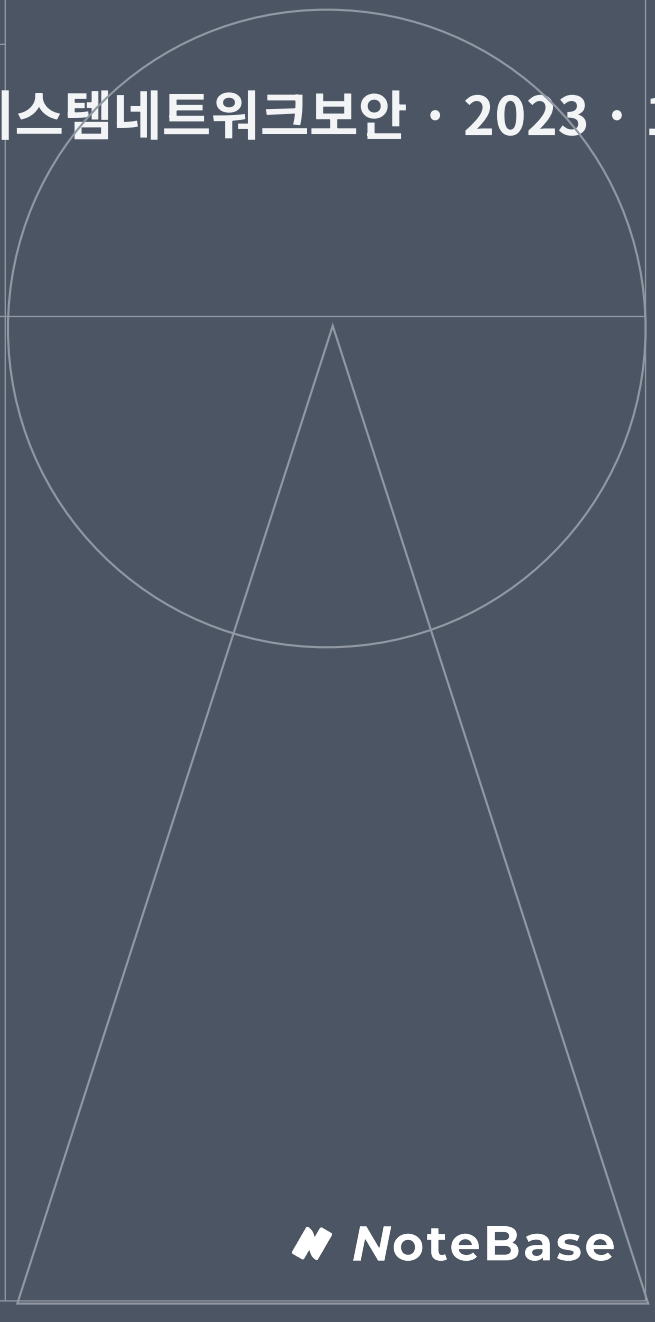
# 기출OX 해설집

공무원/경찰/공채(순경) · 시스템네트워크보안 · 2023 · 1차



NoteBase

# 기출OX 해설집

## 공무원/경찰/공채(순경) · 시스템네트워크보안 · 2023 · 1차

### 공무원/경찰/공채(순경) · 시스템네트워크보안 · 2023 · 1차

**문 1. Linux의 i-node가 가지고 있지 않은 정보는?**

① 파일의 이름
② 파일의 유형
③ 파일의 링크 수
④ 마지막으로 수정된 시간

**정답 1번**

**출제 포인트**

Linux의 i-node에 저장되는 파일 메타데이터와 디렉터리 엔트리에 저장되는 파일 이름을 구분하는 문제이다.

**핵심 개념**

i-node는 파일 유형·권한, 링크 수, 소유자, 크기, 시간 정보, 데이터 블록 위치 등 파일의 메타데이터를 저장하는 구조이다. 파일 이름은 i-node가 아니라 디렉터리 엔트리에 i-node 번호와 함께 저장된다.

**선지별 해설**

① O — 파일 이름은 i-node에 저장되지 않고 디렉터리 엔트리에서 해당 i-node 번호와 연결되므로 정답이다.
② X — 파일 유형은 i-node의 모드 정보에 저장된다. ‘i-node가 가지고 있지 않은 정보’가 아니라 ‘i-node가 가지고 있는 정보’로 고쳐야 한다.
③ X — 파일의 링크 수는 해당 i-node를 가리키는 하드 링크의 수를 나타내며 i-node에 저장된다. ‘i-node가 가지고 있지 않은 정보’가 아니라 ‘i-node가 가지고 있는 정보’로 고쳐야 한다.
④ X — 마지막으로 수정된 시간인 mtime은 i-node의 시간 정보에 저장된다. ‘i-node가 가지고 있지 않은 정보’가 아니라 ‘i-node가 가지고 있는 정보’로 고쳐야 한다.

**오답 포인트**

파일 이름도 파일의 속성처럼 보이지만, Linux 파일 시스템에서는 이름이 디렉터리 엔트리에 있고 i-node에는 파일 자체의 메타데이터가 있다는 점이 함정이다.

NoteBase

**다시 나오면 이렇게 판단**

이름과 i-node 번호의 연결은 디렉터리 엔트리, 파일 유형·권한·링크 수·크기·시간·블록 위치는 i-node로 구분한다.

**암기 포인트**

이름은 디렉터리, 속성은 i-node이다.

NoteBase

**문 2. IANA가 정한 사설 IP 주소로 사용하기에 옳지 않은 것은?**

① 10.0.0.0 - 10.255.255.255

② 172.16.0.0 - 172.31.255.255

③ 192.168.0.0 - 192.168.255.255

④ 220.83.33.0 - 220.83.33.255

**정답 4번**

**출제 포인트**

사설 IPv4 주소로 예약된 세 범위와 그 밖의 공인 주소 범위를 구별하는 문제이다.

**핵심 개념**

사설 IPv4 주소는 내부 네트워크에서 사용하도록 예약되어 인터넷에서 직접 라우팅되지 않는 주소이다. 범위는 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16의 세 가지이다.

**선지별 해설**

① O
10.0.0.0 - 10.255.255.255는 10.0.0.0/8에 해당하는 사설 IPv4 주소 범위이다.

② O
172.16.0.0 - 172.31.255.255는 172.16.0.0/12에 해당하는 사설 IPv4 주소 범위이다. 두 번째 옥텟이 16부터 31까지인 주소만 포함된다.

③ O
192.168.0.0 - 192.168.255.255는 192.168.0.0/16에 해당하는 사설 IPv4 주소 범위이다.

④ X
220.83.33.0 - 220.83.33.255는 사설 IPv4 주소로 예약된 범위가 아니다. 틀린 표현은 이 범위를 사설 IP 주소로 본 부분이며, 올바르게는 RFC 1918의 세 사설 범위 밖에 있는 공인 주소 영역이다.

**오답 포인트**

172로 시작하는 모든 주소가 사설 주소라고 생각하기 쉽지만, 172 대역에서는 두 번째 옥텟이 16부터 31까지인 범위만 사설 주소이다. 또한 220.83.33.0처럼 하나의 /24 형태로 제시되어도 익숙한 네트워크 범위라는 이유만으로 사설 주소가 되는 것은 아니다.

NoteBase

### 다시 나오면 이렇게 판단

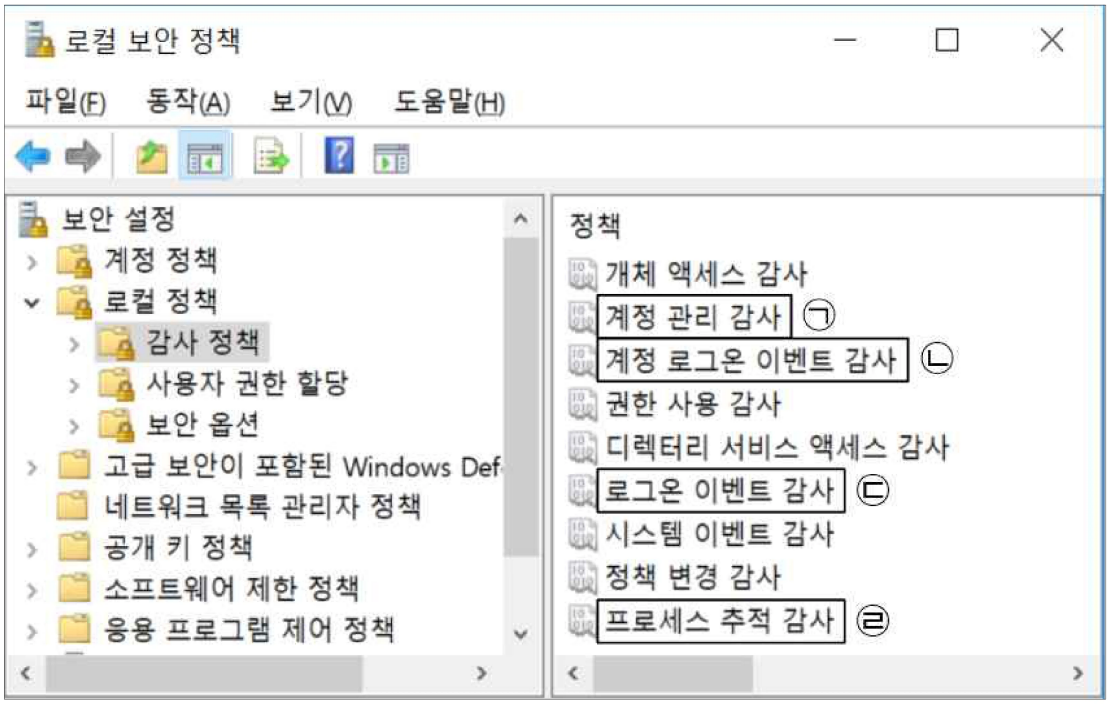
첫 옥텟이 10이면 10.0.0.0/8, 앞의 두 옥텟이 192.168이면 192.168.0.0/16인지 확인한다. 172로 시작하면 두 번째 옥텟이 16~31인지 추가로 확인하고, 이 세 범위에 없으면 사설 IPv4 주소가 아니다.

### 암기 포인트

사설 IPv4는 10 전체, 172.16~31, 192.168이다.

NoteBase

**문 3. 다음 그림에서 Windows 감사 정책에 관한 설명으로 가장 적절하지 않은 것은?**




① ㉠ 계정 관리 감사: 사용자 계정 또는 그룹의 생성/변경/삭제, 사용자 계정의 이름 변경 및 설정 등을 감사한다.

② ㉡ 계정 로그온 이벤트 감사: 사용자 권한 할당 정책, 감사 정책, 계정 정책 또는 트러스트 정책을 변경하려는 각 인스턴스를 감사한다.

③ ㉢ 로그온 이벤트 감사: 각 사용자 로그온 또는 로그오프 인스턴스를 감사한다.

④ ㉣ 프로세스 추적 감사: 프로세스 생성/종료, 핸들 복제 및 간접 개체 액세스 같은 프로세스 관련 이벤트를 감사한다.

**정답 2번**

**출제 포인트**

Windows 감사 정책의 각 범주가 어떤 보안 이벤트를 기록하는지 구분하는 문제이다. 특히 계정 로그온 이벤트와 정책 변경 이벤트의 차이가 핵심이다.

NoteBase

### 핵심 개념

계정 관리 감사는 사용자·그룹 계정의 생성, 변경, 삭제 등 계정 자체의 변경을 기록한다.
계정 로그온 이벤트 감사는 계정의 자격 증명을 확인하는 컴퓨터에서 이루어진 인증 시도를 기록한다.
로그온 이벤트 감사는 해당 컴퓨터에 대한 사용자의 로그온·로그오프를 기록한다.
정책 변경 감사는 사용자 권한 할당 정책, 감사 정책, 계정 정책, 트러스트 정책 등의 변경을 기록한다.
프로세스 추적 감사는 프로세스 생성·종료 등 프로세스 관련 세부 동작을 기록한다.

### 선지별 해설

① O — ㉠ 계정 관리 감사는 사용자 계정이나 그룹의 생성·변경·삭제, 계정 이름 변경과 같은 계정 관리 작업을 기록하므로 적절하다.
② X — '사용자 권한 할당 정책, 감사 정책, 계정 정책 또는 트러스트 정책의 변경을 감사한다'는 부분이 틀렸다. 이는 계정 로그온 이벤트 감사가 아니라 정책 변경 감사에 해당한다. 계정 로그온 이벤트 감사는 계정의 자격 증명을 확인하는 컴퓨터에서 발생한 인증 시도를 기록한다.
③ O — ㉢ 로그온 이벤트 감사는 해당 컴퓨터에서 발생한 사용자 로그온과 로그오프를 기록하므로 적절하다.
④ O — ㉣ 프로세스 추적 감사는 프로세스 생성·종료, 핸들 복제, 간접 개체 액세스 등 프로세스와 관련된 세부 이벤트를 기록하므로 적절하다.

### 오답 포인트

②는 '계정'이라는 말 때문에 계정 정책의 변경까지 계정 로그온 이벤트 감사에 포함된다고 착각하게 만든다. 그러나 인증 시도는 계정 로그온 이벤트 감사이고, 감사 정책·계정 정책·트러스트 정책 등의 설정 변경은 정책 변경 감사이다.

### 다시 나오면 이렇게 판단

감사 대상의 동작을 기준으로 구분한다. 계정 자체의 생성·삭제는 계정 관리, 자격 증명 확인은 계정 로그온, 특정 컴퓨터에 들어오고 나가는 것은 로그온 이벤트, 보안 정책 설정의 수정은 정책 변경, 실행 중인 프로세스의 생성·종료는 프로세스 추적에 대응한다.

### 암기 포인트

계정 로그온은 인증, 로그온 이벤트는 컴퓨터 출입, 정책 변경은 보안 설정 수정이다.

NoteBase

**문 4. NAT(Network Address Translation) 기술에 관한 설명으로 가장 적절하지 않은 것은?**

① NAT는 사설 IP 주소와 공인 IP 주소를 서로 매핑할 수 있다.

② NAT는 IPv4 주소 고갈문제를 완화할 수 있다.

③ NAT를 사용하면 네트워크 속도가 향상된다.

④ NAT를 사용하면 내부 시스템의 네트워크 구조를 노출하지 않는 보안상 이점을 제공한다.

**정답 3번**

**출제 포인트**

이 문제는 NAT의 주소 변환 기능과 그 효과를 구분하는 문제이다.

**핵심 개념**

NAT는 라우터나 방화벽 등에서 패킷의 IP 주소를 다른 주소로 변환하는 기술이다. 여러 내부 호스트가 제한된 공인 IPv4 주소를 공유하게 하여 주소 부족을 완화하고, 외부에서 내부 주소 체계가 직접 드러나지 않게 할 수 있다. 다만 주소 변환 자체가 통신 속도를 높이는 기술은 아니다.

**선지별 해설**

① O — NAT는 내부의 사설 IP 주소와 외부 통신에 사용하는 공인 IP 주소 사이의 대응 관계를 만들어 주소를 변환할 수 있다.
② O — 여러 사설 IP 주소가 하나 또는 소수의 공인 IP 주소를 공유할 수 있으므로 IPv4 공인 주소의 소비를 줄여 주소 고갈 문제를 완화한다.
③ X — 틀린 표현은 '네트워크 속도가 향상된다'이다. 올바르게는 NAT는 주소를 변환하는 기술이며, 사용한다고 해서 네트워크 속도가 본질적으로 향상되지는 않는다. 오히려 주소와 포트 변환 처리로 추가 부담이 생길 수 있다.
④ O — 외부에서는 변환된 공인 주소가 보이고 내부의 사설 주소와 주소 구조는 직접 노출되지 않으므로 일정한 보안상 이점이 있다. 다만 NAT 자체가 방화벽의 모든 보안 기능을 대신하는 것은 아니다.

**오답 포인트**

③은 NAT의 부수 효과를 성능 향상으로 바꿔 놓은 선지이다. NAT의 대표 효과는 공인 IPv4 주소 절약과 내부 주소 은닉이지 전송 속도 향상이 아니다.

**다시 나오면 이렇게 판단**

NAT 선지는 '주소 변환·공인 주소 절약·내부 주소 은닉'에 해당하면 타당성을 검토하고, '속도 향상'처럼 NAT의 목적과 직접 관련 없는 성능 효과를 단정하면 틀린 표현으로 판단한다.

NoteBase

**암기 포인트**

NAT는 주소를 바꾸고 아끼며 감추지만, 속도를 높이는 기술은 아니다.

NoteBase

**문 5. APT(Advanced Persistent Threat) 공격 행위로 가장 적절한 것은?**

① 공격자는 봇넷에 명령을 전달하여 대규모의 트래픽을 유발시키거나 취약한 서버를 악용하여 공격을 수행한다.

② 공격자는 인증 작업 등이 완료되어 정상적으로 통신이 이루어지고 있는 다른 사용자의 세션을 가로채서 별도의 인증 없이 가로챈 세션으로 통신한다.

③ 공격자는 공격대상을 특정하고 네트워크에 침투하여 거점을 마련한 뒤, 제로데이 공격과 같은 기존에 알려지지 않았던 취약점을 이용하여 공격한다.

④ 공격자는 컴퓨터 시스템에 저장된 사용자 파일을 암호화하거나 컴퓨터 시스템을 잠그고 금전을 요구한다.

**정답 3번**

**출제 포인트**

APT의 핵심인 특정 표적, 지속적 침투, 내부 거점 확보를 다른 사이버 공격 유형과 구별하는 문제이다.

**핵심 개념**

APT(지능형 지속 위협)는 특정 조직이나 시스템을 목표로 삼아 여러 침투 기법을 사용하고, 장기간 은밀하게 접근 권한과 내부 거점을 유지하면서 정보를 탈취하거나 시스템을 훼손하는 공격이다. 제로데이 취약점은 사용할 수 있는 수단의 하나일 뿐 APT의 필수 조건은 아니다.
APT는 특정 표적에 대한 지속적·단계적 침투, DDoS는 대량 트래픽에 의한 서비스 마비, 세션 하이재킹은 인증된 통신 세션 탈취, 랜섬웨어는 파일 암호화·시스템 잠금 후 금전 요구로 구별된다.

**선지별 해설**

① X — 봇넷에 명령을 내려 대규모 트래픽을 발생시키는 것은 분산 서비스 거부(DDoS) 공격의 전형적인 방식이다. 틀린 표현은 이를 APT 공격 행위로 본 부분이며, 올바르게는 '다수의 감염 기기가 동시에 트래픽을 보내 서비스 가용성을 떨어뜨리는 DDoS 공격'이다.
② X — 정상 사용자의 인증된 세션을 탈취하여 별도 인증 없이 통신하는 것은 세션 하이재킹이다. 틀린 표현은 이를 APT 공격 행위로 본 부분이며, 올바르게는 '이미 성립된 세션의 식별 정보나 연결을 가로채는 세션 하이재킹 공격'이다.
③ O — 공격 대상을 특정하고 네트워크에 침투한 뒤 내부 거점을 확보하여 공격을 이어 간다는 설명은 표적성과 지속성을 가진 APT의 특징에 부합한다. 제로데이 취약점은 APT에서 활용할 수 있는 고도화된 침투 수단의 예이다.
④ X — 사용자 파일을 암호화하거나 시스템을 잠근 뒤 금전을 요구하는 것은 랜섬웨어 공격이다. 틀린 표현은 이를 APT 공격 행위로 본 부분이며, 올바르게는 '데이터나 시스템의 사용을 제한하고 복구 대가를 요구하는 랜섬웨어 공격'이다.

NoteBase

**오답 포인트**

①의 봇넷과 ③의 제로데이는 모두 공격자가 활용하는 기술이어서 APT와 혼동하기 쉽다. 그러나 ①은 대량 트래픽에 의한 서비스 마비가 목적이고, ③은 특정 표적을 정한 뒤 침투·거점 확보·지속 공격으로 이어지는 전체 공격 양상을 설명한다.

**다시 나오면 이렇게 판단**

공격 수단 하나보다 공격의 전체 양상을 본다. '특정 표적 선정 → 은밀한 침투 → 내부 거점 확보 → 장기간 지속'이 나타나면 APT로 판단하고, 대량 트래픽·세션 탈취·파일 암호화와 금전 요구가 중심이면 각각 DDoS·세션 하이재킹·랜섬웨어로 판단한다.

**암기 포인트**

APT는 특정 표적을 지능적으로 침투해 오래 머무는 공격이다.

NoteBase

**문 6. 데이터 링크 계층의 프레임에서 사용되는 6bytes 크기의 주소로 제조사에 의해 할당되며, 홉에서 홉으로 갈 때마다 변경되는 주소로 가장 적절한 것은?**

① 논리 주소

② 물리 주소

③ IP 주소

④ 포트 주소

**정답 2번**

**출제 포인트**

이 문제는 데이터 링크 계층에서 사용하는 물리 주소와 네트워크·전송 계층의 주소를 구별하는 문제이다.

**핵심 개념**

물리 주소(MAC 주소)는 네트워크 인터페이스에 부여되는 6바이트 주소이며 데이터 링크 계층의 프레임 전달에 사용된다. 라우터를 거칠 때마다 프레임이 새로 만들어지므로 출발지·목적지 물리 주소도 다음 홉에 맞게 바뀐다. 논리 주소인 IP 주소는 네트워크 계층에서 호스트와 네트워크를 식별하고, 포트 주소는 전송 계층에서 호스트 내부의 응용 프로세스를 식별한다.

**선지별 해설**

① X — '논리 주소'는 네트워크 계층에서 사용하는 주소라는 점이 틀렸다. 올바르게는 제시된 6바이트 프레임 주소가 물리 주소(MAC 주소)이다.
② O — 물리 주소(MAC 주소)는 일반적으로 제조사가 네트워크 인터페이스에 할당하는 6바이트 주소이며, 각 홉에서 프레임이 재구성될 때 다음 링크에 맞게 변경된다.
③ X — 'IP 주소'는 네트워크 계층의 논리 주소라는 점이 틀렸다. 올바르게는 데이터 링크 계층의 프레임에 사용되고 홉마다 바뀌는 주소가 물리 주소(MAC 주소)이다.
④ X — '포트 주소'는 전송 계층에서 응용 프로세스를 식별하는 주소라는 점이 틀렸다. 올바르게는 6바이트 크기로 프레임 전달에 쓰이는 주소가 물리 주소(MAC 주소)이다.

**오답 포인트**

'홉마다 변경된다'는 표현 때문에 IP 주소를 고르기 쉽다. 그러나 라우터는 다음 링크로 보낼 때 새 프레임을 만들므로 링크별로 바뀌는 것은 프레임의 물리 주소이다.

**다시 나오면 이렇게 판단**

'데이터 링크 계층·프레임·6바이트·제조사 할당·홉마다 변경'이 함께 나오면 물리 주소(MAC 주소)로 판단한다. 네트워크 계층과 패킷은 IP 주소, 전송 계층과 프로세스는 포트 주소에 연결한다.

NoteBase

**암기 포인트**

프레임은 MAC, 패킷은 IP, 프로세스는 포트이다.

NoteBase

**문 7. 다음 소스코드의 빈칸 ㉠에 들어갔을 때 버퍼 오버플로우 공격이 발생할 수 있는 함수로 가장 적절한 것은?**

```
#include <stdio.h>
void main()
{
        char buffer[100];
        ㉠        (buffer);
        printf("%s\n",buffer);
}
```

① vfscanf

② strncat

③ gets

④ snprintf

**정답 3번**

**출제 포인트**

이 문제는 문자 배열의 크기를 전달받지 않고 입력을 저장하는 gets가 버퍼 오버플로우를 일으킬 수 있다는 점을 묻는다.

**핵심 개념**

버퍼 오버플로우는 버퍼의 경계를 넘는 데이터를 기록하여 인접한 메모리를 훼손하는 현상이다. gets는 목적지 버퍼의 크기를 알 수 없고 입력 길이를 제한하는 인자도 없으므로 안전한 경계 검사를 할 수 없다. 반면 크기를 지정하는 함수도 인자와 크기 값을 올바르게 사용해야 안전하다.

NoteBase

**선지별 해설**

① X
- vfscanf는 지정한 스트림에서 형식에 따라 입력을 읽는 함수이므로 vfscanf(buffer)처럼 문자 배열 하나만 인자로 호출할 수 없다. 틀린 부분은 빈칸에 vfscanf를 넣어 제시된 호출을 완성할 수 있다는 점이다. 올바르게는 스트림, 형식 문자열, 저장 대상 등을 전달하며, 문자열 변환에는 필드 폭도 지정해야 넘침을 막을 수 있다.

② X
- strncat는 문자열을 입력받는 함수가 아니라 원본 문자열의 문자를 목적지 문자열 뒤에 이어 붙이는 함수이다. 틀린 부분은 strncat(buffer)라는 한 인자 호출이다. 올바르게는 목적지, 원본, 덧붙일 최대 문자 수를 전달해야 하며 목적지의 남은 공간도 따로 확인해야 한다.

③ O
- gets(buffer)는 표준 입력에서 개행 전까지 문자를 읽으면서 buffer의 크기를 전달받지 않는다. 100자를 담는 배열보다 긴 입력도 계속 기록할 수 있으므로 버퍼 오버플로우 공격에 취약하다.

④ X
- snprintf는 지정한 크기 범위 안에서 형식화한 문자열을 버퍼에 출력하는 함수이다. 틀린 부분은 snprintf(buffer)라는 한 인자 호출이다. 올바르게는 출력 버퍼, 버퍼 크기, 형식 문자열 등을 전달하며, 정확한 버퍼 크기를 지정하면 기록 범위를 제한할 수 있다.

**오답 포인트**

② strncat도 남은 공간을 잘못 계산하면 오버플로우가 날 수 있지만, 제시된 코드는 함수 이름 뒤에 buffer 하나만 전달한다. 이 호출 형태와 입력 길이 제한이 전혀 없다는 두 조건을 모두 만족하는 것은 ③ gets이다.

**다시 나오면 이렇게 판단**

문자열 입력 함수의 위험성을 판단할 때는 목적지 버퍼의 크기 또는 입력 최대 길이를 함수에 전달하는지 확인한다. 크기 정보 없이 한 개의 문자 배열만 받고 입력을 저장하는 gets는 즉시 위험 함수로 판단한다.

**암기 포인트**

gets는 길이 제한이 없다. 입력 버퍼에는 fgets처럼 최대 길이를 지정할 수 있는 함수를 사용한다.

NoteBase

**문 8. DoS 공격에 관한 설명으로 가장 적절하지 않은 것은?**

① SYN Flooding 공격은 다량의 SYN 패킷을 전송하여 시스템의 부하를 발생시킨다.

② Teardrop 공격은 패킷 단편화를 이용하는 공격으로 시퀀스 넘버를 조작하여 공격한다.

③ Smurf 공격은 IGMP 패킷을 사용하여 공격을 수행한다.

④ Ping of death 공격은 ping을 이용하여 패킷을 정상 크기보다 크게(최대 65,535바이트) 만들어 전송하는 공격이다.

**정답 3번**

**출제 포인트**

대표적인 DoS 공격이 악용하는 프로토콜과 패킷 처리상의 취약점을 구별하는 문제이다.

**핵심 개념**

SYN Flooding은 TCP 연결 설정의 반개방 상태를 대량으로 만들어 서버 자원을 소진시키는 공격이다. Teardrop은 IP 단편의 재조합 정보를 비정상적으로 조작하는 공격이다. Smurf는 출발지 주소를 피해자의 주소로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수의 응답이 피해자에게 집중되게 하는 공격이다. Ping of Death는 허용 범위를 벗어나는 비정상적으로 큰 IP 패킷이 재조합되도록 하여 시스템 장애를 유발하는 공격이다.

**선지별 해설**

① O — 다량의 TCP SYN 패킷을 보내 연결 대기 상태를 누적시키므로 서버의 연결 자원과 처리 능력에 부하를 준다.
② O — Teardrop은 분할된 IP 패킷의 재조합에 쓰이는 순서·위치 정보를 조작하여 단편이 겹치거나 비정상적으로 재조합되게 한다. 더 정확한 기술 용어는 IP 헤더의 단편 오프셋(fragment offset) 조작이다.
③ X — 틀린 표현은 'IGMP 패킷'이다. 올바르게는 출발지 주소를 피해자의 주소로 위조한 ICMP Echo Request 패킷을 브로드캐스트 주소로 전송하여 ICMP Echo Reply가 피해자에게 집중되게 하는 공격이다.
④ O — Ping of Death는 ping에 사용되는 ICMP를 이용해 비정상적으로 큰 IP 패킷을 단편화하여 보내고, 수신 측에서 재조합할 때 허용 가능한 IP 패킷 크기를 넘게 하여 장애를 일으킨다.

**오답 포인트**

③은 이름이 비슷한 ICMP와 IGMP를 바꾸어 놓았다. Smurf의 증폭에 쓰이는 것은 오류·진단 메시지를 담당하는 ICMP의 Echo 요청·응답이며, 멀티캐스트 그룹 관리를 위한 IGMP가 아니다.

NoteBase

**다시 나오면 이렇게 판단**

공격명마다 핵심 표지를 연결한다. SYN Flooding은 TCP 반개방 연결, Teardrop은 IP 단편 오프셋, Smurf는 ICMP와 브로드캐스트 및 출발지 위조, Ping of Death는 허용 크기를 넘는 패킷 재조합으로 판단한다.

**암기 포인트**

SYN은 연결 대기, Teardrop은 단편 조작, Smurf는 ICMP 증폭, Ping of Death는 초대형 패킷이다.

NoteBase

**문 9. Windows 레지스트리 루트키에 관한 설명으로 가장 적절한 것은?**




① HKEY_CLASSES_ROOT : 파일의 각 확장자에 대한 정보와 파일과 프로그램 간의 연결에 대한 정보를 저장한다.

② HKEY_CURRENT_USER : 시스템 관련 전체 정보를 저장한다.

③ HKEY_USERS : 현재 로그온 된 사용자와 관련된 데이터만 저장한다.

④ HKEY_CURRENT_CONFIG : 설치된 하드웨어와 하드웨어를 구동시키는 데 필요한 드라이버 설정에 대한 정보를 저장한다.

**정답 1번**

**출제 포인트**

Windows 레지스트리의 각 루트키가 어느 범위의 설정과 정보를 담당하는지 구별하는 문제이다.

**핵심 개념**

HKEY_CLASSES_ROOT(HKCR)는 파일 확장자 연결과 COM 클래스 등록 정보를 제공한다.
HKEY_CURRENT_USER(HKCU)는 현재 로그인한 사용자의 개인 설정을 담는다.
HKEY_LOCAL_MACHINE(HKLM)은 하드웨어와 드라이버를 포함한 컴퓨터 전체의 시스템 설정을 담는다.
HKEY_USERS(HKU)는 시스템에 로드된 사용자 프로필별 설정을 담는다.
HKEY_CURRENT_CONFIG(HKCC)는 현재 사용 중인 하드웨어 프로필의 설정을 보여 준다.

NoteBase

**선지별 해설**

① O — HKEY_CLASSES_ROOT는 파일 확장자별 연결 정보와 해당 파일을 여는 프로그램의 연결 정보를 제공하므로 적절한 설명이다.
② X — 틀린 표현은 '시스템 관련 전체 정보'이다. HKEY_CURRENT_USER는 현재 로그인한 사용자의 바탕화면, 환경 설정 등 사용자별 정보를 저장한다. 시스템 전체 정보는 주로 HKEY_LOCAL_MACHINE에 해당한다.
③ X — 틀린 표현은 '현재 로그온 된 사용자와 관련된 데이터만'이다. HKEY_USERS는 로드된 여러 사용자 프로필의 설정을 사용자 SID별로 담으며, 현재 사용자의 설정은 그중 하나가 HKEY_CURRENT_USER로 연결되어 보인다.
④ X — 틀린 표현은 '설치된 하드웨어와 드라이버 설정' 전반을 저장한다는 부분이다. HKEY_CURRENT_CONFIG는 현재 사용 중인 하드웨어 프로필의 설정을 보여 주며, 컴퓨터 전체의 하드웨어·드라이버 구성 정보는 주로 HKEY_LOCAL_MACHINE에 저장된다.

**오답 포인트**

CURRENT라는 단어 때문에 HKEY_CURRENT_USER와 HKEY_CURRENT_CONFIG의 범위를 넓게 해석하기 쉽다. CURRENT_USER는 현재 사용자 한 명, CURRENT_CONFIG는 현재 적용 중인 하드웨어 프로필에 한정된다.

**다시 나오면 이렇게 판단**

루트키 이름의 대상과 범위를 짝지어 판단한다. CLASSES_ROOT는 파일 연결·클래스, CURRENT_USER는 현재 사용자, LOCAL_MACHINE은 컴퓨터 전체, USERS는 여러 사용자 프로필, CURRENT_CONFIG는 현재 하드웨어 프로필이다.

**암기 포인트**

CR은 연결, CU는 현재 사용자, LM은 컴퓨터 전체, U는 사용자들, CC는 현재 하드웨어 구성이다.

NoteBase

**문 10. ICMP 오류 보고 메시지로 가장 적절하지 않은 것은?**

① ICMP Parameter Problem 메시지

② ICMP Echo Request 메시지

③ ICMP Time Exceeded 메시지

④ ICMP Destination Unreachable 메시지

**정답 2번**

**출제 포인트**

ICMP 메시지를 오류 보고 메시지와 질의·정보성 메시지로 구분하는 문제이다.

**핵심 개념**

ICMP 오류 보고 메시지는 IP 패킷 처리나 전달 과정에서 발생한 문제를 송신 측에 알리는 메시지이다. 반면 Echo Request와 Echo Reply는 상대 호스트의 도달 가능성과 응답 여부를 확인하는 질의·응답 메시지이다.

**선지별 해설**

① O — ICMP Parameter Problem 메시지는 IP 헤더의 잘못된 값이나 필수 정보 누락 등으로 패킷을 처리할 수 없을 때 문제 지점을 알리는 오류 보고 메시지이다.
② X — 틀린 표현은 'ICMP 오류 보고 메시지'로 분류한 부분이다. ICMP Echo Request 메시지는 대상의 도달 가능성을 확인하고 Echo Reply를 요청하는 질의 메시지이며, 오류를 보고하는 메시지가 아니다.
③ O — ICMP Time Exceeded 메시지는 패킷의 TTL이 소진되었거나 조각 재조립 제한 시간이 초과되었을 때 보내는 오류 보고 메시지이다.
④ O — ICMP Destination Unreachable 메시지는 네트워크·호스트·포트 등에 패킷을 전달할 수 없음을 알리는 오류 보고 메시지이다.

**오답 포인트**

Echo Request도 ICMP에 속한다는 사실만 보고 오류 보고 메시지로 판단하기 쉽다. 그러나 'ICMP 메시지인가'와 'ICMP 오류 보고 메시지인가'는 다른 분류이며, Echo Request는 연결 상태를 확인하는 질의 메시지이다.

**다시 나오면 이렇게 판단**

패킷 처리 실패의 원인을 송신 측에 알리면 오류 보고 메시지로 판단한다. 상대가 응답하는지 시험하기 위한 요청이면 질의 메시지로 판단한다.

NoteBase

**암기 포인트**

Parameter Problem · Time Exceeded · Destination Unreachable는 오류 보고, Echo Request는 도달 가능성 확인이다.

NoteBase

**문 11. 무선랜 보안 기술에 관한 설명으로 가장 적절하지 않은 것은?**

① WPA2는 CCMP를 사용하여 강력한 보안기능을 제공한다.

② WEP(Wired Equivalent Privacy)는 IEEE 802.11i에서 표준화한 데이터 암호화 방식이다.

③ WPA(Wi-Fi Protected Access)는 TKIP 방식을 사용한다.

④ WPA-PSK는 주로 인증서버가 설치되지 않은 소규모 네트워크에서 사용되는 방식이다.

**정답 2번**

**출제 포인트**

무선랜 보안 방식인 WEP, WPA, WPA2가 각각 어떤 표준과 암호화 방식을 사용하는지 구별하는 문제이다.

**핵심 개념**

WEP: 초기 IEEE 802.11 무선랜에 도입된 보안 방식으로, RC4 기반 암호화를 사용하지만 취약점이 많다.
WPA: WEP의 취약점을 보완하기 위한 과도기적 방식으로, TKIP를 사용한다.
WPA2: IEEE 802.11i에 기반한 보안 방식으로, AES 기반의 CCMP를 사용한다.
WPA-PSK: 별도의 인증 서버 없이 미리 공유한 키로 인증하므로 가정이나 소규모 네트워크에 적합하다.

**선지별 해설**

① O — WPA2는 AES 기반의 CCMP를 사용하여 WEP나 WPA보다 강력한 기밀성·무결성 보호를 제공한다.
② X — 틀린 표현은 'IEEE 802.11i에서 표준화한'이다. WEP는 초기 IEEE 802.11 규격에 포함된 데이터 암호화 방식이며, IEEE 802.11i는 강화된 무선랜 보안 규격으로서 WPA2의 기반이 되었다.
③ O — WPA는 기존 WEP 장비와의 호환성을 고려하면서 보안을 개선하기 위해 TKIP 방식을 사용한다.
④ O — WPA-PSK는 별도의 인증 서버를 두지 않고 사전에 공유한 키를 사용하므로 가정이나 소규모 네트워크에서 주로 사용된다.

**오답 포인트**

②는 WEP와 IEEE 802.11i의 관계를 바꾸어 제시한 선지이다. WEP는 초기 IEEE 802.11, WPA는 TKIP, WPA2는 IEEE 802.11i와 CCMP라는 대응을 구분해야 한다.

**다시 나오면 이렇게 판단**

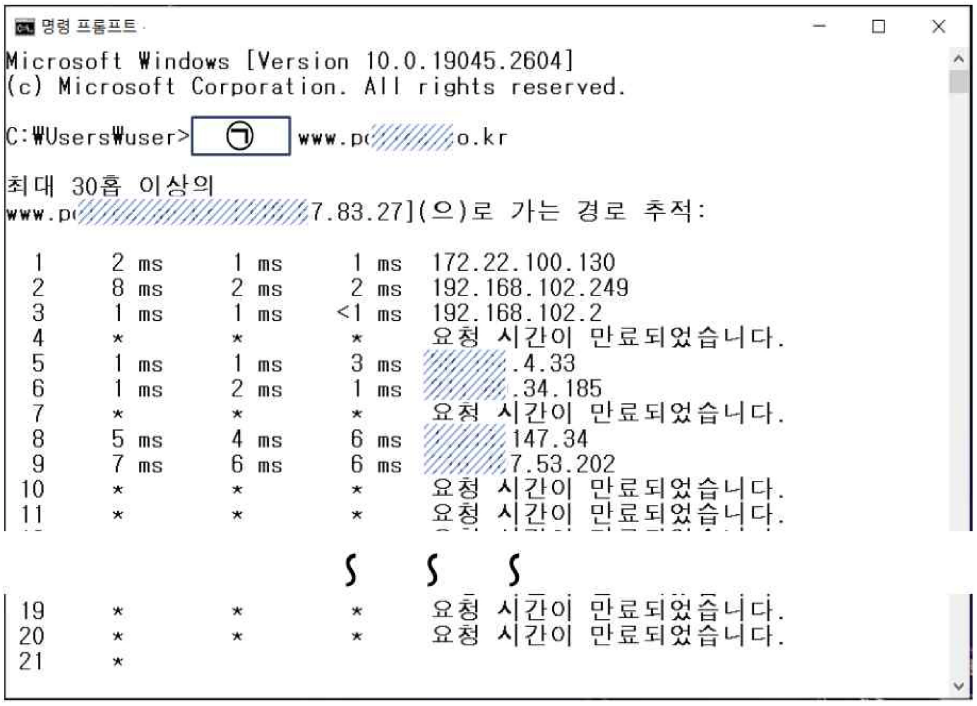
보안 방식과 핵심 키워드를 짝지어 판단한다. WEP는 초기 802.11과 RC4, WPA는 TKIP, WPA2는 802.11i와 CCMP, PSK는 인증 서버가 없는 사전 공유 키 방식이다.

**암기 포인트**

WEP는 초기 802.11, WPA는 TKIP, WPA2는 802.11i·CCMP, WPA-PSK는 소규모망의 사전 공유 키 방식이다.

NoteBase

**문 12. 다음 그림은 빈칸 ㉠의 명령어를 실행한 결과의 일부이다. 빈칸 ㉠에 들어갈 명령어로 옳은 것은?**




① ping

② ipconfig

③ netstat

④ tracert

**정답 4번**

**출제 포인트**

이 문제는 명령 실행 화면의 '최대 30홉'과 '경로 추적', 홉별 응답 시간 표시를 보고 목적지까지의 네트워크 경로를 추적하는 tracert 명령을 식별하는 문제이다.

NoteBase

**선지별 해설**

① X
- ping은 특정 호스트와의 연결 가능 여부와 왕복 응답 시간을 확인하는 명령이다. 화면처럼 목적지까지 거치는 홉을 순서대로 나열하지 않는다. 올바르게는 이 화면의 명령은 tracert이다.

② X
- ipconfig는 Windows 컴퓨터의 IP 주소, 서브넷 마스크, 기본 게이트웨이 등 TCP/IP 설정 정보를 확인하는 명령이다. 홉별 경로 추적 결과를 출력하지 않는다. 올바르게는 이 화면의 명령은 tracert이다.

③ X
- netstat는 활성 네트워크 연결, 수신 대기 포트, 프로토콜별 통계 등의 상태를 확인하는 명령이다. 목적지까지의 홉과 각 홉의 응답 시간을 연속해서 표시하는 명령이 아니다. 올바르게는 이 화면의 명령은 tracert이다.

④ O
- tracert는 목적지에 도달할 때까지 거치는 라우터를 홉 단위로 추적한다. 화면의 '최대 30홉', '경로 추적', 홉 번호, 세 번의 응답 시간, '요청 시간이 만료되었습니다.' 표시는 tracert의 전형적인 실행 결과이다.

**오답 포인트**

ping과 tracert 모두 응답 시간을 표시하므로 혼동하기 쉽다. 그러나 여러 홉 번호와 홉별 응답 시간이 순서대로 나오면 단순 연결 확인인 ping이 아니라 경로 추적인 tracert이다.

**다시 나오면 이렇게 판단**

출력에서 홉 번호가 연속되고 각 홉마다 응답 시간이 반복되며 '경로 추적' 문구가 보이면 tracert로 판단한다. IP 설정 항목이면 ipconfig, 연결·포트 목록이면 netstat, 한 대상의 응답 여부만 확인하면 ping이다.

**암기 포인트**

ping은 도달 여부, ipconfig는 IP 설정, netstat는 연결 상태, tracert는 홉별 경로 추적이다.

NoteBase

**문 13. Linux의 특수 권한에 관한 설명으로 가장 적절하지 않은 것은?**

① Sticky bit가 설정된 디렉터리는 /tmp이다.

② SetUID를 실행 권한이 없는 파일에 설정할 경우 대문자 S로 표기된다.

③ SetGID가 부여된 파일은 소유그룹의 실행 권한이 x에서 s로 변경될 수 있다.

④ Sticky bit가 부여된 디렉터리는 소유자와 소유그룹 외 사용자의 실행권한이 x에서 s로 변경된다.

**정답 4번**

**출제 포인트**

Linux의 특수 권한인 SetUID, SetGID, Sticky bit가 각각 어느 권한 위치에 어떤 문자로 표시되는지를 묻는 문제이다.

**핵심 개념**

SetUID: 파일 소유자의 실행 권한 위치에 표시되며, 실행 권한이 있으면 s, 없으면 S가 된다.
SetGID: 파일 소유그룹의 실행 권한 위치에 표시되며, 실행 권한이 있으면 s, 없으면 S가 된다.
Sticky bit: 기타 사용자의 실행 권한 위치에 표시되며, 실행 권한이 있으면 t, 없으면 T가 된다. 디렉터리에 설정하면 일반적으로 파일 소유자, 디렉터리 소유자 또는 root만 그 안의 파일을 삭제하거나 이름을 바꿀 수 있다.

**선지별 해설**

① O — /tmp는 여러 사용자가 함께 쓰는 대표적인 디렉터리이며, 일반적으로 Sticky bit가 설정되어 있다.
② O — SetUID는 소유자의 실행 권한 자리에 표시되므로, 소유자 실행 권한이 없는 파일에 설정하면 소문자 s가 아니라 대문자 S로 나타난다.
③ O — SetGID가 설정되고 소유그룹의 실행 권한도 있으면, 그룹 실행 권한 자리의 x가 s로 표시된다.
④ X — 틀린 표현은 ‘x에서 s로 변경된다’이다. Sticky bit는 기타 사용자의 실행 권한 자리에 표시되며, 실행 권한이 있으면 x가 t로 바뀐다. 실행 권한이 없으면 대문자 T로 표시된다.

**오답 포인트**

SetUID와 SetGID에는 s/S를 사용하지만 Sticky bit에는 t/T를 사용한다. ④는 Sticky bit의 표시 위치는 맞게 제시하면서 표시 문자를 s로 바꾼 것이 함정이다.

**다시 나오면 이렇게 판단**

특수 권한의 표시 위치와 문자를 함께 확인한다. SetUID는 소유자 자리의 s/S, SetGID는 소유그룹 자리의 s/S, Sticky bit는 기타 사용자 자리의 t/T이다. 소문자는 원래 실행 권한이 있는 경우, 대문자는 없는 경우이다.

NoteBase

**암기 포인트**

SetUID·SetGID는 s/S, Sticky bit는 t/T이다.

NoteBase

**문 14. IPv4 패킷 헤더에 관한 설명으로 가장 적절하지 않은 것은?**

① Version : IP 프로토콜의 버전을 의미하며 값은 $1111_{(2)}$이다.

② TTL(Time to Live) : 라우터를 하나 지날 때마다 TTL 값이 1씩 줄어들고, 그 값이 0이 되면 해당 패킷은 폐기된다.

③ Protocol : IP 계층의 서비스를 사용하는 상위계층의 프로토콜을 정의한다.

④ Header Checksum : 헤더에 대한 오류-검사용으로 사용되는 필드이다.

**정답 1번**

**출제 포인트**

IPv4 기본 헤더의 Version, TTL, Protocol, Header Checksum 필드가 나타내는 값과 기능을 구별하는 문제이다.

**핵심 개념**

Version은 사용 중인 IP 프로토콜의 버전을 나타내는 4비트 필드이며, IPv4에서는 4, 즉 $0100_{(2)}$이다. TTL은 패킷의 무한 순환을 막고, Protocol은 IP 데이터그램에 실린 상위계층 프로토콜을 식별하며, Header Checksum은 IPv4 헤더의 오류를 검사한다.

**선지별 해설**

① X — Version 필드는 IP 프로토콜의 버전을 나타내지만, IPv4의 값은 $1111_{(2)}$이 아니라 4를 나타내는 $0100_{(2)}$이다. 틀린 표현 '값은 $1111_{(2)}$이다'는 '값은 $0100_{(2)}$이다'로 고쳐야 한다.
② O — TTL은 라우터를 거칠 때마다 감소하며, 0이 되면 패킷을 폐기하므로 라우팅 루프에서 패킷이 무한히 순환하는 것을 방지한다.
③ O — Protocol 필드는 IPv4 페이로드를 처리할 상위계층 프로토콜이 무엇인지 식별한다. TCP, UDP, ICMP 등이 이 필드로 구분된다.
④ O — Header Checksum은 IPv4 헤더에 발생한 오류를 검사하는 필드이다. 검사 범위는 전체 패킷이나 데이터가 아니라 헤더이다.

**오답 포인트**

①은 Version 필드의 의미 자체는 맞게 제시한 뒤 실제 비트값만 바꾼 선지이다. 또한 ④의 Header Checksum을 전체 패킷 검사로 확대해서 이해하지 않아야 한다.

**다시 나오면 이렇게 판단**

IPv4 헤더 문제에서는 각 필드를 '식별', '수명 제한', '상위 프로토콜 표시', '헤더 오류 검사'로 대응시킨다. Version이 IPv4이면 값 4와 4비트 표현 $0100_{(2)}$을 함께 확인한다.

NoteBase

**암기 포인트**

IPv4의 Version은 4=$0100_{(2)}$, TTL은 순환 방지, Protocol은 상위 프로토콜 식별, Header Checksum은 헤더만 검사한다.

NoteBase

**문 15. 프로세스가 사용하는 메모리 공간에 관한 설명으로 가장 적절하지 않은 것은?**

① Text 영역 : 읽기와 쓰기가 가능한 영역이며, 프로그램 코드가 저장된다.

② Stack 영역 : 프로그램 함수 내에서 사용하는 지역변수가 저장된다.

③ Heap 영역 : 프로그램 실행 중 메모리를 동적으로 할당하는 경우에 이 영역에 할당된다.

④ Data 영역 : 전역변수를 선언하는 경우 전역변수가 저장된다.

**정답 1번**

**출제 포인트**

프로세스의 대표적인 메모리 영역인 Text, Data, Heap, Stack의 저장 대상과 일반적인 접근 권한을 구분하는 문제이다.

**핵심 개념**

Text 영역은 실행할 프로그램 코드가 저장되는 영역으로, 코드 변조를 막기 위해 일반적으로 읽기 전용으로 보호된다. Data 영역에는 전역변수와 정적변수가 저장되고, Heap 영역에는 실행 중 동적으로 할당한 메모리가 놓이며, Stack 영역에는 함수 호출과 관련된 지역변수·매개변수·복귀 주소 등이 저장된다.

**선지별 해설**

① X - 틀린 표현은 '읽기와 쓰기가 가능한 영역'이다. Text 영역에는 프로그램 코드가 저장되지만 일반적으로 쓰기는 허용되지 않고 읽기 및 실행 권한이 부여된다. 올바르게는 'Text 영역은 프로그램 코드가 저장되며 일반적으로 읽기 전용으로 보호되는 영역이다'라고 해야 한다.
② O - Stack 영역에는 함수가 호출될 때 생성되는 스택 프레임이 놓이며, 함수 내부의 지역변수 등이 여기에 저장된다.
③ O - Heap 영역은 프로그램 실행 중 필요한 메모리를 동적으로 할당할 때 사용하는 영역이다.
④ O - Data 영역에는 프로그램의 전역변수와 정적변수가 저장된다.

**오답 포인트**

①은 Text 영역의 코드를 CPU가 읽는다는 사실을 '읽기와 쓰기가 모두 가능하다'는 뜻으로 바꾼 선지이다. 프로그램 코드의 저장 여부와 메모리 쓰기 권한을 구분해야 한다.

**다시 나오면 이렇게 판단**

각 영역의 대표 저장 대상을 먼저 연결한 뒤 권한 표현을 확인한다. Text는 코드와 읽기·실행, Data는 전역·정적변수, Heap은 동적 할당, Stack은 함수 호출과 지역변수로 판단한다.

NoteBase

**암기 포인트**

Text는 코드, Data는 전역·정적, Heap은 동적 할당, Stack은 함수·지역변수이다.

NoteBase

**문 16. 다음은 이블 트윈(evil twin) 공격에 관한 설명이다. ㉠과 ㉡에 들어갈 용어를 올바르게 짝지은 것은?**

이블 트윈(evil twin) 공격은 공격자가 공공장소에 설치된 무선 네트워크 ( ㉠ )의 ( ㉡ )와/과 동일한 값을 이용하여 사용자들의 접속을 유인한 뒤, 이들의 중요 정보를 중간에서 탈취하는 공격이다.

① ㉠: AP(Access Point), ㉡: SSID

② ㉠: AP(Access Point), ㉡: MAC

③ ㉠: IP(Internet Protocol), ㉡: SSID

④ ㉠: IP(Internet Protocol), ㉡: MAC

**정답 1번**

**출제 포인트**

이블 트윈 공격이 정상 무선 접속 지점(AP)을 사칭할 때 복제하는 식별값이 SSID라는 점을 묻는 문제이다.

**핵심 개념**

AP(Access Point)는 무선 단말을 네트워크에 연결하는 무선 접속 지점이다. SSID(Service Set Identifier)는 사용자가 Wi-Fi 목록에서 확인하는 무선 네트워크 이름이다. 이블 트윈은 공격자가 가짜 AP에 정상 AP와 동일한 SSID를 설정하여 사용자를 접속시킨 뒤 통신 정보 탈취를 시도하는 공격이다.
MAC 주소는 네트워크 인터페이스를 식별하는 주소이고, IP 주소는 IP 네트워크에서 통신 대상을 식별하고 경로를 정하는 데 쓰이는 논리 주소이다. 둘 다 이 문장의 '무선 네트워크 이름'에 해당하지 않는다.

**선지별 해설**

① O — 공격자는 정상 AP와 같은 SSID를 사용하는 가짜 AP를 만들어 사용자의 접속을 유도하므로 ㉠은 AP, ㉡은 SSID이다.
② X — 틀린 표현은 ㉡의 'MAC'이다. 사용자가 같은 무선 네트워크로 오인하게 만드는 값은 MAC 주소가 아니라 SSID이므로, 올바르게는 '㉠: AP, ㉡: SSID'이다.
③ X — 틀린 표현은 ㉠의 'IP(Internet Protocol)'이다. 이블 트윈에서 공격자가 위장하여 설치하는 것은 IP가 아니라 무선 접속 지점인 AP이므로, 올바르게는 '㉠: AP, ㉡: SSID'이다.
④ X — ㉠의 'IP(Internet Protocol)'과 ㉡의 'MAC'이 모두 틀렸다. 공격자가 정상 무선 네트워크를 사칭할 때 설치하는 것은 가짜 AP이고, 정상 AP와 같게 설정하는 무선 네트워크 이름은 SSID이므로, 올바르게는 '㉠: AP, ㉡: SSID'이다.

NoteBase

**오답 포인트**

공격자가 장비의 주소를 복제한다고 생각하여 MAC을 고르기 쉽다. 그러나 이 문항의 핵심 표현은 '사용자들의 접속을 유인'하는 것이다. 사용자가 Wi-Fi 목록에서 네트워크를 구별할 때 보는 이름은 SSID이므로, 정상 AP와 동일하게 꾸미는 값은 SSID이다.

**다시 나오면 이렇게 판단**

정상 Wi-Fi처럼 보이는 가짜 접속 지점을 설치한다는 문맥에서는 장비를 AP로, 사용자가 보는 무선 네트워크 이름을 SSID로 대응한다. IP와 MAC은 주소이고 SSID는 Wi-Fi 이름이라는 차이로 구별한다.

**암기 포인트**

이블 트윈은 '가짜 AP + 정상 AP와 같은 SSID' 조합이다.

NoteBase

**문 17. VPN(Virtual Private Network)에 관한 설명으로 가장 적절하지 않은 것은?**

① SSL VPN은 별도의 장비가 없어도 웹브라우저로 구성이 가능하다.

② L2TP나 PPTP와 같은 2계층 터널링 프로토콜을 사용할 수 있다.

③ IPSec의 터널모드는 IP 헤더를 포함한 전체 IP 패킷을 암호화하여 전송한다.

④ IPSec VPN을 활용하기 위해서는 응용계층의 수정이 반드시 필요하다.

**정답 4번**

**출제 포인트**

VPN의 구현 방식별 특징과 IPSec의 동작 계층·터널 모드를 구분하는 문제이다.

**핵심 개념**

VPN은 공중망을 이용하면서 터널링과 암호화 등을 통해 사설망처럼 안전한 통신 경로를 만드는 기술이다. SSL VPN은 웹 환경을 활용해 원격 접속을 제공하고, L2TP와 PPTP는 2계층 터널링 프로토콜이다. IPSec은 네트워크 계층에서 IP 패킷을 보호하므로 응용계층을 반드시 수정할 필요가 없다. IPSec 터널 모드는 원래 IP 헤더와 데이터 전체를 보호한 뒤 새로운 IP 헤더를 붙여 전송한다.

**선지별 해설**

① O — SSL VPN은 일반적으로 웹브라우저를 이용할 수 있어 이용자 측에 별도의 전용 VPN 장비나 전용 클라이언트 프로그램이 없어도 접속 구성이 가능하다.
② O — L2TP와 PPTP는 데이터링크 계층의 프레임을 터널링하는 대표적인 2계층 터널링 프로토콜이다.
③ O — IPSec 터널 모드는 원래 IP 헤더를 포함한 전체 원본 IP 패킷을 보호 대상으로 캡슐화하고, 바깥쪽에 새로운 IP 헤더를 추가하여 전송한다.
④ X — 틀린 표현은 '응용계층의 수정이 반드시 필요하다'이다. IPSec은 네트워크 계층에서 동작하므로 응용 프로그램을 수정하지 않고도 IP 통신을 보호할 수 있다.

**오답 포인트**

IPSec이 모든 계층의 프로그램을 고쳐야 하는 보안 기능이라고 오해하기 쉽다. 그러나 IPSec은 IP 계층에서 패킷을 보호하므로 ④의 '응용계층의 수정이 반드시 필요하다'가 결정적인 오류이다.

**다시 나오면 이렇게 판단**

VPN 선지는 먼저 동작 계층을 확인한다. SSL VPN은 웹 기반 접속, L2TP·PPTP는 2계층 터널링, IPSec은 네트워크 계층 보호로 구분한다. IPSec 터널 모드에서는 원본 IP 패킷 전체가 캡슐화되고 새 IP 헤더가 추가된다는 점을 적용한다.

NoteBase

**암기 포인트**

SSL은 웹, L2TP·PPTP는 2계층, IPSec은 IP 계층이다. IPSec 터널 모드는 원본 패킷 전체를 감싸며 응용계층 수정은 필수가 아니다.

NoteBase

**문 18. IDS(Intrusion Detection System) 기법에 관한 설명으로 가장 적절한 것은?**

① 이상탐지(anomaly) 기법은 공격에 대한 시그니처를 데이터베이스화하여 침입자의 활동과 비교하여 동일하면 침입으로 식별한다.

② 오용탐지(misuse) 기법은 제로데이 공격에 대응이 용이하다.

③ 이상탐지(anomaly) 기법은 정상적인 상태를 기준으로 했을 때 급격한 변화를 탐지하지만, 오탐율(false positive)이 높은 문제점을 가지고 있다.

④ 오용탐지(misuse) 기법은 신경망과 통계적 분석 방법만을 사용한다.

**정답 3번**

**출제 포인트**

이 문제는 IDS의 이상탐지 기법과 오용탐지 기법을 어떤 기준으로 침입을 판별하는지에 따라 구분하는 문제이다.

**핵심 개념**

이상탐지는 정상적인 행위의 기준선을 학습하거나 설정한 뒤, 그 기준에서 벗어난 행위를 침입으로 판단하는 기법이다. 알려지지 않은 공격도 탐지할 가능성이 있지만 정상 행위를 공격으로 판단하는 오탐이 많을 수 있다.
오용탐지는 알려진 공격의 시그니처나 규칙을 데이터베이스화하고 현재 행위와 대조하는 기법이다. 알려진 공격은 정확하게 탐지하기 쉽지만 시그니처가 없는 새로운 공격이나 제로데이 공격에는 취약하다.
핵심 대비는 '정상 기준에서 벗어났는가'는 이상탐지, '알려진 공격 패턴과 일치하는가'는 오용탐지이다.

NoteBase

**선지별 해설**

① X
공격 시그니처를 데이터베이스화하여 일치 여부를 확인하는 것은 이상탐지가 아니라 오용탐지이다. 틀린 표현은 '이상탐지'이며, 올바르게는 '오용탐지 기법은 공격 시그니처와 현재 행위를 비교하여 일치하면 침입으로 식별한다'이다.

② X
오용탐지는 이미 알려진 공격 패턴을 기준으로 하므로 시그니처가 아직 없는 제로데이 공격에 대응하기 어렵다. 틀린 표현은 '제로데이 공격에 대응이 용이하다'이며, 올바르게는 '이상탐지는 정상 상태에서 벗어난 행위를 탐지하므로 제로데이 공격도 탐지할 가능성이 있다'이다.

③ O
이상탐지는 정상 상태를 기준으로 급격하거나 비정상적인 변화를 탐지한다. 정상 행위의 변동까지 공격으로 판단할 수 있어 오탐률이 높아질 수 있다는 설명도 적절하다.

④ X
오용탐지는 신경망과 통계적 분석 방법만을 사용하는 기법이 아니라 알려진 공격의 시그니처나 규칙을 이용하는 기법이다. 틀린 표현은 '신경망과 통계적 분석 방법만을 사용한다'이며, 올바르게는 '오용탐지는 알려진 공격 패턴을 시그니처 또는 규칙과 대조한다'이다.

**오답 포인트**

①은 이상탐지와 오용탐지의 기준을 서로 바꾸어 놓았고, ②는 새로운 공격 탐지에 관한 두 기법의 장단점을 뒤집었다. ④의 '신경망과 통계적 분석'은 정상 행위의 모델을 만드는 이상탐지에서 활용될 수 있는 방법인데 이를 오용탐지의 유일한 방법처럼 표현한 것이 함정이다.

**다시 나오면 이렇게 판단**

선지에서 '정상 행위의 기준선·기준 이탈·미지의 공격·높은 오탐률'이 보이면 이상탐지로 판단한다. '공격 시그니처·규칙·패턴 일치·알려진 공격·새로운 공격에 취약'이 보이면 오용탐지로 판단한다.

**암기 포인트**

이상탐지는 정상에서 벗어난 것을 찾고, 오용탐지는 알려진 공격과 같은 것을 찾는다.

NoteBase

**문 19. 다음에서 설명하고 있는 공격 방법으로 옳지 않은 것은?**

프로토콜의 오류 제어 기능을 악용하는 방식으로, TCP 패킷의 시퀀스 넘버를 조작하여 공격대상이 반복적인 재요청과 수정을 계속하도록 함으로써 시스템 자원을 고갈시키는 공격이다.

① Boink 공격
② Land 공격
③ Bonk 공격
④ Teardrop 공격

**정답 2번**

**출제 포인트**

비정상적인 패킷의 순서·분할 정보를 이용해 오류 처리와 재조립을 반복시키는 공격과 Land 공격을 구별하는 문제이다.

**핵심 개념**

Boink·Bonk·Teardrop 공격은 패킷의 시퀀스 번호나 조각의 오프셋 등 순서·분할 정보를 비정상적으로 만들어 수신 측의 오류 처리 또는 재조립 과정에 부담을 주는 서비스 거부 공격이다.
Land 공격은 출발지와 목적지의 IP 주소 및 포트 번호를 같게 조작한 패킷을 보내 공격 대상이 자기 자신에게 응답하도록 만드는 서비스 거부 공격이다.

**선지별 해설**

① O — Boink 공격은 비정상적인 TCP 시퀀스 번호를 이용해 수신 측이 오류 처리와 재전송 관련 작업을 반복하게 하므로 제시된 설명에 해당한다.
② X — Land 공격은 TCP 시퀀스 번호를 조작해 반복 재요청을 유발하는 공격이 아니다. 틀린 표현은 ‘Land 공격’이며, 실제로는 출발지와 목적지의 IP 주소 및 포트 번호를 같게 위조하여 공격 대상이 자기 자신에게 응답하도록 만드는 공격이다.
③ O — Bonk 공격은 비정상적인 IP 조각과 오프셋 정보를 보내 재조립 과정에 오류와 과부하를 일으키므로, 프로토콜의 오류 처리 기능을 악용하는 공격에 해당한다.
④ O — Teardrop 공격은 서로 겹치거나 모순되는 IP 조각의 오프셋을 보내 정상적인 재조립을 방해하므로, 오류 처리와 재조립 부담으로 자원을 고갈시키는 공격에 해당한다.

NoteBase

**오답 포인트**

네 공격이 모두 서비스 거부 공격이라는 공통점만 보면 Land 공격도 같은 유형으로 오인하기 쉽다. 이 문항의 구분점은 '패킷 순서·분할 정보의 이상으로 오류 처리나 재조립을 반복시키는가'이다. Land 공격은 주소와 포트를 동일하게 위조하는 방식이므로 작동 원리가 다르다.

**다시 나오면 이렇게 판단**

시퀀스 번호·조각 오프셋·재조립 오류가 핵심이면 Boink·Bonk·Teardrop 계열로 판단한다. 출발지와 목적지의 IP 주소 및 포트가 같아 공격 대상이 자기 자신에게 응답한다면 Land 공격으로 판단한다.

**암기 포인트**

Boink·Bonk·Teardrop은 순서·조각 재조립 교란, Land는 출발지와 목적지를 동일하게 만든 자기 응답 공격이다.

NoteBase

**문 20. HTTP 상태코드에 관한 설명으로 가장 적절하지 않은 것은?**

① 200 OK : 서버의 요청이 성공했다는 것을 나타낸다.

② 403 Forbidden : 클라이언트가 요청한 서버의 접근을 차단한다.

③ 404 Not Found : 클라이언트가 요청한 서버의 페이지가 존재하지 않는다.

④ 500 Internal Server Error : 서버가 클라이언트의 요청을 실행할 수 없을 때 발생한다.

**정답 1번**

**출제 포인트**

HTTP 상태 코드가 나타내는 요청 처리 결과를 정확히 구분하는 문제이다.

**핵심 개념**

2xx는 요청의 성공적인 처리를, 4xx는 클라이언트 요청과 관련된 오류를, 5xx는 서버가 요청을 처리하는 과정에서 발생한 오류를 나타낸다.
200 OK는 클라이언트의 요청이 성공적으로 처리되었음을 뜻한다. 403 Forbidden은 서버가 요청을 이해했지만 그 처리를 거부했음을, 404 Not Found는 요청한 자원을 찾지 못했음을, 500 Internal Server Error는 서버의 예기치 않은 상태 때문에 요청을 처리하지 못했음을 뜻한다.

**선지별 해설**

① X
'서버의 요청이 성공했다'는 표현이 틀렸다. HTTP 응답 상태 코드 200 OK는 서버가 보낸 요청이 아니라 클라이언트가 서버에 보낸 요청이 성공적으로 처리되었음을 나타낸다. 올바르게는 '클라이언트의 요청이 성공적으로 처리되었다'이다.

② O
403 Forbidden은 서버가 클라이언트의 요청을 이해했지만 접근 권한 등의 이유로 요청 처리를 거부하는 상태이다. 따라서 서버가 요청된 자원에 대한 접근을 허용하지 않는다는 취지의 설명은 적절하다.

③ O
404 Not Found는 서버가 클라이언트가 요청한 자원을 찾지 못했음을 나타낸다. 요청한 페이지가 존재하지 않는 경우가 대표적이므로 설명이 적절하다.

④ O
500 Internal Server Error는 서버 내부의 예기치 않은 오류로 인해 서버가 요청을 정상적으로 처리하지 못했음을 나타낸다. 따라서 서버가 클라이언트의 요청을 실행할 수 없을 때 발생한다는 설명은 적절하다.

NoteBase

**오답 포인트**

①은 200 OK의 '성공'이라는 핵심어 자체는 맞지만 성공한 주체를 '서버의 요청'으로 바꿔 놓았다. HTTP 상태 코드는 서버가 클라이언트의 요청을 처리한 결과를 응답으로 알려 주는 코드라는 점이 함정이다.

**다시 나오면 이렇게 판단**

먼저 코드의 첫 자리로 성공·클라이언트 오류·서버 오류를 구분하고, 이어서 상태 설명에서 요청의 주체와 처리 결과가 정확한지 확인한다.

**암기 포인트**

200은 성공, 403은 처리 거부, 404는 자원 없음, 500은 서버 내부 오류이다.

NoteBase