵션이다. 파일의 실제 접근 가능 여부는 별도의 접근제어와 파일 권한에도 영향을 받는다.

② O: **AllowOverride All**은 .htaccess에서 허용 가능한 설정 범주를 모두 사용할 수 있게 하므로, 인증 관련 지시어도 .htaccess에 둘 수 있다. 다만 이 한 줄만으로 사용자 인증이 이미 설정되었다는 뜻은 아니며, 실제 인증에는 별도의 인증 지시어와 사용자 정보 등이 필요하다.

③ X: 의도된 **Allow,Deny 순서에서는 Allow 규칙을 먼저, Deny 규칙을 나중에 평가**한다. Allow from all에 일치하더라도 Deny from all에도 일치하므로, 이 규칙 범위에서는 최종적으로 모든 클라이언트의 접근이 거부된다. 따라서 모든 요청을 허용한다는 설명은 적절하지 않다. 단순히 설정파일에 쓰인 줄의 선후만으로 우선순위를 판단해서는 안 된다.

④ O: **Indexes**는 DirectoryIndex에 해당하는 파일이 없을 때 디렉터리 목록을 생성하는 기능을 허용한다. 이는 목록 생성 옵션의 의미이며, 접근이 거부된 요청에도 목록이 표시된다는 뜻은 아니다. 실제 제공에는 접근 허용과 관련 모듈 등 조건이 충족되어야 한다.

NoteBase

문 14. 다음 중 링크 상태(Link State) 기반 라우팅 프로토콜로 옳은 것은 모두 몇 개인가?

㉠ RIP ㉡ BGP ㉢ OSPF ㉣ EIGRP ㉤ IGRP

① 1개
② 2개
③ 3개
④ 4개

정답 1번

간단한 해설

제시된 프로토콜 중 **링크 상태 기반은 OSPF**이다. EIGRP는 향상된 거리 벡터 방식이고, BGP는 경로 벡터 방식으로 구별한다.

보기별 해설

㉠ X: RIP는 홉 수를 기준으로 경로를 판단하는 **거리 벡터** 방식이다. 링크 상태 정보를 모아 전체 토폴로지를 구성하는 방식과 다르다.

㉡ X: BGP는 AS 경로와 여러 경로 속성을 이용하는 **경로 벡터** 방식이다. 링크 상태 기반 프로토콜로 분류하지 않는다.

㉢ O: OSPF는 **링크 상태** 정보를 교환하여 토폴로지 데이터베이스를 구성하고 SPF 알고리즘으로 경로를 계산한다. 따라서 제시된 항목 중 조건에 해당한다.

㉣ X: EIGRP는 DUAL 알고리즘을 사용하는 **향상된 거리 벡터** 방식이다. 하이브리드라고 소개되기도 하지만, 그 표현만으로 OSPF와 같은 링크 상태 기반 프로토콜로 분류해서는 안 된다.

㉤ X: IGRP는 대역폭·지연 등을 반영한 복합 메트릭을 사용하는 **거리 벡터** 방식이다. 메트릭이 복합적이라는 이유로 링크 상태 방식이 되는 것은 아니다.

링크 상태 기반은 ㉢ **OSPF 하나**이므로, 개수는 1개인 ①과 연결된다.

NoteBase

문 15. 다음에서 설명하는 봇넷(botnet)의 보안장비 우회 방법으로 가장 적절한 것은?

하나의 C&C(Command and Control) 서버 도메인에 다수의 IP주소를 할당하여 DNS 질의 시마다 지속적으로 IP 주소가 변경되도록 하는 방법이다.

① FastFlux DNS
② DGA(Domain Generation Algorithm)
③ Domain Shadowing
④ DNS Sinkhole

정답 1번

간단한 해설

하나의 도메인은 유지하면서 연결되는 **IP 주소를 빠르게 교체**하는 방식은 FastFlux DNS이다. 도메인 이름 자체를 대량 생성하는 DGA와 구별된다.

핵심 풀이

FastFlux DNS는 **같은 도메인에 연결되는 IP 주소를 빠르게 바꾸는** 기법이다. 제시문은 하나의 C&C 서버 도메인을 유지하면서 여러 IP 주소가 번갈아 연결되도록 하므로 이 기법에 해당한다. 고정된 IP 주소만을 기준으로 차단하거나 실제 통신 기반을 추적하기 어렵게 만드는 특성이 있다.

DGA는 알고리즘으로 다수의 도메인 이름을 생성하는 방식이다. 제시문의 핵심은 도메인 이름 생성이 아니라 **동일 도메인의 IP 주소 변경**이므로 구별된다.

Domain Shadowing은 탈취한 도메인 관리 권한 등을 악용하여 정상 도메인 아래에 악성 하위 도메인을 만드는 방식이다.

DNS Sinkhole은 악성 도메인에 대한 통신을 통제된 목적지로 유도하여 차단·관찰하는 방어 기법이다. 둘 다 제시된 IP 주소 교체 방식의 명칭은 아니다.

DNS 캐시와 갱신 시점에 따라 모든 질의에서 반드시 서로 다른 IP가 반환되는 것은 아니다. 여기서는 연결 IP가 빠르게 계속 바뀐다는 특징으로 해석하며, 이에 해당하는 선택지는 ① FastFlux DNS이다.

NoteBase

문 16. SSL/TLS 프로토콜에 관한 설명으로 가장 적절하지 않은 것은?

① Handshake Protocol - 서버와 클라이언트가 서로 인증하고 암호화 알고리즘과 암호키를 협상한다.

② Record Protocol - 신뢰하는 전송서비스를 필요로 하며, TCP 프로토콜을 사용한다.

③ Alert Protocol - SSL/TLS 통신과정에서 발생하는 오류를 통보하기 위해 사용한다.

④ HeartBeat Protocol - 정상적인 동작을 위해 소프트웨어상에서 신호를 생성하며, 개체의 무결성을 위해 사용한다.

정답 4번

간단한 해설

Heartbeat는 **상대방의 응답 가능 여부와 연결 유지**를 확인하는 기능이다. 개체가 변조되지 않았음을 검사하는 무결성 검증과는 목적이 다르다.

선지별 해설

① O: Handshake Protocol은 통신 상대를 인증하고 **암호 알고리즘과 키 생성에 필요한 보안 매개변수**를 협상하는 절차이다. 상호 인증을 지원하지만, 실제 연결에서 클라이언트 인증까지 항상 필수인 것은 아니다.

② O: 일반적인 SSL/TLS의 Record Protocol은 **TCP와 같은 신뢰성 있는 전송 서비스** 위에서 동작한다. 상위 프로토콜의 데이터를 레코드로 나누고 협상된 보안 방식으로 보호하며, 데이터그램 전송을 위한 DTLS와는 구별된다.

③ O: Alert Protocol은 통신 중 발생한 **오류와 경고 등 상태**를 상대방에게 알리는 데 사용된다. 정상적인 연결 종료를 알리는 통지도 포함하므로, 오류 통보만이 유일한 용도는 아니다.

④ X: Heartbeat 확장은 요청과 응답으로 **상대방이 응답 가능한지 확인하고 연결을 유지**하는 기능을 제공한다. 개체의 데이터나 소프트웨어가 변조되지 않았음을 보증하는 무결성 검증 프로토콜이 아니다. 따라서 목적을 개체의 무결성 보장으로 설명한 부분이 잘못이다.

NoteBase

문 17. 다음의 데이터베이스 암호화 방법에서 블록암호화 방식으로 옳은 것을 모두 고른 것은?

㉠ TDE 방식 ㉡ 플러그-인 방식
㉢ 파일 암호화 방식 ㉣ 하이브리드 방식 ㉤ API 방식

① ㉠㉡
② ㉠㉢
③ ㉡㉣㉤
④ ㉢㉣㉤

정답 2번

간단한 해설

이 문제는 암호 알고리즘이 아니라 **데이터베이스 암호화의 적용 단위**를 구분한다. 제시된 분류에서는 TDE와 파일 암호화가 저장 블록 단위 방식에 해당한다.

보기별 해설

㉠ O: 이 분류에서 TDE는 DBMS 내부에서 **저장 블록 단위**로 암·복호화를 처리하는 방식을 뜻한다. 예를 들어 테이블스페이스 암호화가 이에 해당한다. 다만 제품에 따라 TDE라는 이름으로 컬럼 암호화도 제공하므로, 모든 TDE 기능이 반드시 블록 단위라는 뜻은 아니다.

㉡ X: 플러그-인 방식은 DB 서버에 암호화 기능을 추가하여 **선택한 컬럼** 등의 데이터를 암·복호화하는 방식으로 분류한다. 저장 파일 전체의 블록 단위 암호화와 구별한다.

㉢ O: 파일 암호화 방식은 운영체제·파일 계층에서 **데이터 파일의 입출력**을 암·복호화한다. 이 문제의 구분에서는 DB의 개별 컬럼이 아니라 저장 블록을 보호하는 범주에 해당한다.

㉣ X: 여기서 하이브리드 방식은 **플러그-인과 API 방식을 결합**하는 유형이다. 이를 별도의 블록 단위 암호화 방식으로 고르지는 않는다.

㉤ X: API 방식은 응용 프로그램이 **암·복호화 함수를 호출**하여 보호할 데이터를 처리하는 방식이다. 이 분류에서는 컬럼 단위 암호화 쪽에 속한다.

해당하는 것은 **㉠과 ㉢**이므로 ②와 연결된다. 여기서 블록 암호화는 데이터베이스에 적용하는 단위의 구분이며, AES 같은 블록 암호 알고리즘을 사용하는지 여부를 묻는 것이 아니다.

NoteBase

문 18. 다음에서 설명하는 프로토콜로 가장 적절한 것은?

· 시스템 운영 또는 보안사고 발생으로 인한 로그 분석 과정에서 이벤트 간의 인과관계 파악에 도움을 주기 위해 사용한다.
· 보안사고 및 장애 발생 시 로그에 대한 신뢰도를 확보하기 위해 사용한다.
· 1985년 RFC 958로 제안된 프로토콜로 현재 RFC 5905로 대체되었다.

① TIME 프로토콜
② TLS(Transport Layer Secure)
③ SNMP(Simple Network Management Protocol)
④ NTP(Network Time Protocol)

정답 4번

간단한 해설

시스템 간 **시각을 동기화**하여 로그의 시간 순서를 비교하도록 돕는 프로토콜은 NTP이다. 특히 **RFC 958과 RFC 5905**가 NTP를 식별하는 결정적 단서이다.

NoteBase

핵심 풀이

여러 시스템의 로그를 비교하려면 **시각 기준이 일치**해야 한다. NTP는 네트워크를 통해 시스템 시계를 동기화하여 이벤트의 시간 순서를 비교하고 인과관계를 분석하는 데 도움을 준다. 시각의 일관성은 로그 신뢰성의 한 요소이지만, NTP만으로 로그 내용의 무결성이나 모든 인과관계가 보장되는 것은 아니다.

제시문의 **RFC 958과 RFC 5905**가 결정적 단서이다. 1985년 RFC 958은 NTP를 제안했고, RFC 5905는 NTP 버전 4를 규정한다. 중간 버전들을 거쳐 발전한 계보이며, RFC 5905가 문서상 직접 폐기 대상으로 명시한 것은 RFC 1305와 RFC 4330이다.

① TIME은 시각 정보를 제공하는 별개의 간단한 프로토콜이다. 시간과 관련된다는 점만으로는 부족하며, 제시된 RFC 번호와 맞지 않는다.

② TLS는 통신 구간의 보안을 위한 프로토콜이지 시계 동기화 프로토콜이 아니다. 선지의 영문 풀이는 Secure로 적혀 있으나 정식 명칭은 **Transport Layer Security**이다.

③ SNMP는 네트워크 장비의 상태와 관리 정보를 조회·관리하는 프로토콜이다. 제시된 시계 동기화 및 RFC 계보와 구별된다.

④ NTP는 Network Time Protocol로, 시스템 시계 동기화와 제시된 RFC 계보를 모두 만족한다.

따라서 설명에 가장 적절한 것은 ④ NTP이다.

NoteBase

문 19. 다음의 공격 대상이 되는 프로토콜의 설명으로 가장 적절하지 않은 것은?

할당 가능한 IP 주소를 모두 소진하게 만들어 IP 주소 할당이 불가능하게 하는 공격으로 discover 메시지를 서로 다른 MAC 주소에 대량으로 보내고, offer 메시지가 오면 request 메시지를 보낸 후에 실제로는 할당하지 않는다.

① 실제로 호스트를 사용하는 경우에만 IP 주소가 할당되기 때문에 IP 주소가 절약된다.

② 사설 주소와 범용 주소의 매핑을 제공하고 동시에 가상 사설 네트워크를 지원한다.

③ 클라이언트는 부팅 시 브로드캐스트 방식으로 트래픽을 전송하므로 네트워크 성능저하를 발생시킨다.

④ 호스트 전원을 꺼도 IP 주소 임대 기간까지 해당 IP 주소는 다른 단말에 할당되지 못하여, IP 주소 낭비가 발생한다.

정답 2번

간단한 해설

대상은 주소를 임대하는 **DHCP**이다. 사설·공인 주소 변환은 NAT, 가상 사설망 구성은 VPN의 영역이므로 이를 DHCP의 기능으로 설명한 ②가 적절하지 않다.

NoteBase

선지별 해설

DISCOVER·OFFER·REQUEST 메시지와 주소 풀 소진은 **DHCP 고갈 공격**의 단서이다. 원문의 “서로 다른 MAC 주소에”와 “실제로는 할당하지 않는다”는 표현은 부정확하다. 핵심은 서로 다른 클라이언트 MAC 주소 등으로 가장해 임대를 점유하고, 그 주소를 실제 정상 호스트의 통신에 쓰지 않아 가용 주소를 소진시키는 것이다. 서버의 임대가 전혀 생기지 않는다는 뜻으로 이해해서는 안 된다.

① O: DHCP의 **동적 할당**은 요청한 호스트에 주소를 일정 기간 임대하고 반납되거나 만료된 주소를 다시 활용하므로, 모든 호스트에 고정 주소를 계속 확보해 두는 방식보다 주소 이용 효율을 높일 수 있다. 사용 중에만 임대가 존재하거나 전원을 끄면 즉시 회수된다는 뜻은 아니다.

② X: DHCP는 **IP 주소와 서브넷 마스크·게이트웨이 등의 설정을 전달하는 프로토콜**이다. 사설 주소와 공인 주소 사이의 매핑은 NAT의 기능이며, VPN은 별도의 터널링 등으로 가상 사설망을 구성한다. 한 장비가 이 기능들을 함께 제공할 수는 있지만, 주소 변환과 VPN 자체가 DHCP의 기능은 아니다.

③ O: 주소가 없는 클라이언트가 서버를 찾는 초기 DHCPDISCOVER 등은 일반적으로 **브로드캐스트**를 사용하므로 같은 브로드캐스트 도메인에 처리 부하를 줄 수 있다. 대량 요청이나 재전송은 성능에 영향을 주지만, 정상적인 소량 DHCP 교환만으로 항상 체감 성능 저하가 발생한다거나 모든 DHCP 메시지가 브로드캐스트인 것은 아니다.

④ O: 클라이언트가 **임대를 반납하지 않고** 전원을 끄면 서버의 임대 정보가 곧바로 사라지는 것은 아니다. 유효한 임대가 유지되는 동안 같은 주소를 다른 단말에 중복 할당할 수 없어 사용되지 않는 주소가 남을 수 있다. 반납되거나 임대 기간이 만료되면 재할당할 수 있다.

NoteBase

문 20. 악성코드가 시스템 재부팅 시 악성 프로그램을 구동시키기 위해 변조하는 레지스트리로 가장 적절하지 않은 것은?

① HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

② HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

③ HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

④ HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

정답 1번

간단한 해설

Run과 RunOnce는 **사용자 로그온 시 자동 실행**에 쓰이는 대표적인 레지스트리 위치이다. 제시된 Explorer 키 자체는 이와 같은 자동 실행 목록 키로 구분하지 않는다.

핵심 풀이

이 문제는 레지스트리의 **로그온 시 자동 실행 위치**를 구별하는 문제이다. Run은 사용자 로그온 때 프로그램을 실행하는 데 쓰이고, RunOnce는 기본적으로 한 번 실행할 항목을 다룬다. 따라서 재부팅이라는 표현은 여기서 재부팅 뒤 사용자 로그온으로 이어지는 상황을 포함해 이해해야 한다.

②의 HKEY_LOCAL_MACHINE 아래 Run은 컴퓨터 범위의 자동 실행 설정이고, ③의 HKEY_CURRENT_USER 아래 Run은 해당 사용자 범위의 자동 실행 설정이다.

④의 HKEY_CURRENT_USER 아래 RunOnce 역시 해당 사용자의 로그온과 관련된 일회성 실행 위치이므로, 모두 악성코드가 악용할 수 있는 자동 실행 지점이다.

①에서 제시한 CurrentVersion 아래 Explorer 키 자체는 **Run·RunOnce와 같은 표준 자동 실행 목록 키가 아니다**. 따라서 제시된 네 경로 중 목적에 가장 적절하지 않은 것은 ①이다. 다만 Explorer와 관련된 모든 하위 설정이 보안상 무관하거나 다른 자동 실행 악용이 전혀 불가능하다는 뜻은 아니다.

NoteBase