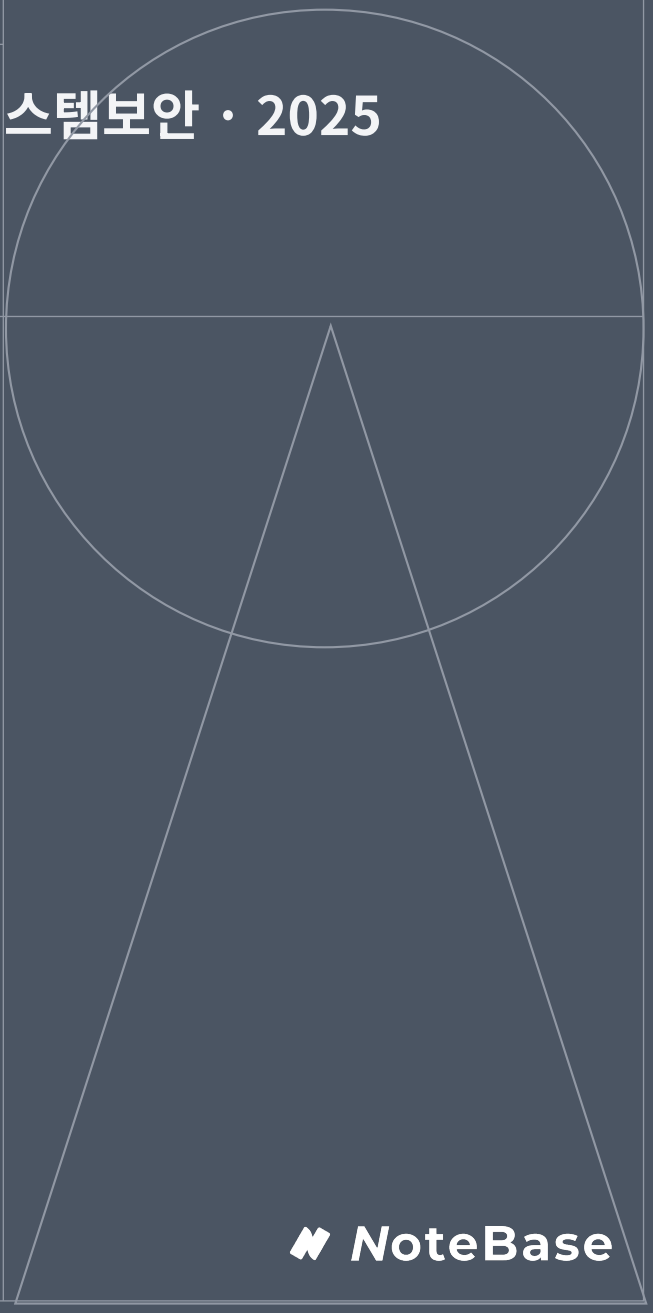
기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2025



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2025

공무원/국가직/9급 · 정보시스템보안 · 2025

문 1. 취약점에 대한 보안 패치가 나오지 않은 시점에서 이루어지는 공격을 의미하는 것은?

① 제로데이(Zero-day)

② 사회공학(Social Engineering)

③ 분산 서비스 거부(DDoS)

④ 무차별 대입(Brute Force)

정답 1번

간단한 해설

제로데이 공격은 취약점을 수정할 **보안 패치가 제공되기 전에** 그 취약점을 악용하는 공격이다.

개념 구분

제로데이(Zero-day): **보안 패치가 아직 나오지 않은 취약점**을 악용하는 공격이다. 문제의 핵심 조건은 공격이 이루어지는 시점에 해당 취약점을 수정할 패치가 제공되지 않았다는 것이다.

사회공학(Social Engineering): **사람의 심리나 신뢰를 이용**하여 비밀 정보를 얻거나 특정 행동을 하도록 유도하는 기법이다. 패치의 제공 여부가 아니라 사람을 속이는 방식에 초점을 둔다.

분산 서비스 거부(DDoS): 여러 공격원에서 트래픽이나 요청을 보내 **정상적인 서비스 이용을 방해**하는 공격이다. 공격원의 분산과 서비스 가용성 침해가 특징이다.

무차별 대입(Brute Force): 비밀번호나 암호키 등의 **가능한 후보를 반복적으로 시도**하여 맞는 값을 찾는 방식이다. 패치가 나오기 전이라는 시점이 아니라 후보를 탐색하는 방식을 나타낸다.

NoteBase

문 2. 침입자에게 거짓 자원을 실제 자원처럼 보이도록 하여 공격을 유도하고, 침입자에 대한 정보를 얻기 위한 시스템은?

① IPS

② DMZ

③ Firewall

④ Honeypot

정답 4번

간단한 해설

허니팟(Honeypot)은 **가짜 자원으로 공격을 유인**하고, 그 과정에서 침입자의 행동과 공격 기법에 관한 정보를 수집하는 시스템이다.

개념 구분

허니팟(Honeypot)은 실제 운영 자원처럼 보이는 미끼 시스템을 제공한다. 침입자가 이 시스템에 접근하면 접속 시도와 수행한 행위 등을 기록하여 공격 기법을 분석할 수 있다. 문제의 '거짓 자원을 실제 자원처럼 보이도록' 한다는 것은 **미끼를 이용한 공격 유인**을 뜻하며, 침입자 정보 수집이라는 목적과 함께 허니팟을 가리킨다.

IPS는 침입 시도를 탐지하고 차단하는 시스템이며, Firewall은 보안 정책에 따라 통신을 허용하거나 차단한다. 이들의 주된 역할은 **위협 차단과 접근 통제**이므로, 가짜 자원을 제공하여 공격을 유도한다는 단서와 구별된다.

DMZ는 외부에 공개할 서버 등을 내부망과 분리하여 배치하는 **별도의 네트워크 구역**이다. 구역을 분리하는 구성과 미끼 시스템으로 침입자의 행동을 관찰하는 기능을 구별해야 한다.

NoteBase

문 3. 다음에서 설명하는 공격은?

게시판이나 이메일 등에 악의적인 스크립트를 삽입하여
게시글이나 이메일을 읽는 사용자의 쿠키를 탈취하는 공격 기법이다.

① XSS
② SQL Injection
③ DNS Spoofing
④ IP Spoofing

정답 1번

간단한 해설

게시글이나 이메일에 삽입한 악성 스크립트로 이를 읽는 사용자의 쿠키를 탈취한다는 점이 **XSS**의 식별 단서이다.

공통 해설

XSS(Cross-Site Scripting)는 웹 콘텐츠에 악성 스크립트를 삽입하여, 이를 열람하는 사용자의 브라우저에서 실행되게 하는 공격이다. 사용자가 신뢰하는 사이트의 콘텐츠로 악성 코드가 전달되면 브라우저는 이를 해당 사이트의 스크립트로 실행할 수 있다. 이때 스크립트가 접근할 수 있는 쿠키를 공격자에게 전송하면 쿠키 탈취가 일어난다. 따라서 지문의 공격을 식별하는 기준은 쿠키 탈취라는 결과만이 아니라 **콘텐츠에 삽입한 악성 스크립트를 사용자 측에서 실행시키는 방식**이며, 이 설명에 대응하는 명칭은 XSS이다.

NoteBase

문 4. 리눅스 커널의 부팅 과정에서 발생하는 로그를 확인할 수 있는 명령어는?

① cron

② dmesg

③ wtmp

④ sulog

정답 2번

간단한 해설

dmesg는 커널의 링 버퍼에 저장된 메시지를 출력한다. 부팅 중 장치 인식과 초기화 과정에서 발생한 커널 메시지도 이를 통해 확인할 수 있다.

핵심 풀이

dmesg는 **커널 링 버퍼의 메시지를 출력**하는 명령어이다. 커널은 부팅하면서 장치를 인식하고 드라이버를 초기화하는 등의 과정에서 메시지를 남기므로, dmesg로 해당 기록을 확인할 수 있다. 부팅이 끝난 뒤 발생한 커널 메시지도 출력 대상에 포함된다.

wtmp는 로그인·로그아웃과 시스템 재부팅 등의 이력을 저장하는 파일이다. 재부팅 시점이 기록될 수는 있지만, **커널의 장치 인식·초기화 메시지**를 확인하는 명령어와는 구별된다.

sulog는 su를 이용한 사용자 전환 관련 활동을 기록하는 로그 파일이다. 커널의 부팅 과정을 출력하는 명령어가 아니다.

cron은 정해진 일정에 따라 작업을 실행하는 데 쓰이는 데몬이다. 커널 메시지를 조회하는 기능과는 다르다.

NoteBase

문 5. 다음에서 설명하는 암호 알고리즘은?

국내의 국가보안기술연구소 주도로 학계, 연구소, 정부기관 등의 암호 전문가들이 공동 개발한 암호화 알고리즘으로 KS인증을 획득하였다.

① ARIA

② DES

③ SEED

④ IDEA

정답 1번

간단한 해설

국가보안기술연구소 주도로 **학계·연구소·정부기관이 공동 개발**했다는 설명은 ARIA의 개발 배경에 해당한다.

공통 해설

ARIA는 국가보안기술연구소 주도로 학계·연구소·정부기관의 암호 전문가들이 공동 개발한 국산 대칭키 블록 암호로, 국가표준(KS)으로 제정되었다. ARIA라는 이름도 Academy(학계), Research Institute(연구소), Agency(정부기관)에서 따온 것으로, 이러한 공동 개발 배경을 나타낸다. SEED 역시 국산 블록 암호이지만 KISA가 개발한 알고리즘이다. 따라서 단순히 국산이라는 점보다 **국가보안기술연구소 주도의 학·연·관 공동 개발**이라는 조건이 지문의 설명을 ARIA와 연결하는 기준이다.

NoteBase

문 6. 리버스 엔지니어링 기법에 해당하는 것은?

① 난독화

② 언패킹

③ 디지털 서명

④ 안티 디버깅

정답 2번

간단한 해설

언패킹은 압축·암호화 등으로 패킹된 실행 파일에서 **분석할 실행 코드를 복원**하는 기법이다. 숨겨진 코드의 구조와 동작을 살펴볼 수 있게 하므로 리버스 엔지니어링에 사용된다.

선지별 해설

① X: 난독화는 프로그램의 기능을 유지하면서 코드의 표현이나 구조를 복잡하게 바꾸어 **분석을 어렵게 하는** 기법이다. 내부 동작을 파악하는 리버스 엔지니어링을 방해하며, 분석자는 난독화된 코드를 해석하거나 난독화를 해제해야 한다.

② O: 언패킹은 압축·암호화 등으로 패킹된 실행 파일에서 **원래 실행 코드를 복원**하는 기법이다. 패킹 상태에서는 코드가 그대로 드러나지 않으므로, 이를 풀어야 실제 명령과 실행 흐름을 분석할 수 있다. 따라서 언패킹은 리버스 엔지니어링 과정에 사용된다.

③ X: 디지털 서명은 서명자의 개인키로 생성하고 대응하는 공개키로 검증하여 **데이터의 무결성과 출처의 진위**를 확인하는 암호 기술이다. 프로그램 내부 구조를 복원하거나 동작을 분석하는 리버스 엔지니어링 기법과는 목적이 다르다.

④ X: 안티 디버깅은 디버거의 존재나 디버깅 상태를 탐지하고 실행을 중단하거나 동작을 바꾸어 **디버거를 이용한 분석을 방해**하는 기법이다. 실행 과정을 추적하여 동작을 파악하는 디버깅과 구별해야 한다.

NoteBase

문 7. 다음에서 설명하는 공격은?

소유자가 root이고 SetUID 비트를 가진 프로세스가 생성한 임시 파일의 처리가 완료되기 전에 공격자의 프로세스가 동일한 이름의 심볼릭 링크 파일을 생성하여 root 소유의 파일 내용을 수정하는 공격 기법이다.

① Race Condition
② Format String
③ Heap Overflow
④ Stack Overflow

정답 1번

간단한 해설

임시 파일 처리가 끝나기 전에 공격자가 심볼릭 링크를 끼워 넣어 접근 대상을 바꾸므로, 공격의 성립 여부가 **두 프로세스의 실행 순서와 시점**에 달려 있다. 이러한 경쟁 조건을 이용하는 공격이 Race Condition이다.

공통 해설

Race Condition(경쟁 조건)은 여러 프로세스나 스레드가 공유 자원에 접근할 때, **실행 순서나 시점에 따라 처리 결과가 달라지는** 상황이다. 공격자는 정상 처리 도중에 개입하여 공유 자원의 상태를 바꾸고, 이후 처리가 의도와 다르게 이루어지도록 한다.

문제의 공유 자원은 임시 파일의 이름으로 접근하는 파일이다. 심볼릭 링크는 다른 파일의 경로를 가리키므로, 임시 파일 처리 사이에 같은 이름의 링크가 개입하면 이후 접근이 링크가 가리키는 root 소유 파일로 향할 수 있다. 이때 root 권한으로 동작하는 프로세스가 쓰기를 수행하면 공격자가 직접 수정할 권한이 없는 파일도 변경될 수 있다. 즉, 정상 프로세스의 파일 처리와 공격자 프로세스의 링크 생성 사이의 시점 경쟁을 이용하므로 Race Condition에 해당한다.

NoteBase

문 8. 리눅스에서 파일 시스템의 상태를 점검하고, 문제가 있을 때 복구하는 기능을 가진 명령어는?

① fdisk

② df

③ fsck

④ fstab

정답 3번

간단한 해설

fsck는 파일 시스템의 오류를 검사하고 복구하는 명령어이다. 디스크 사용량을 보여 주는 df와 달리 **파일 시스템의 일관성**을 점검한다.

개념 구분

fsck: 파일 시스템의 관리 정보가 서로 일치하는지 검사하고, 발견된 오류를 복구하는 데 사용하는 명령어이다. 문제의 **'상태를 점검하고, 문제가 있을 때 복구'**한다는 기능에 해당한다.

다른 후보와의 구분: fdisk는 디스크의 파티션을 조회·설정하는 명령어이고, df는 파일 시스템의 전체 용량과 사용량·남은 공간을 표시하는 명령어이다. fstab은 파일 시스템을 어디에 어떤 옵션으로 마운트할지 등을 기록한 **설정 파일**이다. 이들은 파일 시스템의 오류를 검사하고 복구하는 fsck와 역할이 다르다.

NoteBase

문 9. 다음 리눅스 시스템의 '/etc/passwd' 파일 내용에 대한 설명으로 옳지 않은 것은?

root : x : 0 : 0 : root : /root : /bin/bash

① 계정명은 'root'이다.
② 패스워드는 'x'이다.
③ 홈 디렉터리는 '/root'이다.
④ 기본 shell 설정은 'bash'이다.

정답 2번

간단한 해설

두 번째 필드의 'x'는 실제 패스워드가 아니라, 패스워드 해시가 **/etc/shadow에 별도로 저장됨**을 나타내는 표시이다. 따라서 패스워드가 'x'라는 뜻으로 해석할 수 없다.

선지별 해설

/etc/passwd의 각 행은 콜론(:)으로 구분된 일곱 필드로 구성된다. 필드 순서는 계정명, 패스워드 필드, 사용자 ID(UID), 그룹 ID(GID), 사용자 설명, 홈 디렉터리, 로그인 셸이다.

① O: /etc/passwd의 첫 번째 필드는 **계정명**이다. 제시된 행의 첫 번째 값이 'root'이므로 계정명은 'root'이다.

② X: 두 번째 필드의 'x'는 패스워드 자체가 아니라 **패스워드 해시를 /etc/shadow에 저장한다는 표시**이다. 따라서 이 행만으로 실제 패스워드를 알 수 없으며, 패스워드가 'x'라는 설명은 잘못되었다.

③ O: 여섯 번째 필드는 사용자의 **홈 디렉터리**이다. 제시된 값이 '/root'이므로 이 계정의 홈 디렉터리는 '/root'이다.

④ O: 일곱 번째 필드는 로그인할 때 실행할 **기본 셸의 경로**이다. '/bin/bash'가 지정되어 있으므로 기본 셸은 bash이다.

NoteBase

문 10. 2021년에 발표된 OWASP Top 10의 항목 중, 서버가 적절한 검증 절차를 거치지 않은 요청을 처리하여, 접근통제를 우회하는 방식으로 서버의 내부 데이터가 탈취될 수 있는 취약점은?

① XXE

② SSRF

③ Cryptographic Failures

④ Insufficient Logging & Monitoring

정답 2번

간단한 해설

SSRF는 공격자가 조작한 주소로 **서버가 대신 요청을 보내게 하는** 취약점이다. 외부에서 직접 접근할 수 없는 내부 자원에도 서버를 통해 접근할 수 있어, 접근통제를 우회하고 내부 데이터가 유출될 수 있다.

핵심 풀이

SSRF(Server-Side Request Forgery, 서버 측 요청 위조)는 OWASP Top 10:2021의 A10 항목이다. 웹 애플리케이션이 사용자에게 받은 URL을 적절히 검증하지 않고 자원을 가져오면, 공격자는 **요청 목적지를 내부 서비스 등으로 바꾸어 서버가 접근하게** 할 수 있다. 예를 들어 외부 자료를 가져오는 기능에 내부 서비스의 주소를 입력했을 때, 서버가 그 주소로 요청하고 응답을 공격자에게 반환한다면 내부 데이터가 유출될 수 있다. 문제의 '검증되지 않은 요청 처리'와 '접근통제 우회'는 이러한 작동 방식을 가리킨다.

XXE는 **XML 처리기가 외부 엔터티를 해석하는 과정**을 악용하는 취약점이다. XXE를 통해 SSRF가 발생할 수도 있지만, 문제에는 XML이나 외부 엔터티 처리라는 단서가 없다. 이 문항은 서버를 통해 의도하지 않은 목적지로 요청을 보내 내부 자원에 접근하는 SSRF를 묻는다.

NoteBase

문 11. HTTP 상태 코드에 대한 설명으로 옳지 않은 것은?

① 301: Moved Permanently

② 304: Not Modified

③ 401: Unauthorized

④ 405: Request Entity Too Large

정답 4번

간단한 해설

④는 상태 코드와 의미를 잘못 연결했다. **405는 Method Not Allowed**로, 해당 자원에 요청한 HTTP 메서드가 허용되지 않음을 뜻한다. 요청 본문의 크기가 너무 크다는 'Request Entity Too Large'에 해당하는 코드는 **413**이다.

선지별 해설

① O: 301 Moved Permanently는 요청한 자원이 **새 URI로 영구적으로 이동**했음을 나타낸다. 이후에는 새 URI를 사용하도록 알리는 응답이며, 새 위치는 Location 헤더로 안내한다.

② O: 304 Not Modified는 조건부 GET 요청에서 자원이 클라이언트가 가진 저장본에 비해 **변경되지 않았음**을 나타낸다. 서버는 응답 본문을 다시 보내지 않으며, 클라이언트는 기존에 캐시한 내용을 재사용할 수 있다.

③ O: 401 Unauthorized는 요청한 자원에 접근하려면 **유효한 인증 정보가 필요**함을 나타낸다. 인증 정보가 없거나 제시한 인증 정보가 유효하지 않을 때 사용하며, 서버는 WWW-Authenticate 헤더로 필요한 인증 방식을 알린다.

④ X: 405의 의미는 **Method Not Allowed**이다. 서버가 해당 자원에 대해 요청받은 HTTP 메서드를 허용하지 않는 경우에 사용하며, Allow 헤더로 허용되는 메서드를 알린다. 'Request Entity Too Large'는 요청 본문이 서버가 처리할 수 있는 크기보다 큰 경우를 뜻하므로, 선지의 코드는 **413으로 고쳐야 한다**.

NoteBase

문 12. 삽입된 악성 스크립트를 통해 사용자가 인지하지 못하는 상태에서 사용자의 권한으로 서버에 공격자가 의도한 요청을 하는 공격은?

① Slowloris

② CSRF

③ Heartbleed

④ DNS Cache Poisoning

정답 2번

간단한 해설

CSRF는 **인증된 사용자의 권한을 이용해 원하지 않는 요청을 서버에 보내게 하는** 공격이다. 문제에서는 악성 스크립트의 삽입 자체보다 사용자가 의도하지 않은 요청이 사용자 권한으로 실행된다는 점이 결정적이다.

핵심 풀이

CSRF(Cross-Site Request Forgery, 사이트 간 요청 위조)는 인증된 사용자의 브라우저를 이용하여 공격자가 의도한 요청을 서버에 보내게 하는 공격이다. 쿠키 기반 인증에서는 브라우저가 해당 사이트로 요청을 보낼 때 세션 쿠키를 함께 전송할 수 있으므로, 서버가 요청의 진위를 충분히 확인하지 않으면 **사용자가 직접 의도한 요청처럼 처리**할 수 있다. 예를 들어 로그인한 사용자가 악성 페이지를 열었을 때 본인도 모르게 계정의 이메일 주소 변경 요청이 전송되는 경우이다.

XSS와의 구분: XSS는 웹페이지에 삽입된 악성 스크립트가 사용자의 브라우저에서 실행되도록 하는 공격이다. CSRF의 핵심은 **인증된 사용자 권한으로 요청을 위조**하는 데 있다. 문제의 '삽입된 악성 스크립트'는 요청을 유발하는 수단으로 이해하며, CSRF가 반드시 스크립트 삽입을 필요로 하는 것은 아니다.

NoteBase

문 13. TLS에 속한 프로토콜 중 세션을 활성 상태로 유지하는 목적으로 사용하는 것은?

① Alert Protocol

② Connection Protocol

③ Heartbeat Protocol

④ Application Data Protocol

정답 3번

간단한 해설

Heartbeat Protocol은 요청과 응답을 주고받아 상대방이 통신 가능한 상태인지 확인하고, 응용 데이터를 계속 보내지 않아도 연결을 유지하는 keep-alive 기능을 제공한다.

개념 구분

Heartbeat Protocol은 TLS의 확장 프로토콜로, **재협상 없이 연결을 유지**하는 keep-alive 기능을 제공한다. HeartbeatRequest를 보내고 상대방으로부터 HeartbeatResponse를 받는 방식으로 통신 가능 여부를 확인하므로, 문제의 '세션을 활성 상태로 유지'하는 목적에 해당한다.

Alert Protocol은 오류나 연결 종료 등의 **상태를 알리는** 데 사용한다. 연결이 살아 있는지 확인하기 위한 요청·응답 기능과 구별한다.

Application Data Protocol은 TLS로 보호되는 **실제 응용 데이터를 전달**하는 데 사용한다. 응용 데이터가 없는 상황에서도 연결 유지용 메시지를 주고받는 Heartbeat Protocol과 목적이 다르다.

NoteBase

문 14. 프로세스에서 사용하는 메모리 영역의 위치를 랜덤하게 배치하는 기법은?

① X.509

② PAM

③ ASLR

④ ASBR

정답 3번

간단한 해설

ASLR(주소 공간 배치 무작위화)은 프로세스가 사용하는 메모리 영역의 주소를 무작위로 배치하여 공격자가 목표 주소를 예측하기 어렵게 하는 기법이다.

핵심 풀이

ASLR(Address Space Layout Randomization)은 프로세스의 가상 주소 공간에서 스택·힙·라이브러리 등의 배치 주소를 무작위화하는 기법이다. 특정 코드나 데이터가 늘 같은 주소에 있으면 공격자가 그 주소를 이용하기 쉽다. ASLR은 **메모리 영역의 위치를 예측하기 어렵게** 하여, 알려진 주소에 의존하는 공격의 성공 가능성을 낮춘다. 문제의 '메모리 영역의 위치를 랜덤하게 배치'한다는 설명이 이에 해당한다.

이름이 비슷한 ASBR(Autonomous System Boundary Router)은 **자율 시스템 경계 라우터**를 뜻한다. OSPF에서 외부 경로 정보를 내부에 알리는 역할을 하므로, 프로세스의 메모리 주소 배치를 바꾸는 ASLR과 구별된다.

NoteBase

문 15. 다음에서 설명하는 윈도 운영체제의 레지스트리 루트키는?

현재 시스템에 로그온하고 있는 사용자에 대한 구성 정보를 저장한다.

① HKEY_CLASSES_ROOT
② HKEY_CURRENT_USER
③ HKEY_LOCAL_MACHINE
④ HKEY_CURRENT_CONFIG

정답 2번

간단한 해설

HKEY_CURRENT_USER는 **현재 로그온한 사용자**의 구성 정보를 담는 레지스트리 루트키이다.

공통 해설

레지스트리 루트키를 구분할 때는 구성 정보가 적용되는 대상을 확인한다. HKEY_CURRENT_USER는 **현재 로그온한 사용자 개인에게 적용되는 설정**을 담으며, 색상·프린터·응용 프로그램의 사용자별 환경 설정 등이 여기에 속한다. 지문의 '현재 시스템에 로그온하고 있는 사용자'는 이러한 사용자별 설정의 주체를 가리키므로 HKEY_CURRENT_USER에 해당한다.

NoteBase

문 16. PGP에 대한 설명으로 옳지 않은 것은?

① IETF에 의해 개발되었다.

② 전자 서명을 통해 인증을 제공한다.

③ ZIP 알고리즘으로 압축을 제공한다.

④ 대칭 키 암호를 통해 기밀성을 제공한다.

정답 1번

간단한 해설

PGP는 **필 짐머만(Philip Zimmermann)**이 개발한 전자우편 보안 프로그램이다. 개발 주체를 IETF로 설명한 부분이 잘못되었다.

선지별 해설

① X: PGP는 **필 짐머만(Philip Zimmermann)**이 개발하여 1991년에 처음 공개한 프로그램이다. 'IETF에 의해 개발되었다'는 설명은 개발 주체를 잘못 연결한 것이다.

② O: 송신자는 메시지의 해시값을 바탕으로 자신의 개인 키로 전자 서명을 생성하고, 수신자는 송신자의 공개 키로 이를 검증한다. 이를 통해 **송신자 인증과 메시지 무결성 확인**이 가능하다.

③ O: PGP는 **ZIP 방식의 압축**을 지원하여 전송하거나 저장할 데이터의 크기를 줄인다. 서명과 암호화를 함께 적용할 때는 일반적으로 서명한 뒤 압축하고, 그 결과를 암호화한다.

④ O: PGP는 메시지 본문을 **대칭 키인 세션 키로 암호화**하여 기밀성을 제공한다. 공개 키 방식으로 수신자에게 보낼 때는 이 세션 키를 수신자의 공개 키로 암호화하며, 수신자는 자신의 개인 키로 세션 키를 복구한 뒤 본문을 복호화한다.

NoteBase

문 17. nmap 명령어의 옵션에 대한 설명으로 옳지 않은 것은?

① -O 옵션은 운영체제를 확인한다.

② -R 옵션은 RPC 스캔을 실시한다.

③ -n 옵션은 DNS Lookup을 하지 않는다.

④ -v 옵션은 스캔 결과를 상세하게 출력한다.

정답 2번

간단한 해설

-R은 RPC 스캔이 아니라 **모든 대상 IP 주소에 대해 역방향 DNS 조회를 시도**하는 옵션이다. 역방향 DNS 조회는 IP 주소에 대응하는 호스트 이름을 알아내는 작업이다.

선지별 해설

① O: -O는 **운영체제 탐지**를 활성화한다. 대상에게 보낸 TCP·UDP 패킷의 응답 특성을 운영체제 지문 데이터베이스와 비교하여 운영체제를 추정한다.

② X: -R은 **모든 대상 IP 주소에 대해 역방향 DNS 조회를 시도**하는 옵션이다. 기본적으로는 살아 있는 것으로 확인된 대상에 대해 조회하지만, -R을 지정하면 그 여부와 관계없이 조회를 시도한다. RPC 스캔에 쓰이던 옵션은 -sR이며, 현재는 서비스·버전 탐지 옵션인 -sV의 별칭으로 통합되어 있다.

③ O: -n은 **역방향 DNS 조회를 생략**하는 옵션이다. 대상 IP 주소를 호스트 이름으로 변환하는 조회를 하지 않으므로 DNS 응답을 기다리는 시간을 줄일 수 있다.

④ O: -v는 **출력의 상세 수준을 높이는** 옵션이다. 발견한 열린 포트나 스캔 진행 상황 등 기본 출력보다 많은 정보를 보여 준다.

NoteBase

문 18. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

TCP 포트 번호 (가)을 사용하는 (나)을/를 통해, 사용자는 전자우편 서버에 메일 박스 생성, 삭제 및 이름 변경이 가능하다.

① (가): 110, (나): SMTP

② (가): 143, (나): SMTP

③ (가): 110, (나): IMAP

④ (가): 143, (나): IMAP

정답 4번

간단한 해설

서버의 메일함을 생성·삭제하거나 이름을 바꾸는 기능은 **IMAP**이 제공하며, 기본 TCP 포트는 **143번**이다.

빈칸별 해설

(가) 143: 지문의 메일함 관리 기능을 제공하는 IMAP의 **기본 TCP 포트는 143번**이다. 110번은 메일을 내려받는 데 사용하는 POP3의 기본 TCP 포트이므로 IMAP과 연결할 수 없다.

(나) IMAP: 전자우편을 서버에 보관하면서 조회하고 관리하는 프로토콜이다. **서버의 메일함 생성·삭제·이름 변경**을 지원하므로 지문의 기능에 해당한다. SMTP는 전자우편을 보내고 서버 사이에서 전달하는 프로토콜이므로, 이 메일함 관리 기능을 설명하는 빈칸에는 맞지 않는다.

따라서 (가)는 143, (나)는 IMAP이며, 이 조합은 ④와 일치한다.

NoteBase

문 19. 빈칸에 들어갈 내용은?

프로그램을 실행시키기 위한 가상의 메모리 공간이 할당되면, 할당된 메모리 공간은 여러 영역으로 나뉘어 관리된다. 그중 _____은 프로세스 로직이 실행되는 데 필요한 파라미터, 지역변수, 반환 주소 등이 저장된다.

① 텍스트 영역
② 힙 영역
③ 스택 영역
④ 데이터 영역

정답 3번

간단한 해설

함수 호출에 필요한 파라미터, 지역변수, 반환 주소 등을 보관하는 곳은 **스택 영역**이다. 호출된 함수의 실행이 끝나면 해당 호출에 사용한 스택 공간이 회수된다.

빈칸별 해설

빈칸: 스택 영역. 함수가 호출되면 그 호출을 위한 스택 프레임이 만들어지며, 여기에 파라미터, 지역변수, 반환 주소 등이 저장된다. 반환 주소는 **함수가 끝난 뒤 실행을 이어 갈 위치**를 나타낸다. 예를 들어 함수 A가 B를 호출하면 B의 호출 정보를 스택에 쌓고, B가 끝나면 그 정보를 정리하여 A로 돌아간다.

텍스트 영역은 실행할 명령어를, 데이터 영역은 전역변수와 정적변수 등을 저장하는 영역이다. 힙 영역은 실행 중 동적으로 할당하는 메모리에 쓰인다. 지문의 핵심은 단순히 데이터를 저장한다는 점이 아니라 **함수 호출에 필요한 정보를 저장한다**는 점이다.

따라서 빈칸에는 ③의 '스택 영역'이 들어간다.

NoteBase

문 20. 다음 명령을 수행한 후 '/directory'에 부여된 권한은?

chmod 1111 /directory

① Read
② SetGID
③ SetUID
④ Sticky Bit

정답 4번

간단한 해설

chmod의 네 자리 숫자 모드에서 맨 앞자리는 특수 권한을 나타내며, 그 값이 1이면 **Sticky Bit**를 설정한다. 뒤의 111은 소유자·그룹·기타 사용자에게 각각 디렉터리 탐색 권한을 지정한다.

핵심 풀이

1111의 자릿값: chmod의 숫자 모드는 8진수로 해석한다. 네 자리로 쓰면 맨 앞자리는 특수 권한, 뒤의 세 자리는 차례로 소유자·그룹·기타 사용자의 일반 권한을 나타낸다. 특수 권한의 값은 SetUID가 4, SetGID가 2, **Sticky Bit가 1**이다. 따라서 chmod 1111 /directory는 /directory에 Sticky Bit를 설정한다. 뒤의 각 1은 실행 권한이며, 디렉터리에서는 경로를 따라 접근하는 탐색 권한을 뜻한다. 읽기(Read)는 일반 권한 자리의 값 4에 해당하므로 숫자 1과 구별한다.

Sticky Bit의 기능: 디렉터리에 설정하면 일반 사용자가 그 안의 파일을 삭제하거나 이름을 바꾸는 행위를 **파일 소유자 또는 디렉터리 소유자 등으로 제한**한다. 이는 다른 사용자의 파일을 함부로 삭제하지 못하게 하는 제한이며, 쓰기 권한을 새로 부여하는 기능은 아니다. 따라서 뒤의 111이 지정하는 탐색 권한만으로 파일 생성·삭제가 허용되는 것은 아니다.

NoteBase