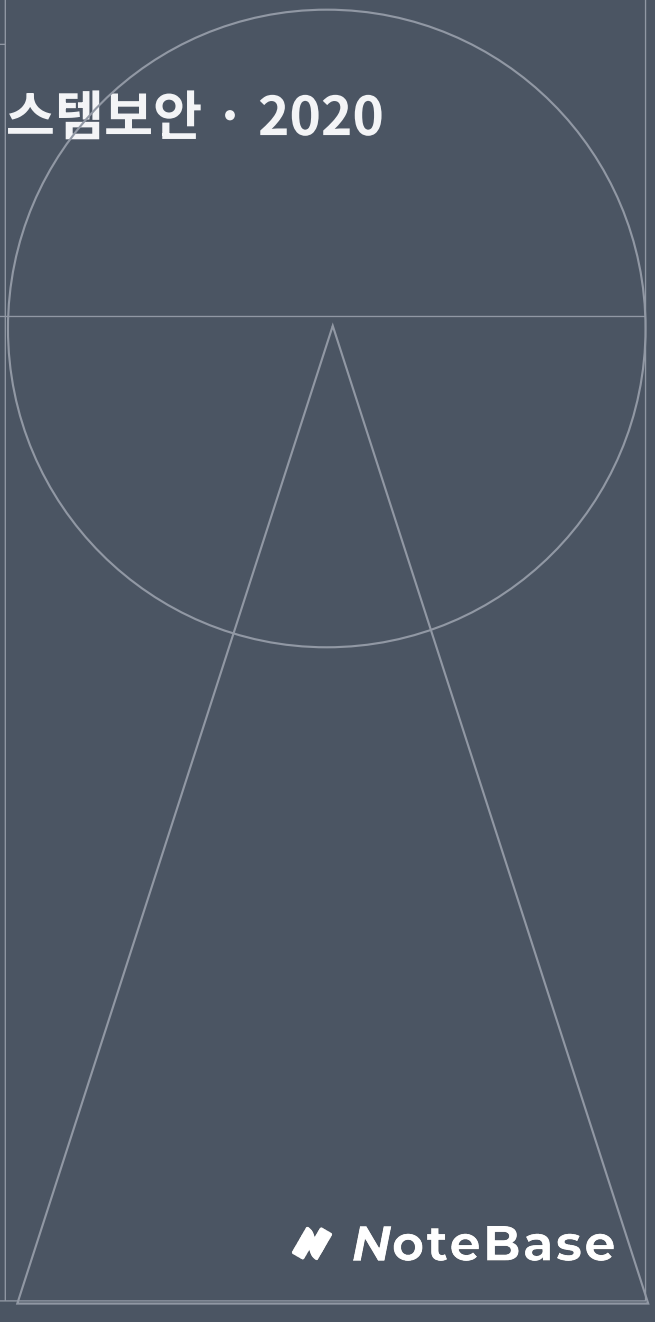
기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2020



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2020

공무원/국가직/9급 · 정보시스템보안 · 2020

문 1. 해시함수 알고리즘에 해당하지 않는 것은?

① SHA1

② MD5

③ RMD160

④ IDEA

정답 4번

간단한 해설

IDEA는 해시함수가 아니라 **대칭키 블록 암호 알고리즘**이다. 메시지를 고정 길이의 요약값으로 바꾸는 해시함수와 달리, 키를 이용해 암호화하고 복호화하여 원문을 복원한다.

선지별 해설

① O: SHA1(SHA-1)은 메시지로부터 **160비트 해시값**을 생성하는 해시함수이다. 입력 메시지의 길이가 달라도 출력 길이는 160비트로 일정하다.

② O: MD5는 메시지로부터 **128비트 해시값**을 생성하는 해시함수이다. SHA1과 출력 길이는 다르지만, 메시지의 요약값을 만든다는 점에서 같은 해시함수 범주에 속한다.

③ O: RMD160은 RIPEMD-160을 가리키며, **160비트 해시값**을 생성하는 해시함수이다. SHA1과 출력 길이는 같지만 서로 다른 알고리즘이다.

④ X: IDEA는 **대칭키 블록 암호 알고리즘**으로 분류해야 한다. 128비트 키를 사용하여 데이터를 64비트 블록 단위로 암호화한다. 키를 이용한 복호화로 원문을 복원하는 방식이며, 메시지의 요약값을 만드는 해시함수와 구별된다.

NoteBase

문 2. 사용자가 별도의 인프라를 구축하지 않고 인터넷을 통해 가상서버, 가상 PC 등의 컴퓨팅 자원을 이용하는 클라우드 서비스 유형은?

① PIMS

② IaaS

③ SaaS

④ ISMS

정답 2번

간단한 해설

가상서버·가상 PC처럼 **인프라 자원을 인터넷으로 제공**받아 이용하는 방식은 IaaS이다. 사용자가 물리적인 서버 등 기반 설비를 직접 구축할 필요가 없다.

공통 해설

IaaS(Infrastructure as a Service)는 서버·저장장치·네트워크 등의 컴퓨팅 기반 자원을 서비스로 제공하는 클라우드 유형이다. 제공자가 물리적인 기반 설비를 구축·관리하고, 사용자는 인터넷을 통해 필요한 자원을 할당받아 이용한다. 문제에서 별도의 인프라 구축 없이 가상서버·가상 PC를 이용한다는 것은 이러한 **기반 자원의 제공**을 뜻하므로 IaaS에 해당한다.

서비스 유형을 구별하는 기준은 인터넷 접속 여부만이 아니라 제공받는 대상이다. SaaS는 **완성된 응용 소프트웨어**를 이용하는 방식인 반면, 여기서는 그 소프트웨어를 실행할 수 있는 컴퓨팅 자원 자체를 제공받는다.

NoteBase

문 3. 리눅스 환경에서 사용되는 명령어에 대한 설명으로 옳지 않은 것은?

① touch - 파일 내의 특정 문자열을 검색할 때 사용한다.

② chown - 파일이나 디렉터리의 소유자를 변경할 때 사용한다.

③ mv - 파일을 다른 디렉터리로 이동하거나 파일명을 바꿀 때 사용한다.

④ df - 파일 시스템의 사용 중이거나 사용 가능한 디스크 공간에 대한 정보를 보여 준다.

정답 1번

간단한 해설

touch는 **파일의 접근·수정 시각을 갱신**하는 명령어이며, 지정한 파일이 없으면 기본적으로 빈 파일을 만든다. 파일 내용에서 특정 문자열을 검색할 때는 **grep**을 사용한다.

선지별 해설

① X: touch는 **파일의 접근·수정 시각을 갱신**하며, 지정한 파일이 없으면 기본적으로 빈 파일을 생성한다. 파일 내용에서 특정 문자열을 검색하는 명령어는 grep이다. 예를 들어 'grep error log.txt'는 log.txt에서 'error'와 일치하는 문자열이 포함된 행을 출력한다.

② O: chown은 파일이나 디렉터리의 **소유자를 변경**한다. 예를 들어 'chown alice report.txt'는 report.txt의 소유자를 alice로 바꾸는 명령이다. 실제 변경에는 해당 작업을 수행할 권한이 필요하다.

③ O: mv는 파일을 **이동하거나 이름을 변경**한다. 예를 들어 'mv report.txt backup/'은 파일을 backup 디렉터리로 옮기고, 'mv old.txt new.txt'는 같은 디렉터리에서 파일명을 바꾼다.

④ O: df는 **파일 시스템별 디스크 공간 사용 현황**을 보여 준다. 전체 공간, 사용 중인 공간, 사용 가능한 공간 등을 확인할 수 있으므로 파일 시스템의 여유 공간을 점검할 때 사용한다.

NoteBase

문 4. 디지털 포렌식의 원칙 중에 “수집된 증거가 위·변조되지 않았음을 증명해야 한다”는 원칙은?

① 정당성의 원칙

② 신속성의 원칙

③ 무결성의 원칙

④ 연계 보관성의 원칙

정답 3번

간단한 해설

수집된 증거가 **위·변조되지 않았음**을 증명하는 것은 증거 내용의 동일성을 보장하는 **무결성의 원칙**이다.

공통 해설

무결성의 원칙은 수집된 디지털 증거의 내용이 바뀌지 않고 유지되어야 한다는 원칙이다. 증거를 수집한 뒤 보관·분석·제출하는 과정에서도 **수집 당시의 내용과 동일함**을 입증할 수 있어야 한다. 문제의 '위·변조되지 않았음을 증명해야 한다'는 요구는 바로 이러한 증거 내용의 동일성에 관한 것이므로 무결성의 원칙에 해당한다.

NoteBase

문 5. 리버스 엔지니어링에 대한 설명으로 옳지 않은 것은?

① 안티 디버거는 안티 리버싱의 방법이다.

② 안티 리버싱은 리버스 엔지니어링을 쉽게 만드는 기술이다.

③ 리버스 엔지니어링에서 이용하는 도구는 OllyDbg와 IDA가 있다.

④ 완성된 소프트웨어를 역으로 분석하는 방법이다.

정답 2번

간단한 해설

②의 '쉽게 만드는'은 안티 리버싱의 목적을 반대로 설명한 것이다. 안티 리버싱은 프로그램의 구조와 동작을 알아내는 **역분석을 어렵게 만드는** 기술이다.

선지별 해설

① O: 안티 디버거는 디버거를 이용한 분석을 탐지하거나 방해하는 수단이다. 프로그램을 실행하면서 내부 상태를 살펴보는 **동적 분석을 어렵게 하므로** 안티 리버싱의 한 방법에 해당한다.

② X: 안티 리버싱은 소프트웨어의 구조와 동작을 분석하기 어렵게 하여 내부 구현을 보호하는 기술이다. 따라서 '리버스 엔지니어링을 쉽게 만드는 기술'은 **'리버스 엔지니어링을 어렵게 만드는 기술'**로 고쳐야 한다. 코드의 의미를 알아보기 어렵게 바꾸는 난독화나 디버깅을 방해하는 기법 등이 이에 해당한다.

③ O: OllyDbg와 IDA는 모두 리버스 엔지니어링에 이용된다. OllyDbg는 프로그램을 실행하면서 명령어와 메모리 등의 상태를 살펴보는 디버거이고, IDA는 **기계어를 어셈블리 명령어로 풀어 보여 주는** 디스어셈블러로 코드 구조와 흐름을 분석하는 데 쓰인다.

④ O: 리버스 엔지니어링은 **완성된 소프트웨어에서 구조와 동작 원리를 거슬러 파악하는** 분석 방법이다. 설계와 소스 코드로 실행 프로그램을 만드는 개발 과정과 반대 방향으로, 실행 파일의 명령어나 실행 중의 동작을 분석하여 내부 구현을 이해한다.

NoteBase

문 6. 스마트폰 이용자들에게 돌잔치, 결혼 청첩장, 교통법규 위반 통보 문자를 보내, 이를 클릭하는 순간 악성코드가 설치되고, 이를 통해 피해자의 개인정보를 탈취하는 기법은?

① 스미싱
② 루트킷
③ 스턱스넷
④ 키로깅

정답 1번

간단한 해설

청첩장이나 교통법규 위반 통보를 가장한 **문자메시지로 악성 링크 클릭을 유도**하고 개인정보를 탈취하는 수법은 **스미싱**이다. 문자 내용을 믿게 만들어 악성코드 감염으로 이어지게 한다.

공통 해설

스미싱은 문자메시지(SMS)를 이용한 피싱이다. 피싱은 상대를 속여 개인정보 등을 빼내는 공격이며, 스미싱은 그 유인 수단으로 **문자메시지**를 사용한다. 따라서 이 사례의 기법을 식별하는 기준은 개인정보 탈취라는 결과뿐 아니라, 문자로 이용자를 속여 악성 링크를 누르게 한다는 공격 방식이다.

제시된 돌잔치·결혼 청첩장·교통법규 위반 통보는 이용자가 내용을 확인하도록 만드는 미끼이다. 이용자가 문자 속 링크를 누르면 악성코드가 설치되고, 이를 통해 개인정보가 탈취되는 흐름이 제시되어 있다. 이처럼 **문자를 통한 기만과 클릭 유도**를 출발점으로 하는 공격이므로 스미싱에 해당한다.

NoteBase

문 7. 백도어에 대한 설명으로 옳지 않은 것은?

① 백도어 공격 도구로는 NetBus, Back Orifice 등이 있다.

② 원격 백도어는 시스템 계정이 필요하고, 서버의 쉘을 얻어 내 관리자로 권한 상승할 때 사용하는 백도어이다.

③ 로컬 백도어는 시스템 내에서 동작하기 때문에 공격자는 해당 시스템에 접속할 수 있는 계정을 획득할 수 있어야 한다.

④ Schoolbus 공격도구는 기존의 트로이 목마처럼 서버 파일과 클라이언트 파일로 이루어져 있다.

정답 2번

간단한 해설

②의 '시스템 계정이 필요하고 관리자 권한으로 상승할 때 사용한다'는 **로컬 백도어**에 대한 설명이다. 원격 백도어는 네트워크를 통해 대상 시스템에 접근하는 통로로, **정상적인 시스템 계정 없이도 접속**할 수 있게 한다.

선지별 해설

① O: NetBus와 Back Orifice는 대상 컴퓨터에 설치되어 외부에서 명령을 보내거나 컴퓨터를 제어할 수 있게 하는 백도어 도구이다. 공격자는 이를 이용해 **정상적인 접근 절차를 우회**하여 시스템을 원격으로 조작할 수 있다.

② X: 시스템 계정을 확보한 뒤 내부에서 실행하여 관리자 권한을 얻는다는 설명은 **로컬 백도어**에 해당한다. 원격 백도어는 네트워크를 통한 접근 통로를 제공하며, 공격자가 대상 시스템의 정상 계정을 갖고 있지 않아도 접속할 수 있게 한다. 따라서 시스템 계정과 내부 권한 상승을 원격 백도어의 필수 조건으로 설명한 부분을 고쳐야 한다.

③ O: 로컬 백도어는 **대상 시스템 내부에서 실행**하는 형태이므로, 공격자는 먼저 해당 시스템에 접속할 수 있는 계정 등 내부 접근 기반을 확보해야 한다. 일반 사용자 권한으로 접속한 뒤 더 높은 권한을 얻는 데 사용하는 경우가 이에 해당한다.

④ O: Schoolbus는 **서버 파일과 클라이언트 파일**로 구성되는 백도어 기능의 트로이 목마이다. 피해 시스템에서 서버 프로그램이 실행되면, 공격자는 클라이언트 프로그램을 통해 명령을 보내 피해 시스템을 원격으로 제어한다.

NoteBase

문 8. 다음 설명에 해당하는 시스템 메모리 기본구조의 영역은?

프로그램이 실행될 때까지 알 수 없는 가변적인 양의 데이터를 저장하기 위해 프로그램의 프로세스가 사용할 수 있도록 예약되어 있는 메인 메모리의 영역으로, 프로그램들에 의해 할당되었다가 회수되는 작용이 되풀이된다. 프로그램들이 요구하는 블록의 크기나 요구/횟수 순서에 일정한 규칙이 없다.

① 힙(Heap) 영역

② 스택(Stack) 영역

③ 텍스트(Text) 영역

④ 데이터(Data) 영역

정답 1번

간단한 해설

실행 중 필요한 크기의 메모리 블록을 할당하고, 사용이 끝나면 회수하는 영역은 **힙(Heap)**이다. 블록의 할당·회수 순서가 스택처럼 일정한 규칙에 묶이지 않는다는 점이 결정적인 단서이다.

공통 해설

힙(Heap) 영역은 프로그램 실행 중 필요한 크기의 메모리 블록을 동적으로 할당하고, 더 이상 필요하지 않은 블록을 회수하여 재사용하는 영역이다. 저장할 데이터의 양이 실행 전에 정해지지 않아도 실행 중 필요에 따라 공간을 확보할 수 있다. 따라서 제시문의 가변적인 데이터와 반복적인 할당·회수는 힙의 동적 메모리 관리에 해당한다.

힙에서는 **할당한 순서의 역순으로만 회수할 필요가 없다**. 예를 들어 A 블록을 할당한 뒤 B 블록을 할당했더라도, A가 먼저 필요 없어지면 B를 유지한 채 A를 해제할 수 있다. 이는 나중에 쌓인 것이 먼저 제거되는 스택의 후입선출 규칙과 구별된다.

NoteBase

문 9. 버퍼 오버플로우 공격에 대한 설명으로 옳지 않은 것은?

① 버퍼 오버플로우 공격의 종류 중에는 스택 기반 오버플로우와 힙 기반 오버플로우 공격이 있다.

② 버퍼 오버플로우 공격은 프로그램의 메모리 버퍼를 넘치게 해서 프로그램의 이상 동작을 유발하는 기법이다.

③ 버퍼 오버플로우 공격에 대응하기 위해서는 프로그램을 작성할 때 strcat(), strcpy(), getwd(), gets(), scanf() 등 입출력에 대한 사용자의 접근 가능성이 높은 함수를 사용한다.

④ 버퍼 오버플로우 공격의 대응 방법 중에는 Non-Executable Stack, Stack Guard, Stack Shield가 있다.

정답 3번

간단한 해설

strcpy(), gets()처럼 **버퍼 크기에 맞춰 쓰기 길이를 제한하지 않는 함수**를 사용하는 것은 버퍼 오버플로우 대응책이 아니다. 입력·복사 길이가 버퍼의 용량을 넘지 않도록 검사하고, 길이를 제한할 수 있는 함수를 사용해야 한다.

선지별 해설

① O: 버퍼가 놓인 메모리 영역에 따라 **스택 기반과 힙 기반** 오버플로우로 구분할 수 있다. 스택 기반은 함수의 지역 배열 등이 저장되는 스택 영역에서, 힙 기반은 malloc() 등으로 동적 할당한 힙 영역에서 버퍼의 경계를 넘겨 쓰는 경우이다.

② O: 버퍼 오버플로우는 **확보된 버퍼의 경계를 넘어 데이터를 쓰는 것**이다. 이 과정에서 인접한 데이터나 함수의 복귀 주소 등이 훼손되면 프로그램이 비정상 종료되거나 공격자가 의도한 코드가 실행되는 등 이상 동작이 발생할 수 있다.

③ X: strcat(), strcpy(), getwd(), gets()는 대상 버퍼의 크기를 인자로 받지 않으므로, 충분한 공간을 확보하거나 길이를 검사하지 않으면 버퍼 경계를 넘겨 쓸 위험이 있다. scanf()도 문자열을 입력받을 때 최대 필드 폭을 지정하지 않으면 같은 문제가 생길 수 있다. 대응의 기준은 사용자의 접근 가능성이 아니라 **입력·복사 길이를 버퍼 용량 안으로 제한하는 것**이다. gets() 대신 버퍼 크기를 지정하는 fgets()를 사용하고, 문자열 저장 시에는 끝을 나타내는 널 문자 공간까지 확보해야 한다.

④ O: Non-Executable Stack은 **스택 영역의 실행 권한을 제거**하여 스택에 주입된 코드의 실행을 막는다. Stack Guard는 스택에 둔 검사값인 카나리의 변조를 확인하여 복귀 주소를 덮어쓰는 공격을 탐지한다. Stack Shield는 복귀 주소의 사본을 별도 영역에 보관하여 변조된 복귀 주소가 사용되는 것을 방지한다.

NoteBase

문 10. 파일 시스템에 대한 설명으로 옳지 않은 것은?

① 파일 시스템은 파일을 체계적으로 기록하는 방식으로 파일이 어디에 저장되어 있는지 조직화하고 구조적으로 정의한다.

② EXT(Extended File System) 파일 시스템은 리눅스 고유의 파일 시스템으로 계속 업그레이드가 되어지고 있다.

③ 슈퍼 블록은 파일 시스템을 관리하는 데 필요한 블록의 총수, 사용 중인 블록 및 이용 가능한 블록 정보를 포함하여 좀 더 빠르고 효과적인 파일 시스템 관리를 가능하게 한다.

④ FAT(File Allocation Table) 파일 시스템은 연결리스트를 사용하기 때문에 검색 시간이 짧으며 단편화 현상이 없도록 NTFS(New Technology File System)의 많은 제약 사항을 개선한 파일 시스템이다.

정답 4번

간단한 해설

FAT는 클러스터의 연결을 따라가는 방식이므로 **임의 위치의 데이터에 빠르게 접근한다고 볼 수 없고**, 파일이 여러 위치에 흩어지는 단편화도 발생할 수 있다. 또한 FAT가 NTFS를 개선한 것이 아니라 **NTFS가 FAT의 제약을 개선한 것**이다.

NoteBase

선지별 해설

① O: 파일 시스템은 저장 장치에서 파일의 이름, 디렉터리 구조, 저장 위치 등을 관리하는 규칙과 자료 구조이다. 파일의 논리적 이름과 **실제 데이터가 저장된 위치를 연결**하여 운영체제가 파일을 저장하고 찾아 읽을 수 있게 한다.

② O: EXT는 리눅스를 위해 개발된 파일 시스템 계열이다. ext에서 ext2·ext3·ext4로 발전했으며, ext3는 ext2에 **저널링 기능**을 추가했다. 저널링은 파일 시스템의 변경 내역을 로그로 기록하여 장애가 발생했을 때 일관성을 복구하는 데 도움을 주는 기능이다. ext4에서는 대용량 지원과 성능 등이 개선되었다.

③ O: 슈퍼 블록은 파일 시스템 전체를 관리하는 데 필요한 요약 정보를 담는다. 전체 블록 수, 빈 블록 수, 블록 크기 등의 정보를 이용해 **공간의 사용 상태와 가용량을 파악**할 수 있다. 예를 들어 전체 블록 수와 빈 블록 수를 알면 사용 중인 블록 수를 구할 수 있으므로, 공간 상태를 확인할 때 모든 데이터 블록을 하나씩 조사할 필요가 없다.

④ X: FAT는 파일 할당 테이블에 각 클러스터의 다음 클러스터 번호를 기록하여 파일을 연결 리스트 형태로 관리한다. 파일 중간의 위치를 찾으려면 앞선 연결을 따라가야 하므로 **연결 리스트라는 이유로 검색 시간이 짧아지는 것은 아니다**. 예를 들어 파일의 클러스터가 2 → 7 → 4로 연결되어 있다면 세 번째 클러스터를 찾을 때 앞의 연결 정보를 거친다. 클러스터들이 떨어져 배치될 수 있으므로 파일 단편화도 발생한다. 또한 개선 관계가 반대로 서술되어 있으며, **NTFS가 FAT의 제약을 개선**하여 접근 권한 관리와 복구 기능 등을 강화한 파일 시스템이다.

NoteBase

문 11. 인증, 무결성, 부인봉쇄, 기밀성 등의 기능을 지원하는 이메일 보안 기술은?

① TFTP

② S/MIME

③ WEP

④ WPA

정답 2번

간단한 해설

S/MIME는 이메일에 **전자서명과 암호화**를 적용한다. 전자서명으로 인증·무결성·부인방지를, 암호화로 기밀성을 지원한다.

공통 해설

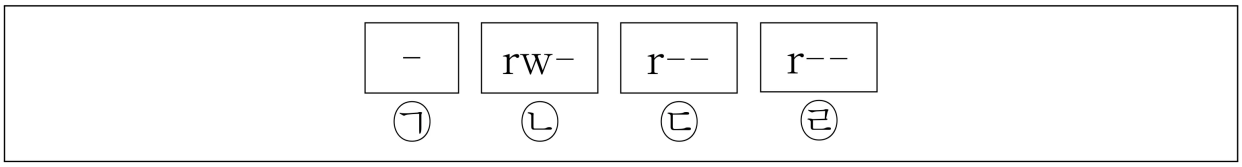
S/MIME는 MIME 형식의 이메일 메시지에 전자서명과 암호화 기능을 제공하는 보안 기술이다. 구별 기준은 **이메일 메시지 자체에 서명과 암호화를 적용**하여 보호하는지이다.

전자서명은 발신자의 개인키로 생성하고 대응하는 공개키로 검증한다. 이를 통해 발신자를 확인하는 인증, 메시지가 변경되었는지 확인하는 무결성, 발신자가 메시지에 서명했다는 증거를 남기는 부인방지를 지원한다. 문제의 '부인봉쇄'는 이러한 부인방지 기능을 가리킨다. 암호화는 허가받지 않은 사람이 이메일 내용을 읽지 못하게 하여 기밀성을 제공한다.

TFTP는 파일 전송 프로토콜이고, WEP와 WPA는 무선 LAN을 보호하는 보안 기술이다. 이들은 S/MIME처럼 이메일 메시지에 전자서명과 암호화를 적용하는 규격이 아니다.

NoteBase

문 12. 유닉스/리눅스 시스템에서 다음의 권한 설정에 대한 설명으로 옳지 않은 것은?



① ㉠은 파일 및 디렉터리의 종류로서 '-'는 디렉터리를 나타낸다.

② ㉡은 파일 및 디렉터리 소유자의 권한이다.

③ ㉢은 파일 및 디렉터리 그룹의 권한이다.

④ ㉣은 해당 파일 및 디렉터리의 소유자도 그룹도 아닌 제3자의 사용자에 대한 권한이다.

정답 1번

간단한 해설

㉠의 '-'는 **일반 파일**을 나타내며, 디렉터리는 **'d'**로 표시한다. 맨 앞의 파일 종류 표시와 뒤에 이어지는 접근 권한을 구분해야 한다.

선지별 해설

권한 표시는 맨 앞 한 자리의 파일 종류와, 그 뒤에 세 자리씩 이어지는 소유자·그룹·기타 사용자의 권한으로 구성된다. 각 권한 묶음에서 r은 읽기, w는 쓰기, x는 실행을 뜻하며, 해당 자리에 '-'가 있으면 그 권한이 없다는 뜻이다.

① X: ㉠은 파일의 종류를 나타내는 첫 번째 문자이다. 그림의 '-'는 **일반 파일**을 뜻하며, 디렉터리를 나타내는 문자는 'd'이다. 따라서 '-'가 디렉터리를 나타낸다는 부분을 일반 파일을 나타낸다는 내용으로 고쳐야 한다.

② O: ㉡은 파일 종류 표시 바로 뒤의 세 자리로, **소유자에게 적용되는 권한**이다. 그림의 'rw-'는 소유자가 파일을 읽고 수정할 수 있지만 실행할 수는 없다는 뜻이다.

③ O: ㉢은 가운데 세 자리로, **파일의 소유 그룹에 속한 사용자에게 적용되는 권한**이다. 그림의 'r--'는 그룹 사용자에게 읽기 권한만 있고 쓰기와 실행 권한은 없다는 뜻이다.

④ O: ㉣은 마지막 세 자리로, **소유자도 아니고 소유 그룹에도 속하지 않는 사용자**에게 적용되는 권한이다. 그림의 'r--'는 이들에게 읽기만 허용하고 쓰기와 실행은 허용하지 않는다는 뜻이다.

NoteBase

문 13. Cookie에 대한 설명으로 옳지 않은 것은?

① 쿠키는 클라이언트의 컴퓨터에 생성된다.

② 사용자와 웹사이트를 연결해 주는 정보가 저장되어 있다.

③ 직접 바이러스를 옮기거나 악성코드를 설치할 수 없다.

④ 사용자들의 로그인, 로그아웃, 시스템 재부팅 정보를 저장한다.

정답 4번

간단한 해설

④는 쿠키와 **로그 기록**의 역할을 혼동한 설명이다. 쿠키는 웹사이트가 사용자를 식별하거나 로그인 상태를 유지하는 데 쓰이며, 시스템의 로그인·로그아웃·재부팅 같은 사건의 이력은 로그에 기록한다.

선지별 해설

① O: 쿠키는 웹사이트의 요청 등에 따라 브라우저가 **클라이언트 컴퓨터에 저장하는 데이터**이다. 서버가 쿠키의 내용과 저장 조건을 지정하더라도 실제 저장은 사용자 측 브라우저가 담당한다.

② O: 쿠키에는 사용자를 구별하는 식별자나 사이트 이용 설정 등이 저장될 수 있다. 브라우저가 이후 요청에 해당 쿠키를 함께 보내면, 웹사이트는 이를 이용해 **이전 이용 상태와 현재 요청을 연결**할 수 있다. 예를 들어 로그인 후 받은 세션 식별자를 다음 요청에 보내면 서버가 해당 로그인 상태를 알아볼 수 있다.

③ O: 쿠키는 **스스로 실행되는 프로그램이 아닌 데이터**이므로, 그 자체가 직접 바이러스를 전파하거나 악성코드를 설치하지는 않는다. 쿠키를 이용한 사용자 추적이나 세션 식별자 탈취의 위험은 쿠키 자체가 악성코드를 실행한다는 뜻과 구별해야 한다.

④ X: 사용자들의 로그인·로그아웃·시스템 재부팅 같은 사건의 이력을 기록하는 것은 **로그**의 역할이다. 쿠키는 웹사이트 이용에 필요한 식별자나 상태 정보를 저장하는 데 쓰인다. 쿠키로 웹사이트의 로그인 상태를 유지할 수 있다는 것과, 운영체제의 로그인·로그아웃·재부팅 이력을 기록한다는 것은 다르다.

NoteBase

문 14. 다음에서 설명하고 있는 알고리즘은?

◯ 순수 국내 기술로 개발된 128비트 크기의 블록 암호 알고리즘
◯ Feistel 구조로 128비트 알고리즘이 있음
◯ 1999년 국내 표준으로 제정, 2005년에는 국제 표준 제정
◯ IETF RFC 4269

① RSA
② Triple DES
③ AES
④ SEED

정답 4번

간단한 해설

국내에서 개발한 128비트 Feistel 블록 암호이며 **RFC 4269**에 기술된 알고리즘은 **SEED**이다.

공통 해설

SEED는 국내에서 개발한 대칭키 블록 암호로, 128비트 데이터를 하나의 블록으로 처리하고 128비트 비밀키를 사용한다. 블록 크기는 한 번에 처리하는 데이터의 길이이고, 키 길이는 암호 연산에 사용하는 비밀키의 길이이다. SEED는 128비트 블록을 두 개의 64비트 부분으로 나누어 처리하는 **16라운드 Feistel 구조**를 사용한다.

RFC 4269는 SEED 암호 알고리즘을 기술한 문서이다. 따라서 국내 개발, 128비트 블록, Feistel 구조라는 특성과 RFC 4269라는 문서 번호를 함께 만족하는 알고리즘이 SEED이다.

NoteBase

문 15. CSRF(Cross Site Request Forgery)의 특징에 대한 설명으로 옳지 않은 것은?

① 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 방법이다.

② 사이트에 방문하는 사용자가 정상적인 요청이 아닌 임의의 요청을 하도록 위조하는 방법이다.

③ 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 사용하여 연결된 세션에 혼란을 줌으로써 공격자가 서버와의 연결을 획득하는 방법이다.

④ 특정 웹사이트가 사용자의 웹브라우저를 신용하는 상태를 악용하는 방법이다.

정답 3번

간단한 해설

③의 시퀀스 넘버를 이용한 연결 탈취는 **TCP 세션 하이재킹**에 관한 설명이다. CSRF는 연결을 탈취하는 대신 **사용자의 브라우저가 의도하지 않은 요청을 보내게** 하여 사용자의 권한을 악용한다.

선지별 해설

① O: CSRF는 사용자가 자신의 의지와 무관하게 공격자가 의도한 요청을 대상 웹사이트로 보내게 하는 공격이다. 요청을 전송하는 주체는 사용자의 브라우저이지만, **요청할 행위를 정한 것은 공격자**라는 점이 핵심이다.

② O: 공격자는 조작한 페이지나 링크 등을 통해 사용자의 브라우저가 대상 사이트로 위조된 요청을 보내도록 유도한다. 예를 들어 로그인된 사용자가 공격용 페이지를 열었을 때 대상 사이트로 계정 정보 변경 요청이 전송되게 하는 방식이다. 여기서 위조하는 것은 **사용자가 의도한 정상 요청인 것처럼 보이는 요청**이다.

③ X: 서버와 클라이언트 사이의 시퀀스 넘버 동기화를 흐트러뜨리고 기존 연결을 가로채는 것은 **TCP 세션 하이재킹**에 관한 설명이다. CSRF는 TCP 시퀀스 넘버를 조작하는 공격이 아니라, 사용자의 브라우저를 통해 위조된 웹 요청을 전송하여 사용자의 권한으로 원치 않는 행위가 실행되게 하는 공격이다.

④ O: 대상 사이트가 사용자의 브라우저에서 온 인증 정보를 신뢰하는 상태를 악용한다. 브라우저가 대상 사이트의 세션 쿠키를 함께 보내고 서버가 요청의 정당성을 별도로 확인하지 않으면, 공격자가 유도한 요청도 인증된 사용자의 요청으로 처리될 수 있다. 즉 **인증된 브라우저의 요청이라는 사실과 사용자가 의도한 요청이라는 사실은 다르다**.

NoteBase

문 16. 다음에서 설명하고 있는 공격에 해당하는 것은?

◯ 파일의 소유자가 root이어야 함
◯ SetUID 비트를 가져야 함
◯ 바로 생성되는 임시 파일의 이름을 알고 있어야 함

① 버퍼 오버플로우
② 포맷 스트링
③ 패스워드 크래킹
④ 레이스 컨디션

정답 4번

간단한 해설

root 권한으로 동작하는 프로그램이 사용할 임시 파일명을 알면, 공격자는 파일을 확인하고 실제로 사용하는 사이에 끼어들 수 있다. 이처럼 **처리 시점과 실행 순서의 틈**을 악용하는 것이 레이스 컨디션 공격이다.

공통 해설

레이스 컨디션은 여러 실행 흐름이 같은 자원에 접근할 때 **실행 시점이나 순서에 따라 결과가 달라지는 현상**이다. 공격자는 그 틈에 자원의 상태를 바꾸어 프로그램이 의도하지 않은 처리를 하도록 유도한다. 지문의 root 소유·SetUID는 공격 대상 실행 파일의 권한에 관한 단서이다. SetUID가 적용되면 실행 프로세스의 유효 사용자 ID가 파일 소유자의 것으로 바뀌므로, root 소유 프로그램은 root 권한으로 파일 작업을 수행할 수 있다.

임시 파일명을 미리 안다는 것은 공격자가 프로그램이 접근할 파일 경로를 예상할 수 있다는 뜻이다. 예를 들어 프로그램이 임시 파일의 존재 여부를 확인한 뒤 실제로 생성하거나 여는 사이에, 공격자가 같은 이름으로 다른 파일을 가리키는 심볼릭 링크를 만들 수 있다. 프로그램이 이를 구별하지 않고 링크를 따라 파일을 열면, 예상한 임시 파일 대신 다른 파일을 root 권한으로 처리할 수 있다. 이는 **확인 시점과 사용 시점 사이의 경쟁**을 악용한 레이스 컨디션의 사례이다.

세 단서는 이와 같은 특권 프로그램의 임시 파일 처리 공격을 함께 가리킨다. root 소유, SetUID, 임시 파일명에 대한 사전 지식이 모든 레이스 컨디션 공격에 반드시 필요한 것은 아니다.

NoteBase

문 17. SQL 인젝션에 대한 설명으로 옳지 않은 것은?

① 공격자가 입력값을 조작하여 원하는 SQL 구문을 실행한다.

② 전송되는 패킷을 가로채어 자신이 송신자인 것처럼 패킷을 변경하여 다시 보내는 기법이다.

③ 대응 방법 중에는 사용자의 입력에 특수문자가 포함되어 있는지 검증하는 방법이 있다.

④ OWASP에서 선정한 10대 웹 어플리케이션 보안 위험으로 SQL 인젝션의 취약점이 2004년, 2007년, 2010년, 2013년, 2017년에 포함되어 있다.

정답 2번

간단한 해설

②의 패킷 가로채기·변조는 SQL 인젝션의 작동 원리가 아니다. SQL 인젝션은 **입력값에 SQL 구문을 삽입**하여 애플리케이션이 의도하지 않은 데이터베이스 명령을 실행하게 하는 공격이다.

선지별 해설

① O: 애플리케이션이 사용자 입력을 SQL 구문에 그대로 이어 붙이면, 공격자가 넣은 내용이 단순한 데이터가 아니라 **SQL 명령의 일부로 해석**될 수 있다. 이를 이용해 조회 조건을 바꾸거나 허가되지 않은 데이터를 조회·변경하는 것이 SQL 인젝션이다.

② X: 전송 중인 패킷을 가로채 변경하고 송신자를 가장하여 보내는 것은 통신 내용의 변조와 송신자 위장에 관한 설명이다. SQL 인젝션은 **사용자 입력을 통해 SQL 구문의 의미를 바꾸는 공격**이며, 패킷을 가로채거나 송신자를 가장하는 과정이 필수인 것은 아니다.

③ O: 작은따옴표 등 SQL 구문의 의미에 영향을 줄 수 있는 특수문자를 검사하여 비정상 입력을 걸러내는 것은 입력값 검증의 한 방법이다. 다만 **특수문자 검사만으로 모든 SQL 인젝션을 막을 수는 없다**. 매개변수화된 질의를 사용하여 SQL 명령 구조와 입력 데이터를 분리하고, 입력값의 허용 형식도 함께 검증해야 한다.

④ O: SQL 인젝션은 OWASP Top 10의 **인젝션 범주에 포함**되어 왔다. 2004년과 2007년에는 'Injection Flaws', 2010년·2013년·2017년에는 'Injection' 항목에서 다루었으므로, 선지에 제시된 다섯 연도 모두에 포함되었다는 설명이 성립한다.

NoteBase

문 18. 와이파이(WiFi) 무선 네트워크에서 공격자가 가짜 AP(Access Point)를 구축하고 강한 신호를 보내어 사용자가 가짜 AP에 접속하게 함으로써 사용자 정보를 중간에서 가로채는 기법은?

① Zero Day

② DDoS

③ Evil Twin

④ DRDoS

정답 3번

간단한 해설

가짜 AP를 정상적인 무선 접속 지점처럼 보이게 하여 사용자를 연결시키고 정보를 가로채는 기법은 **Evil Twin**이다. 강한 신호는 사용자를 가짜 AP로 유인하는 수단이다.

공통 해설

AP(Access Point)는 무선 단말이 네트워크에 접속하도록 연결해 주는 장치이다. Evil Twin은 공격자가 정상 AP를 사칭하는 가짜 AP를 만들어 사용자의 접속을 유도하는 공격이다. 사용자가 이 AP에 연결하면 통신이 공격자의 장비를 거치므로, 공격자는 그 경로에서 사용자 정보를 가로챌 수 있다.

문제에서는 강한 신호로 가짜 AP에 접속하도록 유인한다. 핵심은 신호의 세기 자체가 아니라 **정상 AP로 가장한 접속 지점을 통해 통신을 가로채는 것**이며, 이 작동 방식에 해당하는 명칭이 Evil Twin이다.

NoteBase

문 19. HTTP에 대한 설명으로 옳지 않은 것은?

① 상태 코드 404는 클라이언트의 PUT요청이 성공적이라는 것을 의미한다.

② HTTP 1.0 프로토콜은 RFC 1945이고, HTTP 1.1 프로토콜은 RFC 2616에 기술되어 있다.

③ HTTPS는 SSL을 이용하여 클라이언트와 서버 사이에 주고받는 정보를 보호하는 데 사용된다.

④ Request는 웹서버에 데이터를 요청하거나 전송할 때 보내는 패킷으로 GET, POST와 같은 메소드를 사용한다.

정답 1번

간단한 해설

상태 코드 404는 PUT 요청의 성공이 아니라 **요청한 자원을 찾지 못했음**을 뜻한다. PUT으로 새 자원을 생성하면 201, 기존 자원을 성공적으로 수정하면 200 또는 204로 응답한다.

선지별 해설

① X: 404(Not Found)는 서버가 요청 URI에 해당하는 자원을 찾지 못했음을 나타내는 오류 응답이다. PUT은 지정한 URI의 자원을 생성하거나 수정하는 메소드이며, 성공 시 **새 자원 생성은 201, 기존 자원 수정은 200 또는 204**로 응답한다. 따라서 404를 PUT 요청의 성공 코드로 설명한 부분을 고쳐야 한다.

② O: **HTTP/1.0은 RFC 1945, HTTP/1.1은 RFC 2616**에 기술되어 있다. RFC 2616은 이후 다른 RFC들로 대체되었지만, HTTP/1.1을 기술한 문서라는 대응은 성립한다.

③ O: HTTPS는 HTTP 통신에 SSL을 적용하여 클라이언트와 서버 사이의 정보를 보호하는 방식으로 발전했다. 통신 내용을 암호화하여 도청을 막고 전송 중 변조를 탐지한다. **SSL의 후속 규약은 TLS**이며, 현재의 HTTPS는 TLS를 사용한다.

④ O: Request는 클라이언트가 서버에 보내는 **HTTP 요청 메시지**이다. GET은 지정한 자원의 정보를 가져오도록 요청하고, POST는 데이터를 서버로 보내 처리하도록 요청한다. 선지의 '패킷'은 전송되는 요청을 가리키는 표현이며, 정확한 HTTP 단위는 요청 메시지이다.

NoteBase

문 20. XSS는 'Cross Site Scripting'의 약자로 줄여서 CSS라고도 부르지만, 웹 레이아웃과 스타일을 정의할 때 사용되는 캐스케이딩 스타일 시트(Cascading Style Sheets)와 혼동되어 일반적으로 XSS라고 부른다. 일반적인 XSS 공격 수행 과정을 순서대로 바르게 나열한 것은?

가. 해당 웹 서비스 사용자가 공격자가 작성해 놓은 XSS 코드에 접근한다. 물론 사용자는 자신이 공격자가 작성해 놓은 XSS 코드에 접근한다는 것을 인지하지 못한다. 사용자는 어떤 게시판의 글을 읽는 과정에서 공격자의 XSS 코드에 접근하게 된다.
나. 사용자의 시스템에서 XSS 코드가 실행된다.
다. 웹 서버는 사용자가 접근한 XSS 코드가 포함된 게시판의 글을 사용자에게 전달한다.
라. 임의의 XSS 취약점이 존재하는 서버에 XSS 코드를 작성하여 저장한다. 일반적으로 공격자는 임의의 사용자나 특정인이 이용하는 게시판을 공격한다.
마. XSS 코드가 실행된 결과가 공격자에게 전달되고 공격자는 공격을 종료한다.

① 라 → 가 → 나 → 다 → 마
② 라 → 가 → 다 → 나 → 마
③ 라 → 다 → 가 → 나 → 마
④ 라 → 다 → 나 → 가 → 마

정답 2번

간단한 해설

사용자가 게시글을 요청하면 웹 서버가 XSS 코드가 포함된 글을 보내고, 그 뒤에 **사용자 브라우저에서 코드가 실행**된다. 따라서 사용자의 게시글 접근, 서버의 글 전달, 사용자 측 실행을 구분해야 한다.

NoteBase

올바른 순서

라 → 가 → 다 → 나 → 마

라. 코드 저장: 공격자가 XSS 취약점이 있는 웹 서비스의 게시판 등에 악성 코드를 저장한다. 사용자가 나중에 읽을 글에 코드가 남아 있다는 점에서 **저장형 XSS**의 과정이다.

가. 사용자의 접근: 사용자가 악성 코드가 들어 있는 게시글을 읽으려고 접근한다. 이 단계는 해당 글을 **서버에 요청**하는 단계이며, 사용자는 글에 공격 코드가 포함되어 있다는 사실을 인지하지 못한다.

다. 게시글 전달: 웹 서버가 사용자의 요청에 응답하여 XSS 코드가 포함된 게시글을 사용자에게 보낸다. 사용자 측에서 코드가 실행되려면 먼저 **코드가 포함된 응답을 받아야** 하므로 나보다 앞선다.

나. 코드 실행: 전달받은 게시글을 처리하는 과정에서 사용자 브라우저가 XSS 코드를 실행한다. 코드가 서버에 저장되어 있더라도 이 과정에서의 **실행 위치는 사용자 측**이다.

마. 실행 결과 전달: 제시된 공격 과정에서는 사용자 측에서 코드가 실행된 결과가 공격자에게 전달되고 공격이 종료된다. 실행 결과를 전달하는 단계이므로 코드 실행 뒤에 놓인다.

NoteBase