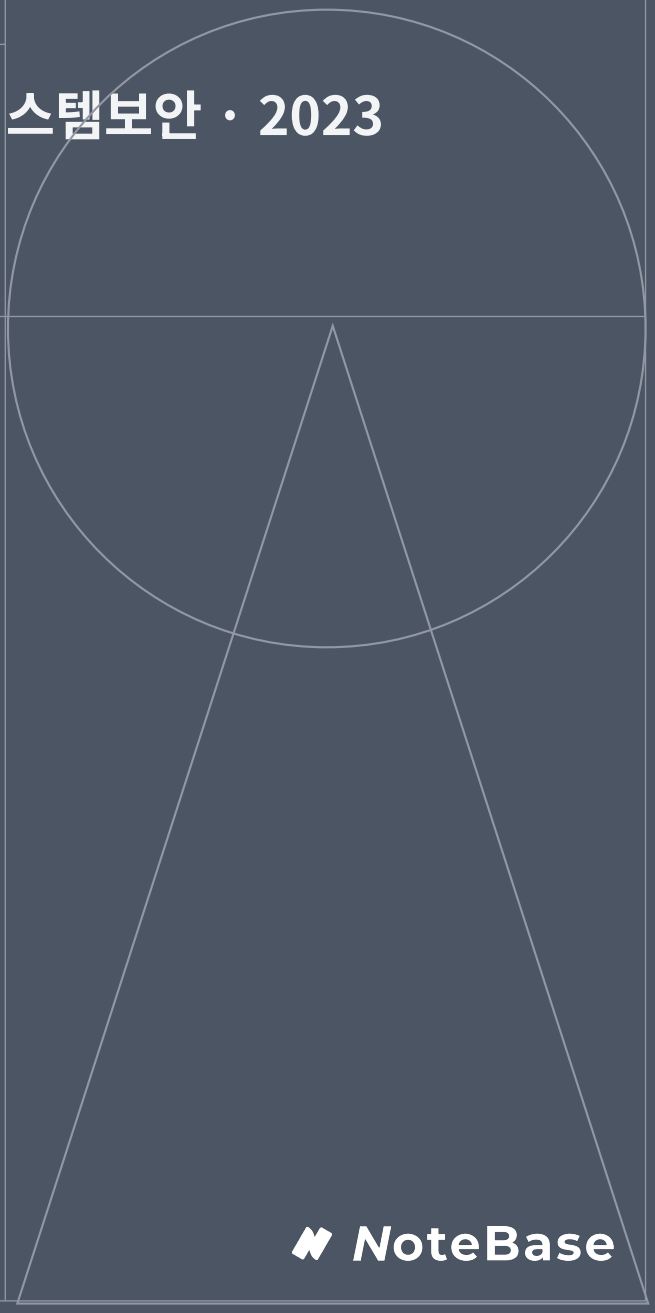
기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2023



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2023

공무원/국가직/9급 · 정보시스템보안 · 2023

문 1. 프로그램이 실행될 때마다 해당 프로그램이 사용하는 메모리 주소를 무작위로 배치하여 공격 대상 프로그램이 사용하는 메모리 주소를 추측하기 어렵게 만드는 리눅스 운영체제의 기능은?

① DLL

② Canary

③ ASLR

④ Packing

정답 3번

간단한 해설

메모리 주소의 무작위 배치는 ASLR의 특징이다. 공격자가 코드나 데이터의 위치를 미리 알아내 이용하기 어렵게 하여 메모리 공격의 성공 가능성을 낮춘다.

핵심 풀이

ASLR(Address Space Layout Randomization)은 주소 공간 배치 무작위화 기법이다. 프로그램 실행 시 스택·힙·공유 라이브러리 등의 가상 메모리 배치 위치를 무작위로 정한다. 공격자가 이전 실행에서 알아낸 주소를 다음 실행에서도 그대로 이용하기 어려워지므로, 발문의 '메모리 주소를 추측하기 어렵게 만든다'는 설명에 해당한다. 핵심은 **공격에 필요한 주소의 예측을 어렵게 하는 것**이다.

Canary는 스택에 검사값을 두고 함수가 복귀하기 전에 그 값의 변조 여부를 확인하여 버퍼 오버플로에 의한 스택 손상을 탐지하는 기법이다. ASLR이 메모리의 배치 위치를 바꾸는 데 비해 Canary는 **검사값의 변조를 탐지**한다는 점에서 구별된다.

NoteBase

문 2. 어떠한 작업을 주기적으로 실행시키기 위한 리눅스 명령어는?

① wc

② ps

③ df

④ crontab

정답 4번

간단한 해설

crontab은 **작업을 실행할 시각과 주기**를 등록·관리하는 명령어이다. 등록된 일정에 따라 cron이 작업을 자동으로 실행한다.

핵심 풀이

주기적 실행: **crontab**은 cron이 실행할 작업과 실행 일정을 등록·관리한다. crontab -e로 설정을 편집하여 실행할 시각과 명령을 지정하면, cron이 그 일정에 맞추어 작업을 실행한다. 예를 들어 매일 정해진 시각에 백업 스크립트를 실행하도록 예약할 수 있다.

다른 명령어와의 구분: wc는 텍스트의 줄 수·단어 수·바이트 수 등을 세고, ps는 프로세스 정보를 보여 주며, df는 파일 시스템의 디스크 공간 사용량을 보여 준다. 이들은 **정보를 집계하거나 조회**하는 명령어로, 작업의 반복 실행 일정을 등록하는 기능과 구별된다.

NoteBase

문 3. (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

리눅스에는 사용자의 비밀번호를 지정하거나 변경할 때 쓰이는 (가) 명령어가 있다. 이 명령어는 사용자의 비밀번호가 저장된 (나) 파일에 접근하여 기존 비밀번호를 새로 입력한 값으로 변경하는 기능을 한다. (가) 명령어를 일반 사용자가 실행하였다고 하더라도, 해당 프로세스가 관리자 계정만 접근권한이 있는 파일에 접근하여 비밀번호를 바꾸는 것이 가능한 이유는 (가) 명령어에 설정된 (다) 때문이다. 일반 사용자가 (다)가 설정된 (가) 명령어를 실행하면 해당 프로세스는 일시적으로 파일 소유자인 관리자(root)의 권한을 얻게 되어 관리자만 접근할 수 있는 (나) 파일에 접근하여 해당 사용자의 비밀번호를 수정할 수 있다.

① (가): passwrd, (나): /etc/shadow, (다): SetUID

② (가): passwrd, (나): /etc/passwd, (다): SetRID

③ (가): passwd, (나): /etc/shadow, (다): SetUID

④ (가): passwd, (나): /etc/shadow, (다): SetRID

정답 3번

간단한 해설

일반 사용자가 보호된 비밀번호 파일을 갱신할 수 있는 이유는 passwd 실행 파일의 **SetUID** 설정으로 프로세스가 **파일 소유자인 root의 권한**으로 동작하기 때문이다. 이때 갱신하는 /etc/shadow에는 비밀번호 원문이 아니라 해시값이 저장된다.

빈칸별 해설

(가) passwd: 사용자의 비밀번호를 설정하거나 변경하는 명령어이다. 일반 사용자는 자신의 비밀번호를 변경할 수 있다. 명령어 이름은 **passwrd가 아니라 passwd**이다.

(나) /etc/shadow: 섀도 비밀번호를 사용하는 리눅스에서 **비밀번호 해시값**과 비밀번호 만료 관련 정보를 저장하는 파일이다. /etc/passwd는 사용자 이름, 사용자 ID, 홈 디렉터리 등 계정 정보를 저장하며, 이 구성에서는 비밀번호 필드에 보통 'x'를 두어 해시값이 /etc/shadow에 따로 있음을 나타낸다. 일반 사용자가 /etc/shadow에 직접 접근하지 못하도록 제한하여 해시값의 노출을 막는다.

(다) SetUID: 실행 파일을 실행할 때 프로세스의 **유효 사용자 ID를 파일 소유자의 사용자 ID로 설정**하는 특수 권한이다. 문제처럼 root 소유의 passwd 실행 파일에 SetUID가 설정되어 있으면, 일반 사용자가 실행해도 해당 프로세스는 root의 권한으로 보호된 /etc/shadow를 갱신할 수 있다. 사용자의 로그인 계정 자체가 root로 바뀌는 것은 아니다.

따라서 (가) passwd, (나) /etc/shadow, (다) SetUID의 조합은 ③에 해당한다.

NoteBase

문 4. 다음과 같이 시스템에 설정된 umask 값이 '022'인 경우, 파일(file1)을 생성하였을 때 생성된 파일의 접근권한은?

```
[root@security ~]# umask
022
[root@security ~]# touch file1
```

① -rwxr-xr-x

② -r-xrwxrwx

③ -rw-r--r--

④ -rw-------

정답 3번

간단한 해설

새 일반 파일의 기본 권한 0666에서 umask 022가 지정한 **그룹·기타 사용자의 쓰기 권한**을 제거하면 0644, 즉 -rw-r--r--가 된다.

계산 과정

기본 권한: touch로 새 일반 파일을 만들 때 요청하는 기본 권한은 **실행 권한이 없는 0666**이다. 세 자리 666은 소유자·그룹·기타 사용자의 권한을 차례로 나타낸다. 읽기(r)는 4, 쓰기(w)는 2, 실행(x)은 1이므로, 각 자리의 6은 4 + 2로 읽기와 쓰기를 모두 허용한다는 뜻이다.

umask 적용: umask는 생성 시 **허용하지 않을 권한 비트를 지정**한다. 022에서 소유자에 해당하는 0은 제거할 권한이 없다는 뜻이고, 그룹과 기타 사용자에 해당하는 2는 쓰기 권한을 제거한다는 뜻이다. 따라서 소유자의 6은 유지되고, 그룹과 기타 사용자는 각각 읽기 권한 4만 남아 최종 권한이 0644가 된다.

결과 표기: 0644는 소유자 rw-, 그룹 r--, 기타 사용자 r--에 해당한다. 맨 앞에 일반 파일을 뜻하는 '-'를 붙이면 -rw-r--r--이며, 이는 ③의 접근권한과 일치한다.

NoteBase

문 5. 유닉스/리눅스 시스템의 로그 파일에 대한 설명으로 옳지 않은 것은?

① utmp 로그는 특정 시간에 로그인한 사용자의 정보를 텍스트 형태로 기록한다.

② wtmp 로그는 사용자의 로그인, 로그아웃, 시스템 재부팅 정보를 바이너리 형태로 기록한다.

③ su 로그는 su 명령어 수행에 따른 권한 변경 시도 및 변경 정보를 텍스트 형태로 기록한다.

④ pacct 로그는 시스템에 로그인한 모든 사용자가 수행한 프로그램의 정보를 바이너리 형태로 기록한다.

정답 1번

간단한 해설

utmp는 현재 로그인한 사용자의 정보를 **바이너리 형태**로 저장한다. '텍스트 형태'로 기록한다는 설명이 잘못되었다.

선지별 해설

① X: utmp는 현재 로그인한 사용자의 이름, 접속 터미널, 로그인 시각 등을 **바이너리 형태**로 저장한다. 따라서 '텍스트 형태'는 '바이너리 형태'로 고쳐야 한다. who 같은 명령으로 내용을 읽기 쉽게 출력할 수 있지만, 출력 결과가 문자로 보인다고 원본 파일이 텍스트 형식인 것은 아니다.

② O: wtmp는 사용자의 로그인·로그아웃과 시스템 재부팅 등의 이력을 바이너리 형태로 누적 기록한다. utmp가 현재 접속 상태를 확인하는 데 쓰인다면, wtmp는 **과거 접속 이력**을 확인하는 데 쓰인다.

③ O: su는 다른 사용자로 전환하여 그 사용자의 권한으로 명령을 실행할 때 사용하는 명령이다. su 로그는 전환을 시도한 사용자, 전환 대상 사용자, 실행 시각, 성공 여부 등을 텍스트 형태로 기록한다. 따라서 권한 변경에 성공한 경우뿐 아니라 **실패한 변경 시도**도 확인할 수 있다.

④ O: pacct는 사용자가 실행한 프로그램의 정보를 바이너리 형태로 남기는 프로세스 회계 로그이다. **프로세스 회계 기능이 활성화되어 있으면** 각 프로세스가 종료될 때 실행한 사용자, 프로그램 이름, CPU 사용 시간 등의 정보가 기록된다. 특정 사용자만이 아니라 시스템 사용자 전반의 프로그램 실행 내역을 확인하는 데 쓰인다.

NoteBase

문 6. 동일한 네트워크에 있는 DHCP 서버와 클라이언트 간의 동작 과정을 순서대로 나열한 것은?

(가) 서버는 UDP 목적지 포트 번호 68, 발신지 포트 번호 67로 지정한 뒤, 유니캐스트 메시지나 브로드캐스트 메시지를 클라이언트에 전송
(나) UDP 사용자 데이터그램(user datagram)으로 캡슐화 이후, IP 데이터그램으로 캡슐화
(다) DHCP 서버는 UDP 포트 번호 67에 수동 개방(passive open) 명령을 수행
(라) 부팅된 클라이언트는 포트 번호 68에 능동 개방(active open) 명령을 수행

① (다)→(나)→(라)→(가)
② (다)→(라)→(나)→(가)
③ (라)→(다)→(가)→(나)
④ (라)→(다)→(나)→(가)

정답 2번

간단한 해설

서버가 먼저 **UDP 67번 포트에서 요청을 기다려야** 부팅된 클라이언트가 통신을 시작할 수 있다. 전송할 DHCP 메시지는 **UDP로 감싼 뒤 IP로 감싸는** 캡슐화 과정을 거친다.

올바른 순서

(다) → (라) → (나) → (가)

(다) 서버의 수동 개방: DHCP 서버는 UDP 67번 포트를 열어 **클라이언트의 요청을 받을 준비**를 한다. 서비스를 제공하는 서버가 먼저 대기하고 있어야 클라이언트의 요청을 처리할 수 있다.

(라) 클라이언트의 능동 개방: 부팅된 클라이언트는 UDP 68번 포트를 사용할 준비를 하고 **먼저 서버에 요청을 보내 통신을 시작**한다. 클라이언트가 보내는 요청의 발신지 포트는 68번, 목적지 포트는 서버의 67번이다.
여기서 개방은 UDP 통신을 위한 준비를 뜻하며, TCP처럼 연결을 설정하는 절차를 뜻하지 않는다.

(나) 메시지의 캡슐화: DHCP 메시지에 UDP 헤더를 붙여 UDP 사용자 데이터그램을 만들고, 여기에 IP 헤더를 붙여 IP 데이터그램을 만든다. 즉, **응용 계층의 메시지를 전송 계층, 인터넷 계층 순으로 감싸야** 네트워크로 보낼 수 있다.

(가) 서버의 응답 전송: 요청을 받은 서버는 클라이언트에 응답을 보낸다. 서버에서 클라이언트로 향하므로 UDP 헤더의 **발신지 포트는 67번, 목적지 포트는 68번**이다. 클라이언트의 상태와 메시지 전달 조건에 따라 유니캐스트 또는 브로드캐스트로 전송한다.

NoteBase

문 7. (가)~(다)에 들어갈 용어를 바르게 연결한 것은?

○ (가)은 블루투스 공격 장치의 검색 활동을 뜻한다.
○ (나)은 블루투스의 취약점을 이용하여 블루투스 기기의 정보에 접근하는 공격이다.
○ (다)은 블루투스 장비 간의 취약한 연결 관리를 악용한 공격이다.

① (가): 블루재킹(Bluejacking), (나): 블루스나핑(Bluesnarfing), (다): 블루프린팅(Blueprinting)
② (가): 블루프린팅, (나): 블루스나핑, (다): 블루재킹
③ (가): 블루스나핑, (나): 블루프린팅, (다): 블루버깅(Bluebugging)
④ (가): 블루프린팅, (나): 블루스나핑, (다): 블루버깅

정답 4번

간단한 해설

블루스나핑은 **저장된 정보에 무단 접근**하는 공격이고, 블루버깅은 취약한 연결을 통해 **기기의 기능을 무단으로 제어**하는 공격이다. 장치를 검색하고 특성을 식별하는 블루프린팅과 구별된다.

빈칸별 해설

(가) 블루프린팅(Blueprinting): 주변 블루투스 장치를 검색하고, 장치 주소와 제공 서비스 등의 특성을 이용해 제조사·모델 등을 식별하는 활동이다. 따라서 제시문의 **장치 검색 활동**에 대응한다. 블루재킹은 주변 기기에 원치 않는 메시지 등을 보내는 행위이므로 장치 식별 활동과 다르다.

(나) 블루스나핑(Bluesnarfing): 블루투스 기기의 취약점을 이용해 주소록·일정 등 **저장된 정보를 허가 없이 읽거나 가져오는** 공격이다. 예를 들어 사용자의 승인 없이 기기의 주소록을 가져오는 경우가 이에 해당한다. 장치의 제조사나 모델을 파악하는 블루프린팅과 달리, 기기 내부 정보에 대한 무단 접근이 핵심이다.

(다) 블루버깅(Bluebugging): 블루투스 장비 사이의 취약한 연결 관리를 악용하여 **사용자 승인 없이 기기에 명령을 내리는** 공격이다. 취약한 기기에서는 전화 걸기나 문자 전송 등의 기능을 공격자가 실행할 수 있다. 저장 정보에 접근하는 데 초점을 둔 블루스나핑과 달리 기기 기능의 무단 제어까지 가능하다는 점이 특징이다.

(가)는 블루프린팅, (나)는 블루스나핑, (다)는 블루버깅으로 연결되며, 이 조합은 ④와 일치한다.

NoteBase

문 8. (가)에 들어갈 용어로 옳은 것은?

x86계열 32-bit CPU 환경에서, 구동 중인 프로세스가 사용하는 메모리 영역 중 스택 영역 관리에 사용되는 주요 레지스터는 EIP, (가), ESP가 있다. 스택 영역에는 함수 호출 시 전달되는 파라미터, 함수 실행 중 할당되는 지역변수, 함수 종료 시 되돌아갈 리턴 주소 등이 저장된다. 파라미터 및 지역변수는 (가)를 기준으로 오프셋 값을 설정하여 접근할 수 있다.

① ESI
② EAX
③ ECX
④ EBP

정답 4번

간단한 해설

파라미터와 지역변수의 위치를 일정한 오프셋으로 나타낼 때 기준이 되는 레지스터는 **EBP(베이스 포인터)**이다. ESP가 스택의 현재 꼭대기를 가리키는 반면, EBP는 함수의 스택 프레임에서 기준점으로 쓰인다.

빈칸별 해설

(가) EBP: 스택 프레임은 함수 호출에 필요한 파라미터, 지역변수, 복귀 정보 등을 담는 스택의 영역이다. 지문처럼 프레임 포인터를 사용하는 방식에서 EBP는 **현재 함수의 스택 프레임 기준 주소**를 유지한다. 따라서 파라미터와 지역변수는 EBP의 값에 각각 정해진 오프셋을 적용하여 접근할 수 있다. ESP는 스택의 현재 꼭대기를 가리키므로 데이터를 넣거나 꺼내면 값이 변하지만, EBP를 기준으로 삼으면 그때마다 변수에 접근할 오프셋을 바꿀 필요가 없다. EIP는 실행할 명령어의 주소를 가리키며, 변수의 위치를 나타내는 프레임 기준점과는 역할이 다르다.

따라서 (가)에 들어갈 레지스터는 ④의 EBP이다.

NoteBase

문 9. (가)에 들어갈 용어로 옳은 것은?

○ (가)은(는) 보안 관리자나 보안 시스템의 탐지를 피하면서 시스템을 제어하기 위해 공격의 의도로 설치되는 악성파일로, 보통 운영체제의 합법적인 명령어처럼 모아 놓은 것을 말한다.
○ (가)은(는) 공격자의 파일, 디렉터리 및 프로세스를 숨기는 것을 제외하고 합법적인 명령어처럼 동작한다.

① 랜섬웨어
② 키로거
③ 웜
④ 루트킷

정답 4번

간단한 해설

루트킷은 공격자의 파일·디렉터리·프로세스를 **숨겨 탐지를 피하면서 시스템 제어를 유지**하는 도구 모음이다. 정상적인 명령어처럼 동작하되 공격 흔적을 조회 결과에서 감추는 것이 핵심이다.

빈칸별 해설

(가) 루트킷: 공격자가 침입한 시스템에서 자신의 활동을 감추고 제어 권한을 유지하기 위해 사용하는 도구 모음이다. 지문은 정상적인 운영체제 명령어의 기능을 수행하면서도 **공격자의 파일·디렉터리·프로세스를 숨긴다**는 특징을 제시한다. 예를 들어 파일 목록을 보여 주는 명령어가 일반 파일은 그대로 표시하면서 공격자의 파일만 목록에서 제외하면, 관리자는 해당 파일이 존재해도 조회 결과로는 알아채기 어렵다. 이처럼 정상 기능을 수행하는 겉모습을 유지하면서 공격 흔적을 감추므로 탐지를 피할 수 있다.

따라서 (가)에 들어갈 용어는 ④의 루트킷이다.

NoteBase

문 10. AAA에 대한 설명으로 옳지 않은 것은?

① Authentication은 자신의 신원을 시스템에 증명하는 과정을 의미한다.

② Authorization은 지문 인식 시스템에 손가락을 댈 때 지문 자체를 의미한다.

③ Accounting은 시스템에 접근한 사용자 추적에 활용될 수 있다.

④ Accounting은 로그인했을 때 시스템이 이에 대한 기록을 남기는 활동을 의미한다.

정답 2번

간단한 해설

Authorization은 사용자가 **어떤 자원에 접근하고 어떤 작업을 할 수 있는지 권한을 부여·판단하는 인가**이다. 지문은 인가 자체가 아니라 신원을 확인하는 인증에 이용되는 생체정보이다.

선지별 해설

① O: Authentication은 사용자가 주장하는 신원이 실제 자신의 신원인지 확인하는 인증이다. 비밀번호나 지문 등을 이용하여 **자신의 신원을 시스템에 증명**하는 과정에 해당한다.

② X: Authorization은 **접근이나 작업을 허용할 권한을 부여·판단하는 인가**를 뜻한다. 예를 들어 인증된 사용자에게 특정 파일의 읽기는 허용하고 수정은 금지할 수 있다. 손가락의 지문 자체는 인가가 아니라 인증에 이용되는 생체정보이다.

③ O: Accounting은 사용자의 접속과 자원 이용 등의 활동을 기록하는 기능이다. 기록된 사용자 식별정보, 접속 시각, 이용 내역 등을 통해 **누가 언제 시스템을 이용했는지 추적**할 수 있다.

④ O: 사용자가 로그인한 시각과 계정 등의 정보를 **로그로 남기는 활동**은 Accounting에 해당한다. 로그인 과정에서 신원을 확인하는 기능은 Authentication이고, 그 접속 사실을 기록하는 기능은 Accounting이다.

NoteBase

문 11. 전자메일 시스템에서 송신 부인방지 기능을 위해 적용하는 기술은?

① 전자 서명(digital signature)

② 대칭키 암호화(symmetric encryption)

③ 앨리어스(alias)

④ 커버로스(Kerberos)

정답 1번

간단한 해설

전자 서명은 **송신자의 개인키로 서명을 생성**하고 공개키로 검증한다. 이를 통해 메일 내용과 송신자를 연결하는 증거를 남겨 **송신 부인방지**를 지원한다.

개념 구분

송신 부인방지는 송신자가 나중에 자신이 해당 메시지를 보냈다는 사실을 부인하는 것에 대비하여 증거를 확보하는 기능이다. 전자 서명에서는 송신자가 메일 내용의 해시값에 자신의 개인키로 서명을 생성하고, 수신자는 송신자의 공개키로 서명을 검증한다. 공개키가 실제 송신자의 것임이 확인되고 개인키가 안전하게 관리된다는 전제에서, **송신자만 가진 개인키로 생성한 서명**이 해당 메일에 대한 송신자의 책임을 입증하는 근거가 된다.

대칭키 암호화는 송수신자가 같은 비밀키를 공유한다. 따라서 공유키를 이용했다는 사실만으로는 **송신자만 그 메시지를 만들었다고 입증할 수 없다**. 메일 내용을 감추는 기밀성과 송신 사실을 부인하지 못하게 하는 부인방지는 구별해야 한다.

커버로스는 티켓을 이용하여 사용자나 서비스의 신원을 인증하는 프로토콜이다. **접속 주체의 신원을 확인하는 인증**과 특정 메일에 대한 송신자의 책임을 입증하는 전자 서명은 목적이 다르다.

NoteBase

문 12. OTP기기는 다음 중 어떤 수단에 해당하는가?

① Something You Know

② Something You Have

③ Something You Are

④ Something You Do

정답 2번

간단한 해설

OTP기기는 일회용 비밀번호를 생성하는 기기의 **소지 여부**를 인증에 이용하므로 'Something You Have'에 해당한다. 생성된 숫자를 입력하더라도, 미리 외운 지식을 확인하는 방식은 아니다.

개념 구분

OTP는 한 번만 사용할 수 있는 비밀번호이다. OTP기기를 이용한 인증은 사용자가 기기에 표시된 일회용 비밀번호를 제시하고, 인증 서버가 그 값의 유효성을 확인하는 방식이다. 여기서 확인하려는 것은 **해당 기기를 소지하고 있는가**이므로 'Something You Have'라는 소지 기반 인증에 해당한다.

인증 수단은 사용자가 무엇을 제시하는지를 기준으로 구분한다. 'Something You Know'는 비밀번호처럼 알고 있는 정보, 'Something You Are'는 지문처럼 신체적 특징, 'Something You Do'는 행동적 특징을 이용한다. OTP 숫자를 읽고 입력한다는 행위 자체가 행동 기반 인증을 뜻하지는 않는다. 이 경우에는 **입력 동작의 특징이 아니라 기기가 생성한 값**을 확인한다.

NoteBase

문 13. 2017년에 발표된 OWASP TOP 10의 항목 중 (가)에 해당되는 것은?

(가)은(는) 신뢰할 수 없는 데이터가 명령어나 쿼리문의 일부분으로서, 인터프리터로 보내질 때 발생한다. 공격자의 악의적인 데이터는 예기치 않은 명령을 실행하거나 올바른 권한 없이 데이터에 접근하도록 인터프리터를 속일 수 있다.

① Broken Access Control

② Broken Authentication

③ Sensitive Data Exposure

④ Injection

정답 4번

간단한 해설

신뢰할 수 없는 입력이 단순한 데이터가 아니라 **명령어나 쿼리의 일부로 해석**되어 실행 흐름을 바꾸는 취약점이 Injection이다. 지문의 권한 없는 데이터 접근은 악의적인 입력으로 인터프리터를 속인 결과이다.

빈칸별 해설

(가) Injection(인젝션): 인터프리터는 명령어나 쿼리의 의미를 해석하여 실행하는 프로그램이다. 인젝션은 신뢰할 수 없는 입력이 명령어나 쿼리에 섞여 들어가, 인터프리터가 그 입력을 **실행할 구문의 일부로 처리**하면서 발생한다. 예를 들어 사용자 입력을 SQL문에 그대로 이어 붙이는 경우, 공격자가 넣은 SQL 구문이 조회 조건을 바꾸어 허용되지 않은 데이터까지 조회하게 할 수 있다. 따라서 지문의 핵심은 데이터에 접근했다는 결과뿐 아니라, 악의적인 데이터로 인터프리터가 의도하지 않은 동작을 하게 했다는 발생 원리이다.

이 취약점은 OWASP TOP 10 2017의 A1: Injection에 해당하므로, (가)에 들어갈 항목은 ④의 Injection이다.

NoteBase

문 14. 다음 설명에 따라 진행되는 공격 유형은?

◯ 공격자는 악의적인 스크립트가 포함된 콘텐츠를 웹 애플리케이션 서버에 업로드한다.
◯ 해당 콘텐츠는 웹 애플리케이션 서버에 저장된다.
◯ 희생자는 해당 콘텐츠를 웹 애플리케이션 서버에 요청하여 수신한다.
◯ 해당 콘텐츠에 포함된 악의적인 스크립트가 희생자의 디바이스에서 실행된다.

① Stored XSS
② Reflected XSS
③ Brute Force
④ Buffer Overflow

정답 1번

간단한 해설

악성 스크립트가 포함된 콘텐츠가 **서버에 저장**되고, 이를 조회한 사용자의 기기에서 실행되는 방식은 **저장형 XSS(Stored XSS)**이다.

핵심 풀이

저장형 XSS(Stored XSS)는 공격자가 삽입한 악성 스크립트가 게시글 등 서버에 저장된 콘텐츠에 포함되어 있다가, 해당 콘텐츠를 조회한 사용자의 브라우저에서 실행되는 공격이다. 제시된 과정에서는 공격자가 콘텐츠를 업로드하고 서버가 이를 저장한 뒤, 희생자가 요청하여 받은 콘텐츠 속 스크립트가 희생자의 기기에서 실행된다. **서버는 악성 콘텐츠를 저장·전달하고, 스크립트는 사용자 측에서 실행**된다는 점을 구분해야 한다.

반사형 XSS(Reflected XSS)는 요청에 포함된 악성 스크립트가 서버의 응답에 반영되어 사용자의 브라우저에서 실행되는 방식이다. 저장형과 달리 **서버에 저장된 콘텐츠를 나중에 조회하는 과정 없이** 요청과 응답을 통해 악성 스크립트가 전달된다. 따라서 이 문항의 '콘텐츠가 서버에 저장된다'는 단서가 두 유형을 가른다.

NoteBase

문 15. CSRF에 대한 설명으로 옳은 것은?

① 취약한 컴포넌트를 악용하여 공격하면 데이터 손실이나 서버 장악 문제가 발생할 수 있는 취약점이다.

② 조작된 XPath(XML Path Language) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리를 이용해 가져올 수 있는 취약점이다.

③ 적절히 보호되지 않은 쿠키를 사용하여, 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등이 가능한 취약점이다.

④ 로그인한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 전송할 수 있는 취약점이다.

정답 4번

간단한 해설

CSRF는 **로그인한 사용자의 인증 상태를 악용하여 원하지 않는 요청을 보내게 하는** 공격이다. 브라우저가 요청에 세션 쿠키 등을 함께 보내면, 서버가 위조된 요청을 사용자의 정상 요청으로 처리할 수 있다.

선지별 해설

① X: **알려진 취약점이 있는 컴포넌트의 사용**에 관한 설명이다. 애플리케이션에 포함된 라이브러리나 프레임워크 등의 취약점을 악용하면 데이터가 손실되거나 서버가 장악될 수 있다. CSRF는 컴포넌트의 결함 자체보다 사용자의 인증 상태를 이용해 위조 요청을 실행시키는 문제이다.

② X: **XPath 삽입**에 관한 설명이다. 검증되지 않은 입력이 XPath 쿼리에 포함되면 공격자가 쿼리의 조건이나 구조를 바꾸어 허용되지 않은 XML 데이터를 조회할 수 있다. CSRF는 XPath 쿼리 조작이 아니라 사용자 브라우저를 통한 요청 위조이다.

③ X: **쿠키 변조**에 관한 설명이다. 서버가 무결성을 확인하지 않은 쿠키의 사용자 식별값이나 권한값을 신뢰하면, 공격자가 그 값을 바꾸어 다른 사용자로 위장하거나 권한을 높일 수 있다. CSRF는 쿠키 값을 바꾸는 것이 아니라 피해자의 유효한 인증 정보가 위조 요청에 함께 전송되는 점을 악용한다.

④ O: CSRF는 사이트 간 요청 위조로, 로그인한 사용자의 브라우저가 **사용자 의사와 무관한 요청**을 대상 사이트로 보내도록 유도하는 공격이다. 해당 요청에 세션 쿠키 등 인증 정보가 함께 전송되고 서버가 요청의 정당성을 충분히 확인하지 않으면, 사용자 권한으로 동작이 수행될 수 있다. 예를 들어 로그인한 사용자가 공격자가 만든 페이지에 접속했을 때, 대상 사이트로 원하지 않는 정보 변경 요청을 보내게 할 수 있다. 공격자가 세션 쿠키 값을 직접 알아내거나 변조할 필요는 없다.

NoteBase

문 16. 다음에서 설명하는 검사 도구는?

어느 한 시점에서 시스템에 존재하는 특정 경로 혹은 모든 파일에 관한 정보를 DB화하여 저장한 후,
수정·삭제·생성된 파일에 관한 정보를 알려주며, 해커들에 의한 파일의 위변조 여부를 판별할 수 있는 기능을 제공해 주는 검사 도구이다.

① Tripwire
② Burp Suite
③ Snort
④ NESSUS

정답 1번

간단한 해설

파일 정보를 저장한 뒤 이후의 상태와 비교하여 수정·삭제·생성을 찾아내는 것은 **파일 무결성 검사**이다.
Tripwire는 이 방식으로 파일의 위변조 흔적을 탐지한다.

공통 해설

Tripwire는 파일의 기준 상태를 데이터베이스로 저장하고, 이후 검사할 때 현재 상태와 대조하는 파일 무결성 검사 도구이다. 여기서 무결성 검사는 **기준 상태에서 파일이 변경되었는지** 확인하는 것을 뜻한다. 기준에 있던 파일의 정보가 달라지면 수정, 파일이 없어지면 삭제, 감시 대상 경로에 기준에 없던 파일이 나타나면 생성으로 탐지한다. 따라서 지문의 '파일 정보의 DB화'와 '수정·삭제·생성 정보 제공'은 Tripwire의 동작을 설명한다. 변경을 판단하는 기준이므로 최초 데이터베이스는 정상임을 확인한 상태에서 만들어야 한다.

NoteBase

문 17. robots.txt 파일에 대한 설명으로 옳은 것은?

① robots.txt 파일은 웹 루트 디렉터리에 위치한다.

② User-agent는 접근거부 디렉터리를 나타내는 키워드이다.

③ Disallow는 검색 엔진 종류를 나타내는 키워드이다.

④ User-agent와 Disallow는 동시에 사용할 수 없다.

정답 1번

간단한 해설

robots.txt는 웹 크롤러가 정해진 위치에서 찾을 수 있도록 **웹 루트 경로의 /robots.txt**로 제공한다. 이 파일에는 적용 대상 크롤러와 수집을 제한할 경로를 지정한다.

선지별 해설

① O: robots.txt 파일은 **웹 루트 디렉터리**에 위치하여 /robots.txt 경로로 제공된다. 크롤러는 이 정해진 경로에서 파일을 찾아 자신에게 적용되는 수집 규칙을 확인한다.

② X: User-agent는 접근을 제한할 디렉터리가 아니라 **규칙을 적용할 크롤러**를 지정하는 키워드이다. 검색 엔진의 크롤러 이름 등을 값으로 쓰며, 수집을 제한할 경로는 Disallow로 지정한다.

③ X: Disallow는 검색 엔진 종류가 아니라 **크롤링을 금지할 경로**를 지정하는 키워드이다. 예를 들어 Disallow: /private/는 해당 경로로 시작하는 주소의 수집을 제한하는 규칙이다. 규칙의 적용 대상 크롤러는 User-agent로 지정한다.

④ X: User-agent와 Disallow는 **같은 규칙 그룹에서 함께 사용**한다. User-agent로 적용 대상을 정하고 그 뒤의 Disallow로 제한할 경로를 정한다. 예를 들어 User-agent: ExampleBot 다음 줄에 Disallow: /private/를 쓰면 ExampleBot에 해당 경로의 수집 제한을 알린다.

NoteBase

문 18. 다음은 Windows 운영체제가 설치된 시스템에서 SID를 출력한 결과이다. (가), (나)에 대한 설명으로 옳지 않은 것은?

S-1-5-21-2823624781-484892517-3265479878-500
(가) (나)

① (가)는 시스템 부팅 시마다 새롭게 부여되는 시스템 ID이다.

② (나)는 RID를 나타내며, 500의 경우 Administrator임을 의미한다.

③ (나)는 RID를 나타내며, 501의 경우 Guest임을 의미한다.

④ (나)는 RID를 나타내며, 일반 사용자에게는 1,000 이상의 숫자가 부여된다.

정답 1번

간단한 해설

(가)의 시스템 식별값은 Windows 설치 시 생성되며, **부팅할 때마다 새로 부여되지 않는다**. 같은 시스템의 로컬 계정은 이 식별 부분을 공유하고, 끝의 RID로 구별된다.

선지별 해설

SID는 Windows가 사용자나 그룹 등을 식별하는 보안 식별자이다. 제시된 그림에서 (가)는 시스템을 구별하는 부분이고, (나)는 그 시스템 안에서 개별 계정을 구별하는 RID이다.

① X: (가)는 계정이 속한 시스템을 식별하는 부분이다. 로컬 계정 SID의 바탕이 되는 컴퓨터 SID는 **Windows 설치 시 생성**되며, 단순히 재부팅한다고 바뀌지 않는다. 따라서 '시스템 부팅 시마다 새롭게 부여된다'는 설명을 '설치 시 생성되어 재부팅 후에도 유지된다'로 고쳐야 한다.

② O: (나)는 SID의 마지막 구성 요소인 상대 식별자(RID)이다. **RID 500은 기본 제공 Administrator 계정**을 나타낸다. 그림에서도 (나)가 500이므로 이 SID는 해당 시스템의 기본 제공 Administrator 계정을 식별한다.

③ O: RID가 **501이면 기본 제공 Guest 계정**을 나타낸다. 같은 시스템에서 Administrator와 Guest는 앞의 시스템 식별 부분을 공유하지만, 끝의 RID가 각각 500과 501이므로 서로 구별된다.

④ O: 기본 제공 계정에 예약된 RID와 달리, 새로 만드는 일반 사용자 계정에는 **1,000 이상의 RID**가 부여된다. 이 RID를 시스템 식별 부분 뒤에 붙여 해당 계정의 SID를 구성한다.

NoteBase

문 19. 디지털 포렌식의 절차에서 사전준비 이후 단계를 순서대로 바르게 나열한 것은?

(가) 증거 수집
(나) 보관 및 이송
(다) 보고서 작성
(라) 증거 분석 및 조사

① (가) → (나) → (다) → (라)
② (가) → (나) → (라) → (다)
③ (나) → (가) → (다) → (라)
④ (나) → (라) → (가) → (다)

정답 2번

간단한 해설

수집한 디지털 증거는 **무결성을 유지하며 보관·이송**한 뒤 분석해야 한다. 보고서에는 분석 방법과 결과를 담아야 하므로 **증거 분석 및 조사 이후**에 작성한다.

올바른 순서

(가) → (나) → (라) → (다)

(가) 증거 수집: 사전준비를 마친 뒤 사건과 관련된 저장매체나 데이터를 확보한다. 이후 조사에 사용할 자료를 마련하는 단계이며, 수집 과정에서도 원래 데이터가 바뀌지 않도록 해야 한다.

(나) 보관 및 이송: 수집한 증거를 안전하게 보관하고 분석 장소로 옮긴다. 분석 전에 증거가 변조되거나 훼손되지 않도록 보호하고, **누가 언제 인수·인계했는지** 기록하여 증거의 관리 경로를 확인할 수 있게 한다.

(라) 증거 분석 및 조사: 확보하고 보존한 데이터에서 사건과 관련된 정보를 추출하고, 파일이나 기록 사이의 관계를 조사한다. 분석 대상의 무결성을 유지하면서 사건의 경위 등을 뒷받침할 근거를 찾아야 하므로 증거 확보와 안전한 보관·이송이 선행한다.

(다) 보고서 작성: 증거를 수집·관리한 과정, 사용한 분석 방법, 발견한 사실과 결론을 문서로 정리한다. 결론이 어떤 자료와 분석에 근거하는지 제시해야 하므로 **분석 결과가 나온 뒤** 작성한다.

NoteBase

문 20. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

○ CVE(Common Vulnerabilities and Exposure)는 공개적으로 알려진 소프트웨어의 보안취약점을 가리키는 고유 표기를 의미한다.
○ 취약점명은 CVE－(가)－(나) 형식으로 구성되어 있다.

① (가): 일련번호, (나): 소프트웨어 버전
② (가): 연도, (나): 소프트웨어 버전
③ (가): 일련번호, (나): 연도
④ (가): 연도, (나): 일련번호

정답 4번

간단한 해설

CVE 식별자는 **CVE-연도-일련번호** 형식이다. 마지막 숫자 부분은 소프트웨어 버전이 아니라 개별 취약점을 구별하는 번호이다.

빈칸별 해설

CVE는 보안취약점을 고유하게 식별하기 위해 'CVE-연도-일련번호' 형식의 식별자를 사용한다.

(가) 연도: CVE 접두어 바로 뒤에는 **네 자리 연도**가 온다. 일련번호는 그다음에 배치되므로, (가)에 일련번호를 넣으면 두 구성 요소의 위치가 바뀐다.

(나) 일련번호: 연도 뒤에는 **개별 취약점을 구별하는 일련번호**가 온다. 이는 취약점의 식별을 위한 번호이며, 해당 소프트웨어의 버전을 나타내는 자리가 아니다.

따라서 (가)는 연도, (나)는 일련번호이며, ④의 조합과 일치한다.

NoteBase